



МУНИЦИПАЛЬНОЕ КАЗЕННОЕ УЧРЕЖДЕНИЕ
«УПРАВЛЕНИЕ МУНИЦИПАЛЬНЫМ
ЖИЛИЩНЫМ ФОНДОМ ГОРОДА ПЕРМИ»

П Р И К А З

15.04.2022

№ 01-03-252/1

Об утверждении политики
информационной безопасности

В целях обеспечения защиты персональных данных муниципального казенного учреждения «Управление муниципальным жилищным фондом города Перми» (далее – МКУ «УМЖФ»), в том числе при обработке в информационной системе персональных данных; в целях исполнения Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных»,

ПРИКАЗЫВАЮ:

1. Утвердить Политику информационной безопасности муниципального казенного учреждения «Управление муниципальным жилищным фондом города Перми» (далее – Политика), согласно приложению к настоящему приказу.
2. Начальнику общего отдела Телесницкой Ю.В. ознакомить всех работников с настоящим приказом.
3. Настоящий приказ вступает в силу с даты подписания.
4. Контроль за исполнением приказа оставляю за собой.

Директор

Д.С. Ватолина

Приложение к приказу
от 15.04.2022
№ 01-03-252/1

УТВЕРЖДЕНО

приказом директора

МКУ «Управление муниципальным
жилищным фондом города Перми»

от 15 июля 2022 г. № 01-03-252/1

**ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
МУНИЦИПАЛЬНОГО КАЗЕННОГО УЧРЕЖДЕНИЯ
«УПРАВЛЕНИЕ МУНИЦИПАЛЬНЫМ ЖИЛИЩНЫМ ФОНДОМ
ГОРОДА ПЕРМИ»**

Оглавление

1. Общие положения	3
2. Порядок и условия обработки персональных данных	8
3. Обработка персональных данных в рамках межведомственного информационного взаимодействия.....	9
4. Сроки обработки и хранения персональных данных.	10
5. Порядок уничтожения персональных данных при достижении целей обработки или при наступлении иных законных оснований.	11
6. Система защиты персональных данных.	12
7. Требования к подсистемам СЗПДн.	13
8. Пользователи ИСПДн.....	15
9. Требования к персоналу по обеспечению защиты ПДн	17
10. Ответственность сотрудников ИСПДн.....	18
11. Правовые основания.	19
Не ниже 5-го уровня защищенности	20
Не ниже 4-го уровня защищенности.....	20
Не ниже 3-го уровня защищенности.....	20

1. Общие положения

1.1 Назначение и цель

Настоящая политика информационной безопасности (далее — политика) муниципального казенного учреждения «Управление муниципальным жилищным фондом города Перми» (далее – МКУ «УМЖФ») определяет цели, содержание и порядок обработки персональных данных, меры, направленные на защиту персональных данных, а также процедуры, направленные на выявление и предотвращение нарушений законодательства российской федерации в области персональных данных в МКУ «УМЖФ».

Целью настоящей политики является обеспечение безопасности объектов защиты МКУ «УМЖФ» от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности ПДн (УБПДн).

Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

Информация и связанные с ней ресурсы должны быть доступны для авторизованных пользователей. Должно осуществляться своевременное обнаружение и реагирование на УБПДн.

Политика разработана в соответствии с целями, задачами и принципами обеспечения безопасности персональных данных, изложенных в положении информационной безопасности ИСПДн МКУ «УМЖФ».

В политике определены требования к сотрудникам, в силу своих должностных обязанностей, допущенных к работе в ИСПДн МКУ «УМЖФ», степень их ответственности, структура и необходимый уровень защищенности ИСПДн, статус и должностные обязанности сотрудников, ответственных за обеспечение безопасности персональных данных в ИСПДн МКУ «УМЖФ».

Должно осуществляться предотвращение преднамеренных или случайных, частичных или полных несанкционированных модификаций или уничтожения данных.

Перечень сведений, содержащих персональные данные, обрабатываемых в МКУ «УМЖФ», утвержден соответствующим приказом директора МКУ «УМЖФ».

1.2 Основные понятия

В настоящем документе используются следующие термины и их определения:

Автоматизированная система — система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Автоматизированная обработка персональных данных — обработка персональных данных с помощью средств вычислительной техники.

Аутентификация отправителя данных — подтверждение того, что отправитель полученных данных соответствует заявленному.

Безопасность персональных данных — состояние защищенности персональных данных, характеризующееся способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

Блокирование персональных данных — временное прекращение сбора,

систематизации, накопления, использования, распространения персональных данных, в том числе их передачи.

Вирус (компьютерный, программный) — исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Вредоносная программа — программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

Вспомогательные технические средства и системы — технические средства и системы, не предназначенные для передачи, обработки и хранения персональных данных, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки персональных данных или в помещениях, в которых установлены информационные системы персональных данных.

Доступ в операционную среду компьютера (информационной системы персональных данных) — получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ.

Доступ к информации — возможность получения информации и ее использования.

Закладочное устройство элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, конструкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации).

Защищаемая информация — информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Идентификация — присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информативный сигнал — электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация (персональные данные) обрабатываемая в информационной системе персональных данных.

Информационная система персональных данных (ИСПДн) — информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

Информационные технологии — процессы, методы поиска, сбора,

хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Использование персональных данных — действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.

Источник угрозы безопасности информации — субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

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

Конфиденциальность персональных данных — обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

Межсетевой экран — локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

Нарушитель безопасности персональных данных — физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных.

