Приложение 5

УТВЕРЖДЕНЫ

распоряжением администрации

муниципального образования

Ленинградский муниципальный округ Краснодарского края

от 15.07.2025 г. № 370-р

**Правила
осуществления внутреннего контроля соответствия обработки**

**информации ограниченного доступа требованиям**

 **к защите информации**

**1. Общие положения**

1.1. Настоящие Правила осуществления внутреннего контроля соответствия обработки информации ограниченного доступа требованиям к защите информации (далее - Правила) в администрации определяют процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в области обработки информации ограниченного доступа, в том числе персональных данных (далее - ИОД, ПДн, соответственно), основания, порядок, формы и методы проведения внутреннего контроля соответствия обработки ИОД требованиям к защите информации.

1.2. Настоящие Правила разработаны на основании Федеральных законов от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и в соответствии с частью 1 «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 или муниципальными органами», утвержденных постановлением Правительства Российской Федерации от 21 марта 2012 г. № 211.

1.3. Администрация использует информационные системы, предназначенные для обработки ИОД (далее - ИС) в целях реализации возложенных на администрацию задач, исполнения функций и полномочий администрации.

1.4. Администрация использует информационные системы персональных данных (далее - ИСПДн) для выполнения основных целей и задач обработки ПДн.

1.5. Пользователями ИС (далее - Пользователь) являются сотрудники администрации, участвующие в рамках выполнения своих функциональных обязанностей в процессах автоматизированной обработки ИОД и имеющие доступ к аппаратным средствам, ПО, данным и средствам защиты информации (далее - СЗИ) ИС.

1.6. В целях реализации возложенных на администрацию задач, исполнение функций и полномочий администрации отдельные функции обработки ИОД могут осуществляться сотрудниками подведомственных администрации учреждений, с учетом требований законодательства Российской Федерации. В данном случае права, обязанности и ответственность указанных сотрудников, связанные с обработкой ИОД и описанные в настоящих Правилах соответствуют правам, обязанностям и ответственности сотрудников администрации.

1.7. Контрольные мероприятия по обеспечению безопасности ИОД, требуемого уровня защищенности ПДн и соблюдению условий использования СЗИ, а также соблюдению требований законодательства Российской Федерации по защите ИОД, обработке и защите ПДн в ИС администрации (далее - контрольные мероприятия) проводятся в следующих целях:

проверка выполнения требований организационно-распорядительной документации по защите информации в администрации и законодательства Российской Федерации в области защиты информации, защиты и обработки ПДн;

оценка уровня осведомленности и знаний сотрудников администрации в области защиты информации, защиты и обработки ПДн;

оценка обоснованности и эффективности применяемых мер и средств защиты ИОД.

**2. Тематика внутреннего контроля соответствия обработки**

**ИОД требованиям к защите информации**

2.1. В администрации проводятся контрольные мероприятия следующих видов:

регулярные;

плановые;

внеплановые.

2.2. Регулярные контрольные мероприятия периодически проводятся в ИС (ИСПДн) администрации администраторами ИС (ИСПДн) и предназначены для осуществления контроля выполнения требований в области защиты ИОД в администрации.

2.3. Плановые контрольные мероприятия периодически проводятся Комиссией по проведению внутреннего контроля соответствия обработки персональных данных требованиям законодательства Российской Федерации администрации (далее - Комиссия), состав которой утверждается правовым актом администрации, не реже одного раза в год и направлены на постоянное совершенствование системы защиты информации в администрации.

2.4. Внеплановые контрольные мероприятия проводятся на основании решения должностного лица, ответственного за защиту информации в администрации, созданной для проведения мероприятий комиссией (создается на период проведения мероприятий). Решение о проведении внеплановых контрольных мероприятий может быть принято в следующих случаях:

по результатам расследования инцидента информационной безопасности;

по результатам внешних контрольных мероприятий, проводимых регулирующими органами в целях устранения выявленных замечаний;

в иных случаях по решению должностного лица, ответственного за защиту информации в администрации.

**3. Планирование контрольных мероприятий**

3.1. Для проведения плановых контрольных мероприятий должностное лицо, ответственное за выполнение работ по защите информации в администрации, утверждает план проведения внутреннего контроля условий обработки персональных данных (иной информации ограниченного доступа) в администрации на текущий год, форма которого утверждается правовым актом администрации.

3.2. Плановые контрольные мероприятия в отношении ИОД, не содержащей ПДн, проводятся совместно с Контрольными мероприятиями в отношении ПДн.

3.3. Плановые контрольные мероприятия осуществляются Комиссией в соответствии с программой (порядком) проведения внутреннего контроля соответствия обработки ПДн требованиям законодательства Российской Федерации, утверждаемой правовым актом администрации.

**4. Порядок проведения плановых и внеплановых**

**контрольных мероприятий**

4.1. При проведении плановых и внеплановых контрольных мероприятий Комиссия руководствуется Положением о комиссии по проведению внутреннего контроля соответствия обработки ПДн требованиям законодательства Российской Федерации, утверждаемым правовым актом администрации.

4.2. Плановые и внеплановые Контрольные мероприятия проводятся Комиссией при участии лица, ответственного за обеспечение информационной безопасности в администрации. Также по его ходатайству к проведению контрольных мероприятий могут привлекаться администраторы ИС и лица, ответственные за эксплуатацию ИС либо за обеспечение безопасности информации в ИС.

4.3. При необходимости к проведению контрольных мероприятий могут привлекаться представители организаций, подведомственных администрации, при условии соблюдения требований законодательства Российской Федерации.

**5. Оформление результатов контрольных мероприятий**

5.1. По итогам проведения регулярных контрольных мероприятий выявленные инциденты и нарушения (при их наличии) фиксируются в журнале учета событий информационной безопасности (приложение 14 к распоряжению).

5.2. По итогам проведения плановых и внеплановых контрольных мероприятий оформляется акт проведения контроля, форма которого утверждается правовым актом администрации.

5.3. При наличии выявленных нарушений процесса обработки ПДн (ИОД) по результатам плановых и внеплановых контрольных мероприятий оформляется план мероприятий по устранению выявленных нарушений, форма которого утверждается правовым актом администрации.

5.4. Оформленные по результатам проведения плановых и внеплановых контрольных мероприятий акт проведения контроля и план мероприятий по устранению выявленных нарушений подписываются членами комиссии и утверждаются ее председателем.

5.5. Результаты проведения плановых и внеплановых контрольных мероприятий доводятся до главы Ленинградского муниципального округа.

Управляющий делами

администрации Ленинградского

муниципального округа А.Л. Мазуров