Компьютерные вирусы
Антивирусные программы

ВВЕДЕНИЕ

- Одна из самых неприятных вещей, с которой сталкивается каждый начинающий пользователь ПК, это **компьютерные вирусы**. Что же это такое? На самом деле под этим названием скрывается несколько видов вредоносных программ, каждая из которых уже давно имеет свою своеобразную методику проникновения в компьютер. На сегодня известно около 50 тысяч компьютерных вирусов. Эти маленькие вредоносные программы живут по трём правилам – Размножаться, Скрываться и Портить. Универсального и абсолютно надёжного средства борьбы с вирусами не существует.

ЧТО ТАКОЕ КОМПЬЮТЕРНЫЙ ВИРУС?

- **Компьютерный вирус** — вид вредоносного программного обеспечения, способного создавать копии самого себя и внедряться в код других программ, системные области памяти, загрузочные секторы, а также распространять свои копии по разнообразным каналам связи.

ИСТОРИЯ ВОЗНИКНОВЕНИЯ ВИРУСОВ

- Первый известный компьютерный вирус был написан в 1982 году 15-ти летним Ричом Скрентой. Этот вирус был назван Elk Clone. Он инфицировал другие компьютеры с помощью дискеты и при каждой 50-ой загрузке на экран выводился стишок:

It will get on all your disks Он придет на все ваши диски
It will infiltrate your chips Он инфицирует все
Ваши чип

Yes, it's Cloner! Да, это Cloner!

It will stick to you like glue Он прилипнет к Вам,
как клей

It will modify RAM too Он также модифицирует
RAM

Send in the Cloner! Отправляйте Cloner!

- Следующий известный компьютерный вирус был вирус под названием Brain (мозг). Этот вирус был создан двумя братьями из Пакистана Баситом и Амджадом Фарук Алви в 1986 году. Вирус вышел за границы Пакистана и заразил большое количество компьютеров по всему миру.

ПРИЗНАКИ ПОЯВЛЕНИЯ ВИРУСОВ

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

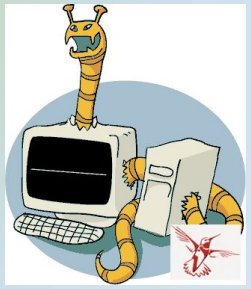
- - прекращение работы или неправильная работа ранее успешно функционирующих программ,
- - медленная работа компьютера,
- - невозможность загрузки операционной системы,
- - исчезновение файлов и каталогов или искажение их содержимого,
- - изменение даты и времени модификации файлов,
- - изменение размеров 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.

КЛАССИФИКАЦИЯ КОМПЬЮТЕРНЫХ ВИРУСОВ

- По среде обитания
- По алгоритмам работы
- По деструктивным,

  то есть разрушительным возможностям
- По способу заражения






КЛАССИФИКАЦИЯ ПО СРЕДЕ ОБИТАНИЯ

КЛАССИФИКАЦИЯ ПО АЛГОРИТМАМ РАБОТЫ

- **Вирусы спутники(companion)** - эти вирусы поражают EXE-файлы путем создания COM-файла двойника, и по этому при запуске программы запустится сначала COM-файл с вирусом, после выполнения своей работы вирус запустит EXE-файл. При таком способе заражения "инфицированная" программа не изменяется.
- **Вирусы "черви" (Worms)**- вирусы, которые распространяются в компьютерных сетях. Они проникают в память компьютера из компьютерной сети, вычисляют адреса других компьютеров и пересылают на эти адреса свои копии. Иногда они оставляют временные файлы на компьютере но некоторые могут и не затрагивать ресурсы компьютера за исключением оперативной памяти и разумеется процессора.
- **"Паразитические"** - все вирусы, которые модифицируют содержимое файлов или секторов на диске. К этой категории относятся все вирусы не являются вирусами-спутниками и вирусами червями.
- **"Стелс-вирусы" (вирусы-невидимки, stealth)**- представляющие собой весьма совершенные программы, которые перехватывают обращения DOS к пораженным файлам или секторам дисков и подставляют вместо себя незараженные участки информации. Кроме этого, такие вирусы при обращении к файлам используют достаточно оригинальные алгоритмы, позволяющие "обманывать" резидентные антивирусные мониторы.
- **"Полиморфные" (самошифрующиеся или вирусы-призраки, polymorphic)** - вирусы достаточно трудно обнаруживаемые, не имеющие сигнатур, т.е. не содержащие ни одного постоянного участка кода. В большинстве случаев два образца одного и того же полиморфного вируса не будут иметь ни одного совпадения. Это достигается шифрованием основного тела вируса и модификациями программы-расшифровщика.

КЛАССИФИКАЦИЯ ПО ДЕСТРУКТИВНЫМ ВОЗМОЖНОСТЯМ

1.Безвредные
Вирусы, никак не влияющие на работу компьютера за исключением, быть может, уменьшения свободного места на диске и объема оперативной памяти.

