Утверждаю:
Директор МБОУСОШ№5 им.В.В.Терешковой

_____ Е.Н.Головина
Приказ №327 от 01.09.2020г.

Правила
осуществления внутреннего контроля соответствия обработки персональных данных требованиям по защите персональных данных в информационной системе персональных данных «Сетевой город. Образование» ,«Е-Услуги»
МБОУ СОШ № 5 им. В.В. Терешковой

I. Общие положении

1.1. Настоящие правила разработаны в соответствии с требованиями Федеральною закона от 27.07.2006 № 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 и соответствии с ним нормативными правовыми актами, операторами, являющимися государственными и муниципальными органами), Постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

1.2. 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 зашиты 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 СОШ № 5 им. В.В. Терешковой (далее - Школа).

1.3. Основные термины и понятия, используемые в Правилах.

— **Инцидент ИБ** - событие, в результате наступления которого в Школе произошло разглашение конфиденциальной информации, персональных данных, нарушение работоспособности информационных систем, внесение несанкционированных изменений в информационные ресурсы Школы

— **Нарушитель ИБ** - лицо, предпринявшее попытку выполнения запрещенных операций (действий) по ошибке, незнанию или осознанно и использовавшее для >того 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 Школы;
— **Система зашиты от несанкционированного доступа** (далее СЗНД) - система защиты информации, предотвращающая или существенно затрудняющая несанкционированный доступ к информации.

2. Порядок проведения проверок условий обработки персональных данных.

2.1. В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям в Школе организуется проведение периодических проверок условий обработки персональных данных.
2.2. Проверки осуществляются комиссией или ответственным лицом за обеспечение безопасности персональных данных в Школе.
2.3. Проверки условий обработки персональных данных могут быть плановыми и внеплановыми, документарными и проводимыми в помещениях Школы, в которых ведется обработка персональных данных.
2.4. Плановые проверки соответствия обработки персональных данных установленным требованиям в Школе проводятся не менее одного раза в год.
2.5. Внеплановые проверки организуются в течение трех рабочих дней при наступлении следующих событий:
— поступившее в Школу письменное заявление субъекта персональных данных персональных данных о нарушениях правил обработки персональных данных;
— поступившее директору Школы сообщение от сотрудников Школы о предполагаемом нарушении правил обработки персональных данных;
— получение предписания органов надзора за соблюдением прав субъектов персональных данных.
2.6. При проведении проверок условий обработки персональных данных должен быть полностью, объективно и всесторонне исследован порядок обработки персональных данных и его соответствие требованиям обработки персональных данных, установленным в Школе, а именно:
— соответствие целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям Оператора персональных данных:

— соответствие объема и характера обрабатываемых персональных данных. способов обработки персональных данных, целям обработки персональных данных;
— достаточность персональных данных для целей обработки персональных данных, заявленных при сборе персональных данных;
— отсутствие (наличие) объединения созданных для несовместимых между собой целен баз данных информационных систем персональных данных;
— порядок и условия применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;
— порядок и условия применения средств зашиты информации;
— соблюдение правил доступа к персональным данным:
— наличие (отсутствие) фактов несанкционированного доступа к персональным данным и принятие необходимых мер;
— мероприятия по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним:
— осуществление мероприятий по обеспечению целостности персональных данных.
2.7. В случае выявления фактов:
— несоблюдения установленного порядка обработки персональных данных;
— несоблюдения условий хранения носителей персональных данных:
— использования средств защиты информации, которые могут привести к нарушению заданного уровня безопасности (конфиденциальность/ целостность/доступность)персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных;
— нарушения заданного уровня безопасности персональных данных (конфиденциальность/целостность/доступность);
в обязательном порядке устанавливаются причины нарушения обработки персональных данных и наличие (отсутствие) вины.
2.8. Комиссия или Лицо, ответственное за обеспечение безопасности персональных данных в Школе, уполномоченное на проведение проверок имеет право:
— запрашивать у сотрудников Школы информацию, необходимую для реализации полномочий;
— требовать от уполномоченных на обработку персональных данных лиц уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных;
— принимать меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований законодательства Российской Федерации:

