МУНИЦИПАЛЬНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ АВТОНОМНОЕ УЧРЕЖДЕНИЕ СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА № 5 ГОРОДА ЗЕИ АМУРСКОЙ ОБЛАСТИ

ПРИНЯТО
Управляющим советом
МОАУ СОШ № 5
протокол от 10.11.2020 № 2

УТВЕРЖДЕНО
приказом директора
МОАУ СОШ № 5
от 11.11.2020 № 240/од

Положение об организации антивирусной защиты средств информатизации МОБУ СОШ № 5

1. Общие положения

1.1. Настоящее Положение об организации антивирусной защиты средств информатизации (далее - Положение) определяет требования к организации зашиты средств информатизации от разрушающего воздействия компьютерных вирусов, порядок организации работ по антивирусной защите средств информатизации в МОАУ СОШ № 5 (далее - Учреждение), устанавливает ответственность пользователей и должностных лиц Учреждения по антивирусной защите средств информатизации.

1.2. Положение разработано в соответствии с требованиями и на основе типовой инструкции по организации антивирусной защиты средств информатизации в образовательных учреждениях.

1.3. Обязательному антивирусному контролю подлежит любая информация: текстовые файлы любых форматов, файлы данных, исполняемые файлы, информация, получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях (магнитных дисках, лентах).

1.4. Средства антивирусной защиты информации должны устанавливаться на всех средствах вычислительной техники, используемых в Учреждении.

1.5. К использованию в Учреждении допускается только лицензионное антивирусное программное обеспечение в соответствии с требованиями действующего законодательства Российской Федерации.

1.6. Директором Учреждения назначается лицо, ответственное за антивирусную защиту средств информатизации Учреждения.

2. Порядок установки настройки антивирусного программного обеспечения

2.1. Антивирусная зашита средств информатизации Учреждения осуществляется посредством специального антивирусного программного обеспечения.

2.2. Установка и настройка средств антивирусного программного обеспечения осуществляются в соответствии с эксплуатационной документацией, поставляемой в комплекте с ним.

2.3. Установка, настройка и регулярное обновление антивирусного программного обеспечения осуществляется только ответственным за антивирусную защиту средств информатизации Учреждения.

2.4. Антивирусное программное обеспечение настраивается таким образом, чтобы обеспечить следующие условия:

- обязательный входной контроль на наличие программных вирусов во всех поступающих электронных носителях информации в автоматическом режиме;

- обязательная проверка всех электронных писем на предмет отсутствия программных вирусов в автоматическом режиме;

- блокирование сетевых атак из сети Интернет в автоматическом режиме.

2.5. Обновление баз данных средств антивирусной защиты информации на рабочих станциях локально-вычислительной сети Учреждения осуществляется:

- централизованно через сервер Учреждения в автоматическом режиме или в ручном режиме;

- в ручном режиме ответственным за антивирусную защиту средств информатизации Учреждения не реже одного раза в неделю.

3. Требования к проведению мероприятий по антивирусной защите средств информатизации Учреждения

3.1. Ответственный за антивирусную защиту средств информатизации Учреждения раз в год проводит инструктаж по работе с антивирусным программным обеспечением.

3.2. Ответственный за антивирусную защиту средств информатизации Учреждения ведет журнал инструктажа по работе с антивирусным программным обеспечением.

3.3. Пользователям, работающим со средствами информатизации Учреждения, запрещается отключать средства антивирусной защиты информации во время работы;

3.4. Устанавливаемое (изменяемое) программное обеспечение на персональные компьютеры Учреждения должно быть предварительно проверено на отсутствие вирусов.

3.5. Проведение мероприятий по антивирусной защите средств информатизации Учреждения должно включать следующее:

- ежедневно в начале работы при загрузке компьютера в автоматическом режиме проводится антивирусный контроль всех дисков и файлов персонального компьютера;

- периодическая проверка в автоматическом режиме на предмет отсутствия программных вирусов жестких магнитных дисков (не реже одного раза в месяц);

- обязательная проверка съемных носителей информации перед началом работы с ними;

- восстановление работоспособности программных средств и информационных массивов, поврежденных программными вирусами.

3.6. Плановые проверки средств информатизации Учреждения должны проводиться не реже одного раза в месяц.

3.7. 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) необходимо провести внеплановую проверку средств информатизации Учреждения (жестких магнитных дисков и съемных носителей информации) на наличие программных вирусов.

3.8. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователи обязаны:

- приостановить работу;

- провести лечение или уничтожение зараженных файлов и поставить в известность ответственного за антивирусную защиту средств информатизации Учреждения;

- в случае если не удается удалить вирус, немедленно поставить в известность о факте обнаружения зараженных вирусом файлов ответственного за антивирусную защиту средств информатизации Учреждения;

- ответственный за антивирусную защиту средств информатизации Учреждения совместно с пользователем зараженных вирусом файлов должен определить необходимость дальнейшего их использования и провести лечение или уничтожение заражённых файлов.

4. Ответственность при организации антивирусной защиты

4.1. Ответственный за антивирусную защиту средств информатизации Учреждения несет персональную ответственность за выполнение данного Положения.

4.2. Контроль соблюдения данного Положения ответственным за антивирусную защиту средств информатизации Учреждения осуществляет директор Учреждения.