Утверждаю
Заведующий МБДОУ ДС №39
_____О.И. Салихова
_____ от _____г.

ИНСТРУКЦИЯ ПО ОРГАНИЗАЦИИ АНТИВИРУСНОЙ ЗАЩИТЫ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

1. Общие требования

1.1. Настоящая Инструкция определяет требования к организации защиты объектов информатизации от разрушающего воздействия компьютерных вирусов и устанавливает ответственность сотрудников ДОУ, эксплуатирующих и сопровождающих информационные системы (далее - ИС) организации, за их выполнение.

1.2. К использованию в ИС допускаются только лицензионные антивирусные средства, централизованно закупленные у разработчиков (поставщиков) указанных средств и прошедшие в установленном порядке процедуру оценки соответствия требованиям по безопасности.

1.3. После установки и настройки средств антивирусного контроля в обязательном порядке должно быть произведено тестирование системы антивирусной защиты.

1.4. Ответственность за организацию и проведение мероприятий антивирусного контроля в подразделении организации в соответствии с требованиями настоящей Инструкции возлагается на руководителя ДОУ.

1.5. Ответственность за ежедневный антивирусный контроль в процессе эксплуатации ИС организации и своевременное информирование руководителя ДОУ в случае обнаружения действий вредоносных программ возлагается на пользователей ИС.

2. Применение средств антивирусного контроля

2.1. Ежедневно в начале работы при загрузке компьютеров в автоматическом режиме должен проводиться антивирусный контроль всех электронных носителей информации, подключаемых к ИС.

Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), информация на съемных носителях.

Настройка средств антивирусной защиты должна реализовывать следующие функции:

-непрерывный автоматический мониторинг информационного обмена в ИС с целью выявления программно-математического воздействия (далее - ПМВ);

-автоматическую проверку на наличие вредоносных программ или последствий ПМВ при импорте в ИС всех программных модулей (прикладных программ), которые могут содержать вредоносные программы, по их типовым шаблонам и с помощью эвристического анализа;

-реализацию механизма автоматического блокирования обнаруженных вредоносных программ путем их удаления из программных модулей или уничтожения;

-автоматическую проверку критических областей автоматизированных рабочих мест и серверов, таких как системная память, загрузочные секторы дисков, объекты автозапуска, каталоги операционной системы "system" и "system32", при каждом запуске операционной системы;

-полную автоматическую проверку носителей информации всех автоматизированных рабочих мест и серверов не реже одного раза в неделю;

-регулярное обновление антивирусных баз и программных модулей средств антивирусной защиты;

-автоматическое документирование состояния системы антивирусной защиты ИС.

2.2. Пользователи ИС при работе со съемными носителями информации (flash-накопители, дискеты 3,5", CD/DVD диски, жесткие диски USB и т.д.) обязаны перед началом работы осуществить их проверку на предмет отсутствия вредоносных программ, выполнив следующие действия:

-подключить съемный носитель информации;

-открыть значок Рабочего стола "Мой компьютер";

-установить курсор мыши на имя выбранного носителя.

По правой клавише мыши открыть контекстное меню Microsoft Windows и выбрать пункт, запускающий антивирусную проверку электронного носителя информации.

2.3. Файлы, помещаемые в электронный архив должны в обязательном порядке проходить антивирусный контроль. Периодические проверки электронных архивов должны проводиться не реже одного раза в месяц.

2.4. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения компьютера пользователем также должна быть выполнена антивирусная проверка электронных средств обработки персональных данных.

2.5. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, появление сообщений о системных ошибках и т.п.) пользователь ИС самостоятельно или вместе с руководителем ДОУ должен провести внеочередной антивирусный контроль рабочей станции.

В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов:

-пользователи ИС обязаны:

-приостановить работу в ИС;

-немедленно поставить в известность о факте обнаружения зараженных вирусом файлов руководителя ДОУ и других сотрудников, использующих эти файлы в работе;

совместно с руководителем ДОУ провести анализ необходимости дальнейшего использования зараженных файлов;

-руководитель ДОУ обязан провести лечение зараженных файлов или их гарантированное удаление.