Росгидромет
Федеральное государственное бюджетное учреждение
«ЗАПАДНО-СИБИРСКОЕ УПРАВЛЕНИЕ ПО ГИДРОМЕТЕОРОЛОГИИ И МОНИТОРИНГУ ОКРУЖАЮЩЕЙ СРЕДЫ»
(ФГБУ «Западно-Сибирское УГМС»)
10.11.2022 № 22-95

УТВЕРЖДАЮ
Начальник
_____ А.О. Люцигер
«10» 11 2022 г.
М.П.

Инструкция
по порядку резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в информационных системах персональных данных

1. Назначение и область действия

1.1. Порядок резервирования и восстановления работоспособности технических средств (ТС) и программного обеспечения (ПО), баз данных и средств защиты информации (СЗИ) (далее - Порядок) определяет действия, связанные с функционированием информационной системы персональных данных (далее - ИСПДн) в ФБГУ «Западно-Сибирское УГМС» (далее - Учреждение), меры и средства поддержания непрерывности работы и восстановления работоспособности ИСПДн.

1.2. Целью настоящего документа является превентивная защита элементов ИСПДн для предотвращения потери защищаемой информации.

1.3. Задачей данной инструкции является:

- определение мер защиты от потери информации;
- определение действий по восстановлению информации в случае ее потери.

1.4. Действие настоящей инструкции распространяется на всех пользователей Учреждения, 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.

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

2. Порядок реагирования на инцидент

2.1. В настоящем документе под инцидентом понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИСПДн, предоставляемых пользователям ИСПДн, а также потерей защищаемой информации.

2.2. Происшествие, вызывающее инцидент, может произойти:

- в результате непреднамеренных действий пользователей;
- в результате преднамеренных действий пользователей и третьих лиц;
- в результате нарушения правил эксплуатации технических средств ИСПДн;

- в результате возникновения внештатных ситуаций и обстоятельств непреодолимой силы.

2.3. В кратчайшие сроки, не превышающие одного рабочего дня, ответственные за реагирование работники Учреждения (администратор информационной безопасности), предпринимают меры по восстановлению работоспособности ИСПДн. Перечень указанных мер согласуется с вышестоящим руководством, за исключением случаев, когда ИСПДн должна быть восстановлена в кратчайшие сроки.

3. Меры обеспечения непрерывности работы и восстановления ресурсов при возникновении инцидентов

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

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

3.2. Системы жизнеобеспечения ИСПДн включают:

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

3.3. Все помещения, в которых размещаются элементы ИСПДн и средства защиты, должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

3.4. Для выполнения требований по эксплуатации (температура, относительная влажность воздуха) программно-аппаратных средств ИСПДн в помещениях, где они установлены, должны применяться системы вентиляции и кондиционирования воздуха.

3.5. Для предотвращения потерь информации при кратковременном отключении электроэнергии все ключевые элементы ИСПДн, сетевое и коммуникационное оборудование, а также наиболее критичные рабочие станции должны подключаться к сети электропитания через источники бесперебойного питания. В зависимости от необходимого времени работы ресурсов после потери питания могут применяться следующие методы резервного электропитания:

- локальные источники бесперебойного электропитания с различным временем питания для защиты отдельных компьютеров;
- источники бесперебойного питания с дополнительной функцией защиты от скачков напряжения;
- дублированные системы электропитания в устройствах (серверы, концентраторы, мосты и т.д.);
- резервные линии электропитания в пределах комплекса зданий;
- аварийные электрогенераторы.

3.6. Системы обеспечения отказоустойчивости:

- кластеризация;
- технология RAID.

3.7. Для обеспечения отказоустойчивости критичных компонентов ИСПДн при сбое в работе оборудования и их автоматической замене без простоев должны использоваться методы кластеризации. Для наиболее критичных компонентов ИСПДн должны использоваться территориально удаленные системы кластеров.

3.8. Для защиты от отказов отдельных дисков серверов, осуществляющих обработку и хранение защищаемой информации, должны использоваться технологии RAID, которые (кроме RAID-0) применяют дублирование данных, хранимых на дисках.

3.9. Система резервного копирования и хранения данных должна обеспечивать хранение защищаемой информации на твердый носитель (ленту, жесткий диск и т.п.).

3.10. Организационные меры.

Резервное копирование и хранение данных должно проводиться в следующем режиме:

- обрабатываемые персональные данные - не реже раза в неделю;
- технологическая информация - не реже раза в месяц;
- эталонные копии программного обеспечения (операционные системы, штатное и специальное программное обеспечение, программные средства защиты), с которых осуществляется их установка на элементы ИСПДн, - не реже раза в месяц и каждый раз при внесении в них изменений (выход новых версий).

3.11. На носителях, предназначенных для хранения резервных копий информации, должны быть указаны их регистрационные номера.

3.12. Носители должны храниться в несгораемом шкафу или помещении, оборудованном системой пожаротушения.
