

СОГЛАСОВАНО

Председатель профсоюзного комитета
МОУ СШ № 117


М.Ю.Рунаева
«29» май 2018 г.



УТВЕРЖДАЮ

Директор МОУ СШ № 117

Л.А.Абрамова
«29» май 2018 г.

Введена в действие приказом по школе
от «29» май 2018 г. № 144 Ⓚ

ИНСТРУКЦИЯ по антивирусной защите информационной системы персональных данных

Общие положения

Данный документ определяет правила и основные требования по обеспечению антивирусной защиты информационной системы персональных данных, используемой в МОУ СШ № 117.

Действие настоящей инструкции распространяется в полном объеме на ОУ и обязательно для выполнения всеми сотрудниками.

1 Инструкция по применению средств антивирусной защиты

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 администратора безопасности информационных систем.

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 администратора безопасности информационных систем

1.7 Средства антивирусной защиты устанавливаются на всех рабочих станциях и серверах ОУ.

1.8 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.

1.9 Контроль входящей информации необходимо проводить непосредственно после ее приема.

1.10 Контроль исходящей информации необходимо проводить непосредственно перед отправкой.

1.11 Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль.

1.12 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 администратору безопасности информационных систем.

1.13 При получении информации о возникновении вирусной эпидемии вне ОУ должно быть осуществлено информирование пользователей о возможной эпидемии и рекомендуемых действиях.

1.14 В случае обнаружения зараженных компьютерными вирусами файлов пользователи обязаны:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения вируса администратору безопасности информационных систем;
- провести лечение зараженных файлов;
- в случае невозможности лечения обратиться к администратору безопасности информационных систем;

1.15 По факту обнаружения зараженных вирусом файлов составляется служебная записка, 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.

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

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

Составитель:

Заместитель директора по УВР



Н.Ю.Бурлакова

