Принята на заседании
педагогического совета
Протокол № 1 от 31.08.2020

Утверждаю:
Директор МБОУ «Каменская СОШ» Л.П.Черных
(приказ от 12 сентября 2020 года № 216-од)

ИНСТРУКЦИЯ
по организации антивирусной защиты в муниципальном бюджетном общеобразовательном учреждении «Каменская средняя общеобразовательная школа»

1. Общие положения

1.1 Настоящая инструкция определяет требования к организации защиты информационной системы муниципального бюджетного общеобразовательного учреждения «Каменская средняя общеобразовательная школа» (далее по тексту – ИС) от разрушающего воздействия компьютерных вирусов и устанавливает ответственность работников, эксплуатирующих и сопровождающих ИС.

1.2 К использованию в МБОУ «Каменская СОШ» (далее - ОО) допускаются только лицензионные антивирусные средства, централизованно закупленные у разработчиков (поставщиков) указанных средств.

1.3 Установка, настройка и обновление средств антивирусного контроля на компьютерах осуществляется уполномоченными работниками, назначенными приказом директора ОО.

2. Применение средств антивирусного контроля

2.1 Ежедневно в начале работы при загрузке компьютера в автоматическом режиме должен проводиться антивирусный контроль всех дисков и файлов.

2.2 Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях (магнитных дисках, лентах, CD-ROM и т.п.). Разархивирование и контроль входящей информации необходимо проводить непосредственно после ее приема на выделенном автономном компьютере или, при условии начальной загрузки операционной системы в оперативную память компьютера с заведомо «чистой» (не зараженной вирусами) и защищенной от записи системной дискеты, на любом другом компьютере. Возможно применение другого способа антивирусного контроля входящей информации, обеспечивающего аналогичный уровень эффективности контроля. Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

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

2.4 Установка (изменение) системного и прикладного программного обеспечения осуществляется уполномоченными работниками. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения компьютера должна быть выполнена антивирусная проверка.

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

2.5 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

самостоятельно или вместе с ответственным за антивирусную защиту должен провести внеочередной антивирусный контроль своей рабочей станции.

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

- приостановить работу;

- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов директора ОО и ответственного за антивирусную защиту, владельца зараженных файлов, а также других работников, использующих эти файлы;

- 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 ответственного за антивирусную защиту);

- в случае обнаружения нового вируса, не поддающегося лечению применяемыми антивирусными средствами, направить зараженный вирусом файл ответственному за антивирусную защиту для дальнейшей передачи его в организацию, с которой заключен договор на антивирусную поддержку;

- по факту обнаружения зараженных вирусом файлов составить служебную записку ответственному за антивирусную защиту, 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.

3. Ответственность

3.1 Ответственность за проведение мероприятий антивирусного контроля и соблюдение требований настоящей инструкции возлагается на ответственного за антивирусную защиту и всех работников ОО, являющихся пользователями ИС.

3.2 Периодический контроль за состоянием антивирусной защиты в ИС, а также за соблюдением установленного порядка антивирусного контроля и выполнением требований настоящей инструкции работниками ОО осуществляет заместитель директора по УВР.