УТВЕРЖДАЮ:

И.о. директора
муниципального предприятия
муниципального образования
г. Магнитогорска
«Единый расчетно-кассовый центр»

_____ Е.Ф. Манолова

М.П.

«17» января 2012 г.

ПОЛОЖЕНИЕ
ПО ОРГАНИЗАЦИИ И ПРОВЕДЕНИЮ РАБОТ
ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ
ПЕРСОНАЛЬНЫХ ДАННЫХ
ПРИ ИХ ОБРАБОТКЕ
В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

СОГЛАСОВАНО:

И.о. заместителя директора
МП «ЕРКЦ»
_____ В. Ю. Разинков

И.о. главного бухгалтера
МП «ЕРКЦ»
_____ О. В. Шилина

И.о. начальника
финансово-экономического отдела
МП «ЕРКЦ»
_____ С. В. Шапошникова

Начальник отдела
регистрационного учета граждан
МП «ЕРКЦ»
_____ Н. В. Щербакова

Начальник отдела
программного обеспечения
МП «ЕРКЦ»
_____ А. А. Галаев

Начальник отдела
приватизации жилья
МП «ЕРКЦ»
_____ И. В. Евдокимова

Начальник юридического отдела
МП «ЕРКЦ»
_____ Н. А. Котова

Начальник абонентского отдела
МП «ЕРКЦ»
_____ И. С. Козлова

Начальник общего отдела
МП «ЕРКЦ»
_____ Л. А. Золенко

Начальник отдела учета и начислений
МП «ЕРКЦ»
_____ И. Н. Андрюнина

Содержание

Основные понятия

В настоящем документе используются следующие основные понятия:

Персональные данные (ПДн) – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Персональные данные работника – информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника.

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

Биометрические персональные данные – сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность, включая фотографии, отпечатки пальцев, образ сетчатки глаза, особенности строения тела и другую подобную информацию.

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, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

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

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.

Трансграничная передача персональных данных – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

Распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

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

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

Уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

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

Информационная система персональных данных (ИСПДн) – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

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

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.

Перечень сокращений

АИБ	Администратор информационной безопасности
АИС «ЖЭО»	АИС «ПАСПОРТНЫЙ СТОЛ ЖЭО» ОРУГ МП «ЕРКЦ» участок №1, участок №2, участок №3, участок №4, участок №5, участок №6, участок №7
АО	Абонентский отдел
АРМ «Бухгалтер»	АРМ «Бухгалтер» участок №1, участок №2, участок №3, участок №4, участок №5, участок №6, участок №7
АРМ	Автоматизированное рабочее место
БД	База данных
ИБ	Информационная безопасность
ИП	Индивидуальный предприниматель
ИС	Информационная система
ИТ	Информационные технологии
ИСПДн	Информационная система персональных данных
ЖКУ	Жилищно-коммунальные услуги
ЛВС	Локальная вычислительная сеть
МП	Муниципальное предприятие
ОО	Общий отдел
ОПЖ	Отдел приватизации жилья
ОПО	Отдел программного обеспечения
ОРУГ	Отдел регистрационного учета граждан
ОУиН	Отдел учета и начислений
ПДн	Персональные данные
РФ	Российская Федерация
СЗИ	Средства защиты информации
СЗПДн	Система защиты персональных данных
ФЗ	Федеральный закон
ФСБ	Федеральная служба безопасности
ФСТЭК	Федеральная служба по техническому и экспортному контролю
ФЭО	Финансово-экономический отдел

1 Общие положения

1.1 Назначение документа

1.1.1. Настоящее Положение определяет порядок и условия обработки персональных данных (далее – ПДн) в муниципальном предприятии муниципального образования г. Магнитогорска «Единый расчетно-кассовый центр» (далее – МП «ЕРКЦ», Предприятие) работников Предприятия, контрагентов, граждан, зарегистрированных и (или) проживающих в зоне обслуживания управляющих компаний, заключивших договор с МП «ЕРКЦ» (далее – Клиентов), включая следующие аспекты защиты ПДн:

– организационная структура обеспечения безопасности ПДн;

– общие требования к обработке ПДн;

– требования к обработке ПДн, осуществляемой с использованием средств автоматизации;

– условия обработки ПДн, осуществляемой без использования средств автоматизации;

– порядок взаимодействия с органами местного самоуправления;

– требования к помещениям, в которых обрабатываются ПДн;

– обеспечение технической защиты ПДн;

– правила доступа к ПДн;

– требования к работникам, допущенным к обработке ПДн;

– организация внутреннего контроля обработки и обеспечения безопасности ПДн;

– порядок действий должностных лиц в случае возникновения нештатных ситуаций, связанных с ПДн;

– ответственность за нарушения при обработке ПДн.

1.1.2. Настоящее Положение предназначено для организации на Предприятии процесса обработки ПДн согласно нормам и принципам действующего федерального законодательства.

1.2 Область действия

1.1.1. Действие настоящего Положения распространяется на все процессы по сбору, систематизации, накоплению, хранению, уточнению, использованию, распространению, предоставлению, обезличиванию, блокированию, уничтожению ПДн, осуществляемые с использованием средств автоматизации и без их использования.

1.1.2. Действие настоящего Положения охватывает все информационные системы ПДн (далее – ИСПДн) Предприятия, перечень которых приведен в Приложение А.

1.1.3. Положение обязательно для ознакомления и исполнения всеми лицами, допущенными к обработке ПДн. Список должностей работников, допущенных к работе с ПДн на Предприятии, приведен в Приложении Б. Порядок формирования перечня должностей работников, допущенных к работе с ПДн, представлен в разделе 9.

1.1.4. Настоящее Положение вступает в силу с момента его подписания руководителем Предприятия и должно быть незамедлительно доведено до всех работников Предприятия и размещено на общедоступном корпоративном ресурсе (внутренний портал).

1.3 Нормативно–правовая основа

Настоящее Положение разработано в соответствии с законодательством Российской Федерации о ПДн и нормативно-методическими документами исполнительных органов государственной власти по вопросам безопасности ПДн при их обработке в ИСПДн, а также внутренними нормативными документами по обеспечению информационной безопасности Предприятия. Перечень нормативных документов приведен в Приложении В.

2 Организационная структура обеспечения безопасности ПДн

2.1 Отдел программного обеспечения

2.1.1. В состав отдела программного обеспечения (далее – ОПО) входят следующие должностные лица, задействованные в процессах автоматизированной обработки ПДн и обеспечения безопасности в ИСПДн:

– начальник отдела;

– ведущий программист, выполняющий обязанности системного администратора (далее – системный администратор);

– ведущий программист, выполняющий обязанности администратора баз данных (далее – администратор БД);

– инженер-программист первой категории, выполняющий обязанности администратора базы данных ОРУГ (далее – администратор БД);

– ведущий программист, выполняющий обязанности администратора информационной безопасности (далее – АИБ).

2.1.2. Начальник ОПО в рамках обеспечения безопасности ПДн организует решение следующих задач:

– проведение инвентаризации ИСПДн и определение характера обработки ПДн с использованием средств автоматизации;

– проведение классификации новых ИСПДн, в которых осуществляется автоматизированная обработка ПДн. Определение требований по обеспечению безопасности ПДн. Проектирование систем защиты. (С целью выполнения данных работ возможно привлечение подрядных организаций, имеющих необходимые лицензии для проведения работ по технической защите информации);

– проведение расследований инцидентов, связанных с несанкционированным распространением ПДн и несоблюдением правил настоящего Положения;

– согласование заявок на предоставление доступа к ИСПДн;

– поддержание в актуальном состоянии Списка работников, допущенных к работе с ПДн;

– выполнение проверок безопасности ИСПДн;

– первоначальное обучение основам безопасности ПДн.

2.1.3. Системный администратор в рамках обеспечения безопасности ПДн выполняют следующие задачи:

– обеспечение информационной безопасности (далее – ИБ) ИСПДн;

– устранение выявленных нарушений при обработке ПДн;

– проведение проверок безопасности ИСПДн;

– учет защищаемых носителей информации, используемых для хранения и обработки ПДн;

– тестирование функций системы защиты ПДн в целом и отдельных средств защиты ПДн в части программно-аппаратных средств.

2.1.4. Администраторы БД в рамках обеспечения безопасности ПДн выполняют следующие задачи:

– участие в проектировании систем защиты ИСПДн и внедрении программных средств защиты ИСПДн, взаимодействие с подрядными организациями, привлеченными для выполнения перечисленных работ;

– выполняют администрирование и сопровождение программных и аппаратных компонентов ИСПДн;

– участвуют, при необходимости, в расследовании инцидентов, связанных с несанкционированным распространением ПДн и несоблюдением правил настоящего Положения.

2.1.5. Администратор информационной безопасности в рамках обеспечения безопасности ПДн выполняют следующие задачи:

– участие в проектировании систем защиты ИСПДн и внедрении программных средств защиты ИСПДн, взаимодействие с подрядными организациями, привлеченными для выполнения перечисленных работ;

– участие в расследовании инцидентов, связанных с несанкционированным распространением ПДн и несоблюдением правил настоящего Положения.

2.2 **Общий отдел**

2.2.1. В состав Общего отдела (далее – ОО) входят следующие должностные лица, задействованные в процессах автоматизированной обработки ПДн и обеспечения безопасности в ИСПДн:

– начальник отдела;

– старший инспектор по кадрам (далее – кадровый работник);

– ведущий инженер, выполняющий обязанности инженера по охране труда и технике безопасности (далее – инженер по охране труда и технике безопасности).

2.2.2. Начальник ОО участвует, при необходимости, в расследовании инцидентов, связанных с несанкционированным распространением ПДн и несоблюдением правил настоящего Положения.

2.2.3. Кадровый работник в рамках обеспечения безопасности ПДн выполняет следующие задачи:

– сбор ПДн работников Предприятия, необходимых для ведения кадрового учета;

– контроль достоверности и полноты ПДн, их регулярное обновление и внесение по мере необходимости соответствующих изменений;

– хранение полученных ПДн работников Предприятия в соответствии с трудовым законодательством РФ;

– поддержание в актуальном состоянии Списка должностей работников, допущенных к работе с ПДн (Список должностей работников, допущенных к работе с ПДн, приведен в Приложении Б);

– учет бумажных носителей информации, используемых для хранения и обработки ПДн, в соответствии с трудовым законодательством РФ;

– контроль за выполнением правил обращения с документами, содержащими персональные данные работников Предприятия (в рамках деятельности ОО);

– контроль за соблюдением установленного порядка копирования документов (хранимых в ОО), содержащих персональные данные работников Предприятия;

– контроль за соблюдением правил рассылки документов, содержащих персональные данные работников Предприятия (в рамках деятельности ОО);

– оформление необходимых согласий при трудоустройстве работников;

– проводят при необходимости разъяснительную работу пунктов трудового договора, касающихся обеспечения конфиденциальности ПДн;

– информирует ОПО о необходимости прекращения доступа к ИСПДн при увольнении работника;

– участвуют, при необходимости, в расследовании инцидентов, связанных с несанкционированным распространением ПДн и несоблюдением правил настоящего Положения.

2.2.4. Инженер по охране труда и технике безопасности в рамках обеспечения безопасности ПДн выполняет следующие задачи:

– сбор ПДн работников Предприятия;

– контроль за достоверностью и полнотой ПДн: производит их регулярное обновление и вносит соответствующие изменения по мере необходимости;

– хранение ПДн работников Предприятия в соответствии с законодательством РФ;

– контроль за выполнением правил обращения с документами, содержащими ПДн работников Предприятия (в рамках своих должностных обязанностей).

2.3 **Бухгалтерия**

Работники Бухгалтерии в рамках обеспечения безопасности ПДн выполняют следующие задачи:

– сбор ПДн работников Предприятия и контрагентов Предприятия, необходимых для ведения бухгалтерского учета;

– контроль за достоверностью и полнотой ПДн, подотчетных лиц;

– контроль за выполнением правил обращения с документами, содержащими персональные данные работников Предприятия (в рамках деятельности Бухгалтерии);

– учет бумажных носителей информации, используемых для хранения и обработки ПДн, в соответствии с трудовым законодательством РФ;

– контроль за соблюдением правил рассылки документов, содержащих персональные данные (в рамках деятельности Бухгалтерии);

– участвуют, при необходимости, в расследовании инцидентов, связанных с несанкционированным распространением ПДн и несоблюдением правил настоящего Положения.

2.4 **Юридический отдел**

Работники Юридического отдела в рамках обеспечения безопасности ПДн выполняют следующие задачи:

– разрабатывают и согласовывают формы договоров, в рамках которых предполагается передача ПДн;

– определяют необходимость уведомления уполномоченного органа по защите прав субъектов ПДн об обработке ПДн, о внесении изменений в обработку ПДн, изменение целей обработки и т.д.;

– определяют необходимость получения согласий субъектов ПДн на обработку ПДн;

– определяют необходимость включения в договоры нужных условий по конфиденциальности ПДн при заключении договоров с контрагентами;

– анализируют правомерность запросов от субъектов ПДн, органов местного самоуправления, органов государственной власти к Предприятию.

– предоставляют ПДн в соответствии с законодательством Р.Ф.;

– участвуют, при необходимости, в расследовании инцидентов, связанных с несанкционированным распространением ПДн и несоблюдением правил настоящего Положения.

2.5 **Отдел регистрационного учета граждан**

Работники Отдела регистрационного учета граждан (далее – ОРУГ) в рамках обеспечения безопасности ПДн выполняют следующие задачи:

– сбор ПДн Клиентов Предприятия;

– получение согласий Клиентов Предприятия на обработку ПДн;

– хранение полученных ПДн в соответствии с законодательством РФ;

– предоставление ПДн в соответствии с законодательством РФ;

– контроль за достоверностью и полнотой ПДн, выполняют их регулярное обновление и внесение по мере необходимости соответствующих изменений;

– контроль за выполнением правил обращения с документами, содержащими ПДн (в рамках деятельности ОРУГ);

– участвуют, при необходимости, в расследовании инцидентов, связанных с несанкционированным распространением ПДн и несоблюдением правил настоящего Положения.

2.6 **Отдел учета и начислений**

Работники Отдела учета и начислений (далее – ОУиН) в рамках обеспечения безопасности ПДн выполняют следующие задачи:

– сбор ПДн Клиентов Предприятия;

– получение согласий Клиентов Предприятия на обработку ПДн;

– хранение полученных ПДн в соответствии с законодательством РФ;

– предоставление ПДн в соответствии с законодательством РФ;

– контроль за достоверностью и полнотой ПДн, выполняют их регулярное обновление и внесение по мере необходимости соответствующих изменений;

– контроль за выполнением правил обращения с документами, содержащими ПДн (в рамках деятельности ОУиН);

– участвуют, при необходимости, в расследовании инцидентов, связанных с несанкционированным распространением ПДн и несоблюдением правил настоящего Положения.

2.7 **Отдел приватизации жилья**

Работники Отдела приватизации жилья (далее – ОПЖ) в рамках обеспечения безопасности ПДн выполняют следующие задачи:

– сбор ПДн Клиентов Предприятия;

– получение согласий Клиентов Предприятия на обработку ПДн;

– предоставление ПДн в соответствии с законодательством РФ;

– хранение полученных ПДн в соответствии с законодательством РФ;

– контроль за достоверностью и полнотой ПДн;

– контроль за выполнением правил обращения с документами, содержащими ПДн (в рамках деятельности ОПЖ);

– участвуют, при необходимости, в расследовании инцидентов, связанных с несанкционированным распространением ПДн и несоблюдением правил настоящего Положения.

2.8 **Финансово-экономический отдел**

Работники Финансово-экономического отдела (далее – ФЭО) в рамках обеспечения безопасности ПДн выполняют следующие задачи:

– контроль за выполнением правил обращения с документами, содержащими ПДн (в рамках деятельности ФЭО);

– участвуют, при необходимости, в расследовании инцидентов, связанных с несанкционированным распространением ПДн и несоблюдением правил настоящего Положения.