2.Неопасные
Вирусы, которые проявляют себя в выводе различных графических, звуковых эффектов и прочих безвредных действий.

3.Опасные
Вирусы, которые могут привести к различным сбоям в работе компьютеров, а также их систем и сетей.

4.Очень опасные
Вирусы, приводящие к потере, уничтожению информации, потере работоспособности программ и системы в целом.

КЛАССИФИКАЦИЯ ПО СПОСОБУ ЗАРАЖЕНИЯ

1.Резидентные

Вирусы, которые при инфицировании компьютера оставляют свою резидентную часть в памяти. Они могут перехватывать прерывания операционной системы, а также обращения к инфицированным файлам со стороны программ и операционной системы. Эти вирусы могут оставаться активными в плоть до выключения или перезагрузки компьютера.

2.Нерезидентные

Вирусы не оставляющие своих резидентных частей в оперативной памяти компьютера. Некоторые вирусы оставляют в памяти некоторые свои фрагменты не способные к дальнейшему размножению такие вирусы считаются не резидентными.

ПУТИ ПРОНИКНОВЕНИЯ В КОМПЬЮТЕР

- **Глобальная сеть Internet**
- **Электронная почта**
- **Локальная сеть**
- **Компьютеры «Общего назначения»**
- **Пиратское программное обеспечение**
- **Ремонтные службы**
- **Съемные накопители, на которых находятся заражённые вирусом файлы**
- **Жёсткий диск, на который попал вирус**
- **Вирус, оставшийся в оперативной памяти после предшествующего пользователя**

ОСНОВНЫЕ МЕРЫ ПО ЗАЩИТЕ ОТ ВИРУСОВ

Для того, чтобы не подвергнуть компьютер заражению вирусами, необходимо соблюдать следующие правила:

- оснастите свой компьютер современными антивирусными программами и постоянно возобновляйте их версии
- перед считыванием с дискет информации 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
- периодически проверяйте на наличие вирусов, жесткие диски компьютера, запуская антивирусные программы для тестирования файлов, памяти и системных областей дисков с защищенной от записи дискеты
- обязательно делайте архивные копии на дискетах ценной для вас информации
- не оставлять Flesh-карту в USB-порту при выключении или перезагрузке операционной системы, чтобы исключить заражение компьютера загрузочными вирусами
- используйте антивирусные программы для входного контроля всех исполняемых файлов, получаемых из компьютерных сетей

