Утверждаю:
И.о. генерального директора
АО «ГМСК «Заполярье»

_____ О.В. Геращенко
«09» января 2019 г.

Модель
угроз безопасности персональных данных при их обработке в информационной системе персональных данных Акционерного общества «Государственная медицинская страховая компания «Заполярье»

2019 г.

СОДЕРЖАНИЕ

Введение 3

1 ИСПДн "Полис ОМС", "ОМС Эксперт", "1С предприятие", "1С зарплата, управление персоналом", "1С Бухгалтерия" 3

1.1 Структура ИСПДн 3
1.2 Состав и структура персональных данных 4
1.3 Конфигурация ИСПДн 5
1.4 Структура обработки ПДн 6
1.5 Режим обработки ПДн 8
1.6 Классификация нарушителей 11
1.7 Исходный уровень защищенности ИСПДн 15
1.8 Вероятность реализации УБПДн 16
1.9 Реализуемость угроз 28
1.10 Оценка опасности угроз 30
1.11 Определение актуальности угроз в ИСПДн 32
1.12 Модель угроз безопасности 35
1.13 Заключение 35

ВВЕДЕНИЕ

Модель угроз безопасности персональных данных (далее – Модель) при их обработке в ИСПДн строится на основании Отчета о результатах проведения внутренней проверки.

В модели угроз представлено описание структуры ИСПДн, состава и режима обработки ПДн, классификация потенциальных нарушителей, оценку исходного уровня защищенности, анализ угроз безопасности персональных данных.

Анализ УБПДн включает:

Описание угроз.

Оценку вероятности возникновения угроз.

Оценку реализуемости угроз.

Оценку опасности угроз.

Определение актуальности угроз.

В заключении даны рекомендации по мерам защиты для уменьшения опасности актуальных угроз ИСПДн "Полис ОМС", "ОМС Эксперт-6", "1С предприятие", "1С зарплата, управление персоналом", "1С Бухгалтерия".

Структура ИСПДн

Таблица 1 – Параметры ИСПДн

Заданные характеристики безопасности персональных данных	Специальная информационная система
Структура информационной системы	Распределенная информационная система
Подключение информационной системы к сетям общего пользования и (или) сетям международного информационного обмена	Имеется
Режим обработки персональных данных	Многопользовательская система
Режим разграничения прав доступа пользователей	Система с разграничение доступа
Местонахождение технических средств информационной системы	Все технические средства находятся в пределах Российской Федерации Ямало-Ненецкий автономный округ г. Салехард, ул. Маяковского 4
Дополнительная информация	К персональным данным предъявляется требование целостности

Состав и структура персональных данных

В ИСПДн "Полис ОМС" обрабатываются следующие персональные данные:

- Фамилия;
- Имя;
- Отчество;
- Пол;
- Дата рождения;
- Возраст;
- Страховой полис;
- Данные документа удостоверяющего личность гражданина (номер, серия, дата выдачи, кем выдан).

Исходя из состава обрабатываемых персональных данных, можно сделать вывод, что они относятся к **2 категории персональных данных.**

Объем обрабатываемых персональных данных, **превышает 100000 записей** о субъектах персональных данных.

В ИСПДн "ОМС Эксперт-6" обрабатываются следующие персональные данные:

- Фамилия
- Имя
- Отчество
- Пол
- Дата рождения;
- Гражданство;
- Состояние о здоровье застрахованных лиц;
- Данные документа удостоверяющего личность гражданина (номер, серия, дата выдачи, кем выдан);

Исходя из состава обрабатываемых персональных данных, можно сделать вывод, что они относятся к **1 категории персональных данных**

Объем обрабатываемых персональных данных, **не превышает 100000 записей** о субъектах персональных данных.

Конфигурация ИСПДн "Полис ОМС", "ОМС Эксперт".

На рисунке 1 представлена конфигурация элементов ИСПДн.

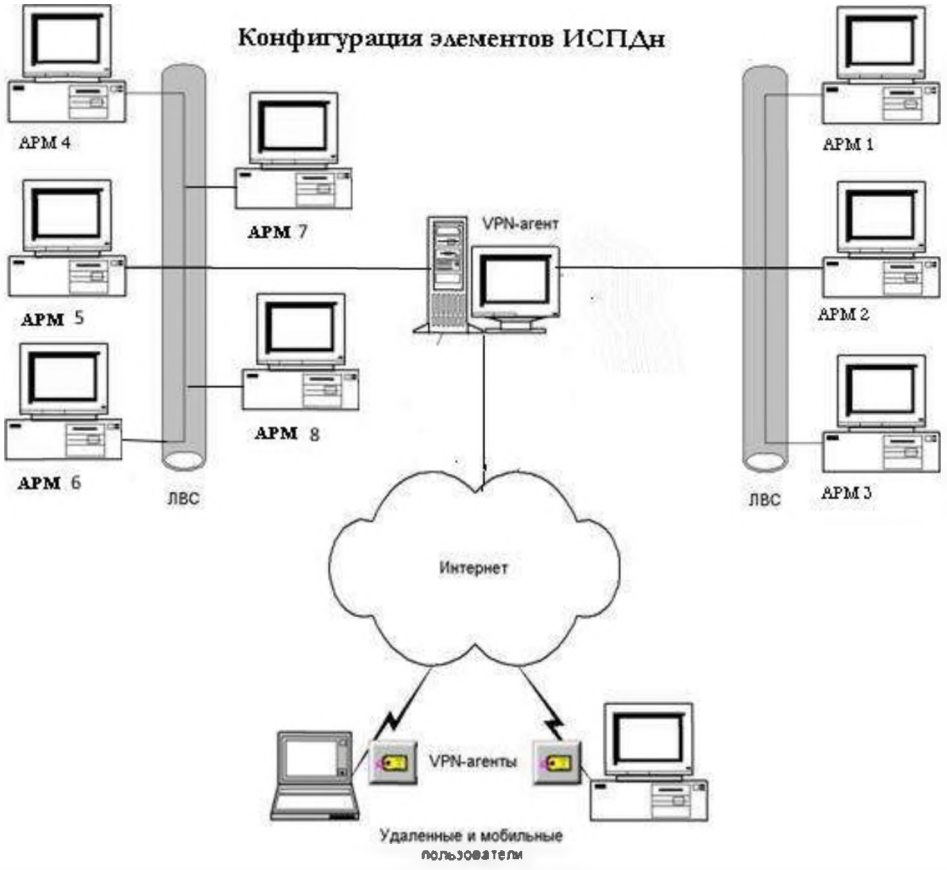

Рис. 1

На рисунке 2 представлено территориальное расположение ИСПДн относительно контролируемой зоны.

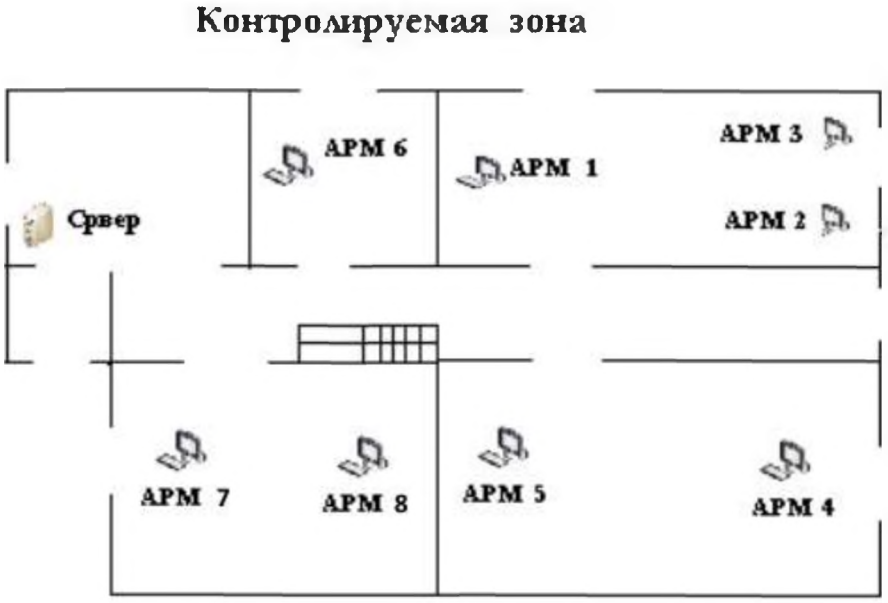

Рис. 2

Структура обработки ПДн

В ИСПДн «ОМС Эксперт-6", обработка персональных данных происходит следующим образом:

1) Оператор авторизуется на своем рабочем месте в ОС Windows 7, 8 в домене.

2) Оператор авторизуется в программе "ОМС Эксперт".

3) Сотрудник получает данные из лечебно профилактических учреждений (по защищенной сети VIpNet), проводит экспертизу и направляет данные в Окружной фонд обязательного медицинского страхования Ямало-Ненецкого автономного округа.

4) Данные хранятся на сервере Firebird.

Структура обработки ПДн

В ИСПДн «Полис ОМС" «обработка персональных данных происходит следующим образом:

1. Сотрудник авторизуется на своем рабочем месте в ОС Windows 7 в домене.

2. Сотрудник авторизуется в программе "Полис ОМС".

3. Сотрудник работает с посетителями, выдача, продление, аннулирование полисов медицинского страхования.

4. Данные хранятся на сервере Firebird.

Состав и структура персональных данных

В ИСПДн "1С предприятие", "1С зарплата, управление персоналом", "1С Бухгалтерия" обрабатываются следующие персональные данные:

- Фамилия;
- Имя;
- Отчество;
- Пол;
- Дата рождения;
- Возраст;
- Страховой полис;
- ИНН;
- Зарплата;
- Данные документа удостоверяющего личность гражданина (номер, серия, дата выдачи, кем выдан).

Исходя из состава обрабатываемых персональных данных, можно сделать вывод, что они относятся **к 2 категории персональных данных.**

Объем обрабатываемых персональных данных, **не превышает 1000 записей** о субъектах персональных данных.

Конфигурация ИСПДн, "1С предприятие", "1С зарплата, управление персоналом", "1С Бухгалтерия".

На рисунке 3 представлена конфигурация элементов ИСПДн.

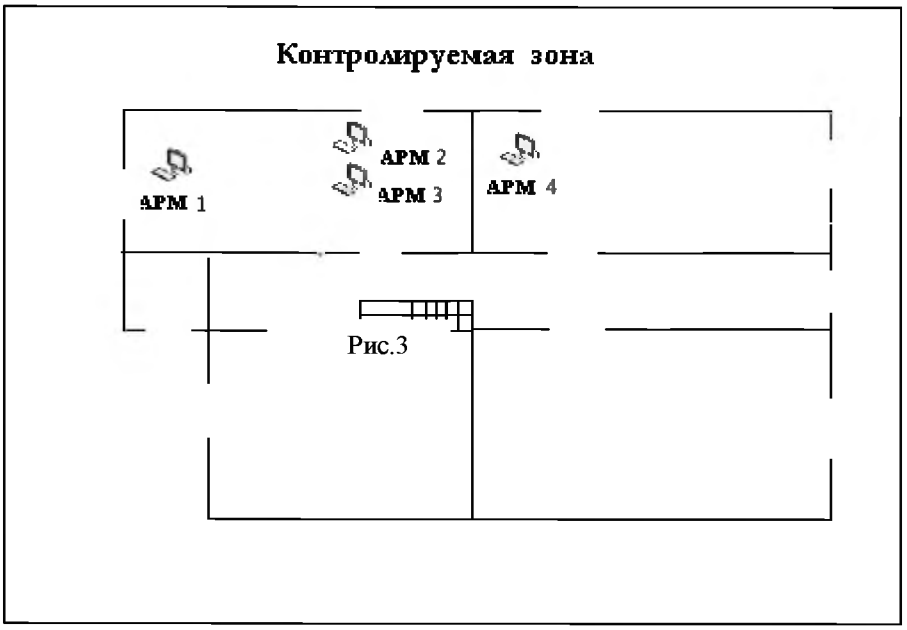

Рис.3

Рис.4

На рисунке 4 представлено территориальное расположение ИСПДн относительно контролируемой зоны

Структура обработки ПДн

В ИСПДн «1С предприятие", "1С зарплата, управление персоналом", "1С Бухгалтерия" обработка персональных данных происходит следующим образом:

5) Сотрудник авторизуется на своем рабочем месте в ОС Windows.

6) Сотрудник авторизуется в программах "1С предприятие", "1С зарплата, управление персоналом", "1С Бухгалтерия".

7) Сотрудник обрабатывает персональные данные работников.

8) Данные хранятся на сервере.

Режим обработки ПДн

В ИСПДн "Полис ОМС", "ОМС Эксперт", "1С предприятие", "1С зарплата, управление персоналом", "1С Бухгалтерия" обработка персональных данных осуществляется в многопользовательском режиме с разграничением с разграничения прав доступа.

Режим обработки предусматривает следующие действия с персональными данными: сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Все пользователи ИСПДн имеют собственные роли. Список типовых ролей представлен в виде матрицы доступа в таблице 2.

Таблица 2 – Матрица доступа

Группа	Уровень доступа к ПДн	Разрешенные действия	Сотрудники отдела
Системный администратор	Обладает полной информацией о системном и прикладном программном обеспечении ИСПДн. "1С предприятие", "1С зарплата, управление персоналом", "1С Бухгалтерия" (далее – ИСПДн 1С) Обладает полной информацией о технических средствах и конфигурации ИСПДн 1С Имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн 1С. Обладает правами конфигурирования и административной настройки технических средств ИСПДн 1С.	- сбор - систематизация - накопление - хранение - уточнение - использование - уничтожение	Кропочев М.И.
Программист	Обладает правами Администратора ИСПДн "Полис ОМС", "ОМС Эксперт-6". Обладает полной информацией об ИСПДн "Полис ОМС", "ОМС Эксперт-6". Имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн "Полис ОМС", "ОМС Эксперт-6".	- сбор - систематизация - накопление - хранение - уточнение - использование - уничтожение	Буянов М.В.

	Не имеет прав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных).		
Операторы ИСПДн с правами записи	Обладает всеми необходимыми атрибутами и правами, обеспечивающими доступ ко всем ПДн "1С предприятие", "1С зарплата, управление персоналом", "1С Бухгалтерия".	- сбор - систематизация - накопление - хранение - уточнение - использование	Бухгалтерия: 1. Козлова Н.И. 2. Дегтярева А.М. 3. Константинова Л.А.
Операторы ИСПДн с правами записи	Обладает всеми необходимыми атрибутами и правами, обеспечивающими доступ ко всем ПДн "ОМС Эксперт-6" .	- сбор - систематизация - накопление - хранение - уточнение - использование	1.Тодорова О.А. 2.Кондыгина Н.И.
Операторы ИСПДн с правами записи	Обладает всеми необходимыми атрибутами и правами, обеспечивающими доступ ко всем ПДн. "Полис ОМС"	- сбор - систематизация - накопление - хранение - уточнение - использование	Отдел медицинской экспертизы и страхования 1. Белоконь А.В. 2. Московская Д.В. 3. Рочева Т.П. 4. Худи Е.Д. 5. Кордова Л.Н.
Операторы ИСПДн с правами записи	Обладает всеми необходимыми атрибутами и правами, обеспечивающими доступ к подмножеству ПДн. "1С зарплата, управление персоналом"	- сбор - накопление - хранение - использование	Отдел кадров: 1. Диброва Д.А.
Операторы ИСПДн с правами чтения	Обладает всеми необходимыми атрибутами и правами, обеспечивающими доступ к подмножеству ПДн. «ОМС Эксперт-6»	- использование	Отдел медицинской экспертизы и страхования: Геращенко О.В. Терещенко Е.Н. Булдашева Т.С.

Классификация нарушителей

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.

1.1.1 Внешний нарушитель

В качестве внешнего нарушителя информационной безопасности, рассматривается нарушитель, который не имеет непосредственного доступа к техническим средствам и ресурсам системы, находящимся в пределах контролируемой зоны.

Предполагается, что внешний нарушитель не может воздействовать на защищаемую информацию по техническим каналам утечки, так как объем информации, хранимой и обрабатываемой в ИСПДн, является недостаточным для возможной мотивации внешнего нарушителя к осуществлению действий, направленных утечку информации по техническим каналам утечки.

Предполагается, что внешний нарушитель может воздействовать на защищаемую информацию только во время ее передачи по каналам связи.

1.1.2 Внутренний нарушитель

Возможности внутреннего нарушителя существенным образом зависят от действующих в пределах контролируемой зоны ограничительных факторов, из которых основным является реализация комплекса организационно-технических мер, в том числе по подбору, расстановке и обеспечению высокой профессиональной подготовки кадров, допуску физических лиц внутрь контролируемой зоны и контролю за порядком проведения работ, направленных на предотвращение и пресечение несанкционированного доступа.

Система разграничения доступа ИСПДн обеспечивает разграничение прав пользователей на доступ к информационным, программным, аппаратным и другим ресурсам ИСПДн в соответствии с принятой политикой информационной безопасности (правилами). К внутренним нарушителям могут относиться:

– системный администратор (категория I);

– программист (категория II);

– пользователи ИСПДн (категория III);

– пользователи, являющиеся внешними по отношению к конкретной АС (категория IV);

– лица, обладающие возможностью доступа к системе передачи данных (категория V);

– сотрудники АО «ГМСК «Заполярье», имеющие санкционированный доступ в служебных целях в помещения, в которых размещаются элементы ИСПДн, но не имеющие права доступа к ним (категория VI);

– обслуживающий персонал АО «ГМСК «Заполярье» (работники инженерно–технических служб и т.д.) (категория VII);

– уполномоченный персонал разработчиков ИСПДн, который на договорной основе имеет право на техническое обслуживание и модификацию компонентов ИСПДн (категория VIII).

На лиц категорий I и II возложены задачи по администрированию программно-аппаратных средств и баз данных ИСПДн для интеграции и обеспечения взаимодействия различных подсистем, входящих в состав ИСПДн. Администраторы потенциально могут реализовывать угрозы ИБ, используя возможности по непосредственному доступу к защищаемой информации, обрабатываемой и хранимой в ИСПДн, а также к техническим и программным средствам ИСПДн, включая средства защиты, используемые в конкретных АС, в соответствии с установленными для них административными полномочиями.

Эти лица хорошо знакомы с основными алгоритмами, протоколами, реализуемыми и используемыми в конкретных подсистемах и ИСПДн в целом, а также с применяемыми принципами и концепциями безопасности.

Предполагается, что они могли бы использовать стандартное оборудование либо для идентификации уязвимостей, либо для реализации угроз ИБ. Данное оборудование может быть, как частью штатных средств, так и может относиться к легко получаемому (например, программное обеспечение, полученное из общедоступных внешних источников).

Кроме того, предполагается, что эти лица могли бы располагать специализированным оборудованием.

К лицам категорий I и II ввиду их исключительной роли в ИСПДн должен применяться комплекс особых организационно-режимных мер по их подбору, принятию на работу, назначению на должность и контролю выполнения функциональных обязанностей.

Предполагается, что в число лиц категорий I и II будут включаться только доверенные лица и поэтому указанные лица исключаются из числа вероятных нарушителей.

Предполагается, что лица категорий III-VIII относятся к вероятным нарушителям.

Предполагается, что возможность сговора внутренних нарушителей маловероятна ввиду принятых организационных и контролирующих мер.

1.1.3 Предположения об имеющейся у нарушителя информации об объектах реализации угроз

В качестве основных уровней знаний нарушителей об АС можно выделить следующие:

общая информация – информации о назначения и общих характеристиках ИСПДн;

эксплуатационная информация – информация, полученная из эксплуатационной документации;

чувствительная информация – информация, дополняющая эксплуатационную информацию об ИСПДн (например, сведения из проектной документации ИСПДн).

В частности, нарушитель может иметь:

данные об организации работы, структуре и используемых технических, программных и программно-технических средствах ИСПДн;

сведения об информационных ресурсах ИСПДн: порядок и правила создания, хранения и передачи информации, структура и свойства информационных потоков;

– данные об уязвимостях, включая данные о недокументированных (недекларированных) возможностях технических, программных и программно-технических средств ИСПДн;

– данные о реализованных в ПСЗИ принципах и алгоритмах;

– исходные тексты программного обеспечения ИСПДн;

– сведения о возможных каналах реализации угроз;

– информацию о способах реализации угроз.

Предполагается, что лица категории III и категории IV владеют только эксплуатационной информацией, что обеспечивается организационными мерами. При этом лица категории IV не владеют парольной, аутентифицирующей и ключевой информацией, используемой в АИС, к которым они не имеют санкционированного доступа.

Предполагается, что лица категории V владеют в той или иной части чувствительной и эксплуатационной информацией о системе передачи информации и общей информацией об АИС, использующих эту систему передачи информации, что обеспечивается организационными мерами. При этом лица категории V не владеют парольной и аутентифицирующей информацией, используемой в АИС.

Предполагается, что лица категории VI и лица категории VII по уровню знаний не превосходят лица категории V.

Предполагается, что лица категории VIII обладают чувствительной информацией об ИСПДн и функционально ориентированных АИС, включая информацию об уязвимостях технических и программных средств ИСПДн. Организационными мерами предполагается исключить доступ лиц категории VIII к техническим и программным средствам ИСПДн в момент обработки с использованием этих средств защищаемой информации.

Таким образом, наиболее информированными об АИС являются лица категории III и лица категории VIII.

Степень информированности нарушителя зависит от многих факторов, включая реализованные в ЛПУ конкретные организационные меры и компетенцию нарушителей. Поэтому объективно оценить объем знаний вероятного нарушителя в общем случае практически невозможно.

В связи с изложенным, с целью создания определенного запаса прочности предполагается, что вероятные нарушители обладают всей информацией, необходимой для подготовки и реализации угроз, за исключением информации, доступ к которой со стороны нарушителя исключается системой защиты информации. К такой информации, например, относится парольная, аутентифицирующая и ключевая информация.

1.1.4 Предположения об имеющихся у нарушителя средствах реализации угроз

Предполагается, что нарушитель имеет:

– аппаратные компоненты СЗПДн и СФ СЗПДн;

– доступные в свободной продаже технические средства и программное обеспечение;

специально разработанные технические средства и программное обеспечение.

Внутренний нарушитель может использовать штатные средства.

Состав имеющихся у нарушителя средств, которые он может использовать для реализации угроз ИБ, а также возможности по их применению зависят от многих факторов, включая реализованные на объектах ЛПУ конкретные организационные меры, финансовые возможности и компетенцию нарушителей. Поэтому объективно оценить состав имеющихся у нарушителя средств реализации угроз в общем случае практически невозможно.

Поэтому, для создания устойчивой СЗПДн предполагается, что вероятный нарушитель имеет все необходимые для реализации угроз средства, возможности которых не превосходят возможности аналогичных средств реализации угроз на информацию, содержащую сведения, составляющие государственную

тайну, и технические и программные средства, обрабатывающие эту информацию.

Вместе с тем предполагается, что нарушитель не имеет:

– средств перехвата в технических каналах утечки;

– средств воздействия через сигнальные цепи (информационные и управляющие интерфейсы СВТ);

– средств воздействия на источники и через цепи питания;

– средств воздействия через цепи заземления;

– средств активного воздействия на технические средства (средств облучения).

Предполагается, что наиболее совершенными средствами реализации угроз обладают лица категории III и лица категории VIII.

Исходный уровень защищенности ИСПДн "Полис ОМС", "ОМС Эксперт", "1С предприятие", "1С зарплата, управление персоналом", "1С Бухгалтерия".

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

В таблице представлены характеристики уровня исходной защищенности для ИСПДн.

Таблица 3 – Исходный уровень защищенности

Позиция	Технические и эксплуатационные характеристики	Уровень защищенности
1	По территориальному размещению	Высокий
2	По наличию соединения с сетями общего пользования	Высокий
3	По встроенным (легальным) операциям с записями баз персональных данных	Средний
4	По разграничению доступа к персональным данным	Высокий
5	По наличию соединений с другими базами ПДн иных ИСПДн	Высокий
6	По уровню (обезличивания) ПДн	Средний
7	По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки	Средний

ИСПДн имеет ***средний*** уровень исходной защищенности, так как менее 70% характеристик ИСПДн соответствуют уровню не ниже «средний».

Показатель исходной защищенности $Y_1 = 5$.

Вероятность реализации УБПДн

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

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

маловероятно - отсутствуют объективные предпосылки для осуществления угрозы ($Y_2 = 0$);

низкая вероятность - объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию ($Y_2 = 2$);

средняя вероятность - объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны ($Y_2 = 5$);

высокая вероятность - объективные предпосылки для реализации угрозы существуют, меры по обеспечению безопасности ПДн не приняты ($Y_2 = 10$).

При обработке персональных данных в ИСПДн можно выделить следующие угрозы:

1.1.5 Угрозы утечки информации по техническим каналам

1.1.5.1 Угрозы утечки акустической (речевой) информации

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

В ИСПДн АО «ГМСК «Заполярье» функции голосового ввода ПДн или функции воспроизведения ПДн акустическими средствами отсутствуют.

Вероятность реализации угрозы – **маловероятная**.

1.1.5.2 Угрозы утечки видовой информации

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

В АО «ГМСК «Заполярье» введен контроль доступа в контролируемую зону, АРМ пользователей расположены так, что практически исключен визуальный доступ к мониторам, а на окнах установлены жалюзи.

Вероятность реализации угрозы – **маловероятная**.

1.1.5.3 Угрозы утечки информации по каналам ПЭМИН

Угрозы утечки информации по каналу ПЭМИН, возможны из-за наличия паразитных электромагнитных излучений у элементов ИСПДн.

Угрозы данного класса **маловероятны**, т.к. размер контролируемой зоны большой, и элементы ИСПДн, находятся в здании и экранируются несущими стенами, и паразитный сигнал маскируется со множеством других паразитных сигналов элементов, не входящих в ИСПДн.

Вероятность реализации угрозы – **маловероятная**.

1.1.6 Угрозы несанкционированного доступа к информации

Реализация угроз НСД к информации может приводить к следующим видам нарушения ее безопасности:

нарушению конфиденциальности (копирование, неправомерное распространение);

нарушению целостности (уничтожение, изменение);

нарушению доступности (блокирование).

В АО «ГМСК «Заполярье» введен контроль доступа в контролируемую зону, установлена охранная сигнализация, ведется видео наблюдение, двери закрываются на замок.

Вероятность реализации угрозы – **маловероятная.**

1.1.6.1 Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн

Кража ПЭВМ.

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где расположены элементы ИСПДн.

В АО «ГМСК «Заполярье» введен контроль доступа в контролируемую зону, установлена охранная сигнализация, ведется видео наблюдение, двери закрываются на замок.

Вероятность реализации угрозы – **маловероятная**.

Кража носителей информации

Угроза осуществляется путем НСД внешними и внутренними нарушителями к носителям информации.

В АО «ГМСК «Заполярье» введен контроль доступа в контролируемую зону, установлена охранная сигнализация, ведется видео наблюдение, двери закрываются на замок.

Вероятность реализации угрозы – **маловероятная.**

Кража ключей и атрибутов доступа

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где происходит работа пользователей.

В АО «ГМСК «Заполярье» установлена охранная сигнализация, ведется видео наблюдение, двери закрываются на замок.

Вероятность реализации угрозы – **маловероятная.**

Кражи, модификации, уничтожения информации

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где расположены элементы ИСПДн и средства защиты, а также происходит работа пользователей.

В АО «ГМСК «Заполярье» установлена охранная сигнализация, ведется видео наблюдение, двери закрываются на замок.

Вероятность реализации угрозы – **маловероятная.**

Вывод из строя узлов ПЭВМ, каналов связи

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где расположены элементы ИСПДн и проходят каналы связи.

В АО «ГМСК «Заполярье» ведется видео наблюдение, установлена охранная сигнализация.

Вероятность реализации угрозы – **низкая.**

Несанкционированное отключение средств защиты

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где расположены средства защиты ИСПДн.

В АО «ГМСК «Заполярье» установлена охранная сигнализация, пользователи ИСПДн проинструктированы о работе с ПДн.

Вероятность реализации угрозы – **маловероятная.**

1.1.6.2 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).

Действия вредоносных программ (вирусов).

Программно-математическое воздействие - это воздействие с помощью вредоносных программ. Программой с потенциально опасными последствиями или вредоносной программой (вирусом) называют некоторую самостоятельную программу (набор инструкций), которая способна выполнять любое непустое подмножество следующих функций:

– скрывать признаки своего присутствия в программной среде компьютера;

– обладать способностью к самодублированию, ассоциированию себя с другими программами и (или) переносу своих фрагментов в иные области оперативной или внешней памяти;

– разрушать (искажать произвольным образом) код программ в оперативной памяти;

– выполнять без инициирования со стороны пользователя (пользовательской программы в штатном режиме ее выполнения) деструктивные функции (копирования, уничтожения, блокирования и т.п.);

– сохранять фрагменты информации из оперативной памяти в некоторых областях внешней памяти прямого доступа (локальных или удаленных);

– искажать произвольным образом, блокировать и (или) подменять выводимый во внешнюю память или в канал связи массив информации, образовавшийся в результате работы прикладных программ, или уже находящиеся во внешней памяти массивы данных.

В АО «ГМСК «Заполярье» на всех элементах ИСПДн установлена антивирусная защита, пользователи проинструктированы о мерах предотвращения вирусного заражения, установлен межсетевой экран Ideco ICS.

Вероятность реализации угрозы – **низкая**.

Недекларированные возможности системного ПО и ПО для обработки персональных данных.

Недекларированные возможности – функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

В АО «ГМСК «Заполярье» есть программное обеспечения разрабатываемого сторонними специалистами.

Вероятность реализации угрозы – **низкая**.

Установка ПО, не связанного с исполнением служебных обязанностей

Угроза осуществляется путем несанкционированной установки ПО внутренним нарушителям, что может привести к нарушению конфиденциальности, целостности и доступности всей ИСПДн или ее элементов.

В АО «ГМСК «Заполярье» введено разграничение правами пользователей на установку ПО и осуществляется контроль, пользователи проинструктированы о политике установки ПО.

Вероятность реализации угрозы – **низкая**.

1.1.6.3 Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз не антропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера.

Утрата ключей и атрибутов доступа

Угроза осуществляется за счет действия человеческого фактора пользователей ИСПДн, которые нарушают положения парольной политике в части их создания (создают легкие или пустые пароли, не меняют пароли по истечении срока их жизни или компрометации и т.п.) и хранения (записывают пароли на бумажные носители, передают ключи доступа третьим лицам и т.п.) или не осведомлены о них.

В АО «ГМСК «Заполярье» введена парольная политика, предусматривающая требуемую сложность пароля и периодическую его смену, введена политика «чистого стола», осуществляется контроль за их выполнением, пользователи проинструктированы о парольной политике и о действиях в случаях утраты или компрометации паролей.

Вероятность реализации угрозы – **маловероятная**.

Непреднамеренная модификация (уничтожение) информации сотрудниками

Угроза осуществляется за счет действия человеческого фактора пользователей ИСПДн, которые нарушают положения принятых правил работы с ИСПДн или не осведомлены о них.

В АО «ГМСК «Заполярье» осуществляется резервное копирование обрабатываемых ПДн, пользователи проинструктированы о работе с ИСПДн.

Вероятность реализации угрозы – **низкая.**

Непреднамеренное отключение средств защиты

Угроза осуществляется за счет действия человеческого фактора пользователей ИСПДн, которые нарушают положения принятых правил работы с ИСПДн и средствами защиты или не осведомлены о них.

В АО «ГМСК «Заполярье» двери закрываются на замок, осуществляется разграничение доступа к настройкам режимов средств защиты, пользователи проинструктированы о работе с ИСПДн.

Вероятность реализации угрозы – **маловероятная.**

Выход из строя аппаратно-программных средств

Угроза осуществляется вследствие несовершенства аппаратно-программных средств, из-за которых может происходить нарушение целостности и доступности защищаемой информации.

В АО «ГМСК «Заполярье» осуществляет резервирование ключевых элементов ИСПДн.

Вероятность реализации угрозы – **низкая.**

Сбой системы электроснабжения

Угроза осуществляется вследствие несовершенства системы электроснабжения, из-за чего может происходить нарушение целостности и доступности защищаемой информации.

В АО «ГМСК «Заполярье» ко всем ключевым элементам ИСПДн подключены источники бесперебойного питания.

Вероятность реализации угрозы – **низкая.**

Стихийное бедствие

Угроза осуществляется вследствие несоблюдения мер пожарной безопасности.

В АО «ГМСК «Заполярье» установлена пожарная сигнализация, пользователи проинструктированы о действиях в случае возникновения внештатных ситуаций.

Вероятность реализации угрозы – **маловероятная.**

1.1.6.4 Угрозы преднамеренных действий внутренних нарушителей

Доступ к информации, модификация, уничтожение лиц, не допущенных к ее обработке

Угроза осуществляется путем НСД внешних нарушителей в помещения, где расположены элементы ИСПДн и средства защиты, а также происходит работа пользователей.

В АО «ГМСК «Заполярье» установлена охранная сигнализация, ведется видео наблюдение, двери закрываются на замок.

Вероятность реализации угрозы – **маловероятная.**

Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке

Угроза осуществляется за счет действия человеческого фактора пользователей ИСПДн, которые нарушают положения о неразглашении обрабатываемой информации или не осведомлены о них.

В АО «ГМСК «Заполярье» пользователи осведомлены о порядке работы с персональными данными, а также подписали Соглашение о неразглашении.

Вероятность реализации угрозы – **маловероятная.**

1.1.6.5 Угрозы несанкционированного доступа по каналам связи

В соответствии с «Типовой моделью угроз безопасности персональных данных, обрабатываемых в распределенных ИСПДн, имеющих подключение к сетям общего пользования и (или) международного информационного обмена» (п. 6.6. Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной заместителем директора ФСТЭК России 21 февраля 2008 г.), для ИСПДн можно рассматривать следующие угрозы, реализуемые с использованием протоколов межсетевого взаимодействия:

– угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации;

– 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.;

– угрозы выявления паролей по сети;

– угрозы навязывание ложного маршрута сети;

– угрозы подмены доверенного объекта в сети;

– угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях;

– угрозы типа «Отказ в обслуживании»;

– угрозы удаленного запуска приложений;

– угрозы внедрения по сети вредоносных программ.

Угроза «Анализ сетевого трафика»

Эта угроза реализуется с помощью специальной программы-анализатора пакетов (sniffer), перехватывающей все пакеты, передаваемые по сегменту сети, и

выделяющей среди них те, в которых передаются идентификатор пользователя и его пароль. В ходе реализации угрозы нарушитель:

– изучает логику работы ИСПДн - то есть стремится получить однозначное соответствие событий, происходящих в системе, и команд, пересылаемых при этом хостами, в момент появления данных событий. В дальнейшем это позволяет злоумышленнику на основе задания соответствующих команд получить, например, привилегированные права на действия в системе или расширить свои полномочия в ней;

– перехватывает поток передаваемых данных, которыми обмениваются компоненты сетевой операционной системы, для извлечения конфиденциальной или идентификационной информации (например, статических паролей пользователей для доступа к удаленным хостам по протоколам FTP и TELNET, не предусматривающих шифрование), ее подмены, модификации и т.п.

На всех компьютерах локальной сети установлены сертифицированные антивирусные средства со средствами обнаружения вторжений, установлен межсетевой экран Ideco ICS.

Вероятность реализации угрозы – **низкая.**

Перехват за переделами с контролируемой зоны.

Вероятность реализации угрозы – **маловероятна**.

Перехват в пределах контролируемой зоны внешними нарушителями

В АО «ГМСК Заполярье» установлена охранная сигнализация, ведется видео наблюдение, двери закрываются на замок.

Вероятность реализации угрозы – **маловероятна**.

Перехват в пределах контролируемой зоны внутренними нарушителями.

В АО «ГМСК Заполярье установлена охранная сигнализация, ведется видео наблюдение, двери закрываются на замок.

Вероятность реализации угрозы – **маловероятна**.

Угроза «сканирование сети»

Сущность процесса реализации угрозы заключается в передаче запросов сетевым службам хостов ИСПДн и анализе ответов от них. Цель - выявление используемых протоколов, доступных портов сетевых служб, законов формирования идентификаторов соединений, определение активных сетевых сервисов, подбор идентификаторов и паролей пользователей.

На всех компьютерах локальной сети установлены сертифицированные антивирусные средства со средствами обнаружения вторжений, установлен межсетевой экран Ideco ICS.

Вероятность реализации угрозы – **низкая.**

Угроза выявления паролей

Цель реализации угрозы состоит в получении НСД путем преодоления парольной защиты. Злоумышленник может реализовывать угрозу с помощью целого ряда методов, таких как простой перебор, перебор с использованием специальных словарей, установка вредоносной программы для перехвата пароля, подмена доверенного объекта сети (IP-spoofing) и перехват пакетов (sniffing). В основном для реализации угрозы используются специальные программы, которые пытаются получить доступ хосту путем последовательного подбора паролей. В случае успеха, злоумышленник может создать для себя «проход» для будущего доступа, который будет действовать, даже если на хосте изменить пароль доступа.

На всех компьютерах локальной сети установлены антивирусные средства со средствами обнаружения вторжений, установлен межсетевой экран Ideco ICS.

Вероятность реализации угрозы – **маловероятна**.

Угрозы навязывание ложного маршрута сети

Данная угроза реализуется одним из двух способов: путем внутрисегментного или межсегментного навязывания. Возможность навязывания ложного маршрута обусловлена недостатками, присущими алгоритмам маршрутизации (в частности из-за проблемы идентификации сетевых управляющих устройств), в результате чего можно попасть, например, на хост или в сеть злоумышленника, где можно войти в операционную среду технического средства в составе ИСПДн. Реализации угрозы основывается на несанкционированном использовании протоколов маршрутизации (RIP, OSPF, LSP) и управления сетью (ICMP, SNMP) для внесения изменений в маршрутно-адресные таблицы. При этом нарушителю необходимо послать от имени сетевого управляющего устройства (например, маршрутизатора) управляющее сообщение.

На всех компьютерах локальной сети установлены антивирусные средства со средствами обнаружения вторжений, установлен межсетевой экран Ideco ICS.

Вероятность реализации угрозы – **маловероятная**.

Угрозы подмены доверенного объекта

Такая угроза эффективно реализуется в системах, в которых применяются нестойкие алгоритмы идентификации и аутентификации хостов, пользователей и

т.д. Под доверенным объектом понимается объект сети (компьютер, межсетевой экран, маршрутизатор и т.п.), легально подключенный к серверу.

Могут быть выделены две разновидности процесса реализации указанной угрозы: с установлением и без установления виртуального соединения.

Процесс реализации с установлением виртуального соединения состоит в присвоении прав доверенного субъекта взаимодействия, что позволяет нарушителю вести сеанс работы с объектом сети от имени доверенного субъекта. Реализация угрозы данного типа требует преодоления системы идентификации и аутентификации сообщений (например, атака rsh-службы UNIX-хоста).

Процесс реализации угрозы без установления виртуального соединения может иметь место в сетях, осуществляющих идентификацию передаваемых сообщений только по сетевому адресу отправителя. Сущность заключается в передаче служебных сообщений от имени сетевых управляющих устройств (например, от имени маршрутизаторов) об изменении маршрутно-адресных данных.

В результате реализации угрозы нарушитель получает права доступа к техническому средству ИСПДн - цели угроз.

На всех компьютерах локальной сети установлены антивирусные средства со средствами обнаружения вторжений, установлен межсетевой экран Ideco ICS.

Вероятность реализации угрозы – **маловероятная.**

Внедрение ложного объекта сети

Эта угроза основана на использовании недостатков алгоритмов удаленного поиска. В случае если объекты сети изначально не имеют адресной информации друг о друге, используются различные протоколы удаленного поиска (например, SAP в сетях Novell NetWare; ARP, DNS, WINS в сетях со стеком протоколов TCP/IP), заключающиеся в передаче по сети специальных запросов и получении на них ответов с искомой информацией. При этом существует возможность перехвата нарушителем поискового запроса и выдачи на него ложного ответа, использование которого приведет к требуемому изменению маршрутно-адресных данных. В дальнейшем весь поток информации, ассоциированный с объектом-жертвой, будет проходить через ложный объект сети.

На всех компьютерах локальной сети установлены антивирусные средства со средствами обнаружения вторжений, установлен межсетевой экран Ideco ICS.

Вероятность реализации угрозы – **маловероятна**.

Угрозы типа «Отказ в обслуживании»

Эти угрозы основаны на недостатках сетевого программного обеспечения, его уязвимостях, позволяющих нарушителю создавать условия, когда операционная система оказывается не в состоянии обрабатывать поступающие пакеты.

Могут быть выделены несколько разновидностей таких угроз:
скрытый отказ в обслуживании, вызванный привлечением части ресурсов ИСПДн на обработку пакетов, передаваемых злоумышленником со снижением пропускной способности каналов связи, производительности сетевых устройств, нарушением требований к времени обработки запросов. Примерами реализации угроз подобного рода могут служить: направленный шторм эхо-запросов по протоколу ICMP (Ping flooding), шторм запросов на установление TCP-соединений (SYN-flooding), шторм запросов к FTP-серверу;

– явный отказ в обслуживании, вызванный исчерпанием ресурсов ИСПДн при обработке пакетов, передаваемых злоумышленником (занятие всей полосы пропускания каналов связи, переполнение очередей запросов на обслуживание), при котором легальные запросы не могут быть переданы через сеть из-за недоступности среды передачи, либо получают отказ в обслуживании ввиду переполнения очередей запросов, дискового пространства памяти и т.д. Примерами угроз данного типа могут служить шторм широковещательных ICMP-эхо-запросов (Smurf), направленный шторм (SYN-flooding), шторм сообщений почтовому серверу (Spam);

– явный отказ в обслуживании, вызванный нарушением логической связности между техническим средствами ИСПДн при передаче нарушителем управляющих сообщений от имени сетевых устройств, приводящих к изменению маршрутно-адресных данных (например, ICMP Redirect Host, DNS-flooding) или идентификационной и аутентификационной информации;

– явный отказ в обслуживании, вызванный передачей злоумышленником пакетов с нестандартными атрибутами (угрозы типа «Land», «TearDrop», «Bonk», «Nuke», «UDP-bomb») или имеющих длину, превышающую максимально допустимый размер (угроза типа «Ping Death»), что может привести к сбою сетевых устройств, участвующих в обработке запросов, при условии наличия ошибок в программах, реализующих протоколы сетевого обмена.

Результатом реализации данной угрозы может стать нарушение работоспособности соответствующей службы предоставления удаленного доступа к ПДн в ИСПДн, передача с одного адреса такого количества запросов на подключение к техническому средству в составе ИСПДн, которое максимально может «вместить» трафик (направленный «шторм запросов»), что влечет за собой переполнение очереди запросов и отказ одной из сетевых служб или полная остановка ИСПДн из-за невозможности системы заниматься ничем другим, кроме обработки запросов.

На всех компьютерах локальной сети установлены антивирусные средства со средствами обнаружения вторжений, установлен межсетевой экран Ideco ICS.

Вероятность реализации угрозы – **маловероятная.**

Угрозы удаленного запуска приложений

Угроза заключается в стремлении запустить на хосте ИСПДн различные предварительно внедренные вредоносные программы: программы-закладки, вирусы, «сетевые шпионы», основная цель которых - нарушение конфиденциальности, целостности, доступности информации и полный контроль за работой хоста. Кроме того, возможен несанкционированный запуск прикладных программ пользователей для несанкционированного получения необходимых нарушителю данных, для запуска управляемых прикладной программой процессов и др.

Выделяют три подкласса данных угроз:

– распространение файлов, содержащих несанкционированный исполняемый код;

– удаленный запуск приложения путем переполнения буфера приложений-серверов;

– удаленный запуск приложения путем использования возможностей удаленного управления системой, предоставляемых скрытыми программными и аппаратными закладками, либо используемыми штатными средствами.

Типовые угрозы первого из указанных подклассов основываются на активизации распространяемых файлов при случайном обращении к ним. Примерами таких файлов могут служить: файлы, содержащие исполняемый код в вид документы, содержащие исполняемый код в виде элементов ActiveX, Java-апплетов, интерпретируемых скриптов (например, тексты на JavaScript); файлы, содержащие исполняемые коды программ. Для распространения файлов могут использоваться службы электронной почты, передачи файлов, сетевой файловой системы.

При угрозах второго подкласса используются недостатки программ, реализующих сетевые сервисы (в частности, отсутствие контроля за переполнением буфера). Настройкой системных регистров иногда удается переключить процессор после прерывания, вызванного переполнением буфера, на исполнение кода, содержащегося за границей буфера. Примером реализации такой угрозы может служить внедрение широко известного «вируса Морриса».

При угрозах третьего подкласса нарушитель использует возможности удаленного управления системой, предоставляемые скрытыми компонентами (например, «троянскими» программами типа Back. Orifice, Net Bus), либо штатными средствами управления и администрирования компьютерных сетей (Landesk Management Suite, Managewise, Back Orifice и т. п.). В результате их использования удается добиться удаленного контроля над станцией в сети.

На всех компьютерах локальной сети установлены антивирусные средства со средствами обнаружения вторжений, межсетевой экран Ideco ICS.

Вероятность реализации угрозы – **маловероятная.**

Угрозы внедрения по сети вредоносных программ

К вредоносным программам, внедряемым по сети, относятся вирусы, которые для своего распространения активно используют протоколы и возможности локальных и глобальных сетей. Основным принципом работы сетевого вируса является возможность самостоятельно передать свой код на удаленный сервер или рабочую станцию. «Полноценные» сетевые вирусы при этом обладают еще и возможностью запустить на выполнение свой код на удаленном компьютере или, по крайней мере, «подтолкнуть» пользователя к запуску зараженного файла.

Вредоносными программами, обеспечивающими осуществление НСД, могут быть:

– программы подбора и вскрытия паролей;

– программы, реализующие угрозы;

– программы, демонстрирующие использование недекларированных возможностей программного и программно-аппаратного обеспечения ИСПДн;

– программы-генераторы компьютерных вирусов;

– программы, демонстрирующие уязвимости средств защиты информации и др.

На всех компьютерах локальной сети установлены антивирусные средства со средствами обнаружения вторжений, установлен межсетевой экран Ideco ICS 2.4.5.

Вероятность реализации угрозы – **низкая.**

Реализуемость угроз

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

Оценка реализуемости УБПДн представлена в таблице.

Таблица 4 – Реализуемость УБПДн.

Тип угроз безопасности ПДн	Коэффициент реализуемости угрозы (Y)	Возможность реализации
1. Угрозы от утечки по техническим каналам.		
1.1. Угрозы утечки акустической информации	0.25	Низкая

1.2. Угрозы утечки видовой информации	0.25	Низкая
1.3. Угрозы утечки информации по каналам ПЭМИН	0.25	Низкая
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	0.25	Низкая
2.1.2. Кража носителей информации	0.25	Низкая
2.1.3. Кража ключей и атрибутов доступа	0.25	Низкая
2.1.4. Кражи, модификации, уничтожения информации	0.25	Низкая
2.1.5. Вывод из строя узлов ПЭВМ, каналов связи	0.35	Средняя
2.1.6. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	0.25	Низкая
2.1.7. Несанкционированное отключение средств защиты	0.25	Низкая
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)	0.35	Средняя
2.2.2. Не декларированные возможности системного ПО и ПО для обработки персональных данных	0.35	Средняя
2.2.3. Установка ПО, не связанного с исполнением служебных обязанностей	0.35	Средняя
2.3. Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз не антропогенного (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	0.25	Низкая
2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками	0.35	Средняя
2.3.3. Непреднамеренное отключение средств защиты	0.25	Низкая
2.3.4. Выход из строя аппаратно-программных средств	0.35	Средняя
2.3.5. Сбой системы электроснабжения	0.35	Средняя
2.3.6. Стихийное бедствие	0.25	Низкая
2.4. Угрозы преднамеренных действий внутренних нарушителей		
2.4.1. Доступ к информации, модификация, уничтожение лиц, не допущенных к ее обработке	0.35	Средняя
2.4.2. Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке	0.25	Низкая
2.5.Угрозы несанкционированного доступа по каналам связи.		
2.5.1.Угроза «Анализ сетевого трафика» с	0.35	Средняя

перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации:		
2.5.1.1. Перехват за переделами с контролируемой зоны	0.25	Низкая
2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями	0.25	Низкая
2.5.1.3.Перехват в пределах контролируемой зоны внутренними нарушителями.	0.25	Низкая
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.	0.35	Средняя
2.5.3.Угрозы выявления паролей по сети	0,25	Низкая
2.5.4.Угрозы навязывание ложного маршрута сети	0.25	Низкая
2.5.5.Угрозы подмены доверенного объекта в сети	0.25	Низкая
2.5.6.Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях	0.25	Низкая
2.5.7.Угрозы типа «Отказ в обслуживании»	0.25	Низкая
2.5.8.Угрозы удаленного запуска приложений	0.25	Низкая
2.5.9.Угрозы внедрения по сети вредоносных программ	0.35	Средняя

Оценка опасности угроз

Оценка опасности УБПДн производится на основе опроса специалистов по защите информации и определяется вербальным показателем опасности, который имеет три значения:

низкая опасность - если реализация угрозы может привести к незначительным негативным последствиям для субъектов персональных данных;

средняя опасность - если реализация угрозы может привести к негативным последствиям для субъектов персональных данных;

высокая опасность - если реализация угрозы может привести к значительным негативным последствиям для субъектов персональных данных.

Оценка опасности УБПДн представлена таблице.

Таблица 5 – Опасность УБПДн

Тип угроз безопасности ПДн	Опасность угрозы
1. Угрозы от утечки по техническим каналам.	
1.1. Угрозы утечки акустической информации	Низкая
1.2. Угрозы утечки видовой информации	Низкая
1.3. Угрозы утечки информации по каналам ПЭМИН	Низкая
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
2.1.2. Кража носителей информации	Низкая
2.1.3. Кража ключей и атрибутов доступа	Низкая
2.1.4. Кражи, модификации, уничтожения информации	Низкая
2.1.5. Вывод из строя узлов ПЭВМ, каналов связи	Низкая
2.1.6. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	Низкая
2.1.7. Несанкционированное отключение средств защиты	Низкая
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)	Низкая
2.2.2. Не декларированные возможности системного ПО и ПО для обработки персональных данных	Низкая
2.2.3. Установка ПО, не связанного с исполнением служебных обязанностей	Низкая
2.3. Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз не антропогенного (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	Низкая
2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками	Низкая
2.3.3. Непреднамеренное отключение средств защиты	Низкая
2.3.4. Выход из строя аппаратно-программных средств	Низкая
2.3.5. Сбой системы электроснабжения	Низкая
2.3.6. Стихийное бедствие	Низкая
2.4. Угрозы преднамеренных действий внутренних нарушителей	
2.4.1. Доступ к информации, модификация, уничтожение лиц, не допущенных к ее обработке	Низкая
2.4.2. Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке	Низкая
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:	Низкая
2.5.1.1. Перехват за переделами с контролируемой зоны	Низкая
2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями	Низкая
2.5.1.3.Перехват в пределах контролируемой зоны внутренними нарушителями.	Низкая
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.	Низкая
2.5.3.Угрозы выявления паролей по сети	Низкая
2.5.4.Угрозы навязывание ложного маршрута сети	Низкая
2.5.5.Угрозы подмены доверенного объекта в сети	Низкая

2.5.6.Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях	Низкая
2.5.7.Угрозы типа «Отказ в обслуживании»	Низкая
2.5.8.Угрозы удаленного запуска приложений	Низкая
2.5.9.Угрозы внедрения по сети вредоносных программ	Низкая

Определение актуальности угроз в ИСПДн

В соответствии с правилами отнесения угрозы безопасности к актуальной, для ИСПДн определяются актуальные и неактуальные угрозы.

Таблица 6 – Правила определения актуальности УБПДн

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

Оценка актуальности угроз безопасности представлена в таблице.

Таблица 7 – Актуальность УБПДн

Тип угроз безопасности ПДн	Опасность угрозы
1. Угрозы от утечки по техническим каналам	
1.1. Угрозы утечки акустической информации	Неактуальная
1.2. Угрозы утечки видовой информации	Неактуальная
1.3. Угрозы утечки информации по каналам ПЭМИН	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	Неактуальная
2.1.2. Кража носителей информации	Неактуальная
2.1.3. Кража ключей и атрибутов доступа	Неактуальная
2.1.4. Кражи, модификации, уничтожения информации	Неактуальная
2.1.5. Вывод из строя узлов ПЭВМ, каналов связи	Неактуальная
2.1.6. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	Неактуальная

2.1.7. Несанкционированное отключение средств защиты	Неактуальная
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)	Неактуальная
2.2.2. Недекларированные возможности системного ПО и ПО для обработки персональных данных	Неактуальная
2.2.3. Установка ПО, не связанного с исполнением служебных обязанностей	Неактуальная
2.3. Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера.	
2.3.1. Утрата ключей и атрибутов доступа	Неактуальная
2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками	Неактуальная
2.3.3. Непреднамеренное отключение средств защиты	Неактуальная
2.3.4. Выход из строя аппаратно-программных средств	Неактуальная
2.3.5. Сбой системы электроснабжения	Неактуальная
2.3.6. Стихийное бедствие	Неактуальная
2.4. Угрозы преднамеренных действий внутренних нарушителей.	
2.4.1. Доступ к информации, модификация, уничтожение лиц, не допущенных к ее обработке	Неактуальная
2.4.2. Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке	Неактуальная
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:	Неактуальная
2.5.1.1. Перехват за переделами с контролируемой зоны	Неактуальная
2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями	Неактуальная
2.5.1.3.Перехват в пределах контролируемой зоны внутренними нарушителями.	Неактуальная
2.5.2.Угрозы сканирования, направленные на выявление	Неактуальная

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	Неактуальная
2.5.4.Угрозы навязывание ложного маршрута сети	Неактуальная
2.5.5.Угрозы подмены доверенного объекта в сети	Неактуальная
2.5.6.Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях	Неактуальная
2.5.7.Угрозы типа «Отказ в обслуживании»	Неактуальная
2.5.8.Угрозы удаленного запуска приложений	Неактуальная
2.5.9.Угрозы внедрения по сети вредоносных программ	Неактуальная

На основании проведенного анализа можно сделать вывод, что актуальных угроз в информационной системе персональных данных не выявлено.

Модель угроз безопасности

Исходный класс защищенности – средний (Y1=5).

