Лекция 6. КОМПЬЮТЕРНЫЕ ВИРУСЫ. АНТИВИРУСНЫЕ ПРОГРАММЫ

Вирусы и антивирусные средства

Компьютерный вирус — *специальная программа, способная самопроизвольно присоединяться к другим программам («заражать» их) и при запуске последних выполнять различные нежелательные действия: порчу файлов и каталогов, искажение результатов вычислений, засорение или стирание памяти, создание помех в работе компьютера.*

Наличие вирусов проявляется в следующих ситуациях:

- некоторые программы перестают работать или начинают работать некорректно;
- на экран выводятся посторонние сообщения, сигналы и другие эффекты;
- работа компьютера существенно замедляется;
- структура некоторых файлов оказывается испорченной и т.д.

1.3.1. Классификация компьютерных вирусов

Имеется несколько признаков классификации существующих компьютерных вирусов:

- по среде обитания;
- по области поражения;
- по особенностям алгоритма;
- по способу заражения;
- по деструктивным возможностям.

Рассмотрим приведенную классификацию более детально.

1. Классификация по среде обитания. Различают файловые, загрузочные, макро- и сетевые вирусы.

Файловые вирусы — наиболее распространенный тип вирусов. Эти вирусы внедряются в выполняемые файлы, создают файлы-спутники

(companion-вирусы) или используют особенности организации файловой системы (link-вирусы).

Загрузочные вирусы записывают себя в загрузочный сектор диска (boot-сектор) или в сектор системного загрузчика жесткого диска (Master Boot Record). Начинают работу при загрузке компьютера и обычно становятся резидентными (постоянно хранящимися во время работы в оперативной памяти). Как правило, эти вирусы состоят из двух частей, поскольку загрузочная запись имеет небольшой размер и в ней трудно разместить целиком программу вируса.

Макровирусы заражают файлы широко используемых пакетов обработки данных. Эти вирусы представляют собой программы, написанные на встроенных в эти пакеты языках программирования. Наибольшее распространение получили макровирусы для приложений Microsoft Office. Для своего размножения такие вирусы используют возможности встроенного языка Visual Basic for Applications (VBA). Вирусы находятся среди макросов, при помощи которых переносят себя из одного зараженного файла (документа или таблицы) в другие. Этот перенос, как правило, осуществляется при выполнении пользователем стандартных операций (открытие документа, сохранение, печать, закрытие и др).

Опишем один из наиболее простых и часто используемых принципов активизации макровирусов редактора Microsoft Word. Существует жесткая зависимость между событиями, возникаемыми в этом редакторе, и именами автоматически запускаемых макрокоманд. Так, при запуске редактора автоматически выполняется макрос с именем AutoExec, при завершении работы — макрос AutoExit, а при создании нового документа — AutoNew.

В случае, если пользователь выбрал в редакторе Word команду открытия документа, осуществляется поиск и запуск макроса AutoOpen, при закрытии документа — макроса AutoClose. При работе с документом редактор MS Word выполняет встроенные макросы: при сохранении файла по команде *Файл-Сохранить как* вызывается макрос FileSaveAs, при печати — FilePrint и

пр. Полный перечень таких макросов пользователь имеет возможность самостоятельно просмотреть, выполнив в редакторе MS Word команду *Сервис-Настройка* и нажав в появившемся диалоговом окне *Настройка* пиктограмму *Клавиатура.*

Первоначальное заражение осуществляется следующим образом. Пользователь, редактируя зараженный документ, заражает сам редактор. Действительно, при выборе пользователем обычной команды меню *(Файл-Открыть, Файп-Закрытъ, Файл-Сохранить как* и пр.) редактор Word автоматически активизирует содержащийся в соответствующем макросе код вируса.

Большинство вирусов редактора MS Word при запуске переносят свой код (макросы) в область глобальных макросов документа. При выходе из редактора глобальные макросы (включая макросы вируса) автоматически записываются в файл шаблона NORMAL.DOT. Таким образом, редактор Word оказывается зараженным. Затем этот редактор заражает все редактируемые файлы. Так, при последующем запуске редактора MS Word вирус активизируется автоматически. Затем вирус переопределяет один или несколько стандартных макросов (например, FileOpen, FileSaveAs, FilePrint), впоследствии перехватывает команды работы с файлами. При вызове этих команд вирус заражает файл, к которому идет обращение. Если вирус перехватывает макрос FileSaveAs, то заражается каждый сохраняемый DOC-файл. Если перехвачен макрос FileOpen, то вирус записывает в файл свои макросы при его считывании с диска.

Похожие механизмы используются и в других приложениях MS Office. Так, алгоритм работы макровирусов для MS Excel во многом аналогичен методам работы вирусов для MS Word. Различия заключаются в командах копирования макросов (например, Sheets.Copy), в отсутствии файла NORMAL.DOT — вирусы сохраняются в файлах, находящихся в каталоге STARTUP.

