|  |
| --- |
| Приложение № 25к постановлениюглавы Администрации сельского поселения Октябрьский сельсовет муниципального района Стерлитамакский район Республики Башкортостан от 07.08. 2018 г. №77 |
|  |
|  |
|  |
|  |

**Инструкция по действиям персонала во внештатных**

 **ситуациях при обработке конфиденциальной информации**

**и персональных данных**

1. **Общие положения**

Данная инструкция призвана регламентировать порядок действий пользователя информационной системы персональных данных Администрации сельского поселения Октябрьский сельсовет муниципального района Стерлитамакский район Республики Башкортостан (далее в Учреждении) при возникновении внештатных ситуаций.

Инструкция утверждается руководителем учреждения. Настоящая Инструкция определяет возможные аварийные ситуации, связанные с функционированием ИСПДн Учреждения, 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 и определение действий восстановления в случае прерывания.

Действие настоящей Инструкции распространяется на всех сотрудников Учреждения, имеющих доступ к ресурсам ИСПДн, а также основные системы обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций, в том числе:

* системы жизнеобеспечения;
* системы обеспечения отказоустойчивости;
* [системы резервного копирования и хранения данных](file://C:\Users\Регина\Google%20Диск\Отдел%20защиты%20информации\АКТИВНЫЕ%20ПРОЕКТЫ\Администрация%20гор.округа%20Дюртюли\НА%20ПРОВЕРКУ\Городской%20округ%20Дюртюли_Final\ОРД\Постановление+приложения\Приложение%2013%20Порядок%20резервирования%20и%20восстановления%20работоспособности%20ТС%20и%20ПО,%20баз%20данных%20и%20СЗИ.doc);
* системы контроля физического доступа.

Пересмотр настоящего документа осуществляется по мере необходимости, но не реже одного одного раза в два года.

1. **Порядок действий при возникновении аварийной ситуации**

В настоящем документе под аварийной ситуацией понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИСПДн, предоставляемых пользователям ИСПДн. Аварийная ситуация становится возможной в результате реализации одной из угроз, приведенных в «Модели угроз».

Все действия в процессе реагирования на аварийные ситуации должны документироваться ответственным за реагирование сотрудником в «Журнал учета нештатных ситуаций, фактов вскрытия и опечатывания ПЭВМ, выполнения профилактических работ, установки и модификации аппаратных и программных средств информационной системы персональных данных» (Приложение 25 к Постановлению «Об утверждении перечня мер , направленных на обеспечение выполнения обязанностей, предусмотренных федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами»).

В кратчайшие сроки, не превышающие одного рабочего дня, ответственный за обеспечение информационной безопасности, администратор баз данных или другой назначенный ответственным за реагирование сотрудник предпринимает меры по восстановлению работоспособности. Предпринимаемые меры по возможности согласуются с вышестоящим руководством. При необходимости привлекаются квалифицированные сотрудники сторонних организаций с целью восстановления работоспособности в кратчайшие сроки.

**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.

К авариям относятся следующие инциденты:

Отказ элементов ИСПДн и средств защиты из-за:

* повреждения водой (прорыв системы водоснабжения, канализационных труб, систем охлаждения), а также подтопления в период паводка или проливных дождей;
* сбоя системы кондиционирования;
* других физических повреждений элементов ИСПДн, критичных для функционирования всей ИСПДн.

Уровень 3 – **Катастрофа**. Любой инцидент, приводящий к полному прерыванию работоспособности всех элементов ИСПДн и средств защиты, а также к угрозе жизни пользователей ИСПДн, классифицируется как катастрофа.

К катастрофам относятся следующие инциденты:

* пожар в здании;
* взрыв;
* просадка грунта с частичным обрушением здания;
* массовые беспорядки в непосредственной близости от Объекта.
1. **Меры обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций**
	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 жизнеобеспечения;
* 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 критичные помещения Учреждения (помещения, в которых размещаются элементы ИСПДн и средства защиты) должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

Порядок предотвращения потерь информации и организации системы жизнеобеспечения ИСПДн описан в «Порядке резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации».

* 1. Организационные меры

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

Должно быть проведено обучение сотрудников Учреждения, имеющих доступ к ресурсам ИСПДн, порядку действий при возникновении аварийных ситуаций.

Сотрудники, ответственные за обеспечение безопасности ИСПДн должны быть дополнительно обучены методам частичного и полного восстановления работоспособности элементов ИСПДн.

Ответственность за организацию обучения должностных лиц несет должностное лицо, ответственное за обеспечение безопасности ИСПДн.

|  |
| --- |
| **Приложение № 1**к Инструкции по действиям персонала во внештатных ситуациях при обработке конфиденциальной информации и персональных данных, утв. Приказомот 07.08.2018 г. № 77 |

**Журнал учета нештатных ситуаций, фактов вскрытия и опечатывания ПЭВМ, выполнения профилактических работ, установки и модификации аппаратных и программных средств**

**информационной системы персональных данных**

|  |  |
| --- | --- |
| Начат: |  |
| Окончен: |  |
| Количество листов: |  |
| Срок хранения: | 5 лет |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **N п/п** | **Дата** | **Краткое описание выполненной работы (нештатной ситуации)** | **ФИО и подпись пользователя** | **ФИО и подпись ответственного за обеспечение безопасности персональных данных** | **Примечание (ссылка на заявку)** |
| 1 | 2 | 3 | 4 | 5 | 7 |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |