**Правила**

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

**в отношении обработки персональных данных**

**(утв. Приказом МБОУ лицея №66 г.Липецка от 01.09.2017 №13)**

1. Настоящие Правила определяют основания, форму и порядок осуществления в МБОУ лицее №66 г.Липецка (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 Российской Федерации 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 Российской Федерации от 27.07.2006 №152-ФЗ «О персональных данных», 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 постановлением Правительства №119 (п.17).
5. Внутренний контроль осуществляется путем проведения проверок не реже 1 раз в год.
6. Проверку проводит Комиссия, назначенная приказом директора Организации или на договорной основе юридическое лицо (индивидуальные 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:
	1. 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 Организации определяющих политику в отношении обработки персональных данных;
	2. Провести анализ выполнения Оператором требований по определению и обеспечению уровня защищенности персональных данных, утвержденных постановлением Правительства №1119;
	3. Провести анализ реализации Оператором организационных и технических мер по обеспечению безопасности персональных данных, утвержденных приказом ФСТЭК России от 18.09.2013 №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
	4. Провести анализ состава оборудования, программных средств, включая средства защиты, входящих в состав информационной системы персональных данных на соответствие Техническому паспорту информационной системы.
	5. 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;
	6. При проведении проверки соблюдать законодательство Российской Федерации, права и законные интересы Оператора.
9. Комиссия при проведении проверки вправе:
	1. Запрашивать и получать необходимые документы (сведения) для достижения целей проведения внутреннего контроля;
	2. Получать доступ к информационным системам персональных данных в части касающейся ее полномочий;
	3. Принимать меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований к защите персональных данных;
	4. 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 вправе:
	1. Требовать предоставления документов и сведений, не относящихся к предмету проверки;
	2. Распространять информацию и сведения конфиденциального характера, полученные при проведении проверки.
11. По результатам проверки составляется Акт проверки, который подписывается членами комиссии и предоставляется директору 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 требований к защите персональных данных и политике Оператора в отношении обработки персональных данных, установленным Федеральным законом Российской Федерации от 27.07.2006 №152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами.