ПРАКТИЧЕСКАЯ РАБОТА №8: ПОСТРОЕНИЕ ЧАСТНОЙ МОДЕЛИ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННОЙ СИСТЕМЕ.

Цель: ознакомиться с содержанием и структурой частной модели угроз безопасности в информационной системе персональных данных (ИСПДн), получить опыт создания частной модели угроз безопасности для учреждения, имеющего информационную систему обработки персональных данных.

Методы и приемы: изучение теоретических источников, анализ, работа по шаблону, проектный кейс-метод, частично-поисковая работа, самостоятельная работа.

Ключевые слова: частная модель угроз, персональные данные, информационная система, модель нарушителя, угрозы утечки информации, технические каналы утечки информации, защищенность информационной системы, вероятность реализации угроз, корпоративная сеть, несанкционированный доступ.

Порядок выполнения работы

1. Изучить исходные условия существующей ИСПДн
2. Копировать шаблон частной модели угроз
3. Заполнить шаблон частной модели угроз по исходным условиям информационной систем обработки персональным данным.
4. Защитить свой проект частной модели угроз ИСПДн.

Исходные условия ИСПДн «Кадры»

Организация: ЗАО «Солнышко».

Директор: Иванов Иван Иванович.

Заместитель директора: Петрова Тамара Васильевна.

Начальник отдела кадров: Южина Мария Ивановна.

Сотрудники отдела кадров: Сидорова Александра Павловна,

Копылова Юлия Фёдоровна.

Состав ИСПДн:

1. Персональные данные сотрудников организации:

- фамилия, имя, отчество
- дата и место рождения
- пол
- сведения об образовании
- сведения о предыдущем месте работы
- семейное положение
- адреса регистрации и фактического проживания
- номера контактных телефонов
- индивидуальный номер налогоплательщика
- номер страхового свидетельства пенсионного страхования
- номер полиса обязательного медицинского страхования
- данные водительского удостоверения

В информационной системе одновременно обрабатываются данные 777 субъектов персональных данных (сотрудников) в пределах Организации.

2. Три автоматизированных рабочих места (АРМ) пользователей, сетевой принтер, сервер, коммутационное оборудование.

Топология: АРМ и сервер составляют сегмент корпоративной вычислительной сети (см. схему – рис. 7).

Корпоративная сеть: Организации не имеет подключения к сетям связи общего пользования и сетям международного информационного обмена.

В состав каждого АРМ входят два жёстких диска, на первом установлена операционная система, прикладное программное обеспечение и общедоступная справочная информация, на втором - информация, составляющая персональные данные сотрудников Организации.

Комплект АРМ №1-3: Системный блок № XXXXXXX01-03, Монитор Samsung N710 – серийный номер YYYYYYY01-03, клавиатура Genius серийный номер ZZZZZZZZ01-03, графический манипулятор (мышь) Genius серийный номер WWWW01-03,

В состав сервера входят три жестких диска, на первом установлена операционная система, прикладное программное обеспечение, второй и третий объединены в RAID массив, в котором хранится информация, составляющая персональные данные сотрудников Организации.

Комплект сервера: Системный блок № XXXXXXX04, Монитор Samsung N710 – серийный номер YYYYYYY04, клавиатура Genius серийный номер ZZZZZZZZ04, графический манипулятор Genius серийный номер WWWW04.

Сервер и коммуникационное оборудование установлены в типовой стойке.

Сетевой принтер HP LaserJet P2015 серийный номер SSSSSSSSS.

3. Технология обработки персональных данных:

Обработка персональных данных сотрудников включает весь перечень действий.

К работе на АРМ допущены сотрудники отдела кадров и заместитель директора.

Полный доступ ко всей информации на АРМ и сервере имеют заместитель директора и начальник отдела кадров.

Сотрудники отдела кадров имеют полный доступ только к каталогу «Личные дела», размещённой на диске №2 своего АРМ, и только на чтение информации из каталога «Личные дела» на сервере.

Системный администратор сегмента сети не имеет доступа к информации, составляющей персональные данные. Имеет права на инсталляцию, настройку программного обеспечения, программных (программно-аппаратных) средств защиты сервера и АРМ № 1-3. Режим работы - одновременный.

Расположение: Отдельный кабинет по адресу: РФ, г. Отрадный, ул. Веселая,, дом 6, офис 25.

Помещение офиса оборудовано охранной сигнализацией и в нерабочее время сдается под охрану.

Доступ в помещение ограничен распорядительными актами Организации и автоматизированной системой контроля и управления доступа.

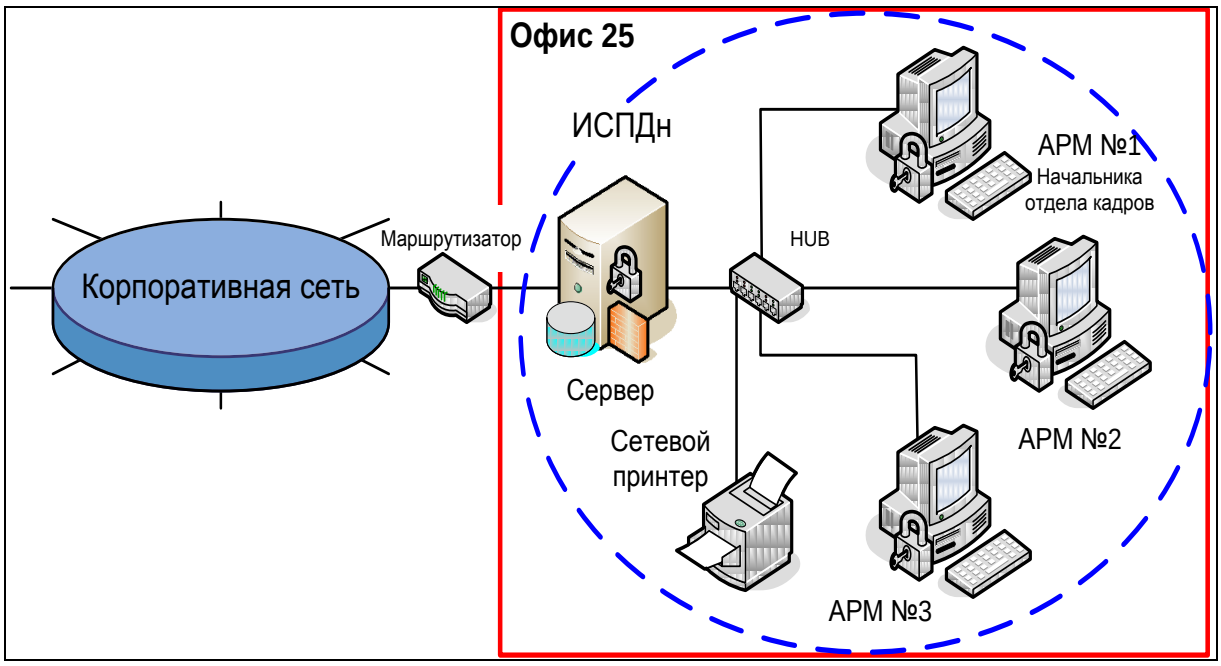

Рисунок 7. Схема корпоративной сети

УТВЕРЖДАЮ

_____

_____

(должность руководителя

организации)

_____

_____

(подпись)

«_____» _____ 201 ____г.

Частная модель угроз

безопасности персональных данных

при их обработке в ИСПДн

_____

(наименование ИСПДн)

СОГЛАСОВАНО

_____

___

«____» _____

201___ г

СОГЛАСОВАНО

_____

___

«____» _____

201___ г.

2017

Сокращения, условные обозначения

Термины и определения

Введение.

Современная система обеспечения информационной безопасности должна строиться на основе комплексирования разнообразных мер защиты и должна опираться на современные методы прогнозирования, анализа и моделирования возможных угроз безопасности информации и последствий их реализации.

Результаты моделирования предназначены для выбора адекватных оптимальных методов парирования угроз.

На стадии моделирования проведено изучение и анализ существующей обстановки и выявлены актуальные угрозы безопасности ПДн в составе ИСПДн

Модель угроз построена в соответствии с

1. Описание ИСПДн

1.1. Описание условий создания и использования ПДн

1.2. Описание форм представления ПДн

1.3. Описание структуры ИСПДн

1.4. Описание характеристик безопасности

2. Описание подхода к моделированию угроз безопасности ПДн.

