Муниципальное бюджетное дошкольное образовательное учреждение
детский сад № 109 г. Пензы «Планета детства»

Утверждаю
Заведующий МБДОУ
детского сада № 109 г. Пензы

_____О.Н. Крайнова
Приказ №263 от «25» мая 2020 г.

Крайнова Ольга Николаевна

Подписан: Крайнова Ольга Николаевна
DN: C=RU, S=Пензенская область, T=Заведующий, O="МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ДОШКОЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ДЕТСКИЙ САД № 109 Г. ПЕНЗЫ ""ПЛАНЕТА ДЕТСТВА""", СНИЛС=06841894705, ИНН=583401310070, E=d.s.109@yandex.ru, G=Ольга Николаевна, SN=Крайнова, CN=Крайнова Ольга Николаевна
Основание: я подтверждаю этот документ своей удостоверяющей подписью
Местоположение: место подписания
Дата: 2023.01.23 14:55:29+03'00'

ПОЛОЖЕНИЕ
о защите персональных данных в Муниципальном бюджетном дошкольном образовательном учреждении детском саду № 109 г. Пензы «Планета детства» и его филиалах

2020 г.

Обозначения и сокращения

ИСПДн – информационная система персональных данных.

НСД - несанкционированный доступ.

ПДн – персональные данные.

Политика – политика образовательных учреждений в отношении обработки персональных данных.

СЗПДн – система защиты персональных данных.

ТЗКИ – техническая защита конфиденциальной информации.

ТС – техническое средство.

Термины и определения

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

Безопасность информации – состояние защищенности информации, характеризуемое способностью технических средств и информационных технологий обеспечивать конфиденциальность, целостность и доступность информации при ее обработке техническими средствами.

Доступ к информации – возможность получения информации и ее использования.

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Источник угрозы безопасности информации – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

Накопитель информации – устройство, предназначенное для записи и (или) чтения информации на носитель информации. Накопитель информации конструктивно может содержать в себе неотчуждаемый носитель информации, либо может быть предназначен для использования сменных носителей информации. Накопители подразделяются на встроенные (в конструктиве системного блока) и внешние (подсоединяемые через порт). Встроенные накопители подразделяются на съемные и несъемные.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по своим функциональному предназначению и техническим характеристикам.

Носитель информации – физический объект, предназначенный для хранения информации.

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.

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

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

Пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

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

Система защиты персональных данных – комплекс организационных мер и программно-технических (в том числе криптографических) средств обеспечения безопасности информации в ИСПДн.

Технические средства информационной системы персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации.

Угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

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

Утечка (защищаемой) информации по техническим каналам – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

Основные положения

1.1. Настоящее Положение о защите персональных данных в Муниципальном бюджетном дошкольном образовательном учреждении детском саду № 109 г. Пензы «Планета детства» и его филиалах (далее Положение) разработано в соответствии с требованиями:

– федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

– федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

– Трудового кодекса Российской Федерации;

– положения «Об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» (постановление Правительства РФ от 15 сентября 2008г. № 687);

– постановления Правительства РФ от 01 ноября 2012 г. N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

1.2. В состав ПДн субъектов ПДн Муниципального бюджетного дошкольного образовательного учреждения детского сада № 109 г. Пензы «Планета детства» и его филиалов (далее МБДОУ) входят:

– паспортные данные;
– анкета;
– автобиография;
– сведения об образовании и специальности;
– сведения о трудовом и общем стаже;
– сведения о предыдущем месте работы;
– сведения о составе семьи;
– сведения о воинском учете;
– сведения о заработной плате;
– сведения о социальных льготах;
– наличие судимостей;
– адрес места жительства;
– номер домашнего телефона;
– адрес электронной почты (личной, служебной);
– содержание трудового договора;
– принадлежность к образовательному учреждению;
– принадлежность к учебной группе;
– данные ДУЛ;

– история обучения (для воспитанников);
– послужной список (для педагогов);
– информация о поощрениях
– подлинники и копии приказов по личному составу;
– основания к приказам по личному составу;
– сведения о повышении квалификации и переподготовке, об аттестации;
– сведения, направляемые в органы статистики;
– сведения о заболеваниях, нетрудоспособности;
– результаты медицинского обследования на предмет годности к осуществлению трудовых обязанностей, обучению;
– информация об ограничениях и потребностях по здоровью;
– информация о физическом развитии;
– информация о поощрениях;
– информация об успеваемости;
– информация о ведении (для педагогов) дополнительных курсов/кружков;
– информация о посещении (для воспитанников) дополнительных курсов/кружков;
– информация о месте в очереди в дошкольное образовательное учреждение;
– информация о родителях/законных представителях (ФИО, данные ДУЛ, телефон);
– рекомендации, характеристики и иные сведения, относящиеся к персональным данным субъектов ПДн;
– иные документы, содержащие сведения о субъекте ПДн нахождение которых в ИСПДн оператора необходимо для корректного документального оформления правоотношений с субъектом ПДн.
– ПДн субъектов ПДн, внесенные в ИСПДн оператора, относятся к сведениям конфиденциального характера, за исключением сведений, которые в установленных федеральными законами случаях могут быть опубликованы в средствах массовой информации.