Неавтоматизированная обработка персональных данных — обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

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

Несанкционированный доступ (несанкционированные действия) — доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

Носитель информации — физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Обезличивание персональных данных — действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

Обработка персональных данных — действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Общедоступные персональные данные — персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

Оператор (персональных данных) — государственный орган, муниципальный орган, юридическое или физическое лицо, организующее и (или) осуществляющее обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

Перехват (информации) — неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

Персональные данные — любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Предоставление персональных данных — действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

Побочные электромагнитные излучения и наводки — 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.

Политика «чистого стола» — комплекс организационных мероприятий, контролирующих отсутствие записывания на бумажные носители ключей и атрибутов доступа (паролей) и хранения их вблизи объектов доступа.

Пользователь информационной системы персональных данных — лицо, участвующее в функционировании информационной системы персональных данных 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 программное обеспечение информационной системы персональных данных и (или) блокировать аппаратные средства.

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

Раскрытие персональных данных — умышленное или случайное нарушение конфиденциальности персональных данных.

Распространение персональных данных — действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга

лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

Ресурс информационной системы — именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

Специальные категории персональных данных — персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья и интимной жизни субъекта персональных данных.

Средства вычислительной техники — совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Субъект доступа (субъект) — лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Технический канал утечки информации — совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

Технические средства информационной системы персональных данных — средства вычислительной техники, 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 и другие технические средства обработки речевой, графической, видео и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

Трансграничная передача персональных данных — передача персональных данных оператором через государственную границу российской федерации органу власти

иностранного государства, физическому или юридическому лицу иностранного государства.

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

Уничтожение персональных данных — действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

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

Уязвимость — слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации.

Целостность информации — способность средства вычислительной техники

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

1.3 Обозначения и сокращения

АВС - антивирусные средства

АРМ - автоматизированное рабочее место

ВТСС - вспомогательные технические средства и системы

ИСПДн - информационная система персональных данных

КЗ - контролируемая зона

ЛВС - локальная вычислительная сеть

МЭ - межсетевой экран

НСД - несанкционированный доступ

ОС - операционная система

ПДн - персональные данные

ПМВ - программно-математическое воздействие

ПО - программное обеспечение

ПЭМИН - побочные электромагнитные излучения и наводки

САЗ - система анализа защищенности

СЗИ - средства защиты информации

СЗПДн - система (подсистема) защиты персональных данных

СОВ - система обнаружения вторжений

ТКУИ - технические каналы утечки информации

УБПДн - угрозы безопасности персональных данных

АИБ - администратор информационной безопасности

2. Порядок и условия обработки персональных данных

2.1. обработка персональных данных осуществляется в связи с исполнением уставной деятельности учреждения и для достижения целей, предусмотренных нормативно-правовыми актами.

2.2. перечень персональных данных, подлежащих обработке, утвержден в приказе директора МКУ «УМЖФ» «Об утверждении перечня сведений, содержащих персональные данные, обрабатываемые в муниципальном казенном учреждении «Управление муниципальным жилищным фондом города Перми».

2.3. обработка персональных данных осуществляется без согласия субъектов ПДн в рамках целей, определенных в федеральных законах и в целях исполнения уставной деятельности.

2.4. обработка персональных данных осуществляется при условии получения согласия субъектов ПДн в следующих случаях:

2.4.1 при передаче (распространении, предоставлении) персональных данных третьим лицам в случаях, не предусмотренных действующим законодательством российской федерации;

2.4.2 при трансграничной передаче персональных данных;

2.4.3 при принятии решений, порождающих юридические последствия в отношении указанных лиц или иным образом затрагивающих их права и законные интересы, на основании исключительно автоматизированной обработки их персональных данных.

2.5. в случаях, предусмотренных пунктом 2.4 настоящей политики, согласие субъекта персональных данных оформляется в письменной форме, если иное не установлено федеральным законом "о персональных данных".

2.6. обработка персональных данных осуществляется сотрудниками МКУ «УМЖФ», допущенных к их обработке, и включает в себя следующие действия: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

2.7. список сотрудников, допущенных к обработке ПДн, утвержден приказом директора МКУ «УМЖФ» «Об утверждении перечня сведений, содержащих персональные данные, обрабатываемые в муниципальном казенном учреждении «Управление муниципальным жилищным фондом города Перми».

2.8. запрещается получать, обрабатывать и запрашивать персональные данные, не предусмотренные п.2.2. Настоящей политики, в том числе касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни.

2.9. при сборе персональных данных сотрудник, осуществляющий сбор (получение) персональных данных непосредственно от субъекта ПДн обязан разъяснить указанным субъектам персональных данных юридические последствия отказа предоставить их персональные данные.

2.10. передача (распространение, предоставление) и использование персональных данных осуществляется лишь в случаях и в порядке, предусмотренных федеральными законами.

3. Обработка персональных данных в рамках межведомственного информационного взаимодействия

3.1. МКУ «УМЖФ» в соответствии с законодательством российской федерации осуществляет обработку персональных данных в рамках межведомственного информационного взаимодействия.

3.2. МКУ «УМЖФ» в рамках межведомственного взаимодействия на основании поступивших межведомственных запросов направляет информацию, включающую персональные данные субъектов, обрабатываемые в МКУ «УМЖФ», в следующие органы власти и учреждения:

- 3.2.1. в Министерство внутренних дел Российской Федерации;
- 3.2.2. в Прокуратуру Российской Федерации;
- 3.2.3. в Федеральную службу судебных приставов;
- 3.2.3. в Военный комиссариат Пермского края;
- 3.2.4. в Пенсионный фонд России и его территориальные органы;
- 3.2.5. в Федеральную налоговую службу;
- 3.2.6. в Федеральный фонд обязательного медицинского страхования РФ и его территориальные органы;
- 3.2.7. в страховые компании в рамках договоров обязательного и добровольного медицинского страхования жизни и здоровья работников, заключаемых работодателем;
- 3.2.8. в МКУ «Центр бухгалтерского учета и отчетности» города Перми;
- 3.2.9. в иные органы государственной власти в пределах представленных законом полномочий.

4. Сроки обработки и хранения персональных данных

4.1. Сроки обработки и хранения персональных данных определяются в соответствии с законодательством российской федерации.

4.2. Сроки обработки и хранения персональных данных утверждены приказом директора МКУ «УМЖФ» «Об утверждении перечня сведений, содержащих персональные данные, обрабатываемые в муниципальном казенном учреждении «Управление муниципальным жилищным фондом города Перми».

4.3. Необходимо обеспечивать раздельное хранение персональных данных на разных материальных носителях, обработка которых осуществляется в различных целях.

4.4. Контроль за хранением и использованием материальных носителей персональных данных, не допускающий несанкционированное использование, уточнение, распространение и уничтожение персональных данных, находящихся на этих носителях, осуществляют директор МКУ «УМЖФ», ответственный за защиту персональных данных МКУ «УМЖФ», администратор информационной безопасности МКУ «УМЖФ».

4.5. Срок хранения персональных данных, внесенных в информационные системы персональных данных МКУ «УМЖФ», должен соответствовать сроку хранения бумажных оригиналов.

5. Порядок уничтожения персональных данных при достижении целей обработки или при наступлении иных законных оснований

5.1. В МКУ «УМЖФ» осуществляется систематический контроль и выделение документов/файлов/данных, содержащих персональные данные, с истекшими сроками хранения, подлежащих уничтожению.

5.2. Вопрос об уничтожении выделенных документов, содержащих персональные данные, рассматривается на заседании комиссии по уничтожению персональных данных, состав которой утвержден приказом директора МКУ «УМЖФ» «О создании комиссии по уничтожению персональных данных».

По итогам заседания составляются протокол и акт о выделении к уничтожению ПДн, опись уничтожаемых ПДн, проверяется их комплектность, акт подписывается председателем и членами комиссии.

6. Система защиты персональных данных

6.1. Система защиты персональных данных (СЗПДн) строится на основании определенного необходимого уровня защищенности ПДн каждой ИСПДн МКУ «УМЖФ». На основании анализа актуальных угроз безопасности ПДн, описанного в модели угроз и отчета о результатах проведения внутренней проверки, делается заключение о необходимости использования технических средств и организационных мероприятий для обеспечения безопасности ПДн. Выбранные необходимые мероприятия отражаются в плане мероприятий по обеспечению защиты ПДн.

6.2. Для каждой ИСПДн должен быть составлен список используемых технических средств защиты, а также программного обеспечения, участвующего в обработке ПДн на всех элементах ИСПДн:

- АРМ пользователей.

- сервера приложений.

- СУБД.

- границы ЛВС.

- каналы передачи в сети общего пользования и (или) международного обмена, если по ним передаются ПДн.

В зависимости от уровня защищенности ИСПДн и актуальных угроз, СЗПДн может включать следующие технические средства:

- антивирусные средства для рабочих станций пользователей и серверов;

- средства межсетевого экранирования;

- средства криптографической защиты информации, при передаче защищаемой информации по каналам связи.

Также в список должны быть включены функции защиты, обеспечиваемые штатными средствами обработки ПДн операционными системами, прикладным по и специальными комплексами, реализующими средства защиты. Список функций защиты может включать:

- управление и разграничение доступа пользователей;

- регистрацию и учет действий с информацией;

- обеспечение целостности данных;

- обнаружение вторжений.

6.3. Список используемых технических средств отражается в плане мероприятий по обеспечению защиты персональных данных. Список используемых средств должен поддерживаться в актуальном состоянии. При изменении состава технических средств защиты или элементов ИСПДн, соответствующие изменения должны быть внесены в список и утверждены директором МКУ «УМЖФ» или лицом, ответственным за обеспечение защиты ПДн.

7. Требования к подсистемам СЗПДн

7.1. СЗПДн включает в себя следующие подсистемы:

- управления доступом, регистрации и учета;
- обеспечения целостности и доступности;
- антивирусной защиты;
- межсетевого экранирования;
- анализа защищенности;
- обнаружения вторжений;
- криптографической защиты.

Подсистемы СЗПДн имеют различную функциональность в зависимости от класса ИСПДн, определенного в акте классификации информационной системы персональных данных. Список соответствия функций подсистем СЗПДн классу защищенности представлен в **Приложении 1**.

7.2. Подсистема управления доступом, регистрации и учета предназначена для реализации следующих функций:

- идентификации и проверки подлинности субъектов доступа при входе в ИСПДн;

- идентификации терминалов, узлов сети, каналов связи, внешних устройств по логическим именам;

- идентификации программ, томов, каталогов, файлов, записей, полей записей по именам;

- регистрации входа (выхода) субъектов доступа в систему (из системы), либо регистрации загрузки и инициализации операционной системы и ее останова.

- регистрации попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам;

- регистрации попыток доступа программных средств к терминалам, каналам связи, программам, томам, каталогам, файлам, записям, полям записей.

7.3. Подсистема управления доступом может быть реализована с помощью штатных средств обработки ПДн (операционных систем, приложений и СУБД). Также может быть внедрено специальное техническое средство или их комплекс, осуществляющий дополнительные меры по аутентификации и контролю. Например, применение единых хранилищ учетных записей пользователей и регистрационной информации, использование биометрических и технических (с помощью электронных пропусков) мер аутентификации и других.

