

МУНИЦИПАЛЬНОЕ УЧРЕЖДЕНИЕ
ДОПОЛНИТЕЛЬНОГО ОБРАЗОВАНИЯ
«ДОМ ДЕТСКОГО ТВОРЧЕСТВА»

ПРИКАЗ

01 декабря 2020 г.

г. Благодарный

№ 152-ОД

О назначении ответственных

Во исполнение требований Федерального закона №152-ФЗ от 27 июля 2006 г. «О персональных данных», приказа ФСТЭК России №21 от 18 февраля 2013 г. «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» и прочих нормативных документов по защите информации,

ПРИКАЗЫВАЮ:

1. Назначить Ответственным за организацию обработки персональных данных - старшего педагога дополнительного образования МУ ДО «ДДТ» Людмилу Васильевну Белоцерковскую.

2. Назначить Администратором информационных систем персональных данных - старшего педагога дополнительного образования МУ ДО «ДДТ» Виталия Эдуардовича Малиновского.

3. На время временного отсутствия (болезнь, отпуск и т.д.) ответственных лиц, указанных в п. 1–3 настоящего Приказа, ответственность за организацию обработки персональных данных, осуществление организационных и технических мероприятий по защите персональных данных и осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных Федеральному закону №152-ФЗ от 27 июля 2006 г. и принятыми в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, и иным локальным нормативным актам, возложить на лиц, исполняющих их обязанности, назначенных и допущенных в установленном порядке.

4. Утвердить и ввести в действие Инструкцию ответственного за организацию обработки персональных данных в МУ ДО «ДДТ» (Приложение 1 к настоящему Приказу).

5. Утвердить и ввести в действие Инструкцию администратора информационных систем персональных данных МУ ДО «ДДТ» (Приложение 3 к настоящему Приказу).

6. Требования настоящего приказа довести до назначенных ответственных лиц.

.Контроль за исполнением настоящего приказа оставляю за собой.

Директор муниципального учреждения
дополнительного образования
«Дом детского творчества»



В.В.Логачева

законодательства Российской Федерации о ПДн, в том числе требований к защите ПДн;

-взаимодействует с уполномоченными органами государственной власти Российской Федерации, органами по аттестации, испытательными лабораториями по вопросам обработки и защиты ПДн (при проведении государственного контроля и надзора, аттестации, сертификации);

-актуализирует перечень должностей работников, имеющих доступ к обработке ПДн;

-актуализирует перечень работников, допущенных в помещения, в которых осуществляется обработка ПДн;

-доводит до сведения работников, обрабатывающих ПДн положения законодательства Российской Федерации о ПДн, локальных актов по вопросам обработки ПДн, требований к защите ПДн, в том числе требований к защите ПДн;

-организовывает прием и обработку обращений и запросов субъектов ПДн или их представителей, чьи ПДн обрабатываются в Учреждении, или их представителей, и осуществляет контроль за приемом и обработкой таких обращений и запросов;

-разрабатывает и корректирует эксплуатационную документацию и организационно-распорядительные документы по защите ПДн.

-принимает участие в деятельности:

-по подготовке, пересмотру, уточнению локальных актов по защите информации;

-по аттестации объектов информатизации.

4.Права

Ответственный имеет право:

-требовать от работников, обрабатывающих ПДн, соблюдения установленной технологии обработки ПДн и выполнения инструкций по обеспечению безопасности информации;

-инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения защиты, несанкционированного доступа, утраты, уничтожения ПДн и технических средств, обрабатывающих ПДн;

-требовать прекращения обработки ПДн в случае нарушения установленного порядка работ или нарушения функционирования средств и систем защиты информации;

-участвовать в анализе ситуаций, касающихся функционирования средств защиты информации и расследования фактов несанкционированного доступа;

-подавать свои предложения по совершенствованию организационных и технических мер по защите ПДн.

5. Ответственность

На Ответственного возлагается персональная ответственность за качество выполняемых им функций по обеспечению защиты ПДн.

Ответственный несет ответственность по действующему законодательству Российской Федерации за разглашение сведений ограниченного доступа, ставших ему известными при выполнении служебных обязанностей, в том числе предусмотренных настоящей Инструкцией.

6. Срок действия и порядок внесения изменений

Настоящая Инструкция вступает в силу с момента ее утверждения и действует бессрочно.

Настоящая Инструкция подлежит пересмотру не реже одного раза в три года.

Изменения и дополнения в настоящую Инструкцию вносятся приказом Директора Учреждения.