2.9 **Абонентский отдел**

Работники Абонентского отдела (далее – АО) в рамках обеспечения безопасности ПДн выполняют следующие задачи:

– сбор данных о показаниях приборов учета Клиентов Предприятия;

– сбор ПДн Клиентов Предприятия;

– получение согласий Клиентов Предприятия на обработку ПДн;

– предоставление ПДн в соответствии с законодательством РФ;

– контроль за достоверностью показаний приборов учета Клиентов Предприятия;

– контроль за выполнением правил обращения с документами, содержащими ПДн (в рамках деятельности АО);

– участвуют, при необходимости, в расследовании инцидентов, связанных с несанкционированным распространением ПДн и несоблюдением правил настоящего Положения.

2.10 **Управление**

Ведущий инженер по экономической безопасности в рамках обеспечения безопасности ПДн выполняет следующие задачи:

– контроль за выполнением правил обращения с документами, содержащими ПДн (в рамках деятельности ведущего инженера по экономической безопасности);

– участвует, при необходимости, в расследовании инцидентов, связанных с несанкционированным распространением ПДн и несоблюдением правил настоящего Положения.

3 Общие требования к обработке ПДн

3.1 Цели обработки ПДн

3.1.1.В соответствии с п.1 ст.5 ФЗ № 152 «О персональных данных» на Предприятии определены следующие цели обработки ПДн:

– исполнение требований законодательства Российской Федерации (включая ведение бухгалтерского и кадрового учета, а также трудового законодательства Российской Федерации);

– идентификация Клиентов с целью последующего выставления счетов на оплату ЖКУ;

– идентификация Клиентов с целью ведения регистрационного учета граждан;

– идентификация Клиентов с целью заключения договоров социального найма жилого помещения от имени собственника жилого помещения – города Магнитогорска;

– идентификация Клиентов с целью заключения договоров приватизации жилого помещения от имени собственника жилого помещения - города Магнитогорска;

– идентификация контрагентов с целью последующего выставления счетов на оплату услуг, предоставляемых Предприятием;

– исполнение договорных обязательств Предприятия перед контрагентами;

– обеспечение справочной и информационной поддержки работы Предприятия.

3.1.2.Установленные цели обработки ПДн являются законными. Обработка ПДн в иных целях на Предприятии не допускается.

3.2 Характеристика персональных данных, обрабатываемых в информационных системах Предприятия

3.2.1.В информационных системах (далее – ИС) Предприятия обрабатываются ПДн следующих категорий субъектов ПДн:

– работников (субъектов), состоящих в трудовых отношениях с Предприятием;

– физических лиц – Клиентов Предприятия;

– юридических лиц[1], индивидуальных предпринимателей (далее – ИП) и физических лиц (контрагентов), состоящих в договорных отношениях с Предприятием;

3.2.2.К ПДн работников (субъектов), состоящих в трудовых отношениях с Предприятием, относятся следующие ПДн:

– Фамилия, имя, отчество;

– Дата рождения;

– Пол;

– Место рождения;

– Адрес: адрес регистрации и адрес проживания;

– Категория инвалидности[2];

– Паспортные данные (номер, серия, дата выдачи, кем выдан);

– Индивидуальный номер налогоплательщика (ИНН);

– Код страхового свидетельства пенсионного фонда;

– Гражданство;

[1)] Под ПДн юридических лиц, понимаются ПДн представителей юридических лиц, осуществляющих работы на основании доверенности юридического лица.

[2)] Данные о категории инвалидности не относятся к сведениям о состоянии здоровья, поскольку не раскрывают диагноза, который характеризует состояние здоровья.

– Образование;
– Подразделение;
– Должность;
– Дата приема на работу;
– Табельный номер;
– Номер банковского счета и реквизиты банка;
– Доходы (заработная плата);
– Данные о родственниках.

Данные о родственниках включают следующую информацию:
– Фамилия, имя, отчество;
– Год рождения;
– Степень родства.

3.2.3.К ПДн физических лиц – Клиентов Предприятия, относятся следующие ПДн:
– Фамилия, имя, отчество;
– Адрес;
– Данные документа удостоверяющего личность;
– Сведения о воинском учете;
– Семейное положение;
– Родственные связи;
– Информация о праве на пользование жилым помещением, его реквизиты;
– Сведения о наличии/отсутствии судимости;
– Сведения о дееспособности;
– Номер телефона (городской, мобильный);
– Адрес электронной почты;
– Категория льготы[1];
– Данные о льготных документах (вид, номер, серия, дата выдачи, кем выдан);
– Данные о выставленных счетах (ежемесячные начисления);
– Информация об оплатах (сумма периодических оплат);
– Информация о нарушениях и актах.

3.2.4. К ПДн юридических лиц[2], ИП и физических лиц (контрагентов), состоящих в договорных отношениях с Предприятием, относятся следующие ПДн:

Общедоступные ПДн
– Фамилия, имя, отчество;
– Адрес;
– Паспортные данные (номер, серия, дата выдачи, кем выдан);
– Индивидуальный номер налогоплательщика (ИНН);

Необщедоступные ПДн
– Номер телефона (городской, мобильный);
– Адрес электронной почты.

[1]) Данные о категории льготы не относятся к сведениям о состоянии здоровья, поскольку не раскрывают диагноза, который характеризует состояние здоровья.

[2]) Под ПДн юридических лиц, понимаются ПДн представителей юридических лиц, осуществляющих работы на основании доверенности юридического лица.

3.2.5. На Предприятии обрабатываются ПДн, позволяющие идентифицировать субъекты ПДн, а также получить о них дополнительную информацию.

3.2.6. Обработка ПДн осуществляется только с письменного согласия субъектов ПДн, за исключением случаев, предусмотренных ФЗ № 152 «О персональных данных» или на основании соответствующего договора на обработку ПДн с физическими, юридическими лицами или ИП.

3.2.7. ПДн подлежат правовой охране как сведения конфиденциального характера в соответствии с федеральным законодательством.

3.3 **Согласие на обработку ПДн**

3.3.1.Согласие субъекта ПДн также должно быть получено Предприятием в следующих случаях:

– в случае, когда клиент заключает договор не от своего имени, а от имени другого (других) физического лица (лиц);

– для физических лиц - клиентов Предприятия, в случае, когда в договоре оператора с субъектом ПДн не указана возможность передачи ПДн третьим лицам в целях исполнения договора (например, передача персональных данных в банки или типографию).

3.3.2.Отдельного согласия на обработку ПДн внештатных работников Предприятия и ИП не требуется, так как обработка их ПДн осуществляется в целях исполнения договора, одной из сторон которого является субъект ПДн (п.2 ст.6 ФЗ «О персональных данных»). Обработка ПДн в данном случае осуществляется в рамках гражданско-правового договора.

3.3.3.В случае передачи ПДн субъектов третьей стороне Предприятие должно иметь согласие на такую передачу от субъектов ПДн.

3.3.4.При формировании перечня общедоступных ПДн работников Предприятия, для использования ПДн в справочных целях необходимо соответствующие согласие субъектов ПДн.

3.3.5.Формы согласия субъектов ПДн приведены в пп.Г.1 – Г.2. (Приложение Г.)

3.4 **Процессы обработки ПДн**

Обработка ПДн в ИСПДн включает в себя следующие основные процессы:

– сбор ПДн;
– хранение ПДн в ИСПДн;
– предоставление ПДн;
– уточнение ПДн;
– блокирование ПДн;
– уничтожение ПДн.

3.4.1 Сбор ПДн

3.4.1.1 Сбор ПДн различных категорий субъектов ПДн осуществляется работниками различных структурных подразделений Предприятия в рамках выполнения их должностных обязанностей. Распределение ответственности за сбор ПДн между работниками Предприятия приведено в таблице 1.

Табл. 1. Распределение ответственности за сбор ПДн между работниками Предприятия

№ п\п	Категория субъекта ПДн	Подразделение Предприятия, ответственное за сбор ПДн
1	Работники Предприятия	ОО, Бухгалтерия
2	Физические, юридические лица и индивидуальные предприниматели (клиенты Предприятия)	Отдел приватизации жилья; Отдел программного обеспечения; Отдел регистрационного учета граждан; Отдел учета и начислений; Финансово-экономический отдел.

3.4.1.2 Сбор ПДн осуществляется в соответствии со следующими правилами:

– ПДн следует получать лично у граждан за исключением случаев получения ПДн из общедоступных источников;

– в случае возникновения необходимости получения ПДн у третьей стороны следует известить об этом субъекта ПДн заранее, получить его письменное согласие и сообщить о предполагаемых пользователях его ПДн, целях, источниках и способах получения ПДн, а также разъяснить ему установленные законом права субъекта ПДн. Форма уведомления субъекта приведена в п. Е.10 (Приложение Е);

– при отсутствии письменного согласия запрещается получать, обрабатывать и приобщать к личному делу субъекта ПДн данные о его политических, религиозных и иных убеждениях, частной жизни, членстве в общественных объединениях, в том числе в профессиональных союзах;

– не запрашивать информацию о состоянии здоровья субъекта ПДн за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником Предприятия его трудовой функции.

3.4.1.3 Предприятие обязано сообщить субъекту ПДн или его законному представителю информацию о наличии ПДн, относящихся к соответствующему субъекту ПДн, а также предоставить возможность ознакомления с ними при обращении субъекта ПДн или его законного представителя в течение 10 рабочих дней с момента получения соответствующего запроса.

3.4.1.4 По запросу субъекта ПДн Предприятие обязано предоставлять ему необходимые бланки запросов, представленные в Приложение Д.

3.4.1.5 Ответственность за предоставление сведений работникам Предприятия (или их доверенным представителям) несут работники ОО.

3.4.1.6 Ответственность за передачу сведений Клиентам Предприятия (или их доверенным представителям) несут начальники ОРУГ, ОУиН, ОПЖ.

3.4.1.7 В ИСПДн должны обрабатываться только те ПДн, которые удовлетворяют вышеприведенным правилам их получения.

3.4.2 Хранение ПДн в ИСПДн

Хранение ПДн в ИСПДн осуществляется работниками ОПО, ответственными за поддержку и сопровождение данных систем. Распределение ответственности за организацию процесса хранения в различных ИСПДн Предприятия приведено в таблице 2.

Табл. 2. Распределение ответственности за процесс хранения в ИСПДн

№ п\п	ИСПДн	Ответственное структурное подразделение

1	АИС «ЖЭО»	Хранение ПДн в СУБД системы, а также с использованием аппаратных средств, необходимых для функционирования ИСПДн, обеспечивается системными администраторами ОПО. Доступность данных с использованием прикладного ПО системы обеспечивается работниками ОПО.
	ПК «Зеркало»	Хранение ПДн на серверах обеспечивается системными администраторами ОПО. Доступность данных с использованием прикладного ПО системы обеспечивается работниками ОПО.
	АРМ «Бухгалтера»	
	Инфо-Предприятие	
	АРМ «Приватизация»	

3.4.2.1 Хранение ПДн в ИСПДн должно осуществляться в соответствии со следующими требованиями:

– хранение ПДн должно осуществляться таким образом, чтобы в отношении каждой категории ПДн можно было определить места их хранения;

– хранение ПДн должно осуществляться в такой форме, которая позволит определить субъекты ПДн, но по сроку хранения не дольше, чем этого требуют цели обработки ПДн или согласие субъектов ПДн;

– при хранении ПДн в ИСПДн должны соблюдаться условия, позволяющие обеспечить конфиденциальность и сохранность ПДн;

– несанкционированный доступ к ПДн должен быть исключен. Доступ должен быть разрешен только работникам, должность которых включена в Список должностей работников, допущенных к работе с ПДн (Приложение Б.);

– запрещается несанкционированное копирование ПДн на отчуждаемые носители информации.

3.4.2.2 Работники Предприятия, обладающие правом доступа к ПДн, несут ответственность за хранение ПДн на автоматизированных рабочих местах.

3.4.2.3 ОПО обеспечивает информационную безопасность при автоматизированной обработке ПДн с использованием аппаратно-программных средств.

3.4.3 Хранение ПДн на бумажных носителях

3.4.3.1 Бумажные документы, содержащие ПДн клиентов Предприятия, должны храниться в специально отведенных местах, запирающихся на ключ, в сейфах, металлических шкафах и т.п.

3.4.3.2 При работе с документами, содержащими персональные данные, запрещается:

– хранить документы в ящиках стола, оставлять их без присмотра;

– брать документы домой для работы и (или) хранения;

– выносить документы из офиса без разрешения руководителя соответствующего подразделения, кроме сотрудников ОРУГ, действующих в рамках выполнения должностных обязанностей;

– хранить документы вне сейфа без необходимости в процессе работы;

– передавать документы на хранение лицам, не имеющим права доступа к данным документам.

3.4.3.3 Текущее хранение кадровых документов, содержащих ПДн работников, организует ОО.

3.4.3.4 Правовое регулирование порядка и сроков хранения кадровых документов осуществляется на основе «Перечня типовых управленческих документов, образующихся в деятель-

ности организаций, с указанием сроков их хранения», утвержденного Росархивом 6 октября 2000 года. Порядок и сроки хранения трудовых книжек регулирует Постановление Правительства Российской Федерации от 16 апреля 2003 года №225 «О трудовых книжках».

3.4.3.5 Организация текущего хранения кадровых документов определяется номенклатурой дел, утверждаемой приказом Директора Предприятия.

3.4.4 Предоставление ПДн

3.4.4.1 Предоставление ПДн осуществляется в следующих случаях:

– выполнение работниками должностных обязанностей, связанных с обработкой ПДн;

– предоставление ПДн в рамках предприятий (банки, типография), с которыми заключены договоры, предполагающие передачу и обработку ПДн, в целях обеспечения бизнес-процессов Предприятия;

– предоставление ПДн в рамках законодательства Р.Ф.

3.4.4.2 При предоставлении ПДн работниками Предприятия должны быть соблюдены следующие правила:

– несанкционированный доступ к ПДн в процессе предоставления должен быть исключен;

– предоставление ПДн возможно только в том случае, если обеспечивается конфиденциальность передаваемой информации. Если Предприятие на основании договора поручает обработку ПДн третьей стороне, существенным условием договора является обязанность обеспечения третьей стороной конфиденциальности и безопасности ПДн при их предоставлении;

– не сообщать ПДн субъекта ПДн третьей стороне без письменного согласия субъекта (форма согласия приведена в пп. Г.1 – 2. Приложение Г) за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в случаях, предусмотренных законодательством Российской Федерации. Также предоставление ПДн третьей стороне возможно на основании договора, предполагающего обработку и предоставление ПДн субъекта ПДн;

– не сообщать ПДн субъекта ПДн в коммерческих целях без его письменного согласия;

– предупредить лиц, получающих ПДн субъектов ПДн, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено.

3.4.4.3 Предоставить ПДн субъектов ПДн представителям субъектов ПДн в порядке, установленном законодательством Российской Федерации, и ограничивать эту информацию только теми ПДн, которые необходимы для выполнения указанными представителями субъектов ПДн их функций.

3.4.4.4 Не требуется согласие работника Предприятия на передачу его ПДн, если предоставление информации или предоставление документов, содержащих ПДн, предусмотрено законодательством Российской Федерации.

3.4.5 Уточнение, блокирование и уничтожение ПДн

3.4.5.1 В случае выявления недостоверных ПДн или неправомерных действий с ними работником подразделения Предприятия, ответственного за содержание ПДн в соответствующей ИСПДн, в течение 1 рабочего дня должно быть осуществлено блокирование ПДн, относящихся к соответствующему субъекту ПДн, с момента обнаружения таких нарушений на период проверки (уточнения).

3.4.5.2 В случае подтверждения факта недостоверности ПДн на основании документов, представленных субъектом ПДн или его законным представителем либо уполномоченным орга-

ном по защите прав субъектов ПДн, или иных необходимых документов необходимо уточнить ПДн и снять блокирование ПДн.

3.4.5.3 В случае выявления неправомерных действий с ПДн в срок, не превышающий 3 рабочих дней с момента выявления таких действий, необходимо устранить допущенные нарушения. В случае невозможности устранения допущенных нарушений в срок, необходимо уничтожить недостоверные ПДн.

3.4.5.4 В случае уточнения (изменения) ПДн необходимо известить всех лиц, которым ранее были сообщены или переданы неверные или неполные ПДн, обо всех исключениях, исправлениях и дополнениях в них.

3.4.5.5 ПДн подлежат уничтожению (или обезличиванию) в ИСПДн в трехдневный срок (если другое не оговорено согласием субъекта ПДн) по достижении целей их обработки, либо в случае утраты необходимости в достижении этих целей или отзыва субъектом ПДн согласия на обработку своих ПДн, так же в случаях применения мер безопасности в отношении субъектов ПДн в случаях предусмотренных законодательством Российской Федерации.

3.4.5.6 Об устранении допущенных нарушений или об уничтожении ПДн требуется уведомить субъект ПДн или его законного представителя, либо уполномоченный орган по защите прав субъектов ПДн в случае, если соответствующую проверку инициировал указанный орган. Формы уведомлений приведены в п.п. Е.9 и Е.11 (Приложение Е).

3.5 **Обеспечение конфиденциальности ПДн**

3.5.1.Предприятие и другие третьи лица, обладающие правом доступа к ПДн (в рамках выполнения должностных обязанностей или в рамках договора), должны обеспечивать их конфиденциальность путем реализации комплекса организационных и технических мероприятий по защите ПДн.

3.5.2.Предприятие может передавать ПДн субъектов ПДн на обработку третьим лицам (принимающей стороне) только в случае, если это необходимо для достижения целей обработки ПДн. Существенным условием договора является обязанность обеспечения третьей стороной конфиденциальности ПДн и безопасности ПДн при их обработке. В том случае, если договор был заключен до вступления в силу ФЗ «О персональных данных» либо условие конфиденциальности ПДн не было прописано по каким-либо причинам, следует подписывать дополнительное соглашение о неразглашении ПДн, форма которого приведена в Приложение З.

3.5.3.Для обеспечения конфиденциальности и других свойств информационной безопасности ПДн необходимы следующие организационные и технические меры:

– знание требований нормативно–методических документов по защите информации работниками, допущенными к работе с ПДн;

– все работники, имеющие действующие трудовые отношения, деятельность которых связана с получением, обработкой и защитой ПДн, обязаны подписать обязательство о неразглашении ПДн (Приложение М), а также быть ознакомлены под роспись с настоящим Положением;

– периодически сменяемые пароли учетных записей работников, имеющих доступ в ИСПДн;

– наличие межсетевых экранов для защиты ИСПДн от неправомерных воздействий из сети Интернет;

– разделение полномочий пользователей в ИСПДн в зависимости от их должностных обязанностей;

– наличие формализованной процедуры по предоставлению доступа, подразумевающей предварительное получение соответствующей авторизации;

– наличие формализованной процедуры по регулярному пересмотру (ревизии) прав доступа работников в зависимости от занимаемой ими должности;

– регулярное резервное копирование данных ИСПДн;

– наличие отказоустойчивых элементов на серверах, обрабатывающих ПДн.

3.6 **Права субъекта в отношении ПДн, обрабатываемых в ИСПДн Предприятия**

3.6.1 В целях обеспечения защиты ПДн, хранящихся на Предприятии, субъект ПДн имеет право:

– свободного бесплатного доступа к своим персональным данным, включая право на получение копии любой записи, содержащей персональные данные субъекта ПДн, за исключением случаев, предусмотренных федеральными законами. Получение указанной информации о своих персональных данных возможно при личном обращении субъекта ПДн в подразделение Предприятия, ответственное за обработку ПДн в соответствующей ИСПДн;

– требовать удаления или исправления неверных или неполных персональных данных, а также данных, обработанных с нарушением требований Трудового кодекса Российской Федерации и Федерального закона от 27 июля 2006 года №152-ФЗ «О персональных данных». Указанное требование должно быть оформлено письменным заявлением работника на имя Директора Предприятия. Персональные данные оценочного характера работник имеет право дополнить заявлением, выражающим его собственную точку зрения;

– требовать извещения Предприятием всех лиц, которым ранее были сообщены неверные или неполные персональные данные работника, обо всех произведенных в них исключениях, исправлениях или дополнениях;

– обжаловать в суде любые неправомерные действия или бездействие Приедприятия при обработке и защите его персональных данных.

3.6.2.Формы возражений, разъяснений и уведомлений субъекта ПДн приведены в п.п. Е.1 - Е.2 и Е.8 - Е.11 (Приложение Е).

4 Обязательные мероприятия по обеспечению безопасности ИСПДн

4.1 Общие требования

4.1.1.На Предприятии до начала проведения работ по обеспечению безопасности ПДн должна быть проведена инвентаризация ИСПДн путем опроса владельцев ИС на предмет наличия обработки в них ПДн.

4.1.2.После инвентаризации ИС выявляются:

– ИСПДн, в которых осуществляется автоматизированная обработка ПДн;

– ИСПДн, в которых осуществляется неавтоматизированная обработка ПДн.

4.1.3.Все эксплуатируемые ИСПДн с автоматизированной обработкой ПДн должны классифицироваться в соответствии с Приказом ФСТЭК России, ФСБ России и Мининформсвязи России от 13 февраля 2008г. №55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных». Классификация ИСПДн проводится в следующей последовательности:

– приказом Директора Предприятия создается Комиссия по проведению классификации ИСПДн;

– Комиссия в определенный приказом срок устанавливает категории и объем обрабатываемых ПДн в ИСПДн, а также определяет необходимость обеспечения целостности и доступности ПДн, наличие при обработке сведений о состоянии здоровья субъектов, принятия решений, порождающих юридические последствия на основании исключительно автоматизированной обработки ПДн;

– Комиссия формирует Акты классификации для каждой ИСПДн, в которых указывается Перечень обрабатываемых ПДн.

4.1.4.На Предприятии должны быть разработаны Модели угроз для всех ИСПДн, класс которых выше 4. Модель угроз разрабатывается на основе методических документов, утвержденных в соответствии с пунктом 2 Постановления Правительства Российской Федерации от 17 ноября 2007 г. №781.

4.1.5.Выбор и реализация методов и способов защиты информации в ИСПДн осуществляются на основе модели угроз и в зависимости от класса ИСПДн.

4.1.6.Выбранные и реализованные методы и способы защиты ПДн в ИСПДн должны обеспечивать нейтрализацию предполагаемых угроз безопасности ПДн при их обработке в ИСПДн в составе создаваемой системы защиты ПДн.

4.1.7.Для проведения работ по выбору и реализации методов и способов защиты ПДн (включая техническое проектирование системы защиты ПДн, внедрение средств защиты ПДн, сопровождение средств защиты ПДн и т.д.) могут привлекаться подрядные организации, имеющие лицензию на осуществление деятельности по технической защите конфиденциальной информации.

4.1.8.Ответственным за организацию проведения данных мероприятий является ОПО.

4.1.9.Конкретные сроки и процедуры проведения данных мероприятий устанавливаются дополнительными нормативными документами.

4.1.10.Технические требования по защите ПДн в ИСПДн Предприятия приведены в разделе 8.

4.1.11.Требования к физической защите помещений, в которых обрабатываются ПДн, приведены в разделе 7.

4.2 **Требования к разрабатываемым и вводимым в эксплуатацию ИСПДн**

4.2.1.Разработка ИСПДн должна включать следующие стадии:

– предпроектная стадия. Включает предварительный анализ целей и условий функционирования ИСПДн, а также обрабатываемых в ней ПДн, на основании которого определяется предварительный класс ИСПДн, степень участия должностных лиц, актуализируются угрозы безопасности;

– стадия проектирования системы защиты ПДн для ИСПДн;

– стадия ввода в действие ИСПДн.

4.2.2.По результатам проведенного анализа и с учетом действующих требований федерального законодательства и регуляторов должны быть разработаны:

– модель угроз безопасности персональных данных при их обработке в ИСПДн;

– требования к защите персональных данных при их обработке в ИСПДн;

– акт о классификации ИСПДн;

– частное техническое задание на создание системы защиты ПДн для ИСПДн.

4.2.3.Проектирование системы защиты ПДн для вводимой в эксплуатацию ИСПДн должно производиться с учетом уже построенной на Предприятии системы защиты ПДн, включающей комплекс организационных и технических мер.

4.2.4.На стадии ввода в эксплуатацию ИСПДн должны быть проведены следующие мероприятия:

– установка прикладного программного обеспечения ИСПДн совместно со средствами защиты информации (встроенными и наложенными);

– опытная эксплуатация средств защиты информации в комплексе с другими техническими и программными средствами в целях проверки их работоспособности в составе ИСПДн;

– приемо-сдаточные испытания средств защиты информации по результатам опытной эксплуатации.

4.2.5.В случае внедрения дополнительных средств защиты информации должны быть составлены Акты внедрения средств защиты информации по результатам их приемо-сдаточных испытаний.

4.2.6.Перед вводом новой ИСПДн в опытную эксплуатацию должен быть составлен Акт о вводе в опытную эксплуатацию ИСПДн, а также Акт классификации ИСПДн.

4.2.7.В случае успешного функционирования ИСПДн на стадии опытной эксплуатации и принятия решения о переводе ее в промышленную эксплуатацию должен быть составлен Акт о вводе в промышленную эксплуатацию новой ИСПДн.

4.3 **Требования к выводу ИСПДн из эксплуатации**

4.3.1.В случае принятия решения о выводе ИСПДн из промышленной эксплуатации должен быть подписан Акт о выводе ИСПДн из промышленной эксплуатации.

4.3.2.При выводе ИСПДн из промышленной эксплуатации с целью обеспечения справочной поддержки Предприятия доступ к ней должен быть ограничен только определенному составу лиц с правами только на чтение.

4.3.3.После подписания Акта о выводе ИСПДн из промышленной эксплуатации (на основании совместного решения руководителя ОПО, администратора и владельца ИСПДн) ИСПДн должна быть переведена в архивный фонд Предприятия (в соответствии с ч.2 чт.13 ФЗ «Об архивном деле»), при этом должны быть выполнены следующие требования:

– доступ к архивной ИСПДн и хранимым в ней документам должен обеспечиваться на основании соответствующей заявки на имя руководства Предприятия, по согласованию с ОПО и владельцем ИСПДн;

– ПДн, хранящиеся в архиве, могут быть использованы и переданы третьим лицам только в целях исполнения законодательства Российской Федерации;

– должны быть обеспечены финансовые, материально-технические и иные условия, необходимые для комплектования, хранения, учета и использования ИСПДн, включая специальное помещение, отвечающее нормативным условиям труда работников архива;

– доступ в помещения, где предполагается хранение выводимой из эксплуатации ИСПДн, должен быть ограничен;

– должен быть регламентирован перечень лиц, допущенных к работе с ИСПДн, переданной в архив;

– все внешние запоминающие устройства (ленты с резервными копиями, дискеты, CD-диски, флеш-накопители и т.п.), относящиеся к архивной ИСПДн, должны храниться в сейфах;

– должно быть разработано описание ИСПДн, переведенной в архивный фонд Предприятия.

5 Условия обработки ПДн, осуществляемой без использования средств автоматизации

5.1 Общие требования

5.1.1.Работники, осуществляющие обработку ПДн без использования средств автоматизации, до начала обработки должны быть проинформированы о категориях ПДн, об особенностях и правилах обработки ПДн, изложенных в настоящем Положении.

5.1.2.В типовых формах, в которые предполагается внесение ПДн должна содержаться следующая информация:

– цель обработки ПДн, наименование и адрес Предприятия, источник получения ПДн, срок обработки ПДн, перечень действий с ПДн, которые будут совершаться в процессе их обработки;

– поле для проставления субъектом ПДн отметки о согласии на обработку ПДн без использования средств автоматизации.

5.1.3.Типовая форма должна заполняться на каждого субъекта в отдельности.

5.1.4.Ведение реестра, содержащего ПДн, необходимые для однократного пропуска субъекта на территорию, на которой находится Предприятие, может осуществляться после разработки Акта о ведении реестра, в котором определены:

– цели обработки ПДн;

– способы фиксации и состав запрашиваемых у субъекта ПДн;

– перечень лиц (поименно и по должностям), имеющих доступ к реестру и ответственных за ведение реестра;

– сроки обработки ПДн.

Ведение реестра может осуществлять подрядная организация на основании договора. Форма Акта приведена в Приложение Ж.

5.1.5.Носители ПДн не должны оставаться без присмотра. При уходе с рабочего места лицо, ответственное за носители ПДн, должно убирать носители в сейф или шкаф, закрывающийся на ключ.

5.2 Хранение материальных носителей ПДн

5.2.1.Хранение материальных носителей ПДн не может осуществляться в открытом доступе. Хранение материальных носителей ПДн по возможности должно осуществляться в отдельных запираемых помещениях с ограниченным доступом или в запираемых металлических или деревянных шкафах.

5.2.2.Доступ к архивам, хранилищам документации или специально выделенным шкафам, должен быть ограничен, и предоставляться только тем работникам, которые осуществляют работу с материальными носителями ПДн.

5.2.3.Ответственным за предоставление доступа к документам в структурных подразделениях является руководитель подразделения, где осуществляется хранение ПДн.

5.2.4.Хранение копий материальных носителей ПДн должно осуществляться в личных запираемых металлических или деревянных шкафах работников, или их непосредственных руководителей.

5.2.5.Хранение материальных носителей ПДн в открытом доступе в рабочих помещениях подразделений Предприятия и на столах работников допускается только в течение рабочего дня, под персональной ответственностью работника.

6 Порядок взаимодействия с государственными органами

6.1 Предприятие обязано уведомить уполномоченный орган по защите прав субъектов ПДн[1)] о своем намерении осуществлять обработку ПДн субъектов ПДн, с которыми его не связывают договорные отношения.

6.2 Предприятие обязано сообщить в уполномоченный орган по защите прав субъектов ПДн по его запросу информацию, необходимую для осуществления деятельности указанного органа, в течение 7 рабочих дней с даты получения запроса.

6.3 В случае получения запроса или обращения уполномоченного органа по защите прав субъектов ПДн о недостоверности ПДн или неправомерных действиях с ними необходимо исправить выявленные нарушения и уведомить указанный орган об устранении нарушений либо об уничтожении ПДн в случае невозможности устранения нарушений в срок, не превышающий 3 дней.

6.4 В установленных федеральным законодательством случаях Предприятие обязано предоставлять информацию, содержащую обрабатываемые ПДн, по мотивированному запросу уполномоченных органов государственной власти по вопросам их компетенции.

6.5 Запросы на предоставление доступа к обрабатываемым ПДн могут быть обжалованы в судебном порядке в соответствии с законодательством Российской Федерации.

6.6 Контроль и надзор за выполнением требований по обработке ПДн в ИСПДн, установленных Правительством Российской Федерации, осуществляются федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности[2)], и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации[3)], в пределах их компетенции и без права ознакомления с ПДн, обрабатываемыми в комплексе ИСПДн Предприятия.

6.7 Шаблоны документов для взаимодействия с уполномоченным органом по защите прав субъектов ПДн приведены в пп. Е.3 -Е.7 (Приложение Е).

[1)] Роскомнадзор
[2)] ФСБ России
[3)] ФСТЭК России
(наименования уполномоченных органов государственной власти даются на момент написания Положения)

7 Требования к помещениям, в которых обрабатываются персональные данные

7.1 Общие требования

7.1.1. Не допускается нахождение сотрудников МП «ЕРКЦ» в помещениях в нерабочее для них время.

7.1.2. Нахождение клиентов МП «ЕРКЦ» в помещениях МП «ЕРКЦ» допускается только в рабочее время.

7.1.3.В помещения, в которых находится ИСПДн пропускаются:

беспрепятственно – Директор Предприятия и сотрудники, имеющие допуск к работе с персональными данными с целью выполнения должностных обязанностей;

при наличии служебного удостоверения, с разрешения Директора Предприятия или руководителя структурного подразделения, в сопровождении ответственного за обеспечение безопасности персональных данных или руководителя отдела - сотрудники контролирующих органов, сотрудники пожарных и аварийных служб, сотрудники милиции;

ограниченно - сотрудники, не имеющие допуска к работе с персональными данными или не имеющие функциональных обязанностей в помещении, сотрудники сторонних организаций и учреждений для выполнения договорных отношений.

