Государственное казенное учреждение для детей-сирот и детей, оставшихся без попечения родителей «Митинский детский дом»
(ГКУ «Митинский детский дом»)

УТВЕРЖДАЮ
Директор Е.Е. Десяткина
Приказ № 24 от «03» марта 2020г.

Инструкция пользователя информационной системы персональных данных при возникновении нештатных ситуаций

1. Настоящая Инструкция определяет возможные аварийные ситуации, связанные с функционированием информационных систем персональных данных ГКУ "Митинский детский дом" (далее – ИСПДн), меры и средства поддержания непрерывности работы и восстановления работоспособности ИСПДн после аварийных ситуаций.
2. Целью настоящего документа является превентивная защита элементов ИСПДн от прерывания работоспособности в случае реализации рассматриваемых угроз.
3. Задачами данной Инструкции являются:
— определение мер защиты от прерывания работоспособности;
— определение действий по восстановлению в случае прерывания работоспособности.
4. Действие настоящей Инструкции распространяется на всех пользователей ИСПДн, имеющих доступ к ресурсам ИСПДн, а также на 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.
5. Под аварийной ситуацией понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИСПДн. Аварийная ситуация становится возможной в результате реализации одной из угроз, приведенных в Приложении № 1.
6. При реагировании на инцидент важно, чтобы пользователь правильно классифицировал критичность инцидента.

Критичность оценивается на основе следующей классификации:
— Уровень 1. Незначительный инцидент – локальное событие с ограниченным разрушением, которое не влияет на общую доступность элементов ИСПДн и

средств защиты;
— Уровень 2. Авария – любой инцидент, который приводит или может привести к прерыванию работоспособности отдельных элементов ИСПДн и средств защиты;
— Уровень 3. Катастрофа – любой инцидент, приводящий к полному прерыванию работоспособности всех элементов ИСПДн и средств защиты, к уничтожению, блокированию, неправомерной модификации или компрометации защищаемых
персональных данных, а также к угрозе жизни пользователей ИСПДн.
7. При возникновении нештатной ситуации любого уровня пользователь обязан оповестить директора, сообщив характер аварийной ситуации, масштаб ситуации по предварительной субъективной оценке.
8. К техническим мерам обеспечения непрерывной работы и восстановления относятся программные, аппаратные (программно-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;
— системы резервного питания.
Все критичные помещения, в которых размещаются элементы ИСПДн и средства защиты, должны быть оборудованы средствами пожарной сигнализации.
9. Директор/заместитель директора:
— ознакомляет всех сотрудников с данной инструкцией в срок, не превышающий 3х рабочих дней с момента выхода нового сотрудника на работу;
— обучает пользователей, имеющих доступ к ресурсам ИСПДн, порядку действий при возникновении аварийных ситуаций.
Пользователи ИСПДн 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 непосредственными руководителями;
— выключение оборудования, электричества, водоснабжения;
— по окончанию ознакомления сотрудников получает их роспись в Журнале учета прохождения первичного инструктажа.
11. Навыки и знания пользователей ИСПДн по реагированию на аварийные

ситуации должны регулярно проверяться. При необходимости должно проводиться дополнительное обучение пользователей ИСПДн порядку действий при возникновении аварийной ситуации. Ответственность за организацию обучения пользователей ИСПДн несет ответственный за организацию обработки персональных данных.

Приложение 1
к Инструкции пользователя ИСПДн
при возникновении нештатной ситуации

Источники угроз безопасности персональных данных

Технологические угрозы:
— Пожар в здании;
— Повреждение водой (прорыв системы водоснабжения, канализационных труб, систем отопления);
Внешние угрозы:
— Массовые беспорядки;
— Теракт.
Стихийные бедствия:
— Удар молнии;
— Сильный снегопад;
— Сильные морозы;
— Просадка грунта (подмыв грунтовых вод, подземные работы) с частичным обрушением здания.
ИТ-угрозы:
— Выход из строя файлового сервера ;
— Частичная потеря информации на сервере без потери его работоспособности;
— Выход из строя локальной сети;
— Выход из строя рабочей станции;
— Частичная потеря информации на рабочей станции без потери её работоспособности.
Угроза, связанная с человеческим фактором:
— Ошибка персонала, имеющего доступ к элементам ИСПДн;
— Нарушение конфиденциальности, целостности и доступности конфиденциальной информации, а также несанкционированные действия, заблокированные средствами защиты и зафиксированные средствами регистрации.
Угрозы, связанные с внешними поставщиками:
— Отключение электроэнергии;
— Сбой в работе интернет-провайдера;
— Физический разрыв внешних каналов связи.