**ИНСТРУКЦИЯ ПО ОРГАНИЗАЦИИ АНТИВИРУСНОЙ ЗАЩИТЫ**

Настоящая инструкция предназначена для организации порядка проведения антивирусного контроля в учреждении и предотвращения возникновения фактов заражения программного обеспечения учреждения компьютерными вирусами.

**Установка, настройка и регулярное обновление антивирусных средств осуществляется только ответственным за информационную безопасность учреждения.**

**Требования к проведению мероприятий по антивирусной защите:**

* Ежедневно в начале работы при загрузке компьютера в автоматическом режиме должно выполняться **обновление антивирусных баз**и проводиться **антивирусная проверка**всех дисков и файлов персонального компьютера.
* Обязательному антивирусному **контролю** подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), **получаемая и передаваемая**по электронной почте, интернет-ресурсам, а также информация на съемных носителях (дисках 3,5 (А:), флешках, CD-ROM и т.п.).

**Действия сотрудников при обнаружении компьютерного вируса:**

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.), либо на наличие **заражения съемного носителя**, сотрудник подразделения самостоятельно или вместе с ответственным за обеспечение безопасности информации должен провести внеочередной антивирусный контроль своей рабочей станции.

В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователи обязаны:

* приостановить работу;
* поставить в известность о факте обнаружения зараженных вирусом файлов ответственного за обеспечение информационной безопасности в учреждении;
* провести лечение или уничтожение зараженных файлов (при необходимости для выполнения требований данного пункта привлечь специалистов отдела IT)

**Пользователям запрещается:**

* отключать средства антивирусной защиты информации во время работы.
* открывать сомнительные эл. письма (необходимо удаление), ссылки, сайты, источники переноса информации.

По вопросам обращайтесь в организационно-методический отдел районной больницы