

## **18. Классификация компьютерных вирусов. Диагностика заражения вирусом. Основы функционирования антивирусного ПО**

### **Свойства компьютерных вирусов**

*Вирус* - это программа.

Такое простое утверждение само по себе способно развеять множество легенд о необыкновенных возможностях компьютерных вирусов. Вирус может перевернуть изображение на вашем мониторе, но не может перевернуть сам монитор. К легендам о вирусах-убийцах, «уничтожающих операторов посредством вывода на экран смертельной цветовой гаммы 25-м кадром» также не стоит относиться серьезно.

*Вирус* - программа, обладающая способностью к самовоспроизведению. Такая способность является единственным средством, присущим всем типам вирусов. Но не только вирусы способны к самовоспроизведению. Любая операционная система и еще множество программ способны создавать собственные копии. Копии же вируса не только не обязаны полностью совпадать с оригиналом, но и могут вообще с ним не совпадать!

*Вирус не может существовать в «полной изоляции»:* сегодня нельзя представить себе вирус, который не использует код других программ, информацию о файловой структуре или даже просто имена других программ. Причина понятна: вирус должен каким-нибудь способом обеспечить передачу себе управления.

### **Классификация вирусов:**

- по среде обитания
- по способу заражения среды обитания
- по степени воздействия
- по особенностям алгоритма

**В зависимости от среды обитания вирусы можно разделить на сетевые, файловые, загрузочные и файлово-загрузочные.**

*Сетевые вирусы* распространяются по различным компьютерным сетям.

*Файловые вирусы* внедряются главным образом в исполняемые модули, т. е. в файлы, имеющие расширения COM и EXE. Файловые вирусы могут внедряться и в другие типы файлов, но, как правило, записанные в таких файлах, они никогда не получают управление и, следовательно, теряют способность к размножению.

*Загрузочные вирусы* внедряются в загрузочный сектор диска (Boot-сектор) или в сектор, содержащий программу загрузки системного диска (Master Boot Record).

*Файлово-загрузочные вирусы* заражают как файлы, так и загрузочные сектора дисков.

**По способу заражения вирусы делятся на резидентные и нерезидентные.**

*Резидентный вирус* при заражении (инфицировании) компьютера *оставляет в оперативной памяти свою резидентную часть*, которая потом перехватывает обращение операционной системы к объектам заражения (файлам, загрузочным секторам дисков и т. п.) и внедряется в них. Резидентные вирусы находятся в памяти и являются активными вплоть до выключения или перезагрузки компьютера.

*Нерезидентные вирусы не заражают память компьютера* и являются активными ограниченное время.

**По степени воздействия вирусы можно разделить на следующие виды:**

- неопасные, не мешающие работе компьютера, но уменьшающие объем свободной оперативной памяти и памяти на дисках, действия таких вирусов проявляются в каких-либо графических или звуковых эффектах
- опасные вирусы, которые могут привести к различным нарушениям в работе компьютера
- очень опасные, воздействие которых может привести к потере программ, уничтожению данных, стиранию информации в системных областях диска.

По особенностям алгоритма вирусы трудно классифицировать из-за большого разнообразия.

**Простейшие вирусы** - паразитические, они изменяют содержимое файлов и секторов диска и могут быть достаточно легко обнаружены и уничтожены.

**Вирусы-репликаторы**, называемые *червями*, которые распространяются по компьютерным сетям, вычисляют адреса сетевых компьютеров и записывают по этим адресам свои копии.

Известны **вирусы-невидимки**, называемые *стелс-вирусами*, которые очень трудно обнаружить и обезвредить, так как они перехватывают обращения операционной системы к пораженным файлам и секторам дисков и подставляют вместо своего тела незараженные участки диска.

Наиболее трудно обнаружить **вирусы-мутанты**, содержащие алгоритмы шифровки-расшифровки, благодаря которым копии одного и того же вируса не имеют ни одной повторяющейся цепочки байтов. Имеются и так называемые квазивирусные или «тройанские» программы, которые хотя и не способны к самораспространению, но очень опасны, так как, маскируясь под полезную программу, разрушают загрузочный сектор и файловую систему дисков.

