С учётом мнения
Совета школы

Протокол № 1 от 27.08.2019

УТВЕРЖДЕНО
приказом директора
от 29.08. 2019 № 248

Инструкция
по организации антивирусной защиты
средств информатизации в МБОУ СОШ № 1

1. Общие положения

1.1. Настоящая Инструкция определяет требования к организации защиты средств информатизации от разрушающего воздействия компьютерных вирусов, порядок организации работ по антивирусной защите средств информатизации в образовательном учреждении (далее – ОУ), устанавливает ответственность пользователей и должностных лиц ОУ по антивирусной защите средств информатизации.

1.2.Настоящая инструкция разработана на основе Типовой инструкции по организации антивирусной защиты средств информатизации в образовательных учреждениях.

1.3. Руководитель образовательного учреждения назначает лицо, ответственное за организацию антивирусной защиты средств информатизации. В противном случае вся ответственность за обеспечение антивирусной защиты средств информатизации ложится на руководителя образовательного учреждения.

1.4. К использованию в образовательном учреждении допускается только лицензионное антивирусное программное обеспечение в соответствии с требованиями действующего законодательства Российской Федерации (Norton Antivirus, Dr. Web, Kaspersky Antivirus, NOD 32 и т.п.).

1.5. При наличии в образовательном учреждении локальной компьютерной сети и сервера рекомендуется использовать версию антивирусного программного обеспечения, позволяющую организовать централизованное управление: установка, настройка, обновление антивирусных баз, антивирусное сканирование и сбор отчетов на всех компьютерах должны осуществляться удаленно на сервере учреждения (Kaspersky Work Space Security, Symantec Antivirus Corporate Edition, Symantec Endpoint Protection и т.п.)

1.6. Требования инструкции являются обязательными для всех работников образовательного учреждения, имеющих доступ к информационным ресурсам.

2. Требования к проведению мероприятий по антивирусной защите средств информатизации

2.1. Обязательному антивирусному контролю подлежит:

- любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам;
- информация на съемных носителях (магнитных дисках, лентах, CD-ROM и т.п.);
- входящая и исходящая информация (перед записью на носители информации, архивированием и отправкой);
- файлы, помещаемые в электронный архив;
- устанавливаемое (изменяемое) программное обеспечение.

2.2. Ежедневно в автоматическом режиме должно выполняться обновление антивирусных баз и проводиться антивирусный контроль всех дисков и файлов персонального компьютера.

2.3. Модуль антивирусной защиты должен загружаться автоматически при загрузке компьютера. Закрытие модуля или остановка его работы на всех компьютерах должна быть отключена или закрыта паролем.

1.1. Периодические антивирусные проверки всех компьютеров образовательного учреждения должны проводиться не реже одного раза в неделю.

2.4. Внеочередной антивирусный контроль всех дисков и файлов персонального компьютера должен выполняться 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.).

3. Профилактика заражения

3.1. Одним из основных методов борьбы с вирусами является своевременная профилактика, состоящая из соблюдения следующих правил:

3.1.1. 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.

3.1.2. Проявлять осторожность при записи новых данных на компьютер:

- Проверить на присутствие вирусов все съемные диски (дискеты, CD-диски, флеш-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.

3.1.3**.** Пользоваться сервисом Windows Update и регулярно устанавливать обновления операционной системы Microsoft Windows.

3.1.4. Создать диск аварийного восстановления, с которого при необходимости можно будет загрузиться, используя «чистую» операционную систему.

3.1.5. Просматривать регулярно список установленных программ.

4. Должностные обязанности пользователей по антивирусной защите средств информатизации

4.1. Не прерывать процесс обновления антивирусных баз и антивирусный контроль всех дисков и файлов персонального компьютера.

4.2. При отправке и получении электронной почты пользователь обязан проверить электронные письма на наличие вирусов.

4.3. При использовании съемных носителей, осуществлять их антивирусную проверку.

4.4. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов или электронных писем пользователи обязаны:

4.4.1. Приостановить работу.

4.4.2. Немедленно поставить в известность о факте обнаружения зараженных вирусом файлов ответственного за обеспечение антивирусной защиты в образовательном учреждении, владельца зараженных файлов, а также сотрудников, использующих эти файлы в работе.

4.4.3. Совместно с лицом, ответственным по антивирусной защите принять меры к локализации и удалению вирусов с помощью имеющихся антивирусных средств защиты.

5. Должностные обязанности ответственного лица за организацию антивирусной защиты средств информатизации

5.1. Лицо, ответственное за организацию антивирусной защиты средств информатизации, обязано:

5.1.1. Устанавливать средства антивирусного контроля на персональных компьютерах и серверах.

5.1.2. Настраивать параметры средств антивирусного контроля на персональных компьютерах и серверах.

5.1.3. Своевременно обновлять антивирусные базы на персональных компьютерах и серверах.

5.1.4. Еженедельно проверять компьютеры на вирусы.

5.1.5. Проводить внеочередную проверку в случае подозрения на наличие вирусов или по просьбе пользователей персональных компьютеров.

5.1.6. Проводить в установленном порядке инструктаж по антивирусной защите пользователей персональных компьютеров.

5.2. В случае обнаружения компьютерного вируса ответственное лицо за антивирусную защиту (или действия при обнаружении вируса):

5.2.1. принимает все необходимые меры для обеспечения сохранности информации;

5.2.2. принимает все необходимые меры по локализации и удалению вируса:

5.2.2.1. отключает компьютер от Интернета и локальной сети, если он к ней был подключен;

5.2.2.2. если симптом заражения состоит в том, что невозможно загрузиться с жесткого диска компьютера (компьютер выдает ошибку при подключении), загружается в режиме защиты от сбоев или с диска аварийной загрузки Microsoft Windows, который был создан при установке операционной системы на компьютер;

5.2.2.3. сохраняет результаты работы на внешнем носителе (дискете, CD-диске, флеш-карте и пр.);

5.2.2.4. обновляет сигнатуру угроз программы;

5.2.2.5. запускает полную проверку компьютера;

5.2.2.6. проводит лечение или уничтожение зараженных файлов;

5.2.2.7. в случае обнаружения нового вируса, не поддающегося лечению применяемыми антивирусными средствами, обязан направить зараженный вирусом файл на гибком магнитном диске в организацию, с которой заключен договор на антивирусную поддержку для дальнейшего исследования.

5.2.3. уведомляет руководителя образовательного учреждения об обнаружении вируса и последствиях его воздействия.

6. Ответственность

6.1. Ответственность за организацию антивирусной защиты средств информатизации возлагается на руководителя образовательного учреждения или лицо им назначенное.

6.2. Ответственность за проведение мероприятий антивирусного контроля в образовательном учреждении и соблюдение требований настоящей Инструкции возлагается на ответственного за обеспечение антивирусной защиты средств информатизации.

6.3. Периодический контроль за состоянием антивирусной защиты средств информатизации в образовательном учреждении осуществляется руководителем.