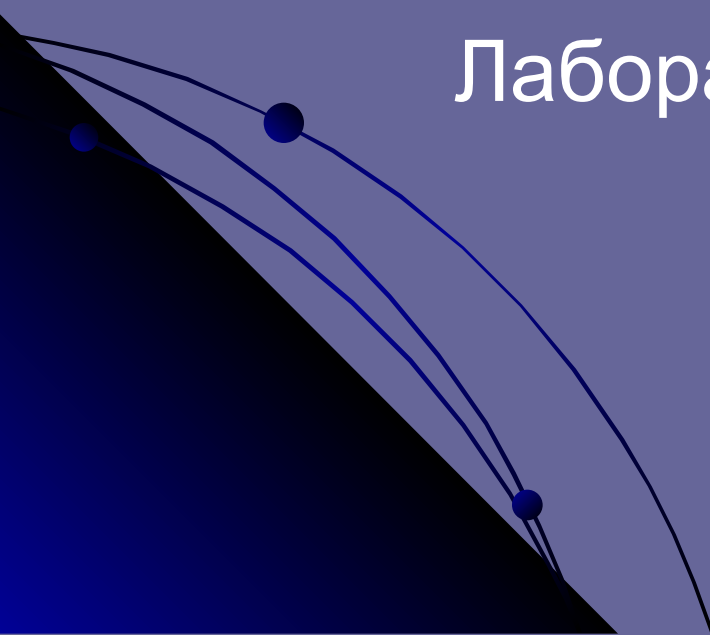


Компьютерные вирусы



Лаборатория прикладной
вирусологии



«Слаб и робок человек, слеп
умом и все тревожит...»

А.С. Пушкин

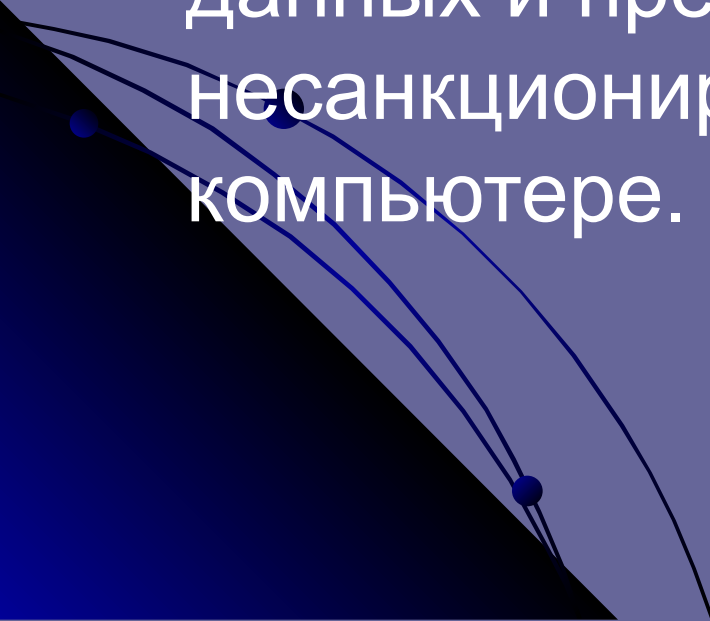
- Интернет подразумевает большую степень свободы, нежели «реал»: огромные залежи бесплатной музыки и графики, онлайн-библиотеки и «клондайки» программного обеспечения. А уж возможностей для мгновенного обогащения и того больше: послания вида «Как заработать 100000 за три часа и жениться на Шамаханской царице» знакомы всем владельцам электронных почтовых ящиков. Но почему-то мало кто задумывается над извечной проблемой «бесплатного сыра»...

- ...мозг превращается в бесформенную массу, отказываясь реагировать на любые раздражители. Господи, ну почему именно я? Почему?! Наверняка виной безобидное на первый взгляд письмо, принесенное расторопным почтальоном...
- Сегодня снова приходил доктор. Кажется его звали Нортон. Или Каспер? Впрочем, какая разница...Из-за неплотно закрытой двери было слышно, как врач деловито-будничным тоном произнес: «Это конец».

- Наделавшие много шума вирусные эпидемии прошлого года заставляют задуматься о
- том, каким же образом предприятия смогут защитить себя в будущем. При этом
- ведущие разработчики антивирусного программного обеспечения исходят из еще
- большего обострения ситуации. Так, в июле 2004 г. было обнаружено 1400
- вредоносных кодов, а в августе — 3300. Для сравнения еще в январе насчитывалось
- «всего лишь» 550 новых угроз.
- Многие предприятия уже инвестировали немалые средства в свои
- структуры обеспечения безопасности и установили антивирусное
- решение. Однако, по данным исследования Computer Economics, вирусы
- наносят все больший ущерб: в одном только 2003 г. последствия
- вирусных атак оцениваются в 12,5 млрд долларов. Это указывает на то,
- что инсталлированные пакеты не свободны от недостатков.

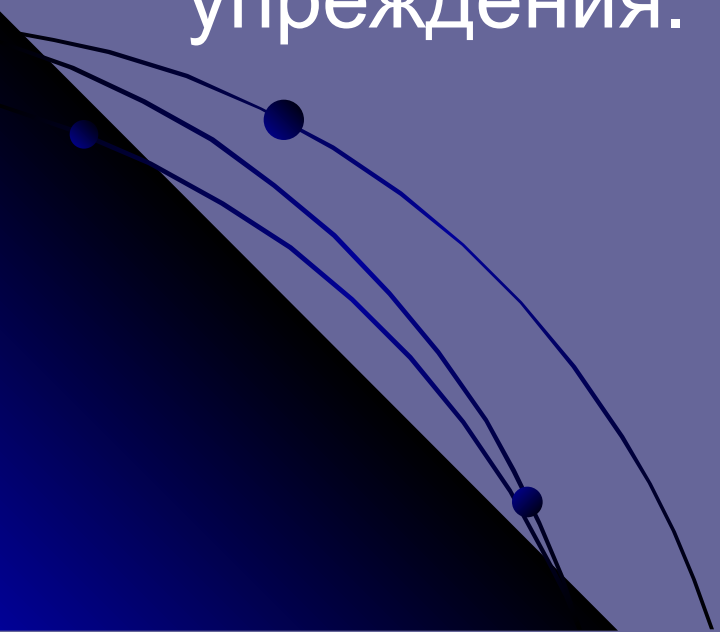
- По данным Computer Economics, в 2004 году сумма финансового ущерба компаний от
- деятельности вирусов и прочего вредоносного ПО приблизилась к отметке 18 млрд долл. В
- представленной статистике не учитываются убытки от спама и огромные суммы, украденные со
- счетов доверчивых пользователей с помощью фишинга. Как свидетельствует Computer
- Economics, наиболее разрушительным в прошлом году оказался MyDoom, разоривший
- пользователей более чем на 4,5 млрд долл. За ним следует Sasser, убытки от которого
- оцениваются примерно в 3,5 млрд долл. Чуть скромнее были Netsky и Bagle, причинившие ущерб
- в 2,7 млрд долл. и 1,5 млрд долл. соответственно.

Компьютерный вирус

- **Компьютерный вирус** – это программный код, встроенный в другую программу, или в документ, или в определенные области носителя данных и предназначенный для несанкционированных действий на компьютере.
- 

Найти и обезвредить.

- Как известно, лучшее лечение-профилактика. Но возбудителя болезни следует изучить и выбрать наиболее оптимальное для каждого средство упреждения.



Классификация не по Дарвину.

- Вирусы можно разделить на классы по следующим основным признакам:
- Среда обитания;
- Операционная система;
- Особенности алгоритма работы;
- Деструктивные возможности.



Среда обитания

- Файловые;
- Загрузочные;
- Макровирусы;
- Сетевые;.



Операционная система

- Каждый файловый или сетевой вирус заражает файлы какой либо одной или нескольких ОС: DOS, Windows, OS/2 и т.д.



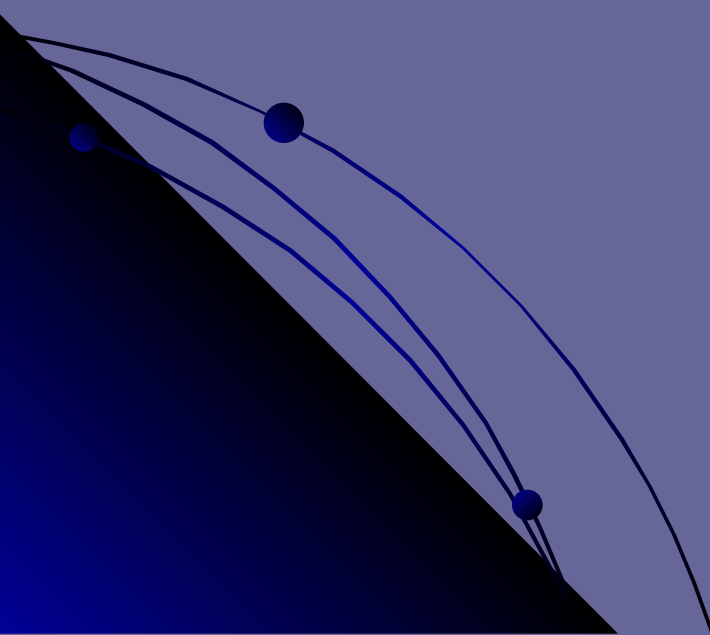
Особенности алгоритма работы

- Резидентность;
- Использование стелс-алгоритмов;
- Самошифрование и полиморфичность;
- Использование нестандартных приемов;

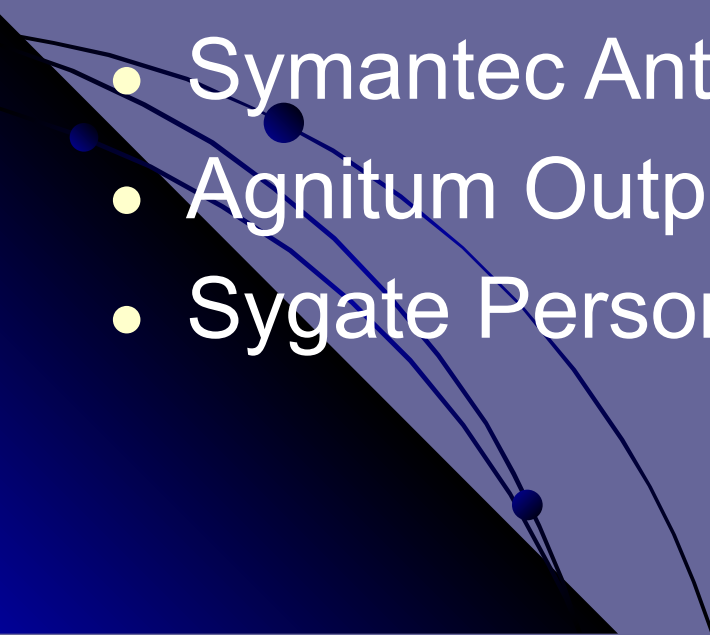


Деструктивные возможности

- Безвредные;
- Неопасные;
- Опасные;
- Очень опасные



Антивирусные программы

- Panda Antivirus Titanium (Platinum)
 - Norton Antivirus
 - Антивирус Касперского Personal
 - Dr. Web
 - Symantec Antivirus
 - Agnitum Outpost Firewall
 - Sygate Personal Firewall Pro
- 

Интерфейсы Антивирусных программ



Пример работы Антивирусной программы.

Dr.Web® Scanner for Windows 95-XP v4.32b

Файл Вид Настройки Язык Помощь

avast! - Предупреждение

Обнаружен троян!

