3. Средства информационных и коммуникационных технологий

3.5 Защита информации

Среди набора программ, используемого большинством пользователей ПК каждый день, антивирусные программы традиционно занимают особое место. Современные антивирусные программы представляют собой многофункциональные продукты, сочетающие в себе как профилактические средства, так и средства лечения вирусов и восстановления данных.

Требования к антивирусным программам достаточно противоречивы. С одной стороны, пользователи хотят иметь надежную, мощную антивирусную защиту. С другой стороны, они хотят, чтобы эта защита не требовала от пользователя много времени и сил.

При этом нельзя отставать от общего развития компьютерного мира. Каждый год приносит новые технологии, в том числе и в мире компьютерных вирусов.

Так, в 1995 г. появился первый макровирус, заражающий документы MS Word.

В 1996 г. появились первые Win32-вирусы для Windows 95.

В 1997 г. вирусы впервые стали использовать для распространения сообщения электронной почты и появились первые вирусы, работающие в защищенном режиме процессоров Intel.

В 1998 г. был создан первый вирус, нарушающий работу аппаратной части компьютеров. Это был Win95.CIH, который «сработал» 26 апреля 1999 г. на миллионах компьютеров по всему миру. В России этот вирус стал известен под именем «Чернобыль».

В самом конце 1998 г. появился первый вирус для Windows NT.

В 1999 г. получили массовое распространение e-mail-черви (вирусные программы-черви), которые используют для распространения сообщения электронной почты.

Эпидемия вируса Win95.Spanska.10000 («Happy99») началась 1 января 1999 г. и продолжается до сих пор. Другой e-mail-червь Melissa в марте 1999 г. парализовал работу нескольких тысяч почтовых серверов в Европе и Америке. По масштабу мартовскую эпидемию червя Melissa можно сравнить с легендарным «червем Морриса», который в ноябре 1988 г. парализовал работу нескольких крупных компьютерных сетей в Америке.

Также в 1999 г. стали очень популярны троянские программы (троянские системы семейств BackOrifice, NetBus, TrojanStealth), дающие удаленный доступ к инфицированному компьютеру через Интернет и позволяющие воровать информацию, например пароли.

Все эти «новинки» заставляют постоянно совершенствовать антивирусные программы. Пользователю важно лишь не забывать об угрозе компьютерных вирусов и принимать для защиты от них меры, не требующие в принципе больших усилий или специальных знаний. Достаточно проводить регулярное резервное копирование важных данных и пользоваться современными антивирусными программами.

Способы противодействия компьютерным вирусам можно разделить на несколько групп:

- профилактика вирусного заражения и уменьшение предполагаемого ущерба от такого заражения;
- методика использования антивирусных программ, в том числе обезвреживание и удаление известного вируса;
- способы обнаружения и удаления неизвестного вируса.

Не существует антивирусов, гарантирующих 100%-ю защиту от вирусов. Таких систем не существует, поскольку на любой алгоритм антивируса всегда можно предложить контралгоритм вируса, невидимого для этого антивируса (обратное тоже верно: на любой алгоритм вируса всегда можно создать антивирус).

Следует также обратить внимание на несколько терминов, применяемых при обсуждении антивирусных программ:

- «ложное срабатывание» (false positive) – определение вируса в незараженном объекте (файле, секторе или системной памяти). Обратный термин – false negative;
- «сканирование по запросу» (on-demand) – поиск вирусов по запросу пользователя. В этом режиме антивирусная программа неактивна до тех пор, пока не будет вызвана пользователем из командной строки, командного файла или программы-расписания (system scheduler);

- «сканирование на лету» (real-time, on-the-fly) – постоянная проверка на вирусы объектов, к которым происходит обращение (запуск, открытие, создание и т. п.). В этом режиме антивирус постоянно активен, он присутствует в памяти постоянно (резидентно) и проверяет объекты без запроса пользователя.

