Приложение № 4
к приказу «Об обеспечении безопасности персональных данных в информационных системах персональных данных ФГБУЗ ММЦ им. Н.И. Пирогова ФМБА России»
№ 01-147 от 12.07.2022

Порядок резервного копирования и восстановления информации в информационных системах персональных данных Федерального государственного бюджетного учреждения здравоохранения «Мурманский многопрофильный центр имени Н.И. Пирогова Федерального медико-биологического агентства»

1. Назначение и область действия

1.1. Порядок резервного копирования и восстановления информации в информационных системах персональных данных в Федеральном государственном бюджетном учреждении здравоохранения «Мурманский многопрофильный центр имени Н.И. Пирогова Федерального медико-биологического агентства» (далее Учреждение и Порядок) определяет действия, связанные с безотказным функционированием информационных систем персональных данных ПО «Парус Бюджет 8», МИС «Медиалог», МИС «ЭконБол 3», 1С:Предприятие 8.х (далее – ИСПДн), меры и средства поддержания непрерывности работы и восстановления работоспособности ИСПДн.

1.2. Целью настоящей Инструкции является превентивная защита элементов ИСПДн от предотвращения потери защищаемой информации.

1.3. Задачами данной Инструкции является:

- определение мер защиты от потери информации;
- определение действий восстановления в случае потери информации.

1.4. Действие настоящей Инструкции распространяется на всех пользователей, 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.

1.5. Ответственным сотрудником за реагирование на инциденты безопасности, приводящие к потере защищаемой информации, назначается администратор ИСПДн.

1.6. Ответственным сотрудником за контроль обеспечения мероприятий по предотвращению инцидентов, приводящих к потере защищаемой информации, назначается администратор информационной безопасности.

2. Порядок реагирования на инцидент

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

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.

2.2. Все действия в процессе реагирования на инциденты должны документироваться администратором ИСПДн в журнале учета инцидентов информационной безопасности.

2.3. Администратор ИСПДн предпринимают меры по восстановлению работоспособности. Предпринимаемые меры по возможности согласуются с вышестоящим руководством.

3. Меры обеспечения непрерывности работы и восстановления информационных систем при возникновении инцидентов

3.1. Технические меры.

3.1.1. 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.

Системы жизнеобеспечения ИС включают:

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

3.1.2. Все помещения, в которых размещаются элементы ИСПДн и средства защиты должны быть оборудованы средствами охранно-пожарной сигнализации.

3.1.3. 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.

3.1.4. Для предотвращения потерь информации при кратковременном отключении электроэнергии все ключевые элементы ИСПДн 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;
- системы обеспечения отказоустойчивости.

3.1.5. Для обеспечения отказоустойчивости критичных компонентов ИСПДн при сбое в работе оборудования и их автоматической замены без простоев могут использоваться методы кластеризации.

3.1.6. Для обеспечения требуемого времени восстановления ИСПДн создается запас резервных технических средств (системные блоки, мониторы, сетевое оборудование, источники бесперебойного питания, жесткие диски и т.д.)

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

3.1.8. Система резервного копирования и хранения данных, должна обеспечивать хранение защищаемой информации на твердый носитель (CD/DVD-диск, съемный жесткий диск и т.п.).

3.2. Организационные меры

3.2.1. Резервное копирование и хранение данных должно осуществляться на периодической основе пользователем ИСПДн или администратором ИСПДн, либо автоматически по расписанию:

- для обрабатываемых персональных данных – не реже одного раза в неделю;
- для технологической информации – не реже одного раза в месяц;
- копии системного раздела серверов баз данных (операционная система, штатное и специальное программное обеспечение, программные средства защиты и т. п.) – не реже одного раза в месяц, и каждый раз перед установкой нового специального программного обеспечения, программных и программно-

аппаратных средств защиты, внесением изменений в специальное программное обеспечение и средства защиты (обновление версий).

3.2.2. Носители, на которые произведено резервное копирование, должны быть пронумерованы, информация должная содержать дату проведения резервного копирования.

3.2.3. Резервное копирование информации, составляющей персональные данные, осуществляется на машинные носители информации, предназначенных для хранения персональных данных.

3.2.4. Информация о проведении резервного копирования заносится в Журнал резервного копирования по форме, приведенной в приложении к настоящей Инструкции.

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

4. Создание архива данных ИСПДн

4.1. Для обеспечения нормальной работы архива ИСПДн необходимо обеспечить следующее:

- пользователи ИСПДн совместно с администраторами ИСПДн обязаны определить часть информации подлежащей архивации;
- администратор ИСПДн определяют временной интервал проведения процесса архивации, исходя из технологических особенностей системы;
- для эффективного доступа к архивным данным информация, время доступа к которой является критичной величиной, записывается в соответствующую директорию (выделенную для хранения архивных копий) на диске сервера либо на учетный съемный машинный носитель информации (такой архив называется оперативным);
- с целью предотвращения переполнения диска сервера архив информации, потерявшей актуальность или время доступа к которой не является критичной величиной, переносится на учетный съемный машинный носитель информации, предназначенный для хранения персональных данных (такой архив называется основным);
- наиболее важная информация записывается одновременно как на диск сервера, так и на съемный машинный носитель.
- целостность и достоверность архивной информации проверяется администратором ИСПДн.
- архивная информация ИСПДн, размещенная на съемных машинных носителях, хранится в надежно запираемых шкафах либо в сейфе, причем копии хранятся отдельно от дубликатов.

4.2. Права на доступ к архиву должны быть определены в Матрице доступа пользователей к информационным ресурсам ИСПДн. Доступ иных лиц

к данным хранящимся в архиве осуществляется на основании служебной записки директору Департамента управления делами и контроля.

4.3. Механизмы резервного копирования задействуются при модернизации и установке нового оборудования и прикладного программного обеспечения, обеспечивая перенос и резервирование данных на обновляемом рабочем месте.

4.4. Программные средства резервного копирования настраиваются таким образом, чтобы осуществлялось копирование открытых файлов, а также прав доступа на файлы и каталоги.

4.5. Процесс резервного копирования должен предусматривать перемещения и архивирования файлов локально на рабочих местах в дневное время, а операции по резервированию на постоянно включенных серверах – в нерабочее время вечером, ночью или в выходные дни.

5. Восстановление информации в случае аварийной ситуации

5.1. Выход из строя не системных дисков (системных разделов) на сервере базы данных.

5.1.1. В случае выхода из строя дисков, не повлекшем за собой разрушения системного раздела или системного диска, на место неисправного диска вставляется новый или форматируется неисправный раздел (логический диск).

После этого производится восстановление данных, которые были на этом диске (разделе) с резервной копии.

5.1.2. В случае выхода из строя диска (раздела), которое повлекло за собой разрушение баз данных, следует:

- остановить работу сервера ИСПДн;
- заменить диск или отформатировать раздел;
- с резервной копии базы данных восстанавливаются последние архивные данные.

5.2. Выход из строя системных дисков на сервере базы данных ИСПДн.

Выполняются следующие действия:

- останавливается сервер;
- на место системных дисков на сервере вставляются новые диски;
- восстанавливается копия системного программного обеспечения данного сервера;
- запускается сервер баз данных (далее – БД).

5.3. При невозможности восстановления программного обеспечения (операционная система, специальное программного обеспечение, программные средства защиты) из резервных копий производится установка с дистрибутивов программного обеспечения и их настройка для обеспечения необходимого

класса защищенности информации. В случаях, когда восстановление работоспособности системы защиты информации невозможно, применяются компенсирующие меры защиты информации.

6. Ответственные за восстановление работоспособности ИСПДн

6.1. Ответственность за организацию восстановительных работ несет администратор ИСПДн.

6.2. Восстановительными работами руководит администратор ИСПДн.

6.3. По окончанию восстановительных работ делается соответствующая запись в журнале регистрации работ технического паспорта ИСПДн (при необходимости).