Не беспокойтесь. Попытайтесь следовать нашим советам и ссылкам.

Имя файла: c:\windows\system32\srvany.exe
Имя вируса: Win32:Trojano-1512 [Trj] [Дополнительно...](#)
Тип вируса: Троян
Версия VPS: 0527-2, 08.07.2005

Возможные действия

[Переименовать...](#) [Удалить...](#) [В Хранилище](#)

Рекомендованное действие: Переместить в хранилище

Выполнить действия

[Продолжить](#) [Остановить](#) Не показывать в следующий раз

[Запланировать сканирование во время начальной загрузки...](#)

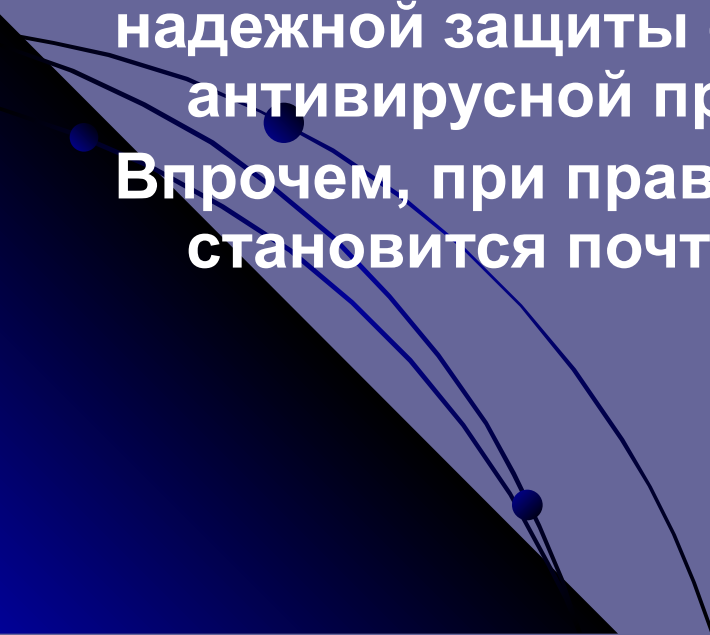
<http://www.avast.com> [Заполните сообщение о вирусе на нашем сайте, чтобы помочь нам улучшить avast!...](#) <http://www.avast.com/for>

NOD32
Antivirus System

Virus detected

Рецепты системного здоровья

- Установите антивирусную программу последней версии и обновите антивирусные базы по состоянию на текущий день. Регулярно проверяйте систему антивирусным сканером.
- Дополнительно к антивирусному пакету установите программу-брандмауэр.
- Никогда не открывайте файлы, прикрепленные к письму от незнакомого человека.
- Любой носитель информации, попавший к вам в руки, нужно сразу проверить антивирусной программой.
- Не заходите на сайты с подозрительной информацией, сайты сомнительного содержания и предложений.
- Незнакомые документы перед запуском переведите в RTF- формат: так вы избавитесь от макровирусов.

- **Антивирусные программы имеются на каждом компьютере и в каждой сети. За последние годы развитие методов сканирования продвинулось далеко вперед — но, к сожалению, изобретатели вирусов тоже. И сегодня все еще справедливо утверждение, что абсолютно надежной защиты с помощью совершенной антивирусной программы не существует. Впрочем, при правильном выборе эта цель все-таки становится почти достижимой.**
- 

Общие рекомендации

- **Важные критерии выбора антивирусного решения**
- • поддержка всех систем и платформ коллективной работы;
- • включение через AVAPI версия 2. 0 и выше (Exchange) или в качестве Server-Add-in-Task
- в процесс маршрутизации сообщений (Notes);
- • модульные/несколько механизмов сканирования;
- • поддержка как сканирования сигнатур, так и эвристического сканирования;
- • высокая степень распознавания (вирусов, троянских коней, «червей»);
- • тщательный поиск в архивах и сжатых файлах;
- