

**МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ СРЕДНЯЯ
ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА № 4
ИМЕНИ ЛАРИСЫ ИВАНОВНЫ ЗОЛОТУХИНОЙ
(МБОУ СОШ № 4 имени Л.И. Золотухиной)**

РАССМОТРЕНО
Педагогическим советом
Протокол № 1
от «31» 09 2020 г.

СОГЛАСОВАНО
Управляющим советом
протокол № 2
от «31» 09 2020 г.

УТВЕРЖДАЮ
Директор Н.П. Буркацкая
Приказ № 474-15-40210
от «04» 09 2020 г.



РЕГЛАМЕНТ

по организации антивирусной защиты средств автоматизации в образовательном учреждении

1. Общие положения.

- 1.1. Директор Муниципального бюджетного общеобразовательного учреждения средней школы №4 имени Л.И. Золотухиной (далее – МБОУ СОШ №4 имени Л.И. Золотухиной) назначает лицо, ответственное за антивирусную защиту средств информатизации.
- 1.2. В МБОУ СОШ №4 имени Л.И. Золотухиной может использоваться только лицензионное антивирусное программное обеспечение в соответствии с требованиями действующего законодательства РФ.
- 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, 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, должны в обязательном порядке проходить антивирусный контроль.
- 1.5. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов.
- 1.6. 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

- 2.1. Ежедневно в начале работы при загрузке компьютера, в автоматическом режиме должно выполняться обновление антивирусных баз, и проводиться антивирусный контроль всех дисков и файлов персонального компьютера.
- 2.2. Периодические проверки электронных архивов должны проводиться не реже одного раза в неделю.
- 2.3. Внеочередной антивирусный контроль всех дисков и файлов персонального компьютера должен выполняться:
 - непосредственно после установки (изменения) программного обеспечения компьютера, должна быть выполнена антивирусная проверка: на сервере и персональных компьютерах ОО. Факт выполнения антивирусной проверки, после установки (изменения) программного обеспечения, должен регистрироваться 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 пользователя обязаны:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов ответственного за обеспечение информационной безопасности в ОО;
- совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;
- провести лечение или уничтожение зараженных файлов.

3. Профилактика заражения

3.1. Одним из основных методов борьбы с вирусами является своевременная профилактика, состоящая из соблюдения следующих правил. Защитить компьютер с помощью антивирусных программ и программ безопасной работы в Интернете. Для этого:

- установить антивирусную программу;
- обновлять регулярно сигнатуры угроз, входящие в состав программы;
- не выгружать из памяти и не останавливать работу антивирусной программы.

3.2. Проявлять осторожность при записи новых данных на компьютер:

- проверить на присутствие вирусов все съемные диски (дискеты, CD–диски, флэш – карты и пр.) перед их использованием;
- не запускать никаких файлов, пришедших по почте, не проверенных с помощью антивирусной программы;
- обратить внимание на наличие сертификата безопасности при установлении новой программы с какого-либо веб-сайта;
- проверить с помощью антивирусной программы копируемый из Интернета или локальной сети исполняемый файл;
- пользоваться сервисом Windows Update и регулярно устанавливать обновления операционной системы Microsoft Windows;
- создать диск аварийного восстановления, с которого при необходимости можно будет загрузиться, используя «чистую» операционную систему;
- просматривать регулярно список установленных программ.

4. Ответственность

4.1. Ответственность за организацию антивирусной защиты возлагается на лицо, ответственное за антивирусную защиту средств информатизации.

4.2. Ответственность за проведение мероприятий антивирусного контроля в МБОУ СОШ №4 имени Л.И. Золотухиной и соблюдение требований настоящего Регламента возлагается на ответственного за обеспечение антивирусной защиты средств информатизации.

4.3. Периодический контроль за состоянием антивирусной защиты в МБОУ СОШ №4 имени Л.И. Золотухиной осуществляется техническим специалистом.