УТВЕРЖДЕНО
Приказом руководителя
МУ ДО «СШ № 1»
от «28» декабря 2024 г. № 134-ОД

Положение
о порядке организации и проведении работ по защите персональных данных в муниципальном бюджетном учреждении дополнительного образования Петрозаводского городского округа «Спортивная школа № 1» (МУ ДО «СШ № 1»)

г. Петрозаводск
2024 год

1. Общие положения

1. Положение о порядке организации и проведении работ по технической защите персональных данных в муниципальном учреждении дополнительного образования Петрозаводского городского округа «Спортивная школа № 1» (МУ ДО «СШ № 1») (далее соответственно - положение, организация) является основным документом планирования и выполнения мероприятий по технической защите персональных данных.

1.2.Положение разработано в соответствии с требованиями законодательства Российской Федерации в области защиты персональных данных.

1.3.Требования настоящего положения направлены на предотвращение утечки защищаемой информации, несанкционированного доступа и неправомерных воздействий на информацию.

1.4.Основные направления работ по защите персональных данных (далее - защите ПДн):

1) предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;

2) разработка и практическая реализация организационных и технических мероприятий по защите:

- информации, обрабатываемой средствами вычислительной техники (далее - СВТ);

- информации, выводимой на экраны видеомониторов;

- информации, хранящейся на физических носителях, в том числе, входящих в состав информационной системы персональных данных (далее - ИСПДн);

3) своевременное обнаружение фактов несанкционированного доступа к информации;

4) недопущение вредоносного воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;

5) возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;

6) постоянный контроль за обеспечением уровня защищенности информации.

1.5. Основные способы и меры защиты персональных данных:

1) категорирование объектов информатизации;

2) противодействие утечке информации по техническим каналам, несанкционированному доступу, программно-техническому воздействию с целью нарушения целостности и доступности ПДн в процессе их обработки, передачи и хранения;

3) применение автоматизированных систем в защищенном исполнении для обработки, хранения и передачи ПДн;

4) использование сертифицированных средств защиты ПДн от утечки по техническим каналам;

использование сертифицированных средств защиты ПДн от несанкционированного доступа (далее - НСД) и контроль их эффективности;

5) использование сертифицированных средств защиты ПДн от несанкционированного доступа (далее - НСД) и контроль их эффективности;

6) аттестация объектов информатизации по требованиям безопасности информации.

1.6.Должностные лица, ответственные за выполнение требований настоящего положения:

1) ответственность за защиту ПДн в организации несет руководитель и все сотрудники, допущенные к работе с данной информацией;

2) организационно-методическое руководство работами по защите ПДн, выполнение работ по защите ПДн и контроль выполнения требований настоящего положения возлагается на ответственного за обеспечение информационной безопасности (администратора информационной безопасности).

2. Планирование и организация работ по защите ПДн

2.1.Планируемые мероприятия по защите ПДн разрабатываются ответственным за обеспечение информационной безопасности и включаются отдельным разделом в годовой план мероприятий организации по Защите ПДн.

Раздел плана по защите ПДн предусматривает следующие подразделы:

мероприятия по выполнению требований законодательства Российской Федерации по защите ПДн;

организационно-методическое обеспечение работ по защите ПДн (разработка, корректировка и согласование организационно-методических документов, планов, отчетов; составление заявок на технические устройства защиты ПДн; обучение сотрудников);

контрольные мероприятия (оценка достаточности применяемых мер и средств защиты ПДн; эффективность принимаемых мер защиты ПДн в организации; участие в работе контролирующих органов).

2.2. Организация работ по защите ПДн, методическое руководство, реализация и контроль за эффективностью мер по защите ПДн возлагается на ответственного за обеспечение информационной безопасности (администратора информационной безопасности).

2.3. Для выполнения мероприятий по защите ПДн могут привлекаться специализированные организации, имеющие соответствующие лицензии ФСТЭК России и/или ФСБ России.

3. Порядок эксплуатации объектов информатизации

3.1. Порядок, методы и способы Защиты ПДн определяются нормативными правовыми актами и документами ФСБ России и ФСТЭК России.

3.2. Достаточность принятых мер по обеспечению безопасности ПДн при ее обработке в системах оценивается при проведении государственного контроля и надзора.

3.3. Безопасность ПДн при их обработке в ИСПДн обеспечивается с помощью системы защиты ПДн, включающей организационные меры и средства защиты

информации, средства предотвращения несанкционированного доступа и утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки, а также используемые в ИСПДн информационные технологии.

3.4. Эксплуатация системы защиты ПДн осуществляется в соответствии с технологическим процессом и инструкциями по эксплуатации средств защиты информации.

3.5. При эксплуатации системы защиты ПДн необходимо соблюдать следующие требования:

- доступ к защищаемой информации лиц, работающих в ИСПДн (пользователей, обслуживающего персонала), должен производиться в соответствии с порядком, установленным разрешительной системой доступа;

- на период обработки ПДн в помещении, где размещаются основные технические средства и системы, могут находиться только лица, допущенные в установленном порядке к обрабатываемой информации, допуск других лиц для проведения необходимых профилактических или ремонтных работ может осуществляться в это помещение только в присутствии ответственного за обеспечение информационной безопасности;

- при размещении в помещении нескольких технических средств отображения информации, должен быть исключен несанкционированный просмотр выводимой на них информации;

- в случае компрометации парольной информации ответственный за обеспечение информационной безопасности должен принять оперативные меры по замене паролей и идентификаторов, а также инициировать служебное расследование.

3.6. Все носители ПДн на бумажной, магнитной, оптической (магнито-оптической) основе, используемые в процессе обработки ПДн в ИСПДн, подлежат учету.

3.7. Временно не используемые учтенные носители информации должны храниться в специально оборудованных для этого местах, недоступных для посторонних лиц.

3.8. Периодический контроль включает в себя: контроль выполнения организационных мероприятий по защите ПДн в соответствии с годовым планом мероприятий по защите ПДн; инструментальный контроль эффективности внедренных средств защиты.

Инструментальный контроль проводится не реже одного раза в год с привлечением на договорной основе организаций, проводивших аттестацию этих объектов или других организаций, имеющих лицензию на соответствующий вид деятельности.

3.9. По результатам контроля составляется акт, в котором оценивается состояние системы защиты ПДн, указываются имеющиеся нарушения и сроки их устранения, оформляется заключение.

В случае выявления серьезных нарушений, работы на объекте информатизации приостанавливаются до их устранения.

4. Ответственность должностных лиц

4.1. Должностными лицами, ответственными за организацию и осуществление мероприятий по защиты ПДн в организации являются:

- руководитель организации;
- ответственный за организацию обработки ПДн;
- ответственный за информационную безопасность организации (администратор информационной безопасности).

4.2. Обязанности руководителя организации применительно к настоящему положению:

Определяет сотрудников организации, привлекаемых к защите ПДн;

Утверждает документы по защите ПДн;

Принимает решение о финансировании работ по защите ПДн;

Принимает решение о прекращении работ в случае выявления нарушений требований по защите ПДн, а также о возобновлении работ после их устранения.

4.3. Обязанности ответственного за организацию обработки ПДн:

- Соблюдать требования законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных, Правил обработки персональных данных и других нормативных документов в области обработки и защиты персональных данных.

- Доводить до сведения сотрудников положения законодательства Российской Федерации о персональных данных, Правил обработки персональных данных и других нормативных документов по вопросам обработки и требований к защите персональных данных.

- Проводить инструктажи и занятия по изучению правовой базы по защите персональных данных с сотрудниками, имеющими доступк персональным данным, и вести Журнал проведения инструктажей по информационной безопасности.

- Оказывать консультационную помощь сотрудникам по применению средств защиты персональных данных.

- Осуществлять контроль соблюдения законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных, и Правил обработки персональных данных согласно Правилам осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных

- Проводить регулярные внутренние проверки, согласно Плану внутренних проверок контроля соответствия обработки персональных данных требованиям к защите персональных данных.

- Участвовать в проведении расследований случаев несанкционированного доступа к персональным данным и других нарушений Правил обработки персональных данных.

- Составлять и предлагать на утверждение руководителю перечень лиц и объема их полномочий, которым разрешен доступ к персональным данным.

- Не допускать к работе с персональными данными лиц, не обладающих для этого соответствующими правами.

- Осуществлять регистрацию обращений и запросов субъектов персональных данных или их представителей в Журнале учёта обращений субъектов

персональных данных о выполнении их законных прав при обработке персональных данных о выполнении их законных прав.

- Осуществлять методическое руководство работой администраторов безопасности и администраторов информационных систем персональных данных в области защиты персональных данных.
- Предлагать руководству мероприятия по совершенствованию работы по защите персональных данных.

4.4. Обязанности ответственного за информационную безопасность организации (администратор информационной безопасности):

- осуществляет годовое планирование мероприятий организации по защите ПДн и контроль за его выполнением;
- организует разработку и внедрение необходимых организационно¬технических мероприятий по защите ПДн в организации;
- оценивает эффективность принимаемых мер по защите ПДн и организует работы по устранению выявленных недостатков;
- выявляет нарушения в технологии обработки ПДн;
- проверяет правильность функционирования систем разграничения доступа к ПДн и контроль состояния средств защиты ПДн;
- осуществляет документальное оформление проводимых контрольных мероприятий по порядку обработки ПДн;
- оказывает методическую помощь сотрудникам организации по правильной обработке ПДн.