

1.2.5. проведение профилактических мероприятий по предотвращению и ограничению вирусных эпидемий, включающих загрузку и развертывание специальных правил нейтрализации (отражению, изоляции и ликвидации) вредоносных программ на основе рекомендаций по контролю атак, подготавливаемых разработчиком средств защиты от вредоносных программ и другими специализированными экспертными антивирусными службами  до того, как будут выпущены файлы исправлений, признаков и антивирусных сигнатур.

1.2.6. проведение регулярных проверок целостности критически важных программ и данных. Наличие лишних файлов и следов несанкционированного внесения изменений должно быть зарегистрировано в журнале и расследовано;

1.2.7. внешние носители информации неизвестного происхождения следует проверять на наличие вирусов до их использования;

1.2.8. необходимо строго придерживаться установленных процедур по уведомлению о случаях поражения автоматизированной информационной среды компьютерными вирусами и принятию мер по ликвидации последствий от их проникновения;

1.2.9. следует иметь планы обеспечения бесперебойной работы Учреждения для случаев вирусного заражения, в том числе планы резервного копирования всех необходимых данных и программ и их восстановления. Эти меры особенно важны для сетевых файловых серверов, поддерживающих большое количество рабочих станций.

1.3.   Технологические инструкции

1.3.1.В ДОУ руководителем должно быть на­значено лицо, ответственное за антивирусную защиту, в должностные инструкции для которого должны быть прописаны порядок действия в период вирусных эпидемий, порядок действий при возникновении внештатных ситуаций, связанных с работоспособностью средств антивирусной защиты, порядок действий для устранения последствий заражений. В противном случае вся ответственность за обеспечение антивирусной защиты ложится на руководителя Учреждения.

1.3.2. В Учреждении может использоваться только лицензион­ное антивирусное программное обеспечение либо свободно-распространяемое программное обеспечение.

1.3.3. Обязательному антивирусному контролю подле­жит любая информация (текстовые файлы любых фор­матов, файлы данных, исполняемые файлы, почтовые сообщения), получае­мая и передаваемая по телекоммуникационным каналам связи, а также информация, находящаяся на съёмных носителях (магнитных дисках, лентах, CD-ROM, DVD, накопителях и т.п.). Контроль исходящей ин­формации необходимо проводить непосредственно пе­ред архивированием и отправкой (записью на съёмный носитель).

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

1. **Требования к проведению мероприятий по антивирусной защите**

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

2.2.  Периодические проверки электронных архивов должны проводиться не реже одного раза в неделю, данные, расположенные на рабочих станциях пользователей – ежедневно, в ночное время по расписанию.

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

2.3.1. Непосредственно после установки (измене­ния) программного обеспечения компьютера должна быть выполнена антивирусная проверка на серверах и персональных компьютерах учреждения.

2.3.2. 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.).

2.3.3. При отправке и получении электронной почты оператор электронной почты обязан проверить электронные письма и их вложения на наличие вирусов.

2.4. В случае обнаружения заражённых вирусами файлов или электронных писем пользователи обязаны:

2.4.1.Приостановить работу.

2.4.2. Немедленно поставить в известность о факте обнаружения заражённых вирусом файлов ответственного за обеспечение антивирусной защиты (в случае его отсутствия – заведующему) ДОУ.

2.4.3.Совместно с владельцем заражённых вирусом файлов провести анализ необходимости дальнейшего их использования.

2.4.4.Провести лечение или уничтожение заражённых файлов.

1. **Ответственность**

3.1.Ответственность за организацию антивирусной защиты возлагается на руководителя Учреждения или лицо, его замещающее.

3.2. Ответственность за проведение мероприятий ан­тивирусного контроля в ДОУ  возлагается на ответственного за обеспечение антивирусной защиты, соблюдение требований настоящей Инструкции при работе на персональных рабочих станциях возлагается на пользователей данных станций.

3.3.Периодический контроль за состоянием антиви­русной защиты в ДОУ осуществляется руководителем и фиксируется Актом проверки (не реже 1 раз в квартал).

Заведующая   МБДОУ ДСКВ № 9 «Олененок»\_\_\_\_\_\_\_\_Н. Д.Фесенко