Государственное казенное учреждение здравоохранения
Детский санаторий «ТОПОЛЁК»
Министерства Здравоохранения Краснодарского края

УТВЕРЖДАЮ
Главный врач
ГКУЗ «Детский санаторий «Тополек»
_____ / М. А. Мугу /
«__» ___12___ 2021 г.

государственное казенное учреждение здравоохранения "Детский санаторий "Тополек" министерства здравоохранения Краснодарского края
ОГРН 1032307156936 ИНН 2312102097

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 информационных системах персональных данных ГКУЗ «Детский санаторий «Тополек», меры и средства поддержания непрерывности работы и восстановления работоспособности Информационных систем персональных данных после аварийных ситуаций.

Целью настоящего документа является превентивная защита элементов информационных систем персональных данных (далее – 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 пользователей-сотрудников ГКУЗ «Детский санаторий «Тополек», 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, но не реже одного раза в два года.

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. Аварийная ситуация возможна в результате реализации одной из угроз, приведенных в Приложении 1.

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

В кратчайшие сроки, не превышающие одного рабочего дня, ответственные за реагирование сотрудники ГКУЗ «Детский санаторий «Тополек» (Администратор безопасности, Администратор и пользователь 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.

2.2 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 ИСПДНи 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.

- 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 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 в непосредственной близости от здания.

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 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 (помещения, в которых размещаются элементы ИСПДНи средства защиты) должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

Порядок предотвращения потерь информации и организации системы жизнеобеспечения ИСПДН описан в инструкцию по организации резервного копирования, восстановления работоспособности технических средств, программного обеспечения и средств защиты информации в информационных системах персональных данных.

3.2 Организационные меры

Ответственные за реагирование сотрудники ознакомляют всех, 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 должностных лиц, 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.

Ответственность за организацию обучения должностных лиц несет Администратор безопасности.

Приложение к инструкции по организации резервного копирования, восстановления инструкций пользователя по обеспечению безопасности обработки персональных данных, при возникновении внештатных ситуаций работоспособности технических средств, программного обеспечения и средств защиты информации в информационных системах персональных данных №1

Источники угроз

Таблица 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