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

Приложение №4
к приказу от 15.11.2013 №515-О

Регламент организации антивирусной защиты в ГБУЗ «Ленинская ЦРБ»

1. Общие положения

1.1. Регламент организации антивирусной защиты информационных систем обработки персональных данных ГБУЗ «Ленинская ЦРБ» определяет требования к организации защиты информационных систем обработки персональных данных (далее ИСПДн) от разрушающего воздействия компьютерных вирусов и другого вредоносного программного обеспечения (ПО) и устанавливает ответственность руководителей и сотрудников подразделений, эксплуатирующих и сопровождающих автоматизированную систему, за их выполнение.

1.2. Требования настоящего Регламента распространяются на всех должностных лиц и сотрудников подразделений ГБУЗ «Ленинская ЦРБ» (далее «Учреждение»), использующих в работе ИСПДн.

1.3. В целях закрепления знаний по вопросам практического исполнения требований Регламента, разъяснения возникающих вопросов, проводятся организуемые Администратором ИСПДн семинары и персональные инструктажи (при необходимости) пользователей ИСПДн Учреждения

1.4. Доведение Регламента до сотрудников Учреждения в части их касающейся осуществляется Администратором ИСПДн под роспись в журнале или на самом документе.

2. Применение средств антивирусной защиты

2.1. Антивирусный контроль дисков и файлов ИСПДн после загрузки компьютера должен проводиться в автоматическом режиме (периодическое сканирование или мониторинг).

2.2. Периодически, не реже одного раза в неделю, должен проводиться полный антивирусный контроль всех дисков и файлов ИСПДн (сканирование).

2.3. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам связи, на съемных носителях (магнитных дисках, CD-ROM и т.п.). Разархивирование и контроль входящей информации необходимо проводить непосредственно после ее приема. Контроль исходящей информации необходимо проводить непосредственно перед отправкой (записью на съемный носитель).

2.4. Установка (обновление и изменение) системного и прикладного программного обеспечения осуществляется в соответствии с «Инструкцией по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств автоматизированных систем ГБУЗ «Ленинская ЦРБ».

2.5. Обновление антивирусных баз должно проводиться регулярно, но не реже, чем 1 раз в неделю.

3. Функции Администратора ИСПДн по обеспечению антивирусной безопасности

Администратор ИСПДн обязан:

3.1. При необходимости проводить инструктажи пользователей ИСПДн по вопросам применения средств антивирусной защиты.

3.2. Настраивать параметры средств антивирусного контроля в соответствии с руководствами по применению конкретных антивирусных средств.

3.3. Предварительно проверять устанавливаемое (обновляемое) программное обеспечение на отсутствие вирусов.

3.4. При необходимости производить обновление антивирусных программных средств.

3.5. Производить получение и рассылку (при необходимости) обновлений антивирусных баз.
3.6. Проводить работы по обнаружению и обезвреживанию вирусов.
3.7. Хранить эталонные копии антивирусных программных средств.
3.8. Осуществлять периодический контроль соблюдения пользователями рабочих станций требований настоящей Инструкции.
3.9. Проводить периодический контроль работы программных средств системы антивирусной защиты информации на рабочих станциях (серверах).

4. Функции пользователей

4.1. Пользователи ИСПДн получают по ЛВС или от Администратора ИСПДн носители с обновлениями антивирусных баз (в случае отсутствия механизмов централизованного распространения антивирусных баз).
4.2. Пользователи проводят обновления антивирусных баз (или совместно с Администратором ИСПДн) на рабочих станциях и серверах (в случае отсутствия механизмов централизованного распространения антивирусных баз).
4.3. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) сотрудник подразделения самостоятельно или вместе с администратором ИСПДн должен провести внеочередной антивирусный контроль на рабочих станциях и серверах. При необходимости он должен привлечь администратора ИСПДн для определения факта наличия или отсутствия компьютерного вируса.
4.4. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов сотрудники подразделений обязаны:
4.4.1. приостановить работу;
4.4.2. немедленно поставить в известность о факте обнаружения зараженных вирусом файлов Администратора ИСПДн, владельца зараженных файлов, а также смежные подразделения, использующие эти файлы в работе;
4.4.3. совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;
4.4.4. провести лечение или уничтожение зараженных файлов (при необходимости для выполнения требований данного пункта привлечь администратора ИСПДн).

5. Ответственные за организацию и контроль выполнения регламента

5.1. Ответственность за соблюдение требований настоящей Инструкции пользователями возлагается на всех сотрудников Учреждения.
5.2. Ответственность за организацию контрольных и проверочных мероприятий по вопросам антивирусной защиты возлагается на Администратора безопасности.
5.3. Ответственность за общий контроль информационной безопасности возлагается на программиста ГБУЗ «Ленинская ЦРБ».

Лист ознакомления с документом «Регламент организации антивирусной защиты»

№ п/п	Фамилия И.О. сотрудника	Дата ознакомления	Расписка сотрудника в ознакомлении