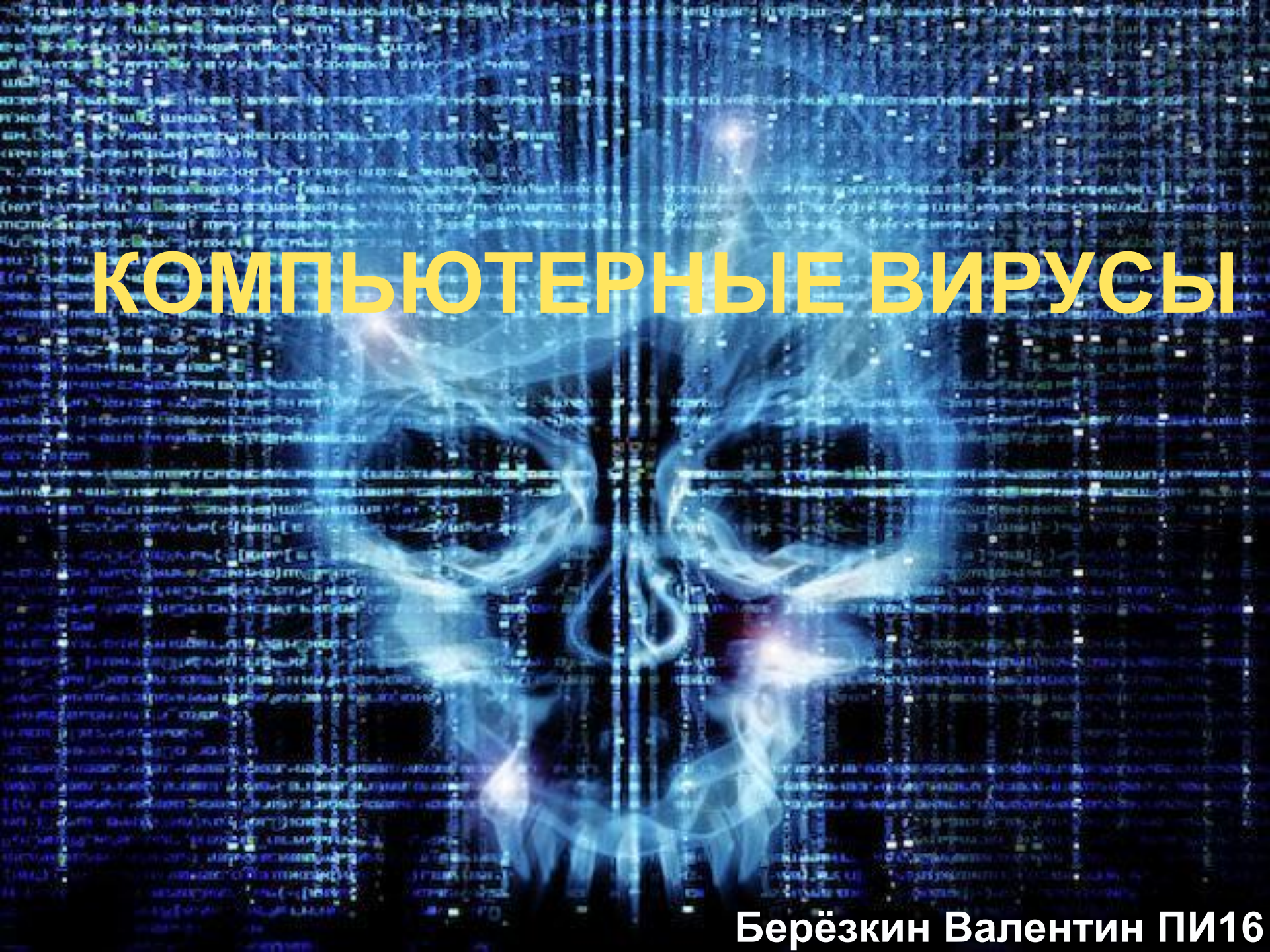


Берёзкин Валентин ПИ16

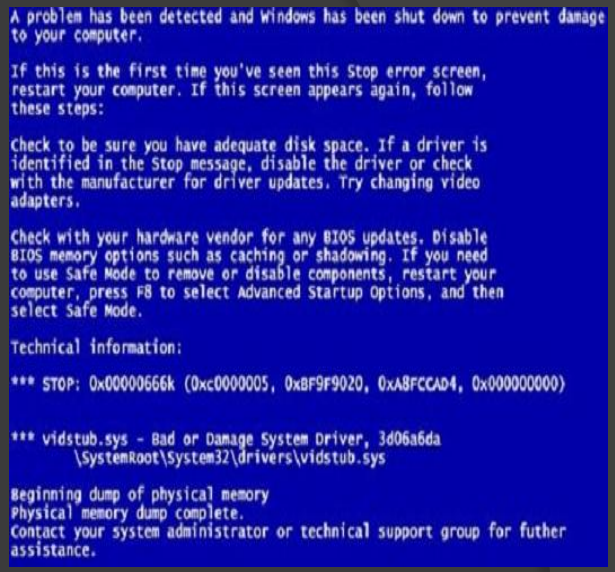
Компьютерные вирусы, их свойства и классификация

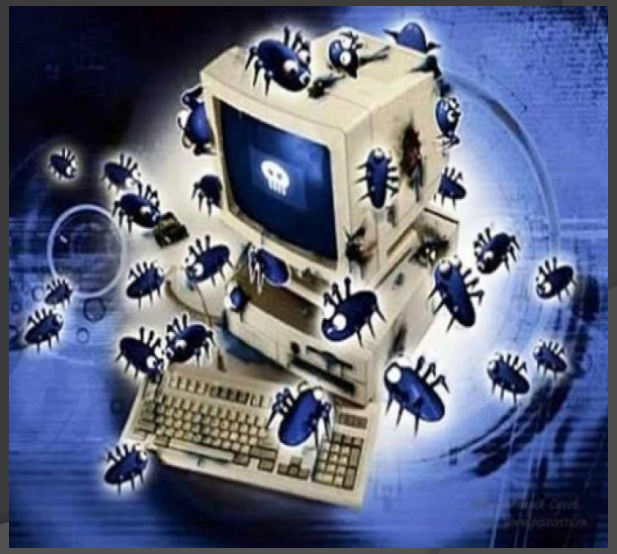
- Сегодня массовое применение персональных компьютеров, к сожалению, оказалось связанным с появлением самовоспроизводящихся программ-вирусов, препятствующих нормальной работе компьютера, разрушающих файловую структуру дисков и наносящих ущерб хранимой в компьютере информации.
- Несмотря на принятые но многих странах законы о борьбе с компьютерными преступлениями и разработку специальных программных средств защиты от вирусов, количество новых программных вирусов постоянно растет. Это требует от пользователя знаний о природе вирусов, способах заражения вирусами и защиты от них.

СВОЙСТВА КОМПЬЮТЕРНЫХ ВИРУСОВ

- Сейчас применяются персональные компьютеры, в которых пользователь имеет свободный доступ ко всем ресурсам машины. Именно это открыло возможность для опасности, которая получила название компьютерного вируса.
- Формальное определение понятия «компьютерный вирус» до сих пор не придумано, и есть серьезные сомнения, что оно вообще может быть дано. Многочисленные попытки дать «современное» определение вируса не привели к успеху. Чтобы почувствовать всю сложность проблемы, попробуйте, к примеру, дать определение понятия «редактор». Вы либо придумаете нечто очень обшее, либо начнете перечислять все известные типы редакторов. И то И другое вряд ли можно считать приемлемым. Поэтому мы ограничимся рассмотрением некоторых свойств компьютерных вирусов, которые позволяют говорить о них как об определенном классе программ.

- Прежде всего вирус — это программа. Такое простое утверждение само по себе способно развеять множество легенд о необыкновенных возможностях компьютерных вирусов Вирус может перевернуть изображение на вашем монитора 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. К сожалению, некоторые авторитетные издания время от времени публикуют самые свежие новости с компьютерных фронтов, которые при ближайшем рассмотрении оказываются следствием не вполне ясного понимания предмета.





- **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 себе передачу управления.

КЛАССИФИКАЦИЯ ВИРУСОВ

- В настоящее время известно более 70 000 программных вирусов, их можно классифицировать по следующим признакам:
- — среда обитания;
- — способ заражения среды обитания;
- — воздействие;
- — особенности 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 чаще всего в исполняемые модули, т. с. 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 и 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. Можно отметить 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 бантов. Имеются и так называемые квазивирусные («троянские») программы, которые хотя и не способны к самораспространению, но очень опасны, так как, маскируясь под полезную программу, разрушают загрузочный сектор и файловую систему дисков.

ОСНОВНЫЕ ВИДЫ ВИРУСОВ И СХЕМЫ ИХ ФУНКЦИОНИРОВАНИЯ

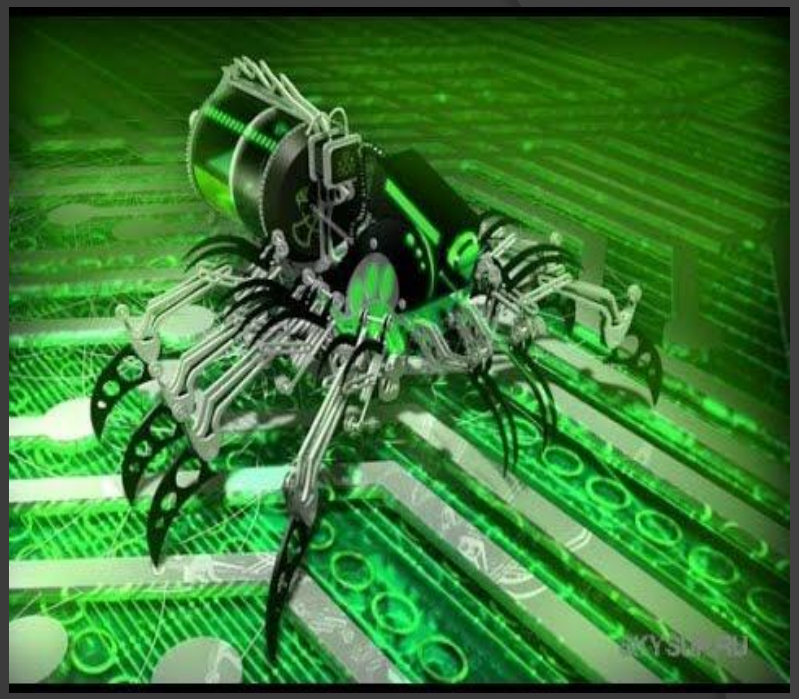
Среди всего разнообразия вирусов можно выделить следующие основные группы:

— загрузочные
— файловые
— файлово - загрузочные

- **Загрузочные вирусы** - записывающийся в первый сектор гибкого или жёсткого диска и выполняющийся при загрузке компьютера.
- При включении или перезагрузке компьютера Boot-вирус заменяет собой загрузочный код и таким образом получает управление ещё до непосредственного запуска операционной системы. Вместо операционной системы загружается вирус, размещая в памяти своё тело, которое хранит в неиспользованных секторах, идущих после главной загрузочной записи (MBR), но до первого загрузочного сектора раздела. Перехватив обращения к дискам, вирус продолжает загрузку операционной системы или нет(MBR-Locker). Размножается вирус записью в загрузочную область других накопителей компьютера.

- Простейшие загрузочные вирусы, находясь в памяти заражённого компьютера, обнаруживают в компьютере не заражённый диск и производят следующие действия:
- выделяют некоторую область диска и делают её недоступной операционной системе; замещают программу начальной загрузки в загрузочном секторе диска, копируя корректную программу загрузки, а также свой код, в выделенную область диска; организуют передачу управления так, чтобы вначале выполнялся код вируса и лишь затем — программа начальной загрузки. Загрузочные вирусы очень редко «уживаются» вместе на одном диске из-за того, что используют одни и те же дисковые сектора для размещения своего кода/данных. В результате код/данные первого вируса оказываются испорченными при заражении вторым вирусом, и система либо зависает, либо зацикливается при загрузке.
- Загрузочные вирусы были широко распространены в эпоху MS-DOS. Вирус Brain - первый в истории компьютерный вирус, вызвавший широкую эпидемию, относился именно к классу загрузочных. Ко второй половине 1990-х годов в связи с повсеместным использованием 32-разрядных версий Windows загрузочные вирусы временно потеряли свою актуальность. Однако в 2007 г. появилась новая разновидность вредоносных программ - буткиты, использующие те же технологии заражения дисков, что и загрузочные вирусы

Файловые вирусы – компьютерный вирус, который для своего размножения использует файловую систему, внедряясь в исполняемые файлы практически любой ОС.



Объектом вирусного поражения могут выступать исполняемые двоичные файлы (EXE, COM), файлы динамических библиотек (DLL), драйверы (SYS), командные файлы (BAT, CMD) и другие.

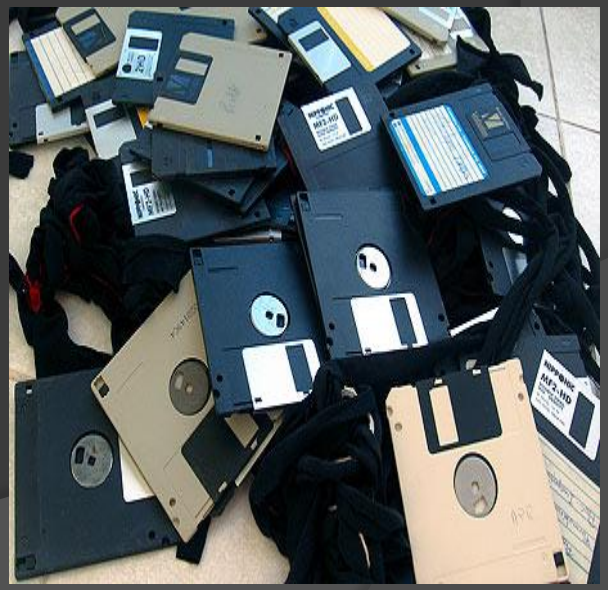
- Заражая файл, вирус может внедриться в его начало, конец или середину. Наиболее распространенным способом заражения COM-программ для MS-DOS является внедрение в конец файла. При этом основной код дописывается в конец файла, а в его начало записывается команда перехода к телу вируса.
- Для вирусов, заражающих PE-программы для Windows, характерно размещение тела вируса либо в дополнительной секции, либо в пустых «хвостах» секций, либо в неиспользуемом пространстве между заголовком и секциями. Общая длина файла при этом может оставаться прежней. Похожими приемами пользуются и немногочисленные файловые вирусы, заражающие программы для операционных систем семейства UNIX (например, ELF-программы для Linux).
- Чтобы скрыть своё присутствие в системе, файловый вирус может предварительно сохранить дату и время последней модификации и значения атрибутов заражаемого файла, восстановив эти данные уже после заражения.

- **Файлово-загрузочный вирус** — комбинация файлового и загрузочного вируса.
- **Пояснение**
- Файлово-загрузочный вирус прикрепляется к загрузочной записи диска или дискет, а также к программным файлам. Вирус этого типа активизируется после загрузки компьютера с зараженного диска (дискеты) или при запуске зараженного файла.
- Файлово-загрузочные вирусы могут распространяться как файловые, прикрепляясь затем к загрузочным записям дисков и дискет. Они также способны распространяться через загрузочные записи дискет, заражая затем файлы.
- Этот факт двойственного поведения и отражен в названии данного типа вирусов.

История компьютерной вирусологии

История компьютерной вирусологии представляется сегодня постоянной «гонкой за лидером», причем, несмотря на век» мощь современных антивирусных программ, лидерами являются именно вирусы. Среди тысяч вирусов лишь несколько десятков являются оригинальными разработками, использующими действительно принципиально новые идеи. Все остальные — «вариации на тему». Но каждая оригинальная разработка заставляет создателей антивирусов приспосабливаться к новым условиям, догонять вирусную технологию. Последнее можно оспорить.

Например, в 1989 году американский студент сумел создать вирус, который вывел из строя около 6000 компьютеров Министерства обороны США. Или эпидемия известного вируса Dir-II, разразившаяся в 1991 году. Вирус использовал оригинальную, принципиально новую технологию и на первых порах сумел широко распространиться за счет несовершенства традиционных антивирусных средств.



- Или всплеск компьютерных вирусов в Великобритании (Кристоферу Пайну удалось создать вирусы Pathogen и Queeq, а также вирус Smeg). Вирус Smeg был самым опасным, его можно было накладывать на первые два вируса, и из-за этого после каждого прогона программы они меняли конфигурацию. Поэтому их было невозможно уничтожить. Чтобы распространить вирусы, Пайн скопировал компьютерные игры и программы, заразил их, а затем отправил обратно в сеть. Пользователи загружали в свои компьютеры зараженные программы и инфицировали диски. Ситуация усугубилась тем, что Пайн умудрился занести вирусы и в программу, которая с ними борется. Запустив ее, пользователи вместо уничтожения вирусов получали еще один, В результате этого были уничтожены файлы множества фирм, убытки составили миллионы фунтов стерлингов.
- Широкую известность получил американский программист Моррис. Его знают как создателя вируса, который в ноябре 1988 года заразил порядка 7 тысяч персональных компьютеров, подключенных к Internet.
- Причины появления и распространения компьютерных вирусов, с одной стороны, скрываются в психологии человеческой личности и ее теневых сторонах (зависти, мести, тщеславии непризнанных таордов, невозможности конструктивно применить свои способности), с другой стороны, обусловлены отсутствием аппаратных средств защиты и противодействия со стороны операционной системы персонального компьютера

ПУТИ ПРОНИКНОВЕНИЯ ВИРУСОВ В КОМПЬЮТЕР

Основными путями проникновения вирусов в компьютер являются съемные диски (гибкие и лазерные), а также компьютерные сети. Заражение жесткого диска вирусами может произойти при загрузке программы с дискеты, содержащей вирус. Такое заражение может быть и случайным, например, если дискету не вынули из дисковода Л и перезагрузили компьютер, при этом дискета может быть к не системной. Заразить дискету гораздо проще. На нее Вирус может попасть, даже если дискету просто вставили в дисковод зараженного компьютера и, например, прочитали ее оглавление.

- Вирус, как правило, внедряется в рабочую программу таким образом, чтобы при ее запуске управление сначала передалось ему и только после выполнения все> ?го команд снова вернулось к рабочей программе. Получив доступ к управлению, вирус прежде всего переписывает сам себя в другую рабочую программу и заражает ее. После запуска программы, содержащей вирус, стэнозится возможным заражение других файлов. Наиболее часто вирусом заражаются загрузочный сектор диска и исполняемые файлы, имеющие расширения EXK, COM, SYS, BAT. Крайне редко заражаются текстовые файлы.
- После заражения программы вирус может выполнить какую-нибудь диверсию (не слишком серьезную, чтобы не привлечь вниманий). И не забывает возвратить управление той программе, из которой был запущен. Каждое выполнение зараженной программы переносит вирус в следующую. Таким образом заразится асе программное обеспечение.

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 успешно функционировавших 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 отметить, что вышеперечисленные явления необязательно вызываются присутствием вируса, а могут быть следствием других причин, Поэтому всегда затруднена правильная диагностика состояния компьютера,
- Как обнаружить вирус
- Как правило, вирусы обнаруживают обычные пользователи, которые замечают те или иные аномалии в поведении компьютера. Они в большинстве случаев не способны самостоятельно справиться с вирусом, но этого от них и не требуется.
- Необходимо обратиться к специалистам. Профессионалы изучат вирус, выяснят, «что он делает», «как он делает», «когда он делает» и пр. В процессе такой работы собирается вся необходимая информация о данном вирусе, в частности, выделяется сигнатура вируса (последовательность байтов, которая его характеризует). Для построения сигнатуры обычно берутся наиболее важные и характерные участки кода вируса. Одновременно становятся ясны механизмы работы вируса. Например, в случае загрузочного вируса важно знать, где он прячет свой хвост, где находится оригинальный загрузочный сектор, а в случае файлового — способ заражения файла. Полученная информация позволяет выяснить, как обнаружить вирус. Для этого уточняются методы поиска сигнатур в потенциальных объектах вирусной атаки (файлах и/или загрузочных секторах). Также необходимо определить, как обезвредить вирус, если это возможно, разрабатываются алгоритмы удаления вирусного кода из пораженных объектов,

ОБНАРУЖЕНИЕ, ЗАЩИТА И ПРОФИЛАКТИКА

Программы обнаружения и защиты от вирусов

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 сигнатуры в оперативной памяти и в файлах и при обнаружении выдают соответствующее сообщение. Недостатком таких антивирусных программ является то, что они могут находить только те вирусы, которые известны разработчикам таких программ.

Программы-доктора, или фаги, а также программы-вакцины 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. Среди фагов выделяют полифаги, предназначенные для поиска и уничтожения большого количества вирусов. Наиболее известные из них:

Kaspcrsky Antivirus, Norton AntiVirus, DoctorWeb.

Учитывая, что постоянно появляются новые вирусы, программы-детекторы и программы-доктора быстро устаревают и требуется регулярное обновление версий.

- **Программы-ревизоры** относятся к самым надежный 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 и другие параметры. Программы-ревизоры имеют достаточно развитые алгоритмы, обнаруживают стелс-вирусы и могут даже очистить изменения версии проверяемой программы от изменений, внесенных вирусом. К числу программ-ревизоров относится широко распространенная и России программа Kaspersky Monitor.

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, EXE;

— изменение атрибутов файла;

— прямая запись на диск по абсолютному адресу;

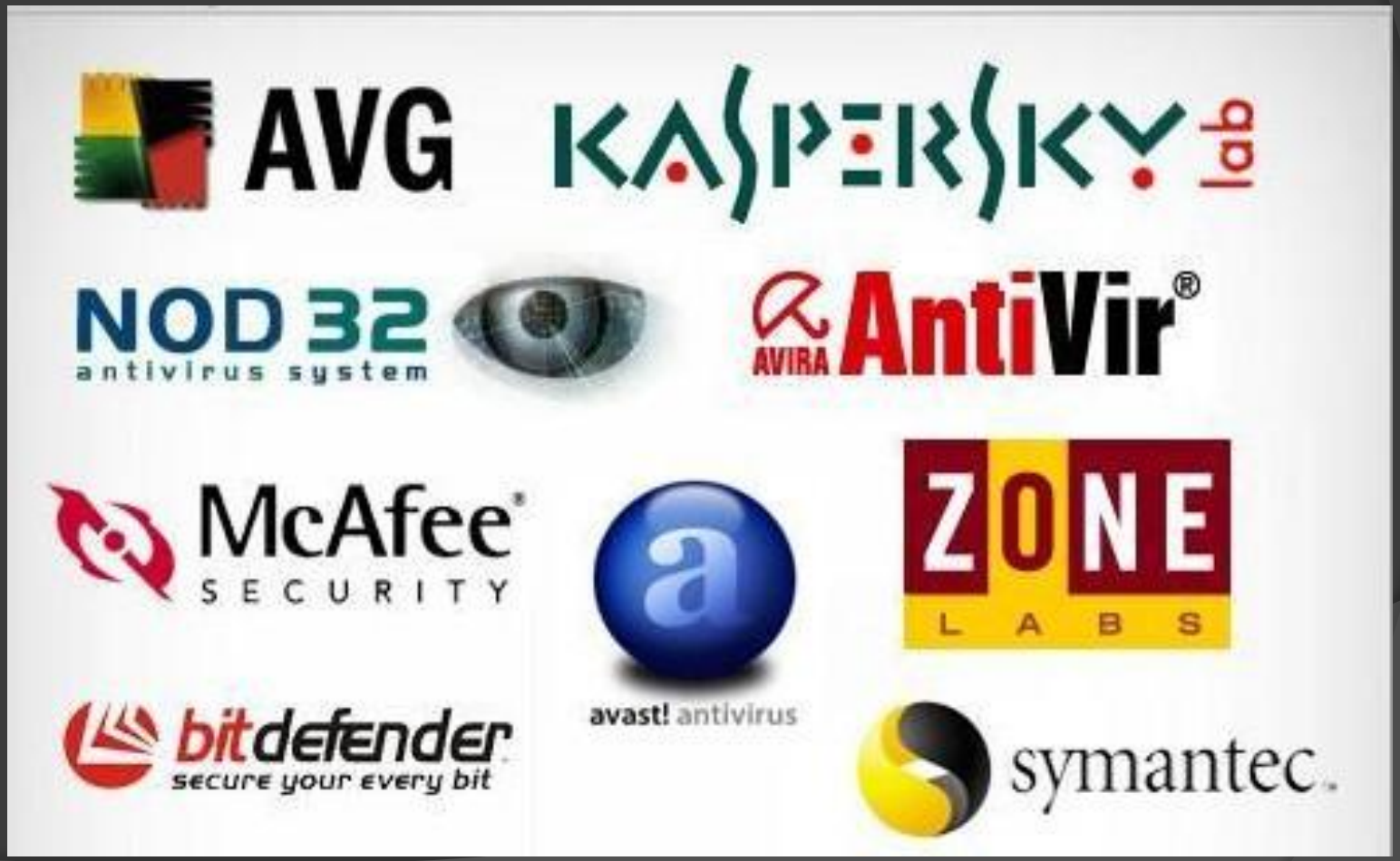
— запись и загрузочные сектора диска;

— загрузка резидентной программы.

Вакцины (иммунизаторы) - это резидентные программы, предотвращающие заражение файлов. Вакцины применяют, если отсутствуют программы-доктора, уничтожающие этот вирус. Вакцинация возможна только от известных вирусов. Вакцина модифицирует программу или диск таким образом, чтобы это не отражалось на их работе, а вирус будет воспринимать их зараженными и поэтому не внедрится. В настоящее время программы-вакцины имеют ограниченное применение.

Своевременное обнаружение зараженных вирусами файлов и дисков, полное уничтожение обнаруженных вирусов на каждом компьютере позволяют избежать распространения вирусной эпидемии на другие компьютеры.

Основным средством борьбы с вирусами были и остаются антивирусные программы



Для того чтобы не подвергнуть компьютер заражению вирусами и обеспечить надежное хранение информации на дисках, необходимо соблюдать следующие правила:

- оснастите свой компьютер современными антивирусными программами, например Kaspersky Antivirus, и постоянно обновляйте их вирусные базы;
- перед считыванием с дискет информации, записано на других компьютерах, всегда проверяйте эти дискеты на наличие вирусов, запуская антивирусные программы своего компьютера;
- при переносе на свой компьютер файлов в архивированном виде проверяйте их сразу же после разархивации на жестком диске, ограничивая область проверки только вновь записанными файлами;
- периодически проверяйте на наличие вирусов жесткие диски компьютера, запуская антивирусные программы для тестирования файлов, памяти и системных областей дисков с защищенной от записи дискеты, предварительно загрузив операционную систему с защищенной от записи системной дискеты;
- всегда защищайте свои дискеты от записи при работе на других компьютерах, если на них не будет производится запись информации;
- обязательно делайте архивные копии на дискетах ценной для вас информации;
- не оставляйте в кармане дисковода А дискеты при включении или перезагрузке операционной системы, чтобы исключить заражение компьютера загрузочными вирусами;
- используйте антивирусные программы для входного контроля всех исполняемых файлов, получаемых из компьютерных сетей;
- для обеспечения большей безопасности применения антивируса необходимо сочетать с повседневным использованием ревизора диска.

Использование литературы

- ***Касперский Е.*** Компьютерные вирусы 1992
- ***Климентьев К.Е.*** Компьютерные вирусы и антивирусы: взгляд программиста.
  ДМК-Пресс 2013