## **Загрузочные вирусы**

Рассмотрим схему функционирования очень простого загрузочного вируса, заражающего дискеты. (boot-sector).

Пусть у вас имеются чистая дискета и зараженный компьютер, под которым мы понимаем компьютер с активным резидентным вирусом. Как только этот вирус обнаружит, что в дисковом диске появилась подходящая жертва - в нашем случае не защищенная от записи и еще не зараженная дискета, он приступает к заражению.

### **Заражая дискету, вирус производит следующие действия:**

- выделяет некоторую область диска и помечает ее как недоступную операционной системе, это можно сделать по-разному, в простейшем и традиционном случае занятые вирусом секторы помечаются как сбойные (bad)
- копирует в выделенную область диска свой хвост и оригинальный (здоровый) загрузочный сектор
- замещает программу начальной загрузки в загрузочном секторе (настоящем) своей головой
- организует цепочку передачи управления согласно схеме.

Таким образом, голова вируса теперь первой получает управление, вирус устанавливается в память и передает управление оригинальному загрузочному сектору.

## **Файловые вирусы**

Рассмотрим теперь схему работы простого файлового вируса.

В отличие от загрузочных вирусов, которые практически всегда резидентны, файловые вирусы совсем не обязательно резидентны. Рассмотрим схему функционирования нерезидентного файлового вируса. Пусть у нас имеется инфицированный исполняемый файл.

При запуске такого файла вирус получает управление, производит некоторые действия и передает управление «хозяину»

*Какие же действия выполняет вирус?* Он ищет новый объект для заражения - подходящий по типу файл, который еще не заражен. Заражая файл, вирус внедряется в его код, чтобы получить управление при запуске этого файла. Кроме своей основной функции - размножения, вирус вполне может сделать что-нибудь замысловатое (сказать, спросить, сыграть) - это уже зависит от фантазии автора вируса.

Если файловый вирус резидентный, то он установится в память и получит возможность заражать файлы и проявлять прочие способности не только во время работы зараженного файла. Заражая исполняемый файл, вирус всегда изменяет его код - следовательно, заражение исполняемого файла всегда можно обнаружить.

*Но, изменяя код файла, вирус не обязательно вносит другие изменения:*

- он не обязан менять длину файла

- неиспользуемые участки кода
- не обязан менять начало файла

Таким образом, при запуске любого файла вирус получает управление (операционная система запускает его сама), резидентно устанавливается в память и передает управление вызванному файлу.

## **Загрузочно-файловые вирусы**

**Основное разрушительное действие** - *шифрование секторов винчестера*. При каждом запуске вирус шифрует очередную порцию секторов, а, зашифровав половину жесткого диска, радостно сообщает об этом. Основная проблема при лечении данного вируса состоит в том, что недостаточно просто удалить вирус из файлов, надо расшифровать зашифрованную им информацию.

## **Полиморфные вирусы**

Этот вид компьютерных вирусов представляется на сегодняшний день наиболее опасным. Объясним же, что это такое.

*Полиморфные вирусы* - вирусы, модифицирующие свой код в зараженных программах таким образом, что два экземпляра одного и того же вируса могут не совпадать ни в одном бите. Такие вирусы не только шифруют свой код, используя различные пути шифрования, но и содержат код генерации шифровщика и расшифровщика, что отличает их от обычных шифровальных вирусов, которые также могут шифровать участки своего кода, но имеют при этом постоянный код шифровальщика и расшифровщика.

*Полиморфные вирусы* - это вирусы с самомодифицирующимися расшифровщиками.

Цель такого шифрования: имея зараженный и оригинальный файлы, вы все равно не сможете проанализировать его код с помощью обычного дизассемблирования. Этот код зашифрован и представляет собой бессмысленный набор команд.

Расшифровка производится самим вирусом уже непосредственно во время выполнения.

При этом возможны варианты: он может расшифровать себя всего сразу, а может выполнить такую расшифровку «по ходу дела», может вновь шифровать уже отработавшие участки. Все это делается ради затруднения анализа кода вируса.

