Муниципальное бюджетное образовательное учреждение дополнительного образования детей Центр детского творчества имени Н.М. Аввакумова»
Асбестовского городского округа

ПРИКАЗ

30.01.2015 г. № 19(а)

Об утверждении Правил осуществления внутреннего контроля соответствия обработки персональных данных требованиям по защите персональных данных

В соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Постановлением 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», Приказом ФСТЭК РФ от 05.02.2010 № 58 «Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных»

П Р И К А З Ы В А Ю:

1. Утвердить Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям по защите персональных данных (Приложение № 1).
2. Осинцевой Д.Н., секретарю, ознакомить работников МБОУ ДОД ЦДТ с указанными изменениями в срок до 31.08.2015.
3. Контроль за исполнением приказа оставляю за собой.

Директор ЦДТ О.В. Дубина

Приложение № 1
к приказу МБОУ ДОД ЦДТ
от 19.01.2015 № 19(а)

Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям по защите персональных данных

1. Общие положения

1.1. Настоящие правила разработаны в соответствии с требованиями Федерального 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 в 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 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 ДОД ЦДТ.

1.3. Основные термины и понятия, используемые в Правилах.

- Инцидент ИБ - событие, в результате наступления которого в МБОУ ДОД ЦДТ произошло разглашение конфиденциальной информации, персональных данных, нарушение работоспособности информационных систем, внесение несанкционированных изменений в информационные ресурсы МБОУ ДОД ЦДТ.
- 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 МБОУ ДОД ЦДТ;
- Система защиты 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 МБОУ ДОД ЦДТ организуется проведение периодических проверок условий обработки персональных данных.

2.2. Проверки осуществляются ответственным лицом за обеспечение безопасности персональных данных в МБОУ ДОД ЦДТ, либо исполнителем, которому делегированы полномочия на проверку в соответствии с приказом МБОУ ДОД ЦДТ.

2.3. Проверки условий обработки персональных данных могут быть плановыми и внеплановыми, документарными и проводимыми в помещениях МБОУ ДОД ЦДТ, в которых ведется обработка персональных данных.

2.4. Плановые проверки соответствия обработки персональных данных установленным требованиям в МБОУ ДОД ЦДТ проводятся не менее одного раза в год.

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

- поступившее в МБОУ ДОД ЦДТ письменное заявление субъекта персональных данных о нарушениях правил обработки персональных данных;
- поступившее директору МБОУ ДОД ЦДТ сообщение от сотрудников МБОУ ДОД ЦДТ 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 МБОУ ДОД ЦДТ, 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 целей 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 защиты 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. Лицо, ответственное за обеспечение безопасности персональных данных в МБОУ ДОД ЦДТ, уполномоченное на проведение проверок имеет право:

– запрашивать у сотрудников МБОУ ДОД ЦДТ 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 МБОУ ДОД ЦДТ предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности персональных данных при их обработке;
– вносить директору МБОУ ДОД ЦДТ 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 МБОУ ДОД ЦДТ, в ходе проведения мероприятий внутреннего контроля, должна обеспечиваться конфиденциальность персональных данных.

2.13. В процессе проверки ответственное лицо заполняет контрольный лист (Приложение № 1), 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 ответственного лица.

3. Порядок разбирательства инцидента ИБ

3.1. Разбирательство по вопросам инцидентов ИБ проводится ответственным лицом за обеспечение безопасности персональных данных в МБОУ ДОД ЦДТ или комиссией по защите персональных данных МБОУ ДОД ЦДТ (далее по тексту – Комиссия), утвержденной приказом МБОУ ДОД ЦДТ (в соответствии с решением директора МБОУ ДОД ЦДТ).

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 МБОУ ДОД ЦДТ;
– 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 МБОУ ДОД ЦДТ 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 МБОУ ДОД ЦДТ. Сотрудник МБОУ ДОД ЦДТ может выявить признаки наличия Инцидента ИБ путем анализа текущей ситуации на предмет ее соответствия требованиям федерального законодательства в области защиты 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 МБОУ ДОД ЦДТ, ответственному лицу за обеспечение безопасности персональных данных в МБОУ ДОД ЦДТ 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 непосредственному 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 МБОУ ДОД ЦДТ.

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 МБОУ ДОД ЦДТ 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

№ 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 защита материальных носителей персональных данных			
3.2.	Защита персональных данных, обрабатываемых с помощью средств вычислительной техники			
4.	Соблюдение 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
внутреннего контроля

«___» _____ 20__ г. № _____

Ответственным лицом за проверку соблюдения обязательных требований в области защиты персональных данных МБОУ ДОД ЦДТ

_____

в присутствии должностного лица МБОУ ДОД ЦДТ, которому поручена обработка персональных данных,_____

были проведены мероприятия по контролю:

- соответствия фактического состояния порядка обработки персональных данных требованиям законодательства и локальным нормативным актам;
- мер по обеспечению безопасности персональных данных.

В ходе контрольных мероприятий 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.

Подпись сотрудника, проводившего проверку_____

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 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 сотрудника, проводившего разбирательство_____

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

Акт № ____ от _____
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 ДОД ЦДТ, 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 члены Комиссии, проводившей разбирательство___
Подпись сотрудника, проводившего разбирательство____