Утверждено:
приказом от 04.04.2019г. № 05
заведующий МБДОУ детский сад №12
«Рябинка» _____ С.А.Степанова

Модель угроз
безопасности персональных данных при их обработке в информационной системе персональных данных МБДОУ детский сад №12 «Рябинка»

г. Топки

ЛИСТ СОГЛАСОВАНИЙ

№ п/п	Должность	Фамилия, имя, отчество	Подпись	Дата
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				

ЛИСТ ИЗМЕНЕНИЙ

Разрешение		Содержание изменений	Код	Примечание
Изм.	№ лис.			

ОГЛАВЛЕНИЕ

НОРМАТИВНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ

1. Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

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

3. Указ Президента РФ от 17.03.2008 N 351 "О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена";

4. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера»;

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

6. Постановление Правительства РФ от 21.03.2012 N 211 "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами";

7. Постановление Правительства Российской Федерации от 15.09.2008 N 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации";

8. Нормативно-методический документ. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утвержден приказом Гостехкомиссии России от 30.08.2002 г. №282;

9. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 15.02.2008 г.;

10. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 14.02.2008т.;

11. Приказ ФСТЭК России от 18.02.2014 N 21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных";

12. Приказ ФСБ России от 10 июля 2014 г. N 378 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты

информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности".

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

АРМ	Автоматизированное рабочее место
БД	База (-ы) данных
ВТСС	Вспомогательные технические средства и системы
ИБП	Источник бесперебойного питания
НС	Информационная система
ИСПДн	Информационная система персональных данных
ИСПДн «УО АТМР»	Информационная система персональных данных «УО АТМР» УО АТМР
КЗ	Контролируемая зона
ЛВС	Локальная вычислительная сеть
МЭ	Межсетевой экран
НСД	Несанкционированный доступ
ОС	Операционная система
ОТСС	Основные технические средства и системы
ПДн	Персональные данные
ПМВ	Программно-математическое воздействие
ПО	Программное обеспечение
НПО	Прикладное ПО
ПЭМИН	Побочные электромагнитные излучения и наводки
СВТ	Средство (-а) вычислительной техники
СЗИ	Средства защиты информации
СЗПДн	Система (системы) защиты ПДн
СКЗИ	Средство криптографической защиты информации
УБПДн	Угрозы безопасности персональных данных
УО АТМР	Управление образования администрации Топкинского муниципального района
ФСТЭК России	Федеральная служба по техническому и экспортному контролю
ЭМИ	Электромагнитные излучения

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

ПДн - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту ПДн).

Обработка ПДн - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с ПДн, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение ПДн.

Оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки ПДн, состав ПДн, подлежащих обработке, действия (операции), совершаемые с ПДн.

Обезличивание ПДн - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность ПДн конкретному субъекту ПДн.

Блокирование ПДн - временное прекращение обработки ПДн (за исключением случаев, если обработка необходима для уточнения ПДн).

Уничтожение ПДн - действия, в результате которых становится невозможным восстановить содержание ПДн в ИСПДн и (или) в результате которых уничтожаются материальные носители ПДн.

ИСПДн - совокупность содержащихся в БД ПДн и обеспечивающих их обработку информационных технологий и технических средств.

УБПДН - совокупность условий факторов, создающих опасность несанкционированного, в том числе случайного, доступа к ПДн, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение ПДн, а также иных несанкционированных действий при обработке в ИСПДн.

Конфиденциальность ПДн - обязательное для соблюдения оператором или иным получившим доступ к ПДн лицом требование не допускать их распространение без согласия субъекта ПДн или наличия иного законного основания.

Целостность информации - способность СВТ или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

Достоверность (или аутентичность) - свойство обеспечения идентичности субъекта или ресурса заявленной идентичности.

Источник угрозы безопасности информации - субъект доступа, территориальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

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

Нарушитель безопасности ПДн - физическое лицо случайно или

преднамеренно совершающее действия, следствием которого является нарушение безопасности ПДн при их обработке техническими средствами в ИСПДн.

НСД - доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых ИСПДн.

ПЭМИН - электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

Пользователь информационной системы ПДн - лицо, участвующее в функционировании ИСПДН или использующее результаты ее функционирования.

Правила разграничения доступа - совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Программная закладка - код программы, преднамеренно внесенный в программу с целью осуществить утечку, изменить, блокировать, уничтожить информацию или уничтожить и модифицировать ПО ИСПДН и (или) блокировать аппаратные средства.

ВТСС - технические средства и системы, не предназначенные для передачи, обработки и хранения ПДн, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки ПДн или в помещениях, в которых установлены ИСПДн.

Программное (программно-математическое) воздействие - несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

Утечка (защищаемой) информации по техническим каналам неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

1. ОБЩИЕ ПОЛОЖЕНИЯ

Настоящая «Модель угроз безопасности персональных данных» при их обработке в ИСГТДн «УО АТМР» (далее Модель угроз) содержит систематизированный перечень УБПДн ИСПДн «УО АТМР» УО АТМР (далее -Оператор).

Настоящая Модель угроз является частной, и разработана с учетом назначения, условий и особенностей функционирования данной системы.

Положения Модели угроз распространяются на серверное и компьютерное оборудование, установленное на него НПО, включенное в единый сегмент локальной сети и расположенное в здании Оператора по адресу Россия, 652300, г. Топки, ул. Топкинская, 4.

Модель угроз содержит данные по УБПДн, связанным с:

- перехватом (съемом) ПДн по техническим каналам с целью их копирования или неправомерного распространения;
- несанкционированным, в том числе случайным, доступом в ИСПДн с целью изменения, копирования, неправомерного распространения ПДн или деструктивных воздействий на элементы ИСПДн и обрабатываемых в них ПДн с использованием программных и программно-аппаратных средств с целью уничтожения или блокирования ПДн.

Моделью угроз необходимо руководствоваться на всех этапах жизненного цикла системы: при проектировании, в режиме эксплуатации, при проведении регламентных и ремонтно-профилактических работ, модернизации и выводе ее из эксплуатации.

Модель угроз применяется при решении следующих задач:

- анализа защищенности от УБПДн в ходе организации и выполнения работ по обеспечению безопасности ПДн;
- разработки системы защиты ПДн, обеспечивающей нейтрализацию угроз с использованием методов и способов защиты ПДн;
- проведения мероприятий, направленных на предотвращении несанкционированного доступа (далее - НСД) к ПДн и (или) передачи их лицам, не имеющим права доступа к такой информации;
- недопущения воздействия на технические средства ИСПДн, в результате которого может быть нарушено их функционирование;
- контроля над обеспечением уровня защищенности ПДн.

УБПДн, содержащиеся в настоящей Модели угроз, могут уточняться и дополняться по мере выявления новых источников угроз, развития способов и средств реализации УБПДн в ИСПДн.

Для обеспечения актуальности Модели угроз должен осуществляться ее плановый (регулярный) и внеплановый пересмотр.

Плановый пересмотр проводится в порядке проведения контроля

состояния защиты информации (не реже одного раза в год) [8].

