

Приложение 2

УТВЕРЖДЕНО  
приказом МОУДО  
«ГДЮЦ «Спортивный»  
от 29.12.2018  
№ 539

**ПРАВИЛА**  
**осуществления внутреннего контроля соответствия обработки**  
**персональных данных требованиям**  
**к защите персональных данных,**  
**политике оператора в отношении обработки**  
**персональных данных**

г. Липецк, 2019 г.

1. Настоящие правила определяют основания, форму и порядок осуществления в Муниципальном образовательном учреждении дополнительного образования «Городской детско-юношеский центр «Спортивный» (далее – Организация или Оператор) внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных и политике оператора в отношении обработки персональных данных, установленным Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Федеральный закон № 152-ФЗ) и принятыми в соответствии с ним нормативными правовыми актами.

2. Настоящие правила разработаны в соответствии с Федеральным законом № 152-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» (далее – постановление Правительства № 1119).

3. Основные понятия и термины, используемые в настоящих правилах, применяются в значениях, определенных статьей 3 Федерального закона № 152-ФЗ.

4. Основанием для проведения внутреннего контроля являются требования Федерального закона № 152-ФЗ (часть 1, статья 18.1) и Постановления Правительства № 1119 (п. 17).

5. Внутренний контроль осуществляется путем проведения проверок не реже 1 раза в год.

6. Проверку проводит Комиссия, назначенная приказом директора Организации или на договорной основе юридическое лицо (индивидуальный предприниматель), имеющее лицензию на осуществление деятельности по технической защите конфиденциальной информации.

7. Состав Комиссии не менее 3-х человек, включая лицо, ответственное за организацию обработки персональных данных. Все члены комиссии при принятии решения обладают равными правами.

8. Комиссия при проведении проверки обязана:

- провести анализ реализации мер, направленных на обеспечение выполнения Оператором обязанностей, предусмотренных Федеральным законом № 152-ФЗ (статья 18.1, статья 19) и принятыми в соответствии с ним локальными актами Оператора, определяющими его политику в отношении обработки персональных данных;

- провести анализ выполнения Оператором требований по определению и обеспечению уровня защищенности персональных данных, утвержденных постановлением Правительства № 1119;

- провести анализ реализации Оператором организационных и технических мер по обеспечению безопасности персональных данных, утвержденных приказом ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

- провести анализ состава оборудования, программных средств, включая средства защиты, входящих в состав информационной системы персональных данных на соответствие Техническому паспорту информационной системы;
- своевременно и в полной мере исполнять предоставленные полномочия по предупреждению, выявлению и пресечению нарушений требований к защите персональных данных, установленных законодательными и нормативными правовыми актами Российской Федерации;
- при проведении проверки соблюдать законодательство Российской Федерации, права и законные интересы Оператора.

9. Комиссия при проведении проверки вправе:

- запрашивать и получать необходимые документы (сведения) для достижения целей проведения внутреннего контроля;
- получать доступ к информационным системам персональных данных в части, касающейся ее полномочий;
- принимать меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований к защите персональных данных;
- вносить директору Организации предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении требований к защите персональных данных, установленных законодательными и нормативными правовыми актами Российской Федерации.

10. При проведении проверки члены комиссии не вправе:

- требовать представления документов и сведений, не относящихся к предмету проверки;
- распространять информацию и сведения конфиденциального характера, полученные при проведении проверки.

11. По результатам проверки составляется Акт проверки, который подписывается членами комиссии и представляется руководителю Организации для принятия соответствующего решения.

12. В Акте отражаются сведения о результатах проверки, в том числе о выявленных нарушениях обязательных требований законодательных и нормативных правовых актов Российской Федерации в области защиты персональных данных, об их характере и о лицах, допустивших указанные нарушения.

13. Акт должен содержать заключение о соответствии или несоответствии обработки персональных данных требованиям к защите персональных данных и политике Оператора в отношении обработки персональных данных, установленным Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами.