

- на других серверах и РС 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 установке (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 ОА для определения ими факта наличия или отсутствия компьютерного вируса.

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

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