Внеплановый пересмотр должен осуществляться в случаях:

- изменения требований законодательства Российской Федерации в области ПДн, нормативно-правовых актов и методических документов, регулирующих защиту ПДн;
- изменения конфигурации и условий размещения ИСПДн;
- изменения в составе основных элементов ИСПДн, которые могут повлиять на состав УБПДн. К таким элементам относятся:
- информационные технологии, как совокупность приемов, способов и методов применения СВТ при обработке ПДн;
- технические средства, осуществляющие обработку ПДн (СВТ, информационно- вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн, средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов, другие технические средства обработки речевой, графической, видео и буквенно-цифровой информации);
- программные средства (ОС, СУБД и т.п.);
- СЗИ; ВТСС.

Внесение изменений в Модель угроз (корректировка) осуществляется по решению Оператора.

2. ОПИСАНИЕ ОБЪЕКТА ИНФОРМАТИЗАЦИИ

2.1 Общие характеристики системы

ИСПДн «УО АТМР» построена на базе ИС УО АТМР.

В ИСПДн «УО АТМР» обработка ПДн осуществляется в следующих целях:

- сбора данных для мониторинга системы образования;
- сбора данных для организации и ведения бухгалтерского и налогового учёта, отчётности;
- представления на награждение;
- организации летнего отдыха;
- планирования ГИА;
- учёта результатов ГИА;
- оформления трудовых отношений.

ИСПДн «УО АТМР» является ИС, обрабатывающей специальные категории ПДн сотрудников и не сотрудников Оператора, в которой обрабатываются ПДн менее чем 100000 субъектов ПДн.

Комиссией по определению уровня защищенности ПДн при их обработке в ИСПДн «УО АТМР», назначенной приказом от «17» марта 2017 г. № 122, был подписан акт №1, и установлено следующее:

для ИСПДн «УО АТМР» актуальны угрозы 3-го типа [5];

- для ИСПДн «УО АТМР» требуется обеспечение 3-го уровня

защищенности ПДн [5].

В ИСПДн «УО АТМР» принятия на основании исключительно автоматизированной обработки ПДн решений, порождающих юридические последствия в отношении субъекта ПДн, не предусмотрено.

Перечень сведений конфиденциального характера, подлежащих защите, в том числе, ПДн утвержден приказом от «17» марта 2017 г. № 120.

Перечень действий с ПДн, осуществляемых в ИСПДн «УО АТМР»: сбор, запись, систематизации, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (предоставление, доступ), удаление.

Способ обработки ПДн - смешанный, с передачей по внутренней сети юридического лица, с передачей по сети Интернет.

Трансграничной передачи ПДн не осуществляется.

БД располагаются в пределах РФ. 2.2 **Структура ИСПДн**

ИСПДн «УО АТМР» является многопользовательской, локальной ИС с системой разграничения прав доступа. ИСПДн «УО АТМР» имеет подключение к сетям общего пользования и сетям международного информационного обмена [4].

Выход пользователей ИСПДн «УО АТМР» в сеть интернет осуществляется через маршрутизатор Eltex ONT NTP-RG-1402G-W rev. C, несертифицированный ФСТЭК России.

Все компоненты ИСПДн «УО АТМР» находятся в пределах КЗ.

Доступ к ПДн в ИСПДн «УО АТМР» регламентируется:

- приказом от «17 »марта 2017 г. № 120;
- приказом от «17» марта 2017 г. № 123;
- приказом от «24» марта 2017 г. № 139.

Перечень аппаратных средств ИСПДн «УО АТМР» представлен в таблице 2.1.

Таблица 2.1 Перечень оборудования ИСПДн «УО АТМР»

Наименование, краткие технические характеристики	**Кол-во**
АРМ сотрудников	**22**
Маршрутизатор, аппаратный МЭ	**1**

2.3 Объекты защиты

В обязательном порядке подлежат защите технические и программные средства, используемые при обработке ПДн, носители информации, а также применяемые СЗИ.

В передаче информации по ЛВС, кроме самой физической среды передачи, участвуют активные сетевые устройства.

На основании анализа данных, полученных в результате обследования, был составлен следующий набор групп объектов защиты:

1)ПДн, обрабатываемые и передаваемые в ИСПДн «УО АТМР» с использованием оборудования ИСПДн: обрабатываемая и передаваемая в ИСПДн информация уровня ОС (объекты ОС: файлы ОС, в том числе включающие информацию, используемую при идентификации и аутентификации пользователей ИСПДн, информация журналов регистрации событий ОС, информация о правах доступа к объектам файловой системы).

2) Программное окружение ИСПДн:

- системное ПО, специальное ПО (специальные прикладные программы, системы
  обработки данных, средства обмена данными и т.п.);
- ПО управления работой компонент ИСПДн;
- коммуникационное ПО.

3) Аппаратное окружение ИСПДн:

- СВТ.

2.4 Оценка существующей системы защиты

В настоящее время в ИСПДн «УО АТМР» используется ряд мер для обеспечения информационной безопасности.

Технические меры защиты

В ИСПДн «УО АТМР» установлены следующие СЗИ (Таблица 2.2)

Таблица 2.2. Перечень СЗИ, используемых в ИСПДн «УО АТМР»

Наименование СЗИ	**Фактическое количество**	**Номер сертификата ФСТЭК/ФСБ России, срок действия**
СЗИ от НСД	2	Сертификат соответствия ФСТЭК России № 2227. Срок действия- 03 декабря 2019 г.
Идентификатор eToken 5	3	Сертификат соответствия ФСТЭК России № 1883. Срок действия- 11 августа 2019 г.
Антивирус ESET Endpoint Security 5	22	Нет
СЗИ «Страж NT», версия 3.0	1	Сертификат соответствия ВСБ России № 2145. Срок действия – 30 июля 2019 г.
СКЗИ VipNet Client КС2, версия 3.1 (сеть 3103 (ДОиН КО)	2	Сертификат соответствия ФСБ России № СФ/515-1838. Срок дейтсвия – 01 июля

		2015 г. Сертификат соответствия ФСБ России № СФ/114-1466. Срок действия – 09 мая 2013 г.
СКЗИ VipNet Client КС2, версия 3.1 (сеть 889 (ОЦМКО)	1	Сертификат соответствия ФСБ России № СФ/515-1838. Срок дейтсвия – 01 июля 2015 г. Сертификат соответствия ФСБ России № СФ/114-1466. Срок действия – 09 мая 2013 г.

Физические меры защиты

Вход в здание, расположенное по адресу: 652300, Кемеровская обл., г. Топки, ул. Топкинская, д. 4, осуществляется через контрольно-пропускной пункт. Единый порядок организации пропускного и внутриобъектового режимов определен Приказом от «28» октября 2016 г. № 486 «Об организации охраны, пропускного, внутриобъектового режимов работы в здании и на территории У О АТМР». Вход в помещения, в которых расположены технические средства ИСПДн, ограничены дверьми с замками. Доступ в помещения имеют только уполномоченные сотрудники Оператора. В помещениях здания работают дежурные, сторожа.

Доступ сотрудников Оператора, не допущенных к обработке ПДн в помещения, в которых расположены технические средства ИСПДн, осуществляется в присутствии лиц, работающих в этих помещениях. Для предотвращения неконтролируемого проникновения посторонних лиц в служебные помещения сотрудники в рабочее время, покидая служебные помещения, входные двери закрывают на замок. По окончании рабочего дня двери помещений закрываются на замок, ключи сдаются дежурному, сторожу.

Документы на бумажных носителях хранятся в металлическом сейфе и закрытых металлических шкафах. Окна в помещениях, в которых производится обработка ПДн, оборудованы жалюзи. Размещение мониторов рабочих мест пользователей частично исключает просмотр выводимой информации.

Серверная комната расположена на первом этаже трёхэтажного здания по адресу: 652300, Кемеровская обл., г. Топки, ул. Топкинская, д. 4. На окне нет решетки. Установлена деревянная дверь с замком. Двери не опечатываются. Сигнализирующие устройства не установлены. Список лиц, имеющих право доступа в серверную комнату утвержден и размещен в помещении. Порядок доступа в серверную и правила поведения

персонала внештатных ситуациях утвержден.

Организационные меры защиты

Оператором приняты следующие правовые, организационные и технические меры по обеспечению безопасности ПДн при их обработке в ИСПДн в соответствии с [2] и требованиями к защите ПДн установленными Правительством Российской Федерации:

1. Разработаны документы, определяющие политику Оператора в отношении обработки ПДн, локальные акты по вопросам обработки ПДн, а также локальные акты, устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;
2. Разработана частная модель угроз, в которой определены угрозы безопасности ПДн при их обработке в ИСПДн «УО АТМР»;
3. Частично применяются прошедшие в установленном порядке процедуру оценки соответствия СЗИ;
4. Назначено ответственное лицо за организацию обработки ПДн;
5. Назначено должностное лицо (работник), ответственное за обеспечение безопасности ПДн в ИС;
6. Назначено должностное лицо (работник), ответственное за обеспечение криптографической защиты ПДн;
7. Обеспечивается восстановление ПДн, модифицированных или уничтоженных вследствие НСД к ним;
8. Обработка ПДн без использования средств автоматизации осуществляется в соответствии с требованиями [7];
9. Работники, непосредственно осуществляющие обработку ПДн, ознакамливаются с положениями законодательства Российской Федерации о ПДн, в том числе с требованиями к защите ПДн, документами, определяющими политику Оператора в отношении обработки ПДн, локальными актами по вопросам обработки ПДн;
10. Разработаны правила доступа к ПДн, обрабатываемым в ИСПДн «УО АТМР», а также обеспечивается регистрация и учет всех действий, совершаемых с ПДн в ИСПДн;
11. Проведена оценка эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию ИСПДн «УО АТМР» и ИСПДн «УО АТМР»;
12. Осуществляется внутренний контроль и аудит за соответствием обработки ПДн требованиям [2] и принятым в соответствии с ним нормативными правовыми актами, требованиям к защите ПДн, политике Оператора в отношении обработки ПДн, локальным актам Оператора;
13. Проведена оценка вреда, который может быть причинен субъектам ПДн в случае нарушения [2]. Проведено соотношение указанного вреда и принимаемыми мерами, направленными на обеспечение выполнения обязанностей, предусмотренных законодательством;
14. Осуществляется контроль за принимаемыми мерами по обеспечению безопасности ПДн при их обработке в ИСПДн «УО АТМР»;

15. Осуществляется реагирование на инциденты по информационной безопасности.

Оператором не приняты следующие правовые, организационные и технические меры по обеспечению безопасности ПДн при их обработке в ИСПДн в соответствии с [2] и требованиями к защите ПДн установленными Правительством Российской Федерации:

1. Не осуществляется контроль за обнаружением фактов НСД к ПДн;
2. Не применяется межсетевое экранирование сегмента ИСПДн «УО АТМР» от ИСПДн других операторов (подведомственных учреждений);
3. Выход в сеть интернет осуществляется через несертифицированный ФСТЭК России МЭ;
4. Не опубликован документ, определяющий политику Оператора в отношении обработки ПДн на Интернет-странице организации;
5. Не на всех АРМ и сервере используются необходимые сертифицированные СЗИ, согласно требованиям законодательства; [11]
6. Оператором используются СЗИ и СКЗИ с истекшими сертификатами соответствия ФСТЭК и ФСБ России;
7. Не во всех помещениях, в которых используются СКЗИ, выполняются установленные законодательством требования; [12]
8. Оператором не проводилась оценка эффективности реализованных в рамках СЗПДн мер по обеспечению безопасности ПДн; [5],[12]
9. В Уведомление, отправляемое уполномоченному органу по защите прав субъектов ПДн, не внесены все сведения предусмотренные статьей 22 [2].
10. Между Оператором и подведомственными учреждениями не разработано соглашение о совместном использовании ИС, СЗИ, информационном обмене и выходе в сеть интернет. [2]

3. МОДЕЛЬ НАРУШИТЕЛЯ БЕЗОПАСНОСТИ ПДн

3.1 Общие положения

Нарушителями безопасности ПДн являются физические лица, которые преднамеренно или случайно совершают действия, в результате которых нарушаются заданные характеристики безопасности ПДн.

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

- внешние нарушители (не имеющие права пребывания на территории КЗ, в пределах которой размещается оборудование ИСПДн);
- внутренние нарушители (имеющие право пребывания на территории КЗ, в пределах которой размещается оборудование ИСПДн).

3.2 Внешний нарушитель Общие положения

Внешние нарушители - это нарушители, не имеющие доступа к ИСПДн, реализующие угрозы из внешних сетей связи общего пользования и сетей международного информационного обмена. Нарушителями этого типа могут являться:

- криминальные структуры;
- недобросовестные партнеры;
- внешние субъекты (физические лица).

Внешний нарушитель имеет следующие возможности:

- осуществлять НСД к каналам связи, выходящим за пределы служебных помещений;
- осуществлять НСД к информации с использованием специальных программных воздействий посредством программы вирусов, вредоносных программ, алгоритмических или программных закладок;
- осуществлять НСД через элементы информационной инфраструктуры ИСПДн, которые в процессе своего жизненного цикла (модернизация, сопровождение, ремонт, утилизация) оказываются за пределами КЗ;
- осуществлять НСД через ИС взаимодействующих ведомств, организаций и учреждений при подключении к ИСПДн;
- осуществлять сговор с работниками Оператора, которые согласились или оказались вынужденными осуществлять действия по хищению, скрытому копированию, уничтожению ПДн;
- осуществлять перехват информации за счет ПЭМИН;
- осуществлять добывание информации посредством социальной инженерии.

3.3 Внутренний нарушитель.

Общие положения

Внутренними нарушителями являются лица, имеющие доступ к ИСПДн, включая пользователей ИСПДн, реализующих угрозы непосредственно в ИСПДн.

