

Муниципальное общеобразовательное учреждение
«Средняя школа с углубленным изучением
отдельных предметов №97
Дзержинского района Волгограда»

Утверждаю:
Директор МОУ СОШ №97
С.А. Казин
«07» февраля 2015 г.



Инструкция

«06» февраля 2015 г. № 01-26-14

Волгоград

По компьютерной безопасности

1. Установить последние обновления операционной системы Windows (<http://windowsupdate.microsoft.com>)
2. Включить режим автоматической загрузки обновлений. (Пуск->Настройка->панель управления->Автоматическое обновление->Автоматически загружать и устанавливать на компьютер рекомендуемые обновления).
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.
4. Активировать встроенный брандмауэр Windows (Пуск->Настройка->панель управления->Брандмауэр Windows->Включить).
5. 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.
6. Ежедневно проверять состояние антивирусного программного обеспечения, а именно
 - a. Режим автоматической защиты должен быть включен постоянно
 - b. Дата обновления антивирусных баз не должна отличаться более чем на несколько дней от текущей даты.
 - c. Просматривать журналы ежедневных антивирусных проверок. Контролировать удаление вирусов при их появлении.
7. Не реже одного раза в месяц посещать сайт <http://windowsupdate.microsoft.com> и проверять установлены ли последние обновления операционной системы.
8. Быть крайне осторожным при работе с электронной почтой. Категорически запрещается открывать присоединенные к письмам, полученным от незнакомых лиц, файлы.
9. Контролировать посещение Интернет сайтов пользователями. Не допускать посещения т.н. «хакерских», порно и других сайтов с потенциально вредоносным содержанием.
10. Проверять работу контентной фильтрации на ПК (Интернет Цензор) не реже одного раза в неделю.

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

12. 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 специальными утилитами (например, [Лечащая утилита Dr.Web CureIt!](#)). При появлении аналогичных признаков после проделанной процедуры переустановить операционную систему с форматированием системного раздела диска.

13. Для обеспечения безопасности и соблюдения коммерческой тайны, а также для достижения высокой эффективности работы, сохранения жизни и здоровья сотрудников, предотвращения поломок компьютерной техники, рекомендуется следовать нижеприведенным инструкциям.

- Использовать только рекомендованное программное обеспечение и операционные системы, см. Приложение 1.
- Не допускать использования нежелательного ПО, см. Приложение 2.
- Не устанавливать самостоятельно любое ПО, кроме указанного в Приложении 1.
- Не изменять самостоятельно настройки операционной системы.
- Не устанавливать и не удалять драйвера оборудования.
- Не отключать установленное ПО для борьбы с вирусами и прочими заражениями.
- Не допускать третьих лиц к вверенному оборудованию.
- Не разглашать пароли.
- Информировать о возможных утечках коммерческой информации.
- Не использовать без разрешения администрации съемные диски, флэшки, не подключать к компьютеру сотовые телефоны, фотоаппараты и т.п.
- Своевременно докладывать о поломках и сбоях компьютерной техники.
- Поддерживать чистоту вверенного оборудования.
- Остерегаться поражения электрическим током, не браться руками за оголенные провода.
- Правильно сидеть на рабочем месте, не допускать повышенной нагрузки на позвоночник.
- Соблюдать режим работы, не допускать переутомления органов зрения.
- Не приближаться к компьютеру, если существует вероятность возникновения искры от статического напряжения.
- В случае возникновения ситуации, не описанной в данной инструкции, проконсультироваться с системным администратором.

Приложение 1. Разрешенное ПО и операционные системы

1. Операционная система – Windows, версия не ниже SP3. Использование самосборных дистрибутивов, таких как ZverCD, недопустимо.
2. Офисный пакет – Microsoft Office, версия не ниже 11.8 (2003 SP3), или OpenOffice.org, версия не ниже 3.3.0.
3. Архиватор – WinRAR, версия не ниже 4.01, или 7-zip, версия не ниже 9.20.
4. С целью снижения риска заражения вирусами при работе в Интернете, рекомендуется использовать браузер Mozilla FireFox, версии не ниже 6.0, или Opera, версия не ниже 11.50.
5. Антивирусная программа – Dr.Web.

6. ПО для работы с 1С, соответствующей версии.
7. Adobe Reader, версии не ниже 10.1.
8. Программа для воспроизведения звуковых файлов – Winamp, версия не ниже 5.05.
9. В случае необходимости работы с видео файлами, пакет кодеков K-Lite Codec Pack Full, версии не ниже 7.6.0, в состав которого входит видеопроигрыватель Media Player Classic.

Приложение 2. ПО, использование которого недопустимо

1. QiP.Online и ему подобные программы.
2. Программы, модифицирующие настройки ОС Windows и ее реестра.
3. Альтернативные антивирусы, и файрволы (брандмауэры), т.к. антивирус Dr.Web в полной мере берет на себя функции защиты ПК и не поддерживает совместную работу со сторонними антивирусами.
4. Обработчики расписаний, такие как nncron.
5. ПО, открывающее компьютер для удаленного управления, такое как RAdmin, кроме специально оговоренных случаев.