УТВЕРЖДАЮ
Директор ОГБУ «РЦРО»

_____ Н.П. Лыжина
«03» _____08_____ 2015 г.
приказ № 264 прил № 4

ИНСТРУКЦИЯ

**пользователям информационных систем персональных данных,
используемых в ОГБУ «РЦРО»,
на случай возникновения внештатных ситуаций**

Томск 2015

Оглавление

1. Общие положения

1.1. Настоящая Инструкция определяет действия сотрудников по применению основных мер, методов и средств сохранения (поддержания) работоспособности всех информационных систем персональных данных (далее - ИСПДн), используемых в ОГБУ «РЦРО», при возникновении различных кризисных ситуаций, а также способы и средства восстановления информации и процессов ее обработки в случае нарушения работоспособности ИСПДн и их основных компонентов. Кроме того, она описывает действия различных категорий персонала системы в кризисных ситуациях по ликвидации их последствий и минимизации наносимого ущерба.

1.2. Под кризисной ситуацией понимается ситуация, возникшая в результате нежелательного воздействия на ИСПДн, не предотвращенная средствами защиты. Кризисная ситуация может возникнуть в результате злого умысла или случайно (в результате непреднамеренных действий, пожаров, аварий, стихийных бедствий и т.п.).

Под умышленным нападением понимается кризисная ситуация, которая возникла в результате выполнения злоумышленниками в определенные моменты времени заранее обдуманных и спланированных действий.

Под случайной (непреднамеренной) кризисной ситуацией понимается такая кризисная ситуация, которая не была результатом заранее обдуманных действий, и причиной возникновения которой явился результат объективных причин случайного характера, халатности, небрежности или случайного стечения обстоятельств.

По степени серьезности и размерам наносимого ущерба кризисные ситуации разделяются на следующие категории:

Угрожающая - приводящая к полному выходу ИСПДн из строя и их неспособности выполнять далее свои функции, а также к уничтожению, блокированию, неправомерной модификации или компрометации наиболее важной информации;

Серьезная - приводящая к выходу из строя отдельных компонентов системы (частичной потере работоспособности), потере производительности, а также к нарушению целостности и конфиденциальности программ и данных в результате несанкционированного доступа.

Ситуации, возникающие в результате нежелательных воздействий, не наносящих ощутимого ущерба, но, тем не менее, требующие внимания и адекватной реакции (например, зафиксированные неудачные попытки проникновения или несанкционированного доступа к ресурсам системы), к критическим не относятся.

1.3. Источники информации о возникновении кризисной ситуации:

- пользователи, обнаружившие несоответствия или иные подозрительные изменения в работе или конфигурации системы или средств ее защиты в своей зоне ответственности;
- средства защиты или сигнализации, обнаружившие кризисную ситуацию;
- системные журналы, в которых имеются записи, свидетельствующие о возникновении или возможности возникновения кризисной ситуации.

2. Меры обеспечения непрерывной работы и восстановления автоматизированных систем ОГБУ «РЦРО»

2.1. Непрерывность процесса функционирования ИСПДн и своевременность восстановления их работоспособности достигается:

- проведением специальных организационных мероприятий и разработкой организационно-распорядительных документов по вопросам обеспечения непрерывности вычислительного процесса;
- строгой регламентацией процесса обработки информации с применением автоматизированных рабочих мест (АРМ) и действий персонала системы, в том числе в кризисных ситуациях;

- назначением и подготовкой должностных лиц, отвечающих за организацию и осуществление практических мероприятий по обеспечению непрерывности вычислительного процесса;
- четким знанием и строгим соблюдением всеми должностными лицами, использующими средства вычислительной техники ИСПДн, требований руководящих документов по обеспечению непрерывности вычислительного процесса;
- применением различных способов резервирования аппаратных ресурсов, эталонного копирования программных и страхового копирования информационных ресурсов ИСПДн;
- эффективным контролем за соблюдением требований по обеспечению непрерывности вычислительного процесса должностными лицами и ответственным;
- постоянным поддержанием необходимого уровня защищенности компонентов системы, непрерывным управлением и административной поддержкой корректного применения средств защиты;
- проведением постоянного анализа эффективности принятых мер и применяемых способов и средств обеспечения непрерывности вычислительного процесса, разработкой и реализацией предложений по их совершенствованию.

3. Общие требования

Все пользователи, работа которых может быть нарушена в результате возникновения угрожающей или серьезной кризисной ситуации, должны немедленно оповещаться. Дальнейшие действия по устранению причин нарушения работоспособности ИСПДн, возобновлению обработки и восстановлению поврежденных (утраченных) ресурсов определяются функциональными обязанностями персонала и пользователей системы.