Возможности внутреннего нарушителя существенным образом зависят от действующих в пределах КЗ режимных и организационно-технических мер защиты, в том числе от установленного порядка допуска физических лиц к информационным ресурсам ИСПДн и мер по контролю порядка проведения работ. Внутренние потенциальные нарушители подразделяются на восемь категорий в зависимости от способа доступа и полномочий доступа к ПДн [9].

Первая категория

К первой категории относятся лица, имеющие санкционированный доступ к ИСПДн, но не имеющие доступа к ПДн. К этому типу нарушителей относятся должностные лица, обеспечивающие нормальное функционирование ИСПДн. Лицо этой категории может:

- Иметь доступ к фрагментам информации, содержащей ПДн и распространяющейся по внутренним каналам связи ИСПДн;
- Располагать фрагментами информации о топологии ИСПДн (коммуникационной части подсети) и об используемых коммуникационных протоколах и их сервисах;
- располагать именами и вести выявление паролей зарегистрированных пользователей;
- изменять конфигурацию технических средств ИСПДн, вносить в нее программно-аппаратные закладки и обеспечивать съем информации, используя непосредственное подключение к техническим средствам ИСПДн [9].

Вторая категория

Ко второй категории относятся зарегистрированные пользователи ИСПДн, осуществляющие ограниченный доступ к ресурсам ИСПДн с рабочего места. Лицо этой категории:

- обладает всеми возможностями лиц первой категории;
- знает по меньшей мере одно легальное имя доступа;
- обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству ПДн;
- располагает конфиденциальными данными, к которым имеет доступ

[9]. **Третья категория**

К третьей категории относятся зарегистрированные пользователи ИСПДн, осуществляющие удаленный доступ к ПДн по локальным и (или)

распределенным информационным системам. Лицо этой категории:

- обладает всеми возможностями лиц первой и второй категорий;
- располагает информацией о топологии ИСПДн на базе локальной и (или) распределенной информационной системе, через которую он осуществляет доступ, и составе технических средств ИСПДн;
- имеет возможность прямого (физического) доступа к фрагментам технических средств ИСПДн [9].

Четвертая категория

К четвертой категории относятся зарегистрированные пользователи ИСПДн с полномочиями администратора безопасности сегмента (фрагмента) ИСПДн. Лицо этой категории:

- обладает всеми возможностями лиц предыдущих категорий;
- обладает полной информацией о системном и прикладном ПО, используемом в сегменте (фрагменте) ИСПДн;
- обладает полной информацией о технических средствах и конфигурации сегмента (фрагмента) ИСПДн;
- имеет доступ к СЗИ и протоколирования, а также к отдельным элементам, используемым в сегменте (фрагменте) ИСПДн;
- имеет доступ ко всем техническим средствам сегмента (фрагмента) ИСПДн;
- обладает правами конфигурирования и административной настройки некоторого подмножества технических средств сегмента (фрагмента) ИСПДн[9].

Пятая категория

К пятой категории относятся зарегистрированные пользователи с полномочиями системного администратора ИСПДн. Лицо этой категории:

- обладает всеми возможностями лиц предыдущих категорий;
- обладает полной информацией о системном и прикладном ПО ИСПДн;
- обладает полной информацией о технических средствах и конфигурации ИСПДн;
- имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн;
- обладает правами конфигурирования и административной настройки технических средств ИСПДн.

Системный администратор выполняет конфигурирование и управление ПО и оборудованием, включая оборудование, отвечающее за безопасность защищаемого объекта: СКЗИ, мониторинга, регистрации, архивации, защиты от НСД [9].

Шестая категория

К шестой категории относятся зарегистрированные пользователи с полномочиями администратора безопасности ИСПДн. Лицо этой категории:

- обладает всеми возможностями лиц предыдущих категорий;
- обладает полной информацией об ИСПДн;
- имеет доступ к СЗИ и протоколирования и к части ключевых элементов ИСПДн;
- не имеет прав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных).

Администратор безопасности отвечает за соблюдение правил разграничения доступа, за генерацию ключевых элементов, смену паролей. Администратор безопасности осуществляет аудит тех же средств защиты объекта, что и системный администратор [9].

Седьмая категория

К седьмой категории относятся программисты-разработчики (поставщики) ППО и лица, обеспечивающие его сопровождение на защищаемом объекте. Лицо этой категории:

- обладает информацией об алгоритмах и программах обработки информации на ИСПДн;
- обладает возможностями внесения ошибок, недекларированных возможностей, программных закладок, вредоносных программ в ПО ИСПДн на стадии ее разработки, внедрения и сопровождения;
- может располагать любыми фрагментами информации о топологии ИСПДн и технических средствах обработки и защиты ПДн, обрабатываемых в ИСПДн [9].

Восьмая категория

К восьмой категории относятся разработчики и лица, обеспечивающие поставку, сопровождение и ремонт технических средств в ИСПДн. Лицо этой категории:

- обладает возможностями внесения закладок в технические средства ИСПДн на стадии их разработки, внедрения и сопровождения;
- может располагать любыми фрагментами информации о топологии ИСПДн и технических средствах обработки и защиты информации в ИСПДн [9].

3.4 Предположения о возможностях нарушителя

Лица, рассматриваемые в качестве потенциальных нарушителей для ИСПДн «УО АТМР», представлены в таблице 3.1.

Таблица 3.1. - Потенциальные нарушители

№ п/п	Субъект	Характеристика	Категория	Условное обозначение
1	Внешние нарушители	Внешний	-	-
2	Операторы ПДн (легальные пользователи)	Внутренний	2	ПН2
3	Администратор безопасности	Внутренний	6	ПН6
4	Технические специалисты по обслуживанию оборудования	Внутренний	8	ПН8

Внешние нарушители могут осуществлять попытки НСД к ИСПДн «УО АТМР» через каналы связи, выходящие за пределы КЗ, и через элементы информационной инфраструктуры ИСПДн «УО АТМР», которые в процессе жизненного цикла могут оказаться за пределами КЗ. Внешние нарушители относятся к числу потенциальных нарушителей.

Возможности внутреннего нарушителя существенным образом зависят от действующих в пределах КЗ режимных и организационно-технических мер защиты.

Исходя из особенностей функционирования ИСПДн «У О АТМР», допущенные к ней работники имеют разные полномочия на доступ к информационным, программным, аппаратным и другим ресурсам ИСПДн «УО АТМР».

При получении доступа к ИСПДн «УО АТМР» лица ПН2 в обязательном порядке изучают инструкции, регламентирующие порядок работ и требования по обеспечению безопасности ПДн и подписывают соглашение о конфиденциальности. Пользователи ИСПДн «УО АТМР» должны проходить инструктаж по работе в ИСПДн «УО АТМР» и предупреждаться об ответственности за нарушение правил работы в ИСПДн «УО АТМР». Указанные меры являются необходимыми, но их следует признать недостаточными, и лиц ПН2 следует отнести к числу потенциальных нарушителей.

На лицо ПН6 возложены задачи:

- по конфигурированию и управлению ПО и оборудованием, включая оборудование, отвечающее за безопасность защищаемого объекта: СКЗИ, мониторинга, регистрации, архивации, защиты от НСД.

