Второй раздел лабораторных работ предполагает знакомство студентов с защитой персональных данных. Данный раздел содержит 3 лабораторные работы, которые соответствуют стадиям создания системы защиты информации, а именно:

1. Предпроектная стадия, включающая предпроектное обследование объекта информатизации, разработку аналитического обоснования необходимости создания СЗИ и технического (частного технического) задания на ее создание

2. Стадия проектирования (разработки проектов), включающая разработку СЗИ в составе объекта информатизации

3. Стадия ввода в действие СЗИ, включающая опытную эксплуатацию и приемо-сдаточные испытания средств защиты информации, а также аттестацию объекта информатизации на соответствие требованиям безопасности информации

Оглавление

Лабораторная работа №4 . Предпроектная стадия. Обследование объекта информатизации

Термины и определения:

Персональные данные (ПДн)– это любая информация о людях. Это могут быть персональные данные сотрудников, данные пациентов (если речь идет о медучреждении), данные граждан (если речь идет о госучреждении) и т.д.

Контролируемая зона (КЗ) – пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

Информационная система персональных данных (ИСПДн) – это совокупность программных и технических средств (компьютеры, принтеры, сканеры, коммутационное оборудование и т.д.) на которых обрабатываются персональные данные.

Угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

Модель угроз (безопасности информации) – физическое, математическое, описательное представление свойств или характеристик угроз безопасности информации.

ИСПДн-С - информационная система, обрабатывающая специальные категории персональных данных, если в ней обрабатываются персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъектов персональных данных;

ИСПДн-О – информационная система, обрабатывающая общедоступные персональные данные, если в ней обрабатываются персональные данные субъектов персональных данных, полученные только из общедоступных источников персональных данных, созданных в соответствии со статьей 8 Федерального закона "О персональных данных".

ИСПДн-Б - информационная система, обрабатывающая биометрические персональные данные, если в ней обрабатываются сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных, и не обрабатываются сведения, относящиеся к специальным категориям персональных данных.

ИСПДн-И - информационная система, обрабатывающая иные категории персональных данных, если в ней не обрабатываются персональные данные специальные, общедоступные и биометрические.

«Базовая модель» - Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. (Утверждена заместителем директора ФСТЭК России 15.02.2008 г. ДСП.).

АРМ - автоматизированное рабочее место.

ПО - программное обеспечение.

МИО – международный информационный обмен.

БПДн – безопасность персональных данных.

Работы, выполняемые на предпроектной стадии:

- Устанавливается необходимость обработки информации на данном объекте информатизации;
- Определяется перечень сведений конфиденциального характера, подлежащих защите;

- Определяются (уточняются) угрозы безопасности информации и модель вероятного нарушителя применительно к конкретным условиям функционирования объекта;
- Определяются условия расположения объекта информатизации относительно границ контролируемой зоны;
- Определяются конфигурация и топология сети в целом и их отдельных компонентов, физические, функциональные и технологические связи сети с другими системами различного уровня и назначения;
- Определяются конкретные технические средства и системы, предполагаемые к использованию в разрабатываемой автоматизированной системы, условия их расположения, их программные средства
- Определяются режимы обработки информации в автоматизированной системы в целом и в отдельных компонентах
- Определяется класс защищенности автоматизированной системы
- Определяется степень участия персонала в информации, характер их взаимодействия между собой и со службой безопасности
- Определяются мероприятия по обеспечению конфиденциальности информации на этапе проектирования объекта информатизации

Характеристики ИСПДн, обусловливающие возникновение угроз БПДн:

1) структура ИСПДн:

а) автономные ИСПДн АРМ;

Рисунок 1. Автономные ИСПДн АРМ

b) локальные ИСПДн:

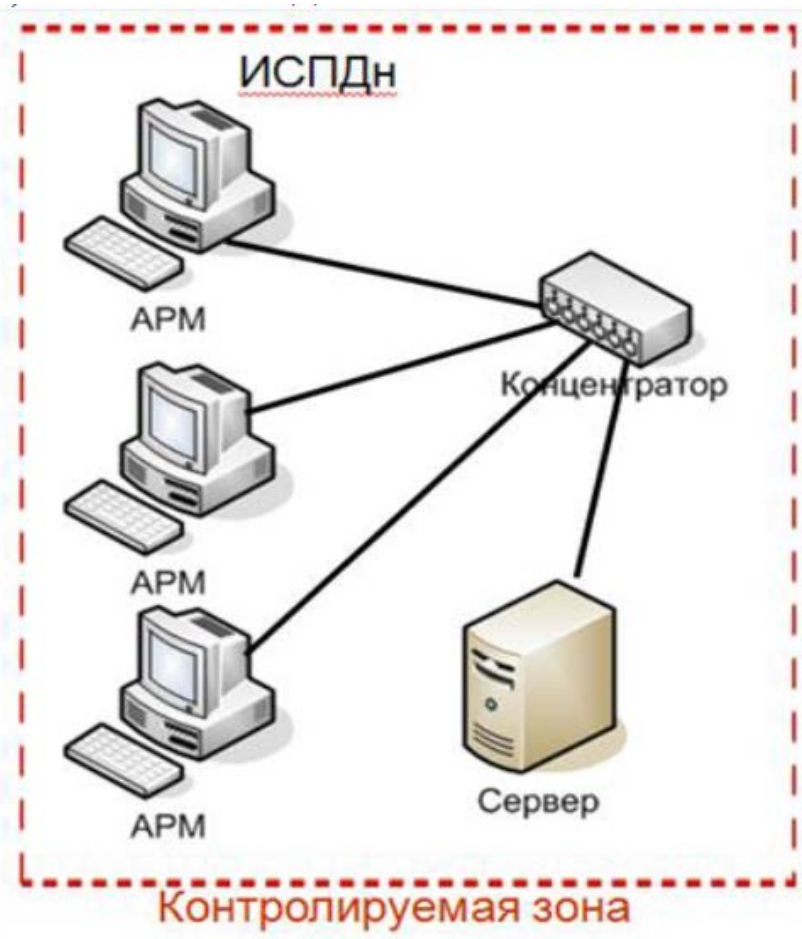

Рисунок 2. Локальные ИСПДн АРМ

c) распределенные ИСПДн):

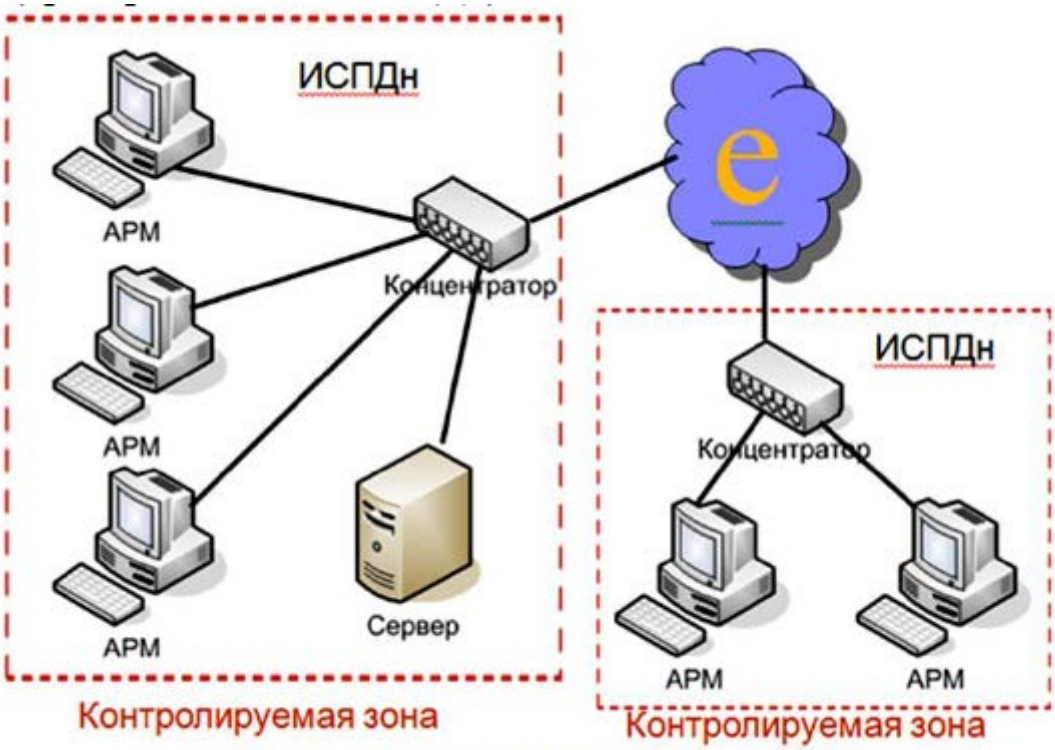

Рисунок 3. Распределенные ИСПДн АРМ

2) категория обрабатываемых в ИСПДн персональных данных:

a) ИСПДн-С;

b) ИСПДн–Б;

c) ИСПДн-И;

d) ИСПДн-О.

3) Объем обрабатываемых в ИСПДн персональных данных:

a) менее чем 100 000 субъектов;

b) более чем 100 000 субъектов.

4) наличие подключений ИСПДн к сетям связи общего пользования/сетям МИО:

a) не имеющие подключение;

b) имеющие подключение.

5) характеристики подсистемы безопасности ИСПДн;

6) режимы обработки персональных данных:

a) однопользовательские ИСПДн;

b) многопользовательские ИСПДН.

7) режимы разграничения прав доступа пользователей ИСПДн:

a) с разграничением доступа;

b) без разграничения доступа;

8) условия размещения технических средств ИСПДн:

a) в пределах контролируемой зоны;

b) вне контролируемой зоны.

9) по территориальному размещению:

a) распределеннаяИСПДн, которая охватывает несколько областей, краев, округов или государство в целом;

b) городскаяИСПДн, охватывающая не более одного населенного пункта (города, поселка);

c) корпоративная распределенная ИСПДн, охватывающая многие подразделения одной организации;

d) локальная (кампусная) ИСПДн, развернутая в пределах нескольких близко расположенных зданий;

e) локальнаяИСПДн, развернутая в пределах одного здания.

Основные этапы расчётов.

1. Определение модели угроз безопасности ПДн.
2. Определение актуальных угроз ПДн.
3. Определение уровня защищенности ПДн.
4. Определение мер по защите ПДн от актуальных угроз.

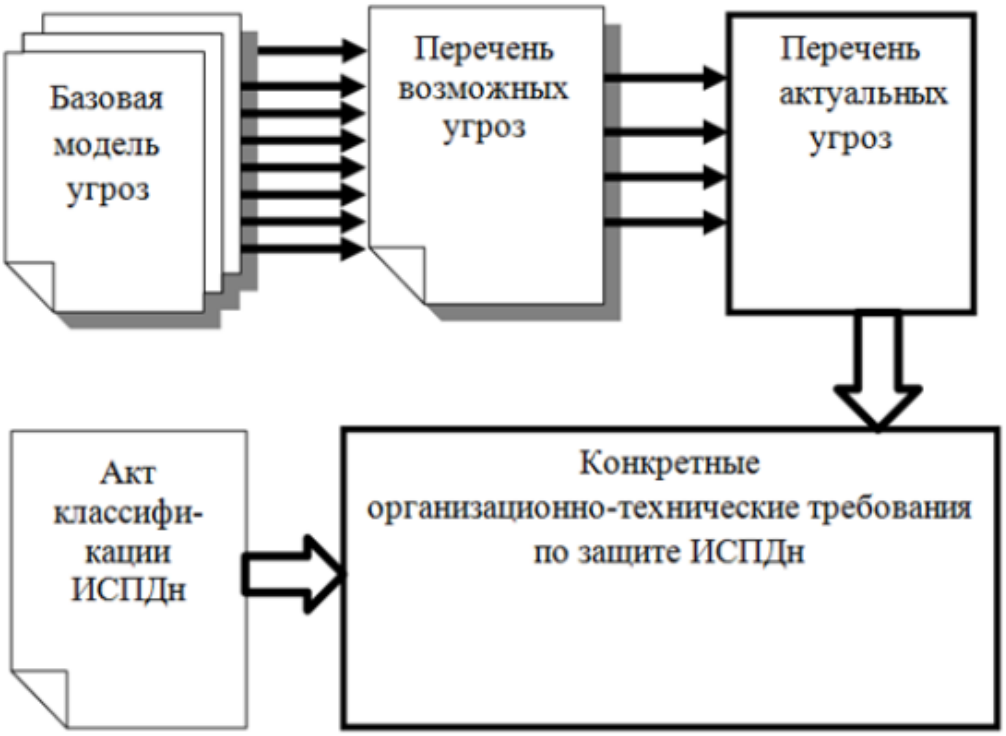

Рисунок 4. Схема определения организационно-технические мер по защите ПДн

По признаку принадлежности к ИСПДн все нарушители делятся на две группы:

- внешние нарушители – физические лица, не имеющие права пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИСПДн;

- внутренние нарушители – физические лица, имеющие право пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИСПДн.

2.1.2 Внешние нарушители.

В роли внешних нарушителей информационной безопасности могут выступать лица, описанные в таблице 1.

Таблица 1.

Категория нарушителя	Описание категории нарушителя
Лица, не имеющие санкционированного доступа к ИСПДн	- физические лица - организации (в том числе конкурирующие) - криминальные группировки

2.1.3 Внутренние нарушители.

Внутренние потенциальные нарушители подразделяются на восемь категорий в зависимости от способа доступа и полномочий доступа к ПДн.

