УТВЕРЖДАЮ
Директор МОБУ СОШ №1 с.Буздяк
И.З. Сакаев

Инструкция по организации антивирусной защиты

1. Общие положения

1.1 Настоящая Инструкция устанавливает требования к организации антивирусной защиты и требования к порядку проведения антивирусного контроля в муниципальном общеобразовательном бюджетном учреждении средняя общеобразовательная школа № 1 с.Буздяк муниципального района Буздякский район Республики Башкортостан (далее – МОБУ СОШ № 1 с.Буздяк).

2. Порядок организации антивирусной защиты

2.1 Для организации антивирусной защиты в МОБУ СОШ № 1 с.Буздяк допускаются к использованию только лицензионное программное обеспечение.

2.2 Антивирусное средство защиты должно быть установлено на все средства вычислительной техники (далее – СВТ), используемые для обработки персональных данных в МОБУ СОШ № 1 с.Буздяк.

2.3 Установку, а также администрирование средств антивирусной защиты осуществляет администратор безопасности информационных систем (далее – администратор безопасности).

2.4 Администратор безопасности МОБУ СОШ № 1 с.Буздяк должен регулярно осуществлять или организовывать периодическое обновление антивирусных баз и контроль их работоспособностью, а также проводить периодическое тестирование всего установленного программного обеспечения и дискового пространства на предмет отсутствия компьютерных вирусов.

3. Порядок проведения антивирусного контроля

3.1 Ежедневно в начале работы при загрузке компьютера (для серверов локально-вычислительной сети – при перезапуске) в автоматическом режиме должен проводиться антивирусный контроль всех дисков и файлов.

3.2 Антивирусный контроль входящей и исходящей информации должен проводиться непосредственно после получения информации и перед отправкой (записью на съемный носитель) путем нажатия правой клавишей мыши на нужный файл (папку) и выбора из контекстного меню пункта «Проверить на вирусы».

3.3 При работе со съемными носителями информации пользователь обязан перед началом работы осуществить их проверку на предмет отсутствия компьютерных вирусов и иных вредоносных программ путем автоматической проверки флеш-носителей с помощью программного средства USB Disk Security или путем выбора из всплывающего окна пункта «Проверить и

исправить ошибки» при подключении устройства к СВТ.

3.4 Еженедельно администратор безопасности организовывает проведение плановой полной проверки СВТ, а также всех подключаемых носителей информации к данному СВТ на наличие или отсутствие вирусов.

3.5 При возникновении подозрения на наличие в системе компьютерного вируса (нетипичная работа программ, искажение данных, частое появление сообщений о системных ошибках и т.п.) пользователем должен быть проведён внеплановый антивирусный контроль СВТ. При необходимости для определения факта наличия или отсутствия вируса может быть привлечен администратор безопасности.

3.6 В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователь обязан:

- приостановить работу;
- поставить в известность о факте обнаружения зараженных вирусом файлов администратора безопасности, а также смежные отделы, использующие эти файлы в работе.

3.7 При обнаружении зараженных файлов администратор безопасности обязан:

- отключить Интернет соединение, в том числе подключение по локальной сети;
- поместить зараженные файлы в карантин;
- провести «лечение» или уничтожение зараженных файлов, а затем осуществить повторную проверку;
- в случае обнаружения на СВТ или на съемном носителе информации вируса, не поддающегося «лечению», в возможно короткие сроки обновить пакет антивирусных программ и провести повторное «лечение» зараженных файлов;
- при необходимости выполнить восстановление системы или переустановку операционной системы;
- по факту обнаружения зараженных вирусом файлов составить служебную записку на имя директора МОБУ СОШ № 1 с.Буздяк, в которой необходимо указать предположительный источник (отправителя, владельца и т.д.) зараженного файла, тип зараженного файла, характер содержащейся в файле информации, тип вируса и выполненные антивирусные мероприятия.

3.8 Пользователю СВТ запрещается:

- изменять настройки и конфигурацию средств антивирусной защиты;
- удалять или добавлять в систему какие-либо другие средства антивирусной защиты;
- использовать на СВТ съемные носители информации без предварительной проверки;
- запускать неизвестные файлы, пришедшие по электронной почте;
- игнорировать проведение антивирусных проверок СВТ, а также всплывающие уведомления средства антивирусного контроля.

4. Ответственность

4.1 Администратор безопасности, а также пользователи несут

ответственность за проведение мероприятий по антивирусному контролю, а также за ненадлежащее исполнение или неисполнение обязанностей, предусмотренных настоящей Инструкцией в рамках ст. 192 Трудового Кодекса Российской Федерации и ст. 273, 274 Уголовного кодекса Российской Федерации.