7.4 подсистема обеспечения целостности и доступности предназначена для обеспечения целостности и доступности ПДн, программных и аппаратных средств ИСПДн МКУ «УМЖФ», а также средств защиты при случайной или намеренной модификации. Подсистема реализуется с помощью организации резервного копирования обрабатываемых данных, а также резервированием ключевых элементов ИСПДн.

7.5. Подсистема антивирусной защиты предназначена для обеспечения антивирусной защиты серверов и АРМ пользователей ИСПДн МКУ «УМЖФ».

Средства антивирусной защиты предназначены для реализации следующих функций:

- резидентный антивирусный мониторинг;
- антивирусное сканирование;
- скрипт-блокирование;

централизованная/удаленная установка/деинсталляция антивирусного продукта, настройка, администрирование, просмотр ответов и статистической информации по работе продукта;

автоматизированное обновление антивирусных баз;

ограничение прав пользователя на остановку исполняемых задач и изменение настроек антивирусного программного обеспечения;

автоматический запуск сразу после загрузки операционной системы.

Подсистема реализуется путем внедрения специального антивирусного программного обеспечения на все элементы ИСПДн.

7.6. Подсистема межсетевое экранирования предназначена для реализации следующих функций:

фильтрации открытого и зашифрованного (закрытого) IP-трафика по различным параметрам;

фиксации во внутренних журналах информации о проходящем открытом и закрытом IP-трафике;

идентификации и аутентификации администратора межсетевого экрана при его локальных запросах на доступ;

регистрации входа (выхода) администратора межсетевого экрана в систему (из системы) либо загрузки и инициализации системы и ее программного обеспечения;

контроля целостности своей программной и информационной части;

фильтрации пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;

фильтрации с учетом входного и выходного сетевого интерфейса как средства проверки подлинности сетевых адресов;

регистрации и учета запрашиваемых сервисов прикладного уровня;

блокирования доступа неидентифицированного объекта или субъекта, подлинность которого при аутентификации не подтвердилась, методами, устойчивыми к перехвату;

контроля за сетевой активностью приложений и обнаружения сетевых атак.

Подсистема реализуется внедрением программно-аппаратных комплексов межсетевого экранирования на границе ЛВС, классом не ниже 4.

7.7. Подсистема анализа защищенности должна обеспечивать выявление уязвимостей, связанных с ошибками в конфигурации по ИСПДн, которые могут быть использованы нарушителем для реализации атаки на систему. Функциональность подсистемы может быть реализована программными и программно-аппаратными средствами.

7.8. Подсистема обнаружения вторжений должна обеспечивать выявление сетевых атак на элементы ИСПДн, подключенные к сетям общего пользования и (или) международного обмена. Функциональность подсистемы может быть реализована программными и программно-аппаратными средствами.

8. Пользователи ИСПДн

8.1. В политике информационной безопасности определены основные категории пользователей. На основании этих категории должна быть произведена типизация пользователей ИСПДн, определен их уровень доступа и возможности.

8.2. В ИСПДн МКУ «УМЖФ» можно выделить следующие группы пользователей, участвующих в обработке и хранении ПДн:

- администратор ИСПДн;
- администратор безопасности ИСПДн; оператор АРМ;
- администратор сети;
- технический специалист по обслуживанию периферийного оборудования; программист-разработчик ИСПДн.

Данные о группах пользователей, уровне их доступа и информированности должен быть отражен в положении о разграничении прав доступа к обрабатываемым персональным данным.

8.2.1. Администратор ИСПДн

Администратор ИСПДн сотрудник МКУ «УМЖФ», ответственный за настройку, внедрение и сопровождение ИСПДн. Обеспечивает функционирование подсистемы управления доступом ИСПДн и уполномочен осуществлять предоставление и разграничение доступа конечного пользователя (оператора АРМ) к элементам, хранящим персональные данные.

Администратор ИСПДн обладает следующим уровнем доступа и знаний:
обладает полной информацией о системном и прикладном программном обеспечении ИСПДн;

обладает полной информацией о технических средствах и конфигурации ИСПДн; имеет доступ ко всем техническим средствам обработки информации и данным

ИСПДн;

обладает правами конфигурирования и административной настройки технических средств ИСПДн.

8.2.2. Администратор безопасности

Администратор безопасности сотрудник МКУ «УМЖФ», ответственный за функционирование СЗПДн, включая обслуживание и настройку административной, серверной и клиентской компонент.

Администратор безопасности обладает следующим уровнем доступа и знаний: обладает правами администратора ИСПДн;

обладает полной информацией об ИСПДн;

имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн;

не имеет прав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных).

Администратор безопасности уполномочен:

реализовывать политику безопасности в части настройки системы контроля защиты информации (СКЗИ), межсетевых экранов и систем

обнаружения атак, в соответствии с которыми пользователь (оператор АРМ) получает возможность работать с элементами ИСПДн;

осуществлять аудит средств защиты;

устанавливать доверительные отношения защищенной сети организации с сетями других организаций.

8.2.3. Оператор АРМ

Оператор АРМ сотрудник МКУ «УМЖФ», осуществляющий обработку ПДн. Обработка ПДн включает: возможность просмотра ПДн, ручной ввод ПДн в систему ИСПДн, формирование справок и отчетов по информации, полученной из ИСПДн. Оператор не имеет полномочий для управления подсистемами обработки данных и СЗПДн.

Оператор ИСПДн обладает следующим уровнем доступа и знаний:

обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству ПДн;

располагает конфиденциальными данными, к которым имеет доступ.

8.2.4. Администратор сети

Администратор сети сотрудник МКУ «УМЖФ», ответственный за функционирование телекоммуникационной подсистемы ИСПДн. Администратор сети не имеет полномочий для управления подсистемами обработки данных и безопасности.

Администратор сети обладает следующим уровнем доступа и знаний:

обладает частью информации о системном и прикладном программном обеспечении ИСПДн;

обладает частью информации о технических средствах и конфигурации ИСПДн; имеет физический доступ к техническим средствам обработки информации и средствам защиты;

знает, по меньшей мере, одно легальное имя доступа.

8.2.5. Технический специалист по обслуживанию периферийного оборудования

Технический специалист по обслуживанию сотрудник МКУ «УМЖФ» (или ИСПДн), осуществляющий обслуживание и настройку периферийного оборудования ИСПДн. Технический специалист по обслуживанию не имеет доступа к ПДн, не имеет полномочий для управления подсистемами обработки данных и безопасности.

Технический специалист по обслуживанию обладает следующим уровнем доступа и знаний:

обладает частью информации о системном и прикладном программном обеспечении ИСПДн;

обладает частью информации о технических средствах и конфигурации ИСПДн; знает, по меньшей мере, одно легальное имя доступа.

8.2.6. Программист-разработчик ИСПДн

Программисты прикладного программного обеспечения обеспечивают его сопровождение на защищаемом объекте. К данной группе могут относиться сотрудники МКУ «УМЖФ».

Лицо этой категории:

обладает информацией об алгоритмах и программах обработки информации в ИСПДн;

обладает возможностями внесения ошибок, недекларированных

возможностей, программных закладок, вредоносных программ в программное обеспечение ИСПДн на стадии ее разработки, внедрения и сопровождения;

может располагать любыми фрагментами информации о топологии ИСПДн и технических средствах обработки и защиты ПДн, обрабатываемых в ИСПДн.

9. Требования к персоналу по обеспечению защиты ПДн

9.1. Все сотрудники МКУ «УМЖФ», являющиеся пользователями ИСПДн, должны четко знать и строго выполнять установленные правила и обязанности по доступу к защищаемым объектам и соблюдению принятого режима безопасности ПДн.

9.2. При вступлении в должность нового сотрудника непосредственный начальник подразделения, в которое поступает сотрудник, вместе с ответственными за обеспечение защиты ПДн в МКУ «УМЖФ» обязан организовать ознакомление нового сотрудника с должностной инструкцией и необходимыми документами, регламентирующими требования по защите ПДн, а также обучение навыкам выполнения процедур, необходимых для санкционированного использования ИСПДн.

9.3. Сотрудник должен быть ознакомлен с положениями настоящей политики, принятых процедур работы с элементами ИСПДн и СЗПДн.

9.4. Сотрудники МКУ «УМЖФ», использующие технические средства аутентификации, должны обеспечивать сохранность идентификаторов (электронных ключей) и не допускать НСД к ним, а также возможность их утери или использования третьими лицами. Пользователи несут персональную ответственность за сохранность идентификаторов.

9.5. Сотрудники МКУ «УМЖФ» должны следовать установленным процедурам поддержания режима безопасности ПДн при выборе и использовании паролей (если не используются технические средства аутентификации).

9.6. Сотрудники МКУ «УМЖФ» должны обеспечивать надлежащую защиту оборудования, оставляемого без присмотра, особенно в тех случаях, когда в помещение имеют доступ посторонние лица. Все пользователи должны знать требования по безопасности ПДн и процедуры защиты оборудования, оставленного без присмотра, а также свои обязанности по обеспечению такой защиты.

9.7. Сотрудникам запрещается устанавливать постороннее программное обеспечение, подключать личные мобильные устройства и носители информации.

9.8. Сотрудникам запрещается разглашать защищаемую информацию, которая стала им известна при работе с информационными системами МКУ «УМЖФ», третьим лицам.

9.9. При работе с ПДн в ИСПДн сотрудники МКУ «УМЖФ» обязаны обеспечить отсутствие возможности просмотра ПДн третьими лицами с мониторов АРМ или терминалов.

9.10. При завершении работы с ИСПДн сотрудники обязаны защитить АРМ или терминалы с помощью блокировки ключом или эквивалентного средства контроля, например, доступом по паролю, если не используются более сильные средства защиты.

9.11. Сотрудники МКУ «УМЖФ» должны быть проинформированы об угрозах нарушения режима безопасности ПДн и ответственности за его нарушение. Они должны быть ознакомлены с утвержденной формальной процедурой наложения дисциплинарных взысканий на сотрудников, которые нарушили принятые политику и процедуры безопасности ПДн.

9.12. Сотрудники обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы ИСПДн, могущих повлечь за собой угрозы

безопасности ПДн, а также о выявленных ими событиях, затрагивающих безопасность ПДн, руководству подразделения и лицу, отвечающему за немедленное реагирование на угрозы безопасности ПДн.

10. Ответственность сотрудников ИСПДн

10.1. В соответствии с федеральным законом российской федерации от 27 июля 2006г. N 152-ФЗ «О персональных данных» лица, виновные в нарушении требований данного федерального закона, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством российской федерации ответственность.

10.2. Действующее законодательство РФ позволяет предъявлять требования по обеспечению безопасной работы с защищаемой информацией и предусматривает ответственность за нарушение установленных правил эксплуатации ЭВМ и систем, неправомерный доступ к информации, если эти действия привели к уничтожению, блокированию, модификации информации или нарушению работы ЭВМ или сетей.

10.3. Администратор ИСПДн и администратор безопасности несут ответственность за все действия, совершенные от имени их учетных записей или системных учетных записей, если не доказан факт несанкционированного использования учетных записей.

10.4. При нарушениях сотрудниками МКУ «УМЖФ» пользователями ИСПДн правил, связанных с безопасностью ПДн, они несут ответственность, установленную действующим законодательством российской федерации.

