УТВЕРЖДАЮ
Директор ГБУ СО ЯО
Красноперекопский
психоневрологический
интернат

_____ М.В.Филиппова
«10» 01 2020 г.

ИНСТРУКЦИЯ

по организации антивирусной защиты в государственном учреждении социального обслуживания Ярославской области Красноперекопский психоневрологический интернат

1. Настоящая Инструкция определяет требования к организации антивирусной защиты информационных систем персональных данных Государственного бюджетного учреждения социального обслуживания Ярославской области Красноперекопский психоневрологический интернат (далее – учреждение).

2. Настоящая Инструкция предназначена для должностного лица, ответственного за обработку персональных данных, и пользователей, осуществляющих обработку персональных данных в Учреждении.

3. В целях обеспечения защиты от деструктивных воздействий компьютерных вредоносных программ производится антивирусный контроль. Обязательному антивирусному контролю подлежит любая информация, поступающая на средства вычислительной техники, в том числе получаемая на внешних носителях из сторонних организаций.

4. Вредоносная программа - программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на ресурсы информационных систем.

5. Основными задачами системы обеспечения антивирусной защиты являются:

- исключение или существенное затруднение противоправных действий в отношении информационных системах персональных данных Учреждения как носителей защищаемой информации;

- обеспечение условий для устойчивой бесперебойной работы объектов, сетей передачи данных.

6. Обеспечение антивирусной защиты включает:

- регулярные профилактические работы;

- анализ ситуации проявления вредоносных программ и причины их появления;

- уничтожение вредоносных программ на автоматизированных рабочих местах

- принятие мер по предотвращению причин появления вредоносных программ.

7. К использованию в организации допускаются только лицензионные антивирусные средства, централизованно закупленные у разработчиков (поставщиков) указанных средств.

8.Установка средств антивирусного контроля на компьютерах осуществляется уполномоченным сотрудником организации. Настройка параметров средств антивирусного контроля в соответствии с руководствами по применению конкретных антивирусных средств.

9. Ежедневно в начале работы при загрузке компьютера в автоматическом режиме должен проводиться антивирусный контроль всех дисков и файлов.

10. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях (магнитных дисках, CD-ROM и т.п.).

11. Контроль входящей и исходящей информации на защищаемых серверах и персональных компьютерах (далее ПК) осуществляется непрерывно посредством постоянно работающего компонента антивирусного программного обеспечения («монитора»). Полная проверка информации, хранящейся на серверах и ПК должна осуществляться не реже одного раза в месяц.

12. Обновление баз вирусов антивирусного программного обеспечения, установленного на ПК и серверах, должно осуществляться регулярно.

13.В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов сотрудники обязаны:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов руководителя и ответственного за обработку персональных данных в учреждении, владельца зараженных файлов, а также сотрудников, использующих эти файлы в работе;
- совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;
- провести лечение или уничтожение зараженных файлов.

14. Ответственность за антивирусный контроль в организации, в соответствии с требованиями настоящей Инструкции возлагается на руководителя организации.

15.Ответственность за проведение мероприятий антивирусного контроля в подразделении и соблюдение требований настоящей Инструкции возлагается на ответственных за обработку персональных данных и всех сотрудников, являющихся пользователями информационных систем.

16.Периодический контроль за состоянием антивирусной защиты, а также за соблюдением установленного порядка антивирусного контроля и выполнением требований настоящей Инструкции сотрудниками осуществляется ответственным за обработку персональных данных в учреждении.