

УТВЕРЖДЕНО

приказом ПАО «МЗИК»

от 31 01 2020 г. № 0115

Мотивированное мнение выборного органа
первичной профсоюзной организации
(протокол от 20.01.2020 № 48) учтено

ПОЛОЖЕНИЕ

ОБ ОБРАБОТКЕ И ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

**Публичного акционерного общества «Машиностроительный
завод имени М.И. Калинина, г. Екатеринбург»**

П.062.001-20

Действует с 01 февраля 2020 г.

2020 г.

Содержание

1. Общие положения.....	3
2. Основные понятия.....	4
3. Состав персональных данных, обрабатываемых в ПАО «МЗИК».....	7
4. Документы, содержащие персональные данные.....	8
5. Обработка персональных данных.....	9
6. Передача персональных данных.....	12
7. Защита персональных данных.....	13
8. Доступ к персональным данным.....	16
9. Права и обязанности субъектов персональных данных.....	18
10. Обязанности ПАО «МЗИК» в области обработки персональных данных.....	19
11. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных.....	20
12. Приложения.....	21

1. Общие положения

1.1. Настоящее Положение об обработке и защите персональных данных Публичного акционерного общества «Машиностроительный завод имени М.И.Калинина, г. Екатеринбург» (далее – Положение) разработано на основании:

- статьи 24 Конституции Российской Федерации;
- главы 14 Трудового кодекса Российской Федерации «Защита персональных данных работника»;
- Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;
- постановления Правительства Российской Федерации от 06.07.2008 № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»;
- постановления Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- приказа Роскомнадзора от 05.09.2013 № 996 «Об утверждении требований и методов по обезличиванию персональных данных».

1.2. Настоящее Положение определяет политику, цели, условия и правила обработки персональных данных (в том числе в информационных системах) в Публичном акционерном обществе «Машиностроительный завод имени М.И. Калинина, г. Екатеринбург» (далее – ПАО «МЗИК», Общество, Оператор), меры по обеспечению режима их защиты, права и обязанности субъектов персональных данных, а также права, обязанности и ответственность лиц, осуществляющих обработку персональных данных.

1.3. Обработка персональных данных работников осуществляется исключительно в целях:

- обеспечения соблюдения законов и иных нормативных правовых актов Российской Федерации;
- обеспечения выполнения трудовых договоров с работниками;
- содействия работникам в обучении и продвижении по службе;
- обеспечения личной безопасности работников;
- контроля количества и качества выполняемой работы и обеспечения сохранности имущества Общества;
- обеспечения пропуска субъектов персональных данных на объекты Общества;
- выполнения социальных обязательств ПАО «МЗИК»;

- обеспечения исполнения обязательств ПАО «МЗИК» по выплатам дивидендов, а также в других целях, предусмотренных уставом и нормативными документами ПАО «МЗИК».

1.4. Настоящее Положение распространяется на все подразделения Общества.

1.5. Действие настоящего Положения не распространяется на отношения, возникающие при:

- хранении, комплектовании, учете и использовании сведений, содержащих персональные данные, архивных документов Общества (документов, законченных делопроизводством и переданных на хранение в соответствующий архив Общества) в соответствии с законодательством об архивном деле в Российской Федерации;

- обработке персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну.

1.6. Руководители структурных подразделений ПАО «МЗИК» несут персональную ответственность за обработку и обеспечение режима защиты персональных данных, выполнение работниками требований законодательства Российской Федерации и нормативных документов ПАО «МЗИК» в области обработки и защиты персональных данных.

1.7. Работники ПАО «МЗИК» должны быть ознакомлены с настоящим Положением под роспись.

1.8. Настоящее Положение действует бессрочно, до замены новым Положением. Все изменения в Положение вносятся приказом генерального директора Общества с учетом мнения ОО Первичная профсоюзная организация ПАО «МЗИК».

2. Основные понятия

В настоящем Положении используются следующие термины и понятия:

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

2.2. Субъекты персональных данных – работники, их близкие родственники, кандидаты для приема на работу (соискатели), акционеры и их официальные представители, а также иные лица, чьи персональные данные стали известны в силу предоставления им со стороны ПАО «МЗИК» социальных льгот, гарантий и компенсаций, обеспечения выплат дивидендов.

