Утверждаю

Заведующая МАДОУ «Центр развития ребенка-детский сад «Солнышко»

_____О.П.Татаурова

«_____»_____20____Г

Инструкция по организации антивирусной защиты

Настоящая Инструкция определяет требования к организации защиты АС организации от разрушающего воздействия со стороны злонамеренного ПО (компьютерных вирусов, сетевых червей, «троянских коней», логических бомб и т.п.) и устанавливает ответственность руководителей и сотрудников подразделений, эксплуатирующих и сопровождающих АС, за их выполнение.

К использованию в организации допускаются только лицензионные антивирусные средства, централизованно закупленные у разработчиков (поставщиков) указанных средств, рекомендованные к применению подразделениями автоматизации и безопасности информации.

В случае необходимости использования антивирусных средств, не вошедших в перечень рекомендованных, их применение необходимо согласовать с подразделениями автоматизации и безопасности информации.

Установка средств антивирусного контроля на компьютерах на серверах и рабочих станциях АС осуществляется уполномоченными сотрудниками подразделения автоматизации в соответствии с «Инструкцией по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств АС».

Настройка параметров средств антивирусного контроля осуществляется сотрудниками подразделения автоматизации в соответствии с руководствами по применению конкретных антивирусных средств.

Применение средств антивирусного контроля

Антивирусный контроль всех дисков и файлов рабочих станций должен проводиться ежедневно в начале работы при загрузке компьютера (для серверов - при перезапуске) в автоматическом режиме.

Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съёмных носителях (магнитных дисках, лентах, CD-ROM и т.п.). Разархивирование и контроль входящей информации необходимо проводить непосредственно после её приёма на выделенном автономном компьютере или, при условии начальной загрузки операционной системы в

оперативную память компьютера с заведомо «чистой» (не заражённой вирусами) и защищённой от записи системной дискеты, - на любом другом компьютере. Возможно применение другого способа антивирусного контроля входящей информации, обеспечивающего аналогичный уровень эффективности контроля. Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съёмный носитель).

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

Установка (изменение) системного и прикладного программного обеспечения осуществляется на основании «Инструкции по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств автоматизированной системы организации».

Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения компьютера должна быть выполнена антивирусная проверка:

- на защищаемых серверах и рабочих станциях - ответственным за обеспечение безопасности информации подразделения;
- на других серверах и рабочих станциях АС не требующих защиты, - лицом, установившим (изменившим) программное обеспечение, - в присутствии и под контролем руководителя данного подразделения или сотрудника, им уполномоченного.

Факт выполнения антивирусной проверки после установки (изменения) программного обеспечения должен регистрироваться в специальном журнале подразделения за подписью лица, установившего (изменившего) программное обеспечение, и лица, его контролировавшего.

Действия при обнаружении вирусов

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.) сотрудник подразделения самостоятельно или вместе с ответственным за обеспечение безопасности информации подразделения (технологического участка) должен провести внеочередной антивирусный контроль своей рабочей станции. При необходимости привлечь специалистов подразделения автоматизации для определения ими факта наличия или отсутствия компьютерного вируса.

В случае обнаружения при проведении антивирусной проверки заражённых компьютерными вирусами файлов сотрудники подразделений обязаны:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения заражённых вирусом файлов руководителя и ответственного за обеспечение безопасности информации своего подразделения, владельца заражённых файлов, а также смежные подразделения, использующие эти файлы в работе;
- совместно с владельцем заражённых вирусом файлов провести анализ необходимости дальнейшего их использования;
- провести лечение или уничтожение заражённых файлов (при необходимости для выполнения требований данного пункта привлечь специалистов подразделения автоматизации);
- в случае обнаружения нового вируса, не поддающегося лечению применяемыми антивирусными средствами, передать заражённый вирусом файл на гибком магнитном диске в подразделение автоматизации для дальнейшей отправки его в организацию, с которой заключён договор на антивирусную поддержку;
- по факту обнаружения заражённых вирусом файлов составить служебную записку в отдел обеспечения безопасности информации, в которой необходимо указать предположительный источник (отправителя, владельца и т.д.) заражённого файла, тип заражённого файла, характер содержащейся в файле информации, тип вируса и выполненные антивирусные мероприятия.

Ответственность

Ответственность за организацию антивирусного контроля в подразделении, эксплуатирующем подсистему АС, в соответствии с требованиями настоящей Инструкции возлагается на руководителя подразделения.

Ответственность за проведение мероприятий антивирусного контроля в подразделении и соблюдение требований настоящей Инструкции возлагается на ответственного за обеспечение безопасности информации и всех сотрудников подразделения, являющихся пользователями АС.

Периодический контроль за состоянием антивирусной защиты, а также за соблюдением установленного порядка антивирусного контроля и выполнением требований настоящей Инструкции сотрудниками подразделений организации осуществляется подразделением обеспечения безопасности ИТ.