## **Стелс-вирусы**

Стелс-вирусы обманывают антивирусные программы и в результате остаются незамеченными. Тем не менее, существует простой способ отключить механизм маскировки стелс-вирусов. Достаточно загрузить компьютер с не зараженной системной дискеты и сразу, не запуская других программ с диска компьютера (которые также могут оказаться зараженными), проверить компьютер антивирусной программой.

## **Троянские кони, программные закладки и сетевые черви**

*Троянский конь* – это программа, содержащая в себе некоторую разрушающую функцию, которая активизируется при наступлении некоторого условия срабатывания. Обычно такие программы маскируются под какие-нибудь полезные утилиты. Вирусы могут нести в себе троянских коней или "троянизировать" другие программы – вносить в них разрушающие функции.

«Троянские кони» представляют собой программы, реализующие помимо функций, описанных в документации, и некоторые другие функции, связанные с нарушением безопасности и деструктивными действиями. Отмечены случаи создания таких программ с целью облегчения распространения вирусов. Списки таких программ широко публикуются в зарубежной печати. Обычно они маскируются под игровые или развлекательные программы и наносят вред под красивые картинки или музыку.

Если вирусы и «троянские кони» наносят ущерб посредством лавинообразного саморазмножения или явного разрушения, то основная функция вирусов типа «червь», действующих в компьютерных сетях, – взлом атакуемой системы, т.е. преодоление защиты с целью нарушения безопасности и целостности.

В более 80% компьютерных преступлений, расследуемых ФБР, "взломщики" проникают в атакуемую систему через глобальную сеть Internet. Когда такая попытка удастся, будущее компании, на создание которой ушли годы, может быть поставлено под угрозу за какие-то секунды. Этот процесс может быть автоматизирован с помощью вируса, сетевого червя.

*Червями называют вирусы, которые распространяются по глобальным сетям, поражая целые системы, а не отдельные программы.* Это самый опасный вид вирусов, так как объектами нападения в этом случае становятся информационные системы государственного масштаба. С появлением глобальной сети Internet этот вид нарушения безопасности представляет наибольшую угрозу, т. к. ему в любой момент может подвергнуться любой из 40 миллионов компьютеров, подключенных к этой сети.

## **Признаки появления вирусов**

При заражении компьютера вирусом важно его обнаружить. Для этого следует знать об основных признаках проявления вирусов. *К ним можно отнести следующие:*

- прекращение работы или неправильная работа ранее исправно работающих программ
- медленная работа компьютера
- невозможность загрузки операционной системы
- исчезновение файлов и каталогов или искажение их содержимого
- изменение даты и времени модификации файлов
- изменение размеров файлов
- неожиданное значительное увеличение количества файлов на диске
- существенное уменьшение размера свободной оперативной памяти
- вывод на экран непредусмотренных сообщений или изображений
- подача непредусмотренных звуковых сигналов
- частые зависания и сбои в работе компьютера

## **Методы защиты от компьютерных вирусов**

Каким бы не был вирус, пользователю необходимо знать основные методы защиты от компьютерных вирусов. *Для защиты от вирусов можно использовать:*

- общие средства защиты информации, которые полезны также и как страховка от физической порчи дисков, неправильно работающих программ или ошибочных действий пользователя;
- профилактические меры, позволяющие уменьшить вероятность заражения вирусом;
- специализированные программы для защиты от вирусов.

Общие средства защиты информации полезны не только для защиты от вирусов. *Имеются две основные разновидности этих средств:*

- копирование информации - создание копий файлов и системных областей дисков;
- разграничение доступа предотвращает несанкционированное использование информации, в частности, защиту от изменений программ и данных вирусами, неправильно работающими программами и ошибочными действиями пользователей.

## **Антивирусные программы**

Несмотря на то, что общие средства защиты информации очень важны для защиты от вирусов, все же их недостаточно. Необходимо и применение специализированных программ для защиты от вирусов. Эти программы можно разделить на несколько видов: детекторы, доктора (фаги), ревизоры, доктора-ревизоры, фильтры и вакцины (иммунизаторы).

