Виды компьютерных вирусов. Ознакомление с антивирусными программами.

Понятие компьютерного вируса.

Массовое применение персональных компьютеров, к сожалению, оказалось связанным с появлением самовоспроизводящихся программ–вирусов, препятствующих нормальной работе компьютера, разрушающих файловую структуру дисков и наносящих ущерб хранимой в компьютере информации. Проникнув в один компьютер, компьютерный вирус способен распространиться на другие компьютеры.

Компьютерный вирус – специально написанная программа деструктивного характера, способная самопроизвольно присоединять к другим программам свои копии и внедрять их в файлы, системные области жестких дисков.

Причины появления и распространения компьютерных вирусов, с одной скрываются в психологии человеческой личности и ее теневых сторонах (тщеславии непризнанных творцов, невозможности конструктивно применить способности), с другой стороны, обусловлены отсутствием аппаратных средств защиты персонального компьютера.

Несмотря на принятые во многих странах законы о борьбе с компьютерными преступлениями и разработку специальных программных средств защиты от вирусов, количество новых программных вирусов постоянно растет. На сегодняшний день известно **более 700 тыс. вирусов!!!**, для которых разработаны антивирусные средства. Это требует от пользователя компьютера знаний о природе вирусов, способах заражения вирусами и защиты от них.

Основными путями проникновения вирусов в компьютер являются **съемные носители (гибкие и лазерные диски), а также компьютерные сети.**

Программа или иной объект, содержащая вирус, называется **зараженной.**

При заражении компьютера вирусом очень важно своевременно его обнаружить. Для этого следует знать об основных **признаках проявления вирусов:**

- прекращение работы или неправильная работа ранее успешно функционирования 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.

Следует заметить, что вышеперечисленные явления необязательно вызываются присутствием вируса, а могут быть следствием других причин. Поэтому всегда затруднена правильная диагностика состояния компьютера.

Основные виды вирусов.

В настоящее время известно более 700 тыс. программных вирусов, их можно классифицировать по следующим признакам:

– среде обитания;

– по воздействию;

– по способу заражения ОЗУ;

– по особенностям алгоритма;

В зависимости от среды обитания вирусы можно разделить на сетевые, файловые, загрузочные.

Сетевые вирусы распространяются по локальным и глобальным компьютерным сетям.

Файловые вирусы внедряются главным образом в исполняемые модули, т.е. в файлы, имеющие расширения .**COM** и .**EXE**. Заражая файл, вирус внедряется в его код, чтобы получить управление при запуске этого файла. После запуска вирус помешается в оперативную память и поражает другие исполняемые файлы, к которым обратился пользователь. Кроме своей основной функции – размножения вирус может сделать что–нибудь: спросить, сыграть, показать изображение.

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

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).

Загрузочный сектор – это сектор на дискете или жестком диске с которого происходит загрузка операционной системы программами BIOS.

Пусть у нас имеется зараженная дискета и "чистый" компьютер. Нормальная схема начальной загрузки такая: ПЗУ – ПНЗ (программа начальной загрузки в загрузочном секторе) – ОС

Заражая дискету, вирус делает следующее:

– выделяет некоторую область диска и помечает ее как недоступную ОС (сбойные секторы bad);

– копирует в выделенную область диска свой «хвост» и здоровый загрузочный сектор;

– Замещает программу загрузки своей «головой».

В итоге последовательность загрузки изменяется и замедляется, так как появилось новое звено – вирус.

При воздействии вируса схема изменяется **ПЗУ–ВИРУС–ПНЗ–ОС**

Таким же образом поражаются загрузочные секторы винчестеров.

По способу функционирования 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 диска и внедряется в них). Резидентные вирусы находятся в памяти и являются активными 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 оперативной и внешней памяти, действия таких вирусов проявляется 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, поражению данных, стиранию информации в системных областях диска (Чернобыль 26 апреля «Chih»).

По особенностям алгоритма можно выделить следующие группы вирусов:

– компаньон–вирусы (companion) – это вирусы, не изменяющие файлы, но создающие файлы–компаньоны. Алгоритм работы этих вирусов состоит в том, что они создают для EXE–файлов файлы–спутники, имеющие то же самое имя, но с расширением .COM, (например, для файла ABC.EXE создается файл ABC.COM. Вирус записывается в COM–файл и никак не изменяет EXE–файл. При запуске такого файла ОС первым обнаружит и выполнит COM–файл, т.е. вирус, который затем запустит и EXE–файл. (Пример: I.Worm.Stator.a).

– сетевые вирусы – (черви, worm) распространяются по информационным сетям с одного сервера на другой, как правило, не выполняя деструктивных действий (по причине большого разнообразия и хорошей защищенности различных серверных ОС). Вред сетевых вирусов состоит в дополнительном расходе памяти и каналов связи, кроме того, черви могут служить транспортом для распространения других видов вирусов. Частный случай сетевых вирусов – почтовые черви (mail worm), распространяемые во вложениях к электронным письмам. Весной 2000 года несколько модификаций такого рода вирусов поразили миллионы компьютеров во всём мире. Почтовые черви могут причинить очень опасные повреждения информации, вплоть до полного уничтожения. Кроме того. Почтовые вирусы быстро распространяются, используя для этого адреса пользователей, содержащиеся в адресной книге почтовой программы.

(Пример: **вирус «Анна Курникова»**).

полиморфик–вирусы (polymorphic) – достаточно труднообнаруживаемые вирусы, модифицирующие свой код в зараженных программах таким образом, что два экземпляра одного и того же вируса не совпадают (имеют разные коды). Это вирусы с

самомодифицирующимися расшифровщиками. Цель такого шифрования – имея зараженный и оригинальный файлы невозможно определить наличие вируса.

Вирусы–невидимки (стелс–вирусы) – такие вирусы при обращении к файлам используют достаточно оригинальные алгоритмы, позволяющие «обманывать» резидентные антивирусные мониторы предотвращают свое обнаружение тем, что перехватывают обращения операционной системы (и тем самым прикладных программ) к зараженным файлам и областям диска и подставляют вместо своего тела незараженные участки диска. Разумеется, этот эффект наблюдается только на зараженном компьютере – на «чистом» компьютере изменения в файлах и загрузочных областях.

«Троянские» программы (шпионы) маскируясь под полезную программу, разрушают загрузочный сектор и файловую систему дисков. Не способны к самораспространению. **Троянцы,** после своего запуска, скрытно выполняют определенные действия, направленные на снижение защищенности информационной системы: передают по электронной почте или сети пароли, файлы и другую информацию с компьютера

Макровирусы распространяются внутри документов Microsoft Office (файлы с расширениями .DOC, .DOT, .XLS, и др.), позволяющих использовать *макросы – последовательности команд,* автоматически выполняемые при открытии документа. Для защиты от заражения макровирусом достаточно включить предупреждение о наличии макросов в документе и не в коем случае не запускать подозрительные макросы, если только полезность их Вам не очевидна.

Антивирусные программы. Антивирусные средства защиты. (Ознакомление с антивирусными программами).

Для обнаружения, удаления и защиты от компьютерных вирусов разработано несколько видов специальных программ, которые позволяют обнаруживать и уничтожать вирусы. Такие программы называются антивирусными.

Различают следующие виды антивирусных программ:

– программы–детекторы;
– программы–доктора или фаги;
– программы–ревизоры;
– программы–фильтры;
– программы–вакцины или иммунизаторы.

Программы–детекторы осуществляют поиск характерной для конкретного вируса последовательности байтов (сигнатуры вируса) в оперативной памяти и в файлах и при обнаружении выдают соответствующее сообщение. Недостатком таких программ является то, что они могут находить только те вирусы, которые известны разработчикам таких программ.(KidoKiller.exe , на вирус Worms Kido – заражает библиотеки и перехватывает управление над сетевым трафиком, происходит перегрузка сетевого канала).

Программы–доктора или фаги («от греч. жрать») не только находят зараженные вирусами файлы, но и «лечат» их, т.е. удаляют из файла тело программы

вируса, возвращая файлы в исходное состояние. В начале своей работы фаги ищут вирусы в оперативной памяти, уничтожая их, и только затем переходят к «лечению» файлов. Учитывая, что постоянно появляются новые вирусы, программы–детекторы и программы–доктора быстро устаревают, и требуется регулярное обновление их версий. NOD 32, Norton Antivirus, Doctor Web, Awast, Panda, KaV.

Программы–ревизоры относятся к самым надежным средствам защиты от вирусов. Ревизоры запоминают исходное состояние программ, каталогов и системных областей диска тогда, когда компьютер не заражен вирусом, а затем периодически или по желанию пользователя сравнивают текущее состояние с исходным. Обнаруженные изменения выводятся на экран монитора. Как правило, сравнение состояний производят сразу после загрузки операционной системы. При сравнении проверяются длина файла, код циклического контроля (контрольная сумма файла), дата и время модификации, другие параметры.

Программы–ревизоры имеют достаточно развитые алгоритмы, обнаруживают стелс–вирусы и могут даже отличить изменения версии проверяемой программы от изменений, внесенных вирусом. К числу программ–ревизоров относится широко распространенная в России программа ADinf фирмы "Диалог–Наука". Awast

Программы–фильтры или "сторожа" представляют собой небольшие резидентные программы, предназначенные для обнаружения подозрительных действий при работе компьютера, характерных для вирусов. Такими действиями могут являться:

– попытки коррекции файлов с расширениями COM и EXE;
– изменение атрибутов файлов;
– запись в загрузочные сектора диска;
–загрузка резидентной программы.

При попытке какой–либо программы произвести указанные действия «сторож» посылает пользователю сообщение и предлагает запретить или разрешить соответствующее действие. Программы–фильтры весьма полезны, так как способны обнаружить вирус на самой ранней стадии его существования до размножения. Однако они не "лечат" файлы и диски. Для уничтожения вирусов требуется применить другие программы, например фаги. К недостаткам программ–сторожей можно отнести их "назойливость" (например, они постоянно выдают предупреждение о любой попытке копирования исполняемого файла), а также возможные конфликты с другим программным обеспечением.

Вакцины или иммунизаторы – это резидентные программы, предотвращающие заражение файлов. Вакцины применяют, если отсутствуют программы–доктора, «лечащие» этот вирус. Вакцинация возможна только от известных вирусов. Вакцина модифицирует программу или диск таким образом, чтобы это не отражалось на их работе вирус будет воспринимать их зараженными и поэтому не внедрится. Panda Reaserch USB Vaccine 1.0

Современные антивирусные пакеты включают несколько программ с различными функциями.

Сегодня одним из наиболее популярных антивирусных пакетов является Dr.Web, антивирус Касперского (Kaspersky Anti–Virus – KAV).

Для проверки функционирования антивируса существует тест, созданный Европейским институтом антивирусных исследований – файл EICAR.com (всего 68 байт). Антивирус выдает сообщение: «Test (Not a Virus)», в графе действие – «неизлечим».

Подробнее:

Антивирус Касперского специально разработан для защиты персонального компьютера. Простые интерфейсы, централизованное управление, автоматическая работа позволяют продукту функционировать в фактически фоновом режиме до тех пор, пока компьютеру и данным не грозит опасность. В случае попытки проникновения вируса продукт автоматически определит источник угрозы и эффективно нейтрализует ее при минимальном участии пользователя.

Антивирус Касперского имеет специальные средства защиты – он проверяет входящую и исходящую почту, контролирует базы почтовых сообщений, обеспечивает безопасность подключений к Интернету и любых устанавливаемых программ.

Антивирус Касперского является последним технологическим достижением Лаборатории Касперского в области защиты домашнего компьютера от вирусных угроз. Возможности: 100%-ная защита от макровирусов. Защита даже от неизвестных вирусов. Надежный контроль целостности данных. Комплексная проверка почтовой корреспонденции. Защита мест хранения данных. Проверка памяти запущенных программ.

NOD 32 Antivirus System обеспечивает хорошо сбалансированную безупречную защиту персональных компьютеров и корпоративных систем, работающих на платформах MS Windows 95/98/ ME/NT/2000/2003/XP и т.д., UNIX/Linux и т.д., Novell, MS DOS, а также для почтовых серверов MS Exchange Server, Lotus Doino и др. Вирусы, черви, троянские программы и другой вредоносный код находятся на безопасном расстоянии от данных. Передовые методы обнаружения, используемые в программном обеспечении, защищают даже от будущих потенциальных опасностей и от большинства новых червей и вирусов.

Главным преимуществом NOD 32 является его быстрая работа, низкое потребление системных ресурсов, способность ловить почти 100 % вирусов.

Широко применяется программа-доктор *Dr. Web.* Она входит в состав антивирусного пакета DSAV, который распространяет фирма «Диалог-Наука». Программа-ревизор ADINF проверяет диски, программа Dr.Web анализирует новые и измененные файлы и выдает на экран сообщения и запросы.

После запуска Dr.Web открывается оболочка с меню, расположенным в верхней строке экрана. Для проверки следует выбрать пункты меню Тест -> Тестирование и указать путь для выполнения теста. После ввода откроется окно тестирования. С

помощью пункта Настройка нужно задать общие установки тестирования, уровень эвристики, высоту экрана, цветовую схему и т. д., а также действия при обнаружении зараженных файлов. После проверки выдается окно отчета о выполнении тестирования. Если обнаружен вирус, Dr.Web выведет отчет красным цветом.

Основные правила лечения файлов и системных областей дисков:
–запрещается выполнять непродуманные действия, которые могут привести к заражению ПК;
–если вирус еще не активизирован, то следует немедленно выключить компьютер;
–при заражении ПК вирусом компьютер следует перезагрузить и начать его лечение с дискет;
–все операции по обнаружению вируса и лечению ПК должны выполняться с эталонной, защищенной от записи дискеты с ОС;
–при лечении поиск вирусов следует проводить во всех файлах (например, задавая в программе Dr.Web параметр /al).

Профилактика заражения компьютера вирусами.

Для того чтобы не подвергнуть компьютер заражению вирусами и обеспечить надежное хранение информации на дисках, необходимо соблюдать следующие правила:
– оснастите свой компьютер современным антивирусным ПО и **постоянно обновляйте их базы;**
– используйте антивирусные программы для входного контроля **всех исполняемых файлов, получаемых из интернета;**
– перед считыванием с дискет, флэшек информации, записанной на других компьютерах**, всегда проверяйте съемные носители на наличие вирусов**, запуская антивирусные программы своего компьютера;
– при переносе на свой компьютер файлов в архивированном виде **проверяйте их перед распаковкой;**
– периодически проверяйте на наличие вирусов жесткие диски компьютера, запуская антивирусные программы для тестирования файлов, памяти и системных областей дисков, предварительно загрузив операционную систему с загрузочного диска;
– обязательно делайте архивные копии ценной для вас информации;
– не оставляйте съемные носители (флэшки, дискеты, мобил-рэк) при включении или перезагрузке операционной системы, чтобы исключить заражение компьютера загрузочными вирусами.