Муниципальное автономное дошкольное образовательное учреждение центр развития ребенка - детский сад № 6 г. Курганинска(МАДОУ ЦРР №6)

ПРИКАЗ

от **01.09.203** года № 125

г. Курганинск

О назначении ответственных за обработку персональных данныхв 2023-2024 учебном году

В целях исполнения Федерального закона от 27 июля 2006 г. «152-ФЗ «О персональных данных», совершенствования системы защиты и обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных

приказываю:

1. Ответственность за осуществление мероприятий по защите персональных данных сотрудников ДОУ, воспитанников и их родителей (законных представителей) возлагаю на себя.

2. Назначить ответственным за сбор, хранение и обработку персональных данных работников и воспитанников МАДОУ ЦРР № 6 г. Курганинска, старшего воспитателя Евсевьеву Н.И..

3. Назначить ответственных за обработку персональных данных в информационных системах персональных данных (приложение № 1)

4. Возложить ответственность за организацию технической защиты персональных данных на Евсевьеву Н.И., старшего воспитателя, ответственного за работу с автоматизированной информационной системой управления сферой образования «Сетевой город. Образование», «Е – услуги».

4. В работе руководствоваться документами:

- Правилами обработки персональных данных в МАДОУ ЦРР№ 6
- Должностная инструкция ответственного за организацию обработки персональных данных (приложение 2)
- Положение о порядке деятельности комиссии по уничтожению персональных данных, обрабатываемых сотрудниками (приложение 3)
- Правилами осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных.

Заведующая МАДОУ ЦРР№ 6 Н.Ю. Тимченко

С приказом ознакомлен(а): Евсевьева Н.И.

Корнеенкова Н.В.

Приложение 1
к приказу №125 от 01.09.2023 года
«О назначении ответственных за обработку персональных данных»

ФИО, должность	*Персональные данные*	*Документы*
Н.Ю. Тимченко Заведующий ДОУ	персональные данные работников, обучающихся и их родителей (законных представителей) ОУ	
Старший воспитатель Евсевьева Н.И.	персональные данные работников, обучающихся и их родителей (законных представителей) ОУ	• личные дела учащихся; • личные дела работников школы; • карточка унифицированной формы Т-2; • трудовые книжки; • медицинские книжки; • приказы по личному составу сотрудников; • трудовые договоры; • электронная база данных по работникам ДОУ; • электронная база данных по учащимся ДОУ; • тарификационные данные
Евсевьева Н.И. Старший воспитатель Воспитатели групп Заместитель заведующей по АХР Гореликова Н.И.	персональные данные работников, обучающихся и их родителей (законных представителей) ОУ	• личные дела учащихся; • личные дела работников школы; • трудовые договора; • материалы служебных расследований; • приказы по личному составу работников и обучающихся школы; • сведения о состоянии здоровья обучающихся; • классные журналы (СГО «Образование»); • статистические отчеты; • официальный сайт ДОУ; • электронная база данных по работникам ДОУ; • электронная база данных по учащимся школы; • сайт школы; • сведения ПМПК; • база данных одарённых детей; • тетрадь учёта больничных листов; • статистическая отчетность; • сведения о состоянии здоровья обучающихся и работников школы. • автоматизированная информационная система «Е-услуги. Образование».
Евсевьева Н.И. администратор автоматизированной информационной системы СГО	персональные данные работников, обучающихся и их родителей (законных представителей) ОУ, будущих первоклассников и их родителей (законных представителей)	• автоматизированная информационная система «Е-услуги. Образование • автоматизированная информационная система СГО «Образование» • автоматизированная информационная система СГО «Внеурочная занятость»

Приложение 2
к приказу №125 от 01.09.2023 года
«О назначении ответственных за обработку персональных данных»

ИНСТРУКЦИЯ
ответственного за организацию обработки персональных данных в муниципальном автономном дошкольном образовательном учреждении центр развития ребенка - детский сад № 6 г. Курганинска

1. Основные понятия

Применяемые в настоящей Инструкции термины и понятия означают:

Администратор безопасности - субъект доступа, ответственный за защиту автоматизированной системы от несанкционированного доступа к информации.

Автоматизированная система (АС) - система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Автоматизированное рабочее место (АРМ) - программно-технический комплекс АС, предназначенный для автоматизации деятельности определенного вида.

Защита информации от разглашения - защита информации, направленная на предотвращение несанкционированного доведения защищаемой информации до заинтересованных субъектов (потребителей), не имеющих права доступа к этой информации.

Защита информации от несанкционированного доступа (ЗИ от НСД) - защита информации, направленная на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением установленных нормативными и правовыми документами (актами) или обладателями информации прав или правил разграничения доступа к защищаемой информации.

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

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

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

Оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных

Основные технические средства и системы (ОТСС) - технические средства и системы, а также их коммуникации, используемые для обработки,

хранения и передачи конфиденциальной информации.

Ответственный за организацию обработку ПДн – лицо, назначенное приказом директора Организации, ответственное за регламентацию процесса обработки и защиты ПДн.

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

Распространение персональных данных - действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

Средство защиты информации (СЗИ) - техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

Трансграничная передача персональных данных - передача персональных данных оператором через Государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства.

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

2. Общие положения

2.1. Настоящая инструкция разработана на основании следующих нормативных документов:

- Федеральный закон «О персональных данных» № 152-ФЗ от 27.07.06 г.;
- Постановление Правительства РФ «Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» №781 от 17.11.07 г.;
- Приказ ФСТЭК России от 05.02.10 г. № 58 «Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных»;
- Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К), Государственная техническая комиссия при президенте Российской Федерации, 2002 г.;
- Постановление Правительства РФ от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».

2.2. Инструкция определяет основные задачи, функции, обязанности и права Ответственного за организацию обработку ПДн (далее Ответственного)

информационной системыперсональных данных.

2.3. В своей деятельности Ответственный руководствуется требованиями действующих федеральных законов, общегосударственных и ведомственных нормативных документов по вопросам защиты персональных данных (указанных в п. 2.1.) и обеспечивает их выполнение.

2.4. Настоящая Инструкция является дополнением к действующим регламентирующим документам по вопросам защиты информации в Организации.

3. Задачи и функции Ответственного

3.1. Основными задачами Ответственного являются:

- разработка организационно-распорядительной документации, регламентирующей порядок обработки и защиты ПДн;
- доведение до сведения сотрудников, допущенных к ПДн, положений законодательства РФ о персональных данных, локальных актов по вопросам обработки персональных данных,требований к защите персональных данных;
- осуществление внутреннего контроля за соблюдением требований законодательства РФи инструкций при обработке ПДн, в том числе требований к защите ПДн;
- организация приема и обработки обращений и запросов субъектов персональных данных или их представителей и (или) осуществление контроля за приемом и обработкой таких обращений и запросов;
- заполнение и отправка уведомления об обработке (о намерении осуществлять обработку) персональных данных;
- контроль эффективности защиты информации.

3.2. Для выполнения поставленных задач на Ответственного возлагаются следующиефункции:

3.2.1. Организация допуска пользователей (разработчиков, эксплуатационного персонала) ктехническим, программным средствам и информационным ресурсам ИСПДн в соответствии с «Матрицей доступа пользователей к защищаемым персональным данным ИСПДн» на всехстадиях жизненного цикла ИСПДн.

3.2.2. Участие на стадии проектирования (внедрения) ИСПДн, в разработке технологииобработки персональных данных по вопросам:

- организации порядка учета, хранения и обращения с документами и носителями информации;
- подготовка новых инструкций и внесение изменений и дополнений в настоящую Инструкцию, определяющих задачи, функции, ответственность, права и обязанности администраторов и пользователей ИСПДн по вопросам защиты персональных данных, а также ответственных по защите персональных данных в процессе их автоматизированной обработки.

3.2.3. Контроль выполнения требований действующих нормативных документов повопросам защиты информации при обработке персональных данных в ИСПДн.

3.2.4. Оперативный контроль за ходом технологического процесса обработки персональныхданных.

3.2.5. Методическое руководство работой пользователей ИСПДн в

вопросах обеспеченияинформационной безопасности.

4. Обязанности Ответственного

4.1. Для реализации поставленных задач и возложенных функций Ответственный обязан:

4.1.1. Разработать и вести:

— Журнал по учету мероприятий по контролю обеспечения защиты персональных данныхв ИСПДн;

— Журнал учета носителей персональных данных;

— Журнал учета передачи персональных данных;

— Журнал поэкземплярного учета средств защиты информации, эксплуатационной и технической документации;

— Журнал поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов.

4.1.2. Разработать перечень ПДн.

4.1.3. Разрабатывать решения по:

— составу рабочей группы в защищаемом сегменте сети, системы доверительных отношений между членами группы;

— определению информационных связей между сегментами сети и требований к изоляции сегментов с использованием средств аппаратной безопасности сегментов;

— определению списка устройств, логических дисков, каталогов общего пользования на серверах с указанием состава допущенных к ним пользователей и режимом допуска;

— разработке порядка пользования электронной почтой (определение списка абонентов из состава пользователей сети, использованию СЗИ при передаче конфиденциальных документов).

4.1.4. Осуществлять учет и периодический контроль за составом и полномочиями пользователей различных ПЭВМ, на которых ведется обработка ПДн.

4.1.5. Своевременно и точно отражать изменения в организационно-распорядительных и нормативных документах по управлению СЗИ от НСД, установленных на ПЭВМ.

4.1.6. Контролировать обеспечение защиты персональных данных при взаимодействии пользователей с информационными сетями общего пользования.

4.1.7. Требовать прекращения обработки информации, как в целом, так и для отдельных пользователей, в случае выявления нарушений установленного порядка работ или нарушенияфункционирования ИСПДн или средств защиты.

4.1.8. Контролировать эффективность защиты персональных данных:

- Проводить работу по выявлению возможности вмешательства в процесс функционирования ПЭВМ и осуществления НСД к информации и техническим средствам ПЭВМ.

4. Права Ответственного

4.2. Ответственный имеет право:

4.2.1. Получать доступ к программным и аппаратным средствам ИСПДн, средствам их защиты, а также просмотру прав доступа к ресурсам на серверах ИСПДн и ПЭВМ пользователей.

4.2.2. Требовать от пользователей ИСПДн выполнения инструкций по обеспечению безопасности персональных данных в ИСПДн.

4.2.3. Участвовать в служебных расследованиях по фактам нарушения установленных требований обеспечения информационной безопасности, НСД, утраты, порчи защищаемой информации и технических компонентов ИСПДн.

4.2.4. Осуществлять оперативное вмешательство в работу пользователя при явной угрозе безопасности информации в результате несоблюдения установленной технологии обработки информации и невыполнения требований по безопасности с последующим отчетом директора Организации.

4.3. Лицо, ответственное за организацию обработки ПДн, несет ответственность за:

4.3.1. Реализацию утвержденных в Организации документов, регламентирующих порядок обеспечения безопасности персональных данных.

4.3.2. Программно - технические и криптографические средства защиты информации, средства вычислительной техники, информационно - вычислительные комплексы, сети и автоматизированные системы обработки информации, закрепленные за ним директором Организации и за качество проводимых им работ по обеспечению защиты персональных данных в соответствии с функциональными обязанностями.

4.3.3. Разглашение персональных данных и сведений ограниченного распространения, ставших известными ему по роду работы.

4.3.4. Качество и последствия проводимых им работ по контролю действий пользователей при работе в ИСПДн.

5. Порядок учета, хранения и выдачи носителей ПДн

5.1. Ответственный организует учет, хранение и выдачу носителей ПДн.