Каждая кризисная ситуация должна анализироваться администратором информационной безопасности, и по результатам этого анализа должны вырабатываться предложения по изменению полномочий пользователей, атрибутов доступа к ресурсам, созданию дополнительных резервов, изменению конфигурации системы или параметров настройки средств защиты и т.д.

Серьезная и угрожающая кризисная ситуация могут требовать оперативной замены и ремонта вышедшего из строя оборудования, а также восстановления поврежденных программ и наборов данных из резервных копий.

Оперативное восстановление программ (используя эталонные копии) и данных (используя страховые копии) в случае их уничтожения или порчи в серьезной или угрожающей кризисной ситуации обеспечивается резервным (страховым) копированием и внешним (по отношению к основным компонентам системы) хранением копий.

Резервному копированию подлежат все программы и данные, обеспечивающие работоспособность системы и выполнение ею своих задач (системное и прикладное программное обеспечение, базы данных и другие наборы данных), а также архивы, журналы транзакций, системные журналы и т.д.

Все программные средства, используемые в системе должны, иметь эталонные (дистрибутивные) копии. Их местонахождение и сведения об ответственных за их создание, хранение и использование должны быть указаны в формулярах на каждую ПЭВМ (рабочую станцию). Там же должны быть указаны перечни наборов данных, подлежащих страховому копированию, периодичность копирования, место хранения и ответственные за создание, хранение и использование страховых копий данных.

Необходимые действия персонала по созданию, хранению и использованию резервных копий программ и данных должны быть отражены в функциональных обязанностях соответствующих категорий персонала.

Каждый носитель, содержащий резервную копию, должен иметь метку, содержащую данные о классе, ценности, назначении хранимой информации, ответственном за создание, хранение и использование, дату последнего копирования, место хранения и др.

Дублирующие аппаратные ресурсы предназначены для обеспечения работоспособности системы в случае выхода из строя всех или отдельных аппаратных

компонентов в результате угрожающей кризисной ситуации. Количество и характеристики дублирующих ресурсов должны обеспечивать выполнение основных задач системой в любой из предусмотренных кризисных ситуаций.

Ликвидация последствий угрожающей или серьезной кризисной ситуации подразумевает, возможно, более полное восстановление программных, аппаратных, информационных и других поврежденных компонентов системы. Для восстановления используются архивирование и резервирование данных.

В случае возникновения любой кризисной ситуации должно производиться расследование причин ее возникновения, оценка причиненного ущерба, определение виновных и принятие соответствующих мер.

Расследование кризисной ситуации производится группой, назначаемой директором ОГБУ «РЦРО». Возглавляет группу администратор информационной безопасности. Выводы группы докладываются непосредственно директору ОГБУ «РЦРО».

Если причиной угрожающей или серьезной кризисной ситуации явились недостаточно жесткие меры защиты и контроля, а ущерб превысил установленный уровень, то такая ситуация является основанием для полного пересмотра планов обеспечения непрерывной работы и восстановления.

4. Порядок пересмотра плана мероприятий по обеспечению непрерывной работы и восстановления

4.1. План мероприятий подлежит полному пересмотру в следующих случаях:

- при изменении перечня решаемых задач, конфигурации технических и программных средств ИСПДн, приводящих к изменению технологии обработки информации;
- при изменении приоритетов в значимости угроз безопасности ИСПДн.

4.2. План подлежит частичному пересмотру в следующих случаях:

- при изменении конфигурации, добавлении или удалении программных и технических средств в ИСПДн, не изменяющих технологию обработки информации;
- при изменении конфигурации используемых программных и технических средств;
- при изменении состава, обязанностей и полномочий пользователей системы.

4.3. Профилактический пересмотр Плана производится не реже 1 раза в год и имеет целью проверку достаточности определенных данным планом мер реальным условиям применения ИСПДн и существующим требованиям.

4.4. В случае частичного пересмотра могут быть добавлены, удалены или изменены различные приложения к плану с обязательным указанием данных о том, кто санкционировал, кто, когда и с какой целью внес изменения.

4.5. Вносимые в План изменения не должны противоречить другим положениям Плана.

4.6. Пересмотр Плана должен осуществляться специальной комиссией, состав которой утверждается директором ОГБУ «РЦРО». Включение администратора информационной безопасности в состав комиссии по пересмотру Плана обязательно.

4.7. Ответственным за реализацию данного документа является администратор информационной безопасности.

5. Обязанности и действия персонала по обеспечению непрерывной работы и восстановлению системы

Действия персонала в кризисной ситуации зависят от степени ее тяжести.

5.1. В случае возникновения ситуации, требующей внимания, администратор информационной безопасности должен провести ее анализ (расследование) собственными силами. О факте систематического возникновения таких ситуаций и принятых мерах необходимо ставить в известность руководство подразделения.

5.2. В случае возникновения угрожающей или серьезной критической ситуации действия сотрудников включают следующие этапы:

- немедленная реакция;

- частичное восстановление работоспособности и возобновление обработки;
- полное восстановление системы и возобновление обработки в полном объеме;
- расследование причин кризисной ситуации и установление виновных.

5.3. Этапы включают следующие действия:

5.3.1. В качестве немедленной реакции:

- обнаруживший факт возникновения кризисной ситуации оператор обязан немедленно оповестить об этом администратора информационной безопасности, по телефону, лично, или по электронной почте;
- администратор должен поставить в известность операторов (сотрудников, обрабатывающих информацию) о факте возникновения кризисной ситуации для их перехода на аварийный режим работы (приостановку работы);
- вызвать ответственных программистов;
- определить степень серьезности и масштабы кризисной ситуации, размеры и область поражения;
- оповестить персонал взаимодействующих подсистем о характере кризисной ситуации и ориентировочном времени возобновления обработки.

Ответственными за этот этап являются операторы ИСПДн и администратор информационной безопасности.

5.3.2. При частичном восстановлении работоспособности (минимально необходимой для возобновления работы системы в целом, возможно с потерей производительности) и возобновлении обработки:

- отключить пораженные компоненты или переключиться на использование дублирующих ресурсов (горячего резерва);
- если не произошло повреждения программ и данных, возобновить обработку и оповестить об этом персонал взаимодействующих (под)систем.
- восстановить работоспособность поврежденных критичных аппаратных средств и другого оборудования, при необходимости произвести замену отказавших узлов и блоков резервными;
- восстановить поврежденное критичное программное обеспечение, используя эталонные (страховые) копии;
- восстановить необходимые данные, используя резервные копии;
- проверить работоспособность поврежденной подсистемы, удостовериться в том, что последствия кризисной ситуации не оказывают воздействия на дальнейшую работу системы;
- уведомить операторов смежных (под)систем о готовности к работе.

Затем необходимо внести все изменения данных за время с момента создания последней страховой копии (за текущий период, операционный день) на основании информации из журналов транзакций либо все связанные с поврежденной (под)системой пользователи должны повторить действия, выполненные в течение последнего периода (дня).

Ответственным за этот этап является администратор информационной безопасности, системный программист и системный инженер.

5.3.3. Для полного восстановления в период неактивности системы следует:

- восстановить работоспособность всех поврежденных аппаратных средств, при необходимости произвести замену отказавших узлов и блоков резервными;
- восстановить и настроить все поврежденные программы, используя эталонные (страховые) копии;
- восстановить все поврежденные данные, используя страховые копии и журналы транзакций;
- настроить средства защиты подсистемы в соответствии с планом защиты;
- о результатах восстановления уведомить администратора системы (базы данных).

Ответственными за этот этап являются администратор информационной безопасности, программисты.

5.3.4. Далее необходимо провести расследование причин возникновения кризисной ситуации. Ответственным за расследование является администратор информационной безопасности. Отчет о результатах расследования и предложениях по совершенствованию системы необходимо направить директору ОГБУ «РЦРО».

5.4. Обязанности системного инженера по обеспечению непрерывности вычислительного процесса

В обязанности инженерного состава входит:

- поддержание аппаратных средств и другого оборудования, включая резервное (дублирующее), в рабочем состоянии и их периодическая проверка;
- восстановление функций аппаратных средств и другого оборудования в случае отказов;
- оперативная замена дефектных узлов резервными в случае отказов;
- подготовка и оперативное включение резервных аппаратных средств и другого оборудования в случае серьезной кризисной ситуации.

ЛИСТ
регистрации изменений

Дата	Содержание вносимого изменения	Кем санкционировано изменение (каким документом)	Подпись лица, произведшего изменения

Приложение 1

Кризисные ситуации, предусмотренные планом обеспечения непрерывной работы и восстановления

1. **К угрожающим кризисным ситуациям** относятся:
   - нарушение подачи электроэнергии в здании;
   - выход из строя файлового сервера (с потерей информации);
   - выход из строя файлового сервера (без потери информации);
   - частичная потеря информации на сервере без потери его работоспособности;
   - выход из строя локальной сети (физической среды передачи данных);

2. **К серьезным кризисным ситуациям** относятся:
   - выход из строя рабочей станции (с потерей информации);
   - выход из строя рабочей станции (без потери информации);
   - частичная потеря информации на рабочей станции без потери ее работоспособности;

3. **К ситуациям, требующим внимания,** относятся:
   - несанкционированные действия, заблокированные средствами защиты и зафиксированные средствами регистрации.