2.3. Работник – физическое лицо, вступившее в трудовые отношения с ПАО «МЗИК».

2.4. Ответственный за организацию обработки персональных данных в подразделении – уполномоченное лицо, назначаемое руководителем подразделения.

2.5. Уполномоченные работники – работники ПАО «МЗИК», имеющие допуск к персональным данным субъектов персональных данных.

2.6. Конфиденциальность персональных данных – обязательное для соблюдения ПАО «МЗИК» требование не раскрывать третьим лицам персональные данные и не допускать их распространение без согласия субъектов персональных данных или наличия иного законного основания.

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

2.8. Защита персональных данных – деятельность ПАО «МЗИК», включающая принятие правовых, организационных и технических мер, направленных на обеспечение защиты от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении персональных данных.

2.9. Общедоступные персональные данные – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия работника или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

2.10. Персональные данные ограниченного доступа – персональные данные субъектов персональных данных, подлежащие защите в установленном законодательством Российской Федерации порядке.

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

2.12. Биометрические персональные данные – сведения, характеризующие физиологические и биологические особенности субъекта персональных данных, которые используются оператором для установления личности субъекта персональных данных.

2.13. Информационная система персональных данных ПАО «МЗИК» – совокупность персональных данных, содержащихся в базах данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

2.14. 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.

2.15. Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.

2.16. Неавтоматизированная обработка персональных данных – обработка персональных данных, осуществляемая при непосредственном участии человека без использования средств вычислительной техники.

2.17. Передача персональных данных – любое действие или совокупность действий, совершаемых с использованием средств автоматизации или без использования таких средств, представляющих собой доступ, распространение, предоставление персональных данных.

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

2.19. Предоставление персональных данных – действия, направленные на раскрытие персональных данных работников определенному лицу или определенному кругу лиц.

2.20. Разглашение персональных данных – действия (бездействие), в результате которых персональные данные в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становятся известными третьим лицам без письменного согласия субъекта персональных данных.

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

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

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

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

2.25. Допуск к обработке персональных данных – процедура оформления права на доступ к персональным данным.

2.26. Доступ к персональным данным – возможность обработки персональных данных.

2.27. Материальный носитель – бумажный или машинный носитель, предназначенный для фиксирования, передачи и хранения персональных данных.

2.28. Машинный носитель – материальный носитель информации, предназначенный для записи и воспроизведения информации средствами вычислительной техники, а также сопрягаемыми с ними устройствами (внутренние жесткие диски, флэш-накопители, внешние жесткие диски, CD-диски и иные устройства).

2.29. Электронный документ – документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах ПАО «МЗИК».

2.30. Уполномоченный орган по защите прав субъектов персональных данных – федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).

3. Состав персональных данных, обрабатываемых в ПАО «МЗИК»

3.1. Фамилия, имя, отчество (в том числе предыдущие фамилии, имена и (или) отчества в случае их изменения).

3.2. Число, месяц, год рождения.

3.3. Место рождения.

3.4. Сведения о гражданстве (подданстве), в том числе предыдущие гражданства, иные гражданства.

3.5. Вид, серия, номер документа, удостоверяющего личность, дата выдачи, наименование органа, выдавшего его.

3.6. Адрес и дата регистрации по месту жительства (месту пребывания), адрес фактического проживания.

3.7. Номера рабочих, домашних и мобильных телефонов или сведения о других способах связи.

3.8. Данные документа, подтверждающего регистрацию в системе индивидуального (персонифицированного) учета.

3.9. Идентификационный номер налогоплательщика.

3.10. Реквизиты полиса обязательного медицинского страхования.

3.11. Реквизиты свидетельства государственной регистрации актов гражданского состояния.

3.12. Сведения о семейном положении, составе семьи и о близких родственниках (в том числе бывших мужьях (женах)).

3.13. Сведения о трудовой деятельности.

3.14. Сведения о воинском учете и реквизиты документов воинского учета.

3.15. Сведения об образовании (когда и какие образовательные, научные и иные организации окончил, номера документов об образовании, направление подготовки или специальность по документу об образовании, квалификация).

3.16. Сведения об ученой степени.

3.17. Сведения о владении иностранными языками, включая уровень владения.

3.18. Изображение работника (фотография и видеозапись) и его биометрические персональные данные, которые позволяют установить личность и используются оператором для установления личности субъекта персональных данных.

3.19. Сведения, содержащиеся в трудовом договоре, дополнительных соглашениях к трудовому договору.

- 3.20. Сведения о пребывании за границей.
- 3.21. Сведения о наличии или отсутствии судимости – только кандидатов для приема на работу (соискателей) – в случаях, определенных федеральными законами.
- 3.22. Сведения об оформленных допусках к государственной тайне.
- 3.23. Сведения о государственных наградах, иных наградах и знаках отличия.
- 3.24. Сведения о профессиональной переподготовке и (или) повышении квалификации.
- 3.25. Результаты медицинского обследования работника на предмет годности к выполнению трудовых обязанностей.
- 3.26. Сведения о ежегодных оплачиваемых отпусках, отпусках по беременности и родам, отпусках по уходу за ребенком, учебных отпусках и отпусках без сохранения заработной платы.
- 3.27. Сведения о заработной плате, о начисленных дивидендах, реквизиты банковского счета, номер банковской карты.
- 3.28. Другие персональные данные, необходимые для обеспечения реализации целей обработки, указанных в пункте 1.3. настоящего Положения.

4. Документы, содержащие персональные данные

- 4.1. Анкета (с приложением фотографии), автобиография, которые заполняются при приеме на работу.
- 4.2. Копия документа, удостоверяющего личность.
- 4.3. Личная карточка работника.
- 4.4. Трудовая книжка или ее копия.
- 4.5. Копии свидетельств о заключении брака, рождении детей.
- 4.6. Копии документов воинского учета (для военнообязанных и лиц, подлежащих призыву на военную службу).
- 4.7. Копии документов об образовании и о квалификации, документов о квалификации, подтверждающих повышение или присвоение квалификации по результатам дополнительного профессионального образования, документов о присвоении ученой степени, ученого звания (если таковые имеются).
- 4.8. Копии решений о награждении государственными наградами, присвоении почетных, воинских и специальных званий, присуждении государственных премий (если таковые имеются).
- 4.9. Трудовой договор, а также экземпляры письменных дополнительных соглашений, которыми оформляются изменения и дополнения, внесенные в трудовой договор.
- 4.10. Подлинники и копии приказов по личному составу.
- 4.11. Материалы по аттестации, служебным расследованиям, о включении в кадровый резерв, о поощрении, а также о наложении дисциплинарного взыскания до его снятия или отмены.

4.12. Документы, связанные с оформлением допуска к сведениям, составляющим государственную или иную охраняемую законом тайну, если исполнение обязанностей по замещаемой должности связано с использованием таких сведений.

4.13. Справки о доходах с предыдущего места работы.

4.14. Копия документа, подтверждающего регистрацию в системе индивидуального (персонифицированного) учета.

4.15. Копия свидетельства о постановке на учет в налоговом органе физического лица по месту жительства на территории Российской Федерации.

4.16. Копия страхового медицинского полиса обязательного медицинского страхования граждан.

4.17. Медицинское заключение об отсутствии у работника медицинских противопоказаний к выполняемой работе.

4.18. Другие документы, содержащие персональные данные.

5. Обработка персональных данных

5.1. Принципы обработки персональных данных:

5.1.1. Обработка персональных данных должна осуществляться на законной и справедливой основе.

5.1.2. Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, не совместимая с целями сбора персональных данных.

5.1.3. Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, не совместимых между собой.

5.1.4. Обработке подлежат только те персональные данные, которые отвечают целям их обработки.

5.1.5. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

5.1.6. При обработке персональных данных должны быть обеспечены их точность и достаточность, а в необходимых случаях и актуальность сведений, предоставляемых субъектом персональных данных, по отношению к целям обработки.

5.1.7. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных.

5.2. Обработка персональных данных включает в себя следующие действия: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

5.3. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) субъектов персональных данных осуществляется путем:

5.3.1. Непосредственного получения оригиналов необходимых документов (заявление, трудовая книжка, анкета, иные документы, предоставляемые субъектами персональных данных).