7.2 Посетители допускаются в помещения, в которых находится ИСПДн МП «ЕРКЦ» в рабочее время, в присутствии сотрудников, допущенных к обработке персональных данных.

7.3 В помещениях, в которых происходит обработка и хранение персональных данных, запрещено использование не предусмотренных служебными обязанностями технических устройств, фотографирование, видеозапись, звукозапись, в том числе с использованием мобильных телефонов.

Сетевое оборудование должно быть расположено в местах, недоступных для посторонних лиц (в специальных помещениях, шкафах, коробах).

В помещениях с серверным оборудованием и агрегатами бесперебойного питания должна устанавливаться отдельная система кондиционирования с мощностью достаточной для вывода тепловыделения всего оборудования и систем, размещенных в серверных помещениях.

Помещения, в которых располагаются технические средства комплекса ИСПДн, должны быть оборудованы пожарной сигнализацией и, по возможности, системой газового пожаротушения.

Уборка помещений и обслуживание технических средств комплекса ИСПДн должны осуществляться под контролем ответственных за данные помещения и технические средства лиц с соблюдением мер, исключающих несанкционированный доступ к ПДн, носителям информации, программным и техническим средствам обработки, передачи и защиты информации комплекса ИСПДн.

Размещение устройств вывода информации средств вычислительной техники, информационно-вычислительных комплексов, технических средств обработки графической, видео - и буквенно-цифровой информации, входящих в состав комплекса ИСПДн, в помещениях, в которых они установлены, осуществляется таким образом, чтобы была исключена возможность просмотра посторонними лицами текстовой и графической видовой информации, содержащей ПДн.

В целях предотвращения утечек по техническим каналам, на окнах в помещениях должны быть жалюзи или шторы.

Защита ПДн от утечек по акустическим каналам в помещениях Предприятия не осуществляется, поскольку в соответствии с Моделью угроз ИСПДн данные угрозы признаны не актуальными.

На Предприятии должны быть выделены помещения или запираемые металлические или деревянные шкафы, в которых должно осуществляться хранение материальных носителей ПДн.

8 Обеспечение технической защиты ПДн

8.1 Общие требования

8.1.1.Обеспечение безопасности ПДн при их обработке в ИСПДн должно осуществляться на всех стадиях жизненного цикла ИСПДн и состоять из согласованных мероприятий, направленных на предотвращение (нейтрализацию) и устранение угроз безопасности ПДн в ИСПДн, на минимизацию возможного ущерба, а также мероприятий по восстановлению данных и нормальному функционированию ИСПДн в случае реализации угроз.

8.1.2.В целях защиты ПДн от несанкционированного доступа и иных неправомерных действий мероприятия по организации и техническому обеспечению безопасности ПДн для каждой ИСПДн должны включать:

а) классификацию ИСПДн на основании установленных критериев в соответствии с «Порядком проведения классификации информационных систем персональных данных», утвержденным совместным Приказом ФСТЭК России № 55, ФСБ России № 86 и Мининформсвязи России № 20 от 13.02.2008 г.;

б) выявление и закрытие технических каналов от утечки ПДн на основе анализа и актуализации модели угроз безопасности ПДн;

в) выбор и реализацию методов и способов защиты информации в ИСПДн на основе модели угроз безопасности ПДн и в зависимости от класса ИСПДн;

г) установку, настройку и применение соответствующих программных, аппаратных и программно-аппаратных средств защиты информации;

д) разработку дополнений к трудовым договорам (или должностных инструкций) по обеспечению безопасности ПДн при их обработке в ИСПДн для персонала, задействованного в эксплуатации данной ИСПДн.

8.1.3.Предотвращение утечки ПДн по техническим каналам за счет побочных электромагнитных излучений и наводок, а также за счет электроакустических преобразований реализуется на Предприятии организационными мерами и не требует специальных технических решений, а именно, размещение устройств вывода информации средств вычислительной техники, информационно-вычислительных комплексов, технических средств обработки графической, видео- и буквенно-цифровой информации, входящих в состав информационной системы, в помещениях, в которых они установлены, осуществляется таким образом, чтобы была исключена возможность просмотра посторонними лицами текстовой и графической видовой информации, содержащей ПДн.

8.1.4.Защита ПДн от несанкционированного доступа и иных неправомерных действий при их обработке в ИСПДн должна осуществляться на Предприятии следующими методами и способами:

– реализация разрешительной системы допуска пользователей (обслуживающего персонала) к информационным ресурсам (включая ПДн), ИСПДн и связанным с ее использованием работам, документам;

– ограничение доступа пользователей в помещения, где размещены технические средства, позволяющие осуществлять обработку ПДн, а также где хранятся носители информации, содержащие ПДн;

– разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам (включая ПДн), программным средствам обработки (передачи) и защиты ПДн;

– регистрация действий пользователей и обслуживающего персонала, контроль несанкционированного доступа и действий пользователей, обслуживающего персонала и посторонних лиц в ИСПДн;

– учет и хранение съемных носителей информации с ПДн и их обращение, исключающее хищение, подмену и уничтожение;

– резервирование технических средств, дублирование массивов и носителей ПДн;

– использование защищенных каналов связи, используемых для передачи ПДн;

– размещение технических средств, позволяющих осуществлять обработку ПДн, в пределах контролируемой территории;

– предотвращение внедрения в ИСПДн вредоносных программ (программ-вирусов) и программных закладок.

8.1.5.При организации взаимодействия ИСПДн с информационно-телекоммуникационными сетями международного информационного обмена (сетями связи общего пользования) наряду с методами и способами, указанными в п. 8.1.4, должны применяться следующие дополнительные методы и способы защиты ПДн от несанкционированного доступа:

– межсетевое экранирование с целью управления доступом, фильтрации сетевых пакетов и трансляции сетевых адресов для скрытия структуры ИСПДн;

– обнаружение вторжений в ИСПДн, нарушающих или создающих предпосылки к нарушению установленных требований по обеспечению безопасности ПДн;

– защита ПДн при их передаче по каналам связи;

– использование смарт-карт, электронных замков и других носителей информации для надежной идентификации и аутентификации пользователей;

– использование средств антивирусной защиты;

– централизованное управление системой защиты ПДн.

8.1.6.На Предприятии также могут разрабатываться и применяться другие методы защиты информации от несанкционированного доступа, обеспечивающие нейтрализацию угроз безопасности ПДн.

8.1.7.Конкретные методы и средства защиты ПДн в ИСПДн должны определяться на основании нормативно-методических документов ФСТЭК и ФСБ России исходя из класса ИСПДн и актуальных угроз безопасности ПДн.

8.1.8.Все технические средства защиты информации должны быть снабжены инструкциями по эксплуатации (рекомендациями по использованию).

8.2 **Тестирование функций системы защиты ПДн**

8.2.1.В соответствии с «Положением о методах и способах защиты информации в информационных системах персональных данных», утвержденным Приказом ФСТЭК от 5 февраля 2010 г. № 58, должно проводиться тестирование системы защиты ПДн при изменении программной среды и пользователей ИСПДн с помощью тест-программ, имитирующих попытки несанкционированного доступа.

8.2.2.Ответственным за проведение тестирования функций системы защиты ПДн является администратор ИБ, ответственный за обеспечение безопасности ИСПДн Предприятия.

8.2.3.Инициатором процесса тестирования функций системы защиты ПДн является руководитель ОПО, который направляет ответственным лицам уведомление о необходимости проведения тестирования.

8.3 **Учет электронных носителей ПДн**

8.3.1.ОПО должно проводить учет защищаемых носителей ПДн. К защищаемым носителям ПДн относятся следующие:

– серверы;

– АРМ;

– внешние запоминающие устройства (дискеты, флеш-накопители и т.п.).

8.3.2.Форма учета защищаемых носителей приведена в п. Е.12 и Е.13 (Приложение Е).

8.4 **Порядок восстановления ПДн**

8.4.1.В случае повреждения ПДн владелец ИСПДн направляет заявку администратору ИСПДн (или лицу, его замещающему) на проведение процедуры восстановления ПДн.

8.4.2.Процедура восстановления ПДн включает в себя выполнение следующих действий:

– уведомление пользователей о временном отключении и недоступности восстанавливаемых ПДн или ИСПДн;

– восстановление поврежденных ПДн или ИСПДн, используя эталонные копии (при необходимости);

– настройка средств защиты системы в соответствии с требованиями политики безопасности (при необходимости);

– проверка корректности восстановленных ресурсов ИСПДн;

– уведомление пользователей о возобновлении полной работоспособности ИСПДн и/или доступности ПДн.

8.4.3.В случае невозможности полного восстановления ресурсов администратор ИСПДн уведомляет собственное руководство, АИБ и пользователей о периоде времени, изменения за который были потеряны.

8.4.4.После проведения восстановления ПДн администратор должен предоставить АИБ Отчет о причинах необходимости проведения работ по восстановлению ПДн, который включает в себя:

– Перечень восстановленных ПДн;

– Ресурс, на котором хранились ПДн;

– Причины выхода из строя ресурса;

– Дату и время обращения владельца ИСПДн;

– ФИО владельца ИСПДн (или обратившегося к администратору ИСПДн);

– Время восстановления ПДн;

– ФИО лица, осуществлявшего восстановление ПДн;

– Дату написания Отчета;

– Подпись лица, осуществлявшего восстановление ПДн.

8.4.5.В случае если причина проведения восстановления ресурсов АС относится к инциденту ИБ, необходимо действовать в соответствии с разделом 12 .

8.4.6.Причины, повлекшие за собой необходимость восстановления ресурсов АС, должны быть проанализированы, и, по возможности, предложены меры по исключению повторения такой ситуации.

9 Правила доступа к ПДн

9.1 Работникам Предприятия предоставляется доступ к работе с ПДн исключительно в пределах и объеме, необходимых для выполнения ими своих должностных обязанностей и в соответствии с порядком, установленным настоящим Положением.

9.2 Объем доступа, необходимый для выполнения работниками своих должностных обязанностей, определяется руководителями структурных подразделений Предприятия по согласованию с ОПО.

9.3 Работники Предприятия, которые в силу выполняемых служебных обязанностей постоянно работают с ПДн, получают допуск к необходимым категориям ПДн с установленными правами доступа на срок выполнения ими соответствующих должностных обязанностей на основании Списка должностей работников, допущенных к работе с ПДн, который утверждается Директором Предприятия по представлению ОПО.

9.4 Список должностей работников, допущенных к работе с ПДн для каждой ИСПДн или к резервируемым информационным и аппаратным ресурсам, должен поддерживаться в актуальном состоянии. С этой целью проводятся следующие действия:

– на основании согласованных заявок на предоставление прав доступа ОПО формирует перечень должностных лиц, допущенных к работе с ПДн (или резервируемым информационным и аппаратным ресурсам), для выполнения своих должностных обязанностей. Список должностей работников, допущенных к работе с ПДн, приведен в Приложении Б.;

– каждые шесть месяцев Список должностей, допущенных к работе с ПДн (или резервируемым информационным и аппаратным ресурсам), актуализируется работниками ОО путем анализа категорий работников, которым необходим доступ к ИСПДн.

9.5 Временный или разовый допуск к работе с ПДн в связи со служебной необходимостью может быть получен работником Предприятия по согласованию с Директором предприятия путем подачи заявки на доступ с указанием цели и срока доступа и категорий ПДн, к которым запрашивается доступ.

9.6 Доступ к ПДн может быть прекращен или ограничен в случае:

– нарушения требований настоящего Положения;

– изменения должностных обязанностей или увольнения работника Предприятия по заявке ОО в ОПО.

9.7 Предоставление и прекращение доступа пользователям к ПДн осуществляется администраторами соответствующей ИСПДн.

10 Требования к работникам, допущенным к обработке ПДн

10.1 Общие требования

10.1.1.Все работники Предприятия, которым стали известны ПДн, обрабатывающиеся в ИСПДн Предприятия, должны обеспечивать их конфиденциальность.

10.1.2.Все работники, допущенные к работе с ПДн, а также связанные с эксплуатацией и техническим сопровождением ИСПДн, должны быть под роспись ознакомлены с требованиями настоящего Положения.

10.1.3.На Предприятии должен быть организован процесс обучения работников, допущенных к работе с ПДн, по направлению обеспечения безопасности ПДн. Ответственность за организацию процесса обучения возлагается на ОПО.

10.1.4.В случае нарушения установленного порядка обработки ПДн работники Предприятия несут ответственность в соответствии с разделом 13 настоящего Положения.

10.1.5.Должностные инструкции работников, допущенных к работе с ПДн, должны содержать раздел, описывающий персональную ответственность за нарушение требований по защите ПДн, включая нарушение свойств целостности, конфиденциальности, доступности и установленного порядка обработки ПДн.

10.1.6.Необходимые разделы должностных инструкций работников Предприятия приведены в Приложение И.

10.2 Требования к администраторам ИСПДн и АИБ

10.2.1.Квалификационные требования и детальный перечень прав и обязанностей администраторов ИСПДн и АИБ закрепляются в соответствующих должностных инструкциях, с которыми работники, назначаемые на данные роли, должны быть ознакомлены под роспись.

10.2.2.В обязанности администраторов ИСПДн входит:

– управление учетными записями пользователей комплекса ИСПДн;

– поддержание штатной работы комплекса ИСПДн;

– обеспечение резервного копирования данных;

– обеспечение безопасного хранения резервируемых ПДн;

– установка и конфигурирование аппаратного и программного обеспечения комплекса ИСПДн, не связанного с обеспечением безопасности ПДн в ИСПДн.

10.2.3.В обязанности АИБ входит:

– обеспечение соответствия порядка обработки и обеспечения безопасности ПДн в ИСПДн требованиям по конфиденциальности, целостности и доступности ПДн, предъявляемым к конкретной ИСПДн, и общим требованиям по безопасности ПДн, установленным федеральным законодательством;

– тестирование системы защиты ПДн;

– предоставление сведений о ПДн в рамках проведения учета защищаемых носителей и проведения инвентаризации;

– установка, конфигурирование и администрирование аппаратных и программных СЗИ комплекса ИСПДн;

– учет и хранение отчуждаемых носителей ПДн;

– периодические проверки журналов безопасности;

– анализ защищенности ИСПДн;

– мониторинг порядка обработки ПДн владельцами ИСПДн;

– участие в проведении внутреннего контроля и служебных расследований по фактам нарушения установленного порядка обработки и обеспечения безопасности ПДн.

10.2.4.В целях обеспечения распределения полномочий, реализации взаимного контроля и недопущения сосредоточения, критичных для безопасности ПДн полномочий у одного лица, запрещается совмещать роли администратора ИСПДн и АИБ в лице одного работника.

11 Организация внутреннего контроля обработки и обеспечения безопасности персональных данных

11.1 Цели организации внутреннего контроля

11.1.1. Организация внутреннего контроля процесса обработки ПДн на Предприятии осуществляется в целях изучения и оценки фактического состояния защищенности ПДн, своевременного реагирования на нарушения установленного порядка их обработки, а также в целях совершенствования этого порядка и обеспечения его соблюдения.

11.1.2. Мероприятия по осуществлению внутреннего контроля обработки и обеспечения безопасности ПДн направлены на решение следующих задач:

– обеспечение соблюдения работниками Предприятия требований настоящего Положения и нормативных правовых актов, регулирующих защиту персональных данных;

– оценка компетентности персонала, задействованного в обработке ПДн;

– обеспечение работоспособности и эффективности технических средств ИСПДн и средств защиты ПДн, их соответствия требованиям уполномоченных органов исполнительной власти по вопросам безопасности ПДн;

– выявление нарушений установленного порядка обработки ПДн и своевременное предотвращение негативных последствий таких нарушений;

– принятие корректирующих мер, направленных на устранение выявленных нарушений, как в порядке обработки ПДн, так и в работе технических средств ИСПДн;

– разработка рекомендаций по совершенствованию порядка обработки и обеспечения безопасности ПДн по результатам контрольных мероприятий;

– осуществление контроля за исполнением рекомендаций и указаний по устранению нарушений.

11.2 Проведение контрольных мероприятий

11.2.1.Один раз в год Юридический отдел организует проведение внутреннего контроля обработки и обеспечения безопасности ПДн.

11.2.2.Проведение контрольных мероприятий по обеспечению безопасности ПДн должно включать:

– проведение руководителями подразделений проверок деятельности работников Предприятия, допущенных к работе с ПДн в ИСПДн, на соответствие порядку обработки и обеспечения безопасности ПДн, установленному настоящим Положением, ФЗ «О персональных данных» и другими нормативными правовыми актами;

– проведение администратором ИБ проверок состояния защищенности ПДн, обрабатываемых в ИСПДн, включая проверку доступов пользователей к ПДн, выполнение требований по защите каждой конкретной ИСПДн, корректности работы системы защиты ПДн и т.д.

11.2.3.Все результаты проверок должны быть предоставлены в ОПО для проведения анализов результатов и подготовки соответствующего Отчета о проведении внутреннего контроля обработки и обеспечения безопасности персональных данных. Шаблон Отчета о проведении внутреннего контроля обработки и обеспечения безопасности персональных данных приведен в Приложение Л.

11.2.4.При необходимости должны быть предложены меры по минимизации последствий выявленных угроз ИБ.

12 Действия должностных лиц в случае возникновения нештатных ситуаций

12.1 Под нештатной ситуацией в рамках данного Положения понимается инцидент ИБ, связанный с нарушением свойств конфиденциальности, целостности или доступности ПДн.

12.2 Порядок реагирования должностных лиц на нештатные ситуации включает в себя следующие этапы:

– отслеживание нештатных ситуаций;

– анализ нештатной ситуации;

– информирование о нештатной ситуации;

– минимизация последствий нештатной ситуации;

– анализ причин возникновения нештатной ситуации;

– принятие мер по недопущению аналогичной ситуации.

12.3 Этап отслеживания нештатных ситуаций включает в себя проведение администратором ИБ следующих действий:

– контроль и фиксирование действий нарушителя имеющимися СЗИ;

– корректировка настроек системы защиты ПДн с учетом действий нарушителя;

– определение целей нарушителя (ресурсов ИСПДн, которые могут пострадать от действий нарушителя), найденных уязвимостей в программных и технических средствах ИСПДн;

– изучение и анализ методов и средств, используемых нарушителем.

12.4 Анализ нештатной ситуации осуществляется администратором ИБ и предполагает выявление последствий нештатной ситуации и оценку их значимости для Предприятия.

12.5 На основе собранной информации руководитель ОПО принимает решение:

– о необходимости информирования начальника Юридического отдела;

– о возможных вариантах реагирования на инцидент.

12.6 Информирование начальника Юридического отдела Предприятия о нештатной ситуации возможно только в случае, если ее анализ показал значительность последствий

12.7 Реагирование на инцидент позволяет минимизировать последствия от реализации угрозы ИБ и может включать следующие действия:

– временная остановка работы отдельных компонентов и сервисов ИСПДн с целью прекращения несанкционированных воздействий на них со стороны нарушителя;

– мониторинг действий нарушителя безопасности без прерывания работы ИСПДн с целью сбора доказательств и фактов, необходимых для привлечения нарушителя к ответственности;

– блокирование конкретных IP-адресов и портов на межсетевых экранах и активном сетевом оборудовании;

– отключения серверов и рабочих станций от сети Интернет или ЛВС;

– выключение питания на серверах и АРМ.

12.8 С целью анализа причин возникновения нештатной ситуации АИБ выполняет сбор доказательств по инциденту. Для этого осуществляется копирование журналов регистрации событий, файлов протоколов работы, конфигурационных файлов, сообщений электронной почты и прикрепленных файлов, данных инсталлированных приложений, графических файлов и прочего со всех ресурсов, вовлеченных в инцидент. Также может быть осуществлено создание точных копий жестких дисков («сектор в сектор») АРМ и серверов, вовлеченных в инцидент.

12.9 На основании анализа нештатной ситуации АИБ составляет отчет о произошедшем инциденте, на основании которого руководитель ОПО принимает решение о проведении служебного расследования.

12.10 Ликвидация последствий инцидентов осуществляется администратором ИБ и включает в себя следующее:

– проверку целостности и работоспособности программных и технических средств, вовлеченных в инцидент;

– восстановление работоспособности компонентов ИСПДн;

– установку новых паролей и формирование новых цифровых сертификатов для доступа к ресурсам ИСПДн;

– перенастройку СЗИ с учетом произошедшего инцидента.

12.11 При необходимости для ликвидации последствий могут быть привлечены администраторы ИСПДн.

12.12 В случае выявления фактов несоблюдения условий хранения носителей ПДн и использования СЗИ, которые могут привести к нарушению конфиденциальности ПДн или другим нарушениям, приводящим к снижению уровня защищенности ПДн Предприятия, руководитель ОПО и АИБ должны провести разбирательства по данным фактам в соответствии с порядком, приведенным в Приложение К.

13 Ответственность за нарушения при обработке персональных данных

13.1 Руководство Предприятия несет ответственность за обеспечение конфиденциальности, целостности и доступности ПДн, а также соблюдение прав и свобод субъектов ПДн в отношении их ПДн, в том числе прав на неприкосновенность частной жизни, личную и семейную тайну в соответствии с законодательством Российской Федерации

13.2 Работники Предприятия несут персональную ответственность за не соблюдение требований по обработке и обеспечению безопасности ПДн, установленных настоящим Положением, в соответствии с законодательством Российской Федерации.

13.3 Работник Предприятия может быть привлечен к ответственности в случаях:

– умышленного или неосторожного раскрытия ПДн;

– утраты материальных носителей ПДн;

– нарушения требований настоящего Положения и других нормативных документов Предприятия в части вопросов доступа и работы с ПДн.

13.4 В случаях нарушения установленного порядка обработки и обеспечения безопасности ПДн, несанкционированного доступа к ПДн, раскрытия ПДн и нанесения Предприятию, его работникам и клиентам материального или иного ущерба материального или иного ущерба, виновные лица несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

Приложение А

Перечень информационных систем персональных данных Предприятия

А.1 В Табл. А.1 приведены перечень и описание ИСПДн, в которых обработка ПДн осуществляется с использованием средств автоматизации.

Табл. А.1. ИСПДн Предприятия, в которых осуществляется автоматизированная обработка ПДн

№ п\п	Название ИСПДн	Описание ИСПДн
1	АИС «ЖЭО»	Автоматизированная информационная система, предназначенная для обеспечения паспортного учета населения.
2	ПК «Зеркало»	Программный комплекс ведения кадрового учета в МП «ЕРКЦ»
3	Инфо-Предприятие	Комплексная автоматизированная система, предназначенная для ведения бухгалтерского учета в МП «ЕРКЦ»
4	АРМ «Бухгалтер»	Комплексная автоматизированная система, предназначенная для ведения бухгалтерского учета в МП «ЕРКЦ»
5	АРМ «Приватизация»	Комплексная автоматизированная система, предназначенная для оформления договоров приватизации и социального найма

Приложение Б

Список должностей работников, допущенных к работе с персональными данными МП «ЕРКЦ»

№ п\п	Должность	Цель доступа	АИС «ЖЭО»				АРМ «Бухгалтер»				Инфопредприятие				ПК «Зеркало»				АРМ «Приватизация»				Срок доступа	Примечания
			Ввод	Просмотр	Редактирование	Удаление	Ввод	Просмотр	Редактирование	Удаление	Ввод	Просмотр	Редактирование	Удаление	Ввод	Просмотр	Редактирование	Удаление	Ввод	Просмотр	Редактирование	Удаление		
I.Управление																								
1	Директор	Контроль за деятельностью предприятия										X				X							До увольнения или изменения должностных обязанностей.	
2	Заместитель директора											X				X								
3	Ведущий инженер по экономической безопасности											X				X								
II.Финансово – экономический отдел																								
1	Оператор ЭВМ	Ввод данных					X																До увольнения или изменения должностных обязанностей.	
III.Бухгалтерия																								
1	Главный бухгалтер	Формирование внешней финансовой отчетности. Выдача доверенностей и ведение отчетных документов.									X	X	X	X									До увольнения или изменения должностных обязанностей.	
2	Заместитель главного бухгалтера										X	X	X	X										
3	Ведущий бухгалтер										X	X	X	X	X	X	X	X						
4	Бухгалтер										X	X	X	X										

Продолжение списка

№ п\п	Должность	Цель доступа	АИС «ЖЭО»				АРМ «Бухгалтер»				Инфопредприятие				ПК «Зеркало»				АРМ «Приватизация»				Срок доступа	Примечания
			Ввод	Просмотр	Редактирование	Удаление	Ввод	Просмотр	Редактирование	Удаление	Ввод	Просмотр	Редактирование	Удаление	Ввод	Просмотр	Редактирование	Удаление	Ввод	Просмотр	Редактирование	Удаление		
IV.Общий отдел																								
1	Начальник отдела	Ведение кадрового учета. Предоставление справочной информации.													X	X	X	X					До увольнения или изменения должностных обязанностей.	
2	Старший инспектор по кадрам														X	X	X	X						
V.Отдел учета и начислений																								
1	Начальник отдела						X	X	X	X													До увольнения или изменения должностных обязанностей.	
2	Заместитель начальника отдела						X	X	X	X														
3	Бухгалтер I категории						X	X	X	X														
4	Бухгалтер II категории						X	X	X	X														
5	Ведущий бухгалтер						X	X	X	X														
VI.Отдел приватизации жилья																								
1	Начальник отдела	Контроль за деятельностью отдела																	X	X	X	X	До увольнения или изменения должностных обязанностей.	
2	Инженер	Обеспечение процесса проведения																	X	X	X	X		
VII.Отдел регистрационного учета граждан																								
1	Начальник отдела	Обеспечение паспортного учета населения	X	X	X	X																	До увольнения или изменения должностных	
2	Заместитель начальника отдела		X	X	X	X																		

																						обязанностей.	

Продолжение списка

№ п\п	Должность	Цель доступа	АИС «ЖЭО»				АРМ «Бухгалтер»				Инфопредприятие				ПК «Зеркало»				АРМ «Приватизация»				Срок доступа	Примечания
			Ввод	Просмотр	Редактирование	Удаление	Ввод	Просмотр	Редактирование	Удаление	Ввод	Просмотр	Редактирование	Удаление	Ввод	Просмотр	Редактирование	Удаление	Ввод	Просмотр	Редактирование	Удаление		
3	Начальник участка	Обеспечение паспортного учета населения	X	X	X	X																	До увольнения или изменения должностных обязанностей.	
4	Паспортист		X	X	X	X																		
5	Инженер участка		X	X	X	X																		
VIII.Абонентский отдел																								
1	Начальник отдела							X															До увольнения или изменения должностных обязанностей	
VIII.Отдел программного обеспечения																								
1	Начальник отдела	Поддержка и сопровождение ИСПДн.	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	До увольнения или изменения должностных обязанностей.	
2	Ведущий программист (администратор БД)						X	X	X	X														
3	Инженер-программист первой категории (администратор БД ОРУГ)		X	X	X	X																		

Приложение В

Перечень нормативных документов

В.1 Основными нормативными правовыми и методическими документами, на которых основывается настоящее Положение:

– Федеральный Закон от 27.07.2006 г. № 152-ФЗ «О персональных данных» (далее – ФЗ «О персональных данных»), устанавливающий основные принципы и условия обработки ПДн, права, обязанности и ответственность участников отношений, связанных с обработкой ПДн;

– «Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденное Постановлением Правительства Российской Федерации от 17.11.2007 г. № 781;

– «Порядок проведения классификации информационных систем персональных данных», утвержденный совместным Приказом ФСТЭК России № 55, ФСБ России № 86 и Мининформсвязи России № 20 от 13.02.2008 г.;

– «Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», утвержденное Постановлением Правительства Российской Федерации от 15.09.2008 г. № 687;

– «Требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных», утвержденные Постановлением Правительства Российской Федерации от 06.07.2008 г. № 512;

В.2 Нормативно-методические документы Федеральной службы по техническому и экспертному контролю Российской Федерации (ФСТЭК России) по обеспечению безопасности ПДн при их обработке в ИСПДн:

– «Положение о методах и способах защиты информации в информационных системах персональных данных», утвержденное Приказом Директора ФСТЭК России от 5 февраля 2010 г. № 58.

В.3 Внутренние нормативные документы Предприятия:

– Приказ о приведении систем в соответствии со 152 ФЗ;

– Положение о порядке обработки персональных данных работников МП «ЕРКЦ».

Приложение Г

Формы согласия субъектов

Г.1 Форма согласия работника МП «ЕРКЦ»

Я, _____,

(Фамилия Имя Отчество субъекта персональных данных полностью)

основной документ, удостоверяющий личность_____

_____,

(вид, номер, сведения о дате выдачи указанного документа и выдавшем его органе)

проживающий по адресу

_____

_____,

настоящим даю свое согласие МП «ЕРКЦ», расположенному по адресу: Челябинская область, г. Магнитогорск, ул. Ленинградская, 17, далее — «Оператор», на автоматизированную и неавтоматизированную обработку моих персональных данных, (см. п.3) на следующих условиях:

1. Согласие дается мною в целях осуществления трудовых (договорных) отношений с МП «ЕРКЦ», соблюдения федеральных законов и иных нормативно-правовых актов Российской Федерации.

2. Настоящее согласие дается на осуществление следующих действий в отношении моих персональных данных, которые необходимы для достижения указанных выше целей, включая, без ограничения: сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передача), обезличивание, блокирование, уничтожение, передачу моих персональных данных, а также любых иных действий с учетом действующего законодательства РФ.

3. Типовой перечень персональных данных передаваемых Оператору на обработку:

3.1. фамилию имя отчество;

3.2. ИНН;

3.3. СНИЛС (№ страхового пенсионного свидетельства);

3.4. табельный номер;

3.5. пол;

3.6. номер, дата трудового договора;

3.7. дата рождения;

3.8. место рождения;

3.9. гражданство;

3.10. наименование и степень знания иностранного языка;

3.11. образование (среднее (полное) общее, начальное профессиональное, среднее профессиональное, высшее профессиональное, аспирантура, адъюнктура, докторантура);

3.12. наименование образовательного учреждения;

3.13. наименование, серия, номер, дата выдачи, направление или специальность, код по ОКСО, ОКИН документа об образовании, о квалификации или наличии специальных знаний

3.14. профессия (в т.ч. код по ОКПДТР);

3.15. стаж работы;

3.16. состояние в браке;

3.17. состав семьи, с указанием степени родства, фамилии, имени, отчества, года рождения ближайших родственников;

3.18. данные документа, удостоверяющего личность (вид, серия, номер, дата выдачи, наименование органа, выдавшего документ);

3.19. адрес и дата регистрации;

3.20. фактический адрес места жительства;

3.21. телефон;

3.22. сведения о воинском учете (категория запаса, воинское звание, состав (профиль), полное кодовое обозначение ВУС; категория годности к военной службе, наименование военного комиссариата по месту жительства, состоит на воинском учете, отметка о снятии с учета);

3.23. дата приема на работу;

3.24. характер работы;

3.25. вид работы (основной, по совместительству);

3.26. структурное подразделение;

3.27. занимаемая должность (специальность, профессия), разряд, класс (категория) квалификации;

3.28. ранее занимаемая должность;

3.29. тарифная ставка (оклад), надбавка, руб.