Принципы диагностики компьютера на основе антивирусных программ приведены ниже.

1. Следите за тем, чтобы антивирусные программы, используемые для проверки, были самых последних версий. Если к программам поставляются обновления, то проверьте их на «свежесть».

2. «Национальность» антивирусов в большинстве случаев не имеет значения, поскольку на сегодняшний день процесс эмиграции вируса в другие страны и иммиграции антивирусных программ ограничивается только скоростью Интернета, поэтому как вирусы, так и антивирусы не признают границ. Если на компьютере обнаружен вирус, то самое главное – не паникуйте. Если вирус обнаружен в каком-то из новых файлов и еще не проник в систему, то нет причин для беспокойства: удалите вирус любимой антивирусной программой и спокойно работайте дальше.

3. В случае обнаружения файлового вируса, если компьютер подключен к сети, отключите его от локальной сети и проинформируйте системного администратора. Если вирус еще не проник в сеть, это защитит сервер и другие рабочие станции от проникновения вируса. Если же вирус уже поразил сервер, то отключение от сети не позволит ему вновь проникнуть на компьютер после его лечения. Подключение к сети возможно лишь после того, как будут вылечены все серверы и рабочие станции.

4. Если обнаружен файловый или загрузочный вирус, убедитесь в том, что вирус либо нерезидентный, либо резидентная часть вируса обезврежена: при запуске некоторые (но не все) антивирусы автоматически обезвреживают резидентные вирусы в памяти. Удаление вируса из памяти необходимо для того, чтобы остановить его распространение.

С помощью антивирусной программы можно восстановить зараженные файлы и затем проверить их работоспособность. Перед лечением или одновременно с ним – создать резервные копии зараженных файлов и распечатать или сохранить где-либо список зараженных файлов (log-файл антивируса). Это необходимо для того, чтобы восстановить файлы, если лечение окажется неуспешным из-за ошибки в лечащем модуле антивируса либо по причине неспособности антивируса лечить данный вирус. В этом случае придется прибегнуть к помощи какого-либо другого антивируса.

Одним из основных методов борьбы с вирусами является, как и в медицине, своевременная профилактика. Компьютерная профилактика предполагает соблюдение небольшого числа правил, которое позволяет значительно снизить вероятность заражения вирусом и потери каких-либо данных.

Для того чтобы определить основные правила компьютерной гигиены, необходимо выяснить основные пути проникновения вируса в компьютер и компьютерные сети.

Основным источником вирусов на сегодняшний день является глобальная сеть Интернет. Наибольшее число заражений вирусом происходит при обмене письмами в форматах Word. Пользователь зараженного макровирусом редактора Word, сам того не подозревая, рассылает зараженные письма адресатам, которые в свою очередь отправляют новые зараженные письма и т.д.

Электронные конференции также служат одним из основных источников распространения вирусов. Практически каждую неделю приходит сообщение о том, что какой-либо пользователь заразил свой компьютер вирусом, который был снят с какой-либо электронной конференции. При этом часто зараженные файлы «закладываются» автором вируса и рассылаются по нескольким конференциям одновременно, а эти файлы маскируются под новые версии какого-либо ПО (иногда под новые версии антивирусов).

Главный путь быстрого заражения – локальные сети. Если не принимать необходимых мер защиты, то зараженная рабочая станция при входе в сеть заражает один или несколько служебных файлов через компьютерную сеть.

Нелегальные копии ПО, как это было всегда, являются одной из основных зон риска. Часто пиратские копии на компакт-дисках содержат файлы, зараженные самыми разнообразными типами вирусов.

Файлы, с которыми ведется работа, необходимо периодически сохранять на внешнем носителе. Такие резервные копии носят название backup-копий. Затраты на копирование файлов, содержащих исходные тексты программ, БД, документацию, значительно меньше затрат на восстановление этих файлов при проявлении вирусом агрессивных свойств или сбое компьютера.