Модель угроз безопасности ПДн в составе ИСПДн разработана на основе методических документов ФСТЭК:

На основе «Базовой модели угроз безопасности ПДн при их обработке в ИСПДн» проведена классификация угроз безопасности ПДн в составе ИСПДн и составлен перечень угроз безопасности ПДн в составе ИСПДн.

На основе составленного перечня угроз безопасности ПДн в составе ИСПДн с помощью «Методики определения актуальных угроз безопасности ПДн при их обработке в ИСПДн» построена модель угроз безопасности ПДн в составе ИСПДн и выявлены актуальные угрозы.

3. Классификация угроз безопасности персональных данных в ИСПДн

Состав и содержание УБПДн определяется совокупностью условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к ПДн.

Совокупность таких условий и факторов формируется с учетом характеристик ИСПДн, свойств среды (пути) распространения информативных сигналов, содержащих защищаемую информацию, и возможностей источников угроз.

К характеристикам ИСПДн, обуславливающим возникновение УБПДн, можно отнести:

_____

_____

_____

ИСПДн представляет собой совокупность информационных и программно-аппаратных элементов и их особенностей как объектов обеспечения безопасности.

Основными элементами ИСПДн являются:

Основными **элементами канала реализации** УБПДн являются:

Носители ПДн могут содержать информацию, представленную в следующих видах:

В целях формирования систематизированного перечня УБПДн при их обработке в ИСПДн угрозы классифицируются в соответствии со следующими признаками:

Реализация одной из УБПДн перечисленных классов или их совокупности может привести к следующим **типам последствий** для субъектов ПДн:

Угрозы утечки ПДн по техническим каналам однозначно описываются характеристиками источника информации, среды (пути) распространения и

приемника информативного сигнала, то есть определяются характеристиками технического канала утечки ПДн и описываются следующим образом:

Угрозы, связанные с НСД, представляются в виде совокупности обобщенных классов возможных источников угроз НСД, уязвимостей программного и аппаратного обеспечения ИСПДн, способов реализации угроз, объектов воздействия (носителей защищаемой информации) и возможных деструктивных действий. Такое представление описывается следующей формализованной записью:

3.1. Общее описание угроз безопасности ПДн, обрабатываемых в ИСПДн

При обработке ПДн в ИСПДн возможна реализация следующих видов УБПДн:

3.2. Угрозы утечки информации по техническим каналам.

Основными элементами угроз утечки информации по техническим каналам являются:

При обработке ПДн в ИСПДн возможно возникновение УБПДн за счет реализации следующих технических каналов утечки информации:

Возникновение угроз утечки акустической (речевой) информации, содержащаяся 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.

Реализация угрозы утечки видовой информации возможна за счет просмотра информации с помощью оптических (оптикоэлектронных) 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.

Угрозы утечки информации по каналу ПЭМИН, возможны из-за наличия электромагнитных излучений, в основном, монитора и системного блока компьютера. Основную опасность представляют угрозы утечки из-за наличия электромагнитных излучений монитора.

3.3. Угрозы несанкционированного доступа.

Угрозы НСД в ИСПДн с применением программных и программно-аппаратных средств реализуются при осуществлении несанкционированного, в

том числе случайного доступа, в результате которого осуществляется нарушение конфиденциальности (копирования, несанкционированного распространения), целостности (уничтожения, изменения) и доступности (блокирования) ПДн, и включают в себя:

4. Модель угроз безопасности ПДн, обрабатываемых в ИСПДн.

При обработке ПДн в ИСПДн, возможна реализация следующих видов УБПДн:

4.1. Угрозы утечки информации по техническим каналам.

При обработке ПДн в ИСПДн возможно возникновение УБПДн за счет реализации следующих технических каналов утечки информации:

4.1.1. Угрозы утечки акустической (речевой) информации.

Возникновение угроз утечки акустической (речевой) информации, содержащейся непосредственно в произносимой речи пользователя ИСПДн, при обработке ПДн в ИСПДн, обусловлено наличием функций голосового

ввода ПДн в ИСПДн или функций воспроизведения ПДн акустическими средствами ИСПДн.

Утечка акустической (речевой) информации может быть осуществлена:

_____

_____

_____

В ИСПДн не реализованы функции голосового ввода ПДн в ИСПДн. Акустические средства воспроизведения ПДн в ИСПДн не предусмотрены.

Рассмотрение угроз утечки акустической (речевой) информации не целесообразно в связи с отсутствием предпосылок возникновения угроз.

4.1.2. Угрозы утечки видовой информации.

Угрозы утечки видовой информации реализуются за счет просмотра ПДн с помощью оптических (оптикоэлектронных) 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.

Необходимым условием осуществления просмотра (регистрации) ПДн является наличие прямой видимости между средством наблюдения и носителем ПДн.

Утечка видовой информации может быть осуществлена:

_____

_____

_____

В ИСПДн отсутствует возможность неконтролируемого пребывания физических лиц в служебных помещениях или в непосредственной близости от

них, соответственно отсутствует возможность непосредственного наблюдения посторонними лицами ПДн.

Рассмотрение угроз утечки видовой информации не целесообразно в связи с отсутствием предпосылок возникновения угроз.

4.1.3. Угрозы утечки информации по каналам ПЭМИН.

Возникновение угрозы ПДн по каналам ПЭМИН возможно за счет перехвата техническими средствами побочных информативных электромагнитных полей и электрических сигналов, возникающих при обработке ПДн техническими средствами ИСПДн.

Рассмотрение угроз безопасности ПДн, связанных с перехватом ПЭМИН в ИСПДн, избыточно, так как носители ПДн (технические средства ИСПДн, создающие физические поля, в которых информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин) находятся в пределах контролируемой зоны. Утечка ПДн по каналам ПЭМИН – маловероятна из-за несоответствия стоимости средств съема информации и полученной в результате регистрации ПЭМИН информации, а защита ПДн от данного вида угроз – экономически нецелесообразна.

4.2. Угрозы НСД к ПДн, обрабатываемым в ИСПДн.

Угрозы НСД связаны с действиями нарушителей, имеющих доступ к ИСПДн, включая пользователей ИСПДн, реализующих угрозы

непосредственно в ИСПДн. Кроме этого, источниками угроз НСД к информации в ИСПДн могут быть аппаратные закладки и отчуждаемые носители вредоносных программ.

В ИСПДн возможны:

5. Общая характеристика источников угроз НСД.

Источниками угроз НСД в ИСПДн могут быть:

Нарушители:

Внутренние потенциальные нарушители подразделяются на **восемь категорий** в зависимости от способа доступа и полномочий доступа к ПДн (Таблица 4)

Таблица 4 Категории нарушителей

Категория нарушителя	**Способ доступа и полномочия**

Носитель вредоносной программы.

Носителем вредоносной программыможет быть аппаратный элемент компьютера или программный контейнер. Если вредоносная программа не ассоциируется с какой-либо прикладной программой, то в качестве ее носителя рассматриваются:

_____

_____

_____

_____

Если вредоносная программа ассоциируется с какой-либо прикладной программой, с файлами, имеющими определенные расширения или иные атрибуты, с сообщениями, передаваемыми по сети, то ее носителями являются:

1. пакеты передаваемых по компьютерной сети сообщений;
2. файлы (текстовые, графические, исполняемые и т.д.).

Аппаратная закладка.

В ИСПДн имеется опасность применения аппаратных средств, предназначенных для регистрации вводимой с клавиатуры информации, например:

_____

_____

_____

В ИСПДн отсутствует возможность неконтролируемого пребывания физических лиц в служебных помещениях или в непосредственной близости от них, соответственно отсутствует возможность установки аппаратных закладок посторонними лицами.

Существование данного источника угроз маловероятно также из-за несоответствия стоимости аппаратных закладок, сложности их скрытой установки и полученной в результате информации.

5.1. Общая характеристика уязвимостей ИСПДн.

Уязвимость ИСПДн – недостаток или слабое место в системном или прикладном программном (программно-аппаратном) обеспечении автоматизированной информационной системы, которое может быть использовано для реализации угрозы безопасности персональных данным.

Причины возникновения уязвимостей:

_____

_____

_____

К основным группам уязвимостей ИСПДн, относятся:

Характеристика уязвимостей системного ПО.

Уязвимости системного программного обеспечения необходимо рассматривать с привязкой к архитектуре построения вычислительных систем. При этом возможны уязвимости:

Уязвимости в микропрограммах и в средствах операционной системы, предназначенных для управления локальными ресурсами и вспомогательными функциями, могут представлять собой:

Уязвимости протоколов сетевого взаимодействия связаны с особенностями их программной реализации и обусловлены ограничениями на размеры применяемого буфера, недостатками процедуры аутентификации, отсутствием проверок правильности служебной информации и др.

Характеристика уязвимостей прикладного ПО.

К прикладному программному обеспечению относятся прикладные программы общего пользования и специальные прикладные программы.

Прикладные программы общего пользования – это

Специальные прикладные программы – это

Уязвимости прикладного программного обеспечения могут представлять собой:

5.3. Характеристика угроз непосредственного доступа в операционную среду ИСПДн.

Угрозы доступа (проникновения) в операционную среду компьютера и несанкционированного доступа к ПДн связаны с доступом:

Эти угрозы могут быть реализованы в случае получения физического доступа к ИСПДн или, по крайней мере, к средствам ввода информации в ИСПДн:

Угрозы, реализуемые в ходе загрузки операционной системы

Угрозы, реализуемые после загрузки операционной среды независимо от того, какая прикладная программа запускается пользователем

Угрозы, реализация которых определяется тем, какая из прикладных программ запускается пользователем, или фактом запуска любой из прикладных программ.Большая часть таких угроз – это угрозы внедрения вредоносных программ.

5.4. Общая характеристика УБПДн, реализуемых с использованием протоколов межсетевого взаимодействия.

Классификация угроз, реализуемых по сети, приведена в Таблице 5. В ее основу положено семь первичных признаков классификации.

Таблица 5 Описание угроз

№ п/п	Признак классификации	Тип угрозы	Описание

С учетом проведенной классификации можно выделить _____угроз, реализуемых с использованием протоколов межсетевого взаимодействия:

Анализ сетевого трафика.

Сканирование сети.

Угроза выявления пароля.

Подмена доверенного объекта сети и передача по каналам связи сообщений от его имени с присвоением его прав доступа.

Навязывание ложного маршрута сети.

Внедрение ложного объекта сети.

Отказ в обслуживании.

Удаленный запуск приложений.

5..5. Общая характеристика угроз программно-математических воздействий.

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

Вредоносные программы могут быть внесены (внедрены) как преднамеренно, так и случайно в программное обеспечение, используемое в ИС, в процессе его разработки, сопровождения, модификации и настройки. Кроме этого, вредоносные программы могут быть внесены в процессе эксплуатации ИС с внешних носителей информации или посредством сетевого взаимодействия как в результате НСД, так и случайно пользователями ИС.

Основными видами вредоносных программ являются:

Вредоносными программами, обеспечивающими осуществление НСД, могут быть:

5.6. Общая характеристика нетрадиционных информационных каналов.

Нетрадиционный информационный канал – это_____

Для формирования нетрадиционных каналов могут использоваться методы:

Методы компьютерной стеганографии предназначены для скрытия факта передачи сообщения путем встраивания скрываемой информации во внешне безобидные данные (текстовые, графические, аудио- или видеофайлы) и включают в себя **две группы методов**, основанных:

Нетрадиционные информационные каналы могут быть сформированы на различных уровнях функционирования ИСПДн:

5.7. Общая характеристика результатов несанкционированного или случайного доступа.

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

Нарушению конфиденциальности (копирование, неправомерное распространение), которое может быть осуществлено в случае утечки информации за счет:

Нарушению целостности (уничтожение, изменение) за счет воздействия (модификации) на программы и данные пользователя, а также технологическую (системную) информацию, включающую:

Нарушение целостности информации в ИСПДн может также быть вызвано внедрением в нее вредоносной программы программно-аппаратной закладки или воздействием на систему защиты информации или ее элементы.

