Регламент
работы по обеспечению антивирусной безопасности
«точки доступа к Интернет» гимназии

1. Основные положения.

1.1. Запрещается использование компьютеров "точки доступа к Интернет" образовательного учреждения без установленного на них антивирусного программного обеспечения с регулярно обновляемыми антивирусными базами.

1.2. Для большей степени защиты от вирусов и других вредоносных программ необходимо совместное использование антивирусного программного обеспечения, брандмауэра, обнаруживающего сетевые атаки и "шпионское" программное обеспечение, и регулярного резервного копирования пользовательских данных.

1.3. В случае наличия в образовательном учреждении других компьютеров кроме автоматизированного рабочего места "точки доступа к Интернету" необходимо принять меры к обеспечению и их антивирусной защиты.

2. Подготовка к работе "точки доступа к Интернет".

2.1. Перед вводом в эксплуатацию "точки доступа к Интернет" необходимо проверить не только факт наличия на компьютерах антивирусного программного обеспечения, но и правильность его настроек. В частности, корректность настроек для обновления антивирусных баз с веб-сайта производителя антивирусной программы, запуск при загрузке компьютера резидентного антивирусного монитора (программы-сторожа), настройки резидентного антивирусного монитора на сканирование наиболее уязвимых типов файлов и электронной почты.

2.2. Не допускать к самостоятельной работе на компьютерах "точки доступа к Интернет" лиц не прошедших предварительного инструктажа по антивирусной безопасности. В инструктаже указать возможные действия антивирусной программы (появляющиеся диалоговые окна) в случае заражения вирусом или появления подозрительных объектов и соответствующие действия пользователя компьютера.

3. В процессе работы "точки доступа к Интернет".

3.1. Проводить регулярное обновление антивирусных баз не реже двух раз в неделю на всех компьютерах образовательного учреждения, настроив соответствующим образом "Планировщик заданий" Windows или вручную.

3.2 Перед использованием внешних носителей информации (дискет, CD-ROM, флеш-накопителей и т.п.) проверять их на наличие вирусов и опасных программ.

3.3. В случае корректной работы резидентного антивирусного монитора (программы-сторожа) полученная из Интернет информация (документы, программы и т.п.) будет проверяться на вирусы автоматически. В противном случае проверку всех скачиваемых файлов необходимо провести вручную.

4. Действия при обнаружении вируса.

4.1. При обнаружении антивирусной защитой "точки доступа к Интернет" вируса или вредоносной программы необходимо выполнить:

1. лечение зараженного файла;
2. удаление зараженного файла, если лечение невозможно;
3. блокирование зараженного файла, если его невозможно удалить.

4.2. В случае блокирования зараженного файла необходимо принять меры к его удалению. Например, при перезагрузке компьютера или при загрузке операционной системы в "Безопасном режиме".

4.3. Если устранение вирусной опасности своими силами не получается, то необходимо связаться с технической поддержкой производителя антивирусной программы (по электронной почте, телефону или через специальный форум на веб-сайте производителя) для получения консультаций.