Под внутренним нарушителем информационной безопасности рассматривается нарушитель, имеющий непосредственный доступ к каналам связи, техническим средствам и ресурсам системы, находящимся в пределах контролируемой зоны, на территории Российской федерации.

К внутренним нарушителям могут относиться лица, описанные в таблице 2.

Таблица 2.

Категория нарушителя	Перечень лиц	Описание категории нарушителя
	Работники предприятия, не имеющие санкционированного доступа к ИСПДн	· имеет доступ к фрагментам информации, содержащей ПДн и распространяющейся по внутренним каналам связи ИСПДн; · располагает фрагментами информации о топологии ИСПДн (коммуникационной части подсети) и об используемых коммуникационных протоколах и их сервисах; · располагает именами и возможностью выявления паролей зарегистрированных пользователей; · изменяет конфигурацию технических средств ИСПДн, вносит в нее программно-аппаратные закладки и обеспечивать съем информации, используя непосредственное подключение к техническим средствам ИСПДн.
	Пользователи ИСПДн	· обладает всеми возможностями лиц первой категории; · знает, по меньшей мере, одно легальное

		имя доступа; · обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству ПДн; · располагает конфиденциальными данными, к которым имеет доступ.
	Администраторы ППО ИСПДн	· Обладает всеми возможностями лиц первой и второй категорий; · располагает информацией о топологии ИСПДн на базе локальной и (или) распределенной информационной системы, через которую осуществляется доступ, и о составе технических средств ИСПДн; · имеет возможность прямого (физического) доступа к фрагментам технических средств ИСПДн.
	Администраторы локальной сети	· Обладает всеми возможностями лиц предыдущих категорий; · обладает полной информацией о системном и прикладном программном обеспечении, используемом в сегменте (фрагменте) ИСПДн; · обладает полной информацией о технических средствах и конфигурации сегмента (фрагмента) ИСПДн; · имеет доступ к средствам защиты информации и протоколирования, а также к отдельным элементам, используемым в сегменте (фрагменте) ИСПДн; · имеет доступ ко всем техническим средствам сегмента (фрагмента) ИСПДн; · обладает правами конфигурирования и административной настройки некоторого подмножества технических средств сегмента (фрагмента) ИСПДн.
	Зарегистрированные пользователи с	· Обладает всеми возможностями лиц предыдущих категорий; ·

	полномочиями системного администратора ИСПДн Администраторы информационной безопасности	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
	Работники сторонних организаций, обеспечивающие поставку, сопровождение и ремонт технических средств ИСПДн	· обладает всеми возможностями лиц предыдущих категорий; · обладает полной информацией об ИСПДн; · имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн; · не имеет прав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных).
	Программисты-разработчики (поставщики) прикладного программного обеспечения и лица, обеспечивающие его сопровождение на защищаемом объекте	· обладает информацией об алгоритмах и программах обработки информации на ИСПДн; · обладает возможностями внесения ошибок, недекларированных возможностей, программных закладок, вредоносных программ в программное обеспечение ИСПДн на стадии ее разработки, внедрения и сопровождения; · может располагать любыми фрагментами информации о топологии ИСПДн и технических средствах обработки и защиты ПДн, обрабатываемых в ИСПДн.
	Разработчики и лица, обеспечивающие поставку, сопровождение и ремонт технических средств на ИСПДн	· обладает возможностями внесения закладок в технические средства ИСПДн на стадии их разработки, внедрения и сопровождения; · может располагать любыми фрагментами информации о топологии ИСПДн и

		технических средствах обработки и защиты информации в ИСПДн.

Перечень всех возможных угроз безопасности ПДн.. Показан в таблице 3.

Таблица 3.

Возможные угрозы безопасности ПДн
1. Угрозы от утечки по техническим каналам
1.1. Угрозы утечки акустической информации
1.2. Угрозы утечки видовой информации
1.3. Угрозы утечки информации по каналам ПЭМИН
2. Угрозы несанкционированного доступа к информации
2.1. Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн
2.1.1. Кража ПЭВМ
2.1.2. Кража носителей информации
2.1.3. Кража ключей и атрибутов доступа
2.1.4. Кражи, модификации, уничтожения информации
2.1.5. Вывод из строя узлов ПЭВМ, каналов связи
2.1.6. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ
2.1.7. Несанкционированное отключение средств защиты
2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий)
2.2.1. Действия вредоносных программ (вирусов)
2.2.2. Недекларированные возможности системного ПО и ПО для обработки персональных данных
2.2.3. Установка ПО, не связанного с исполнением служебных обязанностей
2.3. Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и систем защиты ПДн в ее составе из-за сбоев в программном обеспечении, а также от сбоев аппаратуры, из-за ненадежности элементов, сбоев электропитания и стихийного (ударов молний, пожаров, наводнений и т. п.) характера
2.3.1. Утрата ключей и атрибутов доступа
2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками
2.3.3. Непреднамеренное отключение средств защиты
2.3.4. Выход из строя аппаратно-программных средств
2.3.5. Сбой системы электроснабжения

2.3.6. Стихийное бедствие
2.4. Угрозы преднамеренных действий внутренних нарушителей
2.4.1. Доступ к информации, копирование, модификация, уничтожение, лицами, не допущенными к ее обработке
2.4.2. Разглашение информации, копирование, модификация, уничтожение сотрудниками, допущенными к ее обработке
2.5.Угрозы несанкционированного доступа по каналам связи
2.5.1.Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации:
2.5.1.1. Перехват за переделами с контролируемой зоны
2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями
2.5.1.3.Перехват в пределах контролируемой зоны внутренними нарушителями.
2.5.2.Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.
2.5.3.Угрозы выявления паролей по сети
2.5.4.Угрозы навязывание ложного маршрута сети
2.5.5.Угрозы подмены доверенного объекта в сети
2.5.6.Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях
2.5.7.Угрозы типа «Отказ в обслуживании»
2.5.8.Угрозы удаленного запуска приложений
2.5.9.Угрозы внедрения по сети вредоносных программ

Под уровнем исходной защищенности ИСПДн понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИСПДн, приведенных в таблице 4.

Таблица 4.

Показатели исходной защищенности ИСПДн.

Технические и эксплуатационные характеристики ИСПДн	Уровень защищенности		
Высокий	Средний	Низкий	
1. По территориальному размещению:			
Распределенная ИСПДн, которая охватывает несколько областей, краев, округов или государство в целом;	–	–	+
Городская ИСПДн, охватывающая не более одного населенного пункта (города, поселка);	–	–	+
корпоративная распределенная ИСПДн, охватывающая многие подразделения одной организации;	–	+	–

локальная (кампусная) ИСПДн, развернутая в пределах нескольких близко расположенных зданий;	–	+	–
Локальная ИСПДн, развернутая в пределах одного здания	+	–	–
2. По наличию соединения с сетями общего пользования:			
ИСПДн, имеющая многоточечный выход в сеть общего пользования;	–	–	+
ИСПДн, имеющая одноточечный выход в сеть общего пользования;	–	+	–
ИСПДн, физически отделенная от сети общего пользования	+	–	–
3. По встроенным (легальным) операциям с записями баз персональных данных:			
чтение, поиск;	+	–	–
запись, удаление, сортировка;	–	+	–
модификация, передача	–	–	+
4. По разграничению доступа к персональным данным:			
ИСПДн, к которой имеют доступ определенные перечнем сотрудники организации, являющейся владельцем ИСПДн, либо субъект ПДн;	–	+	–
ИСПДн, к которой имеют доступ все сотрудники организации, являющейся владельцем ИСПДн;	–	–	+
ИСПДн с открытым доступом	–	–	+
5. По наличию соединений с другими базами ПДн иных ИСПДн:			
интегрированная ИСПДн (организация использует несколько баз ПДн ИСПДн, при этом организация не является владельцем всех используемых баз ПДн);	–	–	+
ИСПДн, в которой используется одна база ПДн, принадлежащая организации – владельцу данной ИСПДн	+	–	–
6. По уровню обобщения (обезличивания) ПДн:			
ИСПДн, в которой предоставляемые пользователю данные являются обезличенными (на уровне организации, отрасли, области, региона и т.д.);	+	–	–
ИСПДн, в которой данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в организации;	–	+	–
ИСПДн, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта ПДн)	–	–	+
7. По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки:			
ИСПДн, предоставляющая всю базу данных с ПДн;	–	–	+
Количество «+» в колонках			

РЕЗУЛЬТАТ (Y_1)	

Где Y1- числовой коэффициент исходной защищенности, а именно:

0 – для высокой степени исходной защищенности;

5 – для средней степени исходной защищенности;

10 – для низкой степени исходной защищенности.

Не менее 70% характеристик ИСПДн соответствуют уровню не ниже "средний", следовательно Y1=5.

Задание на лабораторную работу

1. Изучить исходную ИСПДн.

2. Изучить документ «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных». ФСТЭК России от 15.02.2008 г.

3. На основании документа «Базовая модель угроз» определяют Модель вероятного нарушителя путём сбора всех возможных категорий нарушителей.

4. На основании документа «Базовая модель угроз определить перечень угроз безопасности для конкретной структуры ИСПДн

5. Изучить документ «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», разработанный ФСТЭК России.

6. Заполнить таблицу 4, проставив в виде «+» показатели высокого, среднего и низкого уровня защищённости для всех технических и эксплуатационных характеристик ИСПДн.

7. Рассчитать исходную степень защищенности. Результаты занести в таблицу.

Содержание отчета

На основе изученных документов и примера приведенного в Приложении А и Б, оформить отчет, который содержит МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ и УРОВЕНЬ ЗАЩИЩЕННОСТИ ИСПДн

Лабораторная работа №5 . Стадия проектирования (разработки проектов), включающая разработку СЗИ в составе объекта информатизации

Определив уровень защищенности ИСПДн, актуальные угрозы безопасности ПДн и класс необходимых к применению СКЗИ необходимо разработать мероприятия, внедрение и реализация которых позволит снизить вероятность реализации угроз безопасности ПДн и минимизировать ущерб от возможной реализации этих угроз.

В техническом проекте отражаются исходные данные защищаемой ИСПДн, определяются основные направления защиты информации, определяются способы и средства защиты информации по различным направлениям.

Дополнительно по каждой актуальной угрозе формируется перечень средств защиты, применение которых позволит минимизировать вероятность реализации актуальной угрозы.

Определяются меры для обеспечения безопасности ПДн в соответствии с требованиями приказа ФСТЭК России №21 от 18.02.2014 г..

Предлагаются решения вопросов управления защитой ПДн:

- организация охраны ИСПДн и ее составных частей;
- управления защитой ПДн на уровне взаимодействия персонала Заказчика с сотрудниками, отвечающими за обеспечение информационной безопасности;
- производится выбор подходящих средств защиты или формируются несколько вариантов с различными средствами защиты с целью оптимизации бюджета, необходимого на внедрение СЗИ;
- рассматриваются кадровые вопросы обеспечения защиты информации;

- определяются этапы внедрения системы защиты информации с указанием сроков исполнения каждого этапа.

После согласования технического проекта с Заказчиком можно приступать непосредственно к закупке и внедрению средств защиты информации.

Задание на лабораторную работу

1. Изучить возможные мероприятия, технические и программные средства, которые можно использовать при защите от актуальных угроз.

2. Сравнить с аналогами и обосновать выбор технических и программных средств защиты.

3. Рассмотреть пример , Приложение В - ТЕХНИЧЕСКИЙ ПРОЕКТ НА СОЗДАНИЕ СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ.

Содержание отчета

Отчет должен содержать обоснованный выбор средств защиты и возможных мероприятий от актуальные угрозы безопасности ПДн .

***Разработать технический проект на создание системы защиты персональных данных

Лабораторная работа №6 . Ввод в действие СЗИ

На данном этапе согласованные с Заказчиком и закупленные на стадии технического проекта средства защиты информации устанавливаются в технические средства информационной системы обработки персональных данных. Также на данном этапе осуществляется разработка и внедрение требований к настройкам средств защиты информации. Данные требования должны содержать указания по настройке парольной политики, указания по формированию замкнутой программной среды (ЗПС), замкнутой аппаратной среды (ЗАС), контроль ЗПС и ЗАС, количество циклов затирания информации

Для успешной эксплуатации ИС Заказчику передаются на согласование и утверждение проекты документов:

1) Концепция информационной безопасности ИСПДн;
2) Политика информационной безопасности ИСПДн;
3) Инструкция администратора ИСПДн;
4) Инструкция пользователя ИСПДн;
5) Инструкция администратора безопасности ИСПДн;
6) Инструкция пользователя ИСПДн по обеспечению безопасности обработки ПДн при возникновении внештатных ситуаций;
7) Положение об Электронном журнале регистрации событий безопасности;
8) Журнал учёта обращений субъектов ПДн о выполнении их законных прав;
9) Журнал по учету мероприятий по контролю состояния защиты ПДн;
10) Порядок резервирования и восстановления работоспособности;
11) Перечень ПДн, подлежащих защите в ИСПДн;
12) Перечень применяемых СЗИ, эксплуатационной и технической документации к ним;

13) План мероприятий по обеспечению защиты ПДн в ИСПДн;

14) План внутренних проверок режима защиты ПДн в ИСПДн;

15) Положение о разграничении прав доступа к обрабатываемым ПДн в ИСПДн;

16) Матрица доступа;

17) Положение об организации работы с персональными данными.

Методика проведения аттестационных испытаний определяет условия и порядок проведения аттестационных испытаний ИСПДн «Бухгалтерия» на соответствие требованиям по безопасности ПДн.

Данный документ разрабатывается на основании ГОСТ РО 0043-004-2013 Защита Информации. Аттестация объектов информатизации. Программа и методики аттестационных испытаний [5].

Документ определяет и подробно описывает перечень работ, которые необходимо выполнить в ходе аттестационных испытаний:

– анализ внутренней и распорядительной документации по защите информации в ИСПДн, технологического процесса обработки информации и анализ информационных потоков;

– проведение оценки защищенности ИСПДн и отдельных ее компонентов в условиях эксплуатации;

– проверка состояния организации работ и выполнения организационно-технических требований по защите информации, оценка правильности классификации ИСПДн;

– оценка полноты и уровня разработки организационно-распорядительной, проектной и эксплуатационной документации;

– оценка уровня подготовки кадров и распределения ответственности за выполнением требований по защите информации;

– испытания отдельных программных средств ИСПДн, средств и систем защиты информации на соответствие требованиям защиты информации;

– комплексные испытания ИСПДн на соответствие требованиям по защите информации;

– подготовка отчетной документации - протокола и заключения по результатам аттестационных испытаний ИСПДн, «Аттестата соответствия…».

В документе приводится описание защищаемой ИСПДн, условия и порядок проведения аттестационных испытаний, описание анализа технологического процесса автоматизированной обработки информации, описание проверки на соответствие организационно-техническим требованиям по защите информации, описания непосредственно испытаний ИСПДн на соответствие требованиям по защите информации от НСД. Указываются требования к оформлению отчетной документации по результатам аттестационных испытаний.

Аттестационные испытания проводятся в строгом соответствии с разработанной методикой проведения аттестационных и испытаний и ГОСТ РО 0043-003-2012 Защита информации. Аттестация объектов информатизации. Общие положения [4].

Целью аттестационных испытаний является оценка защищенности ИСПДн в соответствии с действующими специальными требованиями и нормами ФСТЭК России по защите информации, обрабатываемой ИСПДн, от несанкционированных действий (НСД) к информации.

Аттестационные испытания ИСПДн проводятся в эксплуатационных режимах работы ОТСС с использованием тестирующих программных средств.

На момент проведения аттестации ИСПДн аттестационной комиссии должны быть представлены следующие исходные данные и документация:

18) Приказ о проведении работ по защите персональных данных;
19) Приказ о проведении внутренней проверки;
20) Приказ об утверждении перечня сведений конфиденциального характера;
21) Отчет о результатах проведения внутренней проверки обеспечения защиты персональных данных в информационной системе персональных данных «Бухгалтерия»;
22) Концепция информационной безопасности информационной системы персональных данных;
23) Политика информационной безопасности информационной системы персональных данных;
24) Инструкция администратора информационной системы персональных данных;
25) Инструкция пользователя информационной системы персональных данных;
26) Инструкция администратора безопасности информационной системы персональных данных;
27) Инструкция пользователя информационной системы персональных данных по обеспечению безопасности обработки персональных данных при возникновении внештатных ситуаций
28) Инструкция по антивирусной защите;
29) Положение об электронном журнале обращений пользователей информационной системы к персональным данным;
30) Журнал учёта обращений субъектов персональных данных о выполнении их законных прав;
31) Журнал по учету мероприятий по контролю состояния защиты персональных данных;

32) Порядок резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в информационной системе персональных данных;
33) Перечень персональных данных, подлежащих защите в информационной системе персональных данных «Бухгалтерия»;
34) Акт определения уровня защищенности информационной системы персональных данных «Бухгалтерия»;
35) Перечень применяемых средств защиты информации, эксплуатационной и технической документации к ним;
36) План мероприятий по обеспечению защиты персональных данных в информационной системе персональных данных «Бухгалтерия»;
37) План внутренних проверок режима защиты персональных данных в информационных системах персональных данных;
38) Положение о разграничении прав доступа к обрабатываемым персональным данным в информационных системах персональных данных;
39) Матрица доступа;
40) Положение об организации работы с персональными данными;
41) Частная модель угроз безопасности персональных данных при их обработке в информационной системе персональных данных «Бухгалтерия»;
42) Модель угроз безопасности персональных данных при их обработке в информационной системе персональных данных «Бухгалтерия» (по требованиям ФСБ России)»;
43) Технический проект на создание системы защиты персональных данных в информационной системе персональных данных «Бухгалтерия»;
44) Паспорт (руководство по эксплуатации) на СЗИ;

45) Сертификаты соответствия требованиям безопасности информации на используемые СЗИ.

Объем аттестационных испытаний ИСПДн определяется следующим перечнем работ:

– анализ техпроцесса автоматизированной обработки информации;

– проверка ИСПДн на соответствие организационно-техническим требованиям по защите информации;

– испытания ИСПДн на соответствие требованиям по защите информации от НСД;

– оформление отчетных материалов (протокол НСД и заключение по результатам аттестационных испытаний, «Аттестат соответствия…»).

При изучении техпроцесса автоматизированной обработки и хранения информации анализу подвергаются такие компоненты ИСПДн как объекты и субъекты доступа, средства обработки и передачи информации:

– к объектам доступа относятся средства обработки и передачи информации, информационные носители на магнитной и бумажной основе, накопители и все виды памяти ПЭВМ, в которых может находиться информация, отдельные документы и их архивы, используемые в технологическом процессе автоматизированной обработки информации, файлы, записи и другие единицы информационных ресурсов, доступ к которым необходимо регламентировать;

– к субъектам доступа относятся персонал и все лица, которые имеют возможность доступа к средствам обработки информации, а также программные средства, посредством которых осуществляется доступ к объектам;

– к средствам обработки и передачи информации относятся технические и программные средства, средства и линии связи, предоставляющие возможности как для перемещения (копирования) информации между различными областями памяти и информационными

носителями, различными средствами обработки, определенными для ИСПДн, так и по выводу информации из установленной для нее сферы обращения.

Используя исходные данные по технологии обработки и передачи информации, матрицу доступа персонала к защищаемым ресурсам, анализируется обобщенная технологическая схема ИСПДн с существующими и возможными информационными потоками, возможностями доступа к обрабатываемой и передаваемой информации.

Проверяется соответствие описания технологического процесса обработки, хранения и передачи информации реальной практике.

Проверяются исходные данные на ИСПДн и устанавливаются опасные факторы и угрозы, критические места, снижающие уровень защиты, комплектность и характеристики средств защиты.

Проверяются наличие оформленных разрешений на допуск персонала к информации, содержащей персональные данные (ПДн), метки на информационных носителях, соответствие инструкций пользователей и администратора безопасности информации установленным требованиям.

По результатам изучения уточняется схема техпроцесса с привязкой к конкретным средствам обработки и передачи информации и штатному персоналу.

Затем проводится проверка достаточности представленных документов и соответствия их содержания требованиям стандартов и руководящих документов по безопасности информации ФСТЭК (Гостехкомиссии) России и других органов государственного управления в пределах компетенции.

Состав и структура программно-технических средств, включенных в реальный техпроцесс обработки информации, сверяется с представленной документацией.

Проверка правильности классификации ИСПДн проводится в соответствии с требованиями Постановление Правительства РФ от 1 ноября 2012 г. N 1119 «Об утверждении требований к защите персональных данных

при их обработке в информационных системах персональных данных» [14] и на основании следующих определяющих признаков:

– категории ПДн;

– типа актуальных угроз;

– количества обрабатываемых субъектов ПДн.

Требуемый класс ИСПДн и уровень защищенности сравнивается с установленным на ИСПДн.

Проверка уровня подготовки кадров и распределения ответственности производится на основе следующих показателей:

– экспертной оценки знания инструкций по безопасности информации пользователями ИСПДн;

– наличия матрицы доступа персонала к защищаемым ресурсам, определяющей полномочия по доступу к ПДн, и процедуры их оформления, системы распределения ответственности персонала за выполнение требований по безопасности информации, оформленной приказами и распоряжениями главного врача больницы;

– экспертной оценки системы технической учебы и повышения квалификации персонала и пользователей ИСПДн.

Путем опроса персонала проверяется доведение до конкретных исполнителей руководящих документов, приказов, актов, инструкций и уровень овладения персоналом технологией безопасной обработки информации, описанной в этих инструкциях.

Проводится проверка наличия документов, подтверждающих возможность применения технических и программных средств, средств защиты для обработки информации (сертификатов соответствия).

Проводится проверка выполнения требований руководящих документов по условиям размещения ИСПДн в рабочем помещении, которые исключали бы возможность несанкционированного просмотра информации с экранов мониторов, с распечаток принтеров и с других устройств ввода-

вывода информации лицами, не имеющими права доступа к обрабатываемой информации.

По результатам проверки комиссия должна сделать выводы о соответствии (или несоответствии) предъявленных документов и исходных данных установленным требованиям по безопасности информации.

Проводятся испытания ИСПДн на соответствие требованиям по защите информации от НСД.

Испытания проводятся в объеме, указанном в таблице 3.

Таблица 3 – Объем испытаний

Наименование проверок и испытаний	**Пункт методики испытаний**
Анализ и оценка технологического процесса обработки информации	7.1
Выбор инструментальных средств и методики испытаний	7.2
Испытания подсистемы управления доступом	7.2
Проверка механизма идентификации	7.2
Проверка механизма аутентификации	7.2
Проверка механизма контроля доступа	7.2
Проверка механизмов управления потоками информации	7.2
Испытания подсистемы обеспечения целостности	7.3
Испытания подсистемы регистрации и учета	7.4
Испытания подсистемы антивирусной защиты	7.5

Объем испытаний на соответствие требованиям по ЗИ от НСД может уточняться в зависимости от установленного класса ИСПДн.

В ходе анализа и оценки технологического процесса обработки информации в части НСД комиссии представляется описание техпроцесса обработки информации в аттестуемой ИСПДн, включающее в себя следующую информацию:

- перечень объектов доступа;
- перечень субъектов доступа;
- перечень штатных средств доступа к информации в ИСПДн;

– перечень средств защиты информации;

– описание реализованных правил разграничения доступа;

– описание информационных потоков.

В качестве объекта доступа принята ИСПДн на базе ПЭВМ в целом.

В качестве субъектов доступа рассматриваются лица и процессы (общесистемные и прикладные программы пользователей), имеющие возможность доступа к объектам штатными средствами указанной ИСПДн.

Субъекты доступа могут иметь официальное разрешение (допуск) к ПДн.

Комиссия проверяет соответствие описания технологического процесса обработки и хранения информации реальному процессу.

Проводится анализ разрешенных и запрещенных связей между субъектами и объектами доступа с привязкой к конкретной ИСПДн и штатному персоналу, оценка их соответствия разрешительной системе доступа персонала к защищаемым ресурсам на всех этапах обработки.

Затем проводятся тестирования ИСПДн на соответствие требованиям защиты информации от НСД с помощью специальных программных средств, описанных в методике проведения аттестационных испытаний.

Испытания подсистемы обеспечения целостности СЗИ от НСД проводится по перечню функций, определенных приказом Федеральной службы по техническому и экспортному контролю Российской Федерации от 18 февраля 2014 г. № 21 [12] для ИСПДн установленного уровня защищенности.

Надежность функций контроля целостности программных средств может быть проверена при помощи внесения изменений в отдельные программы или их подмены. При этом отслеживается реакция системы защиты на произведенные нарушения. При помощи программы «ФИКС 2.0.2» осуществляется расчет контрольных сумм файлов из состава системы

защиты для их сравнения с эталонными контрольными суммами на момент аттестации и при дальнейших проверках.

При проверке обеспечения неизменности программной среды определяется наличие и работоспособность технологии внесения новых программных средств в операционную среду, предусматривающую процедуры экспертной оценки или верификации новых программных средств для выявления потенциально опасных для СЗИ программных функций, критерии санкционирования ввода программ в операционную среду и допуска определенных категорий пользователей к этим программам.

Проверяется наличие и работоспособность средств и мер предотвращения несанкционированного ввода программ в операционную среду.

По результатам анализа техпроцесса обработки и хранения информации в ИСПДн проверяется выполнение требований по физической охране средств ИСПДн и носителей информации в ИСПДн, пропускному режиму и оборудованию помещений необходимыми защитными средствами.

Проверяется наличие в системе администратора безопасности ИСПДн, оценивается его уровень подготовленности и степень оснащения его рабочего места необходимыми средствами оперативного контроля и сопровождения СЗИ.

Проверяется наличие и работоспособность средств периодического тестирования всех функций СЗИ от НСД, наличие графика проведения тестирования. Средства тестирования должны давать однозначную информацию обо всех функциях СЗИ, предусмотренных требованиями к данному классу ИСПДн.

Проверяется наличие и работоспособность технологии восстановления программных средств защиты информации в ИСПДн, ведения архива программных средств защиты, условия и периодичность их обновления и тестирования.

Автоматическое оперативное восстановление функций СЗИ от НСД при сбоях проверяется путем моделирования сбойных ситуаций и последующей проверки (тестирования) функций СЗИ от НСД.

Проверяется наличие сертификатов соответствия на СЗИ, а также установленные в них классы защищенности, уровни контроля, классы и т.п.

Регистрация и учет событий, определенных требованиями по безопасности информации к установленному классу ИСПДн, должны производиться на всех этапах технологического процесса хранения и обработки информации. Регистрация должна охватывать все события, определенные требованиями приказа Федеральной службы по техническому и экспортному контролю Российской Федерации от 18 февраля 2014 г. № 21 [12] для ИСПДн установленного уровня защищенности.

Для проверки необходимо при помощи стандартных средств ИСПДн просмотреть результаты регистрации всех действий, которые были произведены с защищаемыми ресурсами при проверках по п. 7.2 таблицы 2. Должны быть зарегистрированы все требуемые события с требуемыми параметрами регистрации.

Для проверки регистрации изменения полномочий субъектов доступа необходимо произвести эти изменения при помощи средств СЗИ и просмотреть результаты регистрации.

Для проверки процедуры автоматического учета создаваемых защищаемых информационных ресурсов необходимо смоделировать создание защищаемого носителя информации.

При помощи средств СЗИ просматриваются результаты учета. Должны быть автоматически учтены все созданные защищаемые информационные ресурсы с требуемыми параметрами учета.

Проверяется ведение учета всех защищаемых носителей информации, осуществляемого вручную персоналом, путем проверки технологических инструкций, степени ознакомления с ними конкретных исполнителей, проверки правильности ведения журналов учета.

Проверка отработки средств сигнализации на попытки нарушения защиты осуществляется путем моделирования несанкционированных обращений к защищаемым объектам доступа и отслеживания появления определенных сигналов в местах интерфейса с администратором системы защиты и нарушителем.

Оценка эффективности разработанных мероприятий по защите персональных данных по результатам испытаний.

Результаты аттестационных испытаний ИСПДн по всем рассмотренным выше направлениям обеспечения безопасности информации оформляются протоколом испытаний, содержащим:

- состав комиссии, дату испытаний, наименование ИСПДн;
- цель испытаний;
- перечень нормативных документов и методик испытаний;
- результаты испытаний на момент их окончания.

На основании полученных результатов испытаний принимается заключение по аттестации ИСПДн, которое должно включать:

- оценку соответствия ИСПДн требованиям безопасности информации;
- перечень выявленных недостатков и нарушений;
- рекомендации по устранению выявленных недостатков и нарушений;
- вывод о возможности выдачи «Аттестата соответствия…».

Оценка соответствия ИСПДн требованиям безопасности информации производится на основании анализа общих результатов испытаний и выявленных в процессе испытаний конкретных недостатков и нарушений.

В случае несоответствия ИСПДн установленным требованиям по защите информации комиссия может рассмотреть предложения заявителя по

оперативному устранению выявленных недостатков и нарушений. При этом могут рекомендоваться следующие меры:

- доработка организационно-распорядительной документации;
- уточнение класса ИСПДн;
- исключение отдельных технический средств из состава ИСПДн;
- исключение отдельных программных средств из состава ИСПДн.
- применение дополнительных организационно-технических мер защиты;
- применение дополнительных сертифицированных СЗИ.

Если в процессе аттестационных испытаний выявлены недостатки, не приводящие к нарушению установленных требований и норм защищенности информации, то комиссия может рекомендовать следующие меры:

- оперативное устранение выявленных недостатков в процессе аттестационных испытаний;
- устранение установленных недостатков и нарушений в согласованные с комиссией сроки с представлением необходимых документов в организацию, проводящую аттестационные испытания;
- проведение дополнительных частичных испытаний в согласованные сроки.

После устранения всех замечаний принимается решение о выдаче аттестата соответствия. Данный документ оформляется в соответствии с ГОСТ РО 0043-003-2012 Защита информации. Аттестация объектов информатизации. Общие положения [7].

Задание на лабораторную работу

Рассмотреть порядок установки и настройки выбранных аппаратных и программных средств защиты и методики проверки эффективности средств защиты.

Содержание отчета

Подготовить отчет в виде реферат о установки, настройки и проверки эффективности выбранных средств защиты.

Особое внимание уделить разработке политики безопасности и встроенным средствам защиты операционной системы

ПРИЛОЖЕНИЕ А - МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ

Исходная степень защищенности – **средняя**.

Таблица А1 – Итоговая модель угроз безопасности ПДн

Наименование угрозы	**Вероятность реализации угрозы (Y2)**	**Возможность реализации угрозы (Y)**	**Опасность угрозы**	**Актуальность угрозы**
1 Угрозы от утечки по техническим каналам				
1.1 Угрозы утечки акустической (речевой) информации	Маловероятно	Низкая	Низкая	Неактуальная
1.2 Угрозы утечки видовой информации	Средняя вероятность	Средняя	Средняя	Актуальная
1.3 Угрозы утечки информации по каналам ПЭМИН	Маловероятно	Низкая	Низкая	Неактуальная
2 Угрозы несанкционированного доступа к информации				
2.1 Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн				
2.1.1 Кража ПЭВМ	Низкая вероятность	Средняя	Низкая	Неактуальная
2.1.2 Кража носителей информации	Низкая вероятность	Средняя	Низкая	Неактуальная
2.1.3 Кража ключей доступа	Низкая вероятность	Средняя	Низкая	Неактуальная
2.1.4 Кражи, модификации, уничтожения информации	Средняя вероятность	Средняя	Средняя	Актуальная
2.1.5 Вывод из строя узлов ПЭВМ, каналов связи	Маловероятно	Низкая	Низкая	Неактуальная
2.1.6 Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	Низкая вероятность	Средняя	Низкая	Неактуальная
2.1.7 Несанкционированное отключение средств защиты	Средняя вероятность	Средняя	Средняя	Актуальная
2.2 Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий)				
2.2.1 Действия вредоносных программ	Средняя вероятность	Средняя	Средняя	Актуальная

Наименование угрозы	Вероятность реализации угрозы (Y2)	Возможность реализации угрозы (Y)	Опасность угрозы	Актуальность угрозы
(вирусов)				
2.2.2 Установка ПО, не связанного с исполнением служебных обязанностей	Средняя вероятность	Средняя	Средняя	Актуальная
2.2.3 Перехват паролей или идентификаторов	Средняя вероятность	Средняя	Средняя	Актуальная
2.2.4 Модификация базовой системы ввода/вывода (BIOS)	Средняя вероятность	Средняя	Средняя	Актуальная
2.2.5 Перехват управления загрузкой	Средняя вероятность	Средняя	Средняя	Актуальная
2.2.6 Использование остаточной информации, «сбор мусора»	Средняя вероятность	Средняя	Средняя	Актуальная
2.2.7 Программно-аппаратная закладка	Маловероятно	Низкая	Низкая	Неактуальная
2.2.8 Программная закладка	Средняя вероятность	Средняя	Средняя	Актуальная
2.2.9 Недекларированные возможности в системном программном обеспечении	Маловероятно	Низкая	Низкая	Неактуальная
2.2.10 Недекларированные возможности в прикладном программном обеспечении	Низкая вероятность	Средняя	Низкая	Неактуальная
2.3 Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера				
2.3.1 Утрата ключей и атрибутов доступа	Средняя вероятность	Средняя	Средняя	Актуальная
2.3.2 Непреднамеренная модификация (уничтожение) информации сотрудниками	Средняя вероятность	Средняя	Средняя	Актуальная
2.3.3 Непреднамеренное отключение средств защиты	Средняя вероятность	Средняя	Средняя	Актуальная
2.3.4 Выход из строя аппаратно-программных средств	Низкая вероятность	Средняя	Низкая	Неактуальная

Наименование угрозы	Вероятность реализации угрозы (Y2)	Возможность реализации угрозы (Y)	Опасность угрозы	Актуальность угрозы
2.3.5 Сбой системы электроснабжения	Средняя вероятность	Средняя	Низкая	Неактуальная
2.3.6 Стихийное бедствие	Маловероятно	Низкая	Низкая	Неактуальная
2.4 Угрозы преднамеренных действий нарушителей				
2.4.1 Доступ к информации, модификация, уничтожение лицами не допущенных к ее обработке	Низкая вероятность	Средняя	Средняя	Актуальная
2.4.2 Разглашение информации, модификация, уничтожение сотрудниками допущенными к ее обработке	Низкая вероятность	Средняя	Средняя	Актуальная
2.5 Угрозы несанкционированного доступа по каналам связи (в пределах контролируемой зоны)				
2.5.1 Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации	Средняя вероятность	Средняя	Средняя	Актуальная
2.5.2 Угрозы сканирования, направленные на выявление типа операционной системы АРМ, открытых портов и служб, открытых соединений и др.	Средняя вероятность	Средняя	Средняя	Актуальная
2.5.3 Угрозы выявления паролей по сети	Средняя вероятность	Средняя	Средняя	Актуальная
2.5.4 Угрозы подмены доверенного объекта в сети	Средняя вероятность	Средняя	Средняя	Актуальная
2.5.5 Угрозы типа «Отказ в обслуживании»	Средняя вероятность	Средняя	Средняя	Актуальная
2.5.6 Угрозы удаленного запуска приложений	Средняя вероятность	Средняя	Средняя	Актуальная
2.5.7 Угрозы внедрения по сети вредоносных программ	Средняя вероятность	Средняя	Средняя	Актуальная

Наименование угрозы	Вероятность реализации угрозы (Y2)	Возможность реализации угрозы (Y)	Опасность угрозы	Актуальность угрозы
2.6 Угрозы несанкционированного доступа по каналам связи (за пределами контролируемой зоны)				
2.6.1 Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации	Низкая вероятность	Средняя	Средняя	Актуальная
2.6.2 Угрозы сканирования, направленные на выявление типа операционной системы АРМ, открытых портов и служб, открытых соединений и др.	Низкая вероятность	Средняя	Средняя	Актуальная
2.6.3 Угрозы выявления паролей по сети	Низкая вероятность	Средняя	Средняя	Актуальная
2.6.4 Угрозы подмены доверенного объекта в сети	Низкая вероятность	Средняя	Средняя	Актуальная
2.6.5 Угрозы типа «Отказ в обслуживании»	Низкая вероятность	Средняя	Средняя	Актуальная
2.6.6 Угрозы удаленного запуска приложений	Низкая вероятность	Средняя	Средняя	Актуальная
2.6.7 Угрозы внедрения по сети вредоносных программ	Низкая вероятность	Средняя	Средняя	Актуальная

ПРИЛОЖЕНИЕ Б - АКТ ОПРЕДЕЛЕНИЯ УРОВНЯ ЗАЩИЩЕННОСТИ

ООО «ИнфоТех»

УТВЕРЖДАЮ

Генеральный директор ООО «ИнфоТех»

_____ И.И. Иванов

«___» _____ 2016 г.

АКТ
определения уровня защищенности информационной системы персональных данных
«Бухгалтерия»»

По результатам проведенного анализа исходных данных информационной системы персональных данных «Бухгалтерия» выявлены следующие характеристики:

Тип угроз, связанных с наличием недокументированных (недекларированных) возможностей	Угрозы 3-го типа
Объем обрабатываемых персональных данных	Менее 100000
Тип информационной системы персональных данных	Иная
Тип субъектов ПДн	Сотрудники ООО «ИнфоТех»

На основании полученных данных и в соответствии с Постановлением Правительства РФ от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» в информационной системе персональных данных «Бухгалтерия» необходимо обеспечить **3-й уровень защищенности персональных данных**.

Председатель комиссии:

_____ _____ / _____/
должность подпись ФИО

Члены комиссии:

_____ _____ / _____/
должность подпись ФИО

_____ _____ / _____/
должность подпись ФИО

_____ _____ / _____/ дол

ПРИЛОЖЕНИЕ В - ТЕХНИЧЕСКИЙ ПРОЕКТ НА СОЗДАНИЕ СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

УТВЕРЖДАЮ	**УТВЕРЖДАЮ**
Руководитель	Руководитель Заказчика
аттестующей организации	
_____/ _____	_____ / _____
«___» _____ 2017 г.	«___» _____ 2017 г.

Технический проект
на создание системы защиты персональных данных
в ИСПДн «Бухгалтерия»

Разработано	**Согласовано**
должность	должность
_____/ _____	_____/ _____
должность	должность
_____/ _____	_____/ _____

2017

Содержание

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

АРМ – автоматизированное рабочее место

АПКШ – аппаратно-программный комплекс шифрования

ГБУЗ – Государственное бюджетное учреждение здравоохранения

ИСПДн – информационная система персональных данных

СЗПДн – система защиты персональных данных

КЗ – контролируемая зона

ЛВС – локальная вычислительная сеть

МЭ – межсетевой экран

НСД – несанкционированный доступ

ОС – операционная система

ПДн – персональные данные

ПО – программное обеспечение

СЗИ – средства защиты информации

СОВ – средства обнаружения вторжений

СКЗИ – средства криптографической защиты информации

ТФОМС – территориальный фонд обязательного медицинского страхования

УБПДн – угрозы безопасности персональных данных

ОБЩИЕ СВЕДЕНИЯ

Настоящий документ разработан на основании предоставленных исходных данных и нормативно-правовых актов:

Отчет о результатах проведения внутренней проверки обеспечения защиты персональных данных в информационной системе персональных данных «Бухгалтерия»;

Частная модель угроз безопасности персональных данных при их обработке в информационной системе персональных данных «Бухгалтерия»;

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

Приказ Федеральной службы по техническому и экспортному контролю Российской Федерации (далее - ФСТЭК России) от 18 февраля 2014 г. № 21 об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных;

«Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (утверждено заместителем директора ФСТЭК России 15 февраля 2008 года);

«Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (утверждено заместителем директора ФСТЭК России 14 февраля 2008 года);

«Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации» (ФСБ России, № 149/5-144, 2008 г.);

Постановление Правительства РФ от 01.11.2012 г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

«Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных» (ФСБ России, № 149/5-144, 2008).