Кроме этого, в ИСПДн возможно воздействие на технологическую сетевую информацию, которая может обеспечивать функционирование различных средств управления вычислительной сетью:

Нарушению доступности (блокирование) путем формирования (модификации) исходных данных, которые при обработке вызывают неправильное функционирование, отказы аппаратуры или захват (загрузку) вычислительных ресурсов системы, которые необходимы для выполнения программ и работы аппаратуры.

Указанные действия могут привести к нарушению или отказу функционирования практически любых технических средств ИСПДн:

8. Определение уровня исходной защищенности ИСПДн

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

Таблица 6 Показатели исходной защищенности ИСПДн

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

В соответствии с Таблицей Описание угроз, _____ % характеристик ИСПДн соответствуют уровню не ниже "_____", следовательно,Y_1= _____ .

ИСПДн имеет _____ степень исходной защищенности.

9. Определение вероятности реализации угроз в ИСПДн

Под вероятностью реализации угрозы поднимается определяемый экспертным путем показатель, характеризующий, насколько вероятным является реализации конкретной угрозы безопасности ПДн для данной ИСПДн в складывающихся условиях обстановки.

Вероятность (Y_2) определяется по 4 вербальным градациям этого показателя:

Таблица 7 Вероятность реализации угроз (вербальный показатель)

Градация	**Описание**	**Вероятность (Y2)**

Оценка вероятности реализации угрозы безопасности различными категориями нарушителей приведена в следующей таблице

Таблица8 Вероятность реализации угроз (вероятностный показатель)

Угроза безопасности ПДн	Вероятность реализации угрозы нарушителем категории Кn

По итогам оценки уровня исходной защищенности (Y_1) и вероятности реализации угрозы (Y_2), рассчитывается коэффициент реализуемости угрозы (Y) и определяется возможность реализации угрозы (Таблица 9). Коэффициент реализуемости угрозы рассчитывается по формуле: $Y = (Y_1+Y_2)/20$.

Таблица 9 Коэффициент реализуемости угрозы

Угроза безопасности ПДн	Коэффициент реализуемости угрозы (Y)	Возможность реализации угрозы

1.1. Оценка опасности угроз ИСПДн

Оценка опасности производится на основе опроса специалистов по защите информации и определяется вербальным показателем опасности, который имеет 3 значения:

низкая опасность – ……;

средняя опасность – ……;

высокая опасность – ……..

Оценка опасности с учетом приведенных критерием представлена в таблице 10.

Таблица 10 Оценка опасности

Угроза безопасности ПДн	Опасность угроз

1.2. Перечень актуальных УБПДн в ИСПДн

Правила, отнесения угроз к актуальным приведены в Таблице 11.

Таблица 11 Актуальность угроз

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

В соответствии с правилами отнесения угроз безопасности к актуальным, для ИСПДн существуют следующие актуальные угрозы.

Таблица 12 Актуальные угрозы ИСПДн

Угроза безопасности ПДн	Опасность угроз

Таким образом, актуальными угрозами безопасности ПДн в ИСПДн являются:

_____

_____

_____

_____

Заключение

В настоящем документе проведена классификация УБПДн в ИСПДн, дано общее описание УБПДн и построена Модель угроз. В соответствии с требованиями методических документов ФСТЭК России, выявлены актуальные угрозы безопасности ПДн в ИСПДн, на основе которых в дальнейшем должны быть разработаны Требования по обеспечению безопасности ПДн в ИСПДн.

Построенная Модель угроз безопасности ПДн в ИСПДн применима к существующему состоянию ИСПДн при условии соблюдения основных (базовых) исходных данных:

- технические средства ИСПДн находятся в пределах контролируемой зоны;
- ИСПДн физически отделена от сетей общего пользования;
- отсутствует возможность неконтролируемого пребывания посторонних лиц в служебных помещениях ИСПДн и др.

В случае несоблюдения и/или изменения вышеуказанных условий Модель угроз безопасности ПДн в ИСПДн должна быть подвергнута пересмотру.

Информационные источники:

1. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России.

2. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России.

3. Методические рекомендации по технической защите информации, составляющей коммерческую тайну. ФСТЭК России.

4. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»