УТВЕРЖДАЮ
Главный врач
ГБУЗ «Ленинская ЦРБ»
_____Е.А.Крайнов
15.11.2013

Приложение №11
к Приказу от
15.11.2013 №515-О

Порядок резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в ГБУЗ «Ленинская ЦРБ»

1. Назначение и область действия

1.1. Порядок резервирования и восстановления работоспособности технических средств (далее по тексту ТС) и программного обеспечения (далее по тексту ПО), баз данных и средств защиты информации (далее – «СЗИ») определяет действия, связанные с функционированием информационных систем обработки персональных данных (далее – «ИСПДн») ГБУЗ «Ленинская ЦРБ» (далее – «Учреждение»), меры и средства поддержания непрерывности работы и восстановления работоспособности ИСПДн.

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

1.3. Задачей настоящего Порядка является:

– определение мер защиты от потери информации;

– определение действий восстановления в случае потери информации.

1.4. Действие настоящего Порядка 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 резервного копирования и хранения данных;

– системы контроля физического доступа.

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 безопасности, приводящих к потере защищаемой информации, назначается Администратор безопасности.

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 так же 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 сотрудники ГБУЗ «Ленинская ЦРБ» (Администратор безопасности, Администратор 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.

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 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 критичные помещения ГБУЗ «Ленинская ЦРБ» (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, серверное, 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.);

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

3.7. Резервное копирование и хранение данных должно осуществляться на периодической основе:

- для обрабатываемых персональных данных - не реже раза в неделю;
- для технологической информации - 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 изменений в эталонные копии (выход новых версий).

3.8. Носители, на которые произведено резервное копирование, должны быть пронумерованы с указанием номера носителя и датой проведения резервного копирования.

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