Приложение 14
к приказу МАУДО «ДПШ»
от 31.08.2020 № 276/1-од

Инструкция
ответственного за организацию обработки персональных данных

I. Общие положения

1. Данная Инструкция определяет основные обязанности и права ответственного за организацию обработки персональных данных Муниципального автономного учреждения дополнительного образования «Дворец пионеров и школьников им. Н.К. Крупской г.Челябинска» (далее - МАУДО «ДПШ»).

2. Ответственный за организацию обработки персональных данных является штатным работником МАУДО «ДПШ» и назначается приказом директора.

3. Решение вопросов организации защиты персональных данных в МАУДО «ДПШ» входит в прямые служебные обязанности ответственного за организацию обработки персональных данных.

4. Ответственный за организацию обработки персональных данных обладает правами доступа к любым носителям персональных данных МАУДО «ДПШ».

II. Термины и определения

5. **Блокирование персональных данных** – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных) (ст.3 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных»).

Доступ к информации – возможность получения информации и её использования (ст.2 Федерального закона от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и защите информации»).

Информационная система персональных данных (ИСПДн) – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств (ст.3 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных»).

Несанкционированный доступ (НСД) – доступ к информации, хранящейся на различных типах носителей (бумажных, магнитных, оптических и т. д.) в компьютерных базах данных, файловых хранилищах, архивах, секретных частях и т. д. различных организаций путём изменения (повышения, фальсификации) своих прав доступа.

Носитель информации - любой материальный объект или среда, используемый для хранения или передачи информации.

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 (ст.3 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных»).

Пользователь – работник, участвующий в рамках своих функциональных обязанностей в процессах обработки персональных данных.

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) (ст.3 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных»).

Средство защиты информации (СЗИ) – техническое, программное средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

III. Должностные обязанности

6. Ответственный за организацию обработки персональных данных обязан осуществлять внутренний контроль за исполнением сотрудниками МАУДО «ДПШ» требований законодательства Российской Федерации и положений локальных нормативных актов МАУДО «ДПШ» при обработке персональных данных, доводить до сведения работников учреждения нормы законодательства и внутренних локальных актов по работе с персональными данными, в том числе:

1) знать перечень и условия обработки персональных данных в МАУДО «ДПШ»;

2) знать и предоставлять изменения на утверждение директору к списку лиц, доступ которых к персональным данным необходим для выполнения ими своих служебных (трудовых) обязанностей;

3) участвовать в определении полномочий пользователей ИСПДн (оформлении разрешительной системы доступа), минимально необходимых им для выполнения служебных (трудовых) обязанностей;

4) осуществлять учёт документов, содержащих персональные данные, их уничтожение, либо контроль процедуры их уничтожения;

5) блокировать доступ к персональным данным при обнаружении нарушений порядка их обработки;

6) реагировать на попытки несанкционированного доступа к информации в установленном гл. IV настоящей Инструкции порядке;

7) контролировать осуществление мероприятий по установке и настройке средств защиты информации;

8) производить периодический контроль за соблюдением режима безопасности помещений, в которых размещена информационная система, путем:

- контроля расположения мониторов для исключения визуального доступа к нему возможному внешнему нарушителю;

- контроля исключения визуального доступа при обработке персональных данных.

9) поддерживать в актуальном состоянии локальные документы, направленные на обеспечение защиты персональных данных;

10) при приеме/увольнении работников актуализировать документ «Список лиц, доступ которых к защищаемой информации необходим для выполнения служебных (трудовых) обязанностей»;

11) организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов;

12) по указанию руководства своевременно и точно отражать изменения в локальных нормативно-правовых актах по управлению средствами защиты информации в ИСПДн и правилам обработки персональных данных;

13) в установленные законодательством сроки регистрировать и отвечать на поступающие запросы и обращения субъектов ПДн или их законных представителей;

14) проводить занятия и инструктажи с работниками и руководителями структурных подразделений о порядке работы с персональными данными и изучение руководящих документов в области обеспечения безопасности персональных данных;

15) проводить разбирательства и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, нарушения правил работы с документами, содержащими персональные данные, или по другим нарушениям, которые могут привести к снижению уровня защищённости персональных данных;

16) контролировать соблюдение работниками локальных документов, регламентирующих порядок работы с программными, техническими средствами ИСПДн и персональными данными;

