

## ИНСТРУКЦИЯ

### по организации антивирусной защиты в Муниципальном бюджетном общеобразовательном учреждении Ломовской школе

1. Настоящая Инструкция определяет требования к организации защиты по организации антивирусной защиты в МБОУ Ломовской школе (далее - учреждение) от разрушающего воздействия компьютерных вирусов и устанавливает ответственность руководителей и сотрудников учреждения за их выполнение.
2. К использованию в учреждение допускаются только лицензионные антивирусные средства, централизованно закупленные у разработчиков (поставщиков) указанных средств.
3. Установка средств антивирусного контроля на компьютерах осуществляется уполномоченным сотрудником учреждения. Настройка параметров средств антивирусного контроля в соответствии с руководствами по применению конкретных антивирусных средств.
4. Ежедневно в начале работы при загрузке компьютера в автоматическом режиме должен проводиться антивирусный контроль всех дисков и файлов.
5. 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, CD-ROM и т.п.).
6. Контроль входящей и исходящей информации на защищаемых серверах и персональных компьютерах (далее ПК) осуществляется непрерывно посредством постоянно работающего компонента антивирусного программного обеспечения («монитора»). Полная проверка информации хранящейся на серверах и ПК должна осуществляться не реже одного раза в месяц.
7. Обновление баз вирусов антивирусного программного обеспечения, установленного на ПК и серверах, должно осуществляться еженедельно.
8. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения компьютера (локальной вычислительной сети), должна быть выполнена антивирусная проверка:
  - на защищаемом автоматизированном рабочем месте (АРМ) - ответственным за обеспечение информационной безопасности.
1. 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.) сотрудник учреждения самостоятельно или вместе с ответственным за антивирусную защиту учреждения должен провести внеочередной антивирусный контроль своей рабочей станции.
2. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов сотрудники подразделений обязаны:
  - приостановить работу;
  - немедленно поставить в известность о факте обнаружения зараженных вирусом файлов руководителя и ответственного за антивирусную защиту учреждения, владельца зараженных файлов, а также сотрудников, использующих эти файлы в работе;
  - совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;

- провести лечение или уничтожение зараженных файлов.

1. Ответственность за организацию антивирусного контроля в учреждение, в соответствии с требованиями настоящей Инструкции возлагается на руководителя учреждения.
2. Ответственность за проведение мероприятий антивирусного контроля в подразделении и соблюдение требований настоящей Инструкции возлагается на ответственного за антивирусную защиту учреждения и всех сотрудников, являющихся пользователями ПК учреждения.
3. Периодический контроль за состоянием антивирусной защиты в учреждение, а также за соблюдением установленного порядка антивирусного контроля и выполнением требований настоящей Инструкции сотрудниками учреждения осуществляется ответственным за антивирусную защиту учреждения.