Утверждаю
Директор МОБУ СОШ №9
им.М.И.Кершенгольца
_____Черных Н.П.
28.09.2019

Инструкция
по организации антивирусной защиты в образовательных учреждениях

1.1 Защита программного обеспечения ИСПДн от вредоносного ПО осуществляется путем применения специализированных средств антивирусной защиты.
1.2 К использованию допускаются только лицензионные антивирусные средства, обладающие сертификатами регулирующих органов РФ.
1.3 Решение задач по установке и сопровождению средств антивирусной защиты возлагается на ответственного за систему защиты информации (СЗИ) ИСПДн.
1.4 Частота обновления баз данных средств антивирусной защиты устанавливается не реже 1 раза в сутки.
1.5 Все впервые вводимое в эксплуатацию программное обеспечение должно проходить обязательный антивирусный контроль.
1.6 Контроль системы управления средствами антивирусной защиты осуществляется централизованно с рабочего места ответственного за СЗИ ИСПДн.
1.7 Средства антивирусной защиты устанавливаются на всех рабочих станциях и сервере ОУ.
1.8 Ежедневно в установленное время в автоматическом режиме проводится антивирусный контроль всех дисков и файлов рабочих станций и сервера.
1.9 Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы, архивы), получаемая и передаваемая по телекоммуникационным каналам (включая электронную почту), а также информация на съемных носителях.
1.10 Контроль входящей информации необходимо проводить непосредственно после ее приема.
1.11 Контроль исходящей информации необходимо проводить непосредственно перед отправкой.
1.12 Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль.
1.13 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.) пользователь, обнаруживший проблему, должен провести внеочередной антивирусный контроль рабочей станции либо обратиться к ответственному за СЗИ ИСПДн.
1.14 При получении информации о возникновении вирусной эпидемии вне ОУ должно быть осуществлено информирование пользователей о возможной эпидемии и рекомендуемых действиях.
1.15 В случае обнаружения зараженных компьютерными вирусами файлов пользователи обязаны:

- приостановить работу;

- немедленно поставить в известность о факте обнаружения вируса ответственного за СЗИ ИСПДн;
- провести лечение зараженных файлов;
- в случае невозможности лечения обратиться к сотруднику, ответственному за СЗИ ИСПДн;

1.16 По факту обнаружения зараженных вирусом файлов сотрудник, ответственный за СЗИ ИСПДн, должен составить служебную записку, 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.

1.17 Пользователям запрещается отключать, выгружать или деинсталлировать средства антивирусной защиты на рабочих станциях.

1.18 Настройка параметров средств антивирусной защиты осуществляется в соответствии с руководствами по применению конкретных антивирусных средств.

1.19 Ответственный за СЗИ ИСПДн должен проводить расследования случаев появления вирусов для выявления причин и принятия соответствующих действий по их предотвращению.

1.20 Проводить периодическое тестирование функций средств антивирусной защиты.

1.21 Проводить тестирование функций средств антивирусной защиты при изменениях (внедрении новых средств, их обновлении, изменениях в системе).