5.2. Носителями документированных персональных данных могут быть:

- для традиционных текстовых документов - специальный блокнот с отрывными листами и корешком, выполняющим функцию учета листов, нанесения отметок о целевом их использовании; рабочая тетрадь для больших по объему документов; отдельные пронумерованные листы бумаги, типографские формы и бланки документов;
- для чертежно-графических документов - пронумерованные листы ватмана, кальки, пленки, координатной бумаги и т.п.;
- для машиночитаемых документов - маркированные и пронумерованные магнитные ленты, диски, дискеты, карты и т.п.;
- для фотодокументов - маркированные и пронумерованные кассеты с фотопленкой, фотобумага, микрофиши, слайды, кассеты с микрофотопленкой.

5.3. Основные задачи учета носителей персональных данных:

- закрепление факта присвоения носителю категории конфиденциальности, ограниченного доступа;
- присвоение носителю учетного номера и включение его в справочно-информационный банк для обеспечения контроля за использованием и проверки

наличия;

- документирование фактов перемещения носителя между сотрудниками Организации, закрепление персональной ответственности за его сохранность;
- контроль работы исполнителя над документом и своевременного уничтожения носителя или его частей, потерявших практическое значение и составлению акта об уничтожении носителя персональных данных.

5.4. При учете носителей реализуются следующие требования обеспечения защиты персональных данных:

- формирование основы для последующей персональной ответственности сотрудника за сохранность носителя, повышенного внимания к нему;
- предупреждение возможности нецелевого использования носителя или его неправильного хранения;
- формирование грифа конфиденциальности будущего документа;
- предупреждение возможности тайной подмены носителя, изъятия из него или включения в него отдельных частей (листов, частей фото-, видео- или магнитной пленки), для чего фиксируются технические характеристики носителя (количество листов, длина ленты, наличие склеек и др.);
- предупреждение технической возможности тайной разборки кассет, пеналов, футляров, конвертов и иных оболочек, содержащих технические носители информации;
- включение носителя в сферу регулярного контроля сохранности и местонахождения.

5.5. Обязательному инвентарному учету и маркировке подлежат магнитные носители персональных данных, для которых любые угрозы представляют значительно большую опасность, чем для бумажных, а обнаружение реализации этих угроз возможно только на основе сложных аналитических наблюдений.

5.6. Этапы оформления и учета носителей персональных данных, выдачи их исполнителям и приема от исполнителей выполняются как в традиционном, так и автоматизированном режимахи включают в себя следующие процедуры:

- первичное оформление носителя, в процессе которого выполняются специализированные операции, позволяющие в дальнейшем контролировать подлинность носителя и сохранность всех его элементов;
- традиционный или автоматизированный учет носителя, при котором документируется факт включения носителя в категорию носителей ограниченного доступа с присвоением ему инвентарного номера;
- окончательное оформление носителя, в процессе которого учетные данные переносятся на носитель и его составные части для их идентификации;
- выдача учтенного, укомплектованного носителя персональных данных исполнителю, закрепление за исполнителем персональной ответственности за сохранность носителя, его целостность и целевое использование;
- выдача исполнителю при необходимости дополнительных учтенных листов, форм и бланков;
- прием от исполнителя носителя информации, в процессе которого проверяются комплектность носителя, наличие оправдательных отметок за отсутствующие элементы и документирование факта передачи носителя;
- ежедневная проверка правильности учета носителей и их наличия.

6. Порядок применения средств организации архивирования, резервирования и восстановления прикладного программного обеспечения и персональных данных

6.1. Ответственный осуществляет контроль за процессом архивирования, резервирования и восстановления прикладного программного обеспечения и персональных данных.

6.2. Средства организации архивирования и восстановления прикладного программного обеспечения должны устанавливаться на всех средствах вычислительной техники,эксплуатируемых в Организации.

6.3. Порядок применения средств организации архивирования и восстановления прикладного программного обеспечения устанавливается с учетом соблюдения следующих требований:

- обязательное хранение всех архивов в защищенном месте;
- частота архивации данных зависит от их важности и частоты их изменения;
- системные папки операционной системы необходимо архивировать после серьезных изменений конфигурации;
- данные, которые изменяются очень редко, не имеет смысла архивировать.
- восстановление работоспособности программных средств и информационных массивов, в случае утери и повреждения.

