УТВЕРЖДЕНО
Приказом заведующего
МДОУ № 5 «Радуга»
№ 03-13/04 от 16.01.2016
_____И Г. Чистякова

П О Л О Ж Е Н И Е
О МЕРАХ ПО ОРГАНИЗАЦИИ ЗАЩИТЫ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ
в муниципальном дошкольном образовательном учреждении детский сад № 5 «Радуга»

Статья I. ОБЩИЕ ПОЛОЖЕНИЯ

1. Настоящее Положение о мерах по организации защиты информационных систем персональных данных в муниципальном дошкольном образовательном учреждении детский сад № 5 «Радуга» » (далее – Положение) устанавливает состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных МДОУ детский сад № 5 «Радуга»» на протяжении всего цикла их создания и эксплуатации.

Меры по обеспечению безопасности персональных данных принимаются для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

Меры по обеспечению безопасности персональных данных реализуются в рамках системы защиты персональных данных, создаваемой МДОУ детский сад № 5 «Радуга» в соответствии с Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными Постановлением Правительства Российской Федерации от 1 ноября 2012 года №1119, и должны быть направлены на нейтрализацию актуальных угроз безопасности персональных данных.

2. Настоящее Положение является внутренним локальным актом муниципального дошкольного образовательного учреждения детский сад общеразвивающего вида с приоритетным осуществлением познавательно – речевого развития воспитанников № 26 «Алёнушка» (далее – Организация).

Настоящее Положение вступает в силу с момента его утверждения заведующим Организации и действует бессрочно, до замены его новым Положением.

Настоящее Положение подлежит корректировке при изменении законодательных и нормативно-правовых актов, по рекомендациям надзорных органов, по результатам проверок в рамках государственного контроля, а также в целях совершенствования технологий обработки

ПДн.

Изменения к Положению утверждаются заведующим Организации.

3. Все работники Организации должны быть ознакомлены под подпись с данным Положением и изменениями к нему.

Настоящее Положение является обязательным для исполнения всеми работниками Организации, имеющими доступ к персональным данным.

4. Ответственность за актуализацию настоящего Положения и текущий контроль над выполнением норм Положения возлагается на назначаемого приказом по Организации уполномоченного сотрудника, ответственного за обеспечение информационной безопасности и защите персональных данных.

5. Положение разработано с учетом требований принятой в Организации Политики по защите персональных данных в муниципальном дошкольном образовательном учреждении детский сад комбинированного вида № 5 «Радуга». Организация учитывает требования настоящего Положения при разработке и утверждении внутренних локальных актов и иных документов Организации, связанных с обработкой ПДн.

Статья II. ОСНОВНЫЕ ПОНЯТИЯ, ОПРЕДЕЛЕНИЯ И СОКРАЩЕНИЯ

В Положении используются следующие понятия, определения и сокращения:

ПДн - персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу - субъекту персональных данных.

Обработка ПДн - любое действие с персональными данными, совершаемое с использованием средств автоматизации или без использования таких средств.

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

Автоматизированная обработка ПДн – обработка ПДн с помощью средств вычислительной техники.

Обработка ПДн без использования средств автоматизации - 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.

Актуальные угрозы безопасности персональных данных - совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом

которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

Система защиты персональных данных – СЗПДн - организационные и технические меры, определенные с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах.

Закон «О персональных данных» - Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».

Приказ ФСТЭК №21 - Приказ ФСТЭК России от 18.02.2013 года № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

Статья III. ТРЕБОВАНИЯ К ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

В информационной системе объектами защиты являются информация, содержащаяся в информационной системе, технические средства (в том числе средства вычислительной техники, машинные носители информации, средства и системы связи и передачи данных, технические средства обработки буквенно-цифровой, графической и видео информации), общесистемное, прикладное, специальное программное обеспечение, информационные технологии, а также средства защиты информации.

Для обеспечения защиты информации, содержащейся в информационной системе, Организацией назначается работник, ответственный за защиту информации.

Система защиты персональных данных включает в себя организационные и технические меры, определенные с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах.

Выбор средств защиты информации для системы защиты персональных данных осуществляется Организацией в соответствии с требованиями Приказа ФСТЭК России от 18.02.2013 года № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», а также другими нормативными правовыми актами, принятыми Федеральной службой безопасности Российской Федерации и Федеральной службой по техническому и экспортному контролю.

Определение типа угроз безопасности персональных данных, актуальных для информационных систем, производится Организацией с учетом оценки возможного вреда, проведенной во исполнение пункта 5 части 1 статьи 18[1] Закона «О персональных данных».

В связи с этим Организации необходимо классифицировать информационные системы в зависимости от того, какие категории персональных данных в ней обрабатываются и какие типы

угроз актуальны для ИСПДн Организации. По результатам требуется определить набор требований, которые необходимо выполнить для обеспечения того уровня защищенности ПДн, который был определен при классификации ИСПДн Организации.

Оценка эффективности реализованных в рамках системы защиты персональных данных мер по обеспечению безопасности персональных данных, и контроль за выполнением требований к защите ПДн при обработке их в ИСПДн организуется и проводится Организацией самостоятельно, не реже 1 раза в 3 года в сроки, определяемые Организацией.

Статья IV. ОСНОВНЫЕ МЕРЫ ПО СОЗДАНИЮ СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Состав и содержание организационных мер по обеспечению безопасности ПДн

Для обеспечения необходимого уровня защищенности персональных данных при их обработке в информационных системах Организации необходимо принятие следующих основных организационных мер:

а) ввести режим обеспечения безопасности помещений, в которых размещены ИСПДн Организации, препятствующий возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

б) обеспечить безусловную сохранность носителей персональных данных;

в) назначить уполномоченного сотрудника, ответственного за обеспечение информационной безопасности и защиту персональных данных;

г) утвердить перечень персональных данных и иных объектов, подлежащих защите в ИСПДн Организации;

д) утвердить перечень лиц, доступ которых к персональным данным, обрабатываемым в ИСПДн Организации, необходим для выполнения ими служебных обязанностей;

ж) провести классификацию ИСПД Организации, по результатам определить набор требований, которые необходимо выполнить для обеспечения необходимого уровня защищенности ПДн;

з) обеспечить использование только таких средств защиты информации, которые прошли процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации;

и) обеспечить проведение не реже 1 раза в 3 года проверки эффективности реализованных в рамках системы защиты персональных данных мер по обеспечению безопасности персональных данных, и регулярный контроль за выполнением требований к защите ПДн при обработке их в ИСПДн.

Мероприятия по реализации организационных мер по обеспечению безопасности ПДн

С учетом требований, перечисленных в п.1. статьи 6. Положения, необходимо организовать

и провести ниже следующие мероприятия:

1. Назначить приказом заведующего Организации уполномоченного сотрудника, ответственного за обеспечение информационной безопасности и защиту персональных данных в информационных системах Организации. Разработать и ввести в действие должностную инструкцию, регламентирующие права и обязанности такого уполномоченного сотрудника.

2. Ввести в действие приказ заведующего «О создании Комиссии по приведению деятельности Организации в соответствие с требованиями законодательных и нормативных актов, регламентирующих обработку персональных данных» (далее по тексту – Комиссия по персональным данным»).

3. Разработать, утвердить и внедрить систему организации доступа в помещения Организации, где осуществляется обработка ПДн, исключающую возможность несанкционированного доступа к техническим средствам обработки ПДн, хищения и нарушения работоспособности ИСПДн, хищения носителей информации ПДн.

4. Определить состав и категории обрабатываемых в Организации персональных данных. Результат оформить в виде локального нормативного акта с перечнем персональных данных и иных объектов, подлежащих защите в Организации. Разработать и ввести в действие должностную инструкцию пользователя ИСПДн, регламентирующую права и обязанности работника Организации при работе с ИСПДн.

Разработать и ввести в действие локальный нормативный акт, регламентирующий разграничение прав доступа к обрабатываемым в ИСПДн персональным данным.

5. Разработать и ввести в действие инструкцию о порядке учета, использования, транспортировке, хранения и уничтожения в Организации съемных носителей персональных данных.

6. Провести учет съемных носителей ПДн, по результатам ввести в действие журнал учета съемных носителей ПДн.

7. В рамках внутренних локальных актов, регламентирующих обработку и защиту персональных данных работников, воспитанников и родителей (законных представителей) Организации, утвердить перечни подразделений и работников Организации, допущенных к обработке ПДн работников, воспитанников и родителей (законных представителей).

8. Разработать и ввести локальный нормативный акт об ответственности работников Организации за разглашение персональных данных и несанкционированный доступ к персональным данным.

9. Комиссии по персональным данным провести внутреннюю проверку и классификацию ИСПДн Организации. Разработать модель угроз ИСПДн и определить возможный ущерб, который может быть нанесен субъектам ПДн компрометацией их персональных данных. Результаты

оформить в виде письменных отчетов, на основании которых разработать план мероприятий по обеспечению безопасности ПДн в ИСПДн Организации.

2. Технические меры по обеспечению безопасности ПДн в ИСПДн

Организация должна принимать технические меры по обеспечению безопасности информационных систем персональных данных. Применение технических мер защиты, их количество и степень защиты зависят от того, какой уровень защищенности персональных данных при их обработке в ИСПДн необходимо обеспечить.

Статья V. ЛИЦА, ОТВЕТСТВЕННЫЕ В ОРГАНИЗАЦИИ ЗА ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Общее руководство деятельностью Организации по обеспечению безопасности ПДн осуществляет заведующий.

2. Заведующий приказом назначает уполномоченного сотрудника, ответственного за обеспечение информационной безопасности и защиту персональных данных в Организации.

2. Уполномоченный сотрудник, ответственный за обеспечение информационной безопасности и защиту персональных данных, получает указания непосредственно от заведующего.

3. Уполномоченный сотрудник, ответственный за обеспечение информационной безопасности и защиту персональных данных, в частности, обязан:

осуществлять внутренний контроль по соблюдению Организацией и его работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;

доводить до сведения работников Организации положения законодательства Российской Федерации о персональных данных, внутренних локальных нормативных актов, принятых в Организации по вопросам обработки и защите персональных данных;

организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей, и осуществлять контроль за приемом и обработкой таких обращений и запросов;

не реже одного раза в три года проводиться проверку состава и структуры ИСПДн, состава угроз безопасности ПДн в ИСПДн и эффективности реализованных в рамках СЗПДн мер по обеспечению безопасности персональных данных, при необходимости вносить предложения по доработке или модернизации системы защиты ПДн.

4. Заведующий приказом создает в Организации Комиссию по персональным данным, на которую возлагаются следующие обязанности:

реализации мероприятий, предусмотренных настоящим Положением;

осуществление внутреннего контроля и аудита соответствия практики обработки

персональных данных в Организации тем требованиям и нормам, которые установлены Законом «О персональных данных», а также принятым в этой сфере иным нормативным правовым актам и требованиям к защите персональных данных, и локальным нормативным актам Организации;

организационное, методическое и научно-техническое руководство работами по созданию либо модернизации системы защиты ПДн.

Статья VI. ПОРЯДОК МОДЕРНИЗАЦИИ СИСТЕМЫ ЗАЩИТЫ ПДн

Для ИСПДн, находящихся в эксплуатации, модернизация или доработка системы защиты ПДн должна проводиться в следующих случаях:

изменился состав или структура самой ИСПДн или технические особенности ее построения (изменился состав или структура программного обеспечения, технических средств обработки ПДн, топологии ИСПДн);

изменился состав угроз безопасности ПДн в ИСПДн;

изменился уровень защищенности, который необходимо обеспечить при защите ПДн.

Для определения необходимости доработки или модернизации систем защиты ПДн не реже одного раза в три года должна проводиться проверка состава и структуры ИСПДн, состава угроз безопасности ПДн в ИСПДн и эффективности реализованных в рамках СЗПДн мер по обеспечению безопасности персональных данных. Проверка проводится лицом, ответственным за обеспечение безопасности ПДн. Результаты проверки оформляются актом и утверждаются заведующим.

Статья VII. КОНТРОЛЬ СОБЛЮДЕНИЯ УСЛОВИЙ ИСПОЛЬЗОВАНИЯ СИСТЕМ ЗАЩИТЫ ПДн

1. Уполномоченный сотрудник, ответственный за обеспечение информационной безопасности и защиту персональных данных, и Комиссия по персональным данным периодический (не реже одного раза в год) должны проводится контроль соблюдения условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией.

2. В случае выявления фактов несоблюдения условий хранения носителей ПДн, или использования средств защиты информации, которые могут привести к нарушению заданного уровня безопасности ПДн, либо нарушения заданного уровня безопасности ПДн, должно в обязательном порядке проводиться разбирательство.

2.1. В процессе проведения разбирательства необходимо провести разработку и принятие мер по предотвращению возможных негативных последствий подобных нарушений.

2.2. По окончании проведения разбирательства готовится заключение о лицах, виновных в выявленных нарушениях.

Статья VIII. НОРМАТИВНЫЕ И МЕТОДИЧЕСКИЕ ДОКУМЕНТЫ

При организации и проведении работ по обеспечению безопасности ПДн в Организации, работники должны руководствоваться следующими нормативными и методическими документами:

Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных»

Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»

Федеральный закон от 19 декабря 2005 года № 160-ФЗ «О ратификации Конвенции Совета Европы «О защите физических лиц при автоматической обработке персональных данных»

Указ Президента Российской Федерации от 17 марта 2008 года № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»

Указ Президента Российской Федерации от 6 марта 1997 года № 188 «Об утверждении Перечня сведений конфиденциального характера»

Постановление Правительства РФ от 15 сентября 2008 года № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»

Постановление Правительства Российской Федерации от 01 ноября 2012 года № 1119 «Об утверждении требования к защите персональных данных при их обработке в информационных системах персональных данных»

Приказ ФСТЭК России от 18.02.2013 года № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

Локальный нормативный акт Политика по защите персональных данных в муниципальном дошкольном образовательном учреждении детский сад комбинированного вида № 5 «Радуга».

Локальный нормативный акт Положение об обработке и защите персональных данных работников муниципального дошкольного образовательного учреждения детский сад комбинированного вида № 5 «Радуга».

Локальный нормативный акт Положение об обработке и защите персональных данных воспитанников и родителей (законных представителей) муниципального дошкольного образовательного учреждения детский сад комбинированного вида № 5 «Радуга».