Общество с ограниченной ответственностью «Академ-Сервис»

Челябинская область, г. Челябинск, ул. Университетская Набережная, д.99

УТВЕРЖДАЮ

Директор ООО «Академ-Сервис»

_____ Шегалеева А.В.

01.12.2025 года

М. П.

ЧАСТНАЯ МОДЕЛЬ УГРОЗ

безопасности персональных данных при их обработке в информационной системе персональных данных «Управляющая организация»

город Челябинск 2025 год

Раздел I. ОБЩИЕ ПОЛОЖЕНИЯ

1. Настоящий документ подготовлен в рамках реализации мероприятий, утвержденных «Политикой в отношении обработки и защиты персональных данных», утвержденного директором 01.12.2025 года.

2. Частная модель угроз безопасности (далее по тексту – Модель угроз) персональных данных (далее – ПДн) при их обработке в информационных системах персональных данных (далее – ИСПДн) утверждается директором и является внутренним локальным нормативным актом Общества с ограниченной ответственностью «Академ-Сервис» (далее по тексту – Общество).

3. Настоящая Модель угроз определяет перечень угроз для ИСПДн №1 «Управляющая организация» и их актуальность.

4. Данная Модель угроз учитывается при определении необходимого уровня защищенности персональных данных, обрабатываемых в ИСПДн №1 Общества.

5. Модель угроз может быть пересмотрена:

- по решению Комиссии по персональным данным Общества на основе периодически проводимых анализа и оценки угроз безопасности персональных данных с учетом особенностей и (или) изменений данной информационной системы;

- в случае изменения в составе и территориальном расположении технических средств ИСПДн №1;

- по результатам мероприятий по контролю за выполнением требований к обеспечению безопасности персональных данных при их обработке в информационной системе.

6. Частная модель угроз безопасности персональных данных, обрабатываемых в ИСПДн №1 «Управляющая организация» разработана с учетом требований следующих законодательных актов и нормативно-методических документов:

- Федеральный закон от 01.01.2001 года «О персональных данных».

- Постановление Правительства Российской Федерации от 1 ноября 2012 года № 000 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

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

- Порядок проведения классификации информационных систем персональных данных, утвержденный совместным приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 01.01.2001 года № 55/86/20 (далее – «Порядок проведения классификации ИСПДн»).

- Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденная приказом ФСТЭК России 15.02.2008 года.

- Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утверждена приказом ФСТЭК России 14.02.2008 года.

- Положение о методах и способах защиты информации в информационных системах персональных данных, утвержденное приказом ФСТЭК России №58 от 5 февраля 2010 года.

Раздел II. ЧАСТНАЯ МОДЕЛЬ УГРОЗ безопасности ПДн при их обработке в ИСПДн №1 «Управляющая организация»

1. Параметры ИСПДн №1 «Управляющая организация»

В соответствии с требованиями к защите персональных данных при их обработке в информационных системах персональных данных, установленных Постановлением Правительства Российской Федерации от 1 ноября 2012 года №1119, ИСПДн №1 является информационной системой, обрабатывающей иные категории персональных данных менее чем 100.000 субъектов ПДн, для которой актуальны угрозы безопасности персональных данных 2-го типа, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в ИСПДн №1, и для которой необходимо обеспечить 3-й уровень защищенности ПДн при их обработке в данной информационной системе.

В таблице №1 представлены параметры ИСПДн №1 «Управляющая организация».

Таблица №1

Структура ИСПДн	Локальная информационная система, вся обработка ПДн производится в рамках одной локальной вычислительной

Структура ИСПДн	Локальная информационная система, вся обработка ПДн производится в рамках одной локальной вычислительной сети, имеющей автоматизированные рабочие места (АРМ)
Подключение ИСПДн к сетям общего пользования и (или) сетям международного информационного обмена	информационная система имеет подключения к сетям связи общего пользования и/или сетям международного информационного обмена
Режим обработки ПДн	многопользовательский
Режим разграничения прав доступа пользователей	с разграничениями прав доступа
Местонахождение технических средств ИСПДн	в пределах Российской Федерации
Категория ПДн, обрабатываемых в ИСПДн	обрабатывающая персональные данные работников Общества, персональные данные собственников (нанимателей) помещений в МКД, находящихся в управлении Общества, и иные категории персональных данных субъектов персональных данных, не являющихся работниками Общества
Объем ПДн, обрабатываемых в ИСПДн	ПДн менее 100.000 субъектов ПДн
Заданные характеристики безопасности ПДн	Специальная информационная система

2. Исходный уровень защищенности ИСПДн №1.

Под исходным уровнем защищенности - **Y1**. - понимается определяемый экспертным путем обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИСПДн.

В таблице №2 представлены характеристики уровня исходной защищенности ИСПДн №1 «Управляющая организация».

Таблица №2

Технические и эксплуатационные характеристики ИСПДн №1		**Уровень защищенности (Y1)**		
Типы характеристик	**Характеристики ИСПДн №1**	Высокий	Средний	Низкий
По территориальному размещению	локальная ИСПДн, развернутая в пределах одного здания	+	–	–
По наличию соединения с сетями общего пользования	ИСПДн, имеющая одноточечный вход в сеть общего пользования	–	–	+
По встроенным (легальным) операциям с записями баз персональных данных	чтение, поиск, запись, удаление, сортировка, копирование, модификация, передача	+	–	–
По разграничению доступа к персональным данным	ИСПДн, к которой имеет доступ определенный перечень работников Общества, либо субъект ПДн	–	–	+

По наличию соединений с другими базами ПДн иных ИСПДн	ИСПДн, в которой используется несколько баз ПДн, принадлежащих Обществу	+	–	–
По уровню обобщения (обезличивания) ПДн	ИСПДн, в которой ПДн обезличиваются в соответствии с требованиями принятого в Обществе локального нормативного акта	-	+	-
По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки	ИСПДн, предоставляющая часть ПДн	-	+	-

ВЫВОД: ИСПДн №1 имеет **средний уровень исходной защищенности**, так как более 70% характеристик соответствуют уровню не ниже «средний». Показатель исходной защищенности **Y1= 5**[1].

3. Вероятность реализации угроз безопасности ПДн

Под вероятностью реализации угрозы понимается определяемый экспертным путем показатель – **Y2.**, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности ПДн для ИСПДн №1 в складывающихся условиях обстановки.

В таблице №3 приведено описание каждой угрозы и даны обобщенные вероятности реализации угроз и оценка опасности каждой угрозы для ИСПДн №1.

Таблица №3

Тип угроз безопасности ПДн	Коэффициент вероятности реализации (Y2.)[2]	Оценка опасности угрозы**[3]

---

[1] Исходная степень защищенности определяется следующим образом:

ИСПДн имеет высокий уровень исходной защищенности, если не менее 70% характеристик ИСПДн соответствуют уровню «высокий» (суммируются положительные решения по первому столбцу, соответствующему высокому уровню защищенности), а остальные – среднему уровню защищенности (положительные решения по второму столбцу) (Y1= 0).

ИСПДн имеет средний уровень исходной защищенности, если не выполняются условия по пункту 1 и не менее 70% характеристик ИСПДн соответствуют уровню не ниже «средний» (берется отношение суммы положительные решений по второму столбцу, соответствующему среднему уровню защищенности, к общему количеству решений), а остальные - низкому уровню защищенности (Y1= 5).

ИСПДн имеет низкую степень исходной защищенности, если не выполняется условия по пунктам 1 и 2 (Y1= 10).