1.3. Обеспечение конфиденциальности ПДн не требуется:
– в случае обезличивания ПДн;
– в отношении общедоступных ПДн.

1.4. Доступ к ПД субъектов ПДн разрешается только специально уполномоченным лицам, при этом указанные лица могут получать только те ПДн субъектов ПДн, которые необходимы для выполнения конкретных функций.

1.5. Руководитель МБДОУ определяет перечень лиц, уполномоченных на получение, обработку, хранение, передачу и любое другое использование ПДн субъектов ПДн МБДОУ и несущих ответственность за нарушение режима защиты этих ПДн в соответствии с законодательством Российской Федерации.

1.6. Все лица, в функциональные (должностные) обязанности которых входит получение, обработка и защита ПДн субъектов ПДн в ИСПДн оператора ПДн, при приёме на работу обязаны подписать обязательство о неразглашении ПДн.

2. Принципы обеспечения защиты информации, составляющей персональные данные

Защита информации, составляющей ПДн должна осуществляться в соответствии со следующими основными принципами:

2.1. Законность — предполагает обеспечение защиты ПДн в соответствии с действующим в РФ законодательством и нормативными актами в области защиты ПДн. Пользователи и обслуживающий персонал ИСПДн должны быть осведомлены о правилах и порядке работы с защищаемой информацией и об ответственности за их нарушение.

2.2. Системность — предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения проблемы обеспечения безопасности ПДн ИСПДн.

2.3. Комплексность — предполагает согласованное применение разнородных средств и систем при построении комплексной системы защиты информации, перекрывающей все существенные каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов. Для каждого канала утечки информации и для каждой угрозы безопасности должно существовать несколько защитных рубежей. Создание защитных рубежей осуществляется с учетом того, чтобы для их преодоления потенциальному злоумышленнику требовались профессиональные навыки в нескольких невзаимосвязанных областях.

2.4. Непрерывность — предполагает функционирование СЗПДн в виде непрерывного целенаправленного процесса, предполагающего принятие соответствующих мер на всех этапах жизненного цикла ИСПДн. ИСПДн должны находиться в защищенном состоянии на протяжении всего времени их функционирования. В соответствии с этим принципом должны приниматься меры не допускающие переход ИСПДн в незащищенное состояние.

2.5. Своевременность — предполагает упреждающий характер мер обеспечения безопасности ПДн, то есть постановку задач по комплексной защите ИСПДн и реализацию мер обеспечения безопасности ПДн на ранних стадиях разработки ИСПДн в целом и ее системы защиты информации, в частности.

2.6. Совершенствование — предполагает постоянное совершенствование мер и средств защиты информации на основе комплексного применения организационных и технических решений, квалификации персонала, анализа функционирования ИСПДн и ее системы защиты с учетом изменений условий функционирования ИСПДн, появления новых методов и средств перехвата информации, изменений требований нормативных документов по защите ПДн.

2.7. Персональная ответственность — предполагает возложение ответственности за обеспечение безопасности ПДн и ИСПДн на каждого исполнителя в пределах его полномочий. В соответствии с этим принципом распределение прав и обязанностей исполнителей строится таким образом, чтобы в случае любого нарушения круг виновников был четко известен или сведен к минимуму.

2.8. Минимальная достаточность — предполагает предоставление исполнителям минимально необходимых прав доступа к ресурсам ИСПДн в соответствии с производственной необходимостью, на основе принципа «запрещено все, что не разрешено явным образом».

2.9. Гибкость системы защиты — предполагает наличие возможности варьирования уровнем защищенности при изменении условий функционирования ИСПДн.

2.10.Обязательность контроля — предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных правил обеспечения безопасности ПДн на основе используемых систем и средств защиты информации. Контроль за деятельностью каждого пользователя, каждого средства защиты и в отношении каждого объекта защиты должен осуществляться на основе применения средств контроля и регистрации и должен охватывать как несанкционированные, так и санкционированные действия пользователей.

3. Основные требования по защите информации составляющей персональные данные

3.1. Защита информации в ИСПДн является неотъемлемой составной частью деятельности МБДОУ и должна осуществляться во взаимосвязи с другими мерами по защите информации, составляющей ПДн.

3.2. Защита информации является составной частью работ по созданию и эксплуатации ИСПДн и должна осуществляться в установленном настоящим Положением порядке и реализовываться в виде системы (подсистемы) защиты ПДн.

3.3. Защита информации должна осуществляться посредством выполнения комплекса мероприятий по предотвращению утечки информации по техническим каналам, за счет НСД к ней, по предупреждению преднамеренных программно - технических воздействий с целью нарушения целостности (уничтожения, искажения) информации в процессе ее обработки, передачи и хранения, нарушения ее санкционированной доступности и работоспособности ТС.

3.4. Защита информации должна быть дифференцированной в зависимости от применяемых технических средств, обрабатывающих информацию, составляющую ПДн, установленного уровня защищенности ИСПДн, установленного класса ИСПДн и утвержденной для ИСПДн модели угроз.

3.5. Все используемые в ИСПДн средства защиты информации должны быть проверены на соответствие ограничениям и условиям эксплуатации, изложенным в сертификате соответствия, эксплуатационной документации или формуляре (для технических и программных средств защиты информации соответственно).

3.6. Обработка информации составляющей ПДн осуществляется на основании письменного разрешения (приказа) руководителя МБДОУ, в котором эксплуатируется ИСПДн.

3.7. Ответственность за обеспечение выполнения установленных требований по защите информации возлагается на руководителя МБДОУ, в котором создается (совершенствуется) и эксплуатируется ИСПДн.

3.8. Все ИСПДн должны пройти оценку эффективности принимаемых мер по обеспечению безопасности ПДн до начала обработки информации составляющей ПДн.

3.9.Оператор при обработке ПДн обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн.

3.10. Обеспечения безопасности ПДн субъектов ПДн достигается применением следующих организационных и технических мер:

3.10.1. Пропускной режим МБДОУ.

3.10.2. Рациональное размещение рабочих мест сотрудников МБДОУ, при котором исключался бы доступ к защищаемой информации (ПДн) посторонних лиц.

3.10.3. Ограничение и регламентация состава сотрудников МБДОУ, в функциональные обязанности которых предполагают наличие доступа к ПДн в принципе и к конкретным ПДн в частности.

3.10.4. Избирательное и обоснованное распределение документов, носителей и информации между сотрудниками МБДОУ.

3.10.5. Установление правил доступа к ПДн, обрабатываемым в ИСПДн, а также обеспечением регистрации и учета всех действий, совершаемых с ПДн в ИСПДн.

3.10.6. Знание лицами, уполномоченными на обработку и использование ПДн, требований нормативно-методических документов по их защите.

3.10.7. Обеспечение необходимых условий в помещении для работы с носителями ПДн и ИСПДн.

3.10.8. Организация порядка хранения и уничтожения носителей ПДн.

3.10.9. Учет МНИ ПДн.

3.10.10. Обеспечение раздельного хранения ПДн (материальных носителей, информации в электронном виде), обработка которых осуществляется в различных целях.

3.10.11. Определение угроз безопасности ПДн при их обработке в ИСПДн.

3.10.12. Применение организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн, необходимых для выполнения требований к защите ПДн, исполнение которых обеспечивает установленные Правительством РФ уровни защищенности ПДн.

3.10.13. Применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации.

3.10.14. Использование защищённых по требованиям безопасности информации ИСПДн.

3.10.15. Оценка эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию ИСПДн.

3.10.16. Обнаружение фактов НСД к ПДн и принятие соответствующих мер.

3.10.17. Контроль за принимаемыми мерами по обеспечению безопасности ПДн и уровнем защищенности ИСПДн.

4. Порядок организации и проведения работ по защите информации

4.10.Организация работ по защите информации возлагается на руководителя МБДОУ, осуществляющего разработку (модернизацию) и (или) эксплуатацию ИСПДн.

4.11.Организация и проведение работ по защите информации, составляющей ПДн на различных стадиях разработки, внедрения и эксплуатации ИСПДн определяется действующими в РФ нормативными документами и настоящим документом.

4.12.Проведение работ по защите информации, составляющей ПДн, осуществляется МБДОУ, в котором создается (совершенствуется) ИСПДн. В случае невозможности или нецелесообразности выполнения работ по защите информации силами образовательного учреждения к этим работам должна привлекаться специализированная организация, имеющая соответствующие лицензии на право выполнения работ и оказания услуг по ТЗКИ.

4.13.Стадии создания системы защиты информации:

– Предпроектная стадия — включает предпроектное обследование создаваемой ИСПДн, разработку аналитического обоснования необходимости создания системы защиты информации и технического задания на ее создание.

– Стадия проектирования (разработки проектов) и реализации ИСПДн — включает разработку СЗПДн в составе ИСПДн.

– Стадия ввода в действие системы СЗПДн — включает опытную эксплуатацию и приемо-сдаточные испытания средств защиты информации, а также оценку эффективности принимаемых мер по обеспечению безопасности ПДн.

5. Порядок обеспечения защиты информации при эксплуатации ИСПДн

5.10. Ответственность за обеспечение защиты информации в процессе эксплуатации ИСПДн возлагается на руководителя МБДОУ, в ведении которого находится эта ИСПДн.

5.11. Ответственность за соблюдение установленных требований по защите информации при ее обработке в ИСПДн возлагается на непосредственных исполнителей ИСПДн (пользователей, администраторов, обслуживающий персонал).

5.12.За нарушение установленных требований по защите информации руководитель МБДОУ, в ведении которого находится ИСПДн и (или) непосредственный исполнитель привлекаются к ответственности в соответствии с действующим в РФ законодательством.

6. Порядок организации делопроизводства, хранения и обращения накопителей и носителей информации

6.10.Все накопители и носители информации, содержащие ПДн на бумажной, магнитной, магнито - оптической и иной основе, используемые в технологическом процессе обработки информации в ИСПДн, подлежат учету, хранению и обращению в соответствии с требованиями конфиденциального делопроизводства.

6.11.Организация и ведение учета накопителей и носителей ПДн, организация их хранения, обращения и уничтожения осуществляются ответственными лицами.

6.12.ПДн, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях ПДн, в специальных разделах или на полях форм (бланков).

6.13.При фиксации ПДн на материальных носителях не допускается фиксация на одном материальном носителе ПДн, цели обработки которых заведомо не совместимы.

6.14.Для обработки различных категорий ПДн, осуществляемой без использования средств автоматизации, для каждой категории ПДн должен использоваться отдельный материальный носитель.

6.15.Обработка ПДн без использования средств автоматизации должна осуществляться таким образом, чтобы в отношении каждой категории ПДн можно было определить места хранения ПДн (материальных носителей) и установить перечень лиц, осуществляющих обработку ПДн либо имеющих к ним доступ.

6.16.Должно обеспечиваться раздельное хранение ПДн (материальных носителей), обработка которых осуществляется в различных целях.

6.17.При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность ПДн и исключающие несанкционированный к ним доступ.

7. Контроль состояния и эффективности защиты ИСПДн

7.10.В ИСПДн должен осуществляться контроль и (или) аудит соответствия обработки ПДн действующим в РФ законодательству и требованиям к защите ПДн.

7.11.Контроль заключается в оценке выполнения требований нормативных документов, обоснованности принятых мер и оценке эффективности принятых мер по обеспечению ПДн.

7.12.Контроль подразделяется на оперативный и плановый (периодический).

7.13.В процессе эксплуатации ИСПДн в целях защиты информации от НСД осуществляются оперативный контроль и периодический контроль за выполнением исполнителями требований действующих нормативных документов по вопросам обеспечения безопасности и защиты ПДн.

7.14.С целью своевременного выявления и предотвращения утечки информации, исключения или существенного затруднения НСД и предотвращения специальных воздействий (программно-технических и др.), вызывающих нарушение целостности информации или работоспособность технических средств, в ИСПДн образовательных учреждений проводится плановый периодический (не реже одного раза в год) контроль состояния защиты информации.

7.15.При проведении плановых проверок осуществляется контроль ведения учетной документации, защищенности ИСПДн от утечки ПДн по техническим каналам, выборочный контроль содержимого накопителей и носителей информации, и т.п.

7.16. Результаты контроля оформляются актами, заключениями и записями в эксплуатационной документации.

8. Ответственность за нарушение режима защиты персональных данных

8.10. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту ПДн, несут предусмотренную законодательством РФ ответственность.

8.11. Моральный вред, причиненный субъекту ПДн вследствие нарушения его прав, нарушения правил обработки ПДн, а также требований к защите ПДн, установленных законодательством РФ, подлежит возмещению в соответствии с законодательством РФ.

8.12. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом ПДн убытков.