

1. МУНИЦИПАЛЬНОЕ ОБРАЗОВАНИЕ
2. ХАНТЫ-МАНСИЙСКИЙ РАЙОН
3. Ханты-Мансийский автономный округ – Югра
4. **АДМИНИСТРАЦИЯ ХАНТЫ-МАНСИЙСКОГО РАЙОНА**

**РАСПОРЯЖЕНИЕ**

от 09.12.2016 № 1200-р

*г. Ханты-Мансийск*

Об утверждении порядка проведения

в администрации Ханты-Мансийского

района внутреннего контроля

соответствия обработки

персональных данных требованиям

На основании статей 18.1, 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»:

1. Утвердить порядок проведения в администрации Ханты-Мансийского района внутреннего контроля соответствия обработки персональных данных требованиям (приложение 1).

2. Утвердить форму отчета по результатам проведения внутреннего контроля соответствия обработки персональных данных требованиям (приложение 2).

3. Ответственному за организацию обработки персональных данных (А.С.Скориков) ознакомить всех сотрудников, задействованных в обработке персональных данных, с настоящим распоряжением.

4. Контроль за выполнением распоряжения возложить на первого заместителя главы Ханты-Мансийского района Р.Н.Ерышева.

Глава Ханты-Мансийского района К.Р.Минулин

Приложение 1

к распоряжению администрации

Ханты-Мансийского района

от.09.12.2016 № 1200-р

Порядок проведения внутреннего контроля

соответствия обработки персональных данных требованиям

1. Общие положения

1. Настоящий порядок осуществления внутреннего контроля соответствия обработки персональных данных Федеральному закону от 27.07.2006 № 152-ФЗ «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике оператора в отношении обработки персональных данных, локальным актам оператора определяет 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.

2. Порядок осуществления внутреннего контроля   
соответствия обработки персональных данных требованиям   
к защите персональных данных

2.1. В целях осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных проводятся периодические проверки условий обработки персональных данных.

2.2. Проверки обработки персональных данных проводятся постоянно действующей технической комиссией по защите государственной тайны.

2.3. Проверки условий обработки персональных данных проводятся ежегодно согласно плану мероприятий по защите персональных данных.

Проведение внеплановой проверки организуется в течение трех рабочих дней со дня поступления информации о нарушениях правил обработки персональных данных.

2.4. Проверки условий обработки персональных данных осуществляются непосредственно на месте обработки персональных данных путем опроса либо (при необходимости) путем осмотра служебных мест гражданских служащих и работников, участвующих в процессе обработки персональных данных.

2.5. При проведении проверки условий обработки персональных данных должны быть полностью, объективно и всесторонне установлены:

порядок и условия применения организационных и технических мер, необходимых для выполнения требований к защите персональных данных;

порядок и условия применения средств защиты информации;

эффективность принимаемых мер по обеспечению безопасности персональных данных до их ввода в муниципальные информационные системы персональных данных;

состояние учета носителей персональных данных;

соблюдение правил доступа к персональным данным;

соблюдение порядка доступа в помещения, в которых ведется обработка персональных данных;

наличие (отсутствие) фактов несанкционированного доступа   
к персональным данным и принятие необходимых мер;

мероприятия по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

2.6. Постоянно действующая техническая комиссия по защите государственной тайны имеет право:

2.6.1. Запрашивать у сотрудников информацию, необходимую для реализации полномочий.

2.6.2. Требовать от сотрудников, осуществляющих обработку персональных данных, уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных.

2.6.3. Вносить предложения о:

совершенствовании правового, технического и организационного обеспечения безопасности персональных данных при их обработке;

приостановлении или прекращении обработки персональных данных, осуществляемой с нарушением требований законодательства Российской Федерации;

привлечении к дисциплинарной ответственности лиц, виновных   
в нарушении законодательства Российской Федерации о персональных данных.

2.7. Проверка условий обработки персональных данных должна быть завершена не позднее чем через 30 календарных дней со дня принятия решения об ее проведении.

2.8. По результатам проведенной проверки условий обработки персональных данных составляется отчет по результатам проведения внутреннего контроля соответствия обработки персональных данных требованиям с указанием мер, необходимых для устранения выявленных нарушений.

Приложение 2

к распоряжению администрации

Ханты-Мансийского района

от 09.12.2016 № 1200-р

Форма отчета

по результатам проведения внутреннего контроля соответствия обработки персональных данных требованиям

Настоящий отчет составлен в том, что с \_\_.\_\_.20\_\_ по \_\_.\_\_.20\_\_ постоянно действующей технической комиссией по защите государственной тайны был проведен внутренний контроль соответствия обработки персональных данных Федеральному закону от 27.07.2006 № 152-ФЗ «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике оператора в отношении обработки персональных данных, локальным актам оператора.

Проверка осуществлялась в соответствии с требованиями следующих нормативных правовых актов:

Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;

Указ Президента Российской Федерации от 17.03.2008 № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»;

Стратегия развития информационного общества в Российской Федерации, утвержденная Президентом Российской Федерации 07.02.2008 № Пр-212;

постановление Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными и муниципальными органами»;

постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

приказ Федеральной службы по техническому и экспортному контролю (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»;

нормативный документ ФСТЭК России «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденный 15.02.2008 заместителем директора ФСТЭК России;

нормативный документ ФСТЭК России «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденный 14.02.2008 заместителем директора ФСТЭК России;

Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации, утвержденные руководством 8 Центра ФСБ России 21.02.2008.

В ходе проверки проверено:

1. Правильность заполнения следующих журналов по информационной безопасности.

2. Актуальность и фактическое соответствие процессов обработки и защиты персональных данных требованиям, описанным в комплекте организационно-распорядительной документации.

3. Проверка знаний работников в области обработки и защиты персональных данных.

4. Проверка настроек средств защиты информации, в том числе криптографических, а также анализ журналов безопасности таких средств.

Выявленные нарушения:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

Меры по устранению нарушений:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

Срок устранения нарушений: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

|  |  |
| --- | --- |
| Председатель комиссии:  Члены комиссии: | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_