УТВЕРЖДАЮ

Главный врач
_____Санчы И.Д.
от «10» января 2023 г.

Инструкция

по действиям персонала во внештатных ситуациях при обработке защищаемой информации в информационных системах Государственного бюджетного учреждения здравоохранения Республики Тыва «Республиканский Центр по профилактике и борьбе со СПИД и инфекционными заболеваниями» (Республиканский Центр СПИД)

г. Кызыл

2023 год

1. Назначение и область действия

1.1. Настоящая Инструкция определяет возможные аварийные ситуации, связанные с функционированием информационных систем (ИС) Республиканского Центра СПИД, меры и средства поддержания непрерывности работы и восстановления работоспособности ИС Республиканского Центра СПИД после аварийных ситуаций.

1.2. Целью настоящего документа является превентивная защита элементов ИС Республиканского Центра СПИД от прерывания в случае реализации рассматриваемых угроз.

1.3. Задачей данной Инструкции является:

- определение мер защиты от прерывания;
- определение действий восстановления в случае прерывания.

1.4. Действие настоящей Инструкции распространяется на всех сотрудников Республиканского Центра СПИД, имеющих доступ к ресурсам ИС Республиканского Центра СПИД, а также к основным системам обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций, в том числе:

- система жизнеобеспечения;
- система обеспечения отказоустойчивости;
- система резервного копирования и хранения данных;
- система контроля физического доступа.

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

2. Порядок реагирования на аварийную ситуацию

2.1. В настоящем документе под аварийной ситуацией (инцидентом) понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИС Республиканского Центра СПИД, предоставляемых пользователям ИС. Аварийная ситуация становится возможной в результате реализации одной из угроз, приведенных в Приложении 1 к настоящей инструкции - «Источники угроз».

2.2. Все действия в процессе реагирования на аварийные ситуации должны документироваться ответственным за реагирование сотрудником в журнале учета мероприятий по контролю обработки и защиты в информационных системах Республиканского Центра СПИД.

2.3. Инцидент может возникнуть в результате преднамеренных действий злоумышленника или непреднамеренных действий пользователей, аварий, стихийных бедствий.

2.4. В кратчайшие сроки, не превышающие одного рабочего дня, ответственные за реагирование сотрудники Республиканского Центра СПИД (администратор информационной безопасности, ответственный за обеспечение безопасности персональных данных, ответственный за организацию обработки персональных данных) 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.

2.5. 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 ИС Республиканского Центра СПИД 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 ИС Республиканского Центра СПИД и средств защиты. Эти инциденты выходят за рамки Республиканского Центра СПИД ответственными за реагирование сотрудниками.

К авариям относятся следующие инциденты:

а) отказ элементов ИС Республиканского Центра СПИД 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.

б) отсутствие администратора информационной безопасности более чем на сутки из-за:

- химического выброса в атмосферу;
- сбоев общественного транспорта;
- эпидемии;
- массового отравления персонала;
- сильного снегопада;
- торнадо;
- сильных морозов.

– уровень 3 - Катастрофа. Любой инцидент, приводящий к полному прерыванию работоспособности всех элементов ИС Республиканского Центра СПИД и средств защиты, а также к угрозе жизни пользователей ИС Республиканского Центра СПИД, классифицируется как катастрофа. Обычно к катастрофам относят обстоятельства непреодолимой силы (пожар, взрыв), которые могут привести к неработоспособности ИС Республиканского Центра СПИД 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 Объекта.

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

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

а) системы жизнеобеспечения, что включает:

- пожарные сигнализации и системы пожаротушения;
- системы вентиляции и кондиционирования;
- системы резервного питания.

б) системы обеспечения отказоустойчивости;

в) системы резервного копирования и хранения данных;

г) системы контроля физического доступа;

д) пожарные сигнализации и системы пожаротушения;

е) системы вентиляции и кондиционирования.

3.2. Все критичные помещения Республиканского Центра СПИД (помещения, в которых размещаются элементы ИС Республиканского Центра СПИД и средства защиты) должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

3.3. Порядок предотвращения потерь информации и организации системы жизнеобеспечения ИС описан в Порядке резервирования и восстановления работоспособности ТС и ПО, баз данных и СЗИ.

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

3.5. Должно быть проведено обучение должностных лиц Республиканского Центра СПИД, имеющих доступ к ресурсам ИС Республиканского Центра СПИД, 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.

3.6. Администратор информационной безопасности должен быть дополнительно обучен методам частичного и полного восстановления работоспособности элементов ИС Республиканского Центра СПИД.

3.7. 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.

3.8. Ответственность за организацию обучения должностных лиц несет руководитель отдела. Сроки и порядок их обучения согласуется с администратором информационной безопасности.

Разработал

Администратор информационной безопасности _____ /Сандаков З.Н.

«09» января 2023 г.

Приложение №1
к инструкции по действиям персонала
во внештатных ситуациях при
обработке защищаемой информации в
информационных системах
Республиканского Центра СПИД

Источники угроз

1. Технологические угрозы	
1.1.	Пожар в здании
1.2.	Повреждение водой (прорыв системы водоснабжения, канализационных труб, систем охлаждения)
1.3.	Взрыв (бытовой газ, теракт, взрывчатые вещества или приборы, работающие под давлением)
1.4.	Химический выброс в атмосферу
2. Внешние угрозы	
2.1.	Массовые беспорядки
2.2.	Сбои общественного транспорта
2.3.	Эпидемия
2.4.	Массовое отравление персонала
3. Стихийные бедствия	
3.1.	Удар молнии
3.2.	Сильный снегопад
3.3.	Сильные морозы
3.4.	Просадка грунта (подмыв грунтовых вод, подземные работы) с частичным обрушением здания
3.5.	Затопление водой в период паводка
3.6.	Наводнение, вызванное проливным дождем
3.7.	Торнадо
3.8.	Подтопление здания (воздействие подпочвенных вод, вызванное внезапным и непредвиденным повышением уровня грунтовых вод)
4. Телеком и ИТ угрозы	
4.1.	Сбой системы кондиционирования
4.2.	Сбой ИТ - систем
5. Угроза, связанная с человеческим фактором	
5.1.	Ошибка персонала, имеющего доступ к помещению, где расположено серверное оборудование
5.2.	Нарушение конфиденциальности, целостности и доступности конфиденциальной информации
6. Угрозы, связанные с внешними поставщиками	
6.1.	Отключение электроэнергии
6.2.	Сбой в работе интернет-провайдера
6.3.	Физически разрыв внешних каналов связи