Приложение № 3
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

Инструкция по антивирусной защите в информационных системах Федерального государственного бюджетного учреждения здравоохранения «Мурманский многопрофильный центр имени Н.И. Пирогова Федерального медико-биологического агентства»

1. Общие положения

Данная инструкция определяет:

- требования к организации защиты информации в информационных системах персональных данных, расположенных в Федеральном государственном бюджетном учреждении здравоохранения «Мурманский многопрофильный центр имени Н.И. Пирогова Федерального медико-биологического агентства» (далее Учреждение): ПО «Парус Бюджет 8», МИС «Медиалог», МИС «ЭконБол 3», ФГИС «ЕВМИАС» (далее - ИСПДн) от воздействия компьютерных вирусов;
- ответственность за состояние антивирусной защиты.

2. Организация антивирусной защиты

Антивирусная защита ИСПДн должна осуществляться сертифицированным по требованиям безопасности информации антивирусным средством. Другие лицензионные антивирусные программы могут использоваться только в исключительных случаях в качестве дополнительного средства контроля и защиты. Установка антивирусного средства и настройка параметров антивирусного контроля осуществляется в соответствии с эксплуатационной и технической документацией на конкретные антивирусные средства.

Ответственность за своевременную установку и переустановку антивирусного средства, поддержание его в рабочем состоянии, контроль за своевременным обновлением антивирусных баз возлагается на администратора ИСПДн.

3. Применение средств антивирусной защиты

Установку и настройку антивирусного средства осуществляет администратор ИСПДн. Пользователю запрещается самостоятельно изменять настройки антивирусного средства.

Пользователь обязан регулярно проверять рабочие каталоги на жестком магнитном диске ПЭВМ, а также подключаемые к ПЭВМ съемные носители информации (дискеты, флеш-накопители и др.) на отсутствие вирусов с помощью штатных средств антивирусного средства.

Антивирусному контролю подлежат все файлы без исключения (текстовые, графические, исполняемые, архивные, служебные, системные и т.д.).

Разархивирование и обработку входящей информации необходимо проводить после ее проверки на наличие компьютерных вирусов непосредственно на носителе, содержащем эту информацию.

4. Действия при обнаружении вирусов

При возникновении подозрения на наличие компьютерного вируса, пользователь самостоятельно или совместно с администратором ИСПДн должен провести внеочередной антивирусный контроль носителей информации.

В случае обнаружения антивирусным средством зараженного компьютерным вирусом файла пользователь обязан:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения вируса администратора информационной безопасности и, при необходимости, других пользователей, ранее работавших с данным файлом;
- провести лечение или уничтожение (при невозможности лечения) зараженного файла;
- решение о лечении (уничтожении) системных и служебных файлов принимается только администратором информационной безопасности.

5. Ответственность за состояние антивирусной защиты

Ответственность за организацию антивирусной защиты ИСПДн, в соответствии с требованиями настоящей Инструкции, возлагается на администратора информационной безопасности.

Ответственность за проведение мероприятий антивирусного контроля на конкретном ПЭВМ и соблюдение требований настоящей Инструкции возлагается на Пользователя ИСПДн.

Периодический контроль за состоянием антивирусной защиты ИСПДн, а также за соблюдением установленного порядка антивирусного контроля и

выполнением требований настоящей Инструкции осуществляется администратором информационной безопасности.