3.30. основание трудоустройства;

3.31. личная подпись сотрудника;

3.32. фотография;

3.33. сведения об аттестации (дата, решение, номер и дата документа, основание);

3.34. сведения о профессиональной подготовке (дата начала и окончания переподготовки, специальность (направление, профессия, наименование, номер, дата документа свидетельствующего о переподготовке, основание переподготовки);

3.35. сведения о наградах, поощрениях, почетных званиях (наименование, номер, дата награды);

3.36. сведения об отпусках (вид, период работы, количество дней, дата начала и окончания, основание);

3.37. сведения о социальных льготах, на которые работник имеет право в соответствии с законодательством (наименование льготы, номер, дата выдачи документа, основание);

3.38. сведения об увольнении (основания, дата, номер и дата приказа);

3.39. объем работы;

3.40. повышение оклада за вредность в %, в руб;

3.41. месячный фонд ЗПЛ (в т.ч. по должностному окладу и районным коэффициентом);

3.42. надбавка за стаж в %, в руб. в г/м/д;

и подтверждаю, что давая такое согласие, я действую своей волей и в своих интересах.

4. В перечень (источник) общедоступных персональных данных работников МП «ЕРКЦ», могут быть включены следующие мои персональные данных (Согласно ст.8 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных»):

4.1. Фамилия, имя, отчество;

4.2. Дата рождения;

4.3. Год рождения;

4.4. Должность;

4.5. Подразделение;

4.6. Номер кабинета;

4.7. Номер телефона (внешний и внутренний);

4.8. Номер факса;

4.9. Адрес электронной почты.

5. Третьим лицам (ОАО «Кредит Урал Банк»), с целью начисления заработной платы, могут быть переданы следующие категории моих персональных данных:

5.1. Данные, включенные в перечень (источник) общедоступных персональных данных;

5.2. Номер счета;

5.3. Сумма к зачислению.

6. Субъект персональных данных по письменному запросу имеет право на получение информации, касающейся обработки его персональных данных (в соответствии с п.4 ст. 14 ФЗ №152 от 27.06.2006г.).

7. Настоящее согласие дается до истечения сроков хранения соответствующей информации или документов содержащих вышеуказанную информацию, определяемых, в соответствии с ФЗ РФ от 22.10.2004 N 125-ФЗ «Об архивном деле в Российской Федерации» и «Перечнем типовой управленческой документации» (75 лет), после чего персональные данные уничтожаются или обезличиваются.

8. Согласие может быть отозвано путем направления соответствующего письменного уведомления в адрес Оператора по почте заказным письмом, с уведомлением о вручении, либо вручен лично под расписку представителю Оператора, после чего Оператор обязуется в течение 3 (Трех) месяцев уничтожить, либо обезличить персональные данные Субъекта.

Г.2 Форма согласия физических лиц (клиентов МП «ЕРКЦ»)

Я, _____,

(Фамилия Имя Отчество субъекта персональных данных полностью)

основной документ, удостоверяющий личность_____

_____,

(вид, номер, сведения о дате выдачи указанного документа и выдавшем его органе)

проживающий по адресу

_____

_____,

настоящим даю свое согласие МП «ЕРКЦ», расположенному по адресу: Челябинская область, г. Магнитогорск, ул. Ленинградская, 17, далее — «Оператор, на автоматизированную и неавтоматизированную обработку моих персональных данных, (см. п.3) на следующих условиях:

1. Согласие дается мною в целях осуществления договорных отношений с МП «ЕРКЦ», в том числе: формирование счетов на оплату, учет показаний приборов учета пожарно-питьевой воды (водомеров), ведение регистрационного учета граждан, идентификацию субъекта персональных данных в информационных системах персональных данных МП «ЕРКЦ», обеспечение справочной поддержки, а также другие процессы, связанные с деятельностью МП «ЕРКЦ» в рамках действующего законодательства, соблюдения федеральных законов и иных нормативно-правовых актов Российской Федерации.

2. Настоящее согласие дается на осуществление следующих действий в отношении моих персональных данных, которые необходимы для достижения указанных выше целей, включая, без ограничения: сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, предоставление (распространение, передача), обезличивание, блокирование, уничтожение, передачу моих персональных данных третьим лицам, а также любых иных действий с учетом действующего законодательства РФ.

3. Типовой перечень персональных данных передаваемых Оператору на обработку:

3.1.Фамилия, имя, отчество;

3.2.Адрес;

3.3.Паспортные данные (номер, серия, дата выдачи, кем выдан);

3.4.Номер телефона (городской, мобильный);

3.5.Адрес электронной почты;

3.6.Индивидуальный номер налогоплательщика (ИНН);

3.7.Данные о льготных документах (вид, номер, серия, дата выдачи, кем выдан);

3.8.Данные о выставленных счетах (ежемесячные начисления);

3.9.Информация об оплатах (сумма периодических оплат);

3.10.Информация о нарушениях и актах.

4.В случае необходимости подачи искового заявления мои персональные данные могут дополнительно включать:

4.1.ФИО ответчика (для ответчиков – физических лиц);

4.2.Наименование ответчика (для ответчиков - юридических лиц);

4.3.Адрес ответчика;

4.4.Сумма и госпошлина для составления искового заявления;

4.5.Сумма и госпошлина по исполнительному листу для взыскания.

5. Третьим лицам: органам местного самоуправления, органам государственной власти, муниципальным автономным учреждениям, управляющим компаниям, ресурсоснабжающим организациям, кредитным организациям, Государственным учреждениям здравоохранения (ГУЗ), Федеральным бюджетным учреждениям (ФБУ), Отделениям военных комиссариатов (ОВК), а также другим контрагентам в рамках действующего законодательства в пределах их осведомленности могут быть переданы все категории моих персональных данных.

6. Согласие действует: до утраты правовых оснований обработки персональных данных.

Приложение Д

Шаблоны запросов

Д.1 Форма требования о блокировании ПДн

Оператору персональных данных:
Муниципальному предприятию
муниципального образования г. Магнитогорска
«Единый расчетно-кассовый центр».
Адрес: Челябинская область, г. Магнитогорск,
ул. Ленинградская, 17

От _____
(фамилия, имя, отчество)

паспорт _____ выданный _____
(номер) (дата выдачи)

_____
(место выдачи паспорта)

Адрес: _____
(адрес места жительства)

Требование о блокировании персональных данных

В соответствии с положениями ст. 14 и ст. 21 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных» прошу осуществить блокирование моих персональных данных в связи с тем, что:

_____
(указать причину: персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки; с персональными данными совершаются неправомерные действия – указать какие; иная причина – указать)

_____ _____
(дата) (подпись)

Д.2 Форма требования об уничтожении ПДн

Оператору персональных данных:

Муниципальному предприятию муниципального образования г. Магнитогорска «Единый расчетно-кассовый центр».

Адрес: Челябинская область, г. Магнитогорск, ул. Ленинградская, 17.

От _____
(фамилия, имя, отчество)

паспорт _____ выданный _____
(номер) (дата выдачи)

_____
(место выдачи паспорта)

Адрес: _____
(адрес места жительства)

Требование об уничтожении персональных данных

В соответствии с положениями ст. 14 и ст. 21 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных» прошу уничтожить мои персональные данные в связи с тем, что:

_____
(указать причину: я отзываю согласие на обработку своих персональных данных; персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки; с персональными данными совершаются неправомерные действия – указать какие; иная причина – указать)

_____ _____
(дата) (подпись)

Д.3 Форма требования об уточнении ПДн

Оператору персональных данных:

Муниципальному предприятию муниципального образования г. Магнитогорска «Единый расчетно-кассовый центр».

Адрес: Челябинская область, г. Магнитогорск, ул. Ленинградская, 17.

От _____
(фамилия, имя, отчество)

паспорт _____ выданный _____
(номер) (дата выдачи)

_____
(место выдачи паспорта)

Адрес: _____
(адрес места жительства)

Требование об уточнении персональных данных

В соответствии с положениями ст. 14 и ст. 21 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных» и на основании:

_____
(документ(ы) на основании которого(ых) оператор обязан уточнить персональные данные)

Прошу произвести уточнение моих персональных данных согласно представленным документам.

_____ _____
(дата) (подпись)

Д.4 Форма заявления об отзыве согласия на обработку ПДн

Оператору персональных данных:

Муниципальному предприятию муниципального образования г. Магнитогорска «Единый расчетно-кассовый центр».

Адрес: Челябинская область, г. Магнитогорск, ул. Ленинградская, 17.

От _____
(фамилия, имя, отчество)

паспорт _____ выданный _____
(номер) (дата выдачи)

_____
(место выдачи паспорта)

Адрес: _____
(адрес места жительства)

ЗАЯВЛЕНИЕ

об отзыве согласия на обработку

персональных данных

Прошу прекратить обработку моих персональных данных, осуществляемую в целях: _____
(цели обработки персональных данных, в отношении которых отзывается согласие)

по причине: _____
(НЕОБЯЗАТЕЛЬНО: указать причину отзыва согласия)

_____ _____
(дата) (подпись)

Д.5 Форма запроса на предоставление сведений об операторе ПДн

Оператору персональных данных:
Муниципальному предприятию муниципального образования г. Магнитогорска «Единый расчетно-кассовый центр».

Адрес: Челябинская область, г. Магнитогорск, ул. Ленинградская, 17.

От _____
(фамилия, имя, отчество)

паспорт _____ выданный _____
(номер) (дата выдачи)

_____
(место выдачи паспорта)

Адрес: _____
(адрес места жительства)

Запрос на предоставление сведений об операторе персональных данных

В соответствии со ст. 14 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных» прошу подтвердить факт обработки моих персональных данных и предоставить следующие сведения:

– способы обработки моих персональных данных;

– сведения о лицах, которые имеют доступ к моим персональным данным или которым может быть предоставлен такой доступ;

– перечень относящихся ко мне персональных данных и источник их получения;

– сроки обработки моих персональных данных, в том числе сроки их хранения;

– сведения о том, какие юридические последствия может повлечь за собой обработка моих персональных данных.

Указанные сведения прошу предоставить:

– на бумаге по адресу:_____

– по адресу электронной почты:_____

_____ _____
(дата) (подпись)

Д.6 Форма возражения против решения, принятого на основании исключительно автоматизированной обработки ПДн

Оператору персональных данных:
муниципальному предприятию
муниципального образования г. Магнитогорска
«Единый расчетно-кассовый центр».
Адрес: Челябинская область, г. Магнитогорск, ул. Ленинградская, 17.

От _____
(фамилия, имя, отчество)

паспорт _____ выданный _____
(номер) (дата выдачи)

_____
(место выдачи паспорта)

Адрес: _____
(адрес места жительства)

ВОЗРАЖЕНИЕ

против решения, принятого на основании

исключительно автоматизированной обработки персональных данных

Прошу отменить решение о _____
(решение, против которого подается возражение)

принятое при обработке моих персональных данных в исключительно автоматизированном режиме в целях:

_____
(цель обработки персональных данных с принятием решений на основании исключительно автоматизированной обработки)

поскольку: _____
(причина несогласия с принятым решением)

_____ _____
(дата) (подпись)

Приложение Е

Дополнительные шаблоны (уведомлений, разъяснений и т.д.)

Е.1 Отказ в предоставлении сведений

Субъекту персональных данных:
(ФИО)

Адрес:

ОТКАЗ
в предоставлении сведений

Оператор персональных данных: муниципальное предприятие муниципального образования г. Магнитогорска «Единый расчетно-кассовый центр».

Адрес: Челябинская область, г. Магнитогорск, ул. Ленинградская, 17.

Вам отказано в предоставлении сведений по запросу от _____
(дата запроса)

на основании _____
(ссылка на нормы ФЗ «О персональных данных» или иных федеральных законов)

_____ _____ _____
(должность) (подпись) (Ф.И.О.)

«__» _____ 20__ г.

Е.2 Разъяснение порядка принятия решений на основании исключительно автоматизированной обработки ПДн

Субъекту персональных данных:

(ФИО)

Адрес:

РАЗЪЯСНЕНИЕ

порядка принятия решений на основании исключительно автоматизированной обработки персональных данных

Оператор персональных данных МП «ЕРКЦ»,

находящийся по адресу: Челябинская область, г. Магнитогорск, ул. Ленинградская, 17

руководствуясь[1]: _____

(правовое основание обработки персональных данных)

с целью: _____

(цель обработки персональных данных)

осуществляет обработку Ваших персональных данных, включая:

_____

_____

(перечисление персональных данных, находящихся в обработке: ФИО, адрес, телефон…)

Указанные персональные данные обрабатываются в информационных системах оператора, как с использованием средств автоматизации, так и без их использования. В ходе автоматизированной обработки персональных данных могут совершаться следующие действия:

_____

_____

(действия с персональными данными, которые совершаются в ходе автоматизированной обработки)

При выполнении указанных действий, Оператор не принимает решений, порождающих юридические последствия для субъекта персональных данных, основываясь исключительно на автоматизированной обработке персональных данных.

_____ _____ _____

(должность) (подпись) (Ф.И.О.)

«__» _____ 20__ г.

[1)] В соответствии с требованиями федерального законодательства РФ, в том числе: Гражданским (ведение бухгалтерского учета), Трудовым (обеспечение необходимых условий труда работников) и Налоговым (регистрация ИНН, ведение налогового учета) кодексов РФ.

Е.3 Уведомление о внесении изменений в ПДн

(на имя руководителя территориального управления Роскомнадзора, субъекта персональных данных, либо его представителя, либо третьего лица, которому были сообщены неверные данные)

Руководителю территориального Управления
Федеральной службы по надзору
в сфере связи, информационных технологий и
массовых коммуникаций
по Челябинской области

УВЕДОМЛЕНИЕ

о внесении изменений в персональные данные

Тип оператора: юридическое лицо

Наименование: МП «ЕРКЦ»

Адрес: Челябинская область, г. Магнитогорск, ул. Ленинградская, 17

действующее в соответствии с[1)]: _____
(правовое основание обработки персональных данных)

в отношении персональных данных: _____
(имя субъекта персональных данных)

на основании: _____
(основание внесения изменений в персональные данные)

внесло следующие изменения:

наименование	**исходное значение**	**изменено**
(наименование категории персональных данных: ФИО, адрес, телефон и т.п.)	(исходное значение)	(новое значение)

Указанные персональные данные вводятся в обработку с учетом внесенных изменений с _____
(дата возобновления обработки)

Срок или условие прекращения обработки персональных данных _____

_____ _____ _____
(должность) (подпись) (Ф.И.О.)

«__» _____ 20__ г.

[1)] В соответствии с требованиями федерального законодательства РФ, в том числе: Гражданским (ведение бухгалтерского учета), Трудовым (обеспечение необходимых условий труда работников) и Налоговым (регистрация ИНН, ведение налогового учета) кодексов РФ.

Е.4 Уведомление об изменениях в реквизитах оператора ПДн

Руководителю территориального Управления
Федеральной службы по надзору
в сфере связи, информационных технологий и
массовых коммуникаций
по Челябинской области

УВЕДОМЛЕНИЕ

об изменениях в реквизитах оператора персональных данных

Тип оператора:	юридическое лицо
Наименование оператора:	Муниципальное предприятие муниципального образования г. Магнитогорска «Единый расчетно-кассовый центр» (МП «ЕРКЦ»)
Адрес оператора:	Челябинская область, г. Магнитогорск, ул. Ленинградская, 17

Сведения об операторе персональных данных МП «ЕРКЦ», представленные Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций в Уведомлении об обработке персональных данных (о намерении осуществлять обработку персональных данных), претерпели изменения.

Ниже представлены актуальные данные для внесения в Реестр операторов персональных данных.

Наименование оператора: _____

Адрес оператора: _____

Правовое основание обработки персональных данных: _____

Цели обработки персональных данных: _____

Категории персональных данных: _____

Категории субъектов персональных данных: _____

Перечень действий с персональными данными: _____

Меры по обеспечению безопасности персональных данных: _____

_____	_____	_____
(должность)	(подпись)	(Ф.И.О.)

«__» _____ 20__ г.