Приложение 2
к приказу МУ ДО «ДДТ»
от «04» декабря 2020 г. № 152-ОД

ИНСТРУКЦИЯ **администратора информационных систем персональных данных** **МУ ДО «ДДТ»**

1. Термины и определения

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

Инцидент информационной безопасности – любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность. Инцидентами информационной безопасности являются:

- утрата услуг, оборудования или устройств;
- системные сбои или перегрузки;
- ошибки пользователей;
- несоблюдение политики или рекомендаций по информационной безопасности;
- нарушение физических мер защиты;
- неконтролируемые изменения систем;
- сбои программного обеспечения и отказы технических средств;
- нарушение правил доступа.

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.

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

Средство защиты информации – программное обеспечение, программно-аппаратное обеспечение, аппаратное обеспечение, вещество или материал, предназначенное или используемое для защиты информации.

2. Общие положения

Настоящая Инструкция определяет функции, обязанности и права администратора информационных систем персональных данных (далее – Администратор ИСПДн) МУ ДО «ДДТ» (далее – Учреждение).

Настоящая Инструкция является дополнением к действующим нормативным документам по вопросам обеспечения безопасности персональных данных (далее – ПДн), не исключает обязательного выполнения их требований.

Администратор ИСПДн назначается приказом Директора Учреждения.

На время отсутствия (болезнь, отпуск, пр.) Администратора ИСПДн, его обязанности возлагаются на работника, назначенного и допущенного в установленном порядке.

3.Функциональные обязанности

Администратор ИСПДн выполняет следующие функции:

- управляет параметрами ИСПДн;
- управляет заведением и удалением учетных записей пользователей;
- управляет полномочиями пользователей;
- поддерживает правила разграничения доступа;
- управляет параметрами настройки программного обеспечения;
- управляет учетными записями пользователей программных средств обработки ПДн;
- оказывает помощь в смене и восстановлению паролей;
- управляет установкой обновлений программного обеспечения;
- регистрирует события в ИСПДн, связанные с защитой ПДн (события безопасности);
- поддерживает конфигурацию ИСПДн (структуру ИСПДн, состава, мест установки и параметров программного обеспечения и технических средств) в соответствии с эксплуатационной документацией на ИСПДн;
- восстанавливает работоспособность программного обеспечения и технических средств ИСПДн.

Выявляет инциденты (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования ИСПДн и (или) к возникновению угроз безопасности ПДн:

- отказы в обслуживании;
- сбои (перезагрузки) в работе технических средств и программного обеспечения;
- нарушения правил разграничения доступа;
- неправомерные действия по сбору ПДн;
- иные события, приводящие к возникновению инцидентов.

Своевременно информирует ответственного за обеспечение безопасности ПДн в ИСПДн, о возникновении инцидентов в ИСПДн;

Принимает меры по устранению инцидентов, в том числе:

- по восстановлению ИСПДн и ее сегментов в случае отказа в обслуживании или после сбоев;
- по устранению последствий нарушения правил разграничения доступа, несанкционированного доступа к ПДн, внедрения вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов.

Ведет учет пользователей ИСПДн;

Принимает участие в деятельности по:

- подготовке, пересмотру, уточнению локальных актов по защите ПДн;
- аттестации объектов информатизации.

4.Права

Администратор ИСПДн имеет право:

- требовать от работников – пользователей ИСПДн соблюдения установленной технологии обработки ПДн и выполнения требований инструкций по обеспечению безопасности ПДн;
- инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения защиты, несанкционированного доступа, утраты, порчи защищаемых ПДн и технических средств, входящих в состав ИСПДн;
- требовать прекращения обработки ПДн в случае нарушения установленного порядка работ или нарушения функционирования системы защиты ПДн;
- участвовать в анализе ситуаций, касающихся функционирования средств защиты информации и расследования фактов несанкционированного доступа;
- подавать свои предложения по совершенствованию организационных и технических мер по защите ПДн.

5.Ответственность

Администратору ИСПДн категорически запрещается:

- использовать компоненты программного и аппаратного обеспечения ИСПДн в неслужебных (личных) целях;
- умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к инцидентам информационной безопасности.

На Администратора ИСПДн возлагается персональная ответственность за качество проводимых им работ по обеспечению бесперебойного и стабильного функционирования ИСПДн.

Администратор несет ответственность по действующему законодательству за разглашение сведений ограниченного доступа, ставших ему известными при выполнении служебных обязанностей, в том числе предусмотренных настоящей Инструкцией.

