Утверждено приказом
Директора МБУК «Ряжский РДК»
№ 40/4 от 29.12. 2017 года

ИНСТРУКЦИЯ № 2

пользователя информационной системы персональных данных Муниципального бюджетного учреждения культуры «Ряжский районный Дом культуры» (МБУК «Ряжский РДК»)
по обеспечению безопасности обработки персональных данных при возникновении внештатных ситуаций

2017 год

1. Назначение и область действия

1.1. Настоящая Инструкция определяет возможные аварийные ситуации, связанные с функционированием ИСПДн МБУК «Ряжский РДК», меры и средства поддержания непрерывности работы и восстановления работоспособности ИСПДн после аварийных ситуаций.

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

1.3. Задачей данной Инструкции является:

1.3.1. определение мер защиты от прерывания;

1.3.2. определение действий восстановления в случае прерывания.

1.4. Действие настоящей Инструкции распространяется на всех пользователей МБУК «Ряжский РДК», имеющих доступ к ресурсам ИСПДн, а также основные системы обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций, в том числе:

1.4.1. системы обеспечения отказоустойчивости;

1.4.2. системы резервного копирования и хранения данных;

1.4.3. системы контроля физического доступа.

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

2. Порядок реагирования на аварийную ситуации

1.6. Действия при возникновении аварийной ситуации

1.6.1. 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 Приложении1.

1.6.2. Все действия в процессе реагирования на аварийные ситуации должны документироваться ответственным за реагирование сотрудником в «Журнале по учету мероприятий по контролю».

1.6.3. В кратчайшие сроки, не превышающие одного рабочего дня, ответственные за реагирование сотрудники МБУК «Ряжский РДК», (Ответственный за эксплуатацию объекта информатизации и Администратора безопасности информации) 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.

1.7. Уровни реагирования на инцидент

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

1.7.2. 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.

1.7.3. 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.

1.8. К авариям относятся следующие инциденты:

1.8.1. Отказ элементов ИСПДн и средств защиты из-за:

1.8.1.1. повреждения водой (прорыв системы водоснабжения, канализационных труб, систем охлаждения), а также подтопления в период паводка или проливных дождей;

1.8.1.2. сбоя системы кондиционирования.

1.9. Отсутствие Ответственного за эксплуатацию объекта информатизации и Администратора безопасности информации более чем на сутки из-за:

1.9.1. химического выброса в атмосферу;

1.9.1.1. сбоев общественного транспорта;

1.9.1.2. эпидемии;

1.9.1.3. массового отравления персонала;

1.9.1.4. сильного снегопада;

1.9.1.5. торнадо;

1.9.1.6. сильных морозов.

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

1.11. К катастрофам относятся следующие инциденты:

1.11.1. пожар в здании;

1.11.2. взрыв;

1.11.3. просадка грунта с частичным обрушением здания;

1.11.4. массовые беспорядки в непосредственной близости от Объекта.

3. Меры обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций

1.12. Технические меры

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

1.12.1.1. системы обеспечения отказоустойчивости;

1.12.1.2. системы резервного копирования и хранения данных;

1.12.1.3. системы контроля физического доступа.

1.12.2. Все критичные помещения МБУК «Ряжский РДК», (помещения, в которых размещаются элементы ИСПДн и средства защиты) должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

1.12.3. Порядок предотвращения потерь информации ИСПДн описан в инструкции по резервированию и восстановлению персональных данных.

1.13. Организационные меры

1.13.1. Должно быть проведено обучение должностных лиц МБУК «Ряжский РДК», имеющих доступ к ресурсам ИСПДн, порядку действий при возникновении аварийных ситуаций. Должностные лица должны получить базовые знания в следующих областях:

1.13.1.1. оказание первой медицинской помощи;

1.13.1.2. пожаротушение;

1.13.1.3. эвакуация людей;

1.13.1.4. защита материальных и информационных ресурсов;

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

1.13.1.6. выключение оборудования, электричества, водоснабжения, газоснабжения.

1.13.2. Ответственный за эксплуатацию объекта информатизации и Администратор безопасности информации должны быть обучены методам частичного и полного восстановления работоспособности элементов ИСПДн.

1.13.3. 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.

Разработал:

Ответственный за организацию обработки
персональных данных
МБУК «Ряжский РДК» _____ /О.Н. Шмелькова/

Приложение 1

Источники угроз

Технологические угрозы	
1	Пожар в здании
2	Повреждение водой (прорыв системы водоснабжения, канализационных труб, систем охлаждения)
3	Взрыв (бытовой газ, теракт, взрывчатые вещества или приборы, работающие под давлением)
4	Химический выброс в атмосферу
Внешние угрозы	
5	Массовые беспорядки
6	Сбои общественного транспорта
7	Эпидемия
8	Массовое отравление персонала
Стихийные бедствия	
9	Удар молнии
10	Сильный снегопад
11	Сильные морозы
12	Просадка грунта (подмыв грунтовых вод, подземные работы) с частичным обрушением здания
13	Затопление водой в период паводка
14	Наводнение, вызванное проливным дождем
15	Торнадо
16	Подтопление здания (воздействие подпочвенных вод, вызванное внезапным и непредвиденным повышением уровня грунтовых вод)
Телеком и ИТ угрозы	
17	Сбой системы кондиционирования
18	Сбой ИТ – систем
Угроза, связанная с человеческим фактором	
19	Ошибка персонала, имеющего доступ к серверной
20	Нарушение конфиденциальности, целостности и доступности конфиденциальной информации
Угрозы, связанные с внешними поставщиками	
21	Отключение электроэнергии
22	Сбой в работе интернет-провайдера
23	Физически разрыв внешних каналов связи