

A person wearing a full-body green protective suit and a clear face shield, standing against a blue background. The person's hands are raised, and they appear to be in a protective or safety-oriented environment. The text is overlaid on this image.

**Компьютерные  
вирусы  
и  
антивирусные  
программы**



**КОМПЬЮТЕРНЫЙ ВИРУС** –  
специально созданная небольшая  
программа, способная к  
саморазмножению, засорению  
компьютера и выполнению других  
нежелательных действий.

Первая эпидемия была вызвана вирусом **Brain** (от англ. «мозг») (также известен как **Пакистанский вирус**), который был разработан братьями Амджатом и Базитом Алви в **1986 г.** и был обнаружен летом **1987 г.**

Вирус заразил только в США более 18 тысяч компьютеров.

Программа должна была наказать местных пиратов, ворующих программное обеспечение у их фирмы. В программке значились имена, адрес и телефоны братьев.

Однако неожиданно для всех The Brain вышел за границы Пакистана и заразил сотни компьютеров по всему миру.



# Признаки заражения



# По способу заражения вирусы делятся на:

- **Резидентные вирусы** при заражении компьютера оставляют 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**, 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.



- общее замедление работы компьютера и уменьшение размера свободной оперативной памяти;
- некоторые программы перестают работать или появляются различные ошибки в программах;
- на экран выводятся посторонние символы и сообщения, появляются различные звуковые и видеоэффекты;
- размер некоторых исполнимых файлов и время их создания изменяются;
- некоторые файлы и диски оказываются испорченными;
- компьютер перестает загружаться с жесткого диска.

# Классификация компьютерных вирусов





# Типы вредоносных программ



- *Компьютерные вирусы*
- *Сетевые черви*
- *Троянские программы*
- *Программы показа рекламы*
- *Хакерские утилиты*

- В настоящее время известно более 5000 программных вирусов, их можно классифицировать по следующим признакам:
  - 1) среде обитания
  - 2) способу заражения среды обитания
  - 3) воздействию
  - 4) особенностям алгоритма



# ПО СРЕДЕ ОБИТАНИЯ

```
graph TD; A[ПО СРЕДЕ ОБИТАНИЯ] --> B[файловые]; A --> C[сетевые]; A --> D[макровирусы];
```

**файловые**

**сетевые**

**макровирусы**

# Файловые вирусы

Внедряются в программы и активизируются при их запуске.

После запуска зараженной программы вирусы находятся в ОЗУ и могут заражать другие файлы до момента выключения ПК или перезагрузки операционной системы.



# Макровирусы

Заражают файлы документов.

После загрузки зараженного документа в соответствующее приложение макровирус постоянно присутствует в оперативной памяти и может заражать другие документы.

Угроза заражения прекращается только после закрытия приложения.





# Сетевые вирусы

Могут передавать по компьютерным сетям свой программный код и запускать его на ПК, подключенных к этой сети.

Заражение сетевым вирусом может произойти при работе с электронной почтой или при «путешествиях» по Всемирной сети.



# ЧЕРВЬ «I LOVE YOU»

Успешно атаковал десятки миллионов компьютеров Windows **в 2000 году**, когда был разослан в виде вложения в электронное сообщение.

В теме письма содержалась строка **«ILoveYou»**, а к письму был приложен скрипт **«LOVE-LETTER-FOR-YOU.TXT.vbs»**.

Расширение **«.vbs»** было по умолчанию скрыто, что и заставило ничего не подозревающих пользователей думать, что это был простой текстовый файл.

При открытии вложения червь рассылал копию самого себя всем контактам в адресной книге Windows, а также на адрес, указанный как адрес отправителя. Он также совершал ряд вредоносных изменений в системе пользователя.

Червь нанёс ущерб мировой экономике в размере **более 10 миллиардов долларов**, поразив **более 3 миллионов ПК по всему миру**, за что вошёл в Книгу рекордов Гиннеса, как самый разрушительный компьютерный вирус в мире.



# 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(черви)- распространяются по компьютерным сетям, вычисляют адреса сетевых компьютеров и записывают по этим адресам свои копии.



- **Вирусы-невидимки (стелс-вирусы)** - 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.
- **Вирусы-мутанты** - содержат алгоритмы шифровки-расшифровки, благодаря которым копии одного и того же вируса не имеют ни одной повторяющейся цепочки байтов.
- **Квазивирусные или «троянские» программы** - хотя они и не способны к самораспространению, но очень опасны, так как, маскируясь под полезную программу, разрушают загрузочный сектор и файловую систему дисков.

## 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.







# 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 обнаружить вирусы, которые ей "известны".



# Программы-ревизоры

- имеют две стадии работы. Сначала они запоминают сведения о состоянии 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.

# Программы-фильтры

- 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 (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.

A computer monitor and keyboard are shown, heavily secured with thick metal chains and padlocks. The chains are draped over the monitor and keyboard, with padlocks locking them in place. The background is a dark, textured blue. The text is overlaid in a bright yellow, bold, sans-serif font.

# Антивирусные программы



# Критерии выбора

- Надежность и удобство в работе
- Качество обнаружения вирусов
- Существование версий под все популярные платформы
- Скорость работы
- Наличие дополнительных функций и возможностей

# АНТИВИРУСНЫЕ ПРОГРАММЫ

```
graph TD; A[АНТИВИРУСНЫЕ ПРОГРАММЫ] --> B[СКАНЕРЫ]; A --> C[СТОРОЖА];
```

## СКАНЕРЫ

Используются для **периодической проверки ПК** на наличие вирусов.

После запуска проверяются файлы и оперативная память, в случае обнаружения вирусов обеспечивается их нейтрализация.

## СТОРОЖА

**Постоянно** находятся в оперативной памяти ПК.

Обеспечивают проверку файлов в процессе их загрузки в ОЗУ.

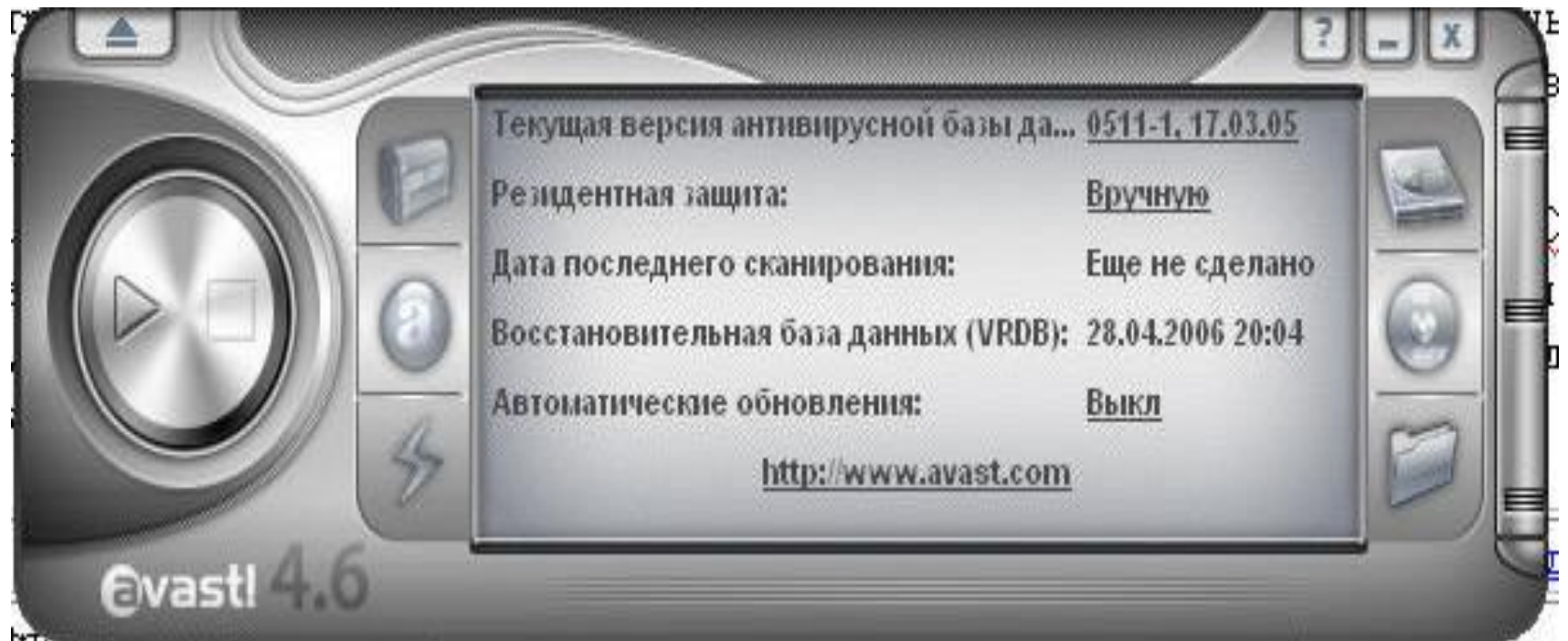
# Dr.Web



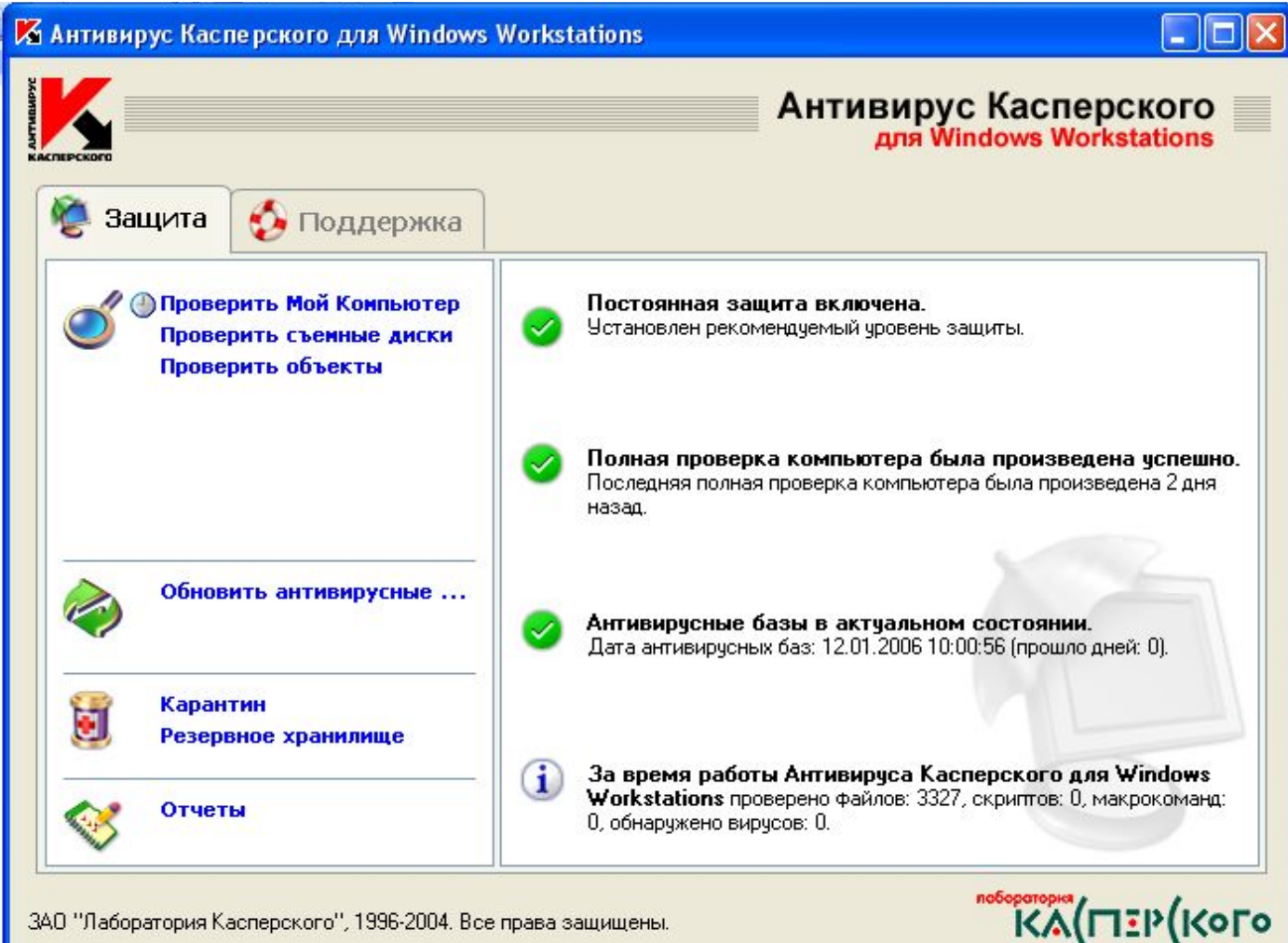
# ADinf32



# Avast



# Антивирус Касперского



Антивирус Касперского для Windows Workstations

Антивирус Касперского  
для Windows Workstations

Защита    Поддержка

Проверить Мой Компьютер  
Проверить съемные диски  
Проверить объекты

Обновить антивирусные ...

Карантин  
Резервное хранилище

Отчеты

Постоянная защита включена.  
Установлен рекомендуемый уровень защиты.

Полная проверка компьютера была произведена успешно.  
Последняя полная проверка компьютера была произведена 2 дня назад.

Антивирусные базы в актуальном состоянии.  
Дата антивирусных баз: 12.01.2006 10:00:56 (прошло дней: 0).

За время работы Антивируса Касперского для Windows Workstations проверено файлов: 3327, скриптов: 0, макрокоманд: 0, обнаружено вирусов: 0.

ЗАО "Лаборатория Касперского", 1996-2004. Все права защищены.

лаборатория  
КАСПЕР(КОГО)





# Правовая охрана программ и данных

# Документы Российской Федерации



- Конституция Российской Федерации ст. 44
- Гражданский Кодекс Российской Федерации
- Закон об авторском праве и смежных правах 1993г.
- **Закон Российской Федерации «О правовой охране программ для ЭВМ и баз данных» 1992г.**

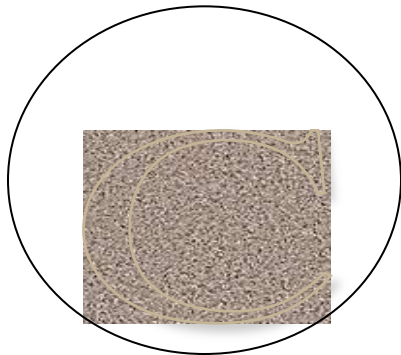


# Знак охраны авторского права

**Латинская буква С внутри круга**

Имя обладателя исключительных авторских  
прав

Дата первого опубликования



**Корпорация Microsoft, 1993-1997**

# **Выписка из Уголовного кодекса Российской Федерации**

## **Глава 28. Преступления в сфере компьютерной информации**

# Статья 272. Неправомерный доступ к компьютерной информации

Неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, - **наказывается**

- ❑ штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда
- ❑ или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев,
- ❑ либо исправительными работами на срок от шести месяцев до одного года,
- ❑ либо лишением свободы на срок до двух лет



# Статья 273. Создание, использование и распространение вредоносных программ для ЭВМ

Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, а равно использование либо распространение таких программ или машинных носителей с такими программами, - **наказываются**

- лишением свободы на срок до трех лет со штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда
- или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев.

**Те же деяния, повлекшие тяжкие последствия, наказываются лишением свободы на срок от трех до семи лет.**



# Статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети

Нарушение правил эксплуатации ЭВМ лицом, имеющим доступ к ЭВМ, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред, - **наказывается**

- лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет,
- либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов,
- либо ограничением свободы на срок до двух лет.