Муниципальное казенное общеобразовательное учреждение

«Усть-Пустынская средняя школа»

|  |  |
| --- | --- |
|  | «УТВЕРЖДАЮ»Директор МКОУ «Усть-Пустынская СОШ»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Е.М. ПодзороваПриказ №\_\_\_\_\_ от «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_20\_\_\_\_г.  |

ИНСТРУКЦИЯ

ПО ОРГАНИЗАЦИИ АНТИВИРУСНОЙ ЗАЩИТЫ

С.Усть-Пустынка

2015

1.ОБЩИЕ ПОЛОЖЕНИЯ

1. В образовательном учреждении руководителем должно быть назначено лицо ответственное за антивирусную защиту. В противном случае вся ответственность за обеспечение антивирусной защиты ложится на руководителя образовательного учреждения.

2. В образовательной организации может использоваться только лицензионное антивирусное программное обеспечение.

3. 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.). Контроль исходящей информации необходимо проводить непосредственно
перед архивированием и отправкой (записью на съемный носитель).

4. Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить
антивирусный контроль.

5. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно
проверено на отсутствие вирусов.

6. Факт выполнения антивирусной проверки после установки (изменения) программного
обеспечения должен регистрироваться в специальном журнале за подписью лица, ответственного за антивирусную защиту.

2. ТРЕБОВАНИЯ

К ПРОВЕДЕНИЮ МЕРОПРИЯТИЙ ПО АНТИВИРУСНОЙ ЗАЩИТЕ

1. Ежедневно в начале работы при загрузке компьютера (для серверов ЛВС — при перезапуске) в автоматическом режиме должно выполняться обновление антивирусных баз и проводиться антивирусный контроль всех дисков и файлов персонального компьютера.
2. Периодические проверки электронных архивов должны проводиться не реже одного раза в неделю.
3. Внеочередной антивирусный контроль всех дисков и файлов персонального компьютера должен выполняться:

• Непосредственно после установки (изменения) программного обеспечения компьютера (локальной вычислительной сети), должна быть выполнена антивирусная проверка: на серверах и персональных компьютерах образовательного учреждения. 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.
• 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.).

4.В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователи обязаны:
• приостановить работу;
• немедленно поставить в известность о факте обнаружения зараженных вирусом файлов ответственного за обеспечение информационной безопасности в образовательном учреждении;
• совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;
• провести лечение или уничтожение зараженных файлов;
• в случае обнаружения нового вируса, не поддающегося лечению применяемыми антивирусными средствами, ответственный за антивирусную защиту обязан направить зараженный вирусом файл на гибком магнитном диске в организацию, с которой заключен договор на антивирусную поддержку для дальнейшего исследования;

3.ОТВЕТСТВЕННОСТЬ

1.Ответственность за организацию антивирусной защиты возлагается на руководителя образовательного учреждения или лицо им назначенное.
2.Ответственность за проведение мероприятий антивирусного контроля в подразделении и соблюдение требований настоящей Инструкции возлагается на ответственного за обеспечение антивирусной защиты.
3.Периодический контроль за состоянием антивирусной защиты в образовательном учреждении осуществляется руководителем.