МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ГИМНАЗИЯ ИМЕНИ Ф.К. САЛМАНОВА

П Р И К А З

04.09.2019 № ГС-13-591/9

Сургут

О назначении ответственного сотрудника за организацию антивирусной защиты в гимназии

В целях организации порядка проведения антивирусного контроля в гимназии и предотвращения возникновения факторов заражения программного обеспечения компьютерными вирусами п р и к а з ы в а ю:

1.Назначить ответственным сотрудником за организацию антивирусной защиты системного администратора В.В.Лемешева.

2.Назначить ответственным сотрудником за установку и настройку антивирусного программного обеспечения техника И.Е.Руденко.

3.Утвердить Регламент по организации антивирусной защиты средств автоматизации в гимназии (Приложение 1).

4.Утвердить Инструкцию по установке и настройке антивирусной программы в гимназии (Приложение 2).

5.Довести до сведения сотрудников и обучающихся Регламент по организации антивирусной защиты средств автоматизации и Инструкцию по установке и настройке антивирусной программы в образовательном учреждении заместителю директора по учебно-воспитательной работе М.Л. Сафаровой в срок до 01.11.2019.

6.Разместить утвержденные настоящим приказом локальные нормативные акты на официальном сайте гимназии лаборанту И.В. Гришиной в срок до 01.11.2019.

6.Контроль за выполнением приказа возложить на заместителя директора по учебно-воспитательной работе М.Л.Сафарову.

Директор  Г.А.Мисюля

М.Л.Сафарова

Приложение 1 к приказу
от 04.09.2019 № ГС-13-591/9

Регламент
по организации антивирусной защиты средств автоматизации
в гимназии

1.Общие положения.

1.1.Директор гимназии имени Ф.К. Салманова (далее – гимназия) назначает лицо, ответственное за антивирусную защиту средств информатизации.

1.2.В гимназии может использоваться только лицензионное антивирусное программное обеспечение в соответствии с требованиями действующего законодательства РФ.

1.3.Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях (магнитных дисках, CD-ROM и т.п.). Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

1.4.Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль.

1.5.Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов.

1.6.Факт выполнения антивирусной проверки после установки (изменения) программного обеспечения должен регистрироваться в специальном журнале за подписью лица, ответственного за антивирусную защиту.

2.Требования к проведению мероприятий по антивирусной защите

2.1.Ежедневно в начале работы при загрузке компьютера, в автоматическом режиме должно выполняться обновление антивирусных баз, и проводиться антивирусный контроль всех дисков и файлов персонального компьютера.

2.2.Периодические проверки электронных архивов должны проводиться не реже одного раза в неделю.

2.3.Внеочередной антивирусный контроль всех дисков и файлов персонального компьютера должен выполняться:

непосредственно после установки (изменения) программного обеспечения компьютера, должна быть выполнена антивирусная проверка: на сервере и персональных компьютерах ОО. Факт выполнения антивирусной проверки, после установки (изменения) программного обеспечения, должен регистрироваться в специальном журнале за подписью лица, установившего (изменившего) программное обеспечение, и лица, его контролировавшего;

при возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.).

2.4.В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователи обязаны:

приостановить работу;

немедленно поставить в известность о факте обнаружения зараженных вирусом файлов ответственного за обеспечение информационной безопасности в гимназии;

совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;

провести лечение или уничтожение зараженных файлов.

3. Профилактика заражения

3.1. Одним из основных методов борьбы с вирусами является своевременная профилактика, состоящая из соблюдения следующих правил. Защитить компьютер с помощью антивирусных программ и программ безопасной работы в Интернете. Для этого:

установить антивирусную программу;

обновлять регулярно сигнатуры угроз, входящие в состав программы;
не выгружать из памяти и не останавливать работу антивирусной программы.
3.2. Проявлять осторожность при записи новых данных на компьютер:
проверить на присутствие вирусов все съемные диски (дискеты, CD–диски, флэш – карты и пр.) перед их использованием;
не запускать никаких файлов, пришедших по почте, не проверенных с помощью антивирусной программы;
обратить внимание на наличие сертификата безопасности при установлении новой программы с какого-либо веб-сайта;
проверить с помощью антивирусной программы копируемый из Интернета или локальной сети исполняемый файл;
пользоваться сервисом Windows Update и регулярно устанавливать обновления операционной системы Microsoft Windows;
создать диск аварийного восстановления, с которого при необходимости можно будет загрузиться, используя «чистую» операционную систему;
просматривать регулярно список установленных программ.

