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

Приложение №14
к Приказу от
15.11.2013 №515-О

Регламент проведения технического обслуживания в ГБУЗ «Ленинская ЦРБ»

1. Общие положения

1.1. Регламент проведения технического обслуживания ГБУЗ «Ленинская ЦРБ» (далее – «Учреждение»), включает в себя описание комплекса организационно-технических мер по проведению работ по техническому обслуживанию программного обеспечения и аппаратных средств Учреждения.

1.2. Требования настоящего Регламента распространяются на всех должностных лиц и сотрудников подразделений Учреждения, использующих в работе ИСПДн, в которых осуществляется обработка информации ограниченного доступа, не составляющая государственной тайны.

1.3. Должностные лица Учреждения, задействованные в обеспечении функционирования ИСПДн Учреждения, знакомятся с основными положениями и приложениями Регламента в части их касающейся и по мере необходимости.

1.4. Администратор ИСПДн ознакомляет пользователей с требованиями настоящего Регламента и выдает под роспись электронные копии соответствующего Регламента для повседневного использования в работе.

2. Порядок проведения работ

2.1. Право внесения изменений в конфигурацию аппаратно-программных средств рабочих станций ИСПДн Учреждения предоставляется Администратору ИСПДн и Администратору безопасности.

2.2. Изменение конфигурации аппаратно-программных средств рабочих станций и серверов кем-либо, кроме Администратора ИСПДн и Администратора безопасности, ЗАПРЕЩЕНО.

2.3. Установка и настройка программного средства осуществляется Администратором ИСПДн согласно эксплуатационной документации.

2.4. Запрещается установка и использование на рабочих станциях (серверах) программного обеспечения (ПО), не входящего в перечень программного обеспечения, разрешенного к использованию в Обществе (см. Приложение 14.2).

2.5. Установка (обновление) ПО (системного, тестового и т.п.) на рабочих станциях и серверах производится с эталонных копий программных средств, хранящихся у администратора ИСПДн. Все добавляемые программные и аппаратные компоненты должны быть предварительно проверены на работоспособность, а также отсутствие вредоносного программного кода в соответствии с «Регламентом организации антивирусной защиты».

2.6. После установки (обновления) ПО Администратор безопасности должен произвести настройку средств управления доступом к компонентам данной задачи (программного средства) в соответствии с требованиями к системе защиты информации и, совместно с пользователем рабочей станции, проверить правильность настройки средств защиты.

2.7. В случае обнаружения не декларированных (не описанных в документации) возможностей программного средства, сотрудники немедленно докладывают начальнику своего подразделения и Администратору ИСПДн. Использование программного средства до получения специальных указаний прекращается.

2.8. После завершения работ по внесению изменений в состав аппаратных средств защищаемых рабочих станций и серверов системный блок должен быть опечатан (опломбирован, защищен специальной наклейкой) Администратором безопасности.

2.9. При изъятии рабочей станции из состава рабочих станций, обрабатывающих информацию ограниченного распространения (защищаемая информация), ее передача на

склад, в ремонт или в другое подразделение для решения иных задач осуществляется только после того, как Администратор безопасности снимет с данной рабочей станции средства защиты и предпримет необходимые меры для затирания (уничтожения) защищаемой информации, которая хранилась на дисках компьютера. Факт затирания (уничтожения) защищаемой информации, которая хранилась на дисках компьютера, фиксируется соответствующим актом (см. Приложение 14.1)

2.10. Допуск новых пользователей к решению задач с использованием вновь развернутого ПО (либо изменение их полномочий доступа) осуществляется после добавления пользователей в «Перечень лиц, допущенных к обработке персональных данных в информационных системах персональных данных».

3. Ответственные за организацию и контроль выполнения Регламента

3.1. Ответственность за соблюдение требований настоящего Регламента пользователями возлагается на всех сотрудников Учреждения.

3.2. Ответственность за организацию контрольных и проверочных мероприятий по вопросам установки, модификации технических и программных средств возлагается на Администратора ИСПДн и Администратора безопасности.

3.3. Ответственность за общий контроль информационной безопасности возлагается на заместителя главного врача по административно-хозяйственной части учреждения.