МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ДОШКОЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ДЕТСКИЙ САД КОМБИНИРОВАННОГО ВИДА № 4 СТАНИЦЫ ЛЕНИНГРАДСКОЙ МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ ЛЕНИНГРАДСКИЙ РАЙОН

Утверждено
приказом заведующего МБДОУ № 4
от 01.09.2021 г. № 85-осн.
_____Т.Ю. Горбенко

ПОЛОЖЕНИЕ

об организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных МБДОУ № 4

1. ОБЩИЕ ПОЛОЖЕНИЯ

1) Настоящее Положение по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных Муниципального бюджетного дошкольного образовательного учреждения детский сад комбинированного вида № 4 станицы Ленинградской муниципального образования Ленинградский район (МБДОУ № 4) (далее – Положение) разработано в соответствии с Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 15 сентября 2008 г.
№ 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», постановлением Правительства Российской Федерации от 1 ноября 2012 г.
№ 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

2) Цель разработки настоящего Положения – установление порядка организации и проведения работ по обеспечению безопасности персональных данных (далее – ПД) в информационных системах персональных данных (далее – ИСПД) МБДОУ № 4. (далее – Учреждение, Оператор) на протяжении всего жизненного цикла ИСПД.

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

1) В настоящем Положении используются следующие термины и их определения:

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

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 или наличия иного законного основания, если иное не предусмотрено федеральным законом.

Межсетевой экран – локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

Обработка персональных данных – действия (операции) 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.

Технические средства информационной системы персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (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).

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.

Ресурс информационной системы – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

Средства вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

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.

Уровень защищенности персональных данных – комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

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

Целостность информации – способность средства вычислительной техники или информационной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

3. ПОРЯДОК ОРГАНИЗАЦИИ И ПРОВЕДЕНИЯ РАБОТ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

1) Под организацией обеспечения безопасности ПД при их обработке в ИСПД понимается формирование и реализация совокупности согласованных по цели, задачам, месту и времени организационных и технических мероприятий, направленных на минимизацию ущерба от возможной реализации угроз безопасности ПД, реализуемых в рамках создаваемой системы защиты персональных данных (далее – СЗПД).

2)СЗПД включает в себя организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности ПД, уровня защищенности ПДн, который необходимо обеспечить, и информационных технологий, используемых в информационных системах.

3) Безопасность ПД при их обработке в ИСПД обеспечивает оператор или лицо, осуществляющее обработку ПД по поручению оператора на основании заключаемого с этим лицом договора (далее – уполномоченное лицо). Договор между оператором и уполномоченным лицом должен предусматривать обязанность уполномоченного лица обеспечить безопасность ПД при их обработке в информационной системе.

4)Выбор средств защиты информации для СЗПД осуществляется оператором в соответствии с нормативными правовыми актами, принятыми Федеральной службой безопасности Российской Федерации (далее – ФСБ России) и Федеральной службой по техническому и экспортному контролю (далее – ФСТЭК России) во исполнение Федерального закона «О персональных данных».

5)Структура, состав и основные функции СЗПД определяются исходя из уровня защищенности ПД при их обработке в ИСПД.

4. ПРОВЕДЕНИЕ РАБОТ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

1)Работы по обеспечению безопасности ПД проводятся в соответствии с Планом мероприятий по защите персональных данных (Приложение № 1). Внутренние проверки режима обработки и защиты ПД Учреждением проводятся в соответствии с Планом внутренних проверок режима обработки и защиты персональных данных .

2) Контроль за проведением работ по обеспечению безопасности ПД осуществляет ответственный за организацию обработки ПД в виде методического руководства, участия в разработке требований по защите ПД, организации работ по выявлению возможных каналов утечки информации, согласования выбора средств вычислительной техники и связи, технических и программных средств защиты, участия в оценке соответствия ИСПД Учреждения требованиям безопасности ПД.

4. РЕШЕНИЕ ВОПРОСОВ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ДИНАМИКЕ ИЗМЕНЕНИЯ ОБСТАНОВКИ И КОНТРОЛЯ ЭФФЕКТИВНОСТИ ЗАЩИТЫ

1) Модернизация СЗПД для функционирующих ИСПД Учреждения должна осуществляться в случае:

– изменения состава или структуры ИСПД или технических особенностей ее построения (изменения состава или структуры программного обеспечения, технических средств обработки ПД, топологии ИСПД);

- изменения состава угроз безопасности П в ИСПД;
- изменения уровня защищенности ПД при их обработке в ИСПД;
- прочих случаях, по решению оператора.

2) В целях определения необходимости доработки (модернизации) СЗПД не реже одного раза в год ответственным за организацию обработки ПД должна проводиться проверка состава и структуры ИСПД, состава угроз безопасности ПД в ИСПД и уровня защищенности ПД при их обработке в ИСПД, соблюдения условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией. Результаты проверки оформляются актом проверки и утверждаются руководителем Учреждения.

3)Анализ инцидентов безопасности ПД и составление заключений в обязательном порядке должно проводиться в случае выявления следующих фактов:

- несоблюдение условий хранения носителей ПД;
- использование средств защиты информации, которые могут привести к нарушению заданного уровня безопасности, конфиденциальность/ целостность/доступность ПД или другим нарушениям, приводящим к снижению уровня защищенности ПД;
- нарушение заданного уровня безопасности ПД (конфиденциальность/ целостность/доступность).

4) В процессе проведения разбирательства необходимо провести разработку и принятие мер по предотвращению возможных негативных последствий подобных нарушений. По окончании проведения разбирательства необходимо провести разработку (доработку) и принятие мер по предотвращению повторения подобных нарушений.

Приложение № _____
к Положению по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных

План внутренних проверок режима обработки и защиты персональных данных МБДОУ № 4

№	Мероприятие	Периодичность	Дата, подпись исполнителя
	Организационные меры по вопросам обработки ПД		
1.	Осуществление внутреннего контроля и (или) аудита соответствия обработки ПД ФЗ-152 «О персональных данных» и принятым в соответствии с ним нормативным правовым актам	Раз в полгода	
2.	Проверка ознакомления сотрудников, непосредственно осуществляющих обработку ПД, с положениями законодательства Российской Федерации о ПД, в том числе требованиями к защите ПД	Раз в полгода	
3.	Проверка получения согласий субъектов ПД на обработку ПД в случаях, когда этого требует законодательство	Раз в полгода	
4.	Проверка подписания сотрудниками, осуществляющими обработку ПД, основных форм, необходимых в целях выполнения требований законодательства в сфере обработки и защиты ПД: – Уведомления о факте обработки ПД без использования средств автоматизации; – Обязательства о соблюдении конфиденциальности ПД; – Формы ознакомления с положениями законодательства Российской Федерации о ПД, локальными актами по вопросам обработки ПД; – Разъяснения субъекту ПД юридических последствий отказа предоставить свои ПД	Раз в полгода	
5.	Проверка уничтожения материальных носителей ПД с составлением соответствующего акта	Ежегодно	
6.	Проверка ведения журналов по учету обращений субъектов ПД и учету передачи ПД субъектов третьим лицам	Раз в полгода	
7.	Проведение внутренних проверок на предмет выявления изменений в правилах обработки и защиты ПД	Ежегодно	
8.	Проверка соблюдения условий хранения материальных носителей ПД	Раз в полгода	
9.	Проверка состояния актуальности Уведомления об обработке (намерении осуществлять обработку) ПД	Раз в полгода	
10.	Поддержание в актуальном состоянии организационно-распорядительных документов по вопросам обработки ПД,в том числе документов, определяющих политику Муниципального автономного общеобразовательного учреждения в отношении обработки ПД	Раз в полгода	

Технические меры по вопросам защиты ПД			
11.	Организация анализа и пересмотра имеющихся угроз безопасности ПД, а также предсказание появления новых, еще неизвестных, угроз	Ежегодно	
12.	Оценка вреда, который может быть причинен субъектам ПД в случае нарушения ФЗ-152 «О персональных данных»	Ежегодно	
13.	Проверка применения для обеспечения безопасности ПД средств защиты информации, прошедших в установленном порядке процедуру соответствия	Раз в полгода	
14.	Оценка эффективности принимаемых мер по обеспечению безопасности ПД до ввода в эксплуатацию ИСПД	При необходимости	
15.	Контроль учета машинных носителей ПД	Раз в полгода	
16.	Контроль за принимаемыми мерами по обеспечению безопасности ПД и уровня защищенности ИСПД	Раз в полгода	
17.	Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в ИСПД	Ежеквартально	
18.	Контроль внесения изменений в структурно-функциональные характеристики ИСПД	Ежеквартально	
19.	Контроль корректности настроек средств защиты информации	Раз в полгода	
20.	Контроль за обеспечением резервного копирования	Ежеквартально	
21.	Поддержание в актуальном состоянии организационно-распорядительных документов по вопросам защиты ПД	Раз в полгода	