УТВЕРЖДАЮ
Директор ГБУДОСО
«Верхнесалдинская ДШИ»

_____ Е.Б. Сурова

приказ от 10 ноября 2021 г. № 56-О

Порядок организации антивирусной защиты средств информатизации в ГБУДОСО «Верхнесалдинская ДШИ»

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 ГБУДОСО «Верхнесалдинская ДШИ» (далее – учреждение), устанавливает ответственность пользователей и должностных лиц учреждения по антивирусной защите средств информатизации.

1.2. К использованию в 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.). Установка, настройка и регулярное обновление антивирусных средств осуществляется только ответственным за информационную безопасность учреждения.

1.3. При наличии в 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.)

1.4. Требования инструкции являются обязательными для всех работников 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;
- файлы, помещаемые на сервер;
- 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.

2.4. Особое внимание следует обратить на недопустимость использования съёмных носителей, принадлежащих лицам, временно допущенным к работе на ЭВМ в учреждении (обучающиеся, участники совещаний, студенты-практиканты и т.п.). Работа этих лиц должна проводиться под непосредственным контролем сотрудника или ответственного за информационную безопасность, особенно, если работа происходит с использованием ресурсов сети Интернет.

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

2.6. 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 сети Интернет. 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, флешнакопители 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 сети Интернет 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:

- Приостановить работу.
- Немедленно поставить в известность о факте обнаружения зараженных вирусом файлов ответственного за обеспечение антивирусной защиты в учреждении, владельца зараженных файлов, а также сотрудников, использующих эти файлы в работе.
- Совместно с лицом, ответственным за обеспечение антивирусной защиты в учреждении, принять меры к локализации и удалению вирусов с помощью имеющихся антивирусных средств защиты.

5. Должностные обязанности лица, ответственного за обеспечение антивирусной защиты средств информатизации

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

- Устанавливать средства антивирусного контроля на персональных компьютерах и серверах.
- Настраивать параметры средств антивирусного контроля на персональных компьютерах и серверах.
- Своевременно обновлять антивирусные базы на персональных компьютерах и серверах.
- Еженедельно проверять компьютеры на вирусы.
- Проводить внеочередную проверку в случае подозрения на наличие вирусов или по просьбе пользователей персональных компьютеров.
- Проводить в установленном порядке инструктаж по антивирусной защите пользователей персональных компьютеров.

5.2. В случае обнаружения компьютерного вируса ответственное лицо за обеспечение антивирусной защиты (или действия при обнаружении вируса):

- Принимает все необходимые меры для обеспечения сохранности информации;
- Принимает все необходимые меры по локализации и удалению вируса:

- отключает компьютер от сети Интернет и локальной сети, если он к ней был подключен;

- 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;

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

- обновляет сигнатуру угроз программы;

- запускает полную проверку компьютера;

- проводит лечение или уничтожение зараженных файлов;

- 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.

- Уведомляет руководителя учреждения об обнаружении вируса и последствиях его воздействия.

6. Ответственность

6.1. Ответственность за организацию антивирусной защиты средств информатизации возлагается на директора учреждения.

6.2. Ответственность за проведение мероприятий антивирусного контроля в учреждении и соблюдение требований настоящей Инструкции возлагается на ответственного за информационную безопасность учреждения.

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