МУНИЦИПАЛЬНОЕ
БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА № 35 ГОРОДСКОГО ОКРУГА САМАРА

«Утверждаю»
Директор МБОУ СОШ № 35
г.о. Самара
_____Н.С.Мушкат
«1» сентября 2014 г.

ИНСТРУКЦИЯ ПО АНТИВИРУСНОЙ ЗАЩИТЕ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Самара, 2014

Общие положения

Компьютерный вирус является разрушающей программной закладкой и характеризуется значительным деструктивным потенциалом для программ, данных и любой информации, хранящейся на компьютерах и магнитных носителях. Особую опасность представляет то обстоятельство, что компьютерные вирусы могут скрытно и постепенно уничтожать, либо мгновенно разрушать хранящуюся в компьютере и магнитных носителях информацию, при этом также могут пострадать аппаратные средства.

Основными путями вирусного вторжения являются неквалифицированное обращение пользователей с компьютерной техникой при использовании ими зараженных дискет и программ, либо целенаправленное спланированное воздействие извне с использованием компьютерных вирусов. При любых обстоятельствах это затрагивает вопросы защиты информации и интересы собственной безопасности Правительства области.

Порядок, обеспечивающий безопасную работу на компьютере и с магнитными носителями:

1. Приобретение средств вычислительной техники (СВТ) и программных продуктов осуществляется исключительно имеющих лицензию (сертификат).

Вновь поступающее программное обеспечение должно быть подвергнуто входному контролю – проверке на отсутствие вирусов.

2. Каждый компьютер решением директора школы персонально закрепляется за ответственным за его эксплуатацию подготовленным работником.

3. Допуск сотрудников к самостоятельной работе на компьютерах и с внешними носителями осуществляется только после овладения ими навыками в работе с компьютером, антивирусными пакетами программ.

4. На компьютерах может использоваться программное и аппаратное обеспечение, необходимое только для выполнения служебной деятельности и согласованное с комитетом по информационным технологиям. Запрещается использовать на компьютерах программные и аппаратные средства, не имеющих лицензию (сертификат).

5. На любом, работающем компьютере, в обязательном порядке должен быть установлен и активирован пакет антивирусных программ. Ответственность за это несет конкретный, отвечающий за его работоспособность сотрудник, а также администратор безопасности подразделения. Установка средств антивирусного контроля (в том числе настройка параметров средств антивирусного контроля) на автоматизированных рабочих местах (АРМ) осуществляется специалистами в соответствии с руководствами по применению конкретных антивирусных средств. Антивирусные средства устанавливаются при вводе в эксплуатацию автоматизированной системы или при их плановой замене.

6. Периодически, не реже 1 раза в четверть, работник, ответственный за компьютер, проверяет его дисковое пространство с использованием антивирусного пакета программ на возможное наличие компьютерного вируса.

7. Пользователь (в случае необходимости совместно с администратором безопасности подразделения) обязан проводить антивирусный контроль любой электронной информации (текстовые файлы любых форматов, файлы данных, исполняемые файлы, архивируемые/разархивируемые файлы и т.д.), получаемой и передаваемой по телекоммуникационным каналам, а также информации на съемных носителях (магнитных дисках, CD-ROM, Flash - память и т.п.).

8. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователь обязан:

- приостановить работу;

- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов специалистов по антивирусной защите, по защите информации (в

автоматизированных системах обработки информации ограниченного доступа), владельца зараженных файлов, а также смежные подразделения, использующие эти файлы в работе;

- совместно со специалистом по антивирусной защите провести анализ необходимости дальнейшего использования зараженных вирусом файлов;

- провести лечение или уничтожение зараженных файлов (при необходимости для выполнения требований данного пункта привлечь специалистов по информационным технологиям, по защите информации);

Все факты обнаружения зараженных вирусом файлов администратор безопасности АС заносит в «Журнал учета работы АС» (приложение 1), где отображается тип зараженного файла, характер содержащейся в файле информации, название вируса и тип вируса и выполненные антивирусные мероприятия.

Ответственность

Ответственность за поддержание установленного в настоящей Инструкции порядка проведения антивирусного контроля возлагается на администратора безопасности информации в структурном подразделении.

Пользователь и администратор безопасности несут ответственность за качество и своевременность выполнения задач и функций, возложенных на них в соответствии с настоящей Инструкцией.

С инструкцией ознакомлены:

Зам. директора по НМР и безопасности — Т.С. Милоенко

Е.В. Тринбачёва

Зам. директора по дошкольному отделению — Е.Г. Кузнецова

Зам. директора по АХЧ
Системный администратор — А. Ю.Ситников

Журнал регистрации работ АС:

Дата	Наименование работ	Ф.И.О. исполнителя работ	Роспись
1	2	3	4
	Обновление антивирусной базы, сканирование дисков	ФИО	
	Антивирусная проверка АС Вирусов не обнаружено	Ф.И.О.	
	Обновление антивирусной базы. Антивирусная проверка АС. Обнаружен вирус «название вируса». Лечение проведено антивирусными средствами. О заражении поставлены в известность администраторы безопасности подразделений _____.	Ф.И.О.	