5.3.2. Получения заверенных в установленном порядке копий документов, содержащих персональные данные, или копирования оригиналов документов.

5.3.3. Внесения сведений (на бумажных и электронных носителях) в учетные формы.

5.3.4. Формирования персональных данных в ходе кадровой работы.

5.3.5. Получения персональных данных в ответ на запросы, направляемые ПАО «МЗИК» в органы государственной власти, государственные внебюджетные фонды, иные государственные органы, органы местного самоуправления, коммерческие и некоммерческие организации, физическим лицам в случаях и порядке, предусмотренных законодательством Российской Федерации.

5.3.6. Получения персональных данных из общедоступных источников.

5.3.7. Фиксации (регистрации) персональных данных в журналах, книгах, реестрах и других учетных формах.

5.3.8. Внесения персональных данных в информационные системы ПАО «МЗИК».

5.3.9. Использования иных средств и способов фиксации персональных данных, получаемых в рамках осуществляемой ПАО «МЗИК» деятельности.

5.4. Источником информации обо всех персональных данных является непосредственно субъект персональных данных. Если персональные данные возможно получить только у третьей стороны, то субъект персональных данных должен быть заранее в письменной форме уведомлен об этом и от него должно быть получено письменное согласие. Оператор обязан сообщить субъекту персональных данных о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа дать письменное согласие на их получение.

Необходимость согласия на получение персональных данных у третьих лиц и направления уведомления об этом может возникнуть, например, при подтверждении факта получения диплома, свидетельства, аттестата об образовании, при восстановлении трудовой книжки, свидетельства о получении квалификации, при подтверждении факта работы в том или ином месте, факта смены фамилии и др., в том числе если утрата сведений произошла в связи со стихийными бедствиями, иными обстоятельствами.

5.5. ПАО «МЗИК» не вправе запрашивать у третьих лиц даже с согласия субъекта персональных данных информацию, не имеющую отношения к целям обработки персональных данных.

5.6. Запрещается получать и обрабатывать персональные данные о расовой, национальной принадлежности, политических взглядах, религиозных и философских убеждениях, состоянии здоровья, интимной жизни субъекта

персональных данных, а также персональные данные о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных Трудовым кодексом РФ и другими федеральными законами.

5.7. При принятии решений, затрагивающих интересы субъекта персональных данных, запрещается основываться на персональных данных, полученных исключительно в результате их автоматизированной обработки или с использованием электронных носителей.

5.8. Оператор имеет право обрабатывать персональные данные только с письменного согласия субъекта персональных данных, кроме ниже перечисленных случаев:

5.8.1. Обработка персональных данных осуществляется на основании Трудового кодекса Российской Федерации или иного федерального закона, устанавливающего ее цель, условия получения персональных данных и круг субъектов, персональные данные которых подлежат обработке, а также определяющего полномочия ПАО «МЗИК».

5.8.2. Обработка персональных данных осуществляется в целях исполнения трудового договора.

5.8.3. Обработка персональных данных осуществляется для статистических или иных научных целей при условии обязательного обезличивания персональных данных.

5.8.4. Обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов работника, если получение его согласия невозможно.

5.9. Обработка биометрических персональных данных может осуществляться только при наличии согласия в письменной форме субъекта персональных данных, за исключением случаев, предусмотренных законодательством Российской Федерации.

Использование и хранение биометрических персональных данных вне информационных систем персональных данных могут осуществляться только на таких материальных носителях информации и с применением такой технологии ее хранения, которые обеспечивают защиту этих данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения.

5.10. Персональные данные могут быть получены, обработаны и переданы на хранение, как на бумажных носителях, так и в электронном виде – в локальной компьютерной сети, программах и других технических средствах.

5.11. Обработка персональных данных с использованием информационных систем персональных данных, осуществляется в отдельной информационной системе персональных данных, физически изолированной от информационно-телекоммуникационных сетей общего пользования.

5.12. В случае выявления недостоверных персональных данных или неправомерных действий с ними лиц допущенных к персональным данным при обращении или по запросу субъекта персональных данных, или его законного представителя либо уполномоченного органа по защите прав субъектов

персональных данных, оператор обязан осуществить блокирование персональных данных, относящихся к соответствующему субъекту персональных данных, с момента такого обращения или получения такого запроса на период проверки.

5.13. Уточнение персональных данных производится путем их обновления или изменения на материальном носителе, а если это не допускается особенностями материального носителя – путем изготовления нового материального носителя с уточненными персональными данными.

5.14. В случае подтверждения факта недостоверности персональных данных, оператор, на основании документов, представленных субъектом персональных данных, или его законным представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов, обязан уточнить персональные данные и снять их блокирование в течение 7 дней.

5.15. В случае выявления неправомерных действий с персональными данными, оператор, в срок, не превышающий 3 рабочих дней с даты такого выявления, обязан устранить допущенные нарушения. Об устранении допущенных нарушений или об уничтожении персональных данных, оператор обязан уведомить субъекта персональных данных, или его законного представителя, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

5.16. Персональные данные уничтожаются либо обезличиваются по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом, в 30-дневный срок.

6. Передача персональных данных

6.1. Передача (распространение, предоставление) персональных данных осуществляется лишь в случаях и порядке, предусмотренных законодательством Российской Федерации, и с соблюдением следующих требований:

6.1.1. Передача персональных данных третьим лицам, в том числе трансграничная передача, допускается только с письменного согласия субъектов персональных данных, за исключением случаев, когда это необходимо для предупреждения угрозы жизни и здоровью субъектов персональных данных, а также в иных случаях, предусмотренных федеральными законами.

6.1.2. Лица, получившие персональные данные, предупреждаются 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.

6.1.3. Передача персональных данных третьим лицам осуществляется только после получения от третьего лица заверенных в установленном порядке документов, подтверждающих выполнение условий соблюдения конфиденциальности и обеспечения безопасности персональных данных при их обработке.

6.1.4. Передача персональных данных работников в пределах ПАО «МЗИК» осуществляется в соответствии с настоящим Положением и только работниками, имеющими доступ к персональным данным.

6.1.5. Доступ к персональным данным работников разрешается только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные работника, которые необходимы для выполнения конкретной функции.

6.1.6. Не запрашивается информация о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции.

6.1.7. Персональные данные работника передаются в порядке, установленном Трудовым кодексом Российской Федерации, ограничиваясь только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функции.

6.2. Передача персональных данных субъектов персональных данных без их согласия допускается, если это необходимо для исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве, по мотивированным запросам правоохранительных органов и иных органов государственной власти в рамках установленных полномочий, а также в иных случаях предусмотренных федеральными законами.

6.3. Передача персональных данных через сети связи общего пользования, Интернет осуществляется с использованием сертифицированных средств криптографической защиты информации и в соответствии с нормативными документами Федеральной службы безопасности Российской Федерации.

6.4. Трансграничная передача персональных данных на территории иностранных государств осуществляется в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».

7. Защита персональных данных

7.1. Защита персональных данных от неправомерного их использования или утраты обеспечивается за счет средств ПАО «МЗИК».

7.2. Защита персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а так же иные несанкционированные действия.

7.3. Режим защиты персональных данных обеспечивает предотвращение нарушения конфиденциальности, целостности и доступности персональных данных при их обработке.

7.4. Персональные данные субъектов персональных данных хранятся на бумажных носителях в соответствии с номенклатурой дел и в электронном виде (в информационных системах ПАО «МЗИК», на ПЭВМ, а также на съемных

магнитных, оптических и других цифровых носителях), с соблюдением условий, обеспечивающих их защиту от несанкционированного доступа.

7.5. Безопасность персональных данных обеспечивается реализацией комплекса мер, определенных федеральными законами, указами Президента Российской Федерации, постановлениями Правительства Российской Федерации, приказами ФСТЭК России, ФСБ России, Роскомнадзора, нормативными документами ПАО «МЗИК», в том числе включающих:

7.5.1. Организацию работы с персональными данными, обеспечивающей сохранность носителей персональных данных и средств защиты информации.

7.5.2. Размещение информационных систем ПАО «МЗИК» и специального оборудования в помещениях, исключающих возможность неконтролируемого пребывания в них посторонних лиц.

7.5.3. Разграничение доступа пользователей и работников, обслуживающих средства вычислительной техники, к информационным ресурсам, программным средствам обработки (передачи) и защиты информации.