17) вносить свои предложения по совершенствованию мер защиты персональных данных в ИСПДн, разработке и принятии мер по предотвращению возможных опасных последствий нарушений, приводящих к снижению уровня защищённости персональных данных;

18) организовать учет обращений субъектов персональных данных, контролировать заполнение «Журнала учета обращений субъектов персональных данных»;

19) представлять интересы МАУДО «ДПШ» при проверках надзорных органов в сфере обработки персональных данных;

20) знать законодательство РФ о персональных данных, следить за его изменениями;

21) выполнять иные мероприятия, требуемые нормативными документами по защите персональных данных.

IV. Действия при обнаружении попыток несанкционированного доступа

7. К попыткам несанкционированного доступа относятся:

- сеансы работы с персональными данными незарегистрированных пользователей, или пользователей, нарушивших установленную периодичность доступа, или срок действия полномочий которых истёк, или превышающих свои полномочия по доступу к данным;
- действия третьего лица, пытающегося получить доступ (или уже получившего доступ) к ИСПДн, при использовании учётной записи администратора или другого пользователя ИСПДн, методом подбора пароля, использования пароля, разглашённого владельцем учётной записи или любым другим методом.

8. При выявлении факта несанкционированного доступа ответственный за организацию обработки персональных данных обязан:

1) прекратить несанкционированный доступ к персональным данным;

2) доложить директору МАУДО «ДПШ» служебной запиской о факте несанкционированного доступа, его результате (успешный, неуспешный) и предпринятых действиях;

3) известить руководителя структурного подразделения, в котором работает пользователь, от имени учетной записи которого была осуществлена попытка несанкционированного доступа, о факте несанкционированного доступа;

4) известить ответственного за обеспечение безопасности персональных данных в информационных системах о факте несанкционированного доступа.

V. Права

9. Ответственный за организацию обработки персональных данных имеет право:

1) доступа ко всем персональным данным субъектов персональных данных, обрабатываемых в МАУДО «ДПШ»;

2) требовать от работников выполнения норм законодательства Российской Федерации о персональных данных, внутренних локальных нормативно-правовых актов в части работы с персональными данными;

3) блокировать доступ к персональным данным любых пользователей, если это необходимо для предотвращения нарушения режима защиты персональных данных;

4) проводить служебные расследования и опрашивать пользователей по фактам несоблюдения условий хранения носителей персональных данных, нарушения правил работы с техническими и программными средствами ИСПДн, в том числе со средствами защиты информации, или по другим нарушениям, которые могут привести к снижению уровня защищённости персональных данных.

VI. Ответственность

10. Ответственный за организацию обработки персональных данных несёт персональную ответственность за соблюдение требований настоящей Инструкции, за качество проводимых им работ по обеспечению безопасности персональных данных и за все действия, совершенные от имени его учётной записи в ИСПДн, если с его стороны не было предпринято необходимых действий для предотвращения несанкционированного использования его учётной записи.

11. Ответственный за организацию обработки персональных данных при нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта, несёт дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с законодательством Российской Федерации.

12. Разглашение персональных данных субъекта (передача их посторонним лицам, в том числе другим работникам, не имеющим к ним допуск), их публичное раскрытие, утрата документов и иных носителей, содержащих персональные данные субъекта, а также иные нарушения обязанностей по их защите и обработке, установленных локальными нормативно-правовыми актами (приказами, распоряжениями) МАУДО «ДПШ», влечет наложение на работника, имеющего доступ к персональным данным, дисциплинарных взысканий в виде: замечания, выговора, увольнения. Работник МАУДО «ДПШ», имеющий доступ к персональным данным субъекта и совершивший указанный дисциплинарный

проступок, несет полную материальную ответственность в случае причинения его действиями ущерба МАУДО «ДПШ» (в соответствии с п.7 ст.243 Трудового кодекса РФ).

В отдельных случаях, при разглашении персональных данных, работник, совершивший указанный проступок, несет ответственность в соответствии со ст.13.11, 13.14 Кодекса об административных правонарушениях РФ.

13. В случае незаконного сбора или публичного распространения информации о частной жизни лица (нарушения неприкосновенности частной жизни), предусмотрена ответственность в соответствии со ст.137 Уголовного кодекса РФ.