11. Правовые основания

Настоящая Политика разработана в соответствии с Трудовым кодексом Российской Федерации, Кодексом Российской Федерации об административных правонарушениях, Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», Федеральным законом от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 25 декабря 2008 г. N 273-ФЗ «О противодействии коррупции», Федеральным законом от 27 июля 2010 г. N 210-ФЗ «Об организации предоставления государственных и муниципальных услуг», постановлением Правительства Российской Федерации от 1 ноября 2012 г. N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», постановлением Правительства Российской Федерации от 21 марта 2012 г. N 211 «Об утверждении перечня мер, направленные 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», приказом Федеральной службы по техническому и экспортному контролю от 18.02.2013 г. N 21 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», приказом ФСБ РФ от 10.07.2014 г. N 378 «Об утверждении Составы 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», приказом ФСБ РФ от 09.02.2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)», приказом ФСБ РФ от 13.06.2001 г. № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну», методическими рекомендациями по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности, утвержденных руководством 8 Центра ФСБ России от 31.03.2015 г. № 149/7/6-432.

Требования настоящей Политики распространяются на всех сотрудников МКУ «УМЖФ» (штатных, временные, работающих по контракту и т.п.), а также всех прочих лиц — представителей организаций, которые находятся в договорных отношениях с МКУ «УМЖФ» (подрядчики, аудиторы и т.п.).

Приложение 1

Классификация ИСПДн (Согласно утратившему силу постановлению Правительства Российской Федерации от 17 ноября 2007 г. N 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» и действующим документам ФСТЭК)

№	План - перечень технических мероприятий по обеспечению безопасности ИСПД	ИСПДн класса К3	ИСПДн класса К2	ИСПДн класса К1
I	В подсистеме управления доступом:			
1	Реализовать идентификацию и проверку подлинности субъектов доступа при входе в операционную систему ИСПДн по паролю условно-постоянного действия, длиной не менее шести буквенно-цифровых символов;	+	+	+
2	Реализовать идентификацию терминалов, технических средств обработки ПДн, узлов ИСПДн, компьютеров, каналов связи, внешних устройств ИСПДн по их логическим именам (адресам, номерам);		+	+
3	Реализовать идентификацию программ, томов, каталогов, файлов, записей, полей записей по именам;		+	+
4	Реализовать контроль доступа субъектов к защищаемым ресурсам в соответствии с матрицей доступа;		+	+
5	При наличии подключения ИСПДн к сетям общего пользования должно применяться межсетевое экранирование.	Не ниже 5-го уровня защищенности	Не ниже 4-го уровня защищенности	Не ниже 3-го уровня защищенности
6	Для обеспечения безопасного межсетевого взаимодействия в ИСПДн для разных классов необходимо использовать МЭ	Не ниже 5-го уровня защищенности	Не ниже 4-го уровня защищенности	Не ниже 3-го уровня защищенности
II	Средство защиты от программно-математических воздействий (ПМВ):			

1	Реализовать идентификацию и аутентификацию субъектов доступа при входе в средство защиты от программно-математических воздействий (ПМВ) и перед выполнением ими любых операций по управлению функциями средства защиты от ПМВ по паролю (или с использованием иного механизма аутентификации) условно-постоянного действия длиной не менее шести буквенно-цифровых символов;	+	+	+
2	Осуществлять контроль любых действий субъектов доступа по управлению функциями средства защиты от ПМВ только после проведения его успешной аутентификации;	+	+	+
3	Предусмотреть механизмы блокирования доступа к средствам защиты от ПМВ при выполнении устанавливаемого числа неудачных попыток ввода пароля;	+	+	+
4	Необходимо проводить идентификацию файлов, каталогов, программных модулей, внешних устройств, используемых средств защиты от ПМВ;	+	+	+
III	В подсистеме регистрации и учета:			
1	Осуществлять регистрацию входа (выхода) субъекта доступа в систему (из системы), либо регистрацию загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратного отключения ИСПДн. В параметрах регистрации указываются дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;	+	+	+
2	Проводить учет всех защищаемым носителей информации с помощью их любой маркировки и с занесением учетных данных в журнал (учетную карточку);	+	+	+
3	Проводить регистрацию входа/выхода субъектов доступа в средство защиты от ПМВ, регистрацию загрузки и инициализации этого средства и ее программного останова. В параметрах регистрации указывается время и дата входа/выхода субъекта доступа в средство защиты от ПМВ или загрузки/останова этого средства, а также идентификатор субъекта доступа, инициировавшего данные действия;	+	+	+

4	Проводить регистрацию событий проверки и обнаружения ПМВ. В параметрах регистрации указываются время и дата проверки или обнаружения ПМВ, идентификатор субъекта доступа, инициировавшего данные действия, характер выполняемых действий по проверке, тип обнаруженной вредоносной программы (ВП), результат действий средства защиты по блокированию ПМВ;	+	+	+
5	Проводить регистрацию событий по внедрению в средство защиты от ПМВ пакетов обновлений. В параметрах регистрации указываются время и дата обновления, идентификатор субъекта доступа, инициировавшего данное действие, версия и контрольная сумма пакета обновления;	+	+	+
6	Проводить регистрацию событий запуска/завершения работы модулей средства защиты от ПМВ. В параметрах регистрации указываются время и дата запуска/завершения работы, идентификатор модуля, идентификатор субъекта доступа, инициировавшего данное действие, результат запуска/завершения работы;	+	+	+
7	должна проводиться регистрация событий управления субъектом доступа функциями средства защиты от ПМВ. В параметрах регистрации указываются время и дата события управления каждой функцией, идентификатор и спецификация функции, идентификатор субъекта доступа, инициировавшего данное действие, результат действия;	+	+	+
8	Проводить регистрацию событий попыток доступа программных средств к модулям средства защиты от ПМВ или специальным ловушкам. В параметрах регистрации указываются время и дата попытки доступа, идентификатор модуля, идентификатор и спецификация модуля средства защиты от ПМВ (специальной ловушки), результат попытки доступа;	+	+	+
9	Проводить регистрацию событий отказа для средства защиты от ПМВ. В параметрах регистрации указываются время и дата события отказа, спецификация действий отказа, идентификатор субъекта доступа, инициировавшего данное действие, результат действия;	+	+	+
10	Обеспечить защиту данных регистрации от их уничтожения или модификации нарушителем;	+	+	+