Документ описывает требования и конкретные технические решения для создания системы защиты персональных данных (далее СЗПДн) в информационной системе персональных данных (далее ИСПДн) «Бухгалтерия», в которой обработка персональных данных (далее – ПДн) осуществляется с использованием средств автоматизации, в объеме, достаточном для приведения ИСПДн в соответствие с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных».

Заказчик – ООО «ИнфоТех».

Исполнитель – наименование исполнителя.

По окончанию выполнения работ по созданию СЗПДн исполнитель предоставляет следующие документы:

Программа и методики проведения аттестационных испытаний информационной системы персональных данных Заказчика на соответствие требованиям безопасности информации;

Протокол испытаний комплексной системы защиты информации информационной системы персональных данных Заказчика на соответствие требованиям безопасности информации в части защиты от НСД и компьютерных вирусов;

Заключение по результатам проведения аттестационных испытаний информационной системы персональных данных Заказчика на соответствие требованиям безопасности информации;

Аттестат соответствия информационной системы персональных данных Заказчика требованиям безопасности информации;

Бухгалтерские документы и акты выполненных работ, сопровождающие отдельные этапы создания СЗПДн.

1 НАЗНАЧЕНИЕ И ЦЕЛИ СОЗДАНИЯ СЗПДН

СЗПДн предназначена для обеспечения безопасности персональных данных, обрабатываемых в ИСПДн Заказчика, в соответствии с действующими нормативно-правовыми актами в области защиты ПДн.

СЗПДн создается с целью нейтрализации или сведения к минимуму опасности актуальных угроз безопасности ПДн при их обработке в ИСПДн.

2 ИСХОДНЫЕ ДАННЫЕ

В ходе проведения оценки обстановки была определена ИСПДн «Бухгалтерия» 3-го уровня защищенности персональных данных.

В ИСПДн обработка персональных данных производится только в рабочее время, установленное внутренними распорядительными документами Заказчика. Обработка персональных данных осуществляется в многопользовательском режиме обработки персональных данных и равных правах доступа к ним.

Режим обработки предусматривает следующие действия с персональными данными: ввод, изменение, хранение, поиск, печать и передачу по каналу связи, уничтожение персональных данных.

ИСПДн предназначена для автоматизации ведения бухгалтерского и кадрового учета организации, обеспечивает оформление хозяйственных операций первичными документами, отражение данных в регистрах учета, получение отчетности в соответствии с действующим законодательством.

ИСПДн предназначена для автоматизации ведения бухгалтерского учета организации, обеспечивает оформление хозяйственных операций первичными документами, отражение данных в регистрах учета, получение отчетности в соответствии с действующим законодательством.

На рисунке В1 представлена исходная схема ИСПДн «Бухгалтерия».

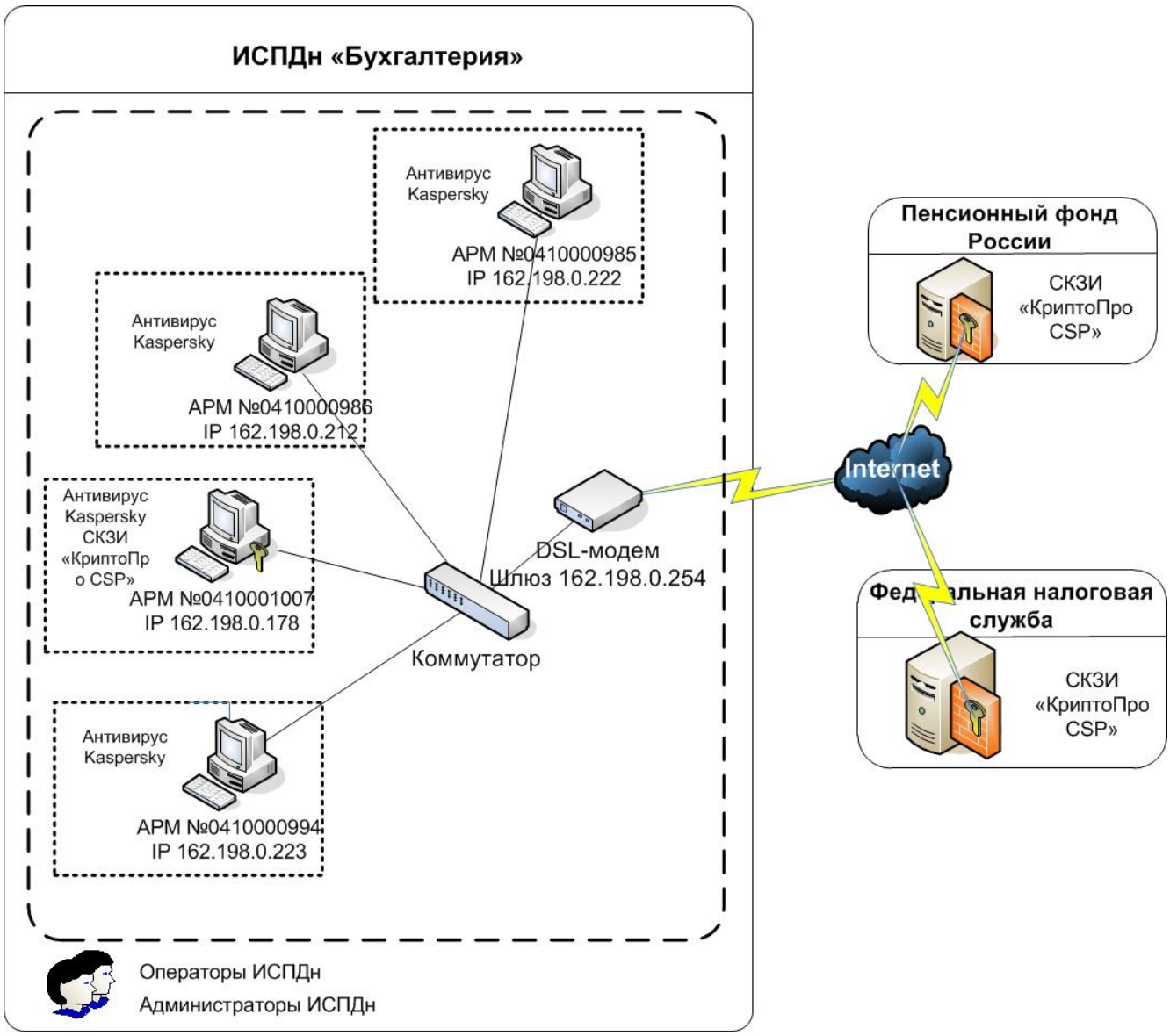

Рис. В1 – Исходная схема ИСПДн

Согласно Постановлению Правительства РФ от 01.11.2012 г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» ИСПДн является информационной системой, обрабатывающей иные категории ПДн. Для ИСПДн актуальными являются угрозы 3-го типа (угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении).

В соответствии с Постановлением Правительства РФ от 01.11.2012 г. №1119 «Об утверждении требований к защите персональных данных при их

обработке в информационных системах персональных данных» определена необходимость обеспечения 3-го уровня защищенности ПДн при их обработке в данной ИСПДн.

Рассмотрена контролируемая зона и характеристика помещений

Таблица 1 - Характеристика помещений с расположенными элементами сети

Наименование помещения	**Этаж расположения**	**Количество этажей здания**	**Дверь**	**Охранная сигнализация**	**Пожарная сигнализация**	**Решетки на окнах**	**Жалюзи на окнах**	**Ограничение допуска в помещение (только контролируемое пребывание)**	**Наличие контролируемой зоны**
Кабинет 1	1	2	Деревянная	Нет	Есть	Нет	Нет	Есть	Помещение
Кабинет 2	1	2	Пластиковая	Нет	Есть	Нет	Нет	Есть	Помещение
Кабинет 3	2	2	Деревянная	Нет	Есть	Нет	Нет	Есть	Помещение

Характеристики помещений в корпусе 1, где располагается предприятие ООО «ИнфоТех», следующие:

Адрес организации: 440000, г. Петровск, ул. Больничная 10

Наименование корпуса/здания: корпус 1

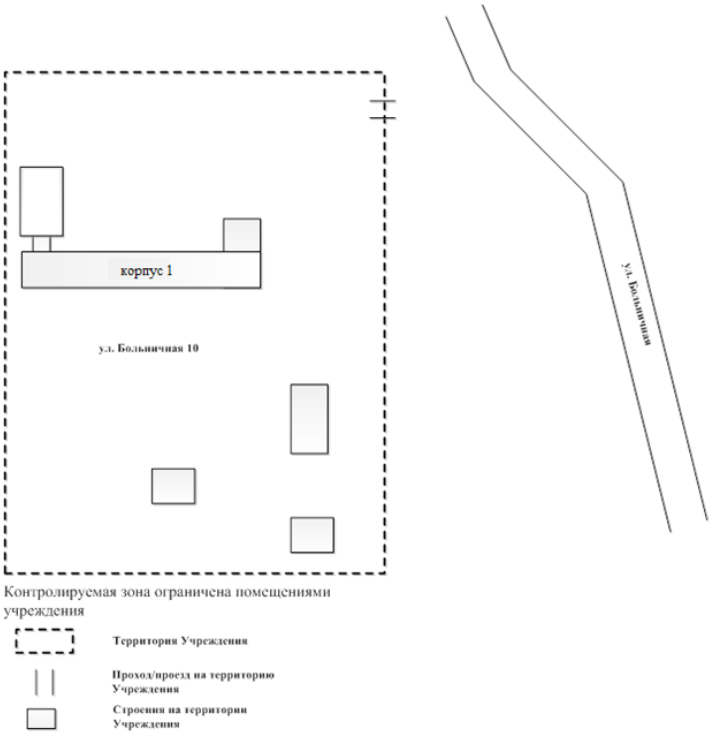

Рисунок В2- Контролируемая зона ООО «ИнфоТех»

Рассмотрим все входящие в сеть АРМ.
1. АРМ инв.(уч.) № 0410000994 (этаж 2, кабинет 1)
Адрес организации: 440000, г. Петровск, ул. Больничная 10
Наименование корпуса/здания: корпус 1
Наименование помещения: кабинет №1
Учетный (инвентарный) номер ПЭВМ: 0410000994

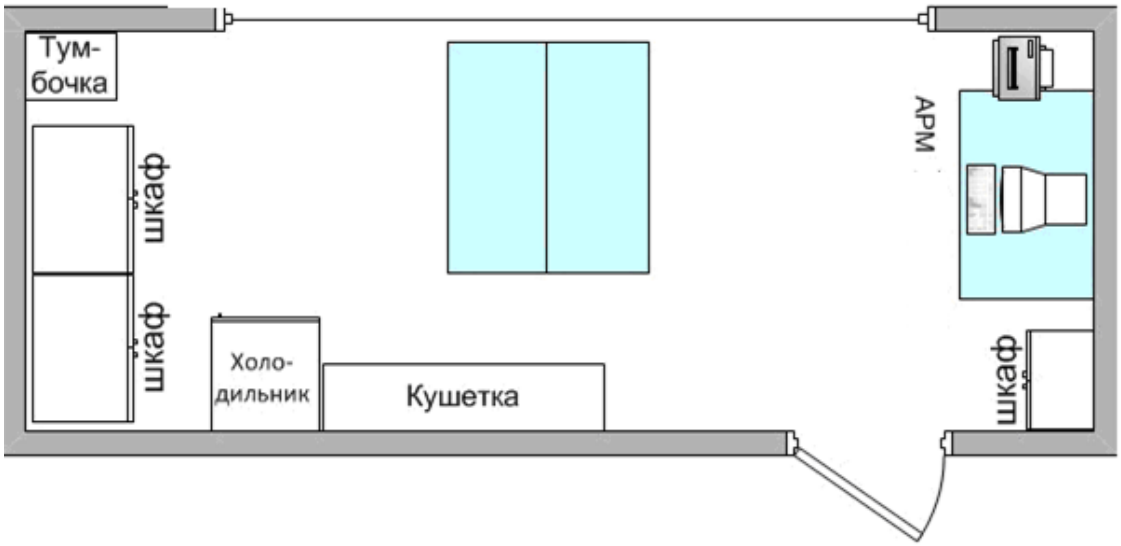

Рисунок 12– Расположение технических средств в помещении кабинет 1

Таблица 2 - Состав комплекса технических средств ПЭВМ: 0410000994

№ п/п	Наименование	Тип (модель)	Серийный (Заводской) номер
1.	Системный блок	ATX	Без номера
2.	Клавиатура	Acer PR1101U	DKPS21P03N239Ab4b4HU01
3.	Мышь	Acer M-U0027-O	lz216av06xh
4.	МФУ	Canon MF4410	PWF51007
5.	ИБП	APC BackUPS CS 500	4B1202P52967
6.	Монитор	Acer V223W	20901564342

Таблица 3 - Перечень программных средств ПЭВМ: 0410000994

Наименование программного средства
1. Microsoft Windows 7 Professional SP1 Rus 32bit
2. Adobe Flash Player 11 ActiveX
3. Canon MF Toolbox 4.9.1.1.mf11
4. Canon MF4400 Series
5. DAEMON Tools Lite 4.45.4.0315
6. Google Chrome 24.0.1312.57
7. Google Update Helper
8. Intel(R) Network Connections Drivers
9. Intel(R) Processor Graphics
10. Microsoft .NET Framework 4 Client Profile RUS Language Pack [Русский (Россия)]
11. Microsoft .NET Framework 4 Client Profile
12. Microsoft Office 2010 Service Pack 1 (SP1)
13. Microsoft Office Professional Plus 2010
14. Microsoft Office Proof (English) 2010
15. Microsoft Office профессиональный плюс 2010
16. Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.17
17. Total Commander (Remove or Repair)
18. Total Commander 7.57a PowerPack
19. WinRAR 4.11 (32-разрядная)

