Приложение №5
к приказу ГАУЗ ТО
«Городская поликлиника №6»
от 26.01.2024 № 35

Положение
об антивирусной защите информационных систем и рабочих станций пользователей ГАУЗ ТО «Городская поликлиника №6»

1. Общие положения

1.1. Система антивирусной защиты информации предназначена для предотвращения заражения программными вирусами информационных систем и автоматизированных рабочих мест пользователей корпоративной сети передачи данных (далее - КСПД).

1.2. Антивирусная защита информации осуществляется посредством применения организационных мер, а также технических средств антивирусной защиты информации.

1.3. Требования настоящего Положения обязательны для выполнения всеми должностными лицами и работниками Учреждения.

2. Организационная структура системы антивирусной защиты информации:

2.1. Учреждение антивирусной защиты, анализ ее состояния, осуществляется администратором информационной безопасности.

2.2. Выполнение мероприятий по организации антивирусной защиты информации на рабочих станциях пользователей осуществляет администратор антивирусной защиты (далее - администратор АВЗ), назначаемый приказом с отражением этих обязанностей в должностной инструкции. Выполнение указанных мероприятий в части серверного оборудования осуществляется в присутствии администратора данного сервера.

2.3. Администратор АВЗ несет ответственность:

- за своевременную инсталляцию средств антивирусной защиты информации;
- за правильную эксплуатацию средств антивирусной защиты информации;
- за обновление баз данных средств антивирусной защиты на рабочих местах пользователей.

2.4. Непосредственную ответственность за соблюдение в повседневной деятельности установленных норм обеспечения антивирусной защиты информации на серверах несет администратор данных серверов.

2.5. Непосредственную ответственность за соблюдение в повседневной деятельности установленных норм обеспечения антивирусной защиты информации на своих рабочих местах несут пользователи.

2.6. Пользователям запрещается:

- отключать средства антивирусной защиты информации во время работы;

- самостоятельно устанавливать на служебные персональные компьютеры любое программное обеспечение.

2.7. Пользователям рекомендуется:

- не создавать самораспаковывающиеся архивы;
- использовать для хранения офисных документов форматы файлов, не содержащих кодов макрокоманд HTML, RTF и др.

2.8. Нелегальное распространение и/или установка антивирусного программного обеспечения запрещена. За несанкционированное распространение средств антивирусной защиты виновные несут ответственность в соответствии с законодательством Российской Федерации.

3. Порядок применения средств антивирусной защиты информации

3.1. Порядок применения средств антивирусной защиты информации устанавливается с учетом соблюдения следующих требований:

- обязательный входной контроль за отсутствием программных вирусов во всех поступающих на машинных носителях информации;
- обязательная проверка всех электронных писем на предмет отсутствия программных вирусов;
- периодическая проверка на предмет отсутствия программных вирусов жестких магнитных дисков (не реже одного раза в месяц) и обязательная проверка используемых в работе съемных накопителей (флэш-карты) перед началом работы с ними;
- внеплановая проверка магнитных носителей информации в случае подозрения на наличие программных вирусов;
- восстановление работоспособности программных средств и информационных массивов, поврежденных программными вирусами.

3.2. Средства антивирусной защиты информации должны устанавливаться на всех средствах вычислительной техники, серверном оборудовании, в том числе на серверах баз данных, почтовых серверах, рабочих станциях.

3.3. На рабочем месте администратора АВЗ должны быть установлены средства, позволяющие на расстоянии управлять компонентами системы антивирусной защиты информации, установленными на рабочих станциях и серверах сегментов локальных вычислительных сетей.

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

4. Действия при обнаружении программных вирусов

4.1. В случае обнаружения программных вирусов пользователь должен:

- прекратить процесс приема-передачи информации;
- сообщить администратору АВЗ и ответственному 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 отправителю, от которого поступили зараженные гибкие магнитные носители, файлы или почтовые сообщения.