11	Реализовать механизмы сохранения данных регистрации в случае сокращения отведенных под них ресурсов;	+	+	+
12	Реализовать механизмы просмотра и анализа данных регистрации и их фильтрации по заданному набору параметров;	+	+	+
13	Проводить автоматический непрерывный мониторинг событий, которые могут являться причиной реализации ПМВ (создание, редактирование, запись, компиляция объектов, которые могут содержать ВП).	+	+	+
14	Реализовать механизм автоматического анализа данных регистрации по шаблонам типовых проявлений ПМВ с автоматическим их блокированием и уведомлением администратора безопасности;	+	+	+
15	Проводить несколько видов учета (дублирующих) с регистрацией выдачи (приема) носителей информации;	+	+	+
16	Осуществлять регистрацию входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы.		+	+
17	Осуществлять регистрацию выдачи печатных (графических) документов на «твердую» копию. В параметрах регистрации указываются (дата и время выдачи (обращения к подсистеме вывода), спецификация устройства выдачи — логическое имя (номер) внешнего устройства, краткое содержание (наименование, вид, шифр, код) и уровень конфиденциальности документа, идентификатор субъекта доступа, запросившего документ;		+	+
18	Осуществлять регистрацию запуска (завершения) программ и процессов (заданий, задал), предназначенных для обработки защищаемых файлов. В параметрах регистрации указываются дата и время запуска, имя (идентификатор) программы (процесса, задания), идентификатор субъекта доступа, запросившего программу (процесс, задание), результат запуска (успешный, неуспешный — несанкционированный),		+	+

19	Осуществлять регистрацию попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам. В параметрах регистрации указываются дата и время попытки доступа к защищаемому файлу с указанием ее результата (успешная, неуспешная — несанкционированная), идентификатор субъекта доступа, спецификация защищаемого файла;	-	+	+
20	Осуществлять регистрацию попыток доступа программных средств к следующим дополнительным защищаемым объектам доступа: терминалам, компьютерам, узлам сети ИСПДн, линиям (каналам) связи, внешним устройствам компьютеров, программам, томам, каталогам, файлам, записям, полям записей. В параметрах регистрации указываются дата и время попытки доступа к защищаемому объекту с указанием ее результата (успешная, неуспешная — несанкционированная), идентификатор субъекта доступа, спецификация защищаемого объекта — логическое имя (номер);		+	+
21	Проводить учет всех защищаемых носителей информации с помощью их маркировки и с занесением учетных данных в журнал (учетную карточку);		+	+
22	Осуществлять очистку (обнуление, обезличивание) освобождаемых областей оперативной памяти компьютеров и внешних накопителей. Очистка осуществляется однократной произвольной записью в освобождаемую область памяти, ранее использованную для хранения защищаемых данных (файлов, информации);		+	+
IV	В подсистеме обеспечения целостности:			
1	Обеспечить целостность программных средств защиты в составе СЗПДн, а также неизменность программной среды. При этом целостность средств защиты проверяется при загрузке системы по наличию имен (идентификаторов) компонент СЗПДн, целостность программной среды обеспечивается отсутствием в ИСПДн средств разработки и отладки программ;	+	+	+
2	Осуществлять физическую охрану ИСПДн (устройств и носителей информации), предусматривающую контроль доступа в помещения ИСПДн посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения ИСПДн и хранилище носителей информации;	+	+	+

3	Проводить периодическое тестирование функций СЗПДн при изменении программной среды и персонала ИСПДн с помощью тест-программ, имитирующих попытки НСД;	+	+	+
4	должны быть в наличии средства восстановления СЗПДн, предусматривающие ведение двух копий программных средств защиты информации, их периодическое обновление и контроль работоспособности;	+	+	+
5	Проводить проверку целостности модулей средства защиты от ПМВ, необходимых для его корректного функционирования, при его загрузке с использованием контрольных сумм;	+	+	+
6	Обеспечить возможность восстановления средства защиты от ПМВ, предусматривающая ведение двух копий программного средств защиты, его периодическое обновление и контроль работоспособности;	+	+	+
7	Реализовать механизмы проверки целостности пакетов обновлений средства защиты от ПМВ с использованием контрольных сумм;	+	+	+
8	Проводить резервное копирование ПДн на отчуждаемые носители информации;		+	+
V	В подсистеме антивирусной защиты:			
1	Проводить автоматическую проверку на наличие ВП или последствий ПМВ при импорте в ИСПДн всех программных модулей (прикладных программ), которые могут содержать ВП, по их типовым шаблонам и с помощью эвристического анализа;	+	+	+
2	Реализовать механизмы автоматического блокирования обнаруженных ВП путем их удаления из программных модулей или уничтожения;	+	+	+
3	Регулярно выполнять (при первом запуске средств защиты ПДн от ПМВ и с устанавливаемой периодичностью) проверка на предмет наличия в них ВП;	+	+	+
4	Должна иницироваться автоматическая проверка ИСПДн на предмет наличия ВП при выявлении факта ПМВ;	+	+	+