- по соблюдению правил разграничения доступа, по генерации ключевых элементов, по смене паролей.

Лицо ПН6 потенциально может реализовывать угрозы безопасности ПДн, используя возможности по непосредственному доступу к защищаемой
информации, обрабатываемой в ИСПДн «УО АТМР», а также к техническим

и программным средствам ИСПДн «УО АТМР», включая СЗИ, в соответствии с установленными для него административными полномочиями. Лицо ПН6 хорошо ознакомлен с основными алгоритмами, протоколами, реализуемыми и используемыми в конкретных подсистемах и ИСПДн «УО АТМР» в целом, а также с применяемыми принципами и концепциями безопасности.

К лицу ПН6 ввиду его исключительной роли в ИСПДн «УО АТМР» должен применяться комплекс особых организационных мер по подбору, принятию на работу, назначению на должность, обучению и контролю выполнения функциональных обязанностей. Также данное лицо в обязательном порядке должно проходить инструктаж, предупреждаться об ответственности за нарушение правил работы в ИСПДн «УО АТМР» и подписывать соглашение о конфиденциальности. Назначение на данные должности случайных лиц должно быть исключено проведением кадровых мероприятий.

Предполагается, что лицо ПН6 владеет в той или иной части чувствительной и эксплуатационной информацией о системе передачи данных и общей информацией об ИСПДн «УО АТМР», использующей эту систему передачи данных, что обеспечивается организационными мерами. При этом лицо ПН6 владеет парольной и аутентифицирующей информацией, используемой в ИСПДн «УО АТМР».

С учетом сказанного предполагается, что в число лиц ПН6 будут включаться только доверенные лица, поэтому указанная категория лиц исключаются из числа потенциальных нарушителей.

Лица ПН8 в рамках выполнения своих должностных обязанностей могут иметь физический доступ к техническим средствам ИСПДн «УО АТМР», к фрагментам ПДн на бумажных носителях, к носителям информации, к информационным и программным ресурсам ИСПДн «УО АТМР». В связи с этим обслуживание компонентов ИСПДн «УО АТМР» и помещений, в которых они расположены, должно производиться в присутствии штатных работников. Указанные меры являются необходимыми, но их следует признать недостаточными, и лиц ПН8 следует отнести к числу потенциальных нарушителей.

Степень информированности нарушителя зависит от многих факторов, включая реализованные у Оператора 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 системы защиты, 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.

4. МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ПДн

4.1 Общие положения

ИСПДн «УО АТМР» представляет собой ЛВС, имеющую подключение к сетям связи общего пользования и (или) сетям международного информационного обмена.

В ИСПДн, имеющей такую структуру, рассматриваются следующие угрозы безопасности ПДн [9]:

1. Угрозы утечки информации по техническим каналам:

- угрозы утечки акустической (речевой) информации;
- угрозы утечки видовой информации;
- угрозы утечки информации по каналу ПЭМИН.

2. Угрозы несанкционированного доступа:

- Угрозы НСД связаны с действиями нарушителей, имеющих доступ к ИСПДн, включая пользователей ИСПДн, реализующих угрозы непосредственно в ИСПДн, а также нарушителей, не имеющих доступа к ИСПДн, реализующих угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена.

4.2 Угрозы утечки информации по техническим каналам

Угрозы утечки акустической (речевой) информации

Реализация угроз утечки акустической (речевой) информации, содержащейся непосредственно в произносимой речи пользователей ИСПДн, при обработке ПДн в ИСПДн, может быть обусловлено наличием следующих функций:

- функции голосового ввода ПДн в ИСПДн;
- функций воспроизведения ПДн акустическими средствами ИСПДн.

Возникновение угрозы утечки акустической (речевой) информации не представляется возможным в связи с отсутствием функций по обработке данного вида информации в рассматриваемой ИСПДн.

Вероятность реализации угрозы - **маловероятна.**

Угрозы утечки видовой информации

Реализация угроз утечки видовой информации возможна за счет просмотра ПДн с помощью оптических (оптикоэлектронных) средств с экранов дисплеев при осуществлении обработки ПДн в ИСПДн «УО АТМР».

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

В организации введен контроль доступа в КЗ, АРМ пользователей

расположены так, что частично исключен визуальный доступ посторонних лиц к мониторам, на окнах установлены жалюзи.

Вероятность реализации угрозы - **низкая.**

Угрозы утечки информации по каналам ПЭМИН

Реализация угроз возможна за счет перехвата техническими средствами (не связанными с прямым функциональным назначением элементов ИСПДн) побочных информативных электромагнитных полей и электрических сигналов, возникающих при обработке ПД техническими средствами ИСПДн.

Угрозы утечки информации по каналу ПЭМИН, возможны из-за наличия электромагнитных излучений, в основном, мониторов и системных блоков АРМ.

Носителями ПДн могут быть источники информации обрабатываемой в ИСПДн:

- СВТ (рабочие станции);
- устройства электропитания;
- устройства заземления;
- устройства сетевого оборудования;
- линии передачи данных.

Средой распространения ПДн является электромагнитное поле:

- электромагнитные излучения СВТ из состава ОТСС и ВТСС;
- ЭМИ, создаваемые линиями связи и каналами передачи данных;
- электрические сигналы, наведенные от ЭМИ в линиях системы электропитания;
- электрические сигналы, наведенные от ЭМИ в линиях системы заземления.

Источниками УБПДн могут быть:

- средства перехвата сигналов ПЭМИН;
- средства съема сигналов с проводных линий;
- закладочные устройства обнаружения и перехвата сигналов, содержащих защищаемую информацию;
- средства перехвата информации в каналах передачи данных.

Предполагается, что объем и состав обрабатываемой и хранимой в ИСПДн «УО АТМР» информации не является достаточным для возможной мотивации внешних нарушителей к осуществлению действий, направленных на утечку информации по каналам ПЭМИН. Предполагается, что возможность сговора внешних нарушителей между собой маловероятна.

Стоимость реализации угрозы, выраженная в стоимости специального

оборудования и его эксплуатации, представляется значительной, при этом выявление информативной составляющей в условиях эксплуатации оборудования в пределах КЗ энергонасыщенного здания маловероятно.

Для исключения утечки ПДн за счет ПЭМИН в ИСПДн реализуются следующие мероприятия:

- все технические средства ИСПДн находятся в одном здании;
- доступ в помещение, в котором ведется обработка ПДн, находятся под охраной;
- аппаратные средства ИСПДн «УО АТМР» заземлены;
- применяются жидкокристаллические мониторы.

Так как технические (аппаратные) средства ИСПДн, используемые для обработки ПДн, соответствуют требованиям стандартов Российской Федерации по электромагнитной совместимости, безопасности и санитарным нормам, вероятность реализации угроз утечки информации по каналу ПЭМИН минимальна.

Вероятность реализации угрозы - **маловероятна.**

4.3 Угрозы несанкционированного доступа к информации

Угрозы доступа (проникновения) в операционную среду компьютера с использованием штатного ПО (средств ОС или прикладных программ общего применения) Угрозы, реализуемые в ходе загрузки ОС

Эти угрозы безопасности информации направлены на перехват, подбор паролей или идентификаторов, модификацию ПО базовой системы ввода-вывода (ВЮ8), перехват управления загрузкой с изменением необходимой технологической информации для получения НСД в ОС ИСПДн.

Так как в ИСПДн «УО АТМР» не на всех АРМ установлены сертифицированные ФСТЭК России СЗИ от НСД, вероятность реализации угрозы нужно признать **высокой.**

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

Эти угрозы, как правило, направлены на выполнение непосредственно НСД к информации. При получении доступа в ОС нарушитель может воспользоваться как стандартными функциями ОС или какой-либо прикладной программы общего пользования (например, системы управления БД), так и специально созданными для выполнения НСД программами, например:

- программами просмотра и модификации реестра;
- программами поиска текстов в текстовых файлах по ключевым словам и копирования;

- специальными программами просмотра и копирования записей в базах данных;
- программами быстрого просмотра графических файлов, их редактирования или копирования;
- программами поддержки возможностей реконфигурации программной среды (настройки ИСПДн в интересах нарушителя) и др.

Так как в ИСПДн «УО АТМР» не на всех АРМ установлены сертифицированные ФСТЭК России СЗИ от НСД, вероятность реализации угрозы нужно признать **высокой.**

Угрозы, реализация которых определяется тем, какая из прикладных программ запускается пользователем, или фактом запуска любой из прикладных программ (угрозы внедрения вредоносных программ)

Большая часть таких угроз - это угрозы внедрения вредоносных программ.

Так как в ИСПДн «УО АТМР» используется антивирусное ПО, установка ПО, не предназначенного для выполнения функциональных задач пользователей, запрещена, вероятность реализации угрозы нужно признать **низкой.**

Угрозы «Анализа сетевого трафика» с перехватом передаваемой во внешние сети и принимаемой из внешних сетей информации

Угроза реализуется с помощью программы-анализатора пакетов (sniffer), перехватывающей все пакеты, передаваемые по сегменту сети, и выделяющей среди них те, в которых передаются идентификатор пользователя и его пароль.

Цель - Исследование характеристик сетевого трафика, перехват передаваемых данных, в том числе идентификаторов и паролей пользователей.

Для исключения возможности реализации угрозы «Анализа сетевого трафика» ИСПДн «УО АТМР» должна подключаться к сетям общего пользования и международного информационного обмена (Интернет) через МЭ, прошедший в установленном порядке процедуру оценки соответствия. Для удаленного доступа к ресурсам ИСПДн должны использоваться средства криптозащиты, обеспечивающие шифрование передаваемого в сеть Интернет трафика.

Так как в ИСПДн «УО АТМР» не установлен сертифицированный ФСТЭК России МЭ, вероятность реализации угрозы признается **высокой.**

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.

Источником угроз «Сканирование сети» могут быть внешние нарушители (физические лица), не имеющие доступа к ИСПДн «УО

АТМР», реализующие свои угрозы из сети Интернет.

Для исключения возможности реализации угрозы «Сканирование сети» ИСПДн «УО АТМР» должна подключаться к сетям общего пользования и международного информационного обмена (Интернет) через МЭ, прошедший в установленном порядке процедуру оценки соответствия.

Так как в ИСПДн «УО АТМР» не установлен сертифицированный ФСТЭК России МЭ, вероятность реализации угрозы признается **высокой.**

Угрозы выявления паролей

Источником являются внешние нарушители, пользователи других ИС, не имеющие доступа к ПДн, работники, производящие обслуживание помещений.

Угроза может быть реализована с помощью следующих методов:

- простой перебор паролей;
- перебор с использованием специальных словарей;
- внедрение вредоносной программы для перехвата паролей;
- перехват пакетов (sniffer).

Деструктивные действия - создание условий для получения прямого доступа к файлам, содержащим ПДн.

Так как в ИСПДн «УО АТМР» осуществляется регулярная смена паролей, обслуживание помещений всегда осуществляется в присутствии лиц, работающих в этих помещениях, вероятность реализации угрозы нужно признать **низкой.**

Угрозы получения НСД путем подмены доверенного объекта

Источником являются внешние нарушители, пользователи ИС, не имеющие доступа к ПДн, работники, производящие обслуживание помещений.

Угрозы реализуются в системах, в которых применяются нестойкие алгоритмы идентификации и аутентификации хостов, пользователей и т.д. Под доверенным объектом понимается объект сети (компьютер, МЭ, маршрутизатор и т.п.), легально подключенный к серверу. Реализуются передачей по каналам связи сообщений от имени легального пользователя (субъекта доступа) с присвоением его прав доступа.

Процесс реализации с установлением виртуального соединения состоит в преодолении системы аутентификации сообщений и присвоении прав доверенного субъекта взаимодействия, что позволяет нарушителю вести сеанс работы с объектом сети от имени доверенного субъекта.

Процесс реализации угрозы без установления виртуального соединения заключается в передаче служебных сообщений от имени сетевых управляющих устройств об изменении маршрутно-адресных данных и может иметь место в сетях, осуществляющих идентификацию

передаваемых сообщения только по сетевому адресу отправителя.

Деструктивные действия - нарушение конфиденциальности информации путем несанкционированного ознакомления с пакетами, предназначенными для доверенного субъекта.

Так как в ИСПДн «УО АТМР» не установлен сертифицированный ФСТЭК России МЭ, вероятность реализации угрозы признается **высокой.**

Угрозы типа «Отказ в обслуживании»

Реализация обусловлена тем, что при разработке системного или прикладного ПО не учитывается возможность преднамеренных действий по целенаправленному изменению:

- содержания служебной информации в пакетах сообщений, передаваемых по сети;
- условий обработки данных (например, игнорирование ограничений на длину пакета сообщения);
- форматов представления данных (с несоответствием измененных форматов установленных для обработки по протоколам сетевого взаимодействия);
- ПО обработки данных.

В результате реализации угроз «Отказа в обслуживании» происходит переполнение буферов и блокирование процедур обработки, «зацикливание» процедур обработки и «зависание» компьютера, отбрасывание пакетов сообщений и др.

Так как в ИСПДн «УО АТМР» не установлен сертифицированный ФСТЭК России МЭ, вероятность реализации угрозы признается **высокой.**

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.

Угрозы удаленного запуска приложений. Распространение файлов, содержащих несанкционированный исполняемый код

Угрозы основываются на активизации распространяемых файлов при случайном обращении к ним. Примерами таких файлов могут служить: файлы, содержащие исполняемый код в виде макрокоманд (документы Mickrosoft Word, Excel и т.п.); html-документы, содержащие исполняемый код в виде элементов AktiveX, jaya-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.

Угрозы удаленного запуска приложений путем переполнения буфера приложений

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.

Угрозы удаленного запуска приложений путем использования возможностей удаленного управления системой, предоставляемых скрытыми программными и аппаратными закладками, либо используемыми штатными средствами

Нарушитель использует возможности удаленного управления системой, предоставляемые скрытыми компонентами, либо штатными средствами управления и администрирования компьютерных сетей. В результате удается добиться удаленного контроля над станцией в сети.