Угрозы утечки видовой информации		
Просмотр информации, отображаемой на дисплее монитора сотрудниками, не допущенными к обработке персональных данных	5	средняя
Просмотр информации, отображаемой на дисплее монитора посторонними лицами, находящимися в помещении, в котором ведется обработка персональных данных	2	низкая
Просмотр информации, отображаемой на дисплее монитора посторонними лицами, находящимися за пределами помещения, в котором ведется обработка персональных данных	0	маловероятна
Угрозы утечки информации по каналам ПЭМИН. Электромагнитные каналы утечки информации.		
Перехват побочных электромагнитных излучений элементов основных технических средств и систем (ОТСС)	0	маловероятна
Съем наводок побочных электромагнитных излучений основных технических средств и систем (ОТСС) с линий связи, технических средств и систем коммуникаций	0	маловероятна
Угрозы утечки информации по каналам ПЭМИН. Электрические каналы утечки информации		
Съем информационных сигналов с линий электропитания основных технических средств и систем (ОТСС)	0	маловероятна
Съем информационных сигналов с цепей заземления основных технических средств и систем (ОТСС) и вспомогательных технических средств и систем (ВТСС)	0	маловероятна
Угрозы утечки информации по каналам ПЭМИН. Параметрические каналы утечки информации		
Перехват информации путем "высокочастотного облучения" основных технических средств и систем (ОТСС)	0	маловероятна

[2] Числовой коэффициент (Y2) для оценки вероятности возникновения угрозы определяется по 4 вербальным градациям этого показателя:

маловероятно - отсутствуют объективные предпосылки для осуществления угрозы (Y2 = 0);

низкая вероятность - объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (Y2 = 2);

средняя вероятность - объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны (Y2 = 5);

высокая вероятность - объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности ПДн не приняты (Y2 = 10).

[3] Оценка опасности угрозы определяется на основе опроса специалистов по вербальным показателям опасности с тремя значениями:

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.

Угрозы, реализуемые при физическом доступе		
Кража ПЭВМ	0	маловероятна
Вывод из строя узлов ПЭВМ, каналов связи	0	маловероятна
Кража элементов (жесткий диск) ПЭВМ	0	маловероятна
Несанкционированный доступ к информации при техническом обслуживании (ремонте, модернизации) ПЭВМ	2	низкая
Кража ключей от помещений, сейфов	2	низкая
Кража носителей ключевой информации	2	низкая
Кража индивидуальных устройств идентификации	2	низкая
Угрозы, возникающие при использовании съемных носителей персональных данных		
Кража съемных носителей ПДн	0	маловероятная
Использование не учтенных носителей ПДн	5	средняя
Утрата съемных носителей ПДн	2	низкая
Угрозы внедрения программных закладок		
Компьютерные вирусы	2	низкая
Несанкционированная модификация или уничтожение защищаемой информации	2	низкая
Несанкционированный перенос защищаемой информации на твердую копию	2	низкая
Несанкционированный доступ внешних нарушителей к ресурсам ИСПДн	2	низкая
Загрузка ОС с внешних носителей (CD, DVD, USB Flash, внешний USB - винчестер и т. д.)	0	маловероятно
Несанкционированное отключение средств защиты	0	маловероятно
Угрозы несанкционированного доступа по каналам связи		
Перехват информации, передаваемой по локальной сети	2	низкая
Перехват информации, передаваемой по сетям международного обмена	0	маловероятно
Сканирование, направленное на выявление типа ОС, открытых портов и служб, открытых соединений и др.	2	низкая
Подбор паролей через локальную вычислительную сеть организации или сети международного обмена	5	средний
Несанкционированный доступ через сети международного обмена	5	средний
Несанкционированный доступ через локальную вычислительную сеть организации	5	средний
Несанкционированный удаленный запуск приложений	2	низкая

Подмена доверенного объекта сети	5	средний
Внедрение ложного объекта	5	средний
Навязывание ложного маршрута	2	низкая
Угрозы непреднамеренных действий внутренних нарушителей		
Непреднамеренная модификация или уничтожение информации сотрудниками, допущенными к ее обработке	0	маловероятно
Непреднамеренное отключение средств защиты	0	маловероятно
Утрата ключей от помещений, сейфов	2	низкая
Утрата носителей ключевой информации	2	низкая
Утрата индивидуальных устройств идентификации	2	низкая
Угрозы недекларированных (недокументированных) возможностей		
Угрозы, связанные с наличием недекларированных (недокументированных) возможностей в системном ПО, используемом в ИСПДн;	0	маловероятна
Угрозы, связанные с наличием недекларированных возможностей в прикладном ПО, используемом в ИСПДн;	2	низкая
Угрозы, не связанные с наличием недекларированных возможностей в программном обеспечении, используемом в ИСПДн	0	маловероятна
Угрозы неатропогенного характера		
Сбой системы электроснабжения	2	низкая
Стихийное бедствие	2	низкая

