ПРИНЯТО
Советом Учреждения
Протокол № 1 от 03. 10. 16

УТВЕРЖДАЮ
Директор МБОУ ДО «Свежий ветер»
_____ С.В. Мурышова
«03» 10 2016 года

Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами и локальными актами МБОУ ДО «Свежий ветер»

I. Общие положения

Настоящие правила разработаны в соответствии с требованиями Федерального закона от 27.07.2006г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 27.07.2006г. № 152-ФЗ «О персональных данных», Постановления Правительства Российской Федерации от 21.03.2012 № 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 и муниципальными органами», Постановления Правительства Российской Федерации от 01.11.2012г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

Правила определяют процедуры, направленные на выявление и предотвращение нарушений законодательства в сфере защиты персональных данных, разбирательства и составления актов разбирательства инцидента информационной безопасности (далее - ИБ) по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности

персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений, а так же выявления и предотвращения нарушений ИБ в МБОУ ДО «Свежий ветер» (далее Учреждение).

Основные термины и понятия, используемые в Правилах.

Инцидент ИБ - событие, в результате наступления которого в Учреждении произошло разглашение конфиденциальной информации, персональных данных, нарушение работоспособности информационных систем, внесение несанкционированных изменений в информационные ресурсы Учреждения.

Нарушитель ИБ - лицо, предпринявшее попытку выполнения запрещенных операций (действий) по ошибке, незнанию или осознанно и использовавшее для этого различные возможности, методы и средства.

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.

Информационные ресурсы (далее - ИР) - совокупность данных, организованных для эффективного получения достоверной информации, документы и отдельные массивы документов в информационных системах.

Автоматизированное рабочее место (далее - АРМ) - индивидуальный комплекс технических и программных средств, предназначенный для автоматизации работы работников Учреждения.

Система защиты от несанкционированного доступа (далее СЗНД) - система защиты информации, предотвращающая или существенно затрудняющая несанкционированный доступ к информации.

II. Порядок проведения проверок условий обработки персональных данных

2.1. В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям в Учреждении организуется проведение периодических проверок условий обработки персональных данных.

2.2. Проверки осуществляются ответственным за организацию обработки персональных данных в Учреждении.

2.3. Плановые проверки соответствия обработки персональных данных установленным требованиям в Учреждении проводятся на основании утвержденного приказом директора ежегодного плана проверок.

Внеплановые проверки организуются в течение трех рабочих дней при наступлении следующих событий:

- поступившее в Учреждении письменное заявление субъекта персональных данных о нарушениях правил обработки персональных данных;

- поступившее Ответственному за организацию обработки персональных данных сообщение от работников Учреждения о предполагаемом нарушении правил обработки персональных данных;

- получение предписания органов надзора за соблюдением прав субъектов персональных данных.

2.4. При проведении любой проверки соответствия обработки персональных данных установленным требованиям устанавливается соответствие принимаемых мер по обеспечению безопасности персональных данных при их обработке, мерам, указанным в положении об обработке персональных данных, утвержденном приказом директора.

2.5. Ответственный за организацию обработки персональных данных в Учреждении имеет право:

- запрашивать у работников Учреждения информацию, необходимую для реализации полномочий;

- принимать меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований законодательства Российской Федерации;

- вносить директору Учреждения предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности персональных данных при их обработке.

Проверка должна быть завершена в срок не позднее чем через тридцать календарных дней со дня принятия решения о её проведении.

Директор Учреждения контролирует своевременность и правильность проведения проверки.

Ответственный за организацию обработки персональных данных предоставляет отчет директору о результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений по форме согласно приложению №1 к настоящим Правилам.

III. Порядок разбирательства инцидента ИБ

3.1. Разбирательство по вопросам инцидентов ИБ проводится ответственным за организацию обработки персональных данных в Учреждении.

3.2. Цели разбирательства инцидентов ИБ:

- выработка организационных и технических решений, направленных на снижение рисков нарушения ИБ, предотвращение подобных нарушений в будущем;

- обеспечение безопасности обработки персональных данных;

- обеспечение прав субъектов персональных данных на обеспечение безопасности и конфиденциальности их персональных данных, обрабатываемых в Учреждении;

- предотвращение несанкционированного доступа к информационным системам.

3.3. Этапы разбирательства инцидента ИБ:

- подтверждение или опровержение факта возникновения инцидента ИБ;

- подтверждение или корректировка уровня значимости инцидента ИБ;

- уточнение дополнительных обстоятельств инцидента ИБ;

- получение доказательств возникновения инцидента ИБ, обеспечение их сохранности и целостности;

- минимизация последствий инцидента ИБ;

- информирование и консультирование работников Учреждения по действиям обнаружения, устранения последствий и предотвращения инцидентов ИБ;

- разработка мероприятий по обнаружению и (или) предупреждению инцидентов ИБ.

3.4. Выявление инцидента ИБ.

Основными источниками информации об инцидентах ИБ являются:

- результаты плановых или внеплановых проверок соответствия обработки персональных данных установленным требованиям;

- факты, выявленные работниками Учреждения.

Работник Учреждения может выявить признаки наличия Инцидента ИБ путем анализа текущей ситуации на предмет ее соответствия требованиям Положения об информационной безопасности в МБОУ ДО «Свежий ветер», утвержденного приказом директора (Далее - Положение об ИБ). Выявленные несоответствия дают основания предполагать факт возникновения инцидента ИБ. Любые сведения о предполагаемом инциденте ИБ незамедлительно передаются выявившим их работником ответственному за организацию обработки персональных данных в Учреждении в произвольной форме любым доступным способом:

- по контактам, указанным на официальном сайте Учреждения;

- лично.

3.5. Ответственный за организацию обработки персональных данных в Учреждении после получения информации о предполагаемом инциденте ИБ незамедлительно фиксирует дату, время и место возникновения предполагаемого инцидента ИБ, определяет и инициирует первоочередные меры (отключение АРМ предполагаемого нарушителя ИБ от информационной системы, восстановление информации из резервной копии, исправление ошибки ввода, проведение дополнительного инструктажа по ИБ), направленные на локализацию инцидента ИБ и минимизацию его последствий.

3.7. В случае нарушения прав субъекта персональных данных разбирательство и реагирование происходит в порядке и в сроки, предусмотренные Правилами рассмотрения запросов субъектов персональных данных в Учреждении, утвержденными приказом директора «Об утверждении Правил рассмотрения запросов субъектов персональных данных или их представителей в МБОУ ДО «Свежий ветер».

3.8. Проведение разбирательства инцидента ИБ.

3.8.1. В процессе проведения разбирательства инцидента ИБ устанавливаются:

- дата и время совершения инцидента ИБ;
- информационные ресурсы, затронутые инцидентом ИБ;
- ФИО, должность предполагаемого нарушителя ИБ;
- уровень критичности инцидента ИБ;
- обстоятельства и мотивы совершения инцидента ИБ;
- характер и размер реального и потенциального ущерба;
- обстоятельства, способствовавшие совершению инцидента ИБ.

3.8.2. Ответственный за организацию обработки персональных данных в Учреждении в процессе проведения расследования инцидента ИБ при необходимости запрашивает информацию у работников Учреждения.

3.8.3. После получения необходимой информации по инциденту ИБ ответственный за организацию обработки персональных данных, осуществляющий разбирательство проводит анализ полученных данных.

3.8.4. С целью минимизации последствий инцидента ИБ возможно временное отключение прав доступа у предполагаемого нарушителя ИБ к информационным ресурсам (далее - ИР) на время проведения расследования. Информация об отключении прав доступа ответственным за организацию обработки персональных данных направляется директору Учреждения.

3.8.5. Восстановление временно отключенных у нарушителя ИБ прав доступа к ИР производится ответственным за организацию обработки персональных данных.

3.9. Собранная в процессе разбирательства инцидента ИБ информация фиксируется в карточке инцидента ИБ (приложение №2 к настоящим Правилам) и учитывается

при подготовке акта разбирательства инцидента ИБ (приложение №3 к настоящим Правилам).

3.10. Ответственный за организацию обработки персональных данных направляет акт разбирательства инцидента ИБ директору Учреждения.

3.11. На основании полученного акта разбирательства инцидента ИБ директор Учреждения, в срок не более трех рабочих дней организует проведение мероприятий, направленных на снижение рисков информационной безопасности в будущем:

- повторное ознакомление нарушителя ИБ с Правилами, с должностной инструкцией, с Положением об ИБ, с Руководством пользователя;

- анализ и пересмотр имеющихся прав доступа к информационным ресурсам у нарушителя ИБ;

- доведение до всех работников Учреждения требований правовых актов в области ИБ.

