УТВЕРЖДЕНО
приказом директора МБУ СОШ №16
№6 от 14.01.2014

Положение
об антивирусной защите

1. Термины и определения

Компьютерным вирусом называется программа, способная создавать свои копии (не обязательно полностью совпадающие с оригиналом) и внедрять их в различные объекты или ресурсы компьютерных систем, сетей и так далее без ведома пользователя. При этом копии сохраняют способность дальнейшего распространения. На сегодняшний день известно 6 основных типов вирусов: файловые, загрузочные, призраки (полиморфные), невидимки, скрипт-вирусы и макро-вирусы. Следует отличать вирусы от вредоносных кодов. К ним относятся Интернет-черви и программы, получившие название "Троянские кони".

Основные симптомы вирусного поражения: замедление работы некоторых программ, увеличение размеров файлов (особенно выполняемых), появление не существовавших ранее подозрительных файлов, уменьшение объема доступной оперативной памяти (по сравнению с обычным режимом работы), внезапно возникающие разнообразные видео и звуковые эффекты. При всех перечисленных выше симптомах, а также при других странных проявлениях в работе системы (неустойчивая работа, частые самостоятельные перезагрузки и прочее) следует немедленно произвести проверку системы на наличие вирусов.

Зараженный диск - это диск, в загрузочном секторе которого находится программа - вирус. После запуска программы, содержащей вирус, становится возможным заражение других файлов. Наиболее часто вирусом заражаются загрузочный сектор диска и исполняемые файлы, имеющие расширения EXE, .COM, SYS или BAT. Крайне редко заражаются текстовые и графические файлы.

Зараженная программа - это программа, содержащая внедренную в нее программу-вирус.

2. Общие положения

1.1. Настоящее Положение определяет требования к организации защиты компьютеров МОУ школы №16 от воздействия компьютерных вирусов и устанавливает ответственность руководителей и сотрудников школы за их выполнение.

1.2. Задачами антивирусной защиты являются:

- определение состава и регламента запуска антивирусных диагностических средств, регламента их ревизии и обновления;
- проведение профилактических работ с применением антивирусных диагностических средств;

3. Организация мероприятий по антивирусной защите

3.1. Заместитель директора школы обеспечивает организацию работ по антивирусной защите.

3.2. К использованию в школе допускаются только лицензионные антивирусные средства.
3.3. Установка средств антивирусной защиты на компьютерах в школе и настройка параметров средств антивирусной защиты осуществляется ответственным за установку в соответствии с руководствами по применению конкретных антивирусных средств.

3.4. Обновление антивирусных баз должно производиться не реже 2 раз в неделю.

3.. Мероприятия по антивирусной защите на компьютерах в школе включают в себя:

- профилактика вирусов;
- анализ ситуаций;
- применение средств антивирусной защиты.

4. Профилактика вирусов

4.1. Регулярно проводимые профилактические работы по выявлению вирусов могут полностью исключить появление и распространение вирусов в компьютере. К основным профилактическим работам и мероприятиям относятся:

- ежедневная автоматическая проверка наличия вирусов при включении компьютера;
- регулярная (не реже одного раза в квартал) проверка компьютеров на наличие вирусов, даже при отсутствии внешних проявлений вирусов;
- изучение информации по сообщениям в компьютерных журналах, газетах и Интернете о новых вирусах;
- тщательная проверка всех поступающих и купленных программ и баз данных;
- ограничение доступа к компьютеру посторонних лиц.

4.2. Регулярную проверку наличия вирусов выполняет сотрудник, ответственный за обеспечение антивирусной безопасности.

4.3. При обнаружении вирусов на компьютере, работающем в локальной сети, проверке подлежат все компьютеры, включенные в эту сеть и работающие с общими данными и программным обеспечением.

5. Анализ ситуаций

5.1. Если антивирусные программы выдают на экран дисплея сообщения о подозрении на наличие вирусов на компьютере, то прежде всего необходимо убедиться в действительном наличии вирусов. Возможны ситуации, при которых эти сообщения являются следствием неисправности компьютера.

При возникновении подобной ситуации необходимо приостановить работу и немедленно известить об этом ответственного за обеспечение антивирусной безопасности..

5.2. Основные источники вирусов:

- съемный носитель (дискета, флеш-карта, CD-ROM, DVD-ROM, мобильное дисковое устройство) на котором находятся зараженные вирусом файлы;
- компьютерная сеть, в том числе система электронной почты и Интернет;
- жесткий диск, на который попал вирус в результате работы с зараженными программами.

Если вирус проник на компьютер со съемного носителя, то необходимо определить источник и, если источник информации на съемном носителе находится в школе, то необходимо проверить на наличие вирусов компьютер - источник информации на съемном носителе. Если источник дискеты или съемного носителя - другая организация, то необходимо сообщить в эту организацию о факте выявления вирусов и в дальнейшем обратить особое внимание на носители информации, поступающие из этой организации.

6. Применение средств антивирусной защиты

6.1. Уничтожение вирусов выполняется сотрудником, ответственным за установку и обновление антивирусного программного обеспечения.

6.2. Если вирус поразил какие-либо программы, то уничтожение вируса выполняется путем уничтожения программы на диске либо на дискете. После уничтожения зараженной программы необходимо восстановить программу, используя резервную копию программы.

6.3. Если вирус поразил файлы, то вирус уничтожается либо путем стирания этих файлов, либо путем использования специальных лечащих программ. Использование лечащих программ не дает полной гарантии восстановления файла. Поэтому после лечения необходима проверка восстановления данного файла. Лечащие программы используются лишь в тех случаях, когда отсутствует резервная копия зараженной программы либо файла с данными, либо восстановление уничтоженного файла с помощью резервной копии очень трудоемко.

6.4. В любом случае после уничтожения вирусов и восстановления зараженных программ и файлов с данными необходимо еще раз выполнить проверку наличия вирусов, используя антивирусные программы. Перед повторной проверкой необходимо перезагрузить компьютер через выключение и последующее включение компьютера. Если повторная проверка не выявила вирусов, то можно быть уверенным в отсутствии вирусов.

7. Ответственность

7.1. Ответственность за выполнение мероприятий по антивирусной защите информации на средствах вычислительной техники, в соответствии с требованиями настоящего Положения, возлагается на заместителя директора школы.

7.2. Ответственность за выполнение мероприятий антивирусного контроля и соблюдение требований настоящего Положения возлагается на всех сотрудников школы, использующих компьютеры в своей работе.

Инструкция пользователя
по антивирусной защите

Общие положения

Настоящее Инструкция определяет требования к организации защиты от воздействия компьютерных вирусов, устанавливает ответственность руководителей и сотрудников школы за их выполнение.

Установка средств антивирусной защиты на компьютерах и настройка их параметров в осуществляется ответственным за установку в соответствии с руководствами по применению конкретных антивирусных средств.

Обновление антивирусных баз должно производиться не реже 2 раз в неделю.

Характерные проявления вирусов

При заражении компьютера вирусом важно его обнаружить. Для этого следует знать об основных признаках проявления вирусов. К ним можно отнести следующие:

- прекращение работы или неправильная работа ранее успешно функционировавших программ;
- медленная работа компьютера;
- невозможность загрузки операционной системы;
- исчезновение файлов и каталогов или искажение их содержимого;
- изменение даты и времени модификации файлов;
- изменение размеров файлов;
- неожиданное значительное увеличение количества файлов на диске;
- существенное уменьшение размера свободной оперативной памяти;
- вывод на экран непредусмотренных сообщений или изображений;
- подача непредусмотренных звуковых сигналов;
- частые зависания и сбои в работе компьютера.

Анализ ситуаций

Если антивирусные программы выдают на экран дисплея сообщения о подозрении на наличие вирусов на компьютере, то прежде всего необходимо убедиться в действительном наличии вирусов.

При возникновении подобной ситуации необходимо приостановить работу и немедленно известить об этом ответственного за информационную безопасность в школе.

Основные источники вирусов:

- съемный носитель (дискета, флеш-карта, CD-ROM, DVD-ROM, мобильное дисковое устройство) на котором находятся зараженные вирусом файлы;
- компьютерная сеть, в том числе система электронной почты и Интернет;
- жесткий диск, на который попал вирус в результате работы с зараженными программами.

Если вирус проник на компьютер со съемного носителя, то необходимо определить источник и, если источник информации на съемном носителе находится в школе, то необходимо проверить на наличие вирусов компьютер - источник информации на съемном носителе. Если источник дискеты или съемного носителя - другая организация, то необходимо сообщить в эту организацию о факте выявления вирусов и в дальнейшем обратить особое внимание на носители информации, поступающие из этой организации.

Применение средств антивирусной защиты

Уничтожение вирусов выполняется сотрудником, ответственным за установку и обновление антивирусного программного обеспечения.

Если вирус поразил какие-либо программы, то уничтожение вируса выполняется путем уничтожения программы на диске либо на дискете. После уничтожения зараженной программы необходимо восстановить программу, используя резервную копию программы.

Если вирус поразил файлы, то вирус уничтожается либо путем стирания этих файлов, либо путем использования специальных лечащих программ. Использование лечащих программ не дает полной гарантии восстановления файла. Поэтому после лечения необходима проверка восстановления данного файла. Лечащие программы используются лишь в тех случаях, когда отсутствует резервная копия зараженной программы либо файла с данными, либо восстановление уничтоженного файла с помощью резервной копии очень трудоемко.

В любом случае после уничтожения вирусов и восстановления зараженных программ и файлов с данными необходимо еще раз выполнить проверку наличия вирусов, используя антивирусные программы. Перед повторной проверкой необходимо перезагрузить компьютер через выключение и последующее включение компьютера. Если повторная проверка не выявила вирусов, то можно быть уверенным в отсутствии вирусов.

Требования к сотрудникам

- Сотрудник обязан проводить антивирусный контроль всех внешних носителей информации (дискет, компакт-дисков, магнитооптических дисков и т.п.), поступающих со стороны или полученных по компьютерным сетям (скопированных на общедоступный ресурс локального компьютера другими пользователями).
- Во всех случаях возможного проявления действия вирусов, обнаружения файлов, пораженных вирусом или подозрении на наличие вируса сотрудник должен:
    - без попытки какого-либо лечения незамедлительно сообщить об ответственному за информационную безопасность и оценить с ним возможные пути заражения и распространения данного вируса;
    - совместно провести лечебно-восстановительные мероприятия.

- Сотрудник не должен самостоятельно устанавливать программное обеспечение, если это не входит в его обязанности. Запрещается устанавливать и запускать нелицензионное или не относящееся к выполнению им своих должностных обязанностей программное обеспечение.