4. Оценка возможности реализации и опасности угроз

По итогам оценки уровня защищенности (Y1) и вероятности реализации угрозы (Y2), рассчитывается коэффициент реализуемости угрозы (Y) и определяется возможность реализации угрозы. Коэффициент реализуемости угрозы Y будет определяться соотношением Y = (Y1 + Y2)/20.[4]

В таблице №4 приведено описание угрозы, дан расчетный коэффициент реализуемости угрозы (Y) и определяется возможность реализации угрозы.

Таблица №4

Тип угроз безопасности ПДн	Коэффициент реализуемости угрозы (Y)	Возможность реализации

[4] Рассчитанный по формуле Y=(Y1+Y2)/20 коэффициент реализуемости угрозы определяется по следующим диапазонам: 0>Y>0,3 – низкая; 0,3>Y>0,6 – средняя; 0,6>Y>0,8 – высокая; Y>0,8 – очень высокая

Угрозы утечки видовой информации		
Просмотр информации, отображаемой на дисплее монитора сотрудниками, не допущенными к обработке персональных данных	0,35	средняя
Просмотр информации, отображаемой на дисплее монитора посторонними лицами, находящимися в помещении, в котором ведется обработка персональных данных	0,35	средняя
Просмотр информации, отображаемой на дисплее монитора посторонними лицами, находящимися за пределами помещения, в котором ведется обработка персональных данных	0,35	средняя
Угрозы утечки информации по каналам ПЭМИН. Электромагнитные каналы утечки информации.		
Перехват побочных электромагнитных излучений элементов основных технических средств и систем (ОТСС)	0,25	низкая
Съем наводок побочных электромагнитных излучений основных технических средств и систем (ОТСС) с линий связи, технических средств и систем коммуникаций	0,25	низкая
Угрозы утечки информации по каналам ПЭМИН. Электрические каналы утечки информации		
Съем информационных сигналов с линий электропитания основных технических средств и систем (ОТСС)	0,25	низкая
Съем информационных сигналов с цепей заземления основных технических средств и систем (ОТСС) и вспомогательных технических средств и систем (ВТСС)	0,25	низкая
Угрозы утечки информации по каналам ПЭМИН. Параметрические каналы утечки информации		
Перехват информации путем "высокочастотного облучения" основных технических средств и систем (ОТСС)	0,25	низкая
Угрозы, реализуемые при физическом доступе		
Кража ПЭВМ	0,35	средняя
Вывод из строя узлов ПЭВМ, каналов связи	0,35	средняя
Кража элементов (жесткий диск) ПЭВМ	0,35	средняя
Несанкционированный доступ к информации при техническом обслуживании (ремонте, модернизации) ПЭВМ	0,25	низкая
Кража ключей от помещений, сейфов	0,35	средняя
Кража носителей ключевой информации	0,35	средняя
Кража индивидуальных устройств идентификации	0,35	средняя
Угрозы, возникающие при использовании съемных носителей персональных данных		
Кража съемных носителей ПДн	0,25	низкая
Использование не учтенных носителей ПДн	0,35	средняя
Утрата съемных носителей ПДн	0,25	низкая

Угрозы внедрения программных закладок		
Компьютерные вирусы	0,25	низкая
Несанкционированная модификация или уничтожение защищаемой информации	0,25	низкая
Несанкционированный перенос защищаемой информации на твердую копию	0,25	низкая
Несанкционированный доступ внешних нарушителей к ресурсам ИСПДн	0,25	низкая
Загрузка ОС с внешних носителей (CD, DVD, USB Flash, внешний USB - винчестер и т. д.)	0,25	низкая
Несанкционированное отключение средств защиты	0,25	низкая
Угрозы несанкционированного доступа по каналам связи		
Перехват информации, передаваемой по локальной сети	0,25	низкая
Перехват информации, передаваемой по сетям международного обмена	0,25	низкая
Сканирование, направленное на выявление типа ОС, открытых портов и служб, открытых соединений и др.	0,25	низкая
Подбор паролей через локальную вычислительную сеть организации или сети международного обмена	0,25	средний
Несанкционированный доступ через сети международного обмена	0,35	средний
Несанкционированный доступ через локальную вычислительную сеть организации	0,35	средний
Несанкционированный удаленный запуск приложений	0,25	низкая
Подмена доверенного объекта сети	0,35	средний
Внедрение ложного объекта	0,35	средний
Навязывание ложного маршрута	0,25	низкая
Угрозы непреднамеренных действий внутренних нарушителей		
Непреднамеренная модификация или уничтожение информации сотрудниками, допущенными к ее обработке	0,25	низкая
Непреднамеренное отключение средств защиты	0,25	низкая
Утрата ключей от помещений, сейфов	0,25	низкая
Утрата носителей ключевой информации	0,25	низкая
Утрата индивидуальных устройств идентификации	0,25	низкая
Угрозы недекларированных (недокументированных) возможностей		
Угрозы, связанные с наличием недекларированных (недокументированных) возможностей в системном ПО, используемом в ИСПДн;	0,25	низкая

Угрозы, связанные с наличием недекларированных возможностей в прикладном ПО, используемом в ИСПДн;	0,35	средняя
Угрозы, не связанные с наличием недекларированных возможностей в программном обеспечении, используемом в ИСПДн	0,25	низкая
Угрозы неатропогенного характера		
Сбой системы электроснабжения	0,25	низкая
Стихийное бедствие	0,25	низкая

5. Модель угроз безопасности

В таблице №5 представлены актуальные угрозы безопасности для ИСПДн №1 «Управляющая организация», а также способы их противодействия.

Таблица №5

Наименование угрозы	Уровень исходной защищенности	Опасность угрозы	Вероятность реализации угрозы	Актуальность угрозы	Рекомендации по противодействию угрозе	
					Технические	Организационные
Угрозы утечки видовой информации						
Просмотр информации, отображаемой на дисплее монитора сотрудниками, не допущенными к обработке персональных данных	средний	средняя	средняя	актуальная		Огораживающие стойки; Должностная инструкция Администратора ПДн; Должностная инструкция пользователя ИСПДн;
Просмотр информации, отображаемой на дисплее монитора посторонними лицами, находящимися в помещении, в котором ведется обработка персональных данных	средний	средняя	средняя	актуальная		Огораживающие стойки; Пропускной режим; Должностная инструкция Администратора ПДн; Должностная инструкция пользователя ИСПДн; Положение о СКУД;
Просмотр информации, отображаемой на дисплее монитора посторонними лицами, находящимися за пределами	средний	средняя	средняя	актуальная	Жалюзи	Должностная инструкция Администратора ПДн; Должностная инструкция пользователя ИСПДн;

помещения, в котором ведется обработка персональных данных						
Угрозы утечки информации по каналам ПЭМИН. Электромагнитные каналы утечки информации.						
Перехват побочных электромагнитных излучений элементов основных технических средств и систем (ОТСС)	средний	низкая	низкая	Не актуальная		
Съем наводок побочных электромагнитных излучений основных технических средств и систем (ОТСС) с линий связи, технических средств и систем коммуникаций	средний	низкая	низкая	Не актуальная		
Угрозы утечки информации по каналам ПЭМИН. Электрические каналы утечки информации						
Съем информационных сигналов с линий электропитания основных технических средств и систем (ОТСС)	средний	низкая	низкая	Не актуальная		
Съем информационных сигналов с цепей заземления основных технических средств и систем (ОТСС) и вспомогательных технических средств и систем (ВТСС)	средний	низкая	низкая	Не актуальная		
Угрозы утечки информации по каналам ПЭМИН. Параметрические каналы утечки информации						
Перехват информации путем "высокочастотного облучения" основных технических средств и систем (ОТСС)	средний	низкая	низкая	Не актуальная		
Угрозы, реализуемые при физическом доступе						

