

**Правила
осуществления внутреннего контроля соответствия обработки
персональных данных требованиям к защите персональных данных в
Государственном автономном учреждении дополнительного
образования Мурманской области «Мурманский областной центр
дополнительного образования «Лапландия»**

1. Общие положения

1.1. Настоящие Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (далее – Правила) регламентируют процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, основания, порядок, формы и методы проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в Государственном автономном учреждении дополнительного образования Мурманской области «Мурманский областной центр дополнительного образования «Лапландия» (далее – Учреждении).

1.2. Правила разработаны в соответствии с:

- Конституцией Российской Федерации;
- Федеральным законом «О персональных данных» от 27.07.2006 № 152-ФЗ;
- Федеральным законом «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ;
- Федеральным законом «Об образовании в Российской Федерации» от 29.12.2012 № 273-ФЗ;
- Постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Уставом Учреждения.

1.3. В настоящих Правилах используются основные понятия, определенные в статье 3 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных».

1.4. Для обработки персональных данных сотрудников, необходимых для обеспечения кадровой и бухгалтерской деятельности в Учреждении,

заявителей, поступающих в Учреждение на обучение по дополнительным образовательным программам, используются информационные системы персональных данных (далее – ИСПДн) – инвентарные объекты, включающие составные устройства: персональные компьютеры в количестве 6 штук с инвентарными номерами системных блоков 1013400273, 1013400222, 1010490730, 1013400011, 1013400060, 10104900269.

1.5. Контрольные мероприятия за обеспечением уровня защищённости персональных данных и соблюдений условий использования средств защиты информации (далее – СЗИ), а также соблюдением требований законодательства Российской Федерации по обработке персональных данных в ИСПДн в Учреждении проводятся в следующих целях:

- проверка выполнения требований организационно-распорядительной документации по защите информации и действующего законодательства Российской Федерации в области обработки и защиты персональных данных;
- оценка уровня осведомлённости и знаний работников учреждения в области обработки и защиты персональных данных;
- оценка обоснованности и эффективности применяемых мер и средств защиты.

2. Тематика внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных

2.1. Проверки соответствия обработки персональных данных установленным требованиям разделяются на следующие виды: плановые и внеплановые.

2.2. Плановые контрольные мероприятия проводятся ответственным за организацию обработки персональных данных в соответствии с утверждённым Планом и направлены на постоянное совершенствование системы защиты персональных данных ИСПДн.

2.3. Внеплановые контрольные мероприятия проводятся на основании решения комиссии по информационной безопасности (создаётся на период проведения мероприятий). Решение о проведении внеплановых контрольных мероприятий и созданию комиссии по информационной безопасности может быть принято в следующих случаях:

- по результатам расследования инцидента информационной безопасности;
- по результатам внешних контрольных мероприятий, проводимых контролирующими органами;
- по решению руководителя.

3. Планирование контрольных мероприятий

3.1. Для проведения плановых внутренних контрольных мероприятий работник, ответственный за организацию обработки персональных данных, разрабатывает План внутренних контрольных мероприятий на текущий год.

3.2. План проведения внутренних контрольных мероприятий включает следующие сведения по каждому из мероприятий:

- объекты контроля (процессы, подразделения, информационные системы и т.п.);
- состав участников, привлекаемых для проведения контрольных мероприятий;
- периодичность проведения контрольных мероприятий.

3.3. Общий срок контрольных мероприятий не должен превышать пяти рабочих дней. При необходимости срок проведения контрольных мероприятий может быть продлён, но не более чем на десять рабочих дней.

4. Оформление результатов контрольных мероприятий

4.1. По итогам проведения плановых и внеплановых контрольных мероприятий составляется акт о результатах внутренней проверки, в котором указывается:

- цель проверки;
- основание проверки;
- время проведения проверки;
- результаты проверки;
- рекомендации по устранению выявленных нарушений.

4.2. Акт передаётся руководству.
