

УТВЕРЖДАЮ  
Директор  
Областного бюджетного учреждения  
«Центр социальной защиты населения  
по Елецкому району»

\_\_\_\_\_ Л.Н. Малютина  
«23» декабря 2014 г.

## ПРАВИЛА

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

**1. Настоящие правила определяют основания, форму и порядок осуществления в Областном бюджетном учреждении «Центр социальной защиты населения по Елецкому району» 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» 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» (далее – Федеральный закон № 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 руководителя Областного бюджетного учреждения «Центр социальной защиты населения по Елецкому району» (далее – Организация или Оператор) 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 определяющих 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 руководителю 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 (форма Акта приведена в приложение 1 к настоящим правилам).**

**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 Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами.**

**Лицо, ответственное за организацию  
обработки персональных данных**

\_\_\_\_\_

**Приложение № 1  
к Правилам осуществления внутреннего  
контроля соответствия обработки  
персональных данных требованиям к защите  
персональных данных, политике оператора в  
отношении обработки персональных данных**

**УТВЕРЖДАЮ**  
**Директор**  
**Областного бюджетного учреждения**  
**«Центр социальной защиты населения**  
**по Елецкому району»**

\_\_\_\_\_ 20\_\_ г.

Дата составления: «\_\_\_» \_\_\_\_\_ 20\_\_ г.

Место проведение проверки: \_\_\_\_\_

Комиссия, назначенная приказом руководителя  
от «\_\_\_» \_\_\_\_\_ 20\_\_ № \_\_\_\_\_ в составе:

**Председатель**

\_\_\_\_\_ - \_\_\_\_\_

**Члены комиссии:**

\_\_\_\_\_ - \_\_\_\_\_

\_\_\_\_\_ - **Ответственный за организацию обработки  
персональных данных**

руководствуясь «Правилами осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, политике оператора в отношении обработки персональных данных провела» провела проверку условий обработки персональных данных в Областном бюджетном учреждении «Центр социальной защиты населения по Елецкому району».

В ходе проведения проверки:

- проведен анализ реализации мер, направленных на обеспечение выполнения оператором обязанностей предусмотренных Федеральным законом Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных» (статья 18.1, статья 19) и принятыми в соответствии с ним локальными актами оператора определяющих его политику в отношении обработки персональных данных;

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

- проведен 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»;

- проведен анализ состава оборудования, программных средств, включая средства защиты, входящих в состав информационной системы персональных данных на соответствие Техническому паспорту информационной системы.

Выявленные нарушения: \_\_\_\_\_.

ЗАКЛЮЧЕНИЕ комиссии:

**Обработка персональных данных соответствует / не соответствует требованиям к защите персональных данных и политике оператора в отношении обработки персональных данных, установленным в Федеральном законе Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, а также локальными актами оператора.**

Председатель комиссии \_\_\_\_\_

Члены комиссии: \_\_\_\_\_

\_\_\_\_\_