Муниципальное автономное общеобразовательное учреждение
"Средняя общеобразовательная школа №23"
городского округа город Стерлитамак Республики Башкортостан

СОГЛАСОВАНО
протокол заседания
Педагогического совета
от «05» февраля 2019 г. № 1

УТВЕРЖДАЮ
Директор МАОУ «СОШ №23»
городского округа г. Стерлитамак РБ
_____ О.Г. [illegible]ойлова
«05» февраля 2019 г.

Положение
об организации антивирусной зашиты средств информатизации

1. Общие положения

1.1. Настоящее положение определяет требования к организации зашиты средств информатизации от разрушающего воздействия компьютерных вирусов, порядок организации работ по антивирусной защите средств информатизации, устанавливает ответственность пользователей и должностных лиц школы по антивирусной защите средств информатизации.

1.2. 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 (флеш-картах, жестких магнитных дисках, оптических дисках и т.п.).

1.3. Средства антивирусной зашиты информации должны устанавливаться на всех средствах вычислительной техники, используемых в школе.

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

1.5. Директором школы назначается лицо ответственное за антивирусную защиту средств информатизации школы.

1.6. Ответственный за антивирусную защиту средств информатизации школы имеет право на стимулирующие выплаты из фонда стимулирования педагогических и руководящих работников учреждения за выполнение функций, определенных настоящим положением.

2. Порядок установки настройки антивирусного программного обеспечения

2.1. Антивирусная зашита средств информатизации школы 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 школы.

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 школьной локально-вычислительной сети осуществляется в автоматическом режиме.

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

3.1. Ответственный за антивирусную защиту средств информатизации школы раз в год проводит инструктаж по работе с антивирусным программным обеспечением.
3.2. Ответственный за антивирусную защиту средств информатизации школы ведет журнал инструктажа по работе с антивирусным программным обеспечением.
3.3. Пользователям, работающим со средствами информатизации школы, запрещается отключать средства антивирусной защиты информации во время работы;
3.4. Устанавливаемое (изменяемое) программное обеспечение на персональные компьютеры образовательного учреждения должно быть предварительно проверено на отсутствие вирусов.
3.5. Проведение мероприятий по антивирусной защите средств информатизации школы должно включать следующее:

- ежедневно в начале работы при загрузке компьютера в автоматическом режиме выполнять обновление антивирусных баз и проводиться 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 школы должны проводиться не реже одного раза в квартал.
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 школы (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 школы;
- в случае, ели не удается удалить вирус, немедленно поставить в известность о факте обнаружения зараженных вирусом файлов ответственного за антивирусную защиту средств информатизации школы;
- ответственный за антивирусную защиту средств информатизации школы, 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 школы несет персональную ответственность за невыполнение данного положения.
4.2. Контроль за соблюдением данного положения ответственным за антивирусную защиту средств информатизации школы, осуществляет директор школы.