6.4. Организации архивирования и восстановления прикладного программного обеспеченияподлежат следующие файлы и документы:

- все файлы операционной системы и установленных приложений. Архивирование
  системных файлов должно производиться только после установки
  новых приложенийили обновления самой операционной системы;
- личные профили пользователей;
- папки, содержащие важные документы;
- базы данных;
- другие файлы и папки, представляющие ценность.

6.5. К техническим мерам обеспечения непрерывной работы и восстановления относятся программные, аппаратные и технические средства и системы, используемые для предотвращения возникновения инцидентов, такие как:

- системы жизнеобеспечения;
- системы обеспечения отказоустойчивости;
- системы резервного копирования и хранения данных;
- системы контроля физического

доступа.Системы жизнеобеспечения

ИСПДн включают:

- пожарные сигнализации и системы пожаротушения;
- системы вентиляции и кондиционирования;
- системы резервного питания.

6.6. Все критичные помещения Организации (помещения, в которых размещаются элементы ИСПДн и средства защиты) должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

6.7. Для выполнения требований по эксплуатации (температура,

относительная влажность воздуха) программно-аппаратных средств ИСПДн в помещениях, где они установлены, должны применяться системы вентиляции и кондиционирования воздуха.

6.8. Для предотвращения потерь информации при кратковременном отключении электроэнергии все ключевые элементы ИСПДн, сетевое и коммуникационное оборудование, а также наиболее критичные рабочие станции должны подключаться к сети электропитания через источники бесперебойного питания. В зависимости от необходимого времени работы ресурсов после потери питания могут применяться следующие методы резервного электропитания:

- локальные источники бесперебойного электропитания с различным временемпитания для защиты отдельных компьютеров;
- источники бесперебойного питания с дополнительной функцией защиты от скачков напряжения;
- дублированные системы электропитания в устройствах (серверы, концентраторы,мосты и т. д.);
- резервные линии электропитания в пределах комплекса зданий;
- аварийные электрогенераторы;
- системы обеспечения отказоустойчивости (кластеризация; технология RAID).

6.9. Резервное копирование и хранение данных должно осуществлять на периодическойоснове:

- для обрабатываемых персональных данных – не реже раза в неделю;
- для технологической информации – не реже раза в месяц;
- эталонные копии программного обеспечения (операционные системы, штатное и специальное программное обеспечение, программные средства защиты), с которых осуществляется их установка на элементы ИСПДн – не реже раза в месяц, и каждый раз при внесении изменений в эталонные копии (выход новых версий).

6.10. Данные о проведение процедуры резервного копирования, должны отражаться в специально созданном журнале учета.

6.11. Носители должны храниться в несгораемом шкафу или помещении оборудованном системой пожаротушения.

6.12. Носители должны храниться не менее года, для возможности восстановления данных.

7. Проведение внутреннего расследования по фактам разглашения персональных данных, нарушения условий функционирования системы обработки и защиты персональных данных

7.1. Основными целями проведения внутреннего расследования являются:

— выявление предпосылок утраты персональных данных в результате нарушения порядкаих обработки;

— выявление лиц из числа сотрудников Организации виновных в утрате персональных данных;

— определение ущерба в результате утраты персональных данных;

— проверка полноты и качества исполнения нормативных документов по работе со средствами защиты персональных данных;

— документальное подтверждение соответствия обработки, хранения и

передачи персональных данных нормам и правилам, установленным федеральными правовыми и нормативными актами;

— определение фактического состояния системы защиты персональных данных.

7.2. Работник, по вине которого произошло нарушение, обязан по требованию Ответственного представить объяснения в письменной форме не позднее одного рабочего дня с момента получения соответствующего требования. Ответственный вправе увеличить указанный срок, а также поставить перед работником перечень вопросов, на которые работник обязан ответить.

