БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ РЕСПУБЛИКИ КАЛМЫКИЯ
«РЕСПУБЛИКАНСКИЙ ДЕТСКИЙ МЕДИЦИНСКИЙ ЦЕНТР
ИМЕНИ МАНДЖИЕВОЙ ВАЛЕНТИНЫ ДЖАЛОВНЫ»

ПРИКАЗ

«23» января 2024 г. № 58

г. Элиста

**Об организации системы
антивирусной защиты информации**

В соответствии с Федеральным законом от 27.06.2007 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», приказа ФСТЭК от 05.02.2010 г. № 58 «Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных»,

п р и к а з ы в а ю :

1. Утвердить Инструкцию по организации системы антивирусной защиты информации в БУ РК «Республиканский детский медицинский центр имени Манджиевой Валентины Джаловны» (далее - Инструкция) (Приложение № 1).
2. Назначить администраторами средств антивирусной защиты системного программиста Сельдикова Б.П., техников-программистов Максимова С.Л. и Пюрбеева С.В.
3. Начальникам структурных подразделений обеспечить:
   1). ознакомление должностных лиц подразделений с настоящим приказом под роспись;
   2). безусловное выполнение требований Инструкции.
4. Признать утратившим силу приказ БУ РК «РДМЦ им. Манджиевой В.Д.» от 29.05.2023г. № 323 «Об организации системы антивирусной защиты информации».
5. Контроль за исполнением настоящего приказа оставляю за собой.

Главный врач Дорджиев А.Н.

Приложение № 1
к приказу БУ РК «РДМЦ
им. Манджиевой В.Д.»
от 23.01.2024г. № 58

Инструкция
по организации системы антивирусной защиты информации

Данная инструкция регламентирует организацию действий и мероприятий, направленных на обеспечение функционирования системы антивирусной защиты информации в БУ РК «Республиканский детский медицинский центр имени Манджиевой Валентины Джаловны» (далее – БУ РК «РДМЦ им. Манджиевой В.Д.»).

1.Система антивирусной защиты информации предназначена для предотвращения заражения программными вирусами информационно-вычислительных ресурсов БУ РК «РДМЦ им. Манджиевой В.Д.».

2.Антивирусная защита информации в БУ РК «РДМЦ им. Манджиевой В.Д.» осуществляется посредством применения организационных мер и средств антивирусной защиты информации.

3.Выполнение мероприятий по организации антивирусной защиты информации в структурных подразделениях БУ РК «РДМЦ им. Манджиевой В.Д.» осуществляет ответственный за эксплуатацию антивирусных средств защиты (далее – администратор АВЗ), назначаемый соответствующим приказом с обязательным отражением этих обязанностей в должностном регламенте.
Администратор АВЗ несет ответственность:

- за своевременную инсталляцию средств антивирусной защиты информации;
- за эксплуатацию средств антивирусной защиты информации;
- за обновление баз данных средств антивирусной защиты. Администратор АВЗ

осуществляет контроль:

- за эксплуатацией средств антивирусной защиты информации в структурных подразделениях БУ РК «РДМЦ им. Манджиевой В.Д.»;
- за регулярностью обновления антивирусных баз и средств антивирусной защиты.

4.Непосредственную ответственность за соблюдение в повседневной деятельности установленных норм обеспечения антивирусной защиты информации на своих рабочих местах, в том числе за обновление антивирусных баз и получение новых лицензионных ключей несут пользователи.

Пользователям запрещается:

- отключать средства антивирусной защиты информации во время работы;
- использовать средства антивирусной защиты информации, не включённые в Перечень сертифицированных средств защиты информации.

5.Состояние антивирусной защиты отражается в отчёте о состоянии информационной безопасности БУ РК «РДМЦ им. Манджиевой В.Д.» с обязательным указанием выявленных нарушений, вызванных заражением информации программными вирусами, причин появления и характера вирусов, последствий их воздействия и принятых мер.

6.Передача полученных средств антивирусной защиты на объекты, не входящие в состав БУ РК «РДМЦ им. Манджиевой В.Д.», запрещена. За несанкционированное распространение средств антивирусной защиты виновные несут ответственность в соответствии с законодательством Российской федерации.

7.Порядок применения средств антивирусной защиты информации устанавливается с учётом соблюдения следующих требований:

- обязательный входной контроль за отсутствием программных вирусов во всех поступающих на объект информатизации машинных носителях информации, информационных массивах, программных средствах общего и специального назначения;
- обязательная проверка всех электронных писем на предмет отсутствия

программных вирусов;

- периодическая проверка на предмет отсутствия программных вирусов жёстких магнитных дисков (не реже одного раза в неделю) и обязательная проверка используемых в работе гибких магнитных дисков, флэш-накопителей перед началом работы с ними;

8. Средства антивирусной защиты информации должны устанавливаться на всех средствах вычислительной техники, эксплуатируемых в БУ РК «РДМЦ им. Манджиевой В.Д.». В первую очередь их устанавливают на сервере баз данных, почтовом сервере, и на рабочих станциях, подключённых к информационно-вычислительным сетям общего пользования.

9. На рабочем месте администратора АВЗ должны быть установлены средства, позволяющие через локальную вычислительную сеть управлять компонентами системы антивирусной защиты информации, установленными на рабочих станциях и сервере локальной вычислительной сети БУ РК «РДМЦ им. Манджиевой В.Д.».

10. Инсталляция и настройка средств антивирусной защиты информации осуществляется в соответствии с программной и эксплуатационной документацией, поставляемой в комплекте с ними.

11. Своевременное обновление баз данных средств антивирусной защиты информации является неотъемлемой частью обеспечения эффективной антивирусной защиты информации.

Обновление баз данных средств антивирусной защиты информации осуществляется централизованно через сервер БУ РК «РДМЦ им. Манджиевой В.Д.» ежечасно. В случае, когда рабочая станция не входит в состав ЛВС, обновление баз данных средств антивирусной защиты производится локально не реже одного раза в неделю.

12. В случае обнаружения вирусов при входном контроле гибких магнитных носителей, флэш-накопителей, файлов или почтовых сообщений, поступивших в структурные подразделения БУ РК «РДМЦ им. Манджиевой В.Д.», пользователь должен:

- сообщить администратору АВЗ о факте обнаружения программного вируса;
- принять меры для локализации и удаления программных вирусов с использованием средств антивирусной защиты информации;
- сообщить о факте обнаружения программных вирусов в таможенный орган или организацию, из которых поступили заражённые гибкие магнитные носители, файлы, почтовые сообщения.

13. При обнаружении программных вирусов в процессе обработки информации пользователь обязан:

- немедленно прекратить все работы;
- сообщить администратору АВЗ о факте обнаружения программных вирусов;
- принять меры для локализации и удаления программных вирусов с использованием средств антивирусной защиты информации.

14. Программные средства общего и специального назначения объекта информатизации, используемые для обработки информации, отнесённой к государственной или служебной тайне, в случае обнаружения программных вирусов подлежат переустановке с рабочих копий эталона.

15. При невозможности ликвидации последствий заражения программными вирусами необходимо:

- заархивировать файлы с внедрёнными программными вирусами и направить их с приложением соответствующего сопроводительного документа в организацию, осуществляющую техническую поддержку эксплуатации средств антивирусной защиты;
- осуществить полную переустановку программного обеспечения на заражённой ПЭВМ.