Е.5 Уведомление об обработке ПДн (о намерении осуществлять обработку ПДн)

Руководителю территориального Управления
Федеральной службы по надзору
в сфере связи, информационных технологий и массовых коммуникаций
по Челябинской области

УВЕДОМЛЕНИЕ
об обработке персональных данных

Тип оператора:	Юридическое лицо
Наименование оператора:	Муниципальное предприятие муниципального образования г. Магнитогорска «Единый расчетно-кассовый центр»
Сокращенное наименование оператора:	МП «ЕРКЦ»
Адрес оператора:	Челябинская область, г. Магнитогорск, ул. Ленинградская, 17
ИНН:	7446041952
ОГРН:	1027402167704
ОКПО	32520304
Филиалы:	отсутствуют
Правовое основание обработки персональных данных:	руководствуясь гл. 2, гл. 4, гл. 5 Федеральным законом № 152-ФЗ «О персональных данных» от 27.07.2006 г., ст. 85-90 Трудовым Кодексом РФ, Федеральным законом от 02.05.2006 г. № 59-ФЗ "О порядке рассмотрения обращений граждан РФ", гл. 48 Гражданского Кодекса РФ, Постановлением Правительства РФ от 17.11.2007 г. № 781 «Об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», постановлением главы города от 15.01.2004 г. № 11-П, постановлением городского Собрания депутатов от 24.12.2003 г. №149
Цели обработки персональных данных:	с целью осуществления деятельности по приему платежей физических лиц, начислению, обработки платежей, перечисления платежей поставщикам, организации трудовых отношений с работниками оператора, обеспечения соблюдения законов и иных нормативно-правовых актов

Категории персональных данных:	Персональные данные, позволяющие идентифицировать субъекта ПДн и получить о нем дополнительную информацию, включая: 1 Фамилия, имя, отчество; 2 Адрес; 3 Паспортные данные (номер, серия, дата выдачи, кем выдан); 4 Дата рождения; 5 Год рождения; 6 Пол; 7 Место рождение; 8 Гражданство; 9 Подразделение; 10 Должность; 11 Дата приема на работу; 12 Табельный номер; 13 Номер банковского счета и реквизиты банка; 14 Доходы (заработная плата); 15 Номер кабинета; 16 Номер факса; 17 Номер телефона (городской, мобильный); 18 Адрес электронной почты; 19 Индивидуальный номер налогоплательщика (ИНН); 20 Категория инвалидности; 21 Код страхового свидетельства пенсионного фонда; 22 Данные о льготных документах (вид, номер, серия, дата выдачи, кем выдан); 23 Данные о выставленных счетах (ежемесячные начисления); 24 Информация об оплатах (сумма периодических оплат); 25 Информация о нарушениях и актах. 26 Сумма и госпошлина для составления искового заявления; 27 Сумма и госпошлина по исполнительному листу для взыскания. 28 Данные о родственниках.
Категории субъектов, персональные данные которых обрабатываются	физические лица, состоящие в трудовых отношениях с оператором, физические лица, являющиеся потребителями услуг, оказываемых управляющими организациями, состоящими в договорных отношениях и иных гражданско-правовых отношениях с оператором
Перечень действий с персональными данными, общее описание используемых оператором способов обработки персональных данных	обработка вышеуказанных персональных данных будет осуществляться путем сбора, систематизации, накопления, хранения, уточнения, использования, распространения, обезличивания, смешанной обработки персональных данных. Обработка персональных данных: смешанная; с передачей по внутренней сети юридического лица
Осуществление трансграничной передачи персональных данных	Не осуществляется

Описание мер, предусмотренных статьями 18.1. и 19 Федерального закона: «О персональных данных»	назначение ответственного за организацию обработки персональных данных; издание Положения об обработке персональных данных; применение правовых, организационных и технических мер по обеспечению безопасности персональных данных; ознакомление работников, непосредственно осуществляющих обработку персональных данных; осуществление внутреннего контроля соответствия обработки персональных данных Федеральному закону и принятым в соответствии с ним нормативными правовыми актами;
Ответственный за организацию обработки персональных данных	
Номера контактных телефонов, почтовые адреса и адреса электронной почты	
Сведения об обеспечении безопасности персональных данных в соответствии с требованиями к защите персональных данных, установленными Правительством РФ	Безопасность персональных данных обеспечивается техническими мерами, включая использование средств физического контроля доступа в помещения, разграничение доступа работников к персональным данным, использование средств межсетевого экранирования для сегментирования и отделения внутренней корпоративной сети от сети Интернет, применение средств антивирусной защиты, средств резервного копирования данных, а также организационными мерами, установленными локальными нормативными актами.
Дата начала обработки персональных данных	12.02.2004г.
Срок или условие прекращения обработки персональных данных	Утрата правовых оснований обработки персональных данных

_____ _____

(должность) (Ф.И.О.)

«__» _____ 20__ г.

Е.6 Уведомление об уничтожении ПДн

Руководителю территориального Управления
Федеральной службы по надзору в сфере связи,
информационных технологий и массовых ком-
муникаций
по Челябинской области

УВЕДОМЛЕНИЕ
об уничтожении персональных данных

Тип оператора: юридическое лицо

Наименование: МП «ЕРКЦ»

Адрес: Челябинская область, г. Магнитогорск, ул. Ленинградская, 17

Руководствуясь: _____
(правовое основание обработки персональных данных)

в целях: _____
(цель обработки персональных данных)

осуществлял обработку следующих категорий персональных данных:

_____

_____
(перечень ПДн, включая специальные категории ПДн и биометрические ПДн при их наличии)

принадлежащих _____
(имя субъекта персональных данных)

_____
(если имеются, дополнительные сведения для идентификации: дата рождения / адрес…)

с _____ по _____
(дата начала обработки персональных данных) (дата прекращения обработки)

Обработка вышеуказанных персональных данных оператором была прекращена, а сами данные уничтожены в связи с:

_____
(причина прекращения обработки персональных данных: окончание срока обработки или событие, с которым связано достижение цели или утрата необходимости обработки)

_____ _____ _____
(должность) (подпись) (Ф.И.О.)

«__» _____ 20__ г.

Е.7 Уведомление об устранении нарушений в порядке обработке ПДн

Руководителю территориального Управления
Федеральной службы по надзору в сфере связи,
информационных технологий и массовых коммуникаций
по Челябинской области

УВЕДОМЛЕНИЕ
об устранении нарушений в порядке обработки персональных данных

Тип оператора: юридическое лицо

Наименование: МП «ЕРКЦ»

Адрес: Челябинская область, г. Магнитогорск, ул. Ленинградская, 17

В отношении порядка обработки персональных данных, принадлежащих:

_____

_____

(имя субъекта персональных данных и дополнительные сведения для идентификации, если имеются: дата рождения / адрес…)

Были допущены следующие нарушения:

_____

(указать выявленные нарушения)

Указанные нарушения были устранены _____

(дата устранения нарушений)

на основании: _____

(правовое основание устранения выявленных нарушений)

Персональные данные вновь вводятся в обработку с _____

(дата ввода в обработку)

Срок или условие прекращения обработки персональных данных:

_____

_____ _____ _____

(должность) (подпись) (Ф.И.О.)

«__» _____ 20__ г.

Е.8 Уведомление субъекта о блокировании ПДн

Субъекту персональных данных:
(ФИО)

Адрес:

УВЕДОМЛЕНИЕ
о блокировании персональных данных

Оператор персональных данных МП «ЕРКЦ»,
находящийся по адресу: Челябинская область, г. Магнитогорск, ул. Ленинградская, 17
осуществил блокирование Ваших персональных данных, включая:

_____

_____
(перечисление блокированных персональных данных: ФИО, адрес, телефон…)

которые обрабатывались в целях: _____
(цель обработки указанных персональных данных)

Указанные персональные данные были заблокированы _____
(дата блокирования)

в связи с: _____
(причина блокирования персональных данных)

_____ _____ _____
(должность) (подпись) (Ф.И.О.)

«__» _____ 20__ г.

Е.9 Уведомление субъекта о прекращении обработки и уничтожении ПДн

Субъекту персональных данных:
(ФИО)

Адрес:

УВЕДОМЛЕНИЕ
о прекращении обработки и уничтожении
персональных данных

Оператор персональных данных МП «ЕРКЦ»,
находящийся по адресу: Челябинская область, г. Магнитогорск, ул. Ленинградская, 17

руководствуясь: _____
(правовое основание обработки персональных данных)

с целью: _____
(цель обработки персональных данных)

осуществлял обработку Ваших персональных данных, включая:

_____

_____
(перечисление персональных данных, находящихся в обработке: ФИО, адрес, телефон…)

с: _____ по: _____
(дата начала обработки) (дата окончания обработки)

Обработка указанных персональных данных была прекращена в связи с:

_____
(причина окончания обработки персональных данных)

Указанные персональные данные уничтожены.

_____ _____ _____
(должность) (подпись) (Ф.И.О.)

«__» _____ 20__ г.

Е.10 Уведомление субъекта об обработке ПДн

Субъекту персональных данных:
(ФИО)

Адрес:

УВЕДОМЛЕНИЕ

об обработке персональных данных

Оператор персональных данных МП «ЕРКЦ»,
находящийся по адресу: Челябинская область, г. Магнитогорск, ул. Ленинградская, 17
руководствуясь: _____
(правовое основание обработки персональных данных)

с целью: _____
(цель обработки персональных данных)

осуществляет обработку Ваших персональных данных, включая:

_____

_____
(перечисление персональных данных, находящихся в обработке: ФИО, адрес, телефон…)

полученные: _____
(источник получения персональных данных)

Обработка вышеуказанных персональных данных осуществляется путем:

_____
(перечень действий с персональными данными,

_____
(общее описание используемых оператором способов обработки персональных данных)

К персональным данным имеют или могут получить доступ следующие лица:

_____

_____
(перечень конкретных лиц или должностей)

Обработка указанных персональных данных будет являться основанием для:

_____
(решения, принимаемые на основании обработки; возможные юридические последствия обработки)

Дата начала обработки персональных данных: _____

Срок или условие прекращения обработки персональных данных:

_____

_____ _____ _____
(должность) (подпись) (Ф.И.О.)

«__» _____ 20__ г.

Е.11 Уведомление субъекта о внесении изменений в ПДн

Субъекту персональных данных:
(ФИО)

Адрес:

УВЕДОМЛЕНИЕ
о внесении изменений в персональные данные

Оператор персональных данных: МП «ЕРКЦ» ,
находящийся по адресу: Челябинская область, г. Магнитогорск, ул. Ленинградская, 17
действующий в соответствии с: _____
(правовое основание обработки персональных данных)

в отношении персональных данных: _____
(имя субъекта персональных данных)

по требованию субъекта персональных данных внес следующие изменения:

наименование	**исходное значение**	**изменено**
(наименование категории персональных данных: ФИО, адрес, телефон и т.п.)	(исходное значение)	(новое значение)

на основании: _____
(документ(ы), на основании которого(ых) внесены указанны изменения)

Указанные персональные данные вводятся в обработку с учетом внесенных изменений с _____
(дата возобновления обработки)

Срок или условие прекращения обработки персональных данных: _____

_____

_____ _____ _____
(должность) (подпись) (Ф.И.О.)

«__» _____ 201_ г.

Е.12 Форма журнала учета материальных носителей с ПДн

№ п/п	Тип материального носителя	Наименование модели	Инвентарный номер	Владелец информации	Ответственное лицо	Дата поступления носителя
1						

Е.13 Форма журнала учета средств защиты информации в ИСПДн

№ п/п	Тип СЗИ	Наименование СЗИ	Индекс или условное наименование* (для сертифицированных СЗИ)	Регистрационный номер* (для сертифицированных СЗИ)	ИСПДн, в которой(ых) применяется СЗИ	Наличие и место хранения документации
1						

* Перечень индексов, условных наименований и регистрационных номеров определяется ФСТЭК России и ФСБ России в пределах их полномочий.

Е.14 Форма журнала учета пользователей ИСПДн

№ п/п	ФИО	Подразделение	Дата заявки на доступ	Предоставленные права
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				
15.				
16.				
17.				
18.				

Приложение Ж

Акт о ведении реестра

Утверждаю
Заместитель директора
муниципального предприятия
муниципального образования
г. Магнитогорска «Единый расчетно-кассовый центр».

«___» _____ 20__ г.

АКТ
О ВЕДЕНИИ РЕЕСТРА «_____»

Необходимость ведения реестра:		
Цели обработка ПДн:		
Способы фиксации ПДн:		
Состав ПДн:		
Перечень лиц, допущенных к материальным носителям	ФИО	Должность
Перечень лиц, ответственных за ведение и сохранность реестра:	ФИО	Должность
Срок обработки ПДн:		
Порядок пропуска субъекта ПДн на территорию компании		

Приложение 3

Соглашение о неразглашении ПДн

СОГЛАШЕНИЕ №___
О НЕРАЗГЛАШЕНИИ ПЕРСОНАЛЬНЫХ ДАННЫХ

г. Магнитогорск “___” _____ 20__ г

Муниципальное предприятие муниципального образования г. Магнитогорска «Единый расчетно – кассовый центр», в лице Директора _____, действующего на основании Устава, именуемое в дальнейшем «Передающая сторона», и _____, в лице Генерального директора _____, действующего на основании Устава, именуемое в дальнейшем «Принимающая сторона», вместе именуемые «Стороны», заключили настоящее Соглашение о неразглашении персональных данных (далее – Соглашение) о нижеследующем:

СТАТЬЯ 1

1. В настоящем Соглашении под «Персональными данными» понимается информация, представленная Передающей стороной Принимающей стороне в письменном, электронном или любом другом виде и 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.

2. Лицами, получающими доступ к персональным данным, должна обеспечиваться конфиденциальность таких данных и безопасность таких данных при их обработке, за исключением общедоступных и обезличенных персональных данных.

СТАТЬЯ 2

1. Принимающая сторона обязуется при обработке персональных данных соблюдать нормы действующего федерального законодательства и требования регуляторов по вопросам безопасности персональных данных.

2. Принимающая сторона обязуется обрабатывать персональные данные, полученные от Передающей стороны, исключительно в целях исполнения Договора №___ от «___»_____ 20__г. (далее – Договор).

3. Принимающая сторона обязуется принимать все необходимые организационные и технические меры по обеспечению конфиденциальности и безопасности персональных данных, по защите их от несанкционированного, в том числе, случайного доступа, уничтожения, изменения, блокирования, копирования, распространения и иных неправомерных действий.

4. Принимающая сторона обеспечивает доступ к Персональным данным только лиц, которым она необходима для выполнения обязательств Принимающей стороны перед Передающей стороной, и только в том случае, если ими приняты обязательства обеспечивать сохранность ставшими им известными Персональные данные на условиях настоящего Соглашения.

5. Принимающая сторона обязуется по требованию Передающей стороны предоставлять информацию о состоянии дел по защите персональных данных.

6. Принимающая сторона обязуется предоставить по запросу Передающей стороне список своих работников, допущенных к работе с персональными данными.

7. Принимающая сторона обязуется не привлекать третьих лиц к обработке персональных данных.

8. Принимающая сторона обязуется не распространять и не предоставлять персональные данные третьим лицам, включая своих работников и работников Передающей стороны, не допущенных к работе с персональными данными, без письменного разрешения Передающей стороны, за исключением случаев, предусмотренных действующим законодательством.

9. Принимающая сторона обязуется не осуществлять без письменного разрешения Передающей стороны копирование базы персональных данных или ее части, перенос персональных данных на какие-либо материальные носители, а также копирование и тиражирование материальных носителей персональных данных за исключением случаев, предусмотренных целями обработки персональных данных, либо условиями Договора.

10. Принимающая сторона обязуется не совершать никаких действий по модификации персональных данных без письменного разрешения Передающей стороны за исключением случаев, когда это предполагается целью обработки персональных данных.

11. Принимающая сторона обязуется не производить объединение созданных для несовместимых между собой целей баз данных информационных систем персональных данных.

12. Принимающая сторона обязуется по запросу субъекта персональных данных или его законного представителя безвозмездно предоставлять информацию о факте и способах обработки его персональных данных и иную информацию, относящуюся к данному субъекту персональных данных в соответствии с Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных».