5	Реализовать механизм отката для устанавливаемого числа операций удаления ВП из оперативной или постоянной памяти, из программных модулей и прикладных программ или программных средств, содержащих ВП.	+	+	+
6	Дополнительно в ИСПДн должен проводиться непрерывный автоматический мониторинг информационного обмена с внешней сетью с целью выявления ВП.	+	+	+
VI	Контроль отсутствия НДВ в ПО СЗИ			
1	Для программного обеспечения, используемого при защите информации в ИСПДн (средств защиты информации — СЗИ, в том числе и встроенных в общесистемное и прикладное программное обеспечение — ПО), должен быть обеспечен соответствующий уровень контроля отсутствия в нем НДВ (не декларированных возможностей).	+	+	+
VII	Обнаружение вторжений в ИСПДн			
	Обнаружение вторжений должно обеспечиваться путем использования в составе ИСПДн программных или программно-аппаратных средств (систем) обнаружения вторжений (СОВ).	+	+	+
1	Необходимо обязательное использование системы обнаружения сетевых атак, использующие сигнатурные методы анализа	+		
2	Необходимо обязательное использование системы обнаружения сетевых атак, использующие сигнатурные методы анализа и методы выявления аномалий		+	+
VIII	Защита ИСПДн от ПЭМИН			
1	Для обработки информации необходимо использовать СВТ, удовлетворяющие требованиям стандартов Российской Федерации по электромагнитной совместимости, по безопасности и эргономическим требованиям к средствам отображения информации, по санитарным нормам, предъявляемым к видеодисплейным терминалам ПЭВМ (например, ГОСТ 29216 91, ГОСТ Р 50948-2001, ГОСТ Р 50949-2001, ГОСТ Р 50923 96, СанПиН 2.2.2.542 96).	+	+	+
IX	Оценка соответствия ИСПДн требованиям безопасности ПДн			
1	Провести обязательную сертификацию (аттестацию) по требованиям безопасности информации;		+	+
2	Декларировать соответствие или обязательную сертификацию (аттестацию) по требованиям безопасности информации (по решению оператора);	+		

Примечание: Для ИСПДн 4-го класса перечень мероприятий по защите ПДн определяется в зависимости от ущерба, который может быть нанесен вследствие несанкционированного или непреднамеренного доступа к ПДн.

Приложение 2. Уровни защищенности ИСПДн (Согласно новому постановлению Правительства РФ от 01.11.2012 N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»).

Требования к защите ПДн \ Уровень защищенности	УЗ 1	УЗ 2	УЗ 3	УЗ 4
Организация режима работы обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения.	+	+	+	+
Обеспечение сохранности носителей персональных данных.	+	+	+	+
Утверждением руководителем оператора ПДн документов, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (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.	+	+	+	+
Необходимость назначения должностного лица (работника), ответственного за обеспечение безопасности персональных данных в информационной системе.	+	+	+	-
Возможность доступа к содержанию электронного журнала сообщений исключительно для должностных лиц (работников) оператора или уполномоченного лица, которым сведения, содержащиеся в указанном журнале, необходимы для выполнения служебных (трудовых) обязанностей.	+	+	-	-
Автоматическая регистрация в электронном журнале безопасности изменения полномочий сотрудника оператора по доступу к персональным данным, содержащимся в информационной системе.	+	-	-	-
Содержание журнала регистрации изменений в информационной системе.	+	-	-	-

безопасности персональных данных в информационной системе, либо вложение на одно из структурных подразделений функций по обеспечению такой безопасности.					
--	--	--	--	--	--

Приложение А

к Политике муниципального казенного
учреждения «Управление муниципальным
жилищным фондом города Перми»

Директору
МКУ «Управление муниципальным
жилищным фондом города Перми»

От _____, паспорт: серия _____,
ФИО

номер _____, выдан _____

_____ кем выдан

дата выдачи _____ Адрес для получения ответа: _____

ЗАПРОС

На основании п.2 ст.9 Федерального Закона от 27.07.2006 г. № 152-ФЗ «О персональных
данных» прошу в установленный срок прекратить обработку моих персональных данных в
информационной системе _____ в связи с отзывом мною
согласия на обработку моих персональных данных.

_____ «__» _____ 20__ г.
Подпись ФИО Дата

к Политике муниципального казенного учреждения «Управление муниципальным жилищным фондом города Перми»

Директору
МКУ «Управление муниципальным
жилищным фондом города Перми»

КЕМ ВЫДАН

дата выдачи _____ Адрес для получения ответа: _____

На основании п.1 ст.14 Федерального Закона от 27.07.2006 года N 152-ФЗ «О персональных данных» прошу в установленный срок предоставить мне как субъекту персональных данных доступ к моим персональным данным, обрабатываемым в Муниципальном казенном учреждении «Информационно-аналитический центр» города Перми на основании заявления № _____, а также следующую информацию:

- 1) подтверждение факта обработки персональных данных оператором;
- 2) правовые основания и цели обработки персональных данных;
- 3) цели и применяемые оператором способы обработки персональных данных;
- 4) наименование и место нахождения оператора, сведения о лицах (за исключением сотрудников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании Федерального закона №152-ФЗ;
- 5) обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен Федеральным законом № 152-ФЗ;
- 6) сроки обработки персональных данных, в том числе сроки их хранения;
- 7) порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом 33152-ФЗ;
- 8) информацию об осуществленной или о предполагаемой трансграничной передаче данных;
- 9) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;
- 10) иные сведения, предусмотренные Федеральным законом №152-ФЗ или другими федеральными законами.

« » 20 г.
Дата

Подпись

ФНО