Таблица 8 – Угрозы безопасности

Наименование угрозы	Вероятность реализации угрозы (Y2)	Возможность реализации угрозы (Y)	Опасность угрозы	Актуальность угрозы	Меры по противодействию угрозе	
					Технические	Организационные
1. Угрозы от утечки по техническим каналам						
1.1. Угрозы утечки акустической информации	Маловероятна	Низкая	Низкая	Неактуальная		Инструкция пользователя Технологический процесс
1.2. Угрозы утечки видовой информации	Маловероятна	Низкая	Низкая	Неактуальная	Жалюзи на окна Расположение монитора	Инструкция пользователя Технологический процесс
1.3. Угрозы утечки информации по каналам ПЭМИН	Маловероятна	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	Маловероятна	Низкая	Низкая	Неактуальная		Охрана
2.1.2. Кража носителей информации	Маловероятна	Низкая	Низкая	Неактуальная	Хранение в сейфе Шифрование данных при помощи ViPNet	Учет носителей информации Инструкция пользователя
2.1.3. Кража ключей доступа	Маловероятна	Низкая	Низкая	Неактуальная	Хранение в сейфе	Инструкция пользователя
2.1.4. Кражи, модификации, уничтожения информации.	Маловероятна	Низкая	Низкая	Неактуальная	Шифрование данных при помощи ViPNet Система защиты от НСД ViPNet (клиент)	Охрана
2.1.5. Вывод из строя узлов ПЭВМ, каналов связи	Низкая вероятность	Средняя	Низкая	Неактуальная		Охрана
2.1.6. **Несанкционированный доступ к информации при техническом обслужи-**	Маловероятна	Низкая	Низкая	Неактуальная	Шифрование данных при помощи ViPNet	Ремонт допущенными сотрудниками учреждения

вании (ремонте, уничтожении) узлов ПЭВМ						
2.1.7. Несанкционированное отключение средств защиты	Низкая вероятность	Средняя	Низкая	Неактуальная	Настройка средств защиты	Инструкция администратора безопасности Технологический процесс обработки
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)	Низкая вероятность	Средняя	Низкая	Неактуальная	Антивирусное ПО Антивирус NOD 32 ESET Autivirus	Инструкция пользователя Технологический процесс обработки Инструкция по антивирусной защите
2.2.2. Недекларированные возможности системного ПО и ПО для обработки персональных данных	Маловероятна	Низкая	Низкая	Неактуальная	Настройка средств защиты	Приобретение ПО у доверенной организации
2.2.3. Установка ПО не связанного с исполнением служебных обязанностей	Низкая вероятность	Средняя	Низкая	Неактуальная	Настройка средств защиты	Инструкция пользователя Технологический процесс обработки

2.3. Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера.						
2.3.1. Утрата ключей и атрибутов доступа	Маловероятна	Низкая	Низкая	Неактуальная	Хранение в сейфе	Инструкция пользователя Журнал учета паролей
2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками	Низкая вероятность	Средняя	Низкая	Актуальная	Настройка средств защиты	Инструкция пользователя
2.3.3. Непреднамеренное отключение средств защиты	Маловероятна	Низкая	Низкая	Неактуальная	Доступ к установлению режимов работы средств защиты предоставляется только администратору безопасности Настройка средств защиты	Инструкция пользователя Инструкция по антивирусной защите
2.3.4. Выход из строя аппаратно-программных средств	Низкая вероятность	Средняя	Низкая	Неактуальная		
2.3.5. Сбой системы электроснабжения	Маловероятна	Низкая	Низкая	Неактуальная	Использование источника бесперебойного электропитания	

2.3.6. Стихийное бедствие	Маловероятна	Низкая	Низкая	Неактуальная	Пожарная сигнализация	Инструкция по действиям в случае возникновения нештатной ситуации
2.4. Угрозы преднамеренных действий внутренних нарушителей						
2.4.1. Доступ к информации, модификация, уничтожение лицами не допущенных к ее обработке	Маловероятна	Низкая	Низкая	Неактуальная	Система защиты от НСД ViPNet (клиент)	Технологический процесс обработки
2.4.2. Разглашение информации, модификация, уничтожение сотрудниками допущенными к ее обработке	Маловероятна	Низкая	Низкая	Неактуальная		Обязательство о не разглашении Инструкция пользователя
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 пределами с контролируемой зоны;	Маловероятна	Низкая	Низкая	Неактуальная		

2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями;	Маловероятна	Низкая	Низкая	Неактуальная		
2.5.1.3. Перехват в пределах контролируемой зоны внутренними нарушителями.	Маловероятна	Низкая	Низкая	Неактуальная		
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.	Низкая вероятность	Средняя	Низкая	Неактуальная	ViPNet (клиент) Межсетевой экран Ideco	
2.5.3. Угрозы выявления паролей по сети.	Маловероятна	Низкая	Низкая	Неактуальная	ViPNet (клиент) Ideco	

2.5.4. Угрозы навязывание ложного маршрута сети.	Маловероятна	Низкая	Низкая	Неактуальная	ViPNet (клиент) Межсетевой экран Ideco	
2.5.5. Угрозы подмены доверенного объекта в сети.	Маловероятна	Низкая	Низкая	Неактуальная	ViPNet (клиент) Межсетевой экран Ideco	
2.5.6. Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях.	Маловероятно	Низкая	Низкая	Неактуальная	ViPNet (клиент) Межсетевой экран Ideco	
2.5.7. Угрозы типа «Отказ в обслуживании».	Маловероятно	Низкая	Низкая	Неактуальная	ViPNet (клиент) Межсетевой экран Ideco	

2.5.8. Угрозы удаленного запуска приложений.	Маловероятно	Низкая	Низкая	Неактуальная	ViPNet (клиент) Межсетевой экран Ideco	
2.5.9. Угрозы внедрения по сети вредоносных программ.	Низкая вероят-ность	Средняя	Низкая	Неактуальная	ViPNet (клиент) Антивирусное ПО Антивирус NOD 32 ESET Autivirus Межсетевой экран Ideco ICS	

10. ЗАКЛЮЧЕНИЕ

Ввиду исключительной роли в ИСПДн лиц категорий I и II в число этих лиц должны включаться только доверенные лица, к которым применен комплекс организационных мер по их подбору, принятию на работу, назначению на должность и контролю выполнения функциональных обязанностей.

Лица категорий III-VII относятся к вероятным нарушителям.

Среди лиц категорий III-VII наиболее опасными вероятными нарушителями являются лица категорий V-VI (уполномоченный персонал разработчиков ИСПДн, который на договорной основе имеет право на техническое обслуживание и модификацию компонентов ИСПДн, бывшие сотрудники).

Представленная модель угроз для ИСПДн должна использоваться при формировании обоснованных требований информационной безопасности и проектировании ИСПДн "Полис ОМС", "ОМС Эксперт-6", "1С предприятие", "1С зарплата, управление персоналом", "1С Бухгалтерия".

1. В соответствии с Требованиями к защите персональных данных при их обработке в информационных системах персональных данных утвержденных Постановлением Правительства РФ от 01.11.2012 г. № 1119, исходя из анализа угроз безопасности ПДн и на основании категории и объема обрабатываемых персональных данных – **ИСПДн** «1С Предприятие», «1С Зарплата и управление персоналом» относится к 3-му уровню защищенности.

2. В соответствии с Требованиями к защите персональных данных при их обработке в информационных системах персональных данных утвержденных Постановлением Правительства РФ от 01.11.2012 г. № 1119, исходя из анализа угроз безопасности ПДн, на основании категории и объема обрабатываемых персональных данных – **ИСПДн «**ОМС Эксперт-6" относится к 1-му уровню защищенности.

3. В соответствии с Требованиями к защите персональных данных при их обработке в информационных системах персональных данных утвержденных Постановлением Правительства РФ от 01.11.2012 г. № 1119, исходя из анализа угроз безопасности ПДн, на основании категории и объема обрабатываемых персональных данных – **ИСПДн «**Полис ОМС» относится к 3-му уровню защищенности.

АО «ГМСК «Заполярье»

Лист ознакомления с Моделью
угроз безопасности персональных данных при их обработке в информационной системе персональных данных Акционерного общества «Государственная медицинская страховая компания «Заполярье»

№ п/п	ФИО работника	Дата ознакомление	Подпись работника
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
10.			
11.			
12.			
13.			
14.			
15.			
16.			
17.			
18.			
19.			
20.			
21.			
22.			
23.			
24.			
25.			
26.			
27.			
28.			
29.			
30.			
31.			
32.			
33.			
34.			
35.			
36.			
37.			