Приложение
к приказу директора МБОУ СОШ № 30
г.Южно-Сахалинска
от 12.03.2014 №83-ОД

ПОЛОЖЕНИЕ
по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных в МБОУ СОШ №30 г.Южно-Сахалииска

1. Термины и определения

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

1.2. 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.

1.3. Информационная система персональных данных (далее - 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.

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

1.5. Конфиденциальность персональных данных - обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных.

1.6. Администратор безопасности персональных данных - юридическое или физическое лицо, организующее и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

1.7. Ответственный сотрудник за обеспечение безопасности персональных данных - лицо, которому на основании договора администратор поручает обработку персональных данных.

II.Общие положения

2.1. Настоящее положение устанавливает требования к обеспечению безопасности персональных данных при их обработке в ИСПДн, представляющих собой совокупность персональных данных, содержащихся в базах данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием и без использования средств автоматизации, в МБОУ СОШ №30 г.Южно-Сахалинска.

2.2. Настоящее Положение разработано в соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении Требований к защите персональных данных при их обработке в информационных системах персональных данных».

2.3. Обработка персональных данных в МБОУ СОШ №30 г .Южно-Сахалинска осуществляется на основе принципов:

- законности целей и способов обработки персональных данных;
- соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям администратора безопасности персональных данных ;
- соответствия объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;
- достоверности персональных данных, их достаточности для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;
- недопустимости объединения созданных для несовместимых между собой целей баз данных информационных систем персональных данных.

III. Порядок определения защищаемой информации

3.1. Ответственный за обеспечение безопасности персональных данных МБОУ СОШ №30 г.Южно-Сахалинска создают в пределах своих полномочий, установленных в соответствии с федеральными законами, школьную ИСПДн, в целях обеспечения реализации прав объектов персональных данных.

3.2. В МБОУ СОШ №30 г.Южно-Сахалинска на основании «Перечня сведений конфиденциального характера», утвержденного Указом Президента Российской Федерации 6 марта 1997 года № 188, определяется и утверждается перечень сведений ограниченного доступа, не относящихся к государственной тайне (далее конфиденциальной информации) и перечень информационных систем персональных данных. Определяется и утверждается список сотрудников школы, которые осуществляют обработку конфиденциальной информации и персональных данных.

3.3. На стадии проектирования каждой ИСПДн определяются цели и содержание обработки персональных данных, утверждается перечень обрабатываемых персональных данных.

IV. Основные условия проведения обработки персональных данных

4.1. Обработка персональных данных осуществляется:

- после получения согласия субъекта персональных данных, составленного по форме согласно приложению 1 к настоящему Положению или сформированного в информационной системе персональных данных, за исключением случаев, предусмотренных частью 2 статьи 6 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;
- после направления уведомления об обработке персональных данных в Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Вологодской области за исключением случаев, предусмотренных частью 2 статьи 22 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

4.2 Ответственный сотрудник ИСПДн, организующим и осуществляющим обработку персональных данных, а также определяющим цели и содержание обработки персональных данных является МБОУ СОШ №30 г.Южно-Сахалинска. Обязанности ответственного сотрудника в установленном порядке возлагаются на сотрудников МБОУ СОШ №30 г.Южно-Сахалинска, осуществляющие деятельность по эксплуатации ИСПДн.

4.3. Ответственный сотрудник при обработке персональных данных обязан принимать необходимые организационные и технические меры *для* зашиты персональных данных от неправомерного или случайного доступа к ним. уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий.

4.4. Для разработки и осуществления мероприятий по обеспечению безопасности персональных данных при их обработке в ИСГЩн назначается должностное лицо, ответственное за обеспечение безопасности персональных данных.

4.5. Директор МБОУ СОШ №30 г.Южно-Сахалинска, в чьём ведении находится ИСПДн, определяют сотрудников, допущенных к обработке персональных данных и

представляют списки данных лиц администратору по безопасности обработки персональных данных.

4.6. Сотрудники, допущенные к обработке персональных данных, в обязательном порядке под роспись знакомятся с настоящим Положением и подписывают обязательство о неразглашении информации, содержащей персональные данные, по форме согласно приложения 2 к настоящему Положению. Должностные инструкции сотрудников, допущенных к обработке персональных данных, должны содержать сведения о допуске к персональным данным и основания, на котором данный допуск осуществлен (наименование, дата и номер соответствующего федерального закона).

4.7. Ответственный сотрудник и третьи лица, получающими доступ к персональным данным, должна обеспечиваться конфиденциальность таких данных. Ответственный сотрудник или иное получившее доступ к персональным данным лицо обязано не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

4.8. В случае, если ответственный сотрудник на основании договора поручает обработку персональных данных другому лицу, существенным условием договора является обязанность обеспечения указанным лицом конфиденциальности персональных данных и безопасности персональных данных при их обработке.

V. Правила обработки и защиты персональных данных в информационных системах с использованием и без использования средств автоматизации

5.1. Обработка персональных данных в ИСПДн с использованием средств автоматизации осуществляется в соответствии с требованиями «Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденного постановлением Правительства Российской Федерации от 01.11.2012 № 1119, нормативных и руководящих документов уполномоченных федеральных органов исполнительной власти.

5.2. Обработка персональных данных без использования средств автоматизации (в виде документов на бумажных носителях и в электронном виде (файлы, базы банных) на электронных носителях информации) осуществляется в соответствии с «Положением об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», утвержденным Постановлением Правительства Российской Федерации 15.09.2008 № 687.

5.3. Администратором осуществляется классификация информационных ■ систем персональных данных в соответствии с Приказом ФСТЭК России, ФСБ России. Мининформсвязи России от 13.02.2008 № 55/86/20 "Об утверждении Порядка проведения классификации информационных систем персональных данных" в зависимости от категории обрабатываемых данных и их количества.

5.4. Мероприятия по обеспечению безопасности персональных данных на стадиях проектирования и ввода в эксплуатацию объектов информатизации проводятся в соответствии с «Основными мероприятиями по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в ИСПДн», утвержденными ФСТЭК Росси от 15.02.2008.

5.5. На стадии ввода в эксплуатацию ИСПДн проводится ее оценка соответствия требованиям безопасности информации:

- для ИСПДн 1 и 2 классов - обязательная сертификация (аттестация) требованиям безопасности информации;
- для ИСПДн 3 класса декларирование соответствия или обязательная сертификация (аттестация) по требованиям безопасности информации (по решению администратора);
- для ИСПДн 4 класса оценка соответствия проводится по решению администратора.

5.6. Не допускается обработка персональных данных в ИСПДн с использованием средств автоматизации при отсутствии:

- утвержденных организационно-технических документов о порядке эксплуатации информационных систем персональных данных, включающих акт классификации ИСПДн, инструкции пользователя, администратора по организации антивирусной защиты,

парольной защиты автоматизированных систем, и других нормативных и методических документов;

- настроенных средств защиты от несанкционированного доступа, средств антивирусной защиты, резервного копирования информации и других программных и технических средств в соответствии с требованиями безопасности информации;

- охраны и организации режима допуска в помещения, предназначенные для обработки персональных данных;

- аттестата (декларации) о соответствии требованиям безопасности информации.

VI. Требовании к обработке и защите персональных данных в информационных системах без использовании средств автоматизации

6.1 Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных были:

- определены места хранения персональных данных (материальных носителей) и установлен перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ;

- обеспечено раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях;

- соблюдены условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ.

6.2. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее - типовые формы), должны соблюдаться следующие условия:

а) типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели неавтоматизированной обработки персональных данных, имя (наименование) и адрес оператора, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки персональных данных;

б) типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на неавтоматизированную обработку персональных данных, - при необходимости получения письменного согласия на обработку персональных данных:

в) типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;

г) типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

6.3. При использовании внешних электронных носителей информации с персональными данными, к ним предъявляются следующие требования:

а) электронные носители информации, содержащие персональные данные, учитываются в журнале учета, выдачи и уничтожения машинных носителей данных, предназначенных для обработки и хранения информации ограниченного доступа, не относящейся к государственной тайне, персональных данных, в мэрии города;

б) к каждому электронному носителю оформляется опись файлов, содержащихся на нем, с указанием цели обработки и категории персональных данных.

6.4. Все документы, содержащие персональные данные, должны храниться в служебных помещениях в надежно запираемых и опечатываемых шкафах (сейфах). При этом должны быть созданы условия, обеспечивающие их сохранность.

VII. Порядок привлечения специализированных сторонних организаций к разработке ИСПДн и средств защиты информации МБОУ СОШ №30 г.Южно- Сахалинска

7.1. Порядок привлечения специализированных сторонних организаций к разработке и эксплуатации новых ИСПДн. их задачи и функции на различных стадиях создания и эксплуатации ИСПДн определяются директором МБОУ СОШ № №30, в чем ведении находится создаваемая ИСПДн, исходя из особенностей автоматизированных систем и по согласованию с заместителем директора по информатизации и защиты информации.

7.2. Разработка систем защиты персональных данных в ИСПДн МБОУ СОШ №30. г.Южно-Сахалинска контроль за эксплуатацией ИСПДн администратором по защите информации.

7.3. Без наличия соответствующих лицензий проведение мероприятий по защите персональных данных возможно только для нераспределенных информационных систем третьего класса, а также для информационных систем четвертого класса.

VIII. Ответственность должностных лиц

Сотрудники, допущенные к персональным данным, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных,- несут дисциплинарную административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством Российской Федерации.