Экз. № 1

УТВЕРЖДАЮ
Директор
МБУ «Школа № 70»
_____О.Б. Жигулевцева
«31» августа 2018 г.
Приказ № 97/5-ОД

ИНСТРУКЦИЯ
по проведению антивирусного контроля на объектах вычислительной техники (ОВТ)

Настоящая Инструкция разработана в соответствии с требованиями Федерального Закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

В тексте настоящей Инструкции применяются следующие сокращения и определения:

АРМ - автоматизированное рабочее место;
ПО - программное обеспечение;
ЛВС - локально-вычислительная сеть;
ОИ - объект информатизации;
ОВТ - объект вычислительной техники (составная часть ОИ);
НСД - несанкционированный доступ;
СЗИ - система защиты информации.

Конфиденциальная информация, в том числе персональные данные - документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации; характер сведений, обусловливающий их сбор, обработку и распространение на условиях соответствующего правового режима. Операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено Федеральным законом № 152-ФЗ «О персональных данных».

1 Общие положения

1.1 Настоящая Инструкция разработана с целью приведения в соответствие с требованиями Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и исполнения законодательных требований при обработке персональных данных в МБУ «Школа № 70» (далее - Школа) и является руководством по работе с персональными данными и

компьютерами сети Школы. Целью настоящей Инструкции является обеспечение антивирусной защиты на объектах вычислительной техники.

1.2 Настоящая Инструкция определяет требования к организации защиты локальной вычислительной сети объектов информатизации, автоматизированных рабочих мест, программного обеспечения, данных, представленных в электронном виде, в том числе персональных данных работников, обучающихся и родителей (законных представителей) обучающихся Школы от разрушающего воздействия компьютерных вирусов и устанавливает порядок безопасной работы на объектах вычислительной техники, ответственность руководителей и работников подразделений, эксплуатирующих и сопровождающих объекты вычислительной техники, за их выполнение.

1.3 К использованию на объектах вычислительной техники допускаются только сертифицированные и лицензионные средства обеспечения антивирусной защиты информации, централизованно закупленные у разработчиков (поставщиков) указанных средств.

1.4 Установка и настройка параметров средств антивирусной защиты осуществляется Администратором информационной безопасности назначенным Приказом директора Школы.

2 Основные требования

2.1 Антивирусный контроль локальных жестких дисков и файлов на рабочих станциях пользователей под управлением ОС Windows должен осуществляться постоянно и запускаться в автоматическом режиме при загрузке системы.

2.2 Обязательному антивирусному контролю подлежит любая информация (текстовые файлы, исполняемые файлы, архивные файлы и т.д.), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях (магнитных дисках, CD/DVD-ROM, USB-Flash дисках и т. п.). Использование входящей информации, не прошедшей предварительно антивирусный контроль не допускается. Перед отправкой по телекоммуникационным каналам связи информация (файлы, архивы, почтовые сообщения и т.п.) должна пройти обязательный антивирусный контроль.

2.3 Полное антивирусное сканирование локальных жестких дисков и рабочих файлов на рабочих станциях пользователей под управлением ОС Windows проводить 1 раз в неделю.

2.4 Полное антивирусное сканирование общих сетевых ресурсов файловых хранилищ проводить ежедневно в нерабочее время.

3 Обязанности пользователей

Пользователь обязан:

3.1 на рабочей станции ежедневно контролировать работоспособность антивирусного программного обеспечения и регулярность обновления антивирусных баз данного программного обеспечения;

3.2 не скачивать, не открывать и не запускать выполнение файлов неизвестного происхождения из сети Интернет, электронной почты и сменных носителей;

3.3 проверять на наличие вирусов любые файлы, скачанные из сети Интернет, электронной почты и сменных носителей;

3.4 не устанавливать самостоятельно на ОВТ программное обеспечение, не связанное с выполнением своих трудовых обязанностей и не предусмотренное технологическим процессом обработки информации на ОВТ;

3.5 при возникновении подозрения на наличие компьютерного вируса (нетипичная работа приложений, появление посторонних графических и прочих эффектов, искажение или исчезновение файлов, частое появление сообщений о системных ошибках) пользователь обязан:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения на своей рабочей станции зараженных вирусом файлов руководителя подразделения и Администратора информационной безопасности;
- провести самостоятельно, а в случае невозможности, совместно с Администратором информационной безопасности поиск, локализацию и уничтожение вирусов в файлах, путем полного сканирования существующим антивирусным программным обеспечением локальных жестких дисков и рабочих файлов на своей рабочей станции;
- в случае невозможности удаления вирусов из зараженных файлов проанализировать необходимость дальнейшего их использования в рабочем процессе, удалить зараженные файлы и воспользоваться их резервными копиями, либо передать зараженные файлы Администратору информационной безопасности для детального анализа возможностей их восстановления.

4 Обязанности Администратора информационной безопасности

Администратор информационной безопасности обязан:

4.1 контролировать работоспособность и регулярность обновления антивирусного программного обеспечения и антивирусных баз на рабочих станциях пользователей Школы;

4.2 оказывать методическую и практическую помощь пользователям в процессе удаления компьютерных вирусов и восстановления испорченных данных;

4.3 докладывать руководству Школы о фактах обнаружения на рабочих станциях пользователей Школы компьютерных вирусов, не удаляемых стандартными средствами антивирусного программного обеспечения и предпринятых мерах, по обеспечению должного уровня антивирусной защиты.

5 Ответственность

5.1 За нарушение требований данной Инструкции Администратор информационной безопасности, пользователи и Ответственные за эксплуатацию ОВТ, обрабатывающие информацию на ОВТ, могут быть привлечены к дисциплинарной ответственности.

5.2 Администратор информационной безопасности, пользователи и Ответственные за эксплуатацию ОВТ обязаны ознакомиться с настоящей Инструкцией, под личную подпись.

Лист ознакомления работников
к инструкции по проведению антивирусного контроля на объектах вычислительной техники (ОВТ)

№ п/п	Ф.И.О.	Дата	Подпись

Лист ознакомления работников
к инструкции по проведению антивирусного контроля на объектах вычислительной техники (ОВТ)

№ п/п	Ф.И.О.	Дата	Подпись

Лист ознакомления работников
к инструкции по проведению антивирусного контроля на объектах вычислительной техники (ОВТ)

№ п/п	Ф.И.О.	Дата	Подпись