Наименование программного средства
20. Антивирус Касперского 6.0 для Windows Workstations [Русский (Россия)] 6.0.4.1611
21. Языковой пакет клиентского профиля Microsoft.NET Framework 4 - RUS

2. АРМ инв.(уч.) № 0410000985 и 0410000986 (этаж 2, кабинет 2)
Адрес организации: 440000, г. Петровск, ул. Больничная 10
Наименование корпуса/здания: корпус 1
Наименование помещения: кабинет №1
Учетный (инвентарный) номер ПЭВМ: 0410000985 и 0410000986

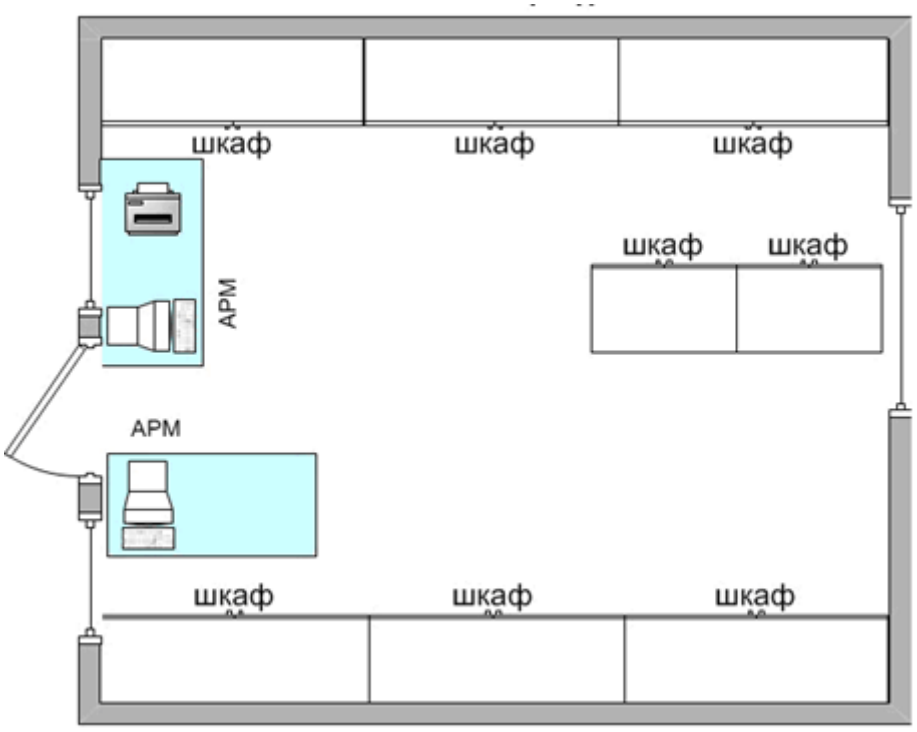

Рисунок 13 – Расположение технических средств в помещении кабинет 2

Таблица 4 - Состав комплекса технических средств ПЭВМ: 0410000985

№ п/п	Наименование	Тип (модель)	Серийный (Заводской) номер
1.	Системный блок	ATX	Без номера
2.	Мышь	Acer M-U0027-O	LZ216AV05LQ
3.	ИБП	APC BackUPS CS 500	4B1202P52965
4.	Монитор	Acer V223W	20901598542
5.	Клавиатура	Acer PR1101U	DKPS21P03N239AB489HU01

Таблица 5 - Перечень программных средств ПЭВМ: 0410000985

Наименование программного средства
1. Microsoft Windows 7 Professional Rus 32bit
2. "ГАРАНТ аэро" (Мобильная Онлайн) Текущий Пользователь
3. 7-Zip 9.20
4. Adobe Flash Player 11 ActiveX
5. Adobe Flash Player 11 Plugin
6. Canon MF Toolbox 4.9.1.1.mf11
7. Canon MF4400 Series
8. DAEMON Tools Lite
9. Google Chrome
10. Google Update Helper
11. Intel(R) Network Connections Drivers
12. Intel(R) Processor Graphics
13. Microsoft Office Professional Plus 2010
14. Microsoft Office профессиональный плюс 2010
15. Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.17
16. Mozilla Firefox 19.0.2 (x86 ru)
17. Mozilla Maintenance Service
18. Total Commander (Remove or Repair)
19. Total Commander 7.57a PowerPack
20. WinRAR 4.10 (32-разрядная)
21. Антивирус Касперского 6.0 для Windows Workstations [Русский (Россия)] 6.0.4.1611

Таблица 6- Состав комплекса технических средств ПЭВМ: 0410000986

№ п/п	Наименование	Тип (модель)	Серийный (Заводской) номер
1.	Системный блок	Acer	инв. №10104184
2.	Клавиатура	Acer PR1101U	DKPS21P03N239AB418HU01
3.	Мышь	Acer M-U0027-O	LZ216AV0VD3
4.	ИБП	APC BackUPS CS 500	4B1210P09033
5.	Монитор	Acer V223W	20901596342

Таблица 7- Перечень программных средств ПЭВМ: 0410000986

Наименование программного средства
1. Microsoft Windows 7 Professional Rus 32bit
2. 7-Zip 9.20
3. ABBYY FineReader 11 Corporate Edition
4. Acronis Disk Director 11 Home [Русский (Россия)]
5. Acronis True Image Home 2012 [Русский (Россия)]
6. Adobe Flash Player 11 ActiveX
7. Adobe Flash Player 11 Plugin
8. Adobe Reader X (10.1.0) - Russian [Русский (Россия)]
9. AIMP3
10. Canon MF Toolbox 4.9.1.1.mf11
11. Canon MF4400 Series
12. CCleaner
13. DAEMON Tools Lite
14. FastStone Image Viewer 4.6
15. Google Chrome
16. Google Update Helper
17. Intel(R) Network Connections Drivers
18. Intel(R) Processor Graphics
19. Kaspersky Internet Security 2011
20. K-Lite Codec Pack 8.4.0 (Full)
21. Microsoft Office 2010 Service Pack 1 (SP1)
22. Microsoft Office Professional Plus 2010
23. Microsoft Office Proof (English) 2010
24. Microsoft Office профессиональный плюс 2010
25. Microsoft Silverlight
26. Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.4148
27. Mozilla Firefox 10.0.2 (x86 ru)

Наименование программного средства
28.Opera 11.61 29.Realtek High Definition Audio Driver 30.TeamViewer 7 31.The KMPlayer (remove only) 32.Total Commander 7.56a Vi7Pack 1.85 (27.12.2011) 33.WinRAR 4.10 (32-разрядная) 34.Антивирус Касперского 2011 [Русский (Россия)]

АРМ инв.(уч.) № 0410001007 (этаж 2, кабинет 3)
Адрес организации: 440000, г. Петровск, ул. Больничная 10
Наименование корпуса/здания: корпус 1
Наименование помещения: кабинет №1
Учетный (инвентарный) номер ПЭВМ: 0410001007

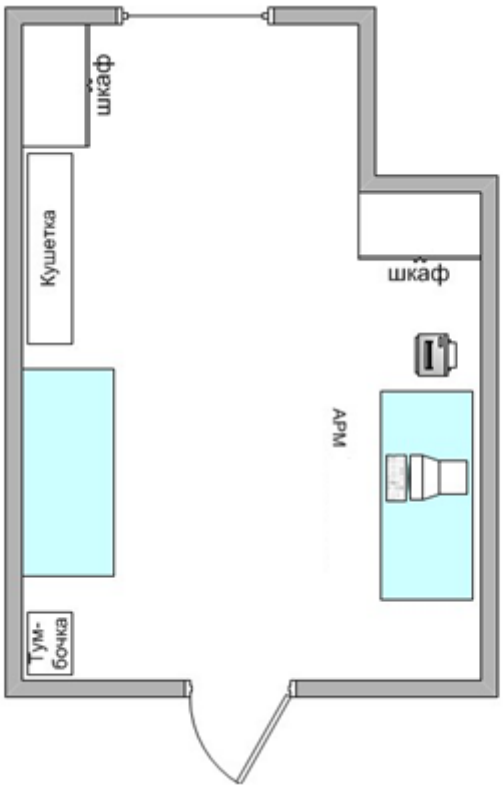

Рисунок 14 – Расположение технических средств в помещении кабинет 3

Таблица 8- Состав комплекса технических средств ПЭВМ: 0410001007

№ п/п	Наименование	Тип (модель)	Серийный (Заводской) номер
1.	Системный блок	AQUARIUS	без номера

№ п/п	Наименование	Тип (модель)	Серийный (Заводской) номер
2.	Монитор	ViewSonic VA2231wa	S13113420697
3.	Клавиатура	Acer PR1101U	DKPS21P03N239AB3A9HU01
4.	Мышь	Logitech B110	LZ130M20PT8
5.	МФУ	Canon MF4430	HCT50168

Таблица 9 - Перечень программных средств ПЭВМ: 0410001007

Наименование программного средства
1. Microsoft Windows 7 Professional Rus 64bit
2. Adobe Flash Player 11 ActiveX
3. Canon MF4400 Series
4. Intel(R) Management Engine Components
5. Intel(R) Processor Graphics
6. Microsoft .NET Framework 4 Client Profile RUS Language Pack [Русский (Россия)]
7. Microsoft .NET Framework 4 Client Profile
8. Microsoft Office 2010
9. Microsoft Office Starter 2010 - русский
10. Microsoft Office нажми и работай 2010 [Русский (Россия)]
11. Microsoft Office нажми и работай 2010
12. OpenOffice.org 3.4.1 [Русский (Россия)]
13. Realtek High Definition Audio Driver [Русский] 6.0.1.6449
14. Skype™ 5.6
15. TeamViewer 7
16. Антивирус Касперского 6.0 для Windows Workstations [Русский (Россия)] 6.0.4.1424
17. КриптоПро CSP [Русский (Россия)] 3.6.6497
18. Языковой пакет клиентского профиля Microsoft.NET Framework 4 - RUS

3 ОПРЕДЕЛЕНИЕ ОСНОВНЫХ НАПРАВЛЕНИЙ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

В соответствии с требованиями нормативно-методической документации ФСТЭК России по защите ПДн необходимо обеспечить защиту по следующим направлениям защиты:

- от утечки по каналам ПЭМИН;
- от видовой разведки;
- от несанкционированного доступа;
- от вирусов;
- от перехвата информации, циркулирующей по каналу связи и сетевых атак.

Исходя из результатов анализа актуальности угроз, приведенных в «Частной модели угроз безопасности персональных данных при их обработке в информационной системе персональных данных «Бухгалтерия» в ИСПДн необходимо обеспечить защиту от следующих угроз:

46) Угрозы утечки видовой информации.

47) Кражи, модификации, уничтожения информации.

48) Несанкционированное отключение средств защиты .

49) Действия вредоносных программ (вирусов).

50) Установка ПО, не связанного с исполнением служебных обязанностей.

51) Перехват паролей или идентификаторов.

52) Модификация базовой системы ввода/вывода (BIOS).

53) Перехват управления загрузкой.

54) Использование остаточной информации, «сбор мусора».

55) Программная закладка.

56) Утрата ключей и атрибутов доступа.

57) Непреднамеренное отключение средств защиты.

58) Непреднамеренное отключение средств защиты

59) Доступ к информации (модификация, уничтожение) лиц, не допущенных к ее обработке.

60) Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке.

61) Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации

62) Угрозы сканирования, направленные на выявление типа операционной системы АРМ, открытых портов и служб, открытых соединений и др.

63) Угрозы выявления паролей

64) Угрозы получения НСД путем подмены доверенного объекта

65) Угрозы типа «Отказ в обслуживании»

66) Угрозы удаленного запуска приложений

67) Угрозы внедрения по сети вредоносных программ

На ПЭВМ ИСПДн необходимо обеспечить защиту информации от НСД, от вирусов, от вредоносных программ, от сетевых атак, от раскрытия информации, циркулирующей в сетях и каналах связи общего пользования, от искажения информации, от ошибочных действий и нарушений требований по эксплуатации ИСПДн с установленными СЗИ лицами, санкционировано взаимодействующими с техническими и программными средствами ИСПДн, от аварий.

В помещениях размещения АРМ ИСПДн необходимо обеспечить защиту от хищения носителей информации.

4 ВЫБОР СПОСОБОВ И СРЕДСТВ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

– 4.1 Выбор способов защиты ПДн по направлениям защиты

Для защиты ПДн должны использоваться сертифицированные средства защиты информации и должны быть реализованы необходимые организационные меры защиты.

В ИСПДн предлагается использовать следующие средства защиты информации (СЗИ) в соответствии с таблице В3.

Таблица В3 – Выбор средств защиты информации по направлениям защиты

№ п/п	Направление защиты	Наименование СЗИ
1	Защита от несанкционированного доступа	СЗИ от НСД «Dallas Lock 8.0-K», организационные меры
2	Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий)	СЗИ от НСД «Dallas Lock 8.0-K», организационные меры
3	Угрозы уничтожения, хищения аппаратных средств ИСПДн, носителей информации путем физического доступа к элементам ИСПДн	Организационные меры
4	Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера	СЗИ от НСД «Dallas Lock 8.0-K», применение источников бесперебойного питания, организационные меры
5	Угрозы преднамеренных действий нарушителей	СЗИ от НСД «Dallas Lock 8.0-K», организационные меры
6	Защита от перехвата информации в канале связи и сетевых атак	Средство обнаружения вторжений (СОВ) со встроенным межсетевым экраном (МЭ) Security Studio Endpoint Protection Personal Firewall HIPS

Средство защиты информации «Dallas Lock 8.0-K», производимое ООО «Конфидент» (г. Москва), имеет сертификат ФСТЭК России № 2720 от 07.09.2015 г., выданный на соответствие требованиям руководящих документов "Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей" (Гостехкомиссия России, 1999 г.) – по 2 уровню контроля и «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1992 г.) – по 3 классу защищенности, а также может использоваться при создании ИСПДн до 1 класса включительно.

Планируемое к использованию средство обнаружения вторжений Security Studio Endpoint Protection имеет следующие сертификаты ФСТЭК России:

– № 2170, выдан 20 сентября 2010 года, подтверждает, что Security Studio Endpoint Protection Firewall является средством защиты от несанкционированного доступа к информации, не содержащей сведения, составляющие государственную тайну, соответствует требованиям на отсутствие НДВ по 4 уровню контроля и требованиям к межсетевым экранам по 4 классу защищенности.

№ 2171, выдан 20 сентября 2010 года, подтверждает, что Security Studio Endpoint Protection HIPS является программным средством защиты информации, предназначенным для обнаружения вторжений из внешних вычислительных сетей и соответствует требованиям на отсутствие НДВ по 4 уровню контроля.

– 4.2 Выбор способов защиты ПДн по актуальным угрозам

С помощью сертифицированных средств защиты информации и выполнения необходимых организационных мер возможна минимизация следующих актуальных угроз (таблица В4).

Таблица В4 – Способы защиты ПДн по актуальным угрозам

№ п/п	Направление защиты	Наименование средств защиты
1	Угрозы утечки видовой информации	Ограничение доступа в помещение, охрана в здании, на время работы с ПДн жалюзи должны быть закрыты, мониторы развернуты таким образом, чтобы исключалась возможность визуального просмотра содержимого на экранах
2	Кражи, модификации, уничтожения информации	Ограничение доступа в помещение, охрана в здании, решетки на окнах СЗИ от НСД «Dallas Lock 8.0-K»
3	Несанкционированное отключение средств защиты	СЗИ от НСД «Dallas Lock 8.0-K»
4	Действия вредоносных программ (вирусов)	Антивирус Касперского 6.0 для Windows Workstations; Kaspersky Endpoint Security 10 для Windows
5	Установка ПО, не связанного с исполнением служебных обязанностей	СЗИ от НСД «Dallas Lock 8.0-K» Инструкция пользователя ИСПДн
6	Перехват паролей или идентификаторов	СЗИ от НСД «Dallas Lock 8.0-K»
7	Модификация базовой системы ввода/вывода (BIOS)	Пароль на права пользователя и права администратора на BIOS Постоянный контроль пребывания посторонних лиц в помещении, в котором расположены элементы ИСПДн Осмотр системного блока до включения на предмет присутствия носителей, с которых возможна загрузка Проверка целостности пломб системного блока до включения питания
8	Перехват управления загрузкой	Пароль на права пользователя и права администратора на BIOS Постоянный контроль пребывания посторонних лиц в помещении, в котором расположены элементы ИСПДн Осмотр системного блока до включения на предмет присутствия носителей, с которых возможна загрузка Проверка целостности пломб системного блока до включения питания
9	Использование остаточной информации, «сбор мусора»	СЗИ от НСД «Dallas Lock 8.0-K»
1	Программная закладка	СЗИ от НСД «Dallas Lock 8.0-K»
1	Утрата ключей и атрибутов доступа	Парольная политика, политика «чистого стола», инструкции по работе пользователей, организационные меры
1	Непреднамеренная модификация (уничтожение) информации сотрудниками	СЗИ от НСД «Dallas Lock 8.0-K»

1	Непреднамеренное отключение средств защиты	Замки на двери, ограничение доступа в помещение, охрана в здании, инструктаж пользователей ИСПДн, инструкция по работе пользователей в ИСПДн СЗИ от НСД «Dallas Lock 8.0-K»
1	Доступ к информации (модификация, уничтожение) лиц, не допущенных к ее обработке	Контроль соблюдения режима безопасности ПДн, организационные меры СЗИ от НСД «Dallas Lock 8.0-K»
1	Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке	Инструктаж пользователей ИСПДн, контроль за выполнением существующих внутренних нормативно-распорядительных документов в области защиты ПДн
1	Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации	СОВ/МЭ «Security Studio Endpoint Protection», Инструкция по работе пользователей в ИСПДн
1	Угрозы сканирования, направленные на выявление типа операционной системы АРМ, открытых портов и служб, открытых соединений и др	СОВ/МЭ «Security Studio Endpoint Protection», Инструкция по работе пользователей в ИСПДн
1	Угрозы выявления паролей	СОВ/МЭ «Security Studio Endpoint Protection», Инструкция по работе пользователей в ИСПДн
1	Угрозы получения НСД путем подмены доверенного объекта	СОВ/МЭ «Security Studio Endpoint Protection» Инструкция по работе пользователей в ИСПДн
2	Угрозы типа «Отказ в обслуживании»	СОВ/МЭ «Security Studio Endpoint Protection», Инструкция по работе пользователей в ИСПДн
2	Угрозы удаленного запуска приложений	СОВ/МЭ «Security Studio Endpoint Protection», Инструкция по работе пользователей в ИСПДн Инструкция по предотвращению вирусного заражения
2	Угрозы внедрения по сети вредоносных программ	СОВ/МЭ «Security Studio Endpoint Protection», Антивирус Касперского 6.0 для Windows Workstations; Kaspersky Endpoint Security 10 для Windows Инструкция по работе пользователей в ИСПДн Инструкция по предотвращению вирусного заражения

– **4.3 Выбор мер по обеспечению безопасности персональных данных (п.9 приказа ФСТЭК России №21 от 18.02.2014 г.)**

Перечень мер, необходимых для обеспечения 3-го уровня защищенности ПДн при их обработке в ИСПДн «Бухгалтерия», приведен таблице В5.

3.1.Таблица В5 - Перечень необходимых мер и средств защиты информации

Номер и условное обозначение меры (Пдн)	**Меры по обеспечению безопасности персональных данных**	**Меры и средства защиты информации**
I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)		
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора	СЗИ от НСД «Dallas Lock 8.0-K»
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов	СЗИ от НСД «Dallas Lock 8.0-K», Организационные мероприятия
ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации	СЗИ от НСД «Dallas Lock 8.0-K», Организационные мероприятия
ИАФ.5	Защита обратной связи при вводе аутентификационной информации	СЗИ от НСД «Dallas Lock 8.0-K»
II. Управление доступом субъектов доступа к объектам доступа (УПД)		
УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей	СЗИ от НСД «Dallas Lock 8.0-K», Организационные мероприятия
УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа	СЗИ от НСД «Dallas Lock 8.0-K», Организационные мероприятия
УПД.3	Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами	СЗИ от НСД «Dallas Lock 8.0-K», Организационные мероприятия
УПД.4	Разделение полномочий (ролей) пользователей,	СЗИ от НСД «Dallas

Номер и условное обозначение меры (Пдн)	Меры по обеспечению безопасности персональных данных	Меры и средства защиты информации
	администраторов и лиц, обеспечивающих функционирование информационной системы	Lock 8.0-K», Организационные мероприятия
УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	СЗИ от НСД «Dallas Lock 8.0-K», Организационные мероприятия
УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)	СЗИ от НСД «Dallas Lock 8.0-K», Организационные мероприятия
УПД.10	Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу	СЗИ от НСД «Dallas Lock 8.0-K», Организационные мероприятия
УПД.11	Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации	СЗИ от НСД «Dallas Lock 8.0-K», Организационные мероприятия
УПД.13	Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети	СЗИ от НСД «Dallas Lock 8.0-K», АПКШ «Континент IPC-100», Организационные мероприятия
УПД.16	Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)	СЗИ от НСД «Dallas Lock 8.0-K», АПКШ «Континент IPC-100», Организационные мероприятия
III. Ограничение программной среды (ОПС)		
ОПС.3	Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов	СЗИ от НСД «Dallas Lock 8.0-K», Организационные мероприятия
IV. Защита машинных носителей информации (ЗНИ)		
ЗНИ.2	Управление доступом к машинным носителям персональных данных	СЗИ от НСД «Dallas Lock 8.0-K»
ЗНИ.3	Контроль перемещения машинных носителей персональных данных за пределы контролируемой зоны	Организационные мероприятия
ЗНИ.8	Уничтожение (стирание) или обезличивание персональных данных на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) или обезличивания	Организационные мероприятия
V. Регистрация событий безопасности (РСБ)		

Номер и условное обозначение меры (Пдн)	Меры по обеспечению безопасности персональных данных	Меры и средства защиты информации
РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения	СЗИ от НСД «Dallas Lock 8.0-K»
РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации	Организационные мероприятия
РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения	СЗИ от НСД «Dallas Lock 8.0-K», Организационные мероприятия
РСБ.7	Защита информации о событиях безопасности	СЗИ от НСД «Dallas Lock 8.0-K», Организационные мероприятия
VI. Антивирусная защита (АВЗ)		
АВЗ.1	Реализация антивирусной защиты	Антивирус Антивирус Касперского 6.0 для Windows Workstations; Kaspersky Endpoint Security 10 для Windows
АВЗ.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)	Антивирус Антивирус Касперского 6.0 для Windows Workstations; Kaspersky Endpoint Security 10 для Windows
VII. Обнаружение вторжений (СОВ)		
СОВ.1	Обнаружение вторжений	АПКШ «Континент IPC-100»
СОВ.2	Обновление базы решающих правил	АПКШ «Континент IPC-100»
VIII. Контроль (анализ) защищенности персональных данных (АНЗ)		
АНЗ.1	Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей	Организационные мероприятия
АНЗ.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации	СЗИ от НСД «Dallas Lock 8.0-K», организационные меры, ведение журнала учета мероприятий по контролю над соблюдением режима защиты персональных данных
АНЗ.3	Контроль работоспособности, параметров настройки и правильности функционирования	СЗИ от НСД «Dallas Lock 8.0-K»,

Номер и условное обозначение меры (Пдн)	Меры по обеспечению безопасности персональных данных	Меры и средства защиты информации
	программного обеспечения и средств защиты информации	организационные меры, ведение журнала учета мероприятий по контролю над соблюдением режима защиты персональных данных
АН3.4	Контроль состава технических средств, программного обеспечения и средств защиты информации	СЗИ от НСД «Dallas Lock 8.0-K», организационные меры, ведение журнала учета мероприятий по контролю над соблюдением режима защиты персональных данных
X. Обеспечение доступности персональных данных (ОДТ)		
ОДТ.4	Периодическое резервное копирование персональных данных на резервные машинные носители персональных данных	Организационные мероприятия
XII. Защита технических средств (ЗТС)		
ЗТС.2	Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования	Замки на дверях, охрана в здании, наличие сейфа (мет. шкафа) для хранения устройств и носителей информации
ЗТС.3	Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены	Замки на дверях, охрана в здании, наличие сейфа (мет. шкафа) для хранения устройств и носителей информации
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр	Замки на дверях, охрана в здании, наличие сейфа (мет. шкафа) для хранения устройств и носителей информации
XIII. Защита информационной системы, ее средств и систем связи и передачи данных (ЗИС)		
ЗИС.3	Обеспечение защиты персональных данных от	СКЗИ КриптоПро CSP

Номер и условное обозначение меры (Пдн)	Меры по обеспечению безопасности персональных данных	Меры и средства защиты информации
	раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи	
ЗИС.11	Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов	СКЗИ КриптоПро CSP
XV. Управление конфигурацией информационной системы и системы защиты персональных данных (УКФ)		
УКФ.1	Определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и системы защиты персональных данных	Организационные мероприятия
УКФ.2	Управление изменениями конфигурации информационной системы и системы защиты персональных данных	СЗИ от НСД «Dallas Lock 8.0-K», Организационные мероприятия
УКФ.3	Анализ потенциального воздействия планируемых изменений в конфигурации информационной системы и системы защиты персональных данных на обеспечение защиты персональных данных и согласование изменений в конфигурации информационной системы с должностным лицом (работником), ответственным за обеспечение безопасности персональных данных	Организационные мероприятия
УКФ.4	Документирование информации (данных) об изменениях в конфигурации информационной системы и системы защиты персональных данных	Организационные мероприятия

5 РЕШЕНИЕ ВОПРОСОВ УПРАВЛЕНИЯ ЗАЩИТОЙ ПДН

– 5.1 Организация охраны ИСПДн и ее составных частей

Необходимо исключить неконтролируемое присутствие посторонних лиц в местах размещения ПЭВМ ИСПДн и ее составных частей (отдельных ПЭВМ, кабелей в случае передачи по ним защищаемой информации в незашифрованном виде).

– **5.2 Управление защитой ПДн**

Необходимо:

обеспечить служебную связь между администратором безопасности и пользователями ИСПДн, посредством телефонной связи, электронной почты и т.п., сигнализацию опасных событий;

обеспечить взаимодействие между пользователями и администратором ИСПДн, администратором безопасности;

обеспечить периодическое обслуживание систем защиты информации на месте эксплуатации;

обеспечить резервирование критически важной информации (создание копий на тех же самых несъемных ЖМД и на съемных носителях информации), а также резервирование аппаратного обеспечения (отдельных блоков, элементов);

исключить наличие в составе ПО ИСПДн средств разработки и отладки программного обеспечения;

разработать внутреннюю документацию на ИСПДн, в которой отразить функции, права, обязанности, ответственность пользователей и администратора безопасности при работе в ИСПДн;

проработать следующие вопросы в динамике изменения обстановки и контроля эффективности защиты:

распределение функций управления доступом к данным и их обработкой между должностными лицами;

определение порядка изменения правил доступа к защищаемой информации;

определение порядка действий должностных лиц в случае возникновения нештатных ситуаций;

определение порядка проведения контрольных мероприятий и действий по его результатам.

Действия персонала при наступлении данных ситуаций также должны быть отражены во внутренней документации на ИСПДн.

6 РЕШЕНИЕ ВОПРОСОВ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ПДН

– 6.1 Решение финансовых вопросов обеспечения защиты ПДн

Для обеспечения защиты ПДн при их обработке в ИСПДн необходимо предусмотреть следующие затраты:

Затраты на приобретение необходимых аппаратных средств;

Затраты на приобретение необходимых лицензионных программных средств;

Затраты на приобретение необходимых сертифицированных средств защиты;

Затраты на проведение установки и настройки средств защиты;

Затраты на проведение аттестационных испытаний;

Затраты на обучение персонала.

– 6.2 Решение технических и программных вопросов обеспечения защиты ПДн

Все используемое в ИСПДн программное обеспечение должно быть лицензионным либо свободно-распространяемым.

После установки средств защиты (аппаратных) корпус системного блока должен быть опечатан. Данное опечатывание служит для защиты от вскрытия системного блока и изъятия из него средств защиты. Печати могут быть выполнены в любом виде, обеспечивающим невозможность восстановления целостности печати злоумышленником после вскрытия в течение всего срока существования ИСПДн. Место опечатывания должно быть таким, чтобы его можно было визуально контролировать.

Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены СКЗИ или хранятся ключевые документы к ним (далее – режимные помещения), должны обеспечивать сохранность ПДн, СКЗИ или ключевых документов к ним.

Режимные помещения должны иметь прочные входные двери с замками, гарантирующими надежное закрытие помещений в нерабочее время.

Должен осуществляться постоянный контроль пребывания посторонних лиц в помещении, в котором расположены элементы ИСПДн. До включения питания компьютера системный блок должен быть осмотрен на предмет присутствия носителей, с которых возможен перехват загрузки, а также на предмет целостности пломб.

При оставлении помещений расположения ИСПДн пользователями должны быть приняты меры по недопущению в данные помещения посторонних лиц. Особенно это касается нерабочего времени, когда помещения надолго остаются без присмотра.

Заземление технических средств и оборудования ИСПДн необходимо осуществлять через «евророзетки», используя штатные сетевые кабели, на контур заземления, расположенный в пределах КЗ.

При расположении устройств отображения информации и печатающих устройств ИСПДн должен быть исключен или затруднен просмотр текстовой и графической информации (защита видовой информации). Окна помещений размещения вышеуказанных устройств должны оснащаться шторами или жалюзи для защиты видовой информации.

– 6.3 Решение информационных вопросов обеспечения защиты ПДн

Должны быть разработаны инструкции для персонала (пользователей, администраторов безопасности) и доведены до их сведения. В инструкциях должны быть отражены права, обязанности, функции, ответственность персонала, действия персонала при возникновении нештатных ситуаций.

Должны быть разработаны инструкции пользователя, администратора безопасности, инструкция по ведению антивирусного контроля.

При необходимости должно проводиться обучение администратора и пользователей в учебных центрах разработчиков систем защиты по соответствующим курсам.

– 6.4 Решение кадровых вопросов обеспечения защиты ПДн

Должен быть определен список лиц, имеющих право работы на различных элементах, входящих в ИСПДн.

Сотрудники должны быть ознакомлены со своими персональными обязанностями, с порядком работы в ИСПДн, в том числе с правилами работы с сертифицированными средствами защиты информации, а также должны быть проинформированы об ответственности за разглашение персональных данных других субъектов ПДн.

Должны быть назначены ответственные из числа сотрудников, в задачу которых входил бы контроль отсутствия в помещениях размещения элементов ИСПДн посторонних лиц, за исключением лиц, находящихся в помещениях для выполнения служебных обязанностей. Бесконтрольное пребывание в помещении, в котором размещены технические средства ИСПДн, посторонних лиц должно быть исключено.

Для обеспечения нормального функционирования СЗИ от НСД и применяемых (планируемых к применению) СОВ и МЭ должен быть назначен минимум один человек, выполняющий функции администратора безопасности. Данный человек должен обладать знаниями в части принципов работы операционных систем, прикладного программного обеспечения, СЗИ, СКЗИ и нормативных актов Российской Федерации в области защиты информации.

7 СОСТАВ, СТОИМОСТЬ ВЫПОЛНЕНИЯ РАБОТ ПО СОЗДАНИЮ СЗПДН

– 7.1 Стоимость сертифицированных средств защиты.

Таблица В6 – стоимость внедрения средств защиты информации

№ п/п	Наименование	Цена, руб	Кол-во, шт.	Сумма, руб.	НДС в сумме, руб
1	Право на использование Dallas Lock 8.0-K	7 500,00	10	75 000,00	без ндс
2	Сертифицированный комплект для установки Dallas Lock 8.0	500,00	10	5 000,00	762,71
3	Право на использование Средств защиты информации Security Studio Endpoint Protection: Personal Firewall, HIPS.	2 600,00	10	26 000,00	без ндс
4	Установочный комплект Security Studio Endpoint Protection: Antivirus, Personal Firewall, HIPS	500,00	10	5 000,00	762,71
5	Право на использование Сканер-ВС стандартная версия, лицензия на 64-IP адресов на год	30 000,00	1	30 000,00	без ндс
6	Установочный комплект "Сканер-ВС" стандартная версия	1 600,00	1	1 600,00	244,07
7	Установка и настройка средств защиты информации	1 500,00	10	15 000,00	2 288,14
			Итого:	157 600,00	4 057,63

– 7.2 Стоимость проведения аттестационных испытаний

3.2.Таблица В7 – Стоимость проведения аттестационных испытаний

№ п/п	Наименование	Цена, руб	Кол-во, шт.	Сумма, руб.	НДС в сумме, руб.
1	Аттестационные испытания ИСПДн на соответствие требованиям безопасности информации с оформлением результатов	15 000,00	10	150 000,00	137 288,14
			Итого:	150 000,00	22 881,36

8 ЭТАПЫ ВЫПОЛНЕНИЯ РАБОТ ПО СОЗДАНИЮ СЗПДН

Ниже приводятся этапы выполнения работ по созданию СЗПДн. Сроки выполнения этапов являются примерными.

- **8.1 Поставка средств защиты информации**

Поставка средств защиты информации осуществляется в течение 15 рабочих дней.

- **8.2 Установка и настройка средств защиты информации**

Установка и настройка средств защиты информации осуществляется в течение 10 рабочих дней с момента завершения этапа 8.1 силами Заказчика и оформляется актом установки/настройки средств защиты.

- **8.3 Опытная эксплуатация СЗПДн**

Опытная эксплуатация СЗПДн осуществляется в течение 5 рабочих дней с момента завершения этапа 8.2. и оформляется актом ввода СЗПДн в опытную эксплуатацию.

- **8.4 Проведение аттестационных испытаний на соответствие требованиям безопасности информации**

Проведение данного этапа осуществляется в течение 5 рабочих дней с момента завершения этапа 8.3.

Перед проведением аттестационных испытаний Исполнитель разрабатывает и передает Заказчику на согласование документ «Программа и методики проведения аттестационных испытаний информационной системы персональных данных «Бухгалтерия» на соответствие требованиям безопасности информации».

По итогам проведением аттестационных испытаний Исполнитель разрабатывает и передает Заказчику следующие документы:

Протокол испытаний комплексной системы защиты информации информационной системы персональных данных «Бухгалтерия», на соответствие требованиям безопасности информации в части защиты от НСД и компьютерных вирусов.

Заключение по результатам проведения аттестационных испытаний информационной системы персональных данных «Бухгалтерия», на соответствие требованиям безопасности информации.

Предписание на эксплуатацию информационной системы персональных данных «Бухгалтерия».

Аттестат соответствия информационной системы персональных данных «Бухгалтерия» требованиям безопасности информации;

Счет-фактура и акт выполненных работ.

ЗАКЛЮЧЕНИЕ

В результате применения в ИСПДн предложенных сертифицированных средств защиты информации: СОВ/МЭ «Security Studio Endpoint Protection», СЗИ от НСД «Dallas Lock 8.0-K», а также выполнения организационных мер (разработка и утверждение приказов, актов, инструкций и других организационно-распорядительных документов, описывающих и регламентирующих действия назначенных лиц в штатных и нештатных ситуациях при эксплуатации ИСПДн) и внедрения технических средств защиты (средства охраны) актуальные для ИСПДн угрозы исключаются или возможность их реализации сводится к минимуму.

Таким образом, в результате выполнения этих мероприятий будут обеспечены требуемые характеристики безопасности ПДн, хранящихся и обрабатываемых в ИСПДн, и данные ИСПДн будут готовы к проведению аттестации по требованиям безопасности ПДн. Конфигурация ИСПДн после установки средств защиты представлена в Приложении А.

Последующая аттестации по требованиям безопасности ПДн будет завершающим этапом в процессе создания и ввода в эксплуатацию СЗПДн.

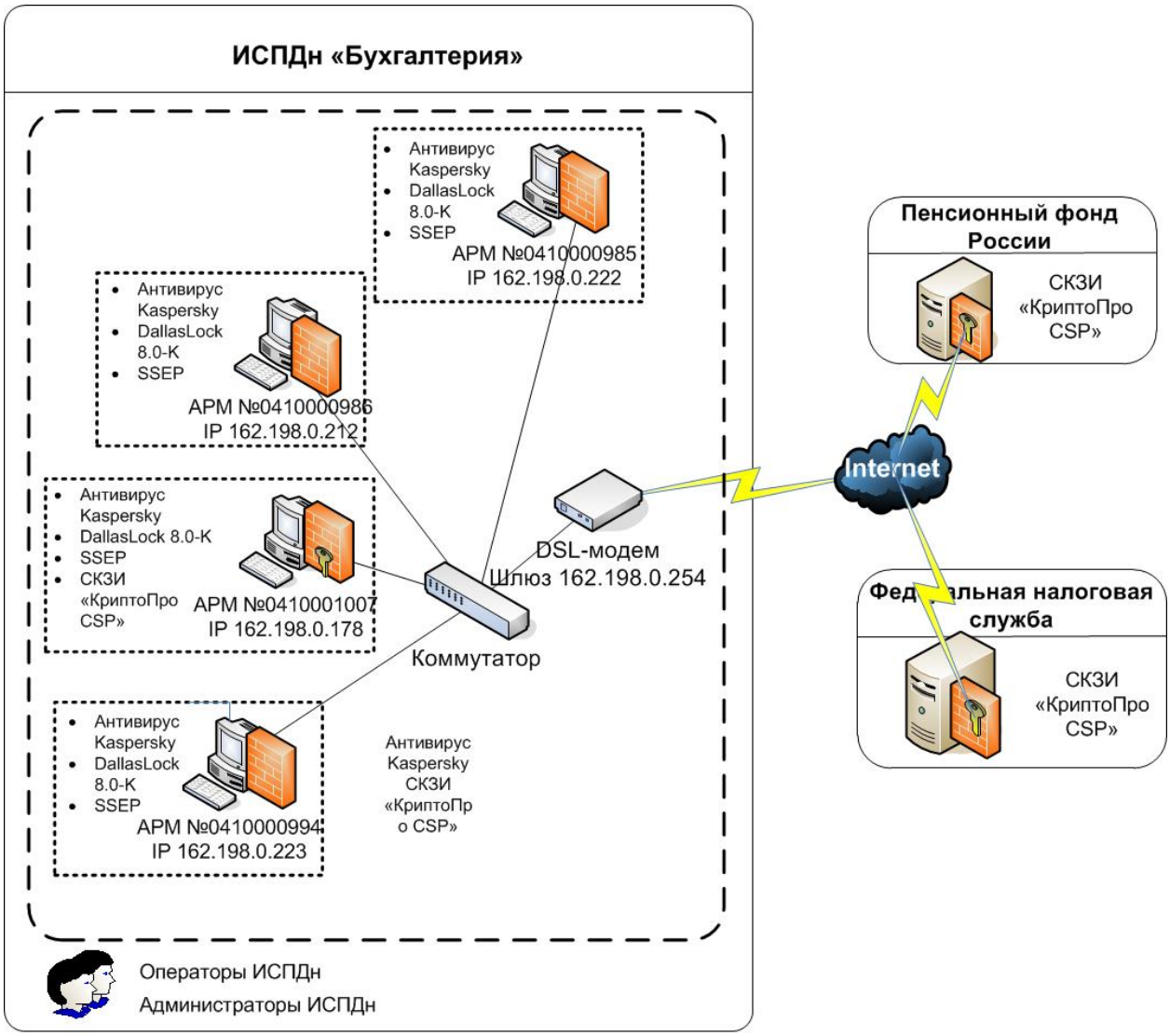

Рис. В2 - Конфигурация ИСПДн после установки средств защиты