13. Принимающая сторона обязуется совершать по согласованию с Передающей стороной все необходимые корректирующие мероприятия в отношении персональных данных при выявлении недостоверных персональных данных или неправомерных действий с ними.

14. Принимающая сторона обязуется незамедлительно сообщить Передающей стороне о допущенном Принимающей стороной, ее Представителями, либо ставшем известным Получающей Стороне факте разглашения или угрозы разглашения, незаконном получении или незаконном использовании переданных персональных данных.

СТАТЬЯ 3

1. Принимающая сторона несет ответственность за действия своих работников, приведшие к раскрытию Персональных данных любым третьим лицам.

2. Обязанность по доказыванию факта разглашения Персональных данных, по сбору доказательств, подтверждающих факт разглашения Персональных данных, возлагается на Передающую сторону.

3. Любой ущерб, причиненный Передающей стороне, вследствие раскрытия Персональных данных, определяется и возмещается в соответствии с действующим законодательством Российской Федерации.

4. Стороны обязуются мирным путем разрешать все споры, противоречия или разногласия, которые могут возникнуть между ними в отношении или в связи с настоящим Соглашением, или исполнением, нарушением, прекращением или недействительностью настоящего Соглашения, однако, если Стороны окажутся не в состоянии достичь согласия, то все споры, противоречия и разногласия подлежат урегулированию в Арбитражном суде в соответствии с действующим законодательством Российской Федерации.

СТАТЬЯ 4

1. Передающая сторона передает персональные данные Принимающей стороне согласно Перечню персональных данных (Приложение 1 к Соглашению).

2. Персональные данные передаются Принимающей стороне:

– на материальном носителе по акту приема-передачи материальных носителей, в котором должны быть зафиксированы вид материального носителя;

– с помощью информационной системы общего пользования.

3. Настоящее Соглашение о неразглашении Персональных данных не предусматривает какое-либо предоставление права на последующее коммерческое использование Персональных данных.

СТАТЬЯ 5

1. Настоящее Соглашение вступает в силу с момента его подписания обеими Сторонами и действует до момента, пока Стороны не заявят о его расторжении. Сторона, расторгающая настоящее Соглашение, обязана уведомить другую Сторону за 30 (тридцать) дней до даты его расторжения. Прекращение срока действия настоящего Соглашения не освобождает Принимающую сторону от обязанности по обеспечению конфиденциальности персональных данных, переданных в рамках настоящего Соглашения.

2. Передающая Сторона вправе потребовать от Принимающей стороны вернуть ей переданные персональные данные в любое время, направив Принимающей стороне уведомление в письменной форме. В течение 15 дней после получения такого уведомления Принимающая сторона должна уничтожить по акту переданные ей для осуществления договорной деятельности персональные данные и вернуть все материальные носители с персональными данными, их копии и экземпляры.

3. Права и обязанности Сторон по настоящему Соглашению в случае реорганизации какой-либо из Сторон переходят к соответствующему правопреемнику (правопреемникам). В случае ликвидации какой-либо Стороны или по прекращению действия настоящего Соглашения Принимающая сторона должна до завершения ликвидации (до прекращения действия настоящего соглашения) уничтожить по акту переданные ей для осуществления договорной деятельности персональные данные и вернуть все материальные носители с персональными данными, их копии и экземпляры.

4. Если Принимающая сторона будет обязана по закону предоставить персональные данные органам государственной власти РФ или органам государственной власти субъектов РФ, либо органам государственной власти иностранных государств, а также иным органам, уполномоченным законодательством требовать предоставления персональных данных, Принимающая Сторона обязана немедленно письменно уведомить об этом факте Передающую Сторону. При этом Принимающая Сторона обязуется сделать все от нее зависящее для того, чтобы обеспечить конфиденциальность предоставленных персональных данных.

5. Дополнения и изменения в настоящее Соглашение могут быть внесены только на основании письменного соглашения, подписанного должным образом уполномоченными представителями Сторон.

6. Настоящим Стороны обязуется не переуступать и не передавать каким-либо иным образом свои права и обязанности, вытекающие из настоящего Соглашения без предварительного письменного согласия другой Стороны.

7. Если какое-либо из положений настоящего Соглашения будет признано недействительным, то такая недействительность не будет распространяться на действие остальных положений настоящего Соглашения, либо на всё Соглашение в целом.

8. В подтверждение изложенного выше, Стороны подписали настоящее Соглашение в 2 (двух) экземплярах, имеющих равную юридическую силу, по одному для каждой из Сторон, в указанном выше месте и в указанную выше дату.

Приложение И

Дополнения в должностные инструкции персонала МП «ЕРКЦ» работающего с ИСПДн

1. В раздел трудовых договоров (должностных инструкций) персонала МП «ЕРКЦ» работающего с информационными системами персональных данных закрепляющих должностные обязанности, необходимо включить следующий пункт:

– При работе с информационными системами персональных данных следует руководствоваться требованиями к порядку обработки и обеспечения безопасности персональных данных, закрепленными в «Положении по организации и проведению работ по обеспечению безопасности ПДн при их обработке в ИСПДн МП «ЕРКЦ».

2. В раздел «Ответственность» трудовых договоров (должностных инструкций) работников МП «ЕРКЦ», допущенных к обработке персональных данных для выполнения своих должностных обязанностей, необходимо включить следующие пункты:

– Работник МП «ЕРКЦ» несет ответственность за обеспечение конфиденциальности ПДн, ставших ему известными в связи с выполнением должностных обязанностей.

– Работник МП «ЕРКЦ» несет персональную ответственность за соблюдение требований по обработке и обеспечению безопасности ПДн, установленных в «Положении по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в ИСПДн МП «ЕРКЦ».

– В случаях нарушения установленного порядка обработки и обеспечения безопасности ПДн, несанкционированного доступа к ПДн, раскрытия ПДн и нанесения МП «ЕРКЦ», ее работникам или клиентам материального или иного ущерба, виновные лица несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

Приложение К

Порядок проведения разбирательств по фактам несоблюдения условий хранения носителей ПДн и использования СЗИ, которые могут привести к нарушению конфиденциальности ПДн или другим нарушениям, приводящим к снижению уровня защищенности ПДн

К.1 Общие положения

Настоящий порядок разработан в соответствии с требованием п.10 «Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденным постановлением Правительства Российской Федерации от 17 ноября 2007 г. №781.

К.2 Порядок проведения разбирательств

К.2.1 Инициирование процесса разбирательства

1. Решение о необходимости проведения разбирательства принимается начальником ОПО при обнаружении фактов нарушения условий хранения носителей ПДн и использования СЗИ.

2. В случае принятия решения о необходимости проведения разбирательства, руководителем ОПО , подготавливается распоряжение, за подписью директора, в котором определяются сроки проведения разбирательства и состав лиц, которые будут учувствовать в проведении разбирательства. Распоряжение доводится до всех заинтересованных лиц.

К.2.2 Проведение расследования

1. АИБ организует опрос очевидцев и подозреваемых лиц, допустивших нарушение.

2. В ходе проведения расследования проводится опрос очевидцев нарушения и лиц, предположительно допустивших нарушение условий хранения носителей ПДн и использования СЗИ, в ходе которого выясняется:

– дата и время совершения нарушения;

– обстоятельства, при которых были совершены действия, приведшие к возникновению нарушения;

– последствия, возникшие вследствие совершения нарушения.

3. Все опрашиваемые лица должны предоставить объяснительные записки (заявления) (показания, изложенные на бумажном носителе с подписью опрашиваемого).

4. АИБ оценивает последствия, возникшие вследствие совершения нарушения.

К.2.3 Формирование заключения по результатам разбирательств

1. По результатам разбирательства АИБ в течение трех рабочих дней составляет заключение по результатам разбирательств (далее – Заключение).

2. В Заключении должны быть приведены:

– краткая справка по нарушению, в отношении которого проводилось разбирательство;

– лицо (а), которое совершило нарушение;

– предложения по привлечению виновника к ответственности (дисциплинарной ответственности: выговор, строгий выговор, лишение премии или увольнение; или к гражданско-правовой ответственности (иск в суд));

– план мероприятий по предотвращению подобных нарушений в будущем (если уместно).

3. Форма Заключения приведена в Приложении 1 к данному порядку.

4. Заключение предоставляется начальнику ОПО.

К.3 Ответственность

1. АИБ ответственен за непредвзятое проведение разбирательств по фактам нарушения условий хранения ПДн и использованию средств защиты ПДн.

2. Работники ОО ответственны за ознакомление работников Предприятия, чьи должностные обязанности связаны с проведением разбирательств, с требованиями настоящего документа при трудоустройстве.

3. Работники, допущенные к обработке ПДн, носителям ПДн и к средствам защиты информации ответственны за соблюдение правил хранения носителей ПДн и использования средств защиты ПДн, изложенных в «Положении о порядке обработки и обеспечении безопасности персональных данных» и в инструкциях на сопровождение СЗИ.

4. При нарушении правил хранения носителей ПДн и сопровождения средств защиты ПДн виновные лица несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

Приложение №1
к Порядку проведения
разбирательств.

Заключение о проведении разбирательства

Утверждаю
Начальник отдела программного обеспечения
муниципального предприятия
муниципального образования г. Магнитогорска
«Единый расчетно-кассовый центр»

_____
«____» _____ 201_ г.

№	Вопросы	Описание
1	Краткая справка по нарушению, в отношении которого проводилось разбирательство	
	Лицо(а), которое совершило нарушение	
	Предложения по привлечению виновника к ответственности	
	План мероприятий по предотвращению подобных нарушений в будущем	
	Состав лиц, проводивших разбирательство	1. _____ _____(ФИО/подпись) 2. _____ _____(ФИО/подпись) 3. _____ _____(ФИО/подпись)

Приложение Л

Шаблон Отчета о проведении внутреннего контроля обработки и обеспечения безопасности персональных данных

<table>
<tr><td>Перечень лиц проводивших внутренний контроль</td><td colspan="4"></td></tr>
<tr><td>Даты проведения внутреннего контроля</td><td colspan="4"></td></tr>
<tr><td rowspan="7">Перечень ИСПДн подлежащих контролю и оценка уровня защищенности ПДн</td><td colspan="2">ИСПДн</td><td colspan="2">Уровень защищенности ПДн в ИСПДн</td></tr>
<tr><td colspan="2"></td><td colspan="2"></td></tr>
<tr><td colspan="2"></td><td colspan="2"></td></tr>
<tr><td colspan="2"></td><td colspan="2"></td></tr>
<tr><td colspan="2"></td><td colspan="2"></td></tr>
<tr><td colspan="2"></td><td colspan="2"></td></tr>
<tr><td colspan="2"></td><td colspan="2"></td></tr>
<tr><td rowspan="6">Перечень структурных подразделений подлежащих контролю и оценка уровня деятельности работников Предприятияа, допущенных к работе с ПДн в ИСПДн, на соответствие порядку обработки и обеспечения безопасности ПДн, установленному настоящим Положением, ФЗ «О персональных данных» и другими нормативными правовыми актами</td><td colspan="2">Структурное подразделение</td><td colspan="2">Уровень соответствия деятельности работников установленному порядку работы с ПДн</td></tr>
<tr><td colspan="2"></td><td colspan="2"></td></tr>
<tr><td colspan="2"></td><td colspan="2"></td></tr>
<tr><td colspan="2"></td><td colspan="2"></td></tr>
<tr><td colspan="2"></td><td colspan="2"></td></tr>
<tr><td colspan="2"></td><td colspan="2"></td></tr>
<tr><td rowspan="6">Мероприятия по повышению уровня защищенности ПДн и устранения выявленных нарушений</td><td>Мероприятие</td><td>Финансовые затраты на реализацию</td><td>Ответственный</td><td>Срок исполнение</td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
</table>

«__»_____201_г.

_____
Должность, ФИО

Приложение М

Шаблон Обязательства о неразглашении конфиденциальной информации.

Администрация города Магнитогорска Челябинской области
Муниципальное предприятие муниципального образования г. Магнитогорска
«ЕДИНЫЙ РАСЧЕТНО-КАССОВЫЙ ЦЕНТР»
(МП «ЕРКЦ»)

ОБЯЗАТЕЛЬСТВО

г. Магнитогорск _____№ _____

О неразглашении конфиденциальной информации

Я, _____,
Ф.И.О. сотрудника
в качестве сотрудника МП «ЕРКЦ» в период трудовых отношений с данным учреждением и в течение 3 (трех) лет после их окончания обязуюсь:

1. не разглашать сведения, составляющие конфиденциальную информацию (документированная информация, доступ к которой ограничивается в соответствии с законодательством РФ) МП «ЕРКЦ», которые мне будут доверены или станут известны в ходе выполнения должностных обязанностей;

2. не передавать третьим лицам и не раскрывать публично сведения, составляющие конфиденциальную информацию МП «ЕРКЦ» (сведения, независимо от формы их предоставления, которые не могут быть переданы лицом, получившим доступ к данным сведениям, третьим лицам без согласия их правообладателя);

3. выполнять требования приказов, инструкций и положений по обеспечению сохранности конфиденциальной информацию МП «ЕРКЦ»;

4. в случае попытки посторонних лиц получить от меня сведения о конфиденциальной информации МП «ЕРКЦ» сообщить об этом факте руководителю своего структурного подразделения;

5. сохранять конфиденциальную информацию тех учреждений (организаций), с которыми у МП «ЕРКЦ» имелись и (или) имеются деловые отношения;

6. не использовать знание конфиденциальной информации МП «ЕРКЦ» для занятий любой деятельностью, которая может нанести ущерб МП «ЕРКЦ», за исключением случаев, установленных законодательством РФ;

7. в случае моего увольнения все носители конфиденциальной информации МП «ЕРКЦ» (рукописи, черновики, машинные носители, распечатки на принтерах, изделия и пр.), которые находились в моем распоряжении в связи с выполнением мною служебных обязанностей во время работы в МП «ЕРКЦ», передать непосредственному руководителю;

8. об утрате или недостаче носителей конфиденциальной информации, ключей, специальных пропусков, хранилищ, сейфов, архивов, личных печатей, которые могут привести к разглашению конфиденциальной информации учреждения, а также о причинах и условиях возможной утечки сведений немедленно сообщать непосредственному руководителю.

Я предупрежден(а), что в случае невыполнения любого из вышеуказанных пунктов настоящего Обязательства, ко мне могут быть применены меры дисциплинарного взыскания в соответствии с трудовым законодательством РФ, вплоть до увольнения из МП «ЕРКЦ».

Я ознакомлен(а) с «Положением по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

Мне известно, что нарушение требований по обеспечению сохранности конфиденциальной информации МП «ЕРКЦ» может повлечь уголовную, административную, гражданско-правовую

или иную ответственность в соответствии с законодательством Российской Федерации, в виде лишения свободы, денежного штрафа, обязанности по возмещению ущерба МП «ЕРКЦ» (убытков, упущенной выгоды) и других наказаний.

_____	_____	_____
(должность)	(подпись)	(И.О.Фамилия.)

Приложение Н.

Шаблон распоряжения о расследовании фактов несоблюдения условий хранения носителей ПДн и использования СЗИ.

Администрация города Магнитогорска Челябинской области
Муниципальное предприятие муниципального образования г. Магнитогорска
«ЕДИНЫЙ РАСЧЕТНО-КАССОВЫЙ ЦЕНТР»

РАСПОРЯЖЕНИЕ

_____ № _____

г. Магнитогорск

О создании комиссии

В целях проведения расследования по факту нарушения условий хранения носителей персональных данных и использования средств защиты информации

ОБЯЗЫВАЮ:

1 Создать комиссию в составе:
Председатель
Члены комиссии:

Секретарь

2 Срок проведения расследования
3 Контроль исполнения распоряжения возложить на начальника отдела программного обеспечения Галаева А.А.

Директор Е.Ф. Манолова

С распоряжением ознакомлены:
_____ И.О. Фамилия
_____ И.О. Фамилия
_____ И.О. Фамилия
_____ И.О. Фамилия

Разослано:

Прошито, пронумеровано
81 (восемьдесят одна) страница

Директор _____ Е.Ф.Манолова