Костюкова Нина Ивановна

МЕТОДЫ ОБНАРУЖЕНИЯ ВИРУСОВ

Адрес статьи: www.gramota.net/materials/1/2011/7/12.html

Источник

Альманах современной науки и образования

Тамбов: Грамота, 2011. № 7 (50). С. 47-57. ISSN 1993-5552.

Адрес журнала: www.gramota.net/editions/1.html

Содержание данного номера журнала: www.gramota.net/materials/1/2011/7/

производная от $P_i(t)$ по t

$$\frac{dP_i}{dt} = \sum_{j=1}^{n} P_i(t) \quad (t) - P_i(t) \sum_{j=1}^{n} \quad _{ij}(t)$$

Таким образом, для вероятностей отказов $P_i(t)$ получим систему обыкновенных дифференциальных уравнений Колмогорова. Для исследования эксплуатационных факторов использован марковский случайный процесс. При этом необходимо иметь:

1) матрицу интенсивностей отказов $\| \ _i(t) \|$ или размеченный мультиграф постоянных показателей;

2) начальные условия $\sum_{i=1}^{n} P_i(0) = 0$.

Тогда все интенсивности отказов записывают в виде матрицы $\| \ _i(t) \|$. По главной диагонали этой матрицы стоят нули, а на пересечении *i*-й строки и *j*-го столбца стоит функция $\| \ _i(t) \|$ – интенсивность пуассоновского потока отказов. Чтобы марковский процесс был однородным, нужно все потоки событий, переводящие систему из одного состояния в другое, были стационарными пуассоновскими, представленными в виде матрицы

$$| \ (t)| = \left\| \begin{array}{cccc} 0 & _{12}(t) & .... & _{1n}(t) \\ _{21}(t) & 0 & ... & _{2n}(t) \\ . & . & ... & ... \\ _{n1}(t) & _{n2} & ... & 0 \end{array} \right\| \leq [\ (t)] \qquad (2)$$

где $[\ (t)]$ – допускаемое значение интенсивности отказов.

Матрицу интенсивностей (2) удобно иллюстрировать с помощью размеченного графа состояний. В задачах, связанных с определением устойчивости решения, следует:

1) задаться шагом итерации, настолько малым, чтобы был практически возможен только переход системы в соседнее состояние, а не в одно из других, и чтобы ни в одном из пуассоновских потоков, действующих на систему, практически не могло появиться более одного события;

2) подсчитать для каждой пары состояний (x_i, x_j), между которыми может иметь место переход $x_i \to x_j$, переходную вероятность;

3) составить матрицу $x_i \to x_j$ этих переходных вероятностей, далее пронумеровать шаги и найти все вероятности.

Связи элементов (показателей) обобщенной модели рассмотрены аналитически методом дискретного анализа. Модели потока отказов позволяют корректировать периодичность и трудоемкость проведения технического обслуживания, и расход запасных частей. По данному критерию оптимальность можно оценить эффективность использования и качества транспортных средств.

Список литературы

1. **Гусев А. С.** Вероятностные методы в механике машин и конструкций. М.: МГТУ им. Н. Э. Баумана, 2009. 223 с.
2. **Дьяков И. Ф., Денисов А. В**. Прикладное оптимальное проектирование в автомобилестроении. Ульяновск: УлГТУ, 2005. 278 с.
3. **Дьяков И. Ф., Садриев Р. М**. Прогнозирование ресурса деталей автотранспортных средств. Ульяновск: УлГТУ, 2008. 166 с.

УДК 519.6

Нина Ивановна Костюкова
Институт вычислительной математики и математической геофизики СО РАН

МЕТОДЫ ОБНАРУЖЕНИЯ ВИРУСОВ©

Определение

Компьютерный вирус - разновидность компьютерной программы, отличительной особенностью которой является способность к размножению (саморепликация). В дополнение к этому он может повреждать

или полностью уничтожать данные, подконтрольные пользователю, от имени которого была запущена заражённая программа.

Неспециалисты к компьютерным вирусам иногда причисляют и другие виды вредоносных программ, такие как трояны, программы-шпионы и даже спам. Вирусы распространялись, внедряя себя в исполняемый код других программ или же заменяя собой другие программы. Какое-то время даже считалось, что, являясь программой, вирус может заразить только программу - какое угодно изменение не-программы является не заражением, а просто повреждением данных. Подразумевалось, что такие копии вируса не получат управления, будучи информацией, не используемой процессором в качестве инструкций. Так, например неформатированный текст не мог бы быть переносчиком вируса.

Однако позднее хакеры показали, что вирусным поведением может обладать не только исполняемый код, содержащий машинный код процессора. Были написаны вирусы на языке пакетных файлов. Потом появились макровирусы, внедряющиеся через макросы в документы таких программ, как *Microsoft Word* и *Excel*. Некоторое время спустя появились вирусы, использующие уязвимости в популярном программном обеспечении (например, *Adobe Photoshop*, *Internet Explorer*, *Outlook*), в общем случае обрабатывающем обычные данные. Вирусы стали распространяться посредством внедрения в последовательности данных (например, картинки, тексты, и т.д.) специального кода, использующего уязвимости программного обеспечения.

Классические вирусы

Типы компьютерных вирусов различаются между собой по следующим основным признакам: среда обитания; способ заражения.

Под «средой обитания» понимаются системные области компьютера, операционные системы или приложения, в компоненты (файлы) которых внедряется код вируса. Под «способом заражения» понимаются различные методы внедрения вирусного кода в заражаемые объекты.

Среда обитания

По среде обитания вирусы можно разделить на: файловые; загрузочные; макро; скриптовые. Файловые вирусы при своем размножении тем или иным способом используют файловую систему какой-либо (или каких-либо) ОС. Они: различными способами внедряются в исполняемые файлы (наиболее распространенный тип вирусов); создают файлы-двойники (компаньон-вирусы); создают свои копии в различных каталогах; используют особенности организации файловой системы (*link*-вирусы). Загрузочные вирусы записывают себя либо в загрузочный сектор диска (*boot*-сектор), либо в сектор, содержащий системный загрузчик винчестера (*Master Boot Record*), либо меняют указатель на активный *boot*-сектор. Данный тип вирусов был достаточно распространён в 1990-х, но практически исчез с переходом на 32-битные операционные системы и отказом от использования дискет как основного способа обмена информацией. Теоретически возможно появление загрузочных вирусов, заражающих *CD*-диски и *USB*-флешки, но на текущий момент такие вирусы не обнаружены. Многие табличные и графические редакторы, системы проектирования, текстовые процессоры имеют свои макроязыки для автоматизации выполнения повторяющихся действий. Эти макроязыки часто имеют сложную структуру и развитый набор команд. Макровирусы являются программами на макроязыках, встроенных в такие системы обработки данных. Для своего размножения вирусы этого класса используют возможности макроязыков и при их помощи переносят себя из одного зараженного файла (документа или таблицы) в другие.