Кража ПЭВМ	средний	средняя	низкая	актуальная	Дверной замок Видеоконтроль	Пропускной режим; Охрана; Должностная инструкция пользователя ИСПДн; Должностная инструкция Администратора ПДн; Положение о СКУД;
Вывод из строя узлов ПЭВМ, каналов связи	средний	средняя	низкая	актуальная	Дверной замок Видеоконтроль	Пропускной режим; Охрана; Должностная инструкция Администратора ПДн; Положение о СКУД;
Кража элементов (жесткий диск) ПЭВМ	средний	средняя	низкая	актуальная	Дверной замок Видеоконтроль	Пропускной режим; Опломбирование ПЭВМ; Охрана; Должностная инструкция пользователя ИСПДн; Должностная инструкция Администратора ПДн; Положение о СКУД;
Несанкционированный доступ к информации при техническом обслуживании (ремонте, модернизации) ПЭВМ	средний	низкая	низкая	Не актуальная		
Кража ключей от помещений, сейфов	средний	средняя	низкая	актуальная		Пропускной режим; Охрана; Должностная инструкция пользователя ИСПДн; Положение о СКУД;
Кража носителей ключевой информации	средний	средняя	низкая	актуальная	Хранение в сейфе	Пропускной режим; Охрана; Должностная инструкция пользователя ИСПДн;

						Журнале учета носителей ключевой информации;
Кража индивидуальных устройств идентификации	средний	средняя	низкая	актуальная	Хранение в сейфе	Пропускной режим; Охрана; Должностная инструкция пользователя ИСПДн; Журнал учета индивидуальных устройств идентификации;
Угрозы, возникающие при использовании съемных носителей персональных данных						
Кража съемных носителей ПДн	средний	средняя	низкая	актуальная	Хранение в сейфе	Пропускной режим; Охрана; Должностная инструкция пользователя ИСПДн; Журнал учета машинных носителей информации; Положение о СКУД;
Использование не учтенных носителей ПДн	средний	средняя	средняя	актуальная	Контроль доступа к внешним устройствам	Должностная инструкция Администратора ПДн; Должностная инструкция пользователя ИСПДн;
Утрата съемных носителей ПДн	средний	средняя	низкая	актуальная		Должностная инструкция пользователя ИСПДн; Журнал учета машинных носителей информации;
Угрозы внедрения программных закладок						
Компьютерные вирусы	средний	средняя	низкая	актуальная	Средства антивирусной защиты; Контроль целостности программных средств защиты;	ИНСТРУКЦИЯ по организации антивирусной защиты в ИСПДн;
Несанкционированная модификация или уничтожение защищаемой	средний	средняя	низкая	актуальная	Резервирование обрабатываемой информации; Регистрация	

информации					действий пользователей;	
Несанкционированный перенос защищаемой информации на твердую копию	средний	средняя	низкая	актуальная	Регистрация печати конфиденциальных документов;	
Несанкционированный доступ внешних нарушителей к ресурсам ИСПДн	средний	средняя	низкая	актуальная	Идентификация и аутентификация; Использование смарт-карт, электронных замков и других носителей информации для надежной идентификации и аутентификации пользователей; Контроль доступа к информации, хранящейся в ПЭВМ; Контроль доступа к информации, хранящейся в БД; Регистрация действий пользователей;	Должностная инструкция Администратора ПДн; Положение о СКУД; ИНСТРУКЦИЯ по организации антивирусной защиты в ИСПДн;
Загрузка ОС с внешних носителей (CD, DVD, USB Flash, внешний USB - винчестер и т. д.)	средний	низкая	маловероятно	Не актуальная		
Несанкционированное отключение средств защиты	средний	низкая	маловероятно	Не актуальная		
Угрозы несанкционированного доступа по каналам связи						
Перехват информации, передаваемой по локальной сети	средний	низкая	низкая	Не актуальная		
Перехват информации, передаваемой по сетям международного обмена	средний	низкая	маловероятно	Не актуальная		
Сканирование, направленное на	средний	средняя	низкая	актуальн	Межсетевое экранирование	Должностная инструкция

выявление типа ОС, открытых портов и служб, открытых соединений и др.				ая	(контроль Internet трафика); Системы обнаружения вторжений;	пользователя ИСПДн;
Подбор паролей через локальную вычислительную сеть организации или сети международного обмена	средний	средний	средний	актуальная	Системы обнаружения вторжений;	Должностная инструкция пользователя ИСПДн; Должностная инструкция Администратора ПДн;
Несанкционированный доступ через сети международного обмена	средний	средний	средний	актуальная	Межсетевое экранирование (контроль Internet трафика); Системы обнаружения вторжений; Системы анализа защищенности;	Должностная инструкция Администратора ПДн;
Несанкционированный доступ через локальную вычислительную сеть организации	средний	средний	средний	актуальная	Межсетевое экранирование (контроль Internet трафика); Системы обнаружения вторжений; Системы анализа защищенности;	Должностная инструкция Администратора ПДн;
Несанкционированный удаленный запуск приложений	средний	низкая	низкая	не актуальная		
Подмена доверенного объекта сети	средний	средний	средний	актуальная	Системы обнаружения вторжений;	Должностная инструкция пользователя ИСПДн;
Внедрение ложного объекта	средний	средний	средний	актуальная	Системы обнаружения вторжений;	Должностная инструкция пользователя ИСПДн;
Навязывание ложного маршрута	средний	низкая	низкая	не актуальная		
Угрозы непреднамеренных действий внутренних нарушителей						
Непреднамеренная модификация или уничтожение информации сотрудниками,	средний	низкая	маловероятно	Не актуальная	Резервирование обрабатываемой информации;	

допущенными к ее обработке						
Непреднамеренное отключение средств защиты	средний	низкая	маловероятно	Не актуальная		
Утрата ключей от помещений, сейфов	средний	низкая	низкая	Не актуальная		Должностная инструкция пользователя ИСПДн;
Утрата носителей ключевой информации	средний	низкая	низкая	Не актуальная		Должностная инструкция пользователя ИСПДн; Журнал учета носителей ключевой информации;
Утрата индивидуальных устройств идентификации	средний	низкая	низкая	Не актуальная		
Угрозы недекларированных (недокументированных) возможностей						
Угрозы, связанные с наличием недекларированных (недокументированных) возможностей в системном ПО, используемом в ИСПДн;	средний	низкая	низкая	Не актуальная	Установка сертифицированных средств защиты и ПО	
Угрозы, связанные с наличием недекларированных возможностей в прикладном ПО, используемом в ИСПДн;	средний	средний	средний	актуальная	Установка сертифицированных средств защиты и ПО	
Угрозы, не связанные с наличием недекларированных возможностей в программном обеспечении, используемом в ИСПДн	средний	низкая	низкая	Не актуальная	Установка сертифицированных средств защиты и ПО	
Угрозы неатропогенного характера						
Сбой системы электроснабжения	средний	средняя	низкая	актуальная	Источники бесперебойного питания; Резервирование обрабатываемой	

					информации;	
Стихийное бедствие	средний	средняя	низкая	актуальная	Пожарная сигнализация;	

ЗАКЛЮЧЕНИЕ

1. Актуальными угрозами безопасности ПДн в ИСПДн №1 являются:

- угрозы от действий вредоносных программ (вирусов);

- угрозы утраты ключей и атрибутов доступа;

- доступ к информации, копирование, модификация, уничтожение лицами, не допущенными к ее обработке

- разглашение информации, копирование, модификация, уничтожение Работниками, допущенными к ее обработке

- угрозы выявления паролей по сети;

- угрозы внедрения по сети вредоносных программ;

- угрозы, связанные с наличием недекларированных возможностей в прикладном ПО, используемом в ИСПДн.