7.3. В целях внутреннего расследования все работники Организации, по первому требованию Ответственного, должны предъявить для проверки все числящиеся за ними материалы, содержащие персональные данные, представить устные или письменные объяснения, в том числе об известных им фактах разглашения персональных данных, утраты документов и изделий, содержащих персональные данные.

7.4. В случае давления на работника со стороны других работников или третьих лиц (просьб, угроз, шантажа и др.) по вопросам, связанным с проведением внутреннего расследования, работник обязан сообщить об этом Ответственному.

7.5. Для проведения внутреннего расследования Руководитель формирует комиссию из опытных и квалифицированных работников в составе не менее трех человек. Председателем комиссии является Ответственный.

7.6. До вынесения решения, членам комиссии запрещается разглашать сведения остальным работникам Организации о ходе проведения внутреннего расследования и ставших известными имв связи с этим обстоятельствах.

7.7. В процессе проведения внутреннего расследования выясняются:

- перечень разглашенных сведений, составляющих персональные данные;
- причины разглашения персональных данных;
- круг лиц, виновных в разглашении персональных данных;
- размер причиненного ущерба;
- недостатки и нарушения, допущенные работниками при работе с персональнымиданными;
- иные обстоятельства.

7.8. По результатам расследования, комиссией составляется акт, с отражением в нем лиц, виновных в разглашении персональных данных, размера причиненного ущерба Организации, наличии ущерба субъектам персональных данных, а также иных выясненных обстоятельствах.

7.9. На основании акта комиссия выносит решение о:

- применении мер дисциплинарного воздействия к работнику;
- информировании регулятора о факте нарушения;
- информировании правоохранительных органов;
- информировании субъектов персональных данных.

8. Порядок реагирования на аварийную ситуацию

8.1. Под аварийной ситуацией понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИСПДн, предоставляемых пользователям ИСПДн.

8.2. Все действия в процессе реагирования на аварийные ситуации должны документироваться Ответственным в «Журнале по учету мероприятий по контролю».

8.3. В кратчайшие сроки, не превышающие одного рабочего дня, Ответственный за реагирование предпринимает меры по восстановлению нарушенной работоспособности. Предпринимаемые меры по возможности согласуются с вышестоящим руководством. По необходимости, иерархия может быть нарушена, с целью получения высококвалифицированной консультации в кратчайшие сроки.

8.4. При реагировании на инцидент, важно правильно классифицировать критичность инцидента. Критичность оценивается на основе следующей классификации:

Уровень 1 – Незначительный инцидент. Незначительный инцидент определяется как локальное событие с ограниченным разрушением, которое не влияет на общую доступность элементов ИСПДн и средств защиты.

Уровень 2 – Авария. Любой инцидент, который приводит или может привести к прерыванию работоспособности отдельных элементов ИСПДн и средств защиты.

Уровень 3 – Катастрофа. Любой инцидент, приводящий к полному прерыванию работоспособности всех элементов ИСПДн и средств защиты, а также к угрозе жизни пользователей ИСПДн, классифицируется как катастрофа. Обычно к катастрофам относят обстоятельства непреодолимой силы (пожар, взрыв), которые могут привести к нарушению работоспособности ИСПДн и средств защиты на сутки и более.

8.5. К техническим мерам обеспечения непрерывной работы и восстановления относятся программные, аппаратные и технические средства и системы, используемые для предотвращения возникновения аварийных ситуаций, такие как:

— системы жизнеобеспечения;

— системы обеспечения отказоустойчивости;

— системы резервного копирования и хранения данных;

— системы контроля физического

доступа. Системы жизнеобеспечения

ИСПДн включают:

— пожарные сигнализации и системы пожаротушения;

— системы вентиляции и кондиционирования;

— системы резервного питания.

8.6. Все критичные помещения Организации (помещения, в которых размещаются элементы ИСПДн и средства защиты) должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

9.10. Ответственным должно быть проведено обучение должностных лиц, имеющих доступ к ресурсам ИСПДн, порядку действий при возникновении аварийных ситуаций. Должностные лица должны получить базовые знания в следующих областях:

— оказание первой медицинской помощи;

— пожаротушение;

— эвакуация людей;

— защита материальных и информационных ресурсов;

— методы оперативной связи со службами спасения и лицами,

ответственными за реагирование сотрудниками на аварийную ситуацию;

— выключение оборудования, электричества, водоснабжения, газоснабжения.

9.11. Администратор безопасности должен быть дополнительно обучен методам частичного и полного восстановления работоспособности элементов ИСПДн.

9.12. Навыки и знания должностных лиц по реагированию на аварийные ситуации должны регулярно проверяться. При необходимости должно проводиться дополнительное обучение должностных лиц порядку действий при возникновении аварийной ситуации.

9. Организация режима безопасности помещений, где осуществляется работа с персональными данными

9.1. Первичный (основной) метод – система контроля и управления доступом в здание организации, включает в себя:

— наличие при входе в здание пункта контрольного пропуска;

— наличие вневедомственной службы охраны;

— определение внешнего контролируемого периметра.

9.2. Вторичный (дополнительный) метод – система контроля перемещения лиц в здании и управления доступом в помещения, включает в себя:

— наличие помещений с активным сетевым оборудованием с определенными правами доступа;

— наличие охранной и пожарной сигнализаций в помещениях Организации;

— использование кодовых замков и иных технических средств ограничения доступа в помещения;

— использование сейфов, шкафов, а также хранение информации с ПДн на внутренних ивнешних носителях.

9.3. Ограничение доступа посторонних лиц в помещения, предназначенные для осуществления профессиональной деятельности, связанной с эксплуатацией ИСПДн, предусматривает следующие:

— Исключение возможности бесконтрольного проникновения в эти помещения посторонних лиц, включая работников других структурных подразделений.

— После окончания рабочего дня двери помещений, в которых эксплуатируется ИСПДн, закрываются на ключ и опечатывается персональным пломбиром. Все помещения имеют разные замки. Дубликаты ключей хранятся в запираемом шкафу у Ответственного. В случае выхода из помещения в течение рабочего дня всех работников, дверь помещения закрывается на ключ.

— Уборка помещения производится в присутствии одного из сотрудников, работающего вэтом помещении.

— Доступ работников в помещения подразделения по выходным и праздничным дням осуществляется только по предварительному распоряжению уполномоченных лиц.

— Строгое ограничение доступа посторонних лиц к серверам, а также сетевому оборудованию.

— Защита мест хранения носителей (USB flash-накопитель, CD, ГМД) от беспрепятственного доступа посторонних лиц.

11. Приостановление обработки персональных данных

11.1. При выявлении недостоверных персональных данных или неправомерных действий с ними при обращении или по запросу субъекта персональных данных или его законного представителя либо уполномоченного органа по защите прав субъектов персональных данных необходимо осуществить блокирование персональных данных, относящихся к соответствующему субъекту персональных данных (приостановки предоставления персональных данных пользователям ИСПДн), с момента такого обращения или получения такого запроса на период проверки.

11.2.В случае подтверждения факта недостоверности персональных данных на основании документов, представленных субъектом персональных данных или его законным представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов требуется уточнить персональные данные и снять их блокирование.

11.3.В случае выявления неправомерных действий с персональными данными в срок, не превышающий трех рабочих дней с даты такого выявления, необходимо устранить допущенные нарушения. В случае невозможности устранения допущенных нарушений в срок, не превышающий трех рабочих дней с даты выявления неправомерности действий с персональными данными, необходимо уничтожить персональные данные. Об устранении допущенных нарушений или об уничтожении персональных данных Организации обязано уведомить субъект 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.

11.4.В случае достижения цели обработки персональных данных необходимо незамедлительно прекратить обработку персональных данных и уничтожить соответствующие персональные данные в срок, не превышающий трех рабочих дней с даты достижения цели обработки персональных данных, если иное не предусмотрено федеральными законами, и уведомить об этом субъект персональных данных или его законного представителя, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектовперсональных данных, - также указанный орган.

11.5.В случае отзыва субъектом персональных данных согласия на обработку своих персональных данных требуется прекратить обработку персональных данных и уничтожить их в срок, не превышающий трех рабочих дней с даты поступления указанного отзыва, если иное не предусмотрено соглашением между Организацией и субъектом персональных данных. Об уничтожении персональных данных необходимо уведомить субъект персональных данных.

11.6. В случае прекращения полномочий работника Администратором безопасности ИСПДн приостанавливается предоставление ему персональных данных, а также немедленно производиться смена пароля после окончания последнего сеанса работы данного пользователя с системой.

Приложение .
к приказу № 125 от 01.09.2023 год
«О назначении ответственных за обработку персональных данных»

Положение
о порядке деятельности комиссии по уничтожению персональных данных, обрабатываемых сотрудниками муниципального автономного дошкольного образовательного учреждения центра развития ребенка - детского сада № 6 г. Курганинска

1. Общие положения

1.1. Настоящее Положение устанавливает порядок формирования и деятельности комиссии по уничтожению персональных данных, обрабатываемых сотрудниками комитета по народному образованию (далее – комитет), в соответствии с Федеральным законом Российской Федерации от 27.06.2006 г. № 152-ФЗ «О персональных данных», нормативно-правовыми актами Российской Федерации в области защиты персональных данных.

1.2. Целями данного Положения является обеспечение в соответствии с законодательством Российской Федерации порядка соблюдения конфиденциальности, обеспечения прав и свобод человека и гражданина, что достигается путем уничтожения персональных данных, содержащихся в документах и иных носителях, полученных из других организаций, в обращениях граждан и иных субъектов персональных данных, по достижению целей их обработки.

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

2. Порядок формирования комиссии

2.1. Комиссия по уничтожению персональных данных, содержащихся в документах и иных носителях, обрабатываемых школой, формируется из руководителя, сотрудников, ответственных за автоматизированную и неавтоматизированную обработку персональных данных, зам заведующей по АХР. Данный состав является постоянно действующим.

2.2. В обязательном порядке в состав комиссии, помимо постоянно действующих членов, включается сотрудник, который обрабатывал уничтожаемые персональные данные.
2.3. Председателем комиссии является руководитель ДОУ .

3. Порядок деятельности комиссии

3.1. Комиссия по уничтожению персональных данных собирается 2 раза в год; в случае необходимости возможно внеплановое заседание комиссии.
3.2. Сроки хранения носителей, содержащих персональные данные, обрабатываемых сотрудниками ДОУ, устанавливаются действующим законодательством, локальными актами ДОУ.
3.3. В течение срока хранения персональные данные не могут быть уничтожены.
3.4. При уничтожении персональных данных комиссией составляется акт об уничтожении персональных данных, который подписывается всеми членами комиссии (приложение 2).

4. Ответственность членов комиссии

4.1. Члены комиссии несут ответственность, предусмотренную действующим законодательством, за разглашение конфиденциальной информации, ставшейим известной в связи с выполнением возложенных на них обязанностей.

УТВЕРЖДАЮ

Заведующая МАДОУ ЦРР № 6

_____Н.Ю. Тимченко

«____»_____202___г.

А К Т №

уничтожения персональных данных и иной конфиденциальной информации

	«		»		20___г
Место уничтожения				Дата уничтожения	

Комиссия, в составе:

1)_____

2)_____

3)_____

4)_____,

5)_____

составили настоящий акт в том, что «____»_____20____г. произведено уничтожение персональных данных или иной конфиденциальной информации, находящейся на

_____

_____

(вид носителя информации, тип удаляемой конфиденциальной информации, способуничтожения информации):

№ п/п	Информация (наименование документа)	Вид носителя, ед. измер.	Коли-чество	Срок хранения

Подписи членов комиссии:

_____ _____

(подпись) (Ф. И. О.)

_____ _____

(подпись) (Ф. И. О.)

_____ _____

(подпись) (Ф. И. О.)

_____ _____

(подпись) (Ф. И. О.)