Инструкция по защите информации от компьютерных вирусов

1. Общие положения

1.1. Инструкция входит в комплект инструктивно-технологической документации по использованию ПЭВМ.

1.2. Инструкция разработана для пользователей ПЭВМ а также для администраторов информационной безопасности (в дальнейшем - администраторов).

1.3. Рекомендации имеют общий характер. Конкретные методы выявления компьютерных вирусов (в дальнейшем - вирусов) и методы борьбы с ними отражены в эксплуатационной документации на антивирусные программные (программно-аппаратные) средства.

1.4. Защита от вирусов состоит из нескольких этапов. На первом этапе выполняются регулярные профилактические работы согласно настоящей Инструкции. На втором этапе производится анализ ситуации проявления вируса (вирусов) и причины появления. И на третьем этапе выполняется уничтожение вируса (вирусов) из ПЭВМ.

1.5. Для обеспечения проверки программных средств на наличие вирусов создается и ведется банк характеристик существующих вирусов банк антивирусных программ. В необходимых случаях для анализа выявленных вирусов могут привлекаться сторонние организации.

1.6. По факту выявления вирусов проводится служебное расследование специалистами подразделения информатизации.

1.7. Настоящие рекомендации доводятся под роспись до лиц, допущенных к работе на ПЭВМ.

2. Наиболее характерные внешние проявления вирусов

2.1. Вирус представляет собой программу, которая разрушает информацию на магнитных носителях или нарушает работу ПЭВМ, а также обладает способностью к размножению, т.е. вирус может самостоятельно внедряться в другие программы, переносить себя на диски и дискеты, передаваться локальной компьютерной сети.

2.2 Можно выделить несколько видов воздействия вирусов на ПЭВМ:

- вирусы разрушительного действия;
- вирусы, замедляющие работу ПЭВМ;
- вирусы рекламного характера;
- вирусы-шутки.

2.3. Самые опасные вирусы - это вирусы разрушительного действия. Наиболее характерные внешние проявления вирусов этого вида:

- осыпание различных символов с экрана;
- появление на экране дисплея световых пятен, черных областей или символов, не запланированных рабочими программами;
- самопроизвольная перезагрузка операционной системы;
- зависание компьютера;
- появление неисправных участков (кластеров) на «винчестере»;
- неожиданные действия рабочих программ (не предусмотренные документацией на программы);
- искажения данных в обрабатываемых файлах.

2.4. Вирусы, замедляющие работу ПЭВМ, проявляют себя тем, что работа процессора замедляется в 30-40 раз.

2.5. Вирусы рекламного характера и вирусы-шутки хотя и не портят информацию в ПЭВМ, однако замедляют работу или навязывают пользователю ненужные диалоги, что также замедляет весь процесс решения задачи.

2.6. Некоторые вирусы проявляют себя внешне тем, что изменяют дату и время создания файла, хотя внутренние изменения могут быть и разрушительными.

2.7. Некоторые внешние неожиданные отклонения в работе ПЭВМ, описанные выше, не обязательно являются следствием наличия вирусов. Так, появление неисправных кластеров на «винчестере» может быть вызвано действительно неисправностью устройства, что определяется анализом ситуации.

3. Профилактика вирусов

3.1. Регулярно проводимые профилактические работы по выявлению вирусов могут полностью исключить появление и распространение вирусов в ПЭВМ. Поэтому целесообразно включать эти работы в планы работ подразделений. К основным профилактическим работам и мероприятиям относятся:

- ежедневная автоматическая проверка наличия вирусов при включении ПЭВМ;
- регулярная (не реже одного раза в месяц) комплексная проверка наличия вирусов во всех ПЭВМ, даже при отсутствии внешних проявлений вирусов;
- проверка наличия вирусов в ПЭВМ, вернувшихся с ремонта (в том числе гарантийного) в сторонних организациях;
- изучение информации по сообщениям в компьютерных журналах и газетах о новых вирусах;
- создание резервной копии программного продукта сразу же после приобретения;
- системные дискеты и дискеты с наиболее важными программами защищаются от записи на них информации путем установки переключателя на 3-5«-дискетах в положение только чтения - тем самым вирусы не смогут проникнуть на дискеты;
- тщательная проверка всех поступающих и купленных программ и баз данных; проверку необходимо выполнять либо на ПЭВМ без «винчестера», либо на отдельно выделенной ПЭВМ, не входящей в локальную сеть;
- ограничение доступа к ПЭВМ посторонних лиц.

3.3. Для ежедневной автоматической проверки наличия вирусов при включении ПЭВМ необходимо включить в файл AUTOEXEC.BAT команду запуска антивирусной программы - ревизора, например, AVP. Это включение выполняет программист управления информатизации.

3.4 Регулярную комплексную проверку наличия вирусов выполняет администратор. Администратор использует для проверки специальные дискеты с антивирусными программами.

3.5. При обнаружении вирусов в ПЭВМ, работающей в локальной сети, проверке подлежат все ПЭВМ, включенные в эту сеть.

3.6. Создание резервной копии программного продукта выполняет программист, ответственный за внедрение этого программного продукта.

3.7. Проверку всех поступающих и купленных программ выполняет управление информатизации.

4. Анализ ситуации

4.1. Если антивирусные программы выдают на экран дисплея сообщения о подозрении на наличие вирусов в ПЭВМ, то прежде всего необходимо убедиться в действительном наличии вирусов. Возможны ситуации, при которых эти сообщения являются следствием неисправности компьютера. Также появление сообщений антивирусных программ может быть вызвано разрушением программного обеспечения вследствие каких-либо аномальных электрических процессов.

4.2. Анализ ситуации наличия вирусов или неисправности какого-либо устройства ПЭВМ выполняет администратор. При анализе могут использоваться специальные программы проверки исправности ПЭВМ, например, программа Sys Info из пакета Norton Utilites и CHECKIT. В результате анализа делается вывод либо об уничтожении вирусов, либо о необходимости ремонта ПЭВМ.

4.3. Если вирус проник в ПЭВМ с дискеты, то необходимо определить источник дискеты и, если источник информации на дискете находится в тональном банке, то необходимо проверить на наличие вирусов ПЭВМ - источник информации на дискете. Если источник дискеты - коммерческая или другая организация, то необходимо сообщить в эту организацию о факте выявления вирусов и в дальнейшем обратить особое внимание на дискеты, поступающие из этой организации.

4.4. В случае действительного наличия вирусов привлекаются специалисты подразделения информатизации для проведения служебного расследования.

5. Уничтожение вирусов

5.1. Уничтожение вирусов выполняется администратором с привлечением других специалистов подразделения информатизации.

5.2. Если вирус поразил какие-либо программы, то уничтожение вируса выполняется путем уничтожения программы на винчестере либо на съемном носителе информации. После уничтожения зараженной программы необходимо восстановить программу, используя резервную копию программы.

5.3. Если вирус поразил файлы, то вирус уничтожается либо путем стирания этих файлов, либо путем использования специальных лечащих программ. Использование лечащих программ не дает полной гарантии восстановления файла. Поэтому после лечения необходима проверки восстановления данного файла. Лечащие программы используются лишь в тех случаях, когда отсутствует резервная копия зараженной программы либо файла с данными, либо восстановление уничтоженного файла с помощью резервной копии очень трудоемко.

5.4. В любом случае после уничтожения вирусов и восстановления зараженных программ и файлов с данными необходимо еще раз выполнить проверку наличия вирусов, используя антивирусные программы. Перед повторной проверкой необходимо перезагрузить ПЭВМ через выключение и последующее включение ПЭВМ. Если повторная проверка не выявила вирусов, то можно быть уверенным в отсутствии вирусов.

5.5. Если вирус поразил таблицу FAT, то можно восстановить эту таблицу, используя пакет программ Norton Utilites, который для восстановления использует вторую таблицу FAT, имеющуюся в ПЭВМ.

5.6. Для восстановления зараженной загрузочной записи винчестера необходимо использовать специальную системную дискету, на которой записана загрузочная запись.