6.Срок действия и порядок внесения изменений

Настоящая Инструкция вступает в силу с момента ее утверждения и действует бессрочно.

Настоящая Инструкция подлежит пересмотру не реже одного раза в три года.

Изменения и дополнения в настоящую Инструкцию вносятся приказом Директора Учреждения.



Приложение № 2
к приказу МУ ДО «ДДТ»
от 30.12.2020 г. №150-ОД

ПРАВИЛА доступа работников в помещения, в которых ведется обработка персональных данных в МУ ДО «ДДТ»

1. Термины и определения

Контролируемая зона — пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

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.

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

2. Общие положения

Настоящие Правила доступа работников в помещения, в которых ведется обработка персональных данных в МУ ДО «ДДТ» (далее – Правила) устанавливают единые требования к доступу работников в помещения, в которых ведется обработка персональных данных (далее – ПДн).

Настоящие Правила разработаны в соответствии с нормативными правовыми актами Российской Федерации в области защиты ПДн, методическими и руководящими документами уполномоченных федеральных органов исполнительной власти.

Правила обязательны для исполнения всеми работниками, которые участвуют в обработке ПДн.

Нарушение Правил влечёт материальную, дисциплинарную, гражданскую, административную и уголовную ответственность в соответствии с нормами действующего законодательства Российской Федерации.

В здании, расположенном по адресу: 356420, Ставропольский край, г. Благодарный, ул. Первомайская, д.48 установлен пропускной режим, проход работников и посетителей в здание по рабочим дням в рабочее время (с 8.00 до 17.00) осуществляется с обязательной регистрацией в журнале учета посетителей.

3. Организация доступа в помещения

Право на бесконтрольный доступ в помещения, в которых ведется обработка ПДн (далее – Помещения), имеют только работники, которым в связи со служебными обязанностями предоставлен доступ к ПДн (далее – Уполномоченные работники).

Нахождение в Помещениях лиц, не имеющих права доступа к ПДн, возможно только в сопровождении (в присутствии в соответствующем Помещении) Уполномоченного работника.

Уборка Помещений должна производиться в присутствии Уполномоченного работника, с соблюдением мер, исключающих доступ посторонних лиц к защищаемым ресурсам. При этом экраны мониторов должны быть выключены (либо осуществлена временная блокировка экранов/учетных записей пользователей автоматизированных рабочих мест), документы, находящиеся в печатающих устройствах, и учетные носители информации должны быть убраны.

Доступ в Помещения разрешается только по рабочим дням в рабочее время (с 8:00 до 17:00).

Доступ в Помещения в нерабочее время возможен только по письменной заявке Уполномоченного работника, имеющей разрешающую резолюцию Директора МУ ДО «ДДТ» (далее – Учреждение).

Работник, покидающий (в том числе в течение рабочего дня и по его завершении) помещение, в котором осуществляется обработка ПДн в Учреждении, обязан:

- проверить закрытие на запоры окон;
- проверить отключение от электросети всех видов электрооборудования и электроприборов, не требующих по условиям эксплуатации постоянного подключения к электросети, отсутствие признаков загорания (запах гари, задымление и т.п.);
- выключить освещение в Помещении;
- закрыть помещение на ключ.

В случае возникновения нештатной ситуации (пожар, затопление, сбой в работе или выход из строя инженерных систем, совершение незаконных действий) работники коммунальных и аварийно-технических служб имеют право незамедлительного, беспрепятственного доступа в Помещения, в которых ведется обработка ПДн, в любое время суток, без какого-либо предварительного уведомления с целью предотвращения или ликвидации нештатной ситуации, или последствий нештатной ситуации. По результатам предотвращения или ликвидации нештатной ситуации, или последствий нештатной ситуации оставляется Акт вскрытия помещения при чрезвычайных ситуациях.

4. Ограничение доступа в помещения

В целях соблюдения требований к ограничению доступа в Помещения обеспечивается:

- наличие на входах в Помещения дверей, оборудованных запорными устройствами;
- содержание дверей Помещений в нерабочее время в закрытом на запорное устройство состоянии;
- содержание окон в Помещениях в нерабочее время в закрытом состоянии.

5.Срок действия и порядок внесения изменений

Настоящие Правила вступают в силу с момента их утверждения и действуют бессрочно.

Настоящие Правила подлежат пересмотру не реже одного раза в три года.

Изменения и дополнения в настоящие Правила вносятся приказом Директора Учреждения.