Регламент
организации антивирусной защиты в МБОУ «Лукашевская СОШ»

1. *Основные положения*

1.1. Запрещается использование компьютеров "точки доступа к Интернету" 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 Интернету"*

2.1. Перед вводом в эксплуатацию "точки доступа к Интернету" 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 Интернету" 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 Интернету" лиц не прошедших предварительного инструктажа по антивирусной безопасности. Факт прохождения инструктажа фиксировать в специальном журнале учета.

3. *В процессе работы "точки доступа к Интернету"*

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. Проводить регулярное резервное копирование на внешние носители памяти (CD-ROM, DVD-ROM) всей важной пользовательской информации не реже 1 раза в месяц на всех компьютерах образовательного учреждения.

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

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

4. *Действия при обнаружении вируса*

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

- ✓ лечение зараженного файла;
- ✓ удаление зараженного файла, если лечение невозможно;
- ✓ 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 Интернету"*

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. Образовательное учреждение 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.

5.3. В случае использования коммерческих антивирусных программ необходимо учитывать, что практически все производители предоставляют, во-первых, скидки для образовательных учреждений, а, во-вторых, скидки при продлении лицензии.