7.5.4. Учет документов, информационных массивов, содержащих персональные данные.

7.5.5. Регистрацию действий пользователей информационных систем и работников, обслуживающих средства вычислительной техники, в порядке, принятом ПАО «МЗИК».

7.5.6. Контроль действий и недопущение несанкционированного доступа к персональным данным пользователей информационных систем ПАО «МЗИК», персонала, обслуживающего средства вычислительной техники.

7.5.7. Хранение и использование материальных носителей, исключающих их хищение, подмену и уничтожение.

7.5.8. Необходимое резервирование технических средств и дублирование массивов и носителей информации, содержащей персональные данные.

7.6. Защита персональных данных в подразделениях ПАО «МЗИК» предусматривает ограничение доступа к ним.

7.7. При работе с документами, содержащими персональные данные, должны быть приняты меры, исключающие возможность ознакомления с этими документами посторонних лиц, в том числе работников, не уполномоченных на обработку персональных данных.

7.8. Документы, содержащие персональные данные, должны храниться в специальном шкафу или помещении, находящимся в контролируемой зоне и обеспечивающем защиту от несанкционированного доступа.

7.9. Дела, содержащие персональные данные, должны находиться в рабочих кабинетах или в специально отведенных для их хранения помещениях, располагаться в запираемых шкафах, обеспечивающих их полную сохранность.

7.10. Во время перерывов в работе, а также после окончания работы с документами, содержащими персональные данные, необходимо:

- блокировать средство вычислительной техники с помощью защищенной паролем экранной заставки;

- принимать необходимые меры по недопущению использования средства вычислительной техники другими работниками и посторонними лицами.

7.11. Черновики и рабочие варианты документов, содержащих персональные данные, уничтожаются исполнителем без возможности восстановления.

7.12. Копирование и печатание документов, содержащих персональные данные, должно осуществляться в порядке, исключающем возможность нарушения конфиденциальности персональных данных.

7.13. В процессе уничтожения дел и документов необходимо исключить возможность ознакомления посторонних лиц с содержащимися в них персональными данными.

7.14. Автоматизированная обработка персональных данных разрешается только при условии применения средств защиты информации, обеспечивающих нейтрализацию актуальных угроз, определенных частью 5 статьи 19 Федерального закона «О персональных данных».

7.15. Средства защиты информации, обеспечивающие защиту персональных данных, должны удовлетворять требованиям, утвержденным постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», а также нормативным правовым актам в области обработки и защиты персональных данных Федеральной службы безопасности Российской Федерации и Федеральной службы по техническому и экспортному контролю.

7.16. При автоматизированной обработке персональных данных для каждой информационной системы организационные и (или) технические меры определяются с учетом уровней защищенности персональных данных, актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационной системе ПАО «МЗИК».

7.17. Во время эксплуатации средств вычислительной техники, предназначенных для обработки персональных данных, должны быть предусмотрены меры по исключению случаев несанкционированного подключения к внешним информационным системам, внешним информационно-телекоммуникационным сетям, а также несанкционированного доступа к этим средствам при проведении ремонтных, профилактических и других видов работ.

7.18. Доступ к обработке персональных данных в информационных системах осуществляется после обязательного прохождения процедуры идентификации и аутентификации.

7.19. Защита персональных данных при их обработке в информационных системах обеспечивается:

- Положением об основах политики в области информационных технологий ОАО «Машиностроительный завод им. М.И. Калинина, г.Екатеринбург» П.371.037-2006;

- Положением о политике информационной безопасности ОАО «Машиностроительный завод им. М.И. Калинина, г. Екатеринбург» П.371.039-2006;
- Положением о средствах и методах защиты в информационной системе персональных данных ОАО «МЗиК»;
- Инструкцией администратора безопасности при использовании ресурсов объекта вычислительной техники ОАО «МЗиК»;
- Инструкцией администратора информационной системы персональных данных (ИСПДн) ОАО «МЗиК»;
- Инструкцией пользователя информационной системы персональных данных ОАО «МЗиК».
- руководящими, нормативными и регламентирующими документами Общества.

