



Утверждаю

Директор МБУ СОШ №4

Л.А. Скопцова

«31» августа 2011 г.

**Регламент работы
по обеспечению антивирусной безопасности "точки доступа к Интернет"
муниципального бюджетного общеобразовательного учреждения
средней общеобразовательной школы №4 городского округа Тольятти
(МБУ СОШ №4)**

1. Основные положения.

Запрещается использование компьютеров "точки доступа к Интернет" МБУ СОШ №4 без установленного на них антивирусного программного обеспечения с регулярно обновляемыми антивирусными базами.

1.2. В случае наличия в МБУ СОШ №4 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. Подготовить и разместить на видном месте краткую памятку для ответственного за "точку доступа к Интернет" и ее пользователей по работе антивирусной защиты. В памятке указать возможные действия антивирусной программы (появляющиеся диалоговые окна) в случае заражения вирусом или появления подозрительных объектов и соответствующие действия пользователя компьютера.

2.3. Не допускать к самостоятельной работе на компьютерах "точки доступа к Интернет" лиц, не прошедших предварительного инструктажа по антивирусной безопасности. Факт прохождения инструктажа фиксировать в специальном журнале учета.

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

3.1. Проводить регулярное обновление антивирусных баз не реже двух раз в неделю на всех компьютерах МБУ СОШ №4, 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.

5. Обеспечение антивирусной безопасности по прошествии срока действия лицензии, входящей в комплект поставки автоматизированного рабочего места "точки доступа к Интернет".

5.1. Необходимо продлить срок действия лицензии на антивирусное программное обеспечение, предусмотрев на следующий год оплату ее стоимости из бюджетных или внебюджетных средств образовательного учреждения.

5.2. МБУ СОШ №4 имеет право самостоятельно решить будет ли продлеваться лицензия на текущую антивирусную программу или же будет приобретена другая программа, в большей степени удовлетворяющая потребности данного конкретного учреждения. Выбор антивирусной программы может производиться как среди коммерческих (платных) программ, так и среди распространяемых бесплатно.