«Утверждаю»

Директор школы

Е.С. Мириуца

ПРИЛОЖЕНИЕ 6 к приказу
№___ от_____
об организационных мерах
для защиты персональных данных

ИНСТРУКЦИЯ ПО ОРГАНИЗАЦИИ АНТИВИРУСНОЙ ЗАЩИТЫ

Настоящая Инструкция определяет требования к организации защиты информации в информационной системе МБОУ Великооктябрьская СОШ от разрушающего воздействия компьютерных вирусов, червей и "троянских" программ, а также устанавливает ответственность сотрудников, эксплуатирующих информационную систему, за их выполнение.

1. Организация антивирусной защиты.

Антивирусная защита информационной системы должна осуществляться антивирусным программным обеспечением (ПО), полученным (закупленным) в централизованном порядке. Другие лицензионные антивирусные программы могут использоваться только в исключительных случаях в качестве дополнительного средства контроля и защиты. Установка программных средств и настройка параметров антивирусного контроля осуществляется в соответствии с руководствами по применению конкретных антивирусных средств. Ответственность за своевременную установку и переустановку антивирусного ПО, поддержание его в рабочем состоянии, своевременное обновление антивирусных баз возлагается на администратора.

2. Применение средств антивирусной защиты.

Необходимость установки средств антивирусной защиты на конкретное автоматизированное рабочее место определяется администратором. В случаях, когда автоматизированное рабочее место имеет доступ к сети, либо в процессе работы используются съемные носители информации - наличие средств антивирусной защиты на данном автоматизированном рабочем месте обязательно. Установку и настройку антивирусного ПО осуществляет администратор. Пользователю запрещается самостоятельно изменять настройки антивирусного ПО. Пользователь обязан регулярно проверять свои рабочие папки на жестком магнитном диске ПЭВМ, а также свои рабочие съемные носители информации (дискеты, флеш-накопители и др.) на отсутствие вирусов с помощью штатных средств антивирусного ПО. Периодичность контроля определяется администратором, исходя из возможностей и настроек рабочего антивирусного ПО. Носители информации других пользователей подлежат обязательной проверке на вирусы непосредственно перед началом работы с ними. Антивирусному контролю подлежат все файлы без исключения (текстовые, графические, исполняемые, архивные, служебные, системные). Разархивирование и обработку входящей информации необходимо проводить после ее проверки на наличие компьютерных вирусов непосредственно на носителе содержащем эту информацию.

3. Действия при обнаружении вирусов.

При возникновении подозрения на наличие компьютерного вируса, пользователь самостоятельно или совместно с администратором должен провести внеочередной антивирусный контроль носителей информации. В случае обнаружения антивирусным ПО зараженного компьютерным вирусом файла пользователь обязан:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения вируса администратора 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.

4. Ответственность за состояние антивирусной защиты

Ответственность за организацию антивирусной защиты информационной системы, возлагается на администратора, ответственность за эксплуатацию средств защиты возлагается на постоянных пользователей информационной системы. Обязанности администратора изложены в должностной инструкции администратора сети.