Приложение №1
к Правилам осуществления внутреннего контроля соответствия
обработки персональных данных требованиям к защите
персональных данных, установленным Федеральным Законом
«О персональных данных», принятыми в соответствии с ним
нормативными правовыми актами и локальными актами МБОУ ДО «Свежий ветер»

Отчет
о результатах проведенной _____ проверки соответствия обработки
дата проведения
персональных данных требованиям к защите персональных данных

Возможные нарушения требований к защите персональных данных	Наличие нарушения
Работа в информационной системе персональных данных на автоматизированном рабочем месте, не защищенном корпоративной системой антивируса	
Обработка персональных данных сотрудниками, не включенными в перечень допущенных к обработке персональных данных	
Отсутствие или неактуальность перечня сотрудников, допущенных к обработке персональных данных	
Обработка персональных данных после достижения цели обработки персональных данных	
Отсутствие журнала учета электронных носителей персональных данных при использовании самих носителей	
Отсутствие подписанных обязательств о неразглашении персональных данных.	
Хранение файлов, содержащих персональные данные на автоматизированном рабочем месте	
Доступность логина, пароля автоматизированного рабочего места, информационной системы персональных данных для посторонних	
Возможность считывания информации с экрана монитора для посторонних	

Рекомендации по устранению выявленных нарушений _____
_____
_____

Подпись Ответственного за организацию обработки персональных данных ___

Приложение №2
к Правилам осуществления внутреннего контроля соответствия
обработки персональных данных требованиям к защите
персональных данных, установленным Федеральным Законом
«О персональных данных», принятыми в соответствии с ним
нормативными правовыми актами и локальными актами МБОУ ДО «Свежий ветер»

Карточка инцидента информационной безопасности (ИБ)

Дата инцидента ИБ _____ Номер инцидента ИБ _____

Информация о сообщившем:	Ф.И.О.	Должность	Телефон	
Тип инцидента:	Действительный	Попытка	Подозрение	
Предполагаемый вид угрозы информационной безопасности:	Непреднамеренная	Ошибка проектирования информационной системы	Технический сбой	
Нарушитель:	Отсутствует	Не установлен	Внешний	Внутренний
			Организация, Ф.И.О., должность нарушителя	Ф.И.О., должность нарушителя
Последствия инцидента:	Без последствий	Нарушение работоспособности компонентов ИС	Нарушение целостности ИР, фальсификация документов	Нарушение режима конфиденциальности информации
Объект, которому нанесен ущерб:	Информация	Средства вычислительной техники	Программное обеспечение	Средства связи
Действия, предпринятые для разрешения инцидента:	Описание действий	Никаких действий не требуется	Без привлечения внешнего исполнителя	С привлечением внешнего исполнителя

Подпись Ответственного за организацию обработки персональных данных ___

Приложение №3
к Правилам осуществления внутреннего контроля соответствия
обработки персональных данных требованиям к защите
персональных данных, установленным Федеральным Законом
«О персональных данных», принятыми в соответствии с ним
нормативными правовыми актами и локальными актами МБОУ ДО «Свежий ветер»

Акт № ____ от _____
Разбирательства инцидента информационной безопасности

Ответственным за организацию обработки персональных данных _____
(должность и Ф.И.О.)
проведено разбирательство инцидента ИБ, выявленного ____
(дата)
в МБОУ ДО «Свежий ветер».
В результате разбирательства установлено:
Работник (и) МБОУ ДО «Свежий ветер», причастные к инциденту ИБ _____ должность и Ф.И.О. работника (ов) МБОУ ДО «Свежий ветер», причастных к возникновению инцидента ИБ

Инцидент ИБ _____
(описание произошедшего инцидента ИБ)
_____
_____
_____Причины возникновения инцидента _____
(причины, по которым стал возможен инцидент ИБ)
_____

Ущерб (при наличии), причиненный инцидентом ИБ
_____
(перечень пострадавших ресурсов(объектов)
Действия, предпринятые для ликвидации последствий инцидента ИБ
_____
_____
_____
(описание действий, направленных на ликвидацию последствий инцидента ИБ)

Подпись Ответственного за организацию обработки персональных данных ___