— вносить директору Школы предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности персональных данных при их обработке;
— вносить директору Школы предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации в отношении обработки персональных данных.
2.9. В процессе проведения внутреннего контроля (проверок) соответствия обработки персональных данных требованиям к защите персональных данных разрабатываются меры, направленные на предотвращение негативных последствий выявленных нарушений.
2.10. В случаях выявления нарушений обработки персональных данных, требующих немедленного устранения, принимаются меры оперативного реагирования.
2.11. Устранение выявленных нарушений проводится не позднее 30 дней с момента завершения проверки.
2.12. В отношении персональных данных, ставших известными лицу, ответственному за обеспечение безопасности персональных данных в Школе в ходе проведения мероприятий внутреннего контроля, должна обеспечиваться конфиденциальность персональных данных.
2.13. В процессе проверки комиссия (ответственное лицо) заполняет контрольный лист (Приложение № I), при этом отметки проставляются по каждому информационному ресурсу в отдельности. Данный документ является обязательным приложениям к акту (Приложение № 2) по результатам контроля и аудита. Акт по результатам контроля и приложение к нему хранятся в кабинете у председателя комиссии или ответственного лица.

3. Порядок разбирательства инцидента ПК.

3.1. Разбирательство но вопросам инцидентов ИБ проводится ответственным лицам за обеспечение безопасности персональных данных в Школе или комиссией по защите персональных данных (далее по тексту - Комиссия), утвержденной приказом Школы (в соответствии с решением директора Школы).
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 Школой;
— 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 сотрудников Школы 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 сотрудниками Школы. Сотрудник Школы может выявить признаки наличия Инцидент ИБ путем анализа текущей ситуации на предмет ее соответствия требованиям федерального законодательства в области зашиты персональных данных и информационной безопасности. Выявленные несоответствия дают основания предполагать факт возникновения инцидента ИБ. Любые сведения о предполагаемом инциденте ИБ незамедлительно передаются выявившим их сотрудником директору Школы, ответственному лицу за обеспечение безопасности персональных данных в Школе, в произвольной форме, любым доступным способом (по телефону, докладной запиской, через непосредственного руководителя).
3.5. В срок не более одного рабочего дня с момента поступления информации об инциденте ИБ, Комиссия (ответственное лицо за защиту персональных данных), осуществляющие разбирательство, определяют и инициируют 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.
3.6. Проведение разбирательства инцидента ИБ.
3.6.1. В процессе проведения разбирательства инцидента ИБ устанавливаются:
— дата и время совершения инцидента ИБ:
— информационные ресурсы, затронутые инцидентом ИБ;
— Ф.И.О. 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.
3.6.2. После получения необходимой информации по инциденту ИБ осуществляющая разбирательство Комиссия (ответственное лицо) проводит анализ полученных данных.
3.6.3. 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 сотрудником, ответственным за проведение разбирательства, направляется непосредственном) руководителю предполагаемого нарушителя ИБ.
3.6.4. Восстановление временно отключенных у нарушителя ИБ прав доступа к ИР производится по заявке руководителя нарушителя ИБ или осуществляющей разбирательство Комиссии (ответственного лица).
3.7. Собранная в процессе разбирательства инцидента ИБ информация фиксируется Комиссией (ответственным лицом) в карточке инцидента ИБ (Приложение №3) и учитывается при подготовке акта разбирательства инцидента ИБ (Приложение №4).
3.8. Комиссия (ответственное лицо) направляет акт разбирательства инцидента ИБ директору Школы.
3.9. На основании полученного акта разбирательства инцидента ИБ в срок не более трех рабочих дней организуется проведение мероприятий, направленных на снижение рисков информационной безопасности в будущем:
— повторное ознакомление нарушителя ИБ с Правилами, с должностной инструкцией, с Положением об обработке и защите персональных данных;
— анализ и пересмотр имеющихся прав доступа к информационным ресурсам у нарушителя ИБ;
— доведение до всех сотрудников Школы требований правовых актов в области ИБ.

Приложение №1
к Правилам осуществления
внутреннего контроля
соответствия обработки
персональных данных
требованиям по защите
персональных данных

Контрольный лист
по проведению внутреннего контроля
соответствия обработки персональных данных требованиям по защите персональных данных в информационной системе персональных данных «Сетевой город. Образование» ,«Е-Услуги»

№ п/п	Критерии проверки	ИР 1	ИР 2	Примечание
1.	Соответствие состава фактически собираемых и обрабатываемых персональных данных утвержденному перечню			
2.	Соблюдение ограниченного доступа к персональным данным			
3.	Соблюдение мер по обеспечению безопасности персональных данных:			
3.1.	физическая зашита материальных носителей персональных данных			
3.2.	защита персональных данных, обрабатываемых с помощью средств вычислительной техники			
4.	Соблюдения порядка уточнения, блокирования и уничтожения персональных данных			
5.	Контроль ведения журналов			
6.	Организация хранения персональных данных/Соответствие хранения персональных данных			
7.	Работа с обращениями субъектов персональных данных			
8.	Соблюдение правил передачи персональных, Данных третьим лицам			

_____
(Фамилия И.О., должность, подпись)

Приложение № 2
к Правилам осуществления
внутреннего контроля
соответствия обработки
персональных данных
требованиям по защите
персональных данных

Акт
от «___»_____20___г.
внутреннего контроля соответствия обработки персональных данных в МБОУ СОШ № 5 им. В.В. Терешковой

Комиссия МБОУ СОШ № 5 им. В.В. Терешковой в составе:

_____
_____
_____
в присутствии должностного лица МБОУ СОШ № 5 им. В.В. Терешковой, которому поручена обработка персональных данных:_____
провели контроль соответствия обработки персональных данных мероприятия по контролю:
- соответствия фактического состояния порядка обработки персональных данных требованиям законодательства и локальным нормативным актам;
- мер по обеспечению безопасности персональных данных.
В ходе проверки комиссией установлено:
- нарушений установленных законодательством и локальными нормативными актами не выявлено/выявлено.

По итогам внутреннего контроля был заполнен контрольный лист являющийся неотъемлемым приложением к данному акту. Объяснения (возражения) к акту о результатах _____ проверки: прилагаются/не прилагаются (ненужное зачеркнуть) на __ л.
Меры по устранению нарушений:
_____
Срок устранения нарушений:
_____
Подписи членов комиссии:
_____/
_____/
_____/

Приложение № 3
к Правилам осуществления
внутреннего контроля
соответствия
обработки персональных данных
требованиям по защите
персональных данных

Карточка инцидента информационной безопасности (ИБ)

Дата инцидента ИБ_____ Номер инцидента ИБ_____

Информация о сообщившем:

Ф.И.О.	Должность	Рабочий телефон

Нужное обвести:

Тип инцидента:	Действительный	Попытка	Подозрение		
Предполагаемый Вид угрозы информационной безопасности:	Непреднамеренная	Преднамеренная	Удаленное вмешательство	Ошибка проектирования информационной системы	Технический сбой
Нарушитель:	Отсутствует	Не установлен	Внутренний: организация, Ф.И.О., должность нарушителя		
Последствия инцидента:	Без последствий	Нарушение работоспособности и 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:	Никаких действий не требуется	Без привлечения внешнего исполнителя	С привлечением внешнего исполнителя	Описание действий	

Подпись сотрудников, проводившего разбирательство_____

Приложение № 4
к Правилам осуществления
внутреннего контроля
соответствия обработки
персональных данных
требованиям по защите
персональных данных

Акт №_____
от «____»_____20____г.
разбирательства инцидента информационной безопасности

Комиссией (ответственным лицом) в составе:
_____
или Ф.И.О. ответственного лица, проводившего разбирательство инцидента ИБ_____.
Проведено разбирательство инцидента ИБ. выявленного_____ (дата). В результате разбирательства установлено:
Сотрудники МБОУ СОШ№5 им.В.В.Терешковой, причастные к инциденту ИБ: должность и Ф.И.О.
_____

Инцидент ИБ (описание произошедшего инцидента ИБ)
_____
_____
_____
Причины возникновения инцидента _____
Ущерб (при наличии), причиненный инцидентом ИБ _____ перечень пострадавших ресурсов (объектов) _____
Действия, предпринятые для ликвидации последствий инцидента ИБ
_____

Подписи членов Комиссии, проводивших разбирательство_____
Подпись сотрудника, проводившего разбирательство_____

Головина Е.Н.

Подписано цифровой подписью:
Головина Е.Н.
Дата: 2021.10.12 13:20:22 +03'00'