ПРОГРАММЫ-ДЕТЕКТОРЫ позволяют обнаруживать файлы, зараженные одним из нескольких известных вирусов. Эти программы проверяют, имеется ли в файлах на указанном пользователем диске специфическая для данного вируса комбинация байтов. При ее обнаружении в каком-либо файле на экран выводится соответствующее сообщение.

Многие детекторы имеют режимы лечения или уничтожения зараженных файлов.

Следует подчеркнуть, что программы-детекторы могут обнаруживать только те вирусы, которые ей "известны". Программа Scan фирмы McAfee Associates и Aidtest Д.Н. Лозинского позволяют обнаруживать около 1000 вирусов, но всего их более пяти тысяч! Некоторые

программы-детекторы, например Norton AntiVirus или AVSP фирмы "Диалог-МГУ", могут настраивать на новые типы вирусов, им необходимо лишь указать комбинации байтов, присущие этим вирусам. Тем не менее невозможно разработать такую программу, которая могла бы обнаруживать любой заранее неизвестный вирус.

Примеры: AIDSTEST, DOCTOR WEB, Microsoft Antivirus, ADINF (Advanced Diskinfoscope).

## **ДЕЙСТВИЯ ПРИ ЗАРАЖЕНИИ ВИРУСОМ**

При заражении компьютера вирусом (или при подозрении на это) важно соблюдать некоторые правила:

*1) Прежде всего не надо торопиться и принимать опрометчивых решений.*

Непродуманные действия могут привести не только к потере части файлов, но к повторному заражению компьютера.

*2) Надо немедленно выключить компьютер, чтобы вирус не продолжал своих разрушительных действий.*

*3) Все действия по обнаружению вида заражения и лечению компьютера следует выполнять при загрузке компьютера с защищенной от записи дискеты с ОС (обязательное правило).*

*4) Если Вы не обладаете достаточными знаниями и опытом для лечения компьютера, попросите помочь более опытных коллег.*

ПРОГРАММЫ-РЕВИЗОРЫ имеют две стадии работы. Сначала они запоминают сведения состояния программ и системных областей дисков (загрузочного сектора и сектора с таблицей разбиения жесткого диска). Предполагается, что в этот момент программы и системные области дисков не заражены. После этого с помощью программы-ревизора можно в любой момент сравнить состояние программ и системных областей дисков с исходным. О выявленных несоответствиях сообщается пользователю.

ДОКТОРА-РЕВИЗОРЫ, - программы, которые не только обнаруживают изменения в файлах и системных областях дисков, но и могут в случае изменений автоматически вернуть их в исходное состояние. Такие программы могут быть гораздо более универсальными, чем программы-доктора, поскольку при лечении они используют заранее сохраненную информацию о состоянии файлов и областей дисков. Это позволяет им вылечивать файлы даже от тех вирусов, которые не были созданы на момент написания программы.

Но они могут лечить не от всех вирусов, а только от тех, которые используют "стандартные", известные на момент написания программы, механизмы заражения файлов.

Существуют также ПРОГРАММЫ-ФИЛЬТРЫ, которые располагаются резидентно в оперативной памяти компьютера и перехватывают те обращения к операционной системе, которые используются вирусами для размножения и нанесения вреда, и сообщают о них пользователя. Пользователь может разрешить или запретить выполнение соответствующей операции.

Некоторые программы-фильтры не "ловят" подозрительные действия, а проверяют вызываемые на выполнение программы на наличие вирусов. Это вызывает замедление работы компьютера.

Однако преимущества использования программ-фильтров весьма значительны – они позволяют обнаружить многие вирусы на самой ранней стадии, когда вирус еще не успел размножиться и что-либо испортить. Тем самым можно свести убытки от вируса к минимуму.

ПРОГРАММЫ-ВАКЦИНЫ, или ИММУНИЗАТОРЫ, модифицируют программы и диски таким образом, что это не отражается на работе программ, но тот вирус, от которого производится вакцинация, считает эти программы или диски уже зараженными. Эти программы крайне неэффективны.

Ни один тип антивирусных программ по отдельности не дает полной защиты от вирусов.