4. Ответственность

4.1.Ответственность за организацию антивирусной защиты возлагается на лицо, ответственное за антивирусную защиту средств информатизации.
4.2.Ответственность за проведение мероприятий антивирусного контроля в гимназии и соблюдение требований настоящего Регламента возлагается на ответственного за обеспечение антивирусной защиты средств информатизации.
4.3.Периодический контроль за состоянием антивирусной защиты в гимназии осуществляется заместителем директора по административно-хозяйственной работе.

Приложение 2 к приказу
от 04.09.2019 № ГС-13-591/9

Инструкция по установке и настройке антивирусной программы

1.Установка антивирусной программы «Kaspersky Endpoint Security 10.2»

Создать папку «Антивирус»:

для «Windows 7» и «Windows 8» в папке «Загрузки»;

для «Windows XP» на «Рабочем столе» компьютера.

Скачать антивирусную программу «Kaspersky Endpoint Security 10.2»:

версия для операционной системы «Windows 7» и «Windows 8» – http://www.kaspersky.ru/downloads-endpoint-security-windows.

Скачивать в, ранее созданную, папку «Антивирус» в папке «Загрузки»;

версия для операционной системы «Windows XP» – http://www.kaspersky.ru/downloads/productupdates/endpoint-security-windows-old.

Скачивать в ранее созданную папку «Антивирус» на «Рабочем столе».

После того, как антивирус скачался находим файл в папке «Антивирус», двойным нажатием левой кнопки мыши запускаем его.

В появившемся окне проверяем, что папка для дистрибутива «Антивирус» и нажимаем «Распаковать».

После окончания распаковки, нажимаем кнопку «Готово».

Переходим в папку «Антивирус», находим в ней файл setup.

Двойным нажатием левой кнопки мыши запускаем файл setup.

Может появиться окно с вопросом: «Разрешить следующей программе внести изменения на это компьютере?» – нажимаем кнопку «Да».

В появившемся окне нажимаем кнопку «Далее». В следующем окне ставим галочку в строке «Я принимаю условия Лицензионного соглашения» и нажимаемся кнопку «Далее»

В появившемся окне, выделяем строку «Я согласен участвовать в Kaspersky Security Network» и нажимаем кнопку «Далее».

В следующем окне устатавливаем галочки в строках «Защитить процесс

установки» и «Добавить путь к файлу avp.com» в системную переменую и нажимаем кнопку «Установить».

По окончании установки откроется окно мастера первоначальной настройки программы.

Если у вас есть файл ключа, выделите указанную строку и нажмите кнопку «Далее».

В окне нажмите кнопку «Обзор», найдите файл ключа и нажмите «Открыть».

Если нет ключа и ключевого файла, нужно выбрать «Активировать позже» и нажать «Далее».

В окне ставим галочку в строке «Запустить Kaspersky Enpoint security 10 для Windows», нажимаем кнопку «Завершить».

2.Настройка антивирусной программы «Kaspersky Endpoint Security 10.2»

Если антивирус «Kaspersky Endpoint Security 10» не запустился, то находим значок антивируса в области у часов.

В появившемся окне, нажимаем на вкладку «Настройка».

Во вкладке «Настройка» в левой части меню, выбираем пункт «Веб-контроль», далее, в правой части окна ставим галочку в строке «Включить Веб-Контроль», нажимаем кнопку «Добавить».

Откроется окно. В строке «Название» вписываем строку – «Запрещенные интернет ресурсы».

В правой части вкладки, ставим галочки в строках «Запускать Kaspersky Endpoint Security 10 для Windows при включении компьютера» и «Применять технологию лечения активного заражения», нажимаем кнопку «Сохранить».

В левой части меню выделяем строку «Файловый Антивирус».

В правой части окна ставим галочку в строке «Включить Файловый Антивирус», выделяем пункт «Выполнять действие: Лечить. Удалять, если лечение невозможно», ставим галочки в строках «Лечить» и «Удалять, если лечение невозможно», нажимаем кнопку «Сохранить».

В правой части окна ставим галочку в строке «Включить Почтовый

Антивирус», выделяем пункт «Выполнять действие: Лечить. Удалять, если лечение невозможно», ставим галочки в строках «Лечить» и «Удалять, если лечение невозможно», нажимаем кнопку «Сохранить».

В левой части меню выделяем пункт «Дополнительные параметры»

В правой части ставим галочки в строках «Включить самозащиту» и «Уступать ресурсы другим программам». Нажимаем кнопку «Сохранить» и закрываем окно.

Теперь необходимо перезагрузить компьютер.