

Компьютерные вирусы и антивирусные программы



Ученик 10 класса «А»
Школа №30, г. Н. Новгород
Беспалов Алексей



Компьютерный вирус –
специально созданная небольшая
программа, способная к
саморазмножению, засорению
компьютера и выполнению других
нежелательных действий.

Происхождение вируса



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.

The Brain вышел за границы Пакистана и заразил сотни компьютеров по всему миру.

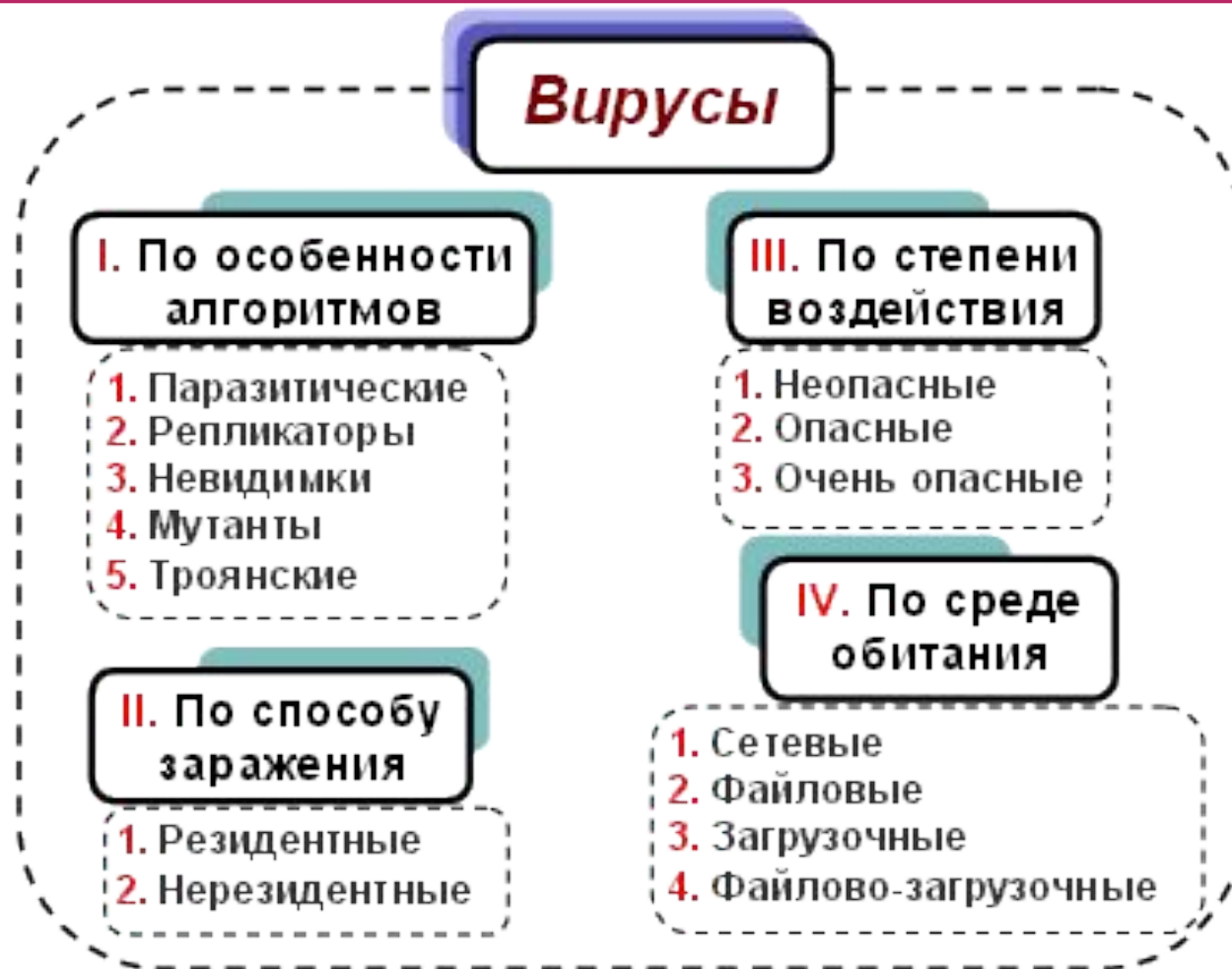
Признаки заражения

- 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 звуки и видеоэффекты;
- размер некоторых исполняемых файлов и время их создания изменяются;
- некоторые файлы и диски оказываются испорченными;
- компьютер перестает загружаться с жесткого диска.

Классификация компьютерных вирусов



Вирусы



По особенностям алгоритмов

- **Паразитические вирусы** и вирусы, заражающие загрузочные секторы, в высокой степени привязаны к определенной платформе. Паразитические вирусы могут присоединяться в начало, конец или в середине исполняемого файла.
- **Вирусы-репликаторы (Worm)** – вирусы, основная задача которых как можно быстрее размножится по всем возможным местам хранения данных и коммуникациям.
- **Вирус-невидимка** - файловый вирус, остающийся "невидимым" для антивирусных программ. При проверке системы вирус невидимка пытается перехватить запросы и выдать сигнализирующий ответ, что все в порядке.
- **Мутанты** – сложно обнаруживаемые вирусы вследствие применяемых алгоритмов шифрования и модификации.
- **Троянская программа** - вредоносная программа, распространяемая людьми, в отличие от **вирусов** и червей, которые распространяются самопроизвольно.

По способу заражения

- По способам заражения **вирусы** бывают **резидентные и нерезидентные**. **Резидентный вирус** при инфицировании компьютера оставляет в оперативной памяти свою **резидентную** часть, которая затем перехватывает обращение операционной системы к объектам заражения и внедряется в них.
- **Нерезидентные вирусы** не заражают память компьютера и являются активными ограниченное время.

По степени воздействия

- Неопасные - не мешают работе компьютера, но уменьшают объем памяти.
- Опасные - могут привести к различным нарушениям в работе компьютера.
- Очень опасные - уничтожают данные, стирают информацию в системных областях диска.

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

Передают по компьютерным сетям свой программный код и запускают его на ПК, подключенный к этой сети.

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



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.

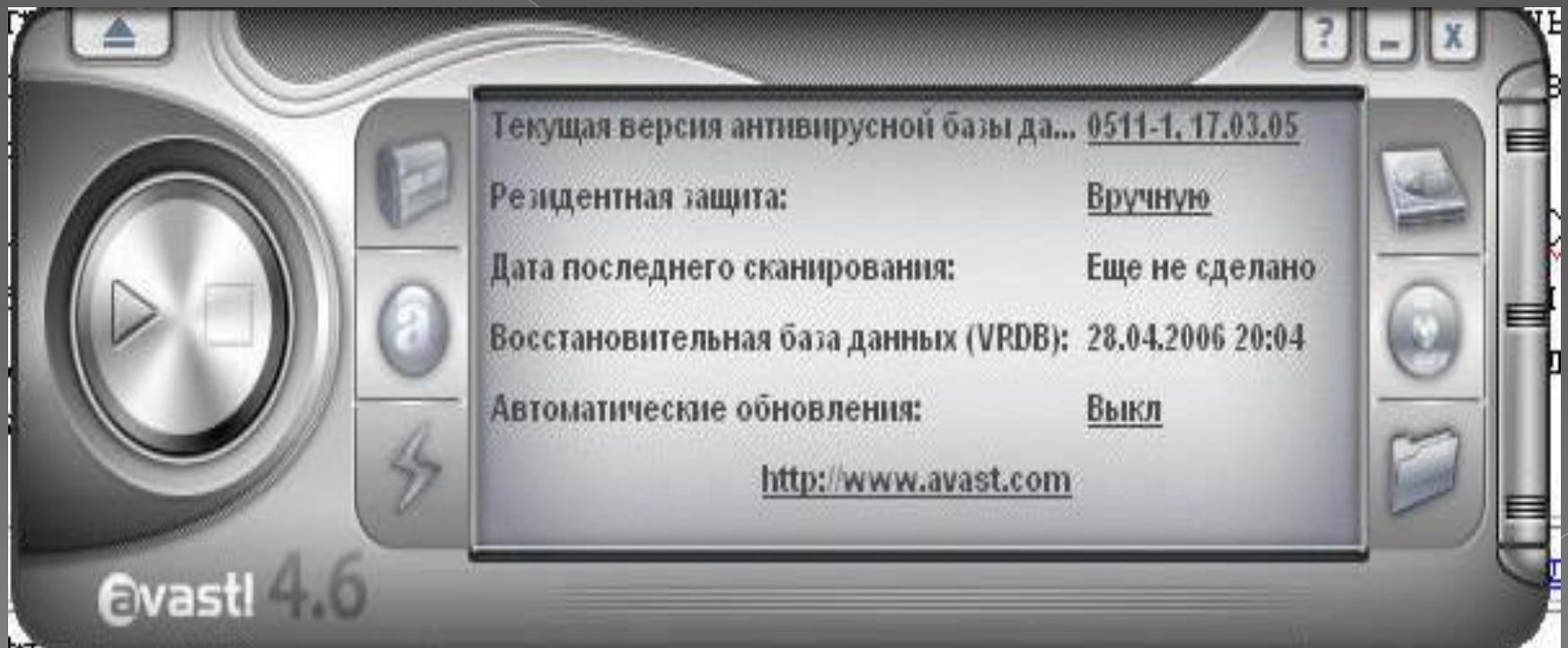
Dr.Web



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)

Заключение

- **Самым** страшным кошмаром любого пользователя сети Интернет являются компьютерные вирусы, которые постоянно совершенствуются. Вирусы попадают на компьютеры часто, причем иногда не сразу понятно, что же произошло с системой.
- **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.
- **Для** предотвращения заражения вирусом и соответственно всех его последствий необходимо правильно выбрать и установить в систему антивирусное программное обеспечение и соблюдать элементарные меры предосторожности.