8. Доступ к персональным данным

8.1. Основанием для допуска работника к обработке персональных данных является приказ о назначении его на должность, должностная инструкция, предусматривающая обработку персональных данных, обязательство о неразглашении персональных данных (ранее – договор об обработке персональных данных), составленное по форме согласно приложению № 1.

8.2. Правом доступа к персональным данным обладают:

- Генеральный директор ПАО «МЗИК»;
- Первый заместитель генерального директора – исполнительный директор ПАО «МЗИК»;
- Заместители генерального директора ПАО «МЗИК»;
- Главный инженер ПАО «МЗИК»;
- Заместители главного инженера ПАО «МЗИК»;
- Главный бухгалтер ПАО «МЗИК»;
- Руководители структурных подразделений ПАО «МЗИК» и их заместители (в рамках возглавляемых ими подразделений и (или) в рамках, предоставленных им полномочий).

• Работники, ответственные за организацию обработки персональных данных и уполномоченные на обработку персональных данных в подразделении.

8.3. Генеральный директор своим приказом назначает ответственного за организацию обработки персональных данных в ПАО «МЗИК».

8.4. Руководитель структурного подразделения:

8.4.1. Своим распоряжением, составленным по форме согласно приложению № 2, назначает ответственного за организацию обработки персональных данных в подразделении.

8.4.2. Утверждает список работников, в должностных обязанностях которых предусмотрено ведение работы с документами, содержащими персональные данные, и уполномоченных на обработку персональных данных, составленный по форме согласно приложению № 3.

8.4.3. До предоставления доступа к обработке персональных данных ответственного за организацию обработки персональных данных в подразделении и уполномоченных на обработку персональных данных работников обеспечивает подписание ими обязательства о неразглашении персональных данных, составленного по форме согласно приложению № 1.

8.4.4. Предоставляет в отдел кадров № 62 копию распоряжения о назначении ответственного за организацию обработки персональных данных в подразделении, копию списка работников, уполномоченных на обработку персональных данных, обязательства (оригинал) о неразглашении персональных данных. Данные документы предоставляются каждый раз, когда происходит назначение нового работника, ответственного за организацию обработки персональных данных в подразделении, и изменение списка работников, уполномоченных на обработку персональных данных.

8.5. Обязательство о неразглашении персональных данных хранится в личном деле работника.

8.6. Ответственные за организацию обработки персональных данных в подразделениях ПАО «МЗИК» обеспечивают:

8.6.1. Соблюдение законодательства Российской Федерации и нормативных документов ПАО «МЗИК» в области обработки и защиты персональных данных.

8.6.2. Доведение до сведения уполномоченных работников подразделения ПАО «МЗИК» положений законодательства Российской Федерации и нормативных документов ПАО «МЗИК» в области обработки и защиты персональных данных.

8.6.3. Осуществление внутреннего контроля за обеспечением режима защиты персональных данных в подразделении ПАО «МЗИК».

8.7. Уполномоченные работники обязаны:

8.7.1. Знать и выполнять законодательные и иные нормативные правовые акты Российской Федерации, а также нормативные документы ПАО «МЗИК» в области обработки и защиты персональных данных.

8.7.2. Выполнять все требования настоящего Положения и других нормативных документов ПАО «МЗИК», устанавливающих режим защиты персональных данных в ПАО «МЗИК».

8.7.3. Не разглашать информацию, содержащую персональные данные субъектов персональных данных.

8.7.4. Обеспечивать конфиденциальность персональных данных, использовать предусмотренные в ПАО «МЗИК» меры для защиты персональных данных от неправомерных действий.

8.7.5. Во время работы с информацией и (или) документами, содержащими персональные данные, исключать возможность ознакомления с ними работников, не имеющих права обработки персональных данных.

8.7.6. При увольнении сдавать все имеющиеся в распоряжении материальные носители лицу, ответственному за организацию обработки персональных данных в подразделении ПАО «МЗИК».

8.7.7. Информировать руководителя подразделения ПАО «МЗИК» обо всех фактах и попытках несанкционированного доступа к персональным данным и о других нарушениях порядка обработки персональных данных.

8.8. Работники, допущенные к обработке персональных данных, имеют право обрабатывать только те персональные данные, которые необходимы для выполнения их должностных обязанностей.

8.9. Работники, допущенные к обработке персональных данных, обязаны руководствоваться в своей деятельности законодательством Российской Федерации в области обработки и защиты персональных данных, настоящим Положением и другими нормативными документами ПАО «МЗИК».

8.10. Обязанность по соблюдению требований законодательства Российской Федерации и нормативных документов ПАО «МЗИК» в области обработки и защиты персональных данных и ответственность за их нарушение закрепляются в должностных инструкциях работников, допущенных к обработке персональных данных.

9. Права и обязанности субъектов персональных данных

9.1. Субъекты персональных данных имеют право на:

9.1.1. Полную информацию о своих персональных данных и обработке этих данных (в том числе автоматизированной).

9.1.2. Доступ к своим персональным данным, включая право на получение копии любой записи, содержащей персональные данные, за исключением случаев, предусмотренных федеральными законами.

9.1.3. Уточнение своих персональных данных, их блокирование или уничтожение в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки.

9.1.4. Дополнение своих персональных данных оценочного характера заявлением, выражающим собственную точку зрения.

9.1.5. Извещение всех лиц, которым ранее были сообщены их неверные или неполные персональные данные, обо всех произведенных в них исправлениях или дополнениях.

9.1.6. Отзыв согласия на обработку своих персональных данных.

9.1.7. Обжалование в соответствии с законодательством Российской Федерации действий ПАО «МЗИК» при обработке персональных данных или его бездействия.

9.1.8. Осуществление иных прав, предусмотренных законодательством Российской Федерации

9.2. Субъекты персональных данных обязаны:

9.2.1. Предоставить ПАО «МЗИК» свои персональные данные в соответствии с законодательством Российской Федерации и настоящим Положением.

9.2.2. Своевременно информировать ПАО «МЗИК» об изменениях своих персональных данных.

9.2.3. Обеспечить конфиденциальность персональных данных других субъектов персональных данных в соответствии с требованиями законодательства Российской Федерации, Кодекса этики ПАО «МЗИК» и других нормативных документов ПАО «МЗИК».

10. Обязанности ПАО «МЗИК» в области обработки персональных данных

10.1. ПАО «МЗИК» обязано принимать следующие необходимые и достаточные меры для выполнения обязанностей оператора, предусмотренных законодательством Российской Федерации:

10.1.1. Издавать нормативные документы по вопросам обработки персональных данных, а также нормативные документы, устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации и устранение последствий таких нарушений.

10.1.2. Применять правовые, организационные и технические меры для защиты персональных данных субъектов персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий.

10.1.3. Разъяснять субъектам персональных данных юридические последствия отказа предоставить их персональные данные, если предоставление персональных данных является обязательным в соответствии с законодательством Российской Федерации.

10.1.4. Блокировать неправомерно обрабатываемые персональные данные, прекращать обработку персональных данных в соответствии с законодательством Российской Федерации.

10.1.5. Уведомлять субъектов персональных данных об устранении допущенных нарушений при обработке их персональных данных.

10.1.6. Представлять субъектам персональных данных по их просьбе или их представителям информацию, касающуюся обработки их персональных данных, в порядке, установленном законодательством Российской Федерации и нормативными документами ПАО «МЗИК».

10.1.7. Осуществлять внутренний контроль и (или) аудит соответствия обработки персональных данных законодательству Российской Федерации о персональных данных, требованиям к защите персональных данных, политике оператора в отношении обработки персональных данных, локальным актам Оператора.

10.1.8. Проводить оценку вреда, который может быть причинен субъектам персональных данных в случае нарушения законодательства Российской Федерации о персональных данных, соотношения указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных законодательством Российской Федерации в области обработки и защиты персональных данных.

11. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных

11.1. Лица, виновные в нарушении законодательства Российской Федерации и нормативных документов ПАО «МЗИК» в области обработки и защиты персональных данных, несут дисциплинарную, гражданско-правовую, административную и уголовную ответственность.

11.2. Моральный вред, причиненный субъектам персональных данных вследствие нарушения их прав, правил обработки персональных данных, а также требований к защите персональных данных, установленных законодательством Российской Федерации и нормативными документами ПАО «МЗИК» в области обработки и защиты персональных данных, подлежит возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.