Способ заражения

Файловые вирусы по способу заражения файлов вирусы делятся на: перезаписывающие (overwriting); паразитические (parasitic); вирусы-компаньоны (companion); вирусы-ссылки (link); вирусы, заражающие объектные модули (OBJ); вирусы, заражающие библиотеки компиляторов (LIB); вирусы, заражающие исходные тексты программ.

Overwriting

Данный метод заражения является наиболее простым: вирус записывает свой код вместо кода заражаемого файла, уничтожая его содержимое. Естественно, что при этом файл перестает работать и не восстанавливается. Такие вирусы очень быстро обнаруживают себя, так как операционная система и приложения довольно быстро перестают работать.

Parasitic

К паразитическим относятся все файловые вирусы, которые при распространении своих копий обязательно изменяют содержимое файлов, оставляя сами файлы при этом полностью или частично работоспособными. Основными типами таких вирусов являются вирусы, записывающиеся в начало файлов (prepending), в конец файлов (appending) и в середину файлов (inserting). В свою очередь, внедрение вирусов в середину файлов происходит различными методами - путем переноса части файла в его конец или копирования своего кода в заведомо неиспользуемые данные файла (*cavity*-вирусы).

Внедрение вируса в начало файла

Известны два способа внедрения паразитического файлового вируса в начало файла. Первый способ заключается в том, что вирус переписывает начало заражаемого файла в его конец, а сам копируется в освободившееся место. При заражении файла вторым способом вирус дописывает заражаемый файл к своему телу.

Таким образом, при запуске зараженного файла первым управление получает код вируса. При этом вирусы, чтобы сохранить работоспособность программы, либо лечат зараженный файл, повторно запускают его, ждут окончания его работы и снова записываются в его начало (иногда для этого используется временный

файл, в который записывается обезвреженный файл), либо восстанавливают код программы в памяти компьютера и настраивают необходимые адреса в ее теле (т.е. дублируют работу ОС).

Внедрение вируса в конец файла

Наиболее распространенным способом внедрения вируса в файл является дописывание вируса в его конец. При этом вирус изменяет начало файла таким образом, что первыми выполняемыми командами программы, содержащейся в файле, являются команды вируса.

Для того чтобы получить управление при старте файла, вирус корректирует стартовый адрес программы (адрес точки входа). Для этого вирус производит необходимые изменения в заголовке файла.

Внедрение вируса в середину файла

Существует несколько методов внедрения вируса в середину файла. В наиболее простом из них вирус переносит часть файла в его конец или «раздвигает» файл и записывает свой код в освободившееся пространство. Этот способ во многом аналогичен методам, перечисленным выше. Некоторые вирусы при этом компрессируют переносимый блок файла так, что длина файла при заражении не изменяется.

Вторым является метод «cavity», при котором вирус записывается в заведомо неиспользуемые области файла. Вирус может быть скопирован в незадействованные области заголовок *EXE*-файла, в «дыры» между секциями *EXE*-файлов или в область текстовых сообщений популярных компиляторов. Существуют вирусы, заражающие только те файлы, которые содержат блоки, заполненные каким-либо постоянным байтом, при этом вирус записывает свой код вместо такого блока.

Кроме того, копирование вируса в середину файла может произойти в результате ошибки вируса, в этом случае файл может быть необратимо испорчен.

Вирусы без точки входа

Отдельно следует отметить довольно незначительную группу вирусов, не имеющих «точки входа» (*EPO*-вирусы - *Entry Point Obscuring viruses*). К ним относятся вирусы, не изменяющие адрес точки старта в заголовке *EXE*-файлов. Такие вирусы записывают команду перехода на свой код в какое-либо место в середину файла и получают управление не непосредственно при запуске зараженного файла, а при вызове процедуры, содержащей код передачи управления на тело вируса. Причем выполняться эта процедура может крайне редко (например, при выводе сообщения о какой-либо специфической ошибке). В результате вирус может долгие годы «спать» внутри файла и выскочить на свободу только при некоторых ограниченных условиях.

Перед тем, как записать в середину файла команду перехода на свой код, вирусу необходимо выбрать «правильный» адрес в файле - иначе зараженный файл может оказаться испорченным. Известны несколько способов, с помощью которых вирусы определяют такие адреса внутри файлов, например, поиск в файле последовательности стандартного кода заголовков процедур языков программирования (C/Pascal), дизассемблирование кода файла или замена адресов импортируемых функций.

Companion

К категории «companion» относятся вирусы, не изменяющие заражаемых файлов. Алгоритм работы этих вирусов состоит в том, что для заражаемого файла создается файл-двойник, причем при запуске зараженного файла управление получает именно этот двойник, т.е. вирус.

К вирусам данного типа относятся те из них, которые при заражении переименовывают файл в какое-либо другое имя, запоминают его (для последующего запуска файла-хозяина) и записывают свой код на диск под именем заражаемого файла. Например, файл *NOTEPAD.EXE* переименовывается в *NOTEPAD.EXD*, а вирус записывается под именем *NOTEPAD.EXE*. При запуске управление получает код вируса, который затем запускает оригинальный *NOTEPAD*. Возможно существование и других типов вирусов-компаньонов, использующих иные оригинальные идеи или особенности других операционных систем. Например, *PATH*-компаньоны, которые размещают свои копии в основном каталоге *Windows*, используя тот факт, что этот каталог является первым в списке *PATH*, и файлы для запуска *Windows* в первую очередь будет искать именно в нем. Данными способом самозапуска пользуются также многие компьютерные черви и троянские программы.

Прочие способы заражения

Существуют вирусы, которые никоим образом не связывают свое присутствие с каким-либо выполняемым файлом. При размножении они всего лишь копируют свой код в какие-либо каталоги дисков в надежде, что эти новые копии будут когда-либо запущены пользователем. Иногда эти вирусы дают своим копиям «специальные» имена, чтобы подтолкнуть пользователя на запуск своей копии - например, *INSTALL.EXE* или *WINSTART.BAT*.

Некоторые вирусы записывают свои копии в архивы (ARJ, ZIP, RAR). Другие записывают команду запуска зараженного файла в *BAT*-файлы.

Link-вирусы также не изменяют физического содержимого файлов, однако при запуске зараженного файла «заставляют» ОС выполнить свой код. Этой цели они достигают модификацией необходимых полей файловой системы.

Загрузочные вирусы

Известные на текущий момент загрузочные вирусы заражают загрузочный (boot) сектор гибкого диска и *boot*-сектор или *Master Boot Record* (MBR) винчестера. Принцип действия загрузочных вирусов основан на алгоритмах запуска операционной системы при включении или перезагрузке компьютера - после необходимых тестов установленного оборудования (памяти, дисков и т.д.) программа системной загрузки считывает

первый физический сектор загрузочного диска (A:, C: или *CD-ROM* в зависимости от параметров, установленных в *BIOS Setup*) и передает на него управление.

При заражении дисков загрузочные вирусы «подставляют» свой код вместо какой-либо программы, получающей управление при загрузке системы. Принцип заражения, таким образом, одинаков во всех описанных выше способах: вирус «заставляет» систему при ее перезапуске считать в память и отдать управление не оригинальному коду загрузчика, но коду вируса.

Заражение дискет производится единственным известным способом - вирус записывает свой код вместо оригинального кода *boot*-сектора дискеты. Винчестер заражается тремя возможными способами - вирус записывается либо вместо кода *MBR*, либо вместо кода *boot*-сектора загрузочного диска (обычно диска C:), либо модифицирует адрес активного *boot*-сектора в таблице разделов диска (*Disk Partition Table*), расположенной в *MBR* винчестера.

При инфицировании диска вирус в большинстве случаев переносит оригинальный *boot*-сектор (или *MBR*) в какой-либо другой сектор диска (например, в первый свободный). Если длина вируса больше длины сектора, то в заражаемый сектор помещается первая часть вируса, остальные части размещаются в других секторах (например, в первых свободных).

Макровирусы

Наибольшее распространение получили макровирусы для *Microsoft Office* (*Word*, *Excel* и *PowerPoint*), хранящих информацию в формате *OLE2* (*Object Linking and Embedding*). Вирусы в прочих приложениях достаточно редки.

Физическое расположение вируса внутри файла *MS Office* зависит от его формата, который в случае продуктов *Microsoft* чрезвычайно сложен - каждый файл-документ *Word*, *Office* или таблица *Excel* представляют собой последовательность блоков данных (каждый из которых также имеет свой формат), объединенных между собой при помощи большого количества служебных данных.

При работе с документами и таблицами *MS Office* выполняет различные действия: открывает документ, сохраняет, печатает, закрывает и т.д. При этом *MS Word*, например, ищет и выполняет соответствующие «встроенные макросы» - при сохранении файла по команде *File/Save* вызывается макрос *FileSave*, при сохранении по команде *File/SaveAs* - *FileSaveAs*, при печати документов - *FilePrint* и т.д., если, конечно, таковые макросы определены.

Существует также несколько «автомакросов», автоматически вызываемых при различных условиях. Например, при открытии документа *MS Word* проверяет его на наличие макроса *AutoOpen*. Если такой макрос присутствует, то *Word* выполняет его. При закрытии документа *Word* выполняет макрос *AutoClose*, при запуске *Word* вызывается макрос *AutoExec*, при завершении работы - *AutoExit*, при создании нового документа - *AutoNew*. Автоматически (т.е. без участия пользователя) выполняются также макросы/функции, ассоциированные с какой-либо клавишей либо моментом времени или датой, т.е. *MS Word/Excel* вызывают макрос/функцию при нажатии на какую-либо конкретную клавишу (или комбинацию клавиш) либо при достижении какого-либо момента времени.

Макровирусы, поражающие файлы *MS Office*, как правило, пользуются одним из перечисленных выше приемов - в вирусе либо присутствует авто-макрос (авто-функция), либо переопределен один из стандартных системных макросов (ассоциированный с каким-либо пунктом меню), либо макрос вируса вызывается автоматически при нажатии на какую-либо клавишу или комбинацию клавиш. Получив управление, макровирус переносит свой код в другие файлы, обычно в файлы, которые редактируются в данный момент. Реже макровирусы самостоятельно ищут другие файлы на диске.

Скрипт-вирусы

Следует отметить также скрипт-вирусы, являющиеся подгруппой файловых вирусов. Данные вирусы, написаны на различных скрипт-языках (VBS, JS, BAT, PHP и т.д.). Они либо заражают другие скрипт-программы (командные и служебные файлы *MS Windows* или *Linux*), либо являются частями многокомпонентных вирусов. Также, данные вирусы могут заражать файлы других форматов (например, *HTML*), если в них возможно выполнение скриптов.

Троянские программы

Троянские программы различаются между собой по тем действиям, которые они производят на зараженном компьютере.

Backdoor - троянские утилиты удаленного администрирования

Троянские программы этого класса являются утилитами удаленного администрирования компьютеров в сети. По своей функциональности они во многом напоминают различные системы администрирования, разрабатываемые и распространяемые фирмами-производителями программных продуктов.

Единственная особенность этих программ заставляет классифицировать их как вредные троянские программы: отсутствие предупреждения об инсталляции и запуске. При запуске «троянец» устанавливает себя в системе и затем следит за ней, при этом пользователю не выдается никаких сообщений о действиях троянца в системе. Более того, ссылка на «троянца» может отсутствовать в списке активных приложений. В результате «пользователь» этой троянской программы может и не знать о ее присутствии в системе, в то время как его компьютер открыт для удаленного управления.

Утилиты скрытого управления позволяют делать с компьютером все, что в них заложил автор: принимать или отсылать файлы, запускать и уничтожать их, выводить сообщения, стирать информацию,

перезагружать компьютер и т.д. В результате эти троянцы могут быть использованы для обнаружения и передачи конфиденциальной информации, для запуска вирусов, уничтожения данных и т.п. - пораженные компьютеры оказываются открытыми для злоумышленных действий хакеров.

Таким образом, троянские программы данного типа являются одним из самых опасных видов вредоносного программного обеспечения, поскольку в них заложена возможность самых разнообразных злоумышленных действий, присущих другим видам троянских программ.

Отдельно следует отметить группу бэкдоров, способных распространяться по сети и внедряться в другие компьютеры, как это делают компьютерные черви. Отличает такие «троянцы» от червей тот факт, что они распространяются по сети не самопроизвольно (как черви), а только по специальной команде «хозяина», управляющего данной копией троянской программы.

Trojan-PSW - воровство паролей

Данное семейство объединяет троянские программы, «ворующие» различную информацию с зараженного компьютера, обычно - системные пароли (PSW - Password-Stealing-Ware). При запуске *PSW*-троянцы ищут системные файлы, хранящие различную конфиденциальную информацию (обычно номера телефонов и пароли доступа к интернету) и отсылают ее по указанному в коде «троянца» электронному адресу или адресам.

Существуют *PSW*-троянцы, которые сообщают и другую информацию о зараженном компьютере, например, информацию о системе (размер памяти и дискового пространства, версия операционной системы), тип используемого почтового клиента, *IP*-адрес и т.п. Некоторые троянцы данного типа «воруют» регистрационную информацию к различному программному обеспечению, коды доступа к сетевым играм и прочее.

Trojan-AOL - семейство троянских программ, «ворующих» коды доступа к сети AOL (America Online) (выделены в особую группу по причине своей многочисленности)

Trojan-Clicker - интернет-кликеры

Семейство троянских программ, основная функция которых - организация несанкционированных обращений к Интернет-ресурсам (обычно к веб-страницам). Достигается это либо посылкой соответствующих команд браузеру, либо заменой системных файлов, в которых указаны «стандартные» адреса Интернет-ресурсов (например, файл *hosts* в *MS Windows*).

У злоумышленника могут быть следующие цели для подобных действий:

- увеличение посещаемости каких-либо сайтов с целью увеличения показов рекламы;
- организация *DoS*-атаки (*Denial of Service*) на какой-либо сервер;
- привлечение потенциальных жертв для заражения вирусами или троянскими программами.

Trojan-Downloader - доставка прочих вредоносных программ

Троянские программы этого класса предназначены для загрузки и установки на компьютер-жертву новых версий вредоносных программ, установки «троянцев» или рекламных систем. Загруженные из интернета программы затем либо запускаются на выполнение, либо регистрируются «троянцем» на автозагрузку в соответствии с возможностями операционной системы. Данные действия при этом происходят без ведома пользователя.

Информация об именах и расположении загружаемых программ содержится в коде и данных троянца или скачивается троянцем с «управляющего» Интернет-ресурса (обычно с веб-страницы).

Trojan-Dropper - инсталляторы прочих вредоносных программ

Троянские программы этого класса написаны в целях скрытной инсталляции других программ и практически всегда используются для «подсовывания» на компьютер-жертву вирусов или других троянских программ.

Данные троянцы обычно без каких-либо сообщений (либо с ложными сообщениями об ошибке в архиве или неверной версии операционной системы) сбрасывают на диск в какой-либо каталог (в корень диска C:, во временный каталог, в каталоги *Windows*) другие файлы и запускают их на выполнение.

Обычно структура таких программ следующая:

Основной код

Файл 1

Файл 2

...

«Основной код» выделяет из своего файла остальные компоненты (файл 1, файл 2, ...), записывает их на диск и открывает их (запускает на выполнение).

Обычно один (или более) компонентов являются троянскими программами, и как минимум один компонент является «обманкой»: программой-шуткой, игрой, картинкой или чем-то подобным. «Обманка» должна отвлечь внимание пользователя и/или продемонстрировать то, что запускаемый файл действительно делает что-то «полезное», в то время как троянская компонента инсталлируется в систему.

В результате использования программ данного класса хакеры достигают двух целей:

- скрытная инсталляция троянских программ и/или вирусов;
- защита от антивирусных программ, поскольку не все из них в состоянии проверить все компоненты внутри файлов этого типа.

Trojan-Proxy - троянские прокси-сервера

Семейство троянских программ, скрытно осуществляющих анонимный доступ к различным Интернет-ресурсам. Обычно используются для рассылки спама.

Trojan-Spy - шпионские программы

Данные троянцы осуществляют электронный шпионаж за пользователем зараженного компьютера: вводимая с клавиатуры информация, снимки экрана, список активных приложений и действия пользователя с ними сохраняются в какой-либо файл на диске и периодически отправляются злоумышленнику.

Троянские программы этого типа часто используются для кражи информации пользователей различных систем онлайновых платежей и банковских систем.

Trojan - прочие троянские программы

К данным троянцам относятся те из них, которые осуществляют прочие действия, попадающие под определение троянских программ, т.е. разрушение или злонамеренная модификация данных, нарушение работоспособности компьютера и прочее.

В данной категории также присутствуют «многоцелевые» троянские программы, например, те из них, которые одновременно шпионят за пользователем и предоставляют rгоху-сервис удаленному злоумышленнику.

Rootkit - сокрытие присутствия в операционной системе

Понятие *rootkit* пришло к нам из *UNIX*. Первоначально это понятие использовалось для обозначения набора инструментов, применяемых для получения прав *root*.

Так как инструменты типа *rootkit* на сегодняшний день «прижились» и на других ОС (в том числе, на *Windows*), то следует признать подобное определение *rootkit* морально устаревшим и не отвечающим реальному положению дел.

Таким образом, *rootkit* - программный код или техника, направленная на сокрытие присутствия в системе заданных объектов (процессов, файлов, ключей реестра и т.д.).

Для поведения *Rootkit* в классификации «Лаборатории Касперского» действуют правила поглощения: *Rootkit* - самое младшее поведение среди вредоносных программ. То есть, если *Rootkit*-программа имеет троянскую составляющую, то она детектируется как *Trojan*.

ArcBomb - «бомбы» в архивах

Представляют собой архивы, специально оформленные таким образом, чтобы вызывать нештатное поведение архиваторов при попытке разархивировать данные - зависание или существенное замедление работы компьютера или заполнение диска большим количеством «пустых» данных. Особенно опасны «архивные бомбы» для файловых и почтовых серверов, если на сервере используется какая-либо система автоматической обработки входящей информации - «архивная бомба» может просто остановить работу сервера.

Встречаются три типа подобных «бомб»: некорректный заголовок архива, повторяющиеся данные и одинаковые файлы в архиве.

Некорректный заголовок архива или испорченные данные в архиве могут привести к сбою в работе конкретного архиватора или алгоритма разархивирования при разборе содержимого архива.

Значительных размеров файл, содержащий повторяющиеся данные, позволяет заархивировать такой файл в архив небольшого размера (например, 5 ГБ данных упаковываются в 200 КБ *RAR* или в 480 КБ *ZIP*-архив).

Огромное количество одинаковых файлов в архиве также практически не сказывается на размере архива при использовании специальных методов (например, существуют приемы упаковки 10100 одинаковых файлов в 30 КБ *RAR* или 230 КБ *ZIP*-архив).

Trojan-Notifier - оповещение об успешной атаке

Троянцы данного типа предназначены для сообщения своему «хозяину» о зараженном компьютере. При этом на адрес «хозяина» отправляется информация о компьютере, например, *IP*-адрес компьютера, номер открытого порта, адрес электронной почты и т.п. Отсылка осуществляется различными способами: электронным письмом, специально оформленным обращением к веб-странице «хозяина», *ICQ*-сообщением.

Данные троянские программы используются в многокомпонентных троянских наборах для извещения своего «хозяина» об успешной инсталляции троянских компонент в атакуемую систему.

Spyware

Spyware - программа, которая скрытным образом устанавливается на компьютер с целью полного или частичного контроля над взаимодействием между пользователем и компьютером без согласия пользователя.

В то время как термин *Spyware* предполагает программу, тайным образом отслеживающую поведение пользователя, функции *Spyware* простираются далеко за пределы простого отслеживания.

Spyware могут заниматься сбором различных типов личной информации, таких, как:

- привычка пользования Интернетом и посещаемые сайты (Tracking Software);
- используются для контроля нажатий клавиш на клавиатуре компьютера (Keyloggers);
- для контроля скриншотов экрана монитора компьютера (Screen Scraper);
- для несанкционированного удалённого контроля и управления компьютерами (Remote Control Software) - *Backdoors*, *Botnets*, *Droneware*;
- для несанкционированного анализа состояния систем безопасности (Security Analysis Software) - *Hacker Tools*, *Port and vulnerability scanners*, *Password crackers*;
- могут также вмешиваться в контроль пользователя над компьютером с других сторон, например:
- инсталлируя дополнительные программы;
- перенаправляя активность браузеров, что влечёт за собой посещение веб-сайтов вслепую с риском заражения вирусами.

Spyware могут даже менять установки в компьютере для несанкционированного внесения изменений в компьютерную систему (System Modifying Software) - например, *Hijackers*, *Rootkits*, результатом чего являются снижение скорости соединения с Интернетом или потеря соединения как такового, открывание других домашних страниц или удаление тех или иных программ.

История и развитие

Согласно данным *AOL* и *National Cyber-Security Alliance* от 2005 года 61% респондентных компьютеров содержали ту или иную форму *Spyware*, из них 92% пользователей не знали о присутствии *Spyware* на их машинах и 91% сообщили, что они не давали разрешения на инсталляцию *Spyware*.

К 2006 году *Spyware* стали одним из превалирующих угроз безопасности компьютерных систем, использующих *Windows*. Компьютеры, в которых *Internet Explorer* служит основным браузером, являются частично уязвимыми не потому, что *Internet Explorer* наиболее широко используется, но из-за того, что его тесная интеграция с *Windows* позволяет *Spyware* получать доступ к ключевым узлам ОС.

До релиза *Internet Explorer 7* браузер автоматически выдавал окно инсталляции для любого компонента *ActiveX*, который веб-сайт хотел установить. Сочетание наивной неосведомлённости пользователя по отношению к *Spyware* и предположение *Internet Explorer*, что все компоненты *ActiveX* безвредны, внесло свой вклад в массовое распространение *Spyware*. Многие компоненты *Spyware* также используют изъяны в *JavaScript*, *Internet Explorer* и *Windows* для инсталляции без ведома и/или разрешения пользователя.

Реестр *Windows* содержит множество разделов, которые после модифицирования значений ключей позволяют программе исполняться автоматически при загрузке ОС. *Spyware* могут использовать такой шаблон для обхождения попыток деинсталляции и удаления.

Spyware обычно присоединяют себя из каждого местонахождения в реестре, позволяющего исполнение. Будучи запущенным, *Spyware* контролирует периодически, не удалено ли одно из этих звеньев. Если да, то оно автоматически восстанавливается. Это гарантирует, что *Spyware* будет выполняться во время загрузки ОС, даже если некоторые (или большинство) звенья в реестре автозапуска удалены.

Spyware, Adware и программы отслеживания

Термин *Adware* часто относится к любой программе, демонстрирующей рекламу с или без согласия пользователя. Некоторые, как, например, *Eudore*, отправляют клиенту рекламу как альтернативу оплаты регистрационных счетов. Такие программы классифицируются как *Adware* в смысле программы с рекламной поддержкой, но не как *Spyware*. *Adware* не действуют скрытно или вводят пользователя в заблуждение, лишь предлагают пользователю дополнительные услуги.

Многие *Adware* являются *Spyware* по другим причинам: они показывают рекламные заставки, базирующиеся на результатах шпионской деятельности на вашем компьютере. Примеры: *Gator Software* от *Claria Corporation* и *Exact Advertising* от *BargainBuddy*. Посещаемые веб-сайты могут устанавливать *Gator* на машинах клиентов тайным способом, таким образом перенаправляя доход с демонстрации множества всплывающих окон на инсталлирующий сайт и на *Claria Corporation*.

Другие модели поведения *Spyware*, такие как доклад о веб-сайтах, посещаемых пользователем, происходят в фоновом режиме. Данные используются для целевого рекламного эффекта.

Широкое распространение *Spyware* бросает тень подозрения на другие программы, отслеживающие посещения страниц веб-сайтов с целью исследований и статистики. Некоторые обозреватели описывают *Alexa Toolbar*, плагин *IE*, как *Spyware* и некоторые анти-*spyware* программы, такие как *Ad-Aware*, подтверждают это.

Spyware и *Adware* сходны с вирусами в том, что они злонамеренны по своей природе.

Аналогичным образом, программы, поставляемые в комплекте с бесплатными программами с рекламной поддержкой, являются *Spyware* (при деинсталляции удаляется только материнская программа), тем не менее, пользователи добровольно их скачивают. Это представляет дилемму для создателей анти-*spyware*, чьи инструменты удаления могут безвозвратно привести в неработоспособность желаемые программы. Например, недавние результаты теста показали, что комплектная программа *WhenUSave* игнорируется *Ad-Aware* (но удаляется как *Spyware* большинством сканеров), потому что она является частью популярного *eDonkey Client*. Для решения этой проблемы *Anti-Spyware Coalition* работает над постройкой единого мнения внутри индустрии анти-*spyware* касательно того, что является приемлемым поведением программы.

Поведение и результат

Spyware редко бывает одинока на компьютере: поражённая машина может в течение короткого времени быть инфицированной многими другими компонентами. Пользователи часто замечают нежелательное поведение и снижение системных показателей. Поражение *Spyware* может создавать значительно возросшую нежелательную активность процессора, использование объёма диска и каналов сетевого трафика, что в суммарном результате ведёт к значительному снижению скорости работы компьютера. Проявления нестабильности, такие как сбои в работе приложений или всей системы также нередки. *Spyware*, вмешиваясь в работу программ, использующих сеть, обычно также вызывают трудности при подсоединении к Интернет.

При некоторых видах заражения наличие *Spyware* может не быть очевидным. Пользователи полагают в таких случаях, что причиной является сбой в работе аппаратного обеспечения, проблемы в инсталляции *Windows* или вирус. Некоторые обладатели тяжело инфицированных систем обращаются к экспертам технической поддержки или даже приобретают новый компьютер, поскольку существующая система «стала слишком медленной». Тяжело инфицированным системам может потребоваться полная переустановка всех компонентов программ для возврата к первоначальной функциональности.

Лишь в редких случаях одна часть *Spyware* приводит компьютер в состояние непригодности. Скорее, он обладает многочисленными инфекциями. Как сообщала *AOL* в 2004 году, «если компьютер содержит хотя бы одну *Spyware*, он, как правило, также содержит десятки других». Кумулятивный эффект и взаимодействие между компонентами *Spyware* влекут за собой симптомы, обычно отмечаемые пользователем: компьютер со скоростью, пониженной до черепашьей, переполненный множеством исполняющихся паразитических процессов. Более того, некоторые типы *Spyware* отключают файрволы и антивирусные программы и/или понижают установки безопасности браузера, таким образом делая систему неприкрытой для дальнейших приспосабливающихся инфекций, что похоже на иммунную недостаточность. Некоторые *Spyware* отключают или даже удаляют другие конкурирующие *Spyware* под предлогом того, что возросшее недовольство пользователя работой системы может привести его к решению принять меры по удалению *Spyware*. Один из создателей *Spyware*, *Avenue Media*, по этому поводу даже подала в суд на конкурента, *Direct Revenue*. Позже эти двое пришли к соглашению не отключать продукты другой стороны.

Некоторые другие типы *Spyware*, например, *Targetsoft*, модифицируют системные файлы, так что они становятся боле трудноудалимыми. *Targetsoft* модифицирует *winsock.dll*. Удаление инфицированного *Spyware* файла *inetadpt.dll* прекратит нормальное использование сети.

В отличие от пользователей других ОС, типичный пользователь *Windows* обладает привилегиями Администратора, по большей части для удобства. Из-за этого любая программа, запускаемая под именем пользователя-Администратора (намеренно или нет) имеет неограниченный доступ к системным файлам. *Spyware* наряду с другими видами угроз привело некоторых пользователей *Windows* к решению перейти на другие платформы, такие как *Linux* или *Apple Macintosh*, которые значительно менее восприимчивы к вредоносным программам. Это потому, что они не предполагают неограниченный доступ к системным файлам по умолчанию. Пользователи *Windows* также имеют возможность следовать принципу наименьших привилегий и использовать неадминистраторский профиль доступа. Или же снижать уровень привилегий таких специфически уязвимых Интернет-связанных процессов, как *Internet Explorer*, посредством таких инструментов как *DropMyRights*. Однако, поскольку эта конфигурация не выбирается по умолчанию, лишь некоторые пользователи делают это.

Многие *Spyware* показывают рекламу. Некоторые просто регулярно выдают всплывающие окна (например, каждые несколько минут или каждый раз, когда пользователь открывает новое окно браузера). Другие показывают рекламу, связанную с конкретными сайтами, посещаемыми пользователем. Операторы *Spyware* представляют это свойство как желательное для рекламодателей, которые могут купить место размещения во всплывающем окне. Это также одна из причин, почему *Spyware* собирают информацию о привычках и поведении пользователя. В некоторых случаях может иметь место подмены баннеров, размещённых на вебсайте (и оплаченных рекламодателем). *Spyware*, работающее как прокси-сервер или *Browser Helper Object*, может заменять ссылки сайта на ссылки, приносящие доход оператору *Spyware*.

Антивирусные программы

Антивирусная программа (антивирус) - *изначально программа для обнаружения и лечения других программ, заражённых компьютерными вирусами, а также для профилактики - предотвращения заражения файла вирусом (например, с помощью вакцинации).*

Многие современные антивирусы позволяют обнаруживать и удалять также троянские программы и прочие вредоносные программы. И напротив - программы, создававшиеся как файрволы, также получают функции, роднящие их с антивирусами.

Первые наиболее простые антивирусные программы появились почти сразу после появления вирусов. Сейчас разработкой антивирусов занимаются крупные компании. Как и у создателей вирусов, в этой сфере также сформировались оригинальные приёмы - но уже для поиска и борьбы с вирусами. Современные антивирусные программы могут обнаруживать десятки тысяч вирусов.

Антивирусное программное обеспечение состоит из компьютерных программ, которые пытаются обнаружить, предотвратить размножение и удалить компьютерные вирусы и другие вредоносные программы.

Методы обнаружения вирусов

Антивирусное программное обеспечение обычно использует два отличных друг от друга метода для выполнения своих задач:

- сканирование файлов для поиска известных вирусов, соответствующих определению в антивирусных базах;
- обнаружение подозрительного поведения любой из программ, похожего на поведение заражённой программы.

Метод соответствия определению вирусов в словаре

Это метод, когда антивирусная программа, просматривая файл, обращается к антивирусным базам, которые составлены производителем программы-антивируса. В случае соответствия какого-либо участка кода просматриваемой программы известному коду (сигнатуре) вируса в базах, программа-антивирус может по запросу выполнить одно из следующих действий:

- Удалить инфицированный файл.
- Заблокировать доступ к инфицированному файлу.
- Отправить файл в карантин (то есть сделать его недоступным для выполнения с целью недопущения дальнейшего распространения вируса).
- Попытаться «вылечить» файл, удалив вирус из тела файла.

- В случае невозможности лечения/удаления, выполнить эту процедуру при следующей перезагрузке операционной системы.

Для того чтобы такая антивирусная программа успешно работала на протяжении долгого времени, в базу сигнатур вирусов нужно периодически загружать (обычно, через Интернет) данные о новых вирусах. Если бдительные и имеющие склонность к технике пользователи определят вирус по горячим следам, они могут послать зараженные файлы разработчикам антивирусной программы, а те затем добавляют информацию о новых вирусах в свои базы.

Для многих антивирусных программ с базой сигнатур характерна проверка файлов в тот момент, когда операционная система создаёт, открывает, закрывает или посылает файлы по почте. Таким образом, программа может обнаружить известный вирус сразу после его получения. При этом системный администратор может установить в антивирусной программе расписание для регулярной проверки (сканирования) всех файлов на жёстком диске компьютера.

Хотя антивирусные программы, созданные на основе поиска сигнатур, при обычных обстоятельствах могут достаточно эффективно препятствовать вспышкам заражения компьютеров, авторы вирусов стараются держаться впереди таких программ-антивирусов, создавая «олигоморфические», «полиморфические» и, самые новые, «метаморфические» вирусы, в которых некоторые части шифруются или искажаются так, чтобы было невозможно обнаружить совпадение с определением в словаре вирусов.

Метод обнаружения странного поведения программ

Антивирусы, использующие метод обнаружения подозрительного поведения программ не пытаются идентифицировать известные вирусы, вместо этого они прослеживают поведение всех программ. Если программа пытается записать какие-то данные в исполняемый файл (.EXE-файл), программа-антивирус может пометить этот файл, предупредить пользователя и спросить что следует сделать.

В настоящее время подобные превентивные методы обнаружения вредоносного кода, в том или ином виде, широко применяются в качестве модуля антивирусной программы, а не отдельного продукта.

Другие названия: проактивная защита, поведенческий блокиратор, *Host Intrusion Prevention System* (HIPS).

В отличие от метода поиска соответствия определению вируса в антивирусных базах, метод обнаружения подозрительного поведения даёт защиту от новых вирусов, которых ещё нет в антивирусных базах. Однако следует учитывать, что программы или модули, построенные на этом методе, выдают также большое количество предупреждений (в некоторых режимах работы), что делает пользователя мало восприимчивым ко всем предупреждениям. В последнее время эта проблема ещё более ухудшилась, так как стало появляться всё больше не вредоносных программ, модифицирующих другие *exe*-файлы, несмотря на существующую проблему ошибочных предупреждений. Несмотря на наличие большого количества предупреждающих диалогов, в современном антивирусном программном обеспечении этот метод используется всё больше и больше. Так, в 2006 году вышло несколько продуктов, впервые реализовавших этот метод: *Kaspersky Internet Security*, *Kaspersky Antivirus*, *Safe-n-Sec*, *F-Secure Internet Security*, *Outpost Firewall Pro*, *DefenceWall*. Многие программы-файрволы издавна имели в своем составе модуль обнаружения странного поведения программ.

Метод обнаружения при помощи эмуляции

Некоторые программы-антивирусы пытаются имитировать начало выполнения кода каждой новой вызываемой на исполнение программы перед тем как передать ей управление. Если программа использует самоизменяющийся код или проявляет себя как вирус (то есть, например, немедленно начинает искать другие .EXE-файлы), такая программа будет считаться вредоносной, способной заразить другие файлы. Однако этот метод тоже изобилует большим количеством ошибочных предупреждений.

Метод «Белого списка»

Общая технология по борьбе с вредоносными программами - это «белый список». Вместо того, чтобы искать только известные вредоносные программы, это технология предотвращает выполнение всех компьютерных кодов за исключением тех, которые были ранее обозначены системным администратором как безопасные. Выбрав этот параметр отказа по умолчанию, можно избежать ограничений, характерных для обновления сигнатур вирусов. К тому же, те приложения на компьютере, которые системный администратор не хочет устанавливать, не выполняются, так как их нет в «белом списке». Так как у современных предприятий есть множество надежных приложений, ответственность за ограничения в использовании этой технологии возлагается на системных администраторов и соответствующим образом составленные ими «белые списки» надежных приложений. Работа антивирусных программ с такой технологией включает инструменты для автоматизации перечня и эксплуатации действий с «белым списком».

Эвристическое сканирование

Эвристическое сканирование - метод работы антивирусной программы, основанный на сигнатурах и эвристике, призван улучшить способность сканеров применять сигнатуры и распознавать модифицированные версии вирусов в тех случаях, когда сигнатура совпадает с телом неизвестной программы не на 100%, но в подозрительной программе налицо более общие признаки вируса. Данная технология, однако, применяется в современных программах очень осторожно, так как может повысить количество ложных срабатываний.

Практически все современные антивирусные средства применяют технологию эвристического анализа программного кода. Эвристический анализ нередко используется совместно с сигнатурным сканированием для поиска сложных шифрующихся и полиморфных вирусов. Методика эвристического анализа позволяет обнаруживать ранее неизвестные инфекции, однако, лечение в таких случаях практически всегда оказывается

невозможным. В таком случае, как правило, требуется дополнительное обновление антивирусных баз для получения последних сигнатур и алгоритмов лечения, которые, возможно, содержат информацию о ранее неизвестном вирусе. В противном случае, файл передается для исследования антивирусным аналитикам или авторам антивирусных программ.

Методы эвристического сканирования не обеспечивают какой-либо гарантированной защиты от новых, отсутствующих в сигнатурном наборе, компьютерных вирусов, что обусловлено использованием в качестве объекта анализа сигнатур ранее известных вирусов, а в качестве правил эвристической верификации - знаний о механизме полиморфизма сигнатур. В тоже время, этот метод поиска базируется на эмпирических предположениях, полностью исключить ложные срабатывания нельзя.

В ряде случаев, эвристические методы оказываются чрезвычайно успешными, к примеру, в случае очень коротких программных частей в загрузочном секторе: если, программа производит запись в сектор 1, дорожку 0, сторону 0, то это приводит к изменению раздела накопителя. Но кроме вспомогательной программы *FDISK* эта команда больше нигде не используется, и потому в случае ее неожиданного появления речь идет о загрузочном вирусе.

В процессе эвристического анализа производится проверка эмулируемой программы анализатором кода. К примеру, программа инфицирована полиморфным вирусом, состоящим из зашифрованного тела и расшифровщика. Эмулятор кода эмулирует работу данного вируса по одной инструкции, после этого анализатор кода подсчитывает контрольную сумму и сверяет ее с той, которая хранится в базе. Эмуляция будет продолжаться до тех пор, пока необходимая для подсчета контрольной суммы часть вируса не будет расшифрована. Если сигнатура совпала - программа идентифицирована.

Другим распространенным методом эвристического анализа, применяемым большой группой антивирусов, является декомпиляция подозрительной программы и анализ ее исходного кода. Исходный код подозрительного файла проходит сверку и сравнение с исходным кодом известных вирусов и образчиков вирусной активности. В случае, если определенный процент исходного кода идентичен коду известного вируса или вирусной активности, файл отмечается как подозрительный, о чем оповещается пользователь.

Firewall

Межсетевой экран или сетевой экран - комплекс аппаратных или программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов на различных уровнях модели *OSI* в соответствии с заданными правилами.

Основной задачей сетевого экрана является защита компьютерных сетей или отдельных узлов от несанкционированного доступа. Также сетевые экраны часто называют фильтрами, так как их основная задача - не пропускать (фильтровать) пакеты, не подходящие под критерии, определённые в конфигурации.

Некоторые сетевые экраны также позволяют осуществлять трансляцию адресов - динамическую замену адресов назначения редиректы или источника мапинг, biNAT, NAT.

Разновидности сетевых экранов

Сетевые экраны подразделяются на различные типы в зависимости от следующих характеристик:

- обеспечивает ли экран соединение между одним узлом и сетью или между двумя или более различными сетями;
- происходит ли контроль потока данных на сетевом уровне или более высоких уровнях модели *OSI*;
- отслеживаются ли состояния активных соединений или нет.

В зависимости от охвата контролируемых потоков данных сетевые экраны делятся на:

- традиционный сетевой (или межсетевой) экран - программа (или неотъемлемая часть операционной системы) на шлюзе (сервере передающем трафик между сетями) или аппаратное решение, контролирующие входящие и исходящие потоки данных между подключенными сетями;
- персональный сетевой экран - программа, установленная на пользовательском компьютере и предназначенная для защиты от несанкционированного доступа только этого компьютера.

Вырожденный случай - использование традиционного сетевого экрана сервером, для ограничения доступа к собственным ресурсам.

В зависимости от уровня, на котором происходит контроль доступа, существует разделение на сетевые экраны, работающие на:

- сетевом уровне, когда фильтрация происходит на основе адресов отправителя и получателя пакетов, номеров портов транспортного уровня модели *OSI* и статических правил, заданных администратором;
- сеансовом уровне (также известные как *stateful*) - отслеживающие сеансы между приложениями, не пропускающие пакеты нарушающих спецификации *TCP/IP*, часто используемых в злонамеренных операциях - сканировании ресурсов, взломах через неправильные реализации *TCP/IP*, обрыв/замедление соединений, инъекция данных.

Антивирусная программа с разнообразными возможностями, позволяющими оптимально защитить персональный компьютер. Легкость в использовании и возможность автоматического обновления делают *BitDefender Antivirus* антивирусным продуктом «установил и забыл». Новый оптимизированный сканирующий механизм *BitDefender Antivirus* проверяет и лечит зараженные файлы в режиме *on access*, минимизируя вероятность потери данных. Стоимость 24.95 $. Без регистрации *BitDefender* работает 30 дней.

Комплексная стратегия защиты

Антивирус не убережет вас от хакерской атаки, так же как ***firewall*** не умеет искать вирусы, и оба они бессильны перед ***spyware***. Для обеспечения полной компьютерной безопасности необходимо использовать комплексную систему защиты: ***Antivirus + Firewall + Antispyware***.

Существуют системы безопасности, сделанные по принципу «все в одном». Одним из лучших представителей этого класса является ***Panda Security***. Однако, по данным сайта ***www.antivirus.ru***, за период с 03.2008 по 02.2009 г. ***Panda*** пропустила 125 вирусов из 283. Результат оставляет желать много лучшего.

Так же, при выборе антивируса не стоит забывать о том, что некоторые вирусы пишутся под определенный антивирус. К примеру, российские хакеры очень «любят» антивирус Касперского и ***DrWeb***.

Предлагаемая система защиты:

Antivirus: ***BitDefender*** либо ***A-SQUARED*** (есть бесплатная версия).

Firewall: ***Outpost firewall***.

Antispyware: ***Spyware Terminator*** (программа бесплатна, в некоторых случаях может заменить ***firewall***).

A-SQUARED

Бесплатное антивирусное решение ***a-squared Free Edition***, которое разрабатывает немецкая компания ***EMSI Software GmbH***, позволяет удалять с компьютера разного рода вредоносные программы, к которым относятся шпионы, рекламные программы, трояны, руткиты, звонилки и прочее. Бесплатная редакция включает в себя только сканер, которым вы сможете проверить свой компьютер и удалить вредоносные программы.

Outpost firewall

Персональный файрволл, проще говоря - программа для защиты компьютера от хакерских атак из Интернета. Кроме этого, Аутпост обеспечивает блокировку загрузки рекламы и активного содержимого вебстраниц, а тем самым - их более быструю загрузку.

С сайта разработчика можно скачать большое и подробное «Руководство пользователя» и не очень большое, но тоже полезное «Приступаем к работе» (оба документа - на русском языке). Стоимость 699 р.

Без регистрации ***Agnitum Outpost Firewall PRO*** работает 30 дней.

Spyware Terminator

Программа для обнаружения шпионских модулей и обеспечения компьютерной безопасности. ***Spyware Terminator*** может обнаружить и удалить практически все виды вредоносных программ. Доступно несколько видов сканирования: быстрое, полное и пользовательское. При полной проверке файлы проверяются наиболее тщательно. Выбрав свои персональные установки, можно найти оптимальный режим сканирования, наиболее подходящий пользователю по скорости и эффективности. Встроенная система безопасности включает защиту приложений и системы, а также ведет мониторинг утилит, непосредственно взаимодействующих с сетью. Таким образом, можно предотвратить заражение компьютера вредоносными программами и некоторыми вирусами. Тут имеется функция восстановления начальных настроек операционной системы, анализ подозрительных файлов и удаление защищенных файлов. Программа бесплатна.

УДК 519.6

Нина Ивановна Костюкова
Институт вычислительной математики и математической геофизики СО РАН

БЕЗОПАСНОСТЬ В ОПЕРАЦИОННЫХ СИСТЕМАХ, СЕТЕВАЯ БЕЗОПАСНОСТЬ©

Сетевые операционные системы

В компьютерных сетях персональные компьютеры могут взаимодействовать с другими сетевыми устройствами посредством кабельной системы и устройства связи. Однако одного аппаратного обеспечения недостаточно для работы сети. Для организации безопасного совместного использования файлов и оборудования серверам и рабочим станциям нужна операционная система (ОС), а для обмена информацией внутри сети требуется *протокол* (или язык), принятый в качестве стандарта.

Компьютерные сети - это нечто более сложное, чем группа ПК, соединенных кабелями и устройствами связи. Основная задача компьютерных сетей состоит в том, чтобы обеспечить совместное использование ресурсов (приложений, файлов, сообщений, принтеров, сканеров и так далее) между этими ПК. Такое совместное использование требует *операционной системы* (программного обеспечения), способной управлять множеством файлов и устройств, существующих в рамках этой компьютерной сети, и в то же время обеспечивать защиту этих ресурсов от несанкционированного использования. В этом заключается роль сетевой операционной системы (СОС).

Операционная система - «душа» любой компьютерной системы - в принципе является очень большой и сложной программой. Так что многие слабости программ присущи и операционным системам.