Приложение 13

УТВЕРЖДЕНА

распоряжением администрации

муниципального образования

Ленинградский муниципальный округ Краснодарского края

от 15.07.2025 г. № 370-р

**Инструкция
пользователя по обеспечению безопасности обработки**

**персональных данных при возникновении**

**внештатных ситуаций**

**1. Назначение и область действия**

Настоящая Инструкция определяет возможные аварийные ситуации, связанные с функционированием ИСПДн в администрации, меры и средства поддержания непрерывности работы и восстановления работоспособности ИСПДн после аварийных ситуаций.

Целью настоящего документа является превентивная защита элементов ИСПДн от прерывания в случае реализации рассматриваемых угроз.

Задачей данной Инструкции является:

определение мер защиты от прерывания;

определение действий восстановления в случае прерывания.

Действие настоящей Инструкции распространяется на всех сотрудников администрации, имеющих доступ к ресурсам ИСПДн.

**2. Порядок реагирования на аварийную ситуацию**

**2.1. Действия при возникновении аварийной ситуации**

В настоящем документе под аварийной ситуацией понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИСПДн, предоставляемых пользователям ИСПДн.

В кратчайшие сроки, не превышающие одного рабочего дня, ответственные за реагирование сотрудники администрации предпринимают меры по восстановлению работоспособности. Предпринимаемые меры по возможности согласуются с руководителями структурных подразделений. По необходимости, иерархия может быть нарушена, с целью получения высококвалифицированной консультации в кратчайшие сроки.

**2.2. Уровни реагирования на инцидент**

При реагировании на инцидент важно, чтобы пользователь правильно классифицировал критичность инцидента. Критичность оценивается на основе следующей классификации:

Уровень 1 - незначительный инцидент. Незначительный инцидент определяется как локальное событие с ограниченным разрушением, которое не влияет на общую доступность элементов ИСПДн и средств защиты. Эти инциденты решаются ответственными за реагирование сотрудниками.

Уровень 2 - авария. Любой инцидент, который приводит или может привести к прерыванию работоспособности отдельных элементов ИСПДн и средств защиты. Эти инциденты выходят за рамки управления ответственными за реагирование сотрудниками.

Уровень 3 - катастрофа. Любой инцидент, приводящий к полному прерыванию работоспособности всех элементов ИСПДн и средств защиты, классифицируется как катастрофа. Обычно к катастрофам относят обстоятельства непреодолимой силы (пожар, взрыв), которые могут привести к прерыванию работоспособности ИСПДн и средств защиты на сутки и более.

**3. Меры обеспечения непрерывности работы и восстановления**

**ресурсов при возникновении аварийных ситуаций**

**3.1. Технические меры**

К техническим мерам обеспечения непрерывной работы и восстановления относятся программные, аппаратные и технические средства и системы, используемые для предотвращения возникновения аварийных ситуаций, такие как:

системы обеспечения отказоустойчивости;

системы резервного копирования и хранения данных;

системы контроля физического доступа.

Системы жизнеобеспечения ИСПДн включают:

пожарные сигнализации и системы пожаротушения;

системы вентиляции и кондиционирования;

системы резервного питания.

Все помещения, в которых размещаются элементы ИСПДн и средства защиты администрации должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

**3.2. Организационные меры**

Ответственные за реагирование сотрудники ознакомляют всех сотрудников администрации, находящихся в их зоне ответственности, с данной инструкцией в срок, не превышающий 3 рабочих дней с момента выхода нового сотрудника на работу.

Должно быть проведено обучение должностных лиц администрации, имеющих доступ к ресурсам ИСПДн, порядку действий при возникновении аварийных ситуаций.

Администраторы ИСПДн и администраторы безопасности должны быть дополнительно обучены методам частичного и полного восстановления работоспособности элементов ИСПДн.

Навыки и знания должностных лиц по реагированию на аварийные ситуации должны регулярно проверяться. При необходимости должно проводиться дополнительное обучение должностных лиц порядку действий при возникновении аварийной ситуации.

**4. Действия в случае возникновения ситуаций,**

**которые могут повлечь неправомерную передачу**

**(предоставление, распространение, доступ)**

**персональных данных**

В случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) ПДн, повлекшей нарушение прав субъектов ПДн, администрация обязана с момента выявления такого инцидента уведомить Роскомнадзор:

в течение двадцати четырех часов - о произошедшем инциденте, о предполагаемых причинах, повлекших нарушение прав субъектов ПДн, и предполагаемом вреде, нанесенном правам субъектов ПДн, о принятых мерах по устранению последствий соответствующего инцидента, а также предоставить сведения об уполномоченном должностном лице администрации на взаимодействие с Роскомнадзором, по вопросам, связанным с выявленным инцидентом;

в течение семидесяти двух часов - о результатах внутреннего расследования выявленного инцидента, а также предоставить сведения о лицах, действия которых стали причиной выявленного инцидента (при наличии).

Управляющий делами

администрации Ленинградского

муниципального округа А.Л. Мазуров