Отметим, что существует простой способ блокировки действия автоматических макросов, которые содержатся в документе и активизируются в момент его открытия, — удержание нажатой клавиши <Shift> при открытии файла.

Сетевые вирусы используют для своего распространения протоколы или команды компьютерных сетей и электронной почты. Основным принципом работы сетевого вируса является возможность самостоятельно передать свой код на удаленный сервер или рабочую станцию. Полноценные сетевые вирусы при этом должны обладать возможностью запустить на удаленном компьютере свой код на выполнение.

Наибольшую известность сетевые вирусы приобрели в конце 1990-х годов. Так, например, макровирус Macro. Word.ShareFim, используя возможности электронной почты Microsoft Mail, создает новое письмо, содержащее зараженный документ, затем выбирает из списка адресов MS Mail несколько случайных адресов и рассылает по ним зараженное письмо. Поскольку многие пользователи устанавливают параметры MS Mail таким образом, чтобы при получении письма он автоматически запускал MS Word, то вирус внедряется в компьютер адресата.

На практике существуют разнообразные сочетания вирусов — например, файлово-загрузочные вирусы, заражающие как файлы, так и загрузочные сектора дисков, или сетевые макровирусы, которые заражают редактируемые документы и рассылают свои копии по электронной почте.

2. Классификация по области поражения. Как правило, каждый вирус заражает файлы одной или нескольких операционных систем: DOS, Windows, Win95/NT, OS/2, Unix. Макровирусы заражают файлы форматов MS Word, MS Excel и других приложений MS Office. Многие загрузочные вирусы также ориентированы на конкретные форматы расположения системных данных в загрузочных секторах дисков.

3. Классификация по особенностям алгоритма. Выделяют резидентные вирусы, стелс-вирусы (stealth — *англ.* невидимка), полиморфные и другие вирусы.

Резидентные вирусы способны оставлять свои копии (или части) в операционной памяти, перехватывать обработку событий (например, обращения к файлам или дискам) и вызывать при этом процедуры заражения объектов (файлов и секторов). Эти вирусы активны в памяти не только в момент работы зараженной программы, но и после. Резидентные копии таких вирусов жизнеспособны до перезагрузки операционной системы, даже если на диске уничтожены все зараженные файлы. От таких вирусов сложно избавиться простым восстановлением копий файлов с дистрибутивных или резервных дисков. Это объясняется тем, что резидентная копия вируса остается активной в оперативной памяти и заражает вновь создаваемые файлы. Если резидентный вирус является также загрузочным и активизируется при загрузке операционной системы, то даже форматирование диска при наличии в памяти этого вируса его не удаляет. Это объясняется тем, что многие резидентные вирусы заражают диск повторно после того, как он отформатирован.

Нерезидентные вирусы, напротив, активны довольно непродолжительное время — только в момент запуска зараженной программы. Для своего распространения они выбирают на диске незараженные файлы и записываются в них. После окончания работы зараженной программы вирус становится неактивным вплоть до очередного запуска какой-либо зараженной программы. Следует отметить, что зараженные нерезидентными вирусами файлы восстанавливаются значительно проще.

К разновидности резидентных вирусов следует отнести и макровирусы, поскольку они постоянно присутствуют в памяти компьютера во время работы зараженного редактора.

Стелс-алгоритмы позволяют вирусам полностью или частично скрыть свое присутствие. Наиболее распространенным стелс-алгоритмом является перехват запросов операционной системы на чтение/запись зараженных объектов. Стелс-вирусы при этом либо временно «лечат» эти объекты, либо подставляют вместо себя незараженные участки информации. Наиболее распространенным способом реализации стеле-алгоритмов в макровирусах является запрет выполнения ряда команд, например *Сервис-Макрос*. Частично к стелс-вирусам относят небольшую группу макровирусов, хранящих свой основной код не в макросах, а в других областях документа — в его переменных или в Auto-text.

Полиморфность (самошифрование) используется для усложнения процедуры обнаружения вируса. Полиморфные вирусы — это трудно выявляемые вирусы, не имеющие постоянного участка кода. В общем случае два образца одного и того же вируса не имеют совпадений. Это достигается шифрованием основного тела вируса и модификациями программы-расшифровщика. Так, например, некоторые макровирусы при создании своих новых копий случайным образом меняют имена своих переменных, вставляют пустые строки или модифицируют свой код иным способом.

При создании вирусов часто используются *нестандартные приемы*. Их применение должно максимально затруднить обнаружение и удаление вируса.

4. Классификация по способу заражения. Различают так называемые троянские программы, утилиты скрытого администрирования, Intended-вирусы и пр.

Троянские программы получили свое название по аналогии с троянским конем. Назначение этих программ — имитация каких-либо полезных программ, новых версий популярных утилит или дополнений к ним. Очень часто они рассылаются через BBS-станции или электронные конференции. При их записи пользователем на свой компьютер троянские программы активизируются и выполняют нежелательные действия.

Разновидностью троянских программ являются *утилиты скрытого администрирования* (backdoor). По своей функциональности и интерфейсу они во многом напоминают системы администрирования компьютеров в сети, разрабатываемые и распространяемые различными фирмами-производителями программных продуктов. При инсталляции эти утилиты самостоятельно устанавливают на компьютере систему скрытого удаленного управления. В результате возникает возможность скрытого управления этим компьютером. Реализуя заложенные алгоритмы, утилиты без ведома пользователя принимают, запускают или отсылают файлы, уничтожают информацию, перезагружают компьютер и пр. Возможно использование этих утилит для обнаружения и передачи паролей и иной конфиденциальной информации, запуска вирусов, уничтожения данных.

К *Intended-вирусам* относятся программы, которые не способны размножаться из-за существующих в них ошибок. Например, вирусы при заражении не помещают в начало файла команду передачи управления на код вируса или записывают в нее неверный адрес своего кода. К этому классу также можно отнести вирусы, которые размножаются только один раз. Заразив какой-либо файл, они теряют способность к дальнейшему размножению через него.

5. Классификация по деструктивным возможностям. Вирусы разделяют на:

- *неопасные,* влияние которых ограничивается уменьшением свободной памяти на диске, замедлением работы компьютера, графическими и звуковыми эффектами;
- *опасные,* которые потенциально могут привести к нарушениям в структуре файлов и сбоям в работе компьютера;
- *очень опасные,* в алгоритм работы которых специально заложены процедуры уничтожения данных и, согласно одной из неподтвержденных гипотез, возможность обеспечивать быстрый износ движущихся частей

механизмов путем ввода в резонанс и разрушения головок записи/чтения некоторых накопителей на жестких дисках.

1.3.2. Конструкторы вирусов

Конструктор вирусов — это утилита, предназначенная для изготовления новых компьютерных вирусов. Известны конструкторы вирусов для DOS, Windows и макровирусов. Они позволяют генерировать исходные тексты вирусов, объектные модули и/или непосредственно зараженные файлы. Некоторые конструкторы снабжены стандартным оконным интерфейсом, где при помощи системы меню можно выбрать тип вируса, поражаемые объекты, наличие или отсутствие самошифровки, противодействие отладчику, внутренние текстовые строки, сопровождающие работу вируса эффекты и др.

Существуют также вспомогательные утилиты, полиморфик-генераторы. Эти генераторы не являются вирусами, поскольку в их алгоритм не закладываются функции размножения. Главной функцией подобного рода утилит является шифрование тела вируса и генерация соответствующего расшифровщика. Обычно полиморфик-генераторы доступны, поэтому автору полиморфного вируса не требуется разрабатывать коды собственного за/расшифровщика. При желании он может подключить к своему вирусу известный полиморфик-генератор и вызывать его из кодов вируса. Вызов полиморфик-генератора создает коды расшифровщика и шифрует тело вируса.

1.3.3. Методы борьбы с компьютерными вирусами

Для борьбы с вирусами существуют программы, которые можно классифицировать по основным группам: мониторы, детекторы, доктора, ревизоры и вакцины.

Программы-мониторы (иначе называемые программы-фильтры) располагаются резидентно в оперативной памяти компьютера, перехватывают и сообщают пользователю об обращениях операционной

системы, которые используются вирусами для размножения и нанесения ущерба. Пользователь имеет возможность разрешить или запретить выполнение этих обращений. К преимуществу таких программ относят возможность обнаружения неизвестных вирусов. Это актуально при наличии самомодифицирующихся вирусов. Использование программ-фильтров позволяет обнаруживать вирусы на ранней стадии заражения компьютера.

Недостатками программ являются: а) невозможность отслеживания вирусов, обращающихся непосредственно к BIOS, а также загрузочных вирусов, активизирующихся до запуска антивируса при загрузке DOS; *б)* частая выдача запросов на выполнение операции.

Программы-детекторы проверяют, имеется ли в файлах и на дисках специфическая для данного вируса комбинация байтов. При ее обнаружении выводится соответствующее сообщение. Однако если программа не опознается детекторами как зараженная, то возможно в ней находится новый вирус или модифицированная версия старого, неизвестного программе-детектору.

Программы-доктора восстанавливают зараженные программы путем удаления из них тела вируса. Обычно эти программы рассчитаны на конкретные типы вирусов и основаны на сравнении последовательности кодов, содержащихся в теле вируса, с кодами проверяемых программ. Программы-доктора необходимо периодически обновлять с целью получения новых версий, обнаруживающих новые виды вирусов.

Программы-ревизоры анализируют изменения состояния файлов и системных областей диска. Проверяют состояния загрузочного сектора и таблицы FAT; длину, атрибуты и время создания файлов; контрольную сумму кодов. Пользователю сообщается о выявлении несоответствий.

Программы-вакцины модифицируют программы и диски так, что это не отражается на работе программ, но вирус, от которого производится вакцинация, считает программы или диски уже зараженными.

Существующие антивирусные программы в основном относятся к классу гибридных программ (детекторы-доктора, доктора-ревизоры и др.).

При заражении или при подозрении на заражение компьютера вирусом необходимо:

1. Оценить ситуацию и не предпринимать действий, приводящих к потере информации. Если вы не обладаете достаточными знаниями и опытом, лучше обратиться к специалистам.
2. Перезагрузить ОС компьютера. При этом использовать специальную, заранее созданную и защищенную от записи системную дискету. В результате будет предотвращена активизация загрузочных и резидентных вирусов с жесткого диска компьютера.
3. Запустить имеющиеся антивирусные программы, пока не будут обнаружены и удалены все вирусы. В случае невозможности удалить вирус и при наличии в файле ценной информации произвести архивирование файла и подождать выхода новой версии антивируса. После окончания перезагрузить компьютер.

К антивирусным программам, получившим распространение в России, странах СНГ и за рубежом, относят программы фирм Symantec (Norton Antivirus), Network Associates (Doctor Solomon) и отечественных фирм — Лаборатории Касперского (AntiViral Toolkit Pro) и ДиалогНаука (ADinf, Dr.Web).

Антивирусный пакет **AntiViral Toolkit Pro** (AVP) включает AVP *Сканер* (рис. 1.6 а), резидентный сторож AVP *Монитор,* программу администрирования установленных компонент AVP *Центр Управления* и ряд других.

AVP *Сканер,* помимо традиционной проверки выполняемых файлов и файлов документов, обрабатывает базы данных электронной почты форматов MS Outlook, Exchange и текстовых почтовых форматов Netscape Navigator, SMTP/POP3 server и др. (рис. 1.6 *б).* Использование сканера позволяет

выявить вирусы в упакованных и архивированных файлах (не защищенных паролями). Обнаруживает и удаляет макровирусы, полиморфные,

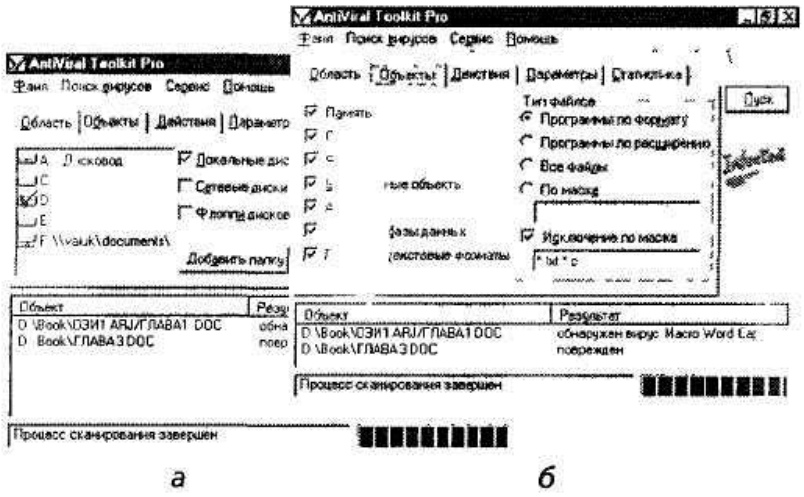

РИС. 1.6. Пользовательский интерфейс приложения AVP Сканер (а) и установка проверяемых объектов (б)

стелс, троянские, а также ранее неизвестные вирусы. Это достигается, например, за счет использования эвристических анализаторов. Такие анализаторы моделируют работу процессора и выполняют анализ действий диагностируемого файла. В зависимости от этих действий и принимается решение о наличии вируса.

AVP *Монитор* — контролирует типовые пути проникновения вируса, например операции обращения к файлам и секторам.

AVP *Центр Управления* — сервисная оболочка, предназначенная для установки времени запуска сканера, автоматического обновления компонент пакета и др.

Вопросы для самопроверки

1. В каких ситуациях требуется использовать: а) программы архивирования; *б)* программы обслуживания дисков; е) антивирусные средства?
2. Каков принцип архивирования данных и оптимизации дисков?
3. Какие функции программ-архиваторов относятся к типовым?
4. Что представляют собой программы обслуживания дисков?
5. Какова разница между оптимизацией и форматированием?
6. Какова классификация компьютерных вирусов?

7. Что представляют собой вирусы, заражающие текстовые файлы?

8. Какова классификация антивирусных программ?

9. Каковы методы борьбы с компьютерными вирусами? Действия при заражении информации компьютерными вирусами.