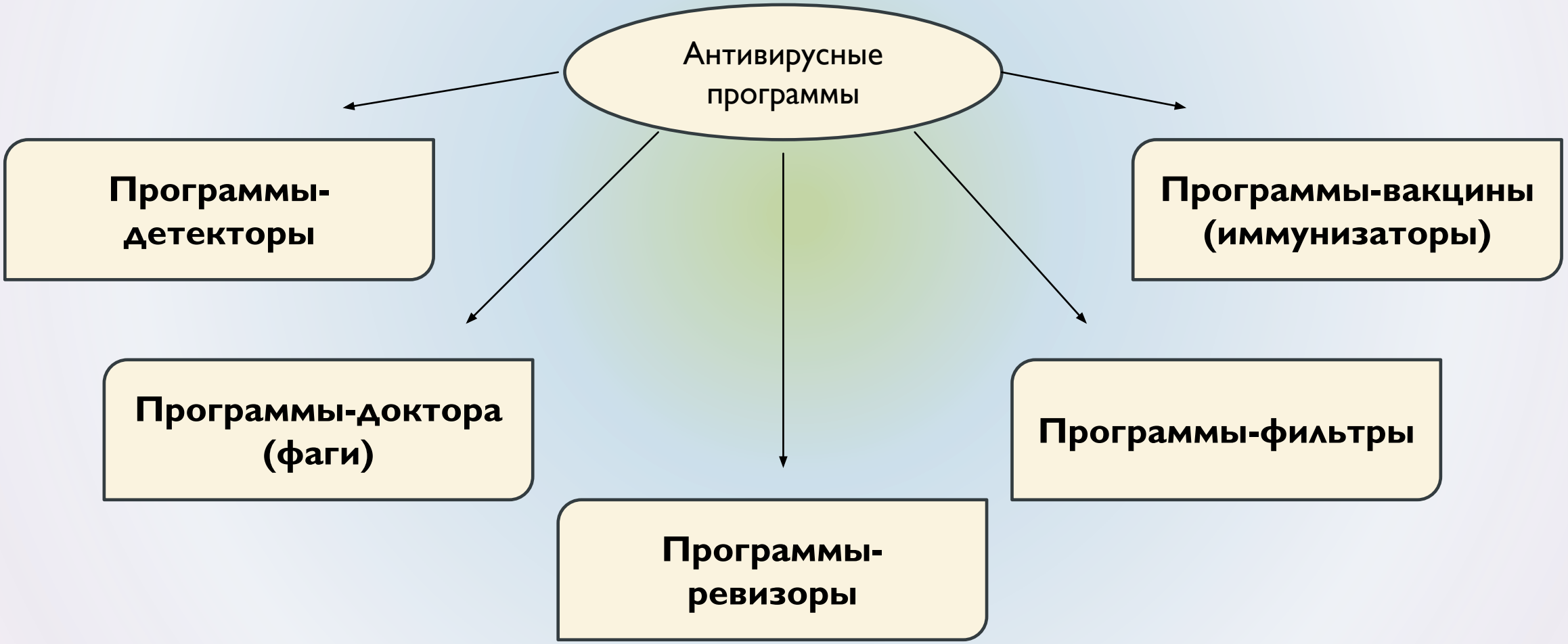
АНТИВИРУСНЫЕ ПРОГРАММЫ

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*

ВИДЫ АНТИВИРУСНЫХ ПРОГРАММ



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(ФАГИ)

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, т.е. программы-доктора, предназначенные для поиска и уничтожения большого количества вирусов. Наиболее известны из них: Scan, Norton, Antivirus, Doctor Web. Учитывая, что постоянно появляются новые вирусы, программы-детекторы и программы-доктора быстро устаревают, и требуется регулярное обновление версий.

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 очистить изменения версии проверяемой программы от изменений, внесенных вирусом.

ПРОГРАММЫ-ФИЛЬТРЫ

Представляют собой небольшие резидентные программы, предназначенные для обнаружения подозрительных действий при работе компьютера, характерных для вирусов. Такими действиями могут являться:

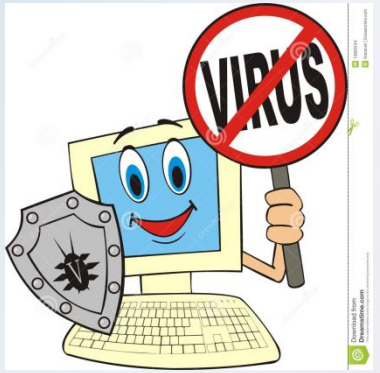
- *попытки коррекции файлов с расширениями .COM, .EXE,*
- *изменение атрибутов файла,*
- *прямая запись на диск по абсолютному адресу,*
- *запись в загрузочные сектора диска,*
- *загрузка резидентной программы.*

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.

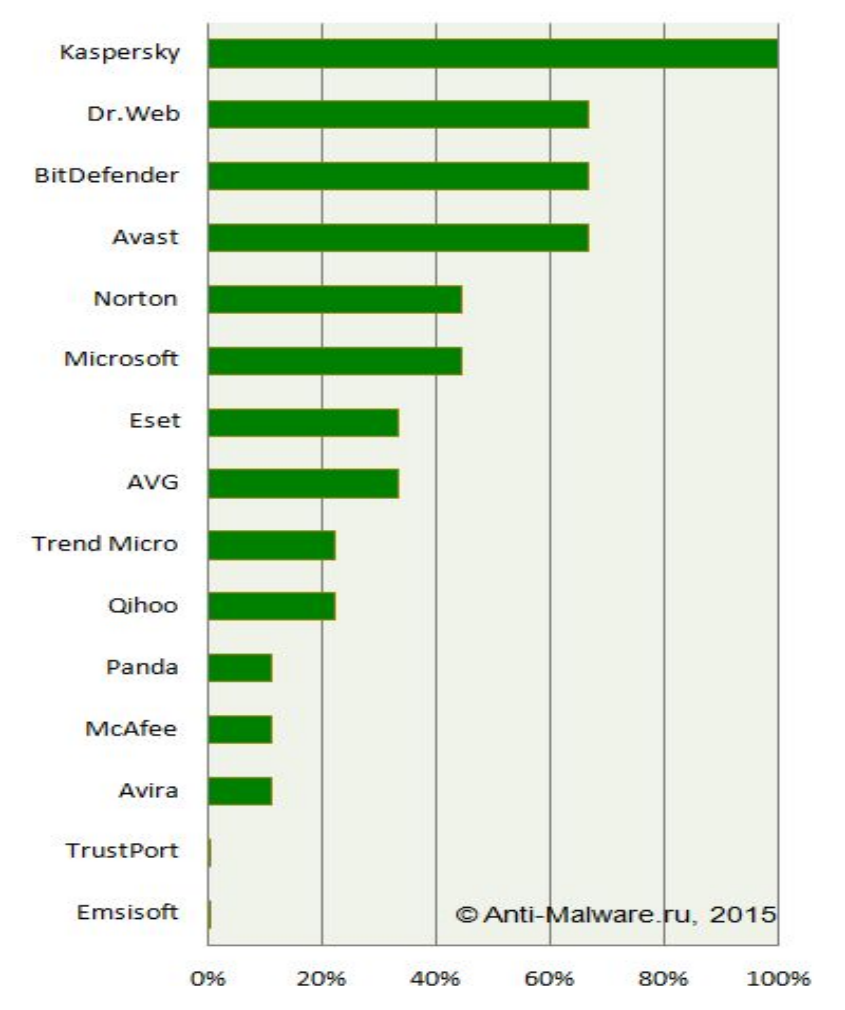
ПРОГРАММЫ-ВАКЦИНЫ

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, 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.



