Министерство образования, науки и молодежи Республики Крым
Государственное бюджетное специализированное учреждение Республики Крым
«Керченский межрегиональный социально-реабилитационный центр для несовершеннолетних»

УТВЕРЖДЕНО
Приказом и. о директора
ГБСУ РК «Керченский
МСРЦН» №241-ХД
«01» 09 2020 года

ИНСТРУКЦИЯ
по организации антивирусной защиты информационных систем ГБСУ РК «Керченский МСРЦН»

1. ОБЩИЕ ПОЛОЖЕНИЯ

Настоящая Инструкция определяет требования к организации защиты информационных систем (далее - ИС) Государственного бюджетного специализированного учреждения Республики Крым «Керченский межрегиональный социально-реабилитационный центр для несовершеннолетних» (далее - Центр) от воздействия защищаемых вирусов и устанавливает ответственность начальников и работников отделов, эксплуатирующих и сопровождающих ИС, за их выполнение.

К использованию в ИС допускаются только лицензионные и сертифицированные антивирусные средства, закупленные у разработчиков (поставщиков) указанных средств, рекомендованные к применению ответственным за защиту информации.

В случае необходимости использования антивирусных средств, не вошедших в перечень рекомендованных, их применение необходимо согласовать с ответственным за защиту информации.

Установка средств антивирусной защиты на автоматизированных рабочих местах (далее – АРМ) осуществляется администратором информационной безопасности (далее – Администратор ИБ) в соответствии с «Инструкция по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств информационных систем…» Организации. Настройка параметров средств антивирусной защиты осуществляется Администратором ИБ в соответствии с руководствами по применению конкретных антивирусных средств.

2. ПРИМЕНЕНИЕ СРЕДСТВ АНТИВИРУСНОГО КОНТРОЛЯ

Антивирусный контроль всех дисков и файлов ИС после загрузки АРМ должен проводиться в автоматическом режиме (периодическое сканирование или мониторинг).

Периодически, не реже одного раза в месяц, должен проводиться полный антивирусный контроль всех дисков и файлов ИС (сканирование).

Обязательной антивирусной защите подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая информация на съемных носителях (магнитных дисках, CD-ROM и т.п.). Разархивирование и контроль входящей информации необходимо проводить непосредственно после ее приема. Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

Файлы, помещаемые в электронный архив должны в обязательном порядке проходить антивирусный контроль. Периодические проверки электронных архивов должны проводиться не реже одного раза в месяц.

Установка (изменение) системного и прикладного программного обеспечения (далее - ПО) осуществляется в соответствии с «Инструкция по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств информационных систем…»

Организации. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено Администратором ИБ на отсутствие вирусов. Непосредственно после установки (изменения) ПО АРМ должна быть выполнена антивирусная проверка жестких дисков АРМ лицом, установившим (изменившим) ПО, под контролем Администратора ИБ.

Факт выполнения антивирусной проверки после установки (изменения) ПО должен регистрироваться в специальном журнале за подписью лица, установившего (изменившего) ПО, и лица, его контролировавшего.

3. ДЕЙСТВИЯ РАБОТНИКОВ ПРИ ПОДОЗРЕНИИ НАЛИЧИЯ 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.) работник отдела самостоятельно или вместе с Администратором ИБ должен провести внеочередной антивирусный контроль АРМ. При необходимости он должен привлечь Администратора ИБ для определения ими факта наличия или отсутствия компьютерного вируса.

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

- приостановить работу;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов начальника отдела и Администратора ИБ, владельца зараженных файлов, а также смежные отделы, использующие эти файлы в работе;
- совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;
- провести лечение или уничтожение зараженных файлов (при необходимости для выполнения требований данного пункта привлечь администратора информационной безопасности);
- в случае обнаружения нового вируса, не поддающегося лечению применяемыми антивирусными средствами, передать зараженный вирусом файл на съемном носителе информации ответственному за защиту информации для дальнейшей передачи его в организацию, с которой заключен договор на антивирусную поддержку (при необходимости, для выполнения требований данного пункта привлечь Администратора ИБ);
- по факту обнаружения зараженных вирусом файлов составить служебную записку ответственному за защиту информации, в которой необходимо указать предположительный источник (отправителя, владельца и т.д.) зараженного файла, тип зараженного файла, характер содержащейся в файле информации, тип вируса и выполненные антивирусные мероприятия.

4. ПОРЯДОК ОБНОВЛЕНИЯ АНТИВИРУСНЫХ БАЗ

Обновление антивирусных баз должно проводиться регулярно, с периодичностью определенной технологией работы в ИС.

Обновление антивирусных баз ИС АРМ имеющих подключение к сети международного телекоммуникационного обмена Интернет, осуществляется с сервера производителя антивирусного ПО ежедневно.

Обновлению подлежат только антивирусные базы.

5. ОТВЕТСТВЕННОСТЬ

Ответственность за организацию антивирусной защиты в отделах, эксплуатирующих ИС, в соответствии с требованиями настоящей Инструкции возлагается на начальников отделов.

Ответственность за проведение мероприятий антивирусного контроля в отделах и соблюдение требований настоящей Инструкции возлагается на ответственного за защиту информации в организации и всех работников, являющихся пользователями ИС.

Периодический контроль за состоянием антивирусной защиты в ИС, а также за соблюдением установленного порядка антивирусного контроля и выполнением требований настоящей Инструкции работниками Организации осуществляется ответственным за защиту информации.