Так как в ИСПДн «УО АТМР» используется антивирусное ПО, установка ПО, не предназначенного для выполнения функциональных задач пользователей, запрещена, вероятность реализации угрозы нужно признать **низкой.**

Угрозы внедрения вредоносных программ по сети

Современные вредоносные программы основаны на использовании уязвимостей различного рода ПО (системного, общего, прикладного) и разнообразных сетевых технологий, обладают широким спектром возможностей (от несанкционированного исследования параметров ИСПДн без вмешательства в функционирование ИСПДн, до уничтожения ПДн и ПО ИСПДн) и могут действовать во всех видах ПО (системного, прикладного, в драйверах аппаратного обеспечения и т.д.).

Основными видами вредоносных программ являются:

- программные закладки;
- классические программные (компьютерные) вирусы;
- вредоносные программы, распространяющиеся по сети (сетевые черви);
- другие вредоносные программы, предназначенные для осуществления НСД.

Вредоносные программы (программы математического воздействия) могут быть внедрены вместе с данными, передаваемыми с АРМ пользователей как преднамеренно, так и случайно.

В данном случае источниками угроз могут являться вредоносные программы, распространяющиеся по сети (сетевые черви).

Так как в ИСПДн «УО АТМР» используется антивирусное ПО, установка ПО, не предназначенного для выполнения функциональных задач пользователей, запрещена, вероятность реализации угрозы нужно признать **низкой.**

4.4 Перечень УБПДн

Таблица 4.1 - Перечень угроз безопасности ПДн в ИСПДн «УО АТМР»

1. Угрозы утечки информации по техническим каналам.
1.1.Угрозы утечки акустической (речевой) информации
1.2.Угрозы утечки видовой информации
1.3.Угрозы утечки информации по каналу ПЭМИН
2. Угрозы НСД к информации в ИСПДн.
2.1. У грозы доступа (проникновения) в ОС компьютера с использованием штатного ПО (средств ОС или прикладных программ общего применения)
2.1.1. Угрозы непосредственного доступа.
2.1.1.1. Угрозы, реализуемые в ходе загрузки ОС.
2.1.1.2. Угрозы, реализуемые после загрузки операционной среды.
2.1.1.3. Угрозы внедрения вредоносных программ.
2.1.2. Угрозы из внешних сетей.
2.1.2.1. Анализ сетевого трафика.
2.1.2.2. Сканирование сети.
2.1.2.3. Выявления паролей.
2.1.2.4. Получения НСД путем подмены доверенного объекта.
2.1.2.5. «Отказ в обслуживании».
2.1.2.6. Удаленный запуск приложений.
2.2. Угрозы внедрения вредоносных программ по сети.

5. ОПРЕДЕЛЕНИЕ АКТУАЛЬНЫХ УГРОЗ

5.1 Уровень исходной защищенности

Описание структуры рассматриваемой ИСПДн приведено в разделе 2.2 настоящего документа.

При определении уровня исходной защищенности ИСПДн используются следующие технические и эксплуатационные характеристики:

Таблица 5.1 - Технические и эксплуатационные характеристики ИСПДн

Технические и эксплуатационные характеристики ИСПДн «УО АТМР»	Уровень защищенности		
	Высокий	Средний	Низкий
По территориальному размещению			
распределенная ИСПДн, которая охватывает несколько областей, краев, округов или государство в целом			
городская ИСПДн, охватывающая не более одного населенного пункта (города, поселка)			
корпоративная распределенная ИСПДн, охватывающая многие подразделения одной организации			
локальная (кампусная) ИСПДн, развернутая в пределах нескольких близко расположенных зданий			
локальная ИСПДн, развернутая в пределах одного здания	+		
По наличию соединения с сетями общего пользования			
ИСПДн, имеющая многоточечный выход в сеть общего пользования			
ИСПДн, имеющая одноточечный выход в сеть общего пользования		+	
ИСПДн, физически отделенная от сети общего пользования			
По встроенным (легальным) операциям с записями баз персональных данных			
чтение, поиск			
запись, удаление, сортировка			
модификация, передача			+
По разграничению доступа к персональным данным			

Технические и эксплуатационные характеристики ИСПДн «УО АТМР»	Уровень защищенности		
	Высокий	Средний	Низкий
ИСПДн, к которой имеет доступ определенный перечень сотрудников организации, являющейся владельцем ИСПДн, либо субъект ПДн		+	
ИСПДн, к которой имеют доступ все сотрудники организации, являющейся владельцем ИСПДн			
ИСПДн с открытым доступом			
По наличию соединений с другими базами ПДн иных ИСПДн			
Интегрированная ИСПДн (организация использует несколько баз ПДн ИСПДн, при этом организация не является владельцем всех используемых баз ПДн)			
ИСПДн, в которой используется одна база ПДн, принадлежащая организации - владельцу данной ИСПДн	+		
По уровню обобщения (обезличивания) ПДн			
ИСПДн, в которой предоставляемые пользователю данные являются обезличенными (на уровне организации, отрасли, области, региона и т.д.)			
ИСПДн, в которой данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в организации			
ИСПДн, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта ПДн)			+
По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки			
ИСПДн, предоставляющая всю БД с ПДн			
ИСПДн, предоставляющая часть ПДн		+	
ИСПДн, не предоставляющие никакой информации			
Количество решений	2	3	2
Общее количество решений	7		

ИСПДн «УО АТМР» имеет средний уровень исходной защищенности с коэффициентом Y 1=5.

5.2 Определение актуальных угроз

Определение актуальных угроз произведено в соответствии с «Методикой определения актуальных угроз».

Таблица 5.2 - Определение актуальных угроз

Наименование угрозы	Y_2	Y	Реализу-емость	Опас-ность	Актуальность
Угрозы утечки информации по техническим каналам					
Угрозы утечки акустической информации	0	0,25	Низкая	Средняя	Неактуальная
Угрозы утечки видовой информации	2	0,35	Средняя	Средняя	Актуальная
Угрозы утечки информации по каналу ПЭМИН	0	0,25	Низкая	Средняя	Неактуальная
Угрозы НСД к информации в ИСПДн					
Угрозы непосредственного доступа					
Угрозы, реализуемые в ходе загрузки ОС	10	0,75	Высокая	Высокая	Актуальная
Угрозы, реализуемые после загрузки операционной среды	10	0,75	Высокая	Высокая	Актуальная
Угрозы внедрения вредоносных программ	2	0,35	Средняя	Высокая	Актуальная
Угрозы удаленного доступа					
Анализ сетевого трафика	10	0,75	Высокая	Высокая	Актуальная
Сканирование сети	10	0,75	Высокая	Высокая	Актуальная
Угрозы выявления пароля	2	0,35	Средняя	Высокая	Актуальная
Угрозы получения НСД путем подмены доверенного объекта	10	0,75	Высокая	Высокая	Актуальная
Угрозы типа «Отказ в обслуживании»	10	0,75	Высокая	Высокая	Актуальная
Угрозы удаленного запуска приложений	2	0,35	Средняя	Высокая	Актуальная
Угрозы внедрения по сети вредоносных программ	2	0,35	Средняя	Высокая	Актуальная

6. ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ 6.1 Общие требования по обеспечению безопасности

1. Для обеспечения 3-го уровня защищенности ПДн при их обработке в ИСПДн «УО АТМР» необходимо выполнение следующих требований: [5]

- организация режима обеспечения безопасности помещений, в которых размещена ИСПДн «УО АТМР», препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;
- должен быть определен порядок использования внешних сменных накопителей, вестись журнал учета сменных накопителей. Должно быть запрещено использование любых несанкционированных внешних накопителей;
- утверждение руководителем Оператора документа, определяющего перечень лиц, доступ которых к ПДн, обрабатываемым в ИСПДн «УО АТМР», необходим для выполнения ими служебных (трудовых) обязанностей;
- использование СЗИ, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз;
- эксплуатация ИСПДн «УО АТМР» должна осуществляться в полном соответствии с утвержденной организационно-технической и эксплуатационной документацией с учетом требований и положений, изложенных в настоящем документе;
- все технические средства ИСПДн «УО АТМР» должны находиться в пределах КЗ;
- должна быть определена матрица доступа или полномочий субъектов доступа по отношению к защищаемым информационным ресурсам;
- должно быть назначено должностное лицо (работник), ответственное за обеспечение безопасности ПДн в ИС.

2. Мероприятия по обеспечению безопасности ПДн должны быть отражены в инструкциях или других утвержденных документах, определяющих:

- порядок изменения состава и конфигурации технических и программных средств;
- порядок допуска пользователей к ИСПДн «УО АТМР»;
- порядок применения СЗИ от НСД;
- обязанности и ответственность администраторов безопасности;
- порядок контроля за выполнением мероприятий по обеспечению защиты информации.

3. Должен быть определен порядок обработки ПДн в ИСПДн «УО АТМР».

6.2 Требования к межсетевому экранированию

1. Должно применяться межсетевое экранирование сегмента ИСПДн «УО АТМР». Должен применяться МЭ, сертифицированный ФСТЭК России, соответствующий требованиям по уровню защищенности не ниже 3 класса. [11]

2. При передаче данных ИСПДн «УО АТМР» через сеть Интернет должны использоваться сертифицированные в установленном порядке алгоритмы шифрования.

3. Должен быть сформирован и утвержден перечень ресурсов и сетевых служб, к которым разрешен доступ пользователям ИСПДн «УО АТМР».

4. Должен осуществляться периодический анализ правил безопасности, установленных на МЭ, на основе имитации внешних атак на ИСПДн «УО АТМР» при помощи систем анализа защищённости.

6.3 Требования к защите от ПМВ

Для обеспечения защиты информационных ресурсов ИСПДн «УО АТМР» от ПМВ должны применяться средства антивирусной защиты не ниже 4 класса.
[Н]

6.4 Требования по защите от НСД к информации

ИСПДн «УО АТМР» должна соответствовать требованиям по защите информации от НСД к ИСПДн 3-го уровня защищенности с учётом следующих требований:

1. Должно быть запрещено использование любых внешних сменных накопителей, кроме допущенных в установленном порядке к использованию в системе;

2. Должно быть запрещено использование всех сетевых интерфейсов, кроме рабочего интерфейса Ethernet, которые могут использоваться для несанкционированного подключения проводных и беспроводных сетевых устройств (WiFi, Bluetooth, инфракрасные передатчики);

3. Для исключения возможности недоверенной загрузки должна быть запрещена загрузка с любых других накопителей, кроме жесткого диска;

4. Должны учитываться требования нормативных документов по уровню сложности используемых паролей;

5. Пользователи ИСПДн «УО АТМР» не должны иметь каких-либо административных полномочий на рабочих станциях ИСПДн;

6. Должно производиться опечатывание системных блоков;

7. Требуется использование специализированных программных или аппаратных СЗИ, настроенных в соответствии с требованиями для ИСПДн 3-го уровня защищенности.

6.5 Требования к используемым СКЗИ

В связи с тем, что для ИСПДн «УО АТМР» требуется обеспечение 3-го уровня защищенности ПДн, и актуальны угрозы 3-го типа, требуется использование СКЗИ класса КС1 и выше. [12]

6.6 Требования по защите информации от утечки по техническим каналам Требования по защите от утечки акустической (речевой) информации

В ИСПДн «УО АТМР» должны отсутствовать функции голосового ввода ПДн и (или) функции воспроизведения ПДн акустическими средствами.

Требования по защите от утечки видовой информации

Должно обеспечиваться исключение просмотра посторонними лицами текстовой и графической видовой информации, отображаемой устройствами отображения информации средств вычислительной техники, информационно-вычислительных комплексов, технических средств обработки графической, видео и буквенно-цифровой информации, входящих в состав ИСПДн «УО АТМР».

Требования по защите от утечки информации по каналам ПЭМИН

1. Система электропитания и заземления должна соответствовать требованиям «Правил устройства электроустановок (ПУЭ)».

2. Технические (аппаратные) средства ИСПДн «УО АТМР», применяемые для обработки ПДн, должны соответствовать требованиям стандартов РФ по электромагнитной совместимости, безопасности и санитарным нормам.

3. В ИСПДн «УО АТМР» должны применять СВТ не ниже 5 класса.

7. ЗАЩИТА ОТ УГРОЗ ПРИ ВЫПОЛНЕНИИ ТРЕБОВАНИЙ ПО БЕЗОПАСНОСТИ ПДн

Приведенная ниже таблица сопоставляет каждой актуальной угрозе (Таблица 5.2) определённые технические средства защиты и (или) организационные меры, обеспечивающие нейтрализацию угроз (Таблица 7.1).

Таблица 7.1 - Реализация мер защиты

Угроза	Реализация мер защиты (пункт раздела 6)
Угрозы утечки акустической информации	6.6
Угрозы утечки видовой информации	6.6
Угрозы утечки информации по каналу ПЭМИН	6.6
Угрозы, реализуемые в ходе загрузки ОС.	6.4
Угрозы, реализуемые после загрузки ОС.	6.4
Угрозы внедрения вредоносных программ.	6.3
Анализ сетевого трафика	6.2
Сканирование сети	6.2
Угрозы выявления пароля	6.1,6.3
Угрозы получения НСД путем подмены доверенного объекта	6.2
Угрозы типа «Отказ в обслуживании»	6.2
Угрозы удаленного запуска приложений	6.3
Угрозы внедрения по сети вредоносных программ	6.3

8. ЗАКЛЮЧЕНИЕ

С использованием составленного перечня актуальных угроз (Таблица 5.2) на основе [5], [11] и сформулированных организационно-технических требований (раздел 6) по защите ПДн при их обработке в ИСПДн «УО АТМР», должен осуществляться выбор программных и технических СЗИ, для использования при модернизации и эксплуатации СЗПДн ИСПДн «УО АТМР».

При выборе программных и технических СЗИ требуется использовать сертифицированные в установленном порядке СЗИ, согласно Приложению №1.

[11]