**ДЕПАРТАМЕНТ СОЦИАЛЬНОЙ ПОЛИТИКИ**

**МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ**

**«ДЕТСКИЙ САД КОМБИНИРОВАННОГО ВИДА № {number} «{name}»**

**ПРИКАЗ**

«\_\_»\_\_\_\_\_\_\_\_ 201\_\_ года № \_\_\_\_\_

г. Курган

**Об утверждении требований по**

**обеспечению безопасности персональных**

**данных при обработке в информационных**

**системах персональных данных**

В целях выполнения требований Федерального закона РФ от 27.07.2006 № 152-ФЗ

«О персональных данных»

ПРИКАЗЫВАЮ:

1. Утвердить требования по обеспечению безопасности персональных данных при обработке в информационных системах персональных данных (Приложение №1).
2. Контроль за исполнением приказа оставляю за собой.

Заведующий МБДОУ

«Детский сад № {number}» {FIO1}

С приказом ознакомлена: {FIO2}

Приложение №1

к Приказу

№\_\_\_ от «\_\_» \_\_\_\_\_\_\_ 201\_г.

### ТРЕБОВАНИЯ

### по обеспечению безопасности персональных данных при обработке в информационных системах персональных данных

1. Общие положения
   1. Данные требования по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (далее - ИСПДн) разработаны на основании:

* «Основных мероприятий по организации и техническому обеспечению безопасности персональных данных при обработке в информационных системах персональных данных», утвержденных 15 февраля 2008 г. заместителем директора ФСТЭК России,
* Федерального Закона от 27 июля 2006 г. №152-ФЗ «О персональных данных».
* Постановления Правительства РФ от 21 марта 2012 г. N 211 "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами".
* Постановления Правительства РФ от 1 ноября 2012 г. N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных".
* Постановления Правительства РФ от 15 сентября 2008 г. N 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации".
* Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденным постановлением Правительства Российской Федерации от 17 ноября 2007 года № 781;
* Положения о методах и способах защиты информации в информационных системах персональных данных, утвержденным приказом Федеральной службы по техническому и экспортному контролю от 05 февраля 2010 года № 58.
* Приказа ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащийся в государственных информационных системах».
* Приказа ФСТЭК России от 11 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
  1. Требования определяют совокупность организационных и технических мероприятий необходимых для обеспечения заданного уровня безопасности персональных данных при их обработке в ИСПДн.

1. Организационные мероприятия по обеспечению безопасности персональных данных
   1. С целью парирования угроз безопасности ИСПДн должен быть реализован следующий комплекс организационных мероприятий, определяющий порядок:

* охраны помещения, в котором расположены ИСПДн;
* допуска персонала в помещение, в котором расположена ИСПДн, а также порядок приема в них посторонних;
* выбора для использования в ИСПДн технических средств;
* расположения технических средств ИСПДн относительно границ пространства (территории, помещения), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств;
* поддержания целостности персональных данных.
  1. Охрана помещения, в котором расположена ИСПДн, должна удовлетворять следующим требованиям:
* вскрытие и закрытие служебного помещения производится сотрудниками, осуществляющими в них трудовую деятельность, закрепленную должностными обязанностями;
* при закрытии помещения и сдаче его под охрану сотрудники обязаны проверить закрытие окон, выключить освещение, бытовые приборы, средства вычислительной техники и проверить противопожарное состояние помещения (при наличии охранной сигнализации);
* при обнаружении повреждения замков (запоров) или наличия других признаков, указывающих на возможное проникновение в служебное помещение посторонних лиц, помещение не вскрывается, а составляется акт, в присутствии сотрудника, осуществляющего охрану. О происшествии немедленно сообщается ответственному за организацию обработки персональных данных.
* при срабатывании охранно-пожарной сигнализации в служебном помещении в нерабочее время сторож (охранник) должен немедленно уведомить ответственною за данное помещение и ответственного за организацию обработки персональных данных;
  1. Допуск лиц в помещение, в котором расположены технические средства ИСПДн, должен соответствовать следующим требованиям:
* в рабочее время допуск лиц в помещение может осуществляться только в присутствии ответственного сотрудника за помещение;
* при уходе сотрудников из помещения, оно должно закрываться на ключ; прием посторонних лиц в данном помещении, как правило, должен быть исключен; в случае приема в помещении посторонних лиц обработка персональных данных должна быть приостановлена, а автоматизированные рабочие места ИСПДн заблокированы сертифицированными по требованиям безопасности информации средствами защиты информации;
* обработка персональных данных в ИСПДн должна проводиться при закрытых жалюзи (шторами) окнах и закрытых дверях.
  1. Выбор технических средств для использования в ИСПДн.

Технические средства, предполагаемые к использованию в ИСПДн должны удовлетворять требованиям стандартов Российской Федерации по электромагнитной совместимости, по безопасности и эргономическим требованиям к средствам отображения информации, по санитарным нормам, предъявляемым к видеодисплейным терминалам ПЭВМ, в том числе требованиям ГОСТ Р МЭК 60950-2002, ГОСТ 26329-84, ГОСТ Р 50948- 2001. ГОСТ Р 51318.22-99, ГОСТ Р51318.24-99, ГОСТ Р 51317.3.2-99, ГОСТ Р 51317.3.3-99, ГОСТ Р 50948-96, ГОСТ Р50949-96, ГОСТ Р50923-96, ГОСТ Р 50628-2000, ГОСТ 29216-91, СапПин 2.2.2.542-96.

* 1. Расположение технических средств ИСПДн в помещении должно осуществляться так, чтобы исключить просмотр текстовой и графической видовой информации, отображаемой устройствами отображения, входящими в состав ИСПДн, посторонними липами.
  2. Поддержание целостности персональных данных должно заключаться в выполнении следующих требований:
* электропитание технических средств ИСПДн, в которых происходит накопление и обработка персональных данных, должно осуществляться через источники бесперебойного питания, позволяющие в случае отключения электропитания закончить работу с массивами персональных данных в штатном режиме;
* подключение любых технических средств к ИСПДн (изменение их состава), а также установка любого программного обеспечения осуществляется только администратором ИСПДн;
* установка пользователями нештатного программного обеспечения, а также нештатных технических средств в ИСПДн ЗАПРЕЩАЕТСЯ;

с целью обеспечения безопасности персональных данных и восстановления работоспособности ИСПДн у администратора должны быть в наличии дистрибутивы (инсталляционные диски) общего и прикладного программного обеспечения, а также средств защиты информации;

с целью обеспечения безопасности персональных данных и возможности их восстановления должно проводиться их ежемесячное копирование на отчуждаемый носитель информации, учтенный в установленном порядке.

1. Организационные требования по обеспечению безопасности персональных данных (далее – ПДн) при обработке в ИСПДн.
   1. Должны быть определены:

* необходимость обработки персональных данных;
* перечень информации, подлежащей защите;
* конфигурация и топология ИСПДн, условия расположения данной ИСПДн относительно границ контролируемой зоны.
* технические средства и системы, предлагаемые к использованию в ИСПДн;
* перечень общесистемного и прикладного программного обеспечения, разрешенного к использованию в ИСПДн;
* перечень работников, допущенных к работе в ИСПДн и обработке ПДн;
* класс ИСПДн ( в соответствии с Приказом ФСТЭК № 21);
* уровень защищенности;
* угрозы безопасности ПДн в конкретных условиях функционирования;
* перечень используемых в ИСПДн средств защиты информации;
* планы организационно-технических мероприятий по защите информации;
* лица, ответственные за эксплуатацию средств защиты информации и обеспечение безопасности ПДн.

3.2. Должны быть разработаны и утверждены следующие организационно-распорядительные документы:

* Акт определения уровня защищенности ПДн при их обработке в ИСПДн (отдельно для каждой ИСПДн).
* Перечень ПДн, обрабатываемых в ИСПДн (отдельно для каждой ИСПДн).
* Перечень ПДн обрабатываемых, в неавтоматизированном виде (отдельно по каждого субъекта ПДн).
* Политика в отношении обработки персональных данных.
* Положение об обработке и защиты ПДн.
* Приказ о назначении ответственного за обработку ПДн.
* Должностная инструкция ответственного за обеспечение безопасности ПДн.
* Приказ о назначении администратора ИСПДн.
* Должностная инструкция администратора ИСПДн.
* Приказ о порядке распространения (передачи) персональных данных.
* Приказ о порядке взаимодействия по вопросам обеспечения безопасности персональных данных.
* Приказ об утверждении требований по обеспечению безопасности персональных данных при их обработке в ИСПДн.
* Приказ об утверждении Инструкция по резервированию и восстановлению информации в ИСПДн.
* Приказ о Контролируемой зоне (КЗ).
* Приказ о создании постоянно действующей комиссии по вопросам обработки и хранения персональных данных.
* Приказ об определении автоматизированных систем предназначенных для обработки и хранения ПДн.
* Приказ о закреплении сотрудников к автоматизированным систем.
* Приказ об определении материальных носителей ПДн.
* Приказ об определении мест хранения ПДн.
* Приказ об утверждении лиц ответственных за хранение материальных носителей ПДн.
* Приказ об определении помещений предназначенных для обработки и хранения ПДн.
* Приказ о внесении изменений в сведения в реестре операторов, осуществляющих обработку персональных данных.
* Информационное письмо о внесении изменений в сведения в реестре операторов, осуществляющих обработку персональных данных.
* Приказ об утверждении типовой формы акта уничтожения ПДн.
* Регламент обработки запросов субъекта персональных данных или уполномоченного органа по защите прав субъектов персональных данных и форм обращений.
* Регламент осуществления внутреннего контроля за обеспечением уровня защищенности персональных данных.
* Приказ об утверждении списка сотрудников допущенных к персональным данным.
* Приказ об утверждении типовых форм журналов.
* Приказ об утверждении типовой формы Согласия на обработку ПДн.
* Приказ об утверждении типовой формы обязательства о неразглашении информации, содержащей персональные данные.
* Разработка типовой формы договора по передаче персональных данных третьей стороне.
* Приказ об утверждении Плана мероприятий по защите ПДн (отдельно по автоматизированной и не автоматизированной обработке).
* План мероприятий по защите ПДн (отдельно по автоматизированной и не автоматизированной обработке).
* Приказ об утверждении Плана внутренних проверок ИСПДн и обработки персональных данных в не автоматизированном виде.
* План внутренних проверок ИСПДн и обработки персональных данных в не автоматизированном виде.
* Приказ об утверждении перечня резервируемой информации.
* Приказ об определении положения и формы журнала об использовании сети Интернет.
* Инструкция по работе в сети.
* Приказ об утверждении списка лиц имеющих право доступа в помещения,
* Приказ об утверждении правил допуска в помещения, где обрабатывается (хранятся) ПДн.
* Приказ об утверждении инструкции пользователя.
* Приказ об утверждении инструкции по ремонту (модернизации) ПЭВМ.
* Приказ об утверждении инструкции по работе с бумажными носителями ПДн.
* Приказ об утверждении инструкции по паролям.
* Приказ об утверждении инструкции по опечатыванию помещений.
* Приказ об утверждении инструкции машинным носителям информации (МНИ).
* Приказ об утверждении инструкции по антивирусному обеспечению.
* Приказ об утверждении инструкции по обезличиванию ПДн.
* Журнал учета хранилищ ПДн.
* Журнал учета МНИ.
* Журнал внутренних проверок.
* Журнал инструктажа по ПДн.
* Журнал проверок госорганами ПДн.
* Журнал учета обращений субъектов ПДн.
* Журнал учета ПДн.
* Журнал учета носителей СЗИ и Криптографических средств (КС).
* Журнал регистрации инструктажа пользователей Интернет.
* Журнал регистрации использования сети Интернет.
* Модель угроз.
* Технологический процесс обработки информации в информационных системах обрабатывающих персональные данные.

1. Мероприятия по обеспечению безопасности персональных данных от несанкционированного доступа при их обработке в информационной системе персональных данных
   1. В комплекс мероприятий по защите персональных данных (далее - ПДн) при их обработке в ИСПДн от несанкционированного доступа (далее - НСД) и неправомерных действий входят следующие направления:

* зашита от НСД при многопользовательском режиме обработки ПДн и равных правах доступа к ним субъектов доступа;
* антивирусная защита;
* обнаружение вторжений.

Мероприятия по защите ПДн реализуются в рамках подсистем:

* управления доступом;
* регистрации и учета;
* обеспечения целостности;
* антивирусной защиты.

1. Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных
   1. Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных в ИСПДн определяются следующими нормативными документами:

* Приказа ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащийся в государственных информационных системах».
* Приказа ФСТЭК России от 11 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».