Частное общеобразовательное учреждение средняя общеобразовательная школа «Общеобразовательный центр «Школа»
юридический адрес: 445028, г. Тольятти, б-р Королева, 22,
почтовый адрес: 445057, г. Тольятти, ул. Юбилейная, 77
тел.: (8482) 34-00-21, 35-56-65, e-mail: ooc-shkola@mail.ru

РАССМОТРЕН
Педагогическим Советом
протокол № 211/4 от 18.11.2019

УТВЕРЖДЕН
приказом директора школы
№ 238-од от 29.11.2019

ЧОУ СОШ «ОБЩЕОБРАЗОВАТЕЛЬНЫЙ ЦЕНТР «ШКОЛА»

Подписан: Светлана Ивановна Сидорова
DN: C=RU, OU=Директор, O="ЧОУ СОШ "" Общеобразовательный центр ""Школа""", CN=Светлана Ивановна Сидорова, E=ooc-shkola@mail.ru
Основание: я подтверждаю этот документ своей удостоверяющей подписью
Дата: 2023-11-08 10:43:44

РЕГЛАМЕНТ РАБОТЫ
по обеспечению антивирусной безопасности «точки доступа к Интернет»

1. Основные положения

1.1. Любой компьютер Школы, имеющий доступ в сеть Интернет, является «Точкой доступа к сети Интернет».

1.2. Запрещается использование компьютеров «точки доступа к Интернет» образовательной организации без установленного на них антивирусного программного обеспечения с регулярно обновляемыми антивирусными базами.

1.3. 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.

2. Подготовка к работе «точки доступа к Интернет»

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.

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.

3.2. Проводить регулярное резервное копирование на внешние носители памяти всей важной пользовательской информации не реже 1 раза в месяц на всех компьютерах образовательного учреждения.

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

3.4. В случае корректной работы резидентного антивирусного монитора 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

При обнаружении антивирусной защитой «точки доступа к Интернет» вируса или вредоносной программы необходимо выполнить удаление зараженного файла.