Муниципальное общеобразовательное учреждение
«Лицей № 7 Дзержинского района Волгограда»

ПРИНЯТО

на педагогическом совете
протокол от 30.08.2021г. № 18
Председатель педсовета
_____ А.Н. Каинов

ВВЕДЕНО

в действие приказом
от 31.08.2021г. № 234
Директор
_____ А.Н. Каинов

ИНСТРУКЦИЯ

31.08.2021г № 02.23.108
Волгоград

каинов Андреи Николаевич я подтверждаю этот документ своей удостоверяющей подписью ул. 51-й Гвардейской Дивизии, 59, Волгоград 2021.11.11 14:38: 03+04'00'

Каинов Андрей Николаевич

по компьютерной безопасности (использование лицензионного ПО, программы фильтрации, антивирусной программы)

1. Общие положения

1.1. В МОУ «Лицей №7 Дзержинского района Волгограда» (далее-Лицей) директором назначается лицо, ответственное за компьютерную безопасность (использование лицензионного ПО, программы фильтрации, антивирусной программы). В случае отсутствия назначенного лица вся ответственность за обеспечение антивирусной защиты ложится на директора Лицея.

1.2. В Лицее используется только лицензионное программное обеспечение, антивирусное программное обеспечение.

1.3. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях (магнитных дисках, лентах, CD-ROM и т.п.). Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

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

2. Требования к проведению мероприятий по компьютерной безопасности

2.1. Установить последние обновления операционной системы Windows (http://update. Microsoft.com).

2.2. Включить режим автоматической загрузки обновлений. (Пуск —> Настройка —> Панель управления —> Автоматическое обновление —> Автоматически загружать и устанавливать на компьютер рекомендуемые обновления).

2.3. Скачать с сайта www.Microsoft.com программное обеспечение Windows Defender и установить на все компьютеры. Включить режим автоматической проверки. Включить режим проверки по расписанию каждый день.

2.4. Установить антивирусное программное обеспечение на каждый компьютер. Включить режим автоматического сканирования файловой системы. Включить режим

ежедневной автоматической проверки всей файловой системы при включении компьютера. Активировать функцию ежедневного автоматического обновления антивирусных баз.

2.5. Ежедневно проверять состояние антивирусного программного обеспечения, а именно:

- режим автоматической защиты должен быть включен постоянно;
- дата обновления антивирусных баз не должна отличаться более чем на несколько дней от текущей даты;
- просматривать журналы ежедневных антивирусных проверок. Контролировать удаление вирусов при их появлении.

2.6. Не реже одного раза в месяц посещать сайт update.microsoft.com и проверять установлены ли последние обновления операционной системы.

2.7. Быть крайне осторожным при работе с электронной почтой. Категорически запрещается открывать присоединенные к письмам, полученным от незнакомых лиц.

2.8. Контролировать посещение Интернет сайтов пользователями. Не допускать посещения т.н. «хакерских», порно и других сайтов с потенциально вредоносным содержанием.

2.9. В обязательном порядке проверять антивирусным программным обеспечением любые внешние носители информации перед началом работы с ними.

2.10. При появлении признаков нестандартной работы компьютера («тормозит», на экране появляются и исчезают окна, сообщения, изображения, самостоятельно запускаются программы и т.п.) немедленно отключить компьютер от Ethernet сети, загрузить компьютер с внешнего загрузочного диска (CD, DVD) и произвести полную антивирусную проверку всех дисков компьютера. При появлении аналогичных признаков после проделанной процедуры переустановить операционную систему с форматированием системного раздела диска.

2.11. В начале работы при загрузке компьютера в автоматическом режиме должно выполняться обновление антивирусных баз и серверов.

2.12. Периодические проверки электронных архивов должны проводиться не реже одного раза в неделю.

2.13. Внеочередной антивирусный контроль всех дисков и файлов персонального компьютера должен выполняться:

- непосредственно после установки (изменения) программного обеспечения компьютера должна быть выполнена антивирусная проверка на серверах и персональных компьютерах лицея;
- 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.);
- при отправке и получении электронной почты пользователь обязан проверить электронные письма на наличие вирусов.

2.14. В случае обнаружения, при проведении антивирусной проверки, зараженных компьютерными вирусами файлов или электронных писем пользователи обязаны:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов ответственного за обеспечение информационной безопасности в Лицее;
- совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;
- провести лечение или уничтожение зараженных файлов.

3. Ответственность

3.1. Ответственность за организацию антивирусной защиты возлагается на директора Лицея или лицо, им назначенное.

3.2. Ответственность, за проведение мероприятий антивирусного контроля в лицее и соблюдение требований настоящей Инструкции, возлагается на ответственного за обеспечение антивирусной защиты.

3.3. Периодический контроль за состоянием антивирусной защиты в Лицее осуществляется руководителем.

Заместитель директора Т.М.Гуляева