2. Необходимо выполнение следующих требований:

- организация режима обеспечения безопасности помещений, в которых размещена ИСПДн №1, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

- обеспечение сохранности носителей персональных данных;

- утверждение директором Общества документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в ИСПДн №1, необходим для выполнения ими трудовых обязанностей;

- использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз;

- реализация парольной политики, устанавливающая обязательную сложность и периодичность смены пароля;

- методы и средства аутентификации пользователей на основе usb-ключей, паролей и логинов доступа

- технически обеспечить обязательную регистрацию и учет всех действий, которые пользователи совершают с персональными данными в ИСПДн №1

- мероприятия по контролю доступа в контролируемую зону лиц, не имеющих доступа к обработке ПДн

- регулярный инструктаж пользователей о мерах предотвращения вирусного заражения

- организация постоянного контроля над выполнением пользователями инструкций по обеспечению защиты ПДн, положений парольной политики, и за их действиями в случаях утраты или компрометации паролей

- подписание пользователями документа о неразглашении ПДн.

3. Состав и содержание мер по обеспечению безопасности ПДн в ИСПДн №1

В соответствии с требованиями Приказа 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» Обществу необходимо обеспечить базовый состав мер по обеспечению 3 уровня защищенности персональных данных в ИСПДн №1, приведенный в таблице №6.

Таблица №6

Условное обозначение и номер меры[5]	**Содержание мер по обеспечению безопасности персональных данных**[6]
I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)	
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора
ИАФ.2	Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных
ИАФ. 3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов
ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации
ИАФ.5	Защита обратной связи при вводе аутентификационной информации
ИАФ.6	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)
II. Управление доступом субъектов доступа к объектам доступа (УПД)	
УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей
УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа

[5] Номер меры приведен в соответствии с Приказом ФСТЭК №21

[6] Нумерация содержания мер приведена в соответствии с Приказом ФСТЭК №21

УПД. 3	Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами
УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы
УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы
УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)
УПД.10	Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу
УПД.11	Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации
УПД.13	Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети
УПД.14	Регламентация и контроль использования в информационной системе технологий беспроводного доступа
УПД.15	Регламентация и контроль использования в информационной системе мобильных технических средств
УПД.16	Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)
IV. Защита машинных носителей персональных данных (ЗНИ)	
ЗНИ.8	Уничтожение (стирание) или обезличивание персональных данных на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) или обезличивания
V. Регистрация событий безопасности (РСБ)	
РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения
РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации
РСБ. 3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения
РСБ. 7	Защита информации о событиях безопасности
VI. Антивирусная защита (АВЗ)	
АВЗ.1	Реализация антивирусной защиты

АВ3.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)
VIII. Контроль (анализ) защищенности персональных данных (АН3)	
АН3.1	Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей
АН3.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации
АН3.3	Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации
АН3.4	Контроль состава технических средств, программного обеспечения и средств защиты информации
XI. Защита среды виртуализации (ЗСВ)	
ЗСВ.1	Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации
ЗСВ.2	Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин
ЗСВ.3	Регистрация событий безопасности в виртуальной инфраструктуре
ЗСВ.9	Реализация и управление антивирусной защитой в виртуальной инфраструктуре
ЗСВ.10	Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки персональных данных отдельным пользователем и (или) группой пользователей
XII. Защита технических средств (ЗТС)	
ЗТС.3	Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр
XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)	
ЗИС.3	Обеспечение защиты персональных данных от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи
ЗИС.20	Защита беспроводных соединений, применяемых в информационной системе
XV. Управление конфигурацией информационной системы и системы защиты персональных данных	

(УКФ)	
УКФ.1	Определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и системы защиты персональных данных
УКФ.2	Управление изменениями конфигурации информационной системы и системы защиты персональных данных
УКФ.3	Анализ потенциального воздействия планируемых изменений в конфигурации информационной системы и системы защиты персональных данных на обеспечение защиты персональных данных и согласование изменений в конфигурации информационной системы с должностным лицом (работником), ответственным за обеспечение безопасности персональных данных
УКФ.4	Документирование информации (данных) об изменениях в конфигурации информационной системы и системы защиты персональных данных