

## **Инструкция по организации антивирусной защиты в МАДОУ № 30**

### **1. Общие положения**

- 1.1 В учреждении заведующий назначает лицо ответственное за антивирусную защиту.
- 1.2 В учреждении используется лицензионное антивирусное программное обеспечение.
- 1.3 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).
- 1.4 Файлы, помещаемые в электронный архив, в обязательном порядке проходить антивирусный контроль.
- 1.5 Устанавливаемое (изменяемое) программное обеспечение предварительно проверяется на отсутствие вирусов.
- 1.6 Факт выполнения антивирусной проверки после установки (изменения) программного обеспечения регистрируется в специальном журнале за подписью лица, ответственного за антивирусную защиту.

### **2. Требования к проведению мероприятий по антивирусной защите**

- 2.1 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.
- 2.2 Периодические проверки электронных архивов проводятся не реже одного раза в неделю.
- 2.3 Внеочередной антивирусный контроль всех дисков и файлов персонального компьютера выполняется:
  - Непосредственно после установки (изменения) программного обеспечения компьютера (локальной вычислительной сети), выполняется антивирусная проверка: на персональных компьютерах образовательного учреждения. Факт выполнения антивирусной проверки после установки (изменения) программного обеспечения регистрируется в специальном журнале за подписью лица, установившего (изменившего) программное обеспечение, и лица, его контролирувавшего.
  - 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.).

2.4 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 учреждении;

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

провести лечение или уничтожение зараженных файлов;

### **3. Ответственность**

3.1 Ответственность за организацию антивирусной защиты возлагается на заведующего учреждения или лицо им назначенное.

3.2 Ответственность за проведение мероприятий антивирусного контроля и соблюдение требований настоящей Инструкции возлагается на ответственного за обеспечение антивирусной защиты.

3.3 Периодический контроль за состоянием антивирусной защиты в учреждении осуществляется заведующим.