Подписан: МБОУ СОШ № 23
DN: STREET="УЛИЦА БОРЗИК, 43А", S=Ростовская область, L=" РАЙОН ОКТЯБРЬСКИЙ, ПОСЕЛОК КРАСНОГОРНЯЦКИЙ", C=RU, G=Галина Михайловна, SN=Ушакова, CN=МБОУ СОШ № 23, T=ДИРЕКТОР, O=МБОУ СОШ № 23, E=maurco@mail.ru, ИНН=006125018357, СНИЛС=05134429731, ОГРН=1026101411434
Основание: я подтверждаю этот документ
Местоположение: п.Красногорняцкий
Дата: 2022-08-15 14:31:52

Приложение № 1/25
«УТВЕРЖДАЮ»
Директор МБОУ СОШ № 23
Г.М.Ушакова/ Ушакова
Приказ № 305 от «08»августа 2022г.

Правила и основные требования по обеспечению антивирусной защиты ИСПДн в МБОУ СОШ № 23

1. Общие положения

Данный документ определяет правила и основные требования по обеспечению антивирусной защиты ИСПДн в МБОУ СОШ № 23 п. Красногорняцкий (далее - Учреждения) и устанавливает ответственность за их выполнение.

Действие настоящей инструкции распространяется в полном объеме на Учреждение и обязательна для выполнения всеми сотрудниками.

2. Инструкция по применению средств антивирусной защиты

2.1.Защита программного обеспечения ИСПДн от вредоносного ПО осуществляется путем применения специализированных средств антивирусной защиты.

2.2. К использованию допускаются только лицензионные антивирусные средства, обладающие сертификатами регулирующих органов РФ.

2.3. Решение задач по установке и сопровождению средств антивирусной защиты возлагается на ответственного за СЗИ ИСПДн.

2.4. Частота обновления баз данных средств антивирусной защиты устанавливается не реже 1 раза в сутки.

2.5. Все впервые вводимое в эксплуатацию программное обеспечение должно проходить обязательный антивирусный контроль.

2.6. Контроль системы управления средствами антивирусной защиты осуществляется централизованно с рабочего места ответственного за СЗИ ИСПДн.

2.7. Средства антивирусной защиты устанавливаются на всех рабочих станциях и серверах Учреждения.

2.8. Ежедневно в установленное время в автоматическом режиме проводится антивирусный контроль всех дисков и файлов рабочих станций и серверов.

2.9. 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.

2.10. Контроль входящей информации необходимо проводить непосредственно после ее приема.

2.11. Контроль исходящей информации необходимо проводить непосредственно перед отправкой.

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

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

2.14. 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;

2.15.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.

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

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

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

2.19. Пользователи должны быть ознакомлены с данной инструкцией под роспись.

2.20. Проводить периодическое тестирование функций средств антивирусной защиты.

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