КТО ЖЕ ЛИДЕР СРЕДИ АНТИВИРУСНЫХ ПРОГРАММ?

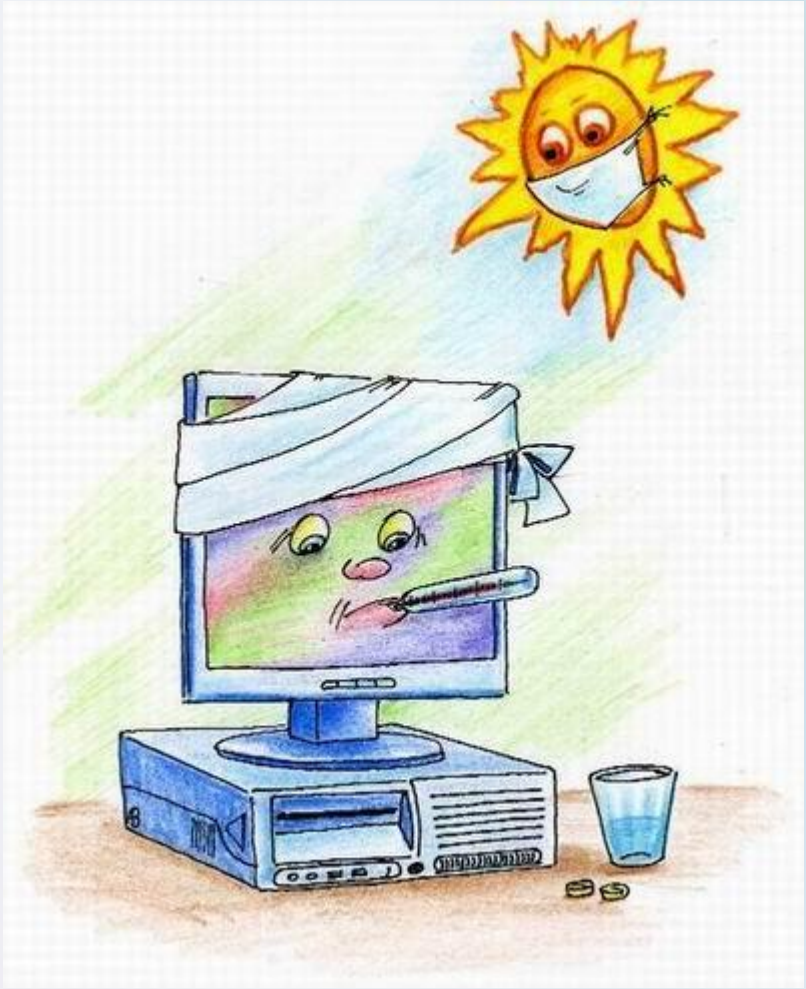


- Kaspersky Internet Security 2015 – безоговорочный лидер среди антивирусных программ по итогам 2015 года. Известный всем и каждому антивирус. Основная причина, по которой он стал лидером – это лучшая система своевременного и качественного лечения файлов от вирусов.
- Bitdefender Internet Security 2015 – лидер среди антивирусного программного обеспечения по итогам прошлых лет. Он является средством комплексной защиты, своеобразным «комбайном» в котором сочетаются файрвол, усиленная защита данных, антивирус и антишпион.

ЗАКЛЮЧЕНИЕ

Ни один тип антивирусных программ по отдельности не дает полной защиты от вирусов. Хочется сразу заметить, что слишком уж бояться вирусов не стоит, особенно если компьютер приобретен совсем недавно, и много информации на жестком диске еще не накопилось. Вирус компьютер не взорвет. Ныне известен только один вирус (*Win95.CIH*), который способен испортить "железо" компьютера. Другие же могут лишь уничтожить информацию, не более того. Из всего вышесказанного можно смело сделать вывод, что необходимость защиты от компьютерных вирусов на данный момент стоит на первом месте.

Для предотвращения заражения вирусом и соответственно всех его последствий необходимо правильно выбрать и установить в систему антивирусное программное обеспечение и соблюдать элементарные меры предосторожности.



Спасибо за внимание!