7.7.

Рассмотрено на
педагогическом совете
Протокол № 1 от «29» августа 2012 г.

Утверждаю
Директор МБОУ «СОШ № 42»
_____ Бастрикова О.А.
Приказ №111 от «01» сентября 2012 г.

Инструкция
по организации защиты автоматизированных рабочих мест от разрушающего воздействия компьютерных вирусов
в МБОУ «СОШ № 42» Энгельсского муниципального района Саратовской области

1 .1. Настоящая инструкция определяет требования к организации защиты автоматизированных рабочих мест от разрушающего воздействия компьютерных вирусов и устанавливает ответственность руководителей и сотрудников МБОУ «Средняя общеобразовательная школа № 42», эксплуатирующих автоматизированные рабочие места, за выполнение этих требований.

1.2. К использованию на автоматизированных рабочих местах допускаются только лицензионные антивирусные средства, централизованно закупленные у разработчиков (поставщиков) указанных средств и согласованных с администратором безопасности информации образовательного учреждения. Установка средств антивирусного контроля на автоматизированных рабочих местах осуществляется администратором безопасности информации. Настройка параметров средств антивирусного контроля осуществляется администратором безопасности информации в соответствии с руководствами инструкции применению конкретных антивирусных средств.

1.3. Применение средств антивирусного контроля.

1.3.1. Перед началом работы на ПЭВМ пользователь обязан проверить свои рабочие папки на жестком магнитном диске (ЖМД), собственные рабочие съемные машинные носители информации (МНИ) на отсутствие вирусов с помощью штатных средств антивирусной защиты.

1.3.2.0бязательному антивирусному контролю подлежит любая получаемая и передаваемая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы) на съемных носителях (дискетах, компакт-дисках, флэш-накопителях и т.п.). Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на системный носитель).

1.3.3. Файлы, помещаемые в электронный архив должны в обязанном порядке проходить антивирусный контроль. Периодические проверки

электронных архивов должны проводиться **не реже одного раза в месяц.**

1.3.4. Вновь устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения компьютера должна быть выполнена антивирусная проверка жестких дисков ПЭВМ.

1.4. Действия пользователя при подозрении наличия компьютерного вируса.

1.4.1. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание фактов, частное появление сообщений о системных ошибках и т.п.) пользователи автоматизированных рабочих мест самостоятельно или вместе с ответственным за осуществление защиты информационных систем персональных данных и их эксплуатации ответственного за организацию, координацию и контроль проведения мероприятий по защите персональных данных должны провести внеочередной антивирусный контроль ПЭВМ.

1.4.2. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователь обязан:

- приостановить работу;

- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов ответственного за безопасности информации (администратора: безопасности информации).

1 .4.3. Ответственный за безопасность информации обязан:

- совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;

- провести лечение или уничтожение зараженных файлов;

- по факту обнаружения зараженных вирусом файлов пользователь, обязан составить служебную записку на имя руководителя образовательного учреждения, 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.

1.5. Ответственность

1.5.1. Ответственность за организацию антивирусного контроля на автоматизированных рабочих местах в соответствии с требованиями настоящей Инструкции возлагается на ответственного за организацию координации и контроль проведения мероприятий по защите персональных данных,

1.5.2. Ответственность за проведение мероприятий антивирусного контроля и соблюдение требований настоящей Инструкции возлагается на ответственного за организацию, координацию и контроль проведения мероприятий по защите персональных данных и пользователя автоматизированного рабочего места.

1.5.3. Периодический контроль за состоянием антивирусной защиты в автоматизированных рабочих местах, а также за соблюдением установленного порядка антивирусного контроля и выполнением требований настоящей Инструкции пользователем осуществляется администратором безопасности информации.

Ответственный за организацию, координацию и контроль проведения мероприятий по защите персональных данных _____

(подпись)