«Утверждаю»

Глава администрации

Трубчевского муниципального района

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_И.И. Обыдённов

«12 » апреля 2016г.

ИНСТРУКЦИЯ № 15/ИБ

при возникновении чрезвычайных ситуаций в информационных системах персональных данных (ИСПДн)

администрации Трубчевского муниципального района

1.     Общие положения

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

Задачей данной Инструкции является:

-       определение мер защиты от прерывания работоспособности;

-       определение действий восстановления в случае прерывания.

Действие настоящей Инструкции распространяется на всех пользователей, 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;

-       системы контроля физического доступа.

Пересмотр настоящего документа осуществляется по мере необходимости.

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 ниже:

-       технологические угрозы (пожар в здании, повреждение водой, взрыв, химический выброс в атмосферу);

-       внешние угрозы (массовые беспорядки, сбои общественного транспорта, эпидемия, массовое отравление персонала);

-       стихийные бедствия (удар молнии, сильный снегопад, сильные морозы, просадка грунта с частичным обрушением здания, затопление водой в период паводка, наводнение, вызванное проливным дождем, торнадо);

-       телекоммуникационные и информационно-технические угрозы (сбой системы кондиционирования, сбой ИТ – систем);

-       угроза, связанная с человеческим фактором (ошибка персонала, имеющего доступ к серверной, нарушение конфиденциальности, целостности и доступности конфиденциальной информации);

-       угрозы, связанные с внешними поставщиками (отключение электроэнергии, сбой в работе интернет-провайдера, физический разрыв внешних каналов связи).

-       Все действия в процессе реагирования на аварийные ситуации, возникающие в ИСПДн, должны документироваться администратором безопасности.

В кратчайшие сроки, не превышающие одного рабочего дня, ответственные за реагирование сотрудники (Администратор и пользователи ИСПДн) предпринимают меры по восстановлению работоспособности. Предпринимаемые меры по возможности согласуются с вышестоящим руководством. По необходимости, иерархия может быть нарушена, с целью получения высококвалифицированной консультации в кратчайшие сроки.

2.     Уровни реагирования на инцидент

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

**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 пользователями и администратором безопасности ИСПДн.

Сбой программного обеспечения. Администратор безопасности выясняет причину сбоя программного обеспечения (далее – ПО). Если исправить ошибку своими силами (в том числе после консультации с разработчиками ПО) не удалось, копия акта и сопроводительных материалов (а также файлов, если это необходимо) направляются разработчику ПО.

Отключение электричества. Администратор безопасности проводит анализ на наличие потерь и (или) разрушения данных и ПО, а так же проверяет работоспособность оборудования. В случае необходимости, производится восстановление ПО и данных из последней резервной копии с составлением акта.

Потеря данных. При обнаружении потери данных администратор безопасности проводит мероприятия по поиску и устранению причин потери данных (антивирусная проверка, целостность и работоспособность ПО, целостность и работоспособность оборудования и др.). При необходимости, производится восстановление ПО и данных из резервных копий с составлением акта.

Обнаружена утечка информации (уязвимость в системе защиты). При обнаружении утечки информации ставится в известность администратор безопасности и начальник подразделения. Проводится служебное расследование. Если утечка информации произошла по техническим причинам, проводится анализ защищённости системы и, если необходимо, принимаются меры по устранению уязвимостей и предотвращению их возникновения.

Физическое повреждение ПЭВМ. Ставится в известность администратор безопасности. Проводится анализ на утечку или повреждение информации. Определяется причина повреждения ПЭВМ и возможные угрозы безопасности информации. В случае возникновения подозрения на целенаправленный вывод оборудования из строя проводится служебное расследование. Проводится проверка ПО на наличие вредоносных программ-закладок, целостность ПО и данных. Проводится анализ электронных журналов. При необходимости проводятся меры по восстановлению ПО и данных из резервных копий с составлением акта.

**2) Авария.** Любой инцидент, который приводит или может привести к прерыванию работоспособности отдельных элементов ИСПДн и средств защиты. Эти инциденты решаются администратором безопасности совместно с руководством.К авариям относятся следующие инциденты:

-       отказ элементов ИСПДн и средств защиты из-за повреждения водой, сбоя системы кондиционирования;

-       отсутствие администратора безопасности более чем на сутки из-за химического выброса в атмосферу, сбоев общественного транспорта, эпидемии, массового отравления персонала, сильного снегопада, торнадо, сильных морозов.

**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. Обычно к катастрофам относят обстоятельства непреодолимой силы (пожар, взрыв), которые могут привести к неработоспособности ИСПДн и средств защиты на сутки и более.

К катастрофам относятся следующие инциденты:

-       пожар в здании;

-       взрыв;

-       просадка грунта с частичным обрушением здания;

-       массовые беспорядки.

3. Меры обеспечения непрерывности работы и восстановления

ресурсов при возникновении аварийных ситуаций

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.

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

Администратор безопасности ознакомляет всех пользователей, находящихся в его зоне ответственности, с данной инструкцией в срок, не превышающий 3-х рабочих дней с момента выхода нового сотрудника на работу.

Должно быть проведено обучение сотрудников, имеющих доступ к ресурсам ИСПДн, порядку действий при возникновении аварийных ситуаций. Должностные лица должны получить базовые знания в следующих областях:

-       оказание первой медицинской помощи;

-       пожаротушение;

-       эвакуация людей;

-       защита материальных и информационных ресурсов;

-       методы оперативной связи со службами спасения и лицами, ответственными  за реагирование сотрудниками на аварийную ситуацию;

-       выключение оборудования, электричества, водоснабжения, газоснабжения.

Администратор безопасности ИСПДндолжен быть дополнительно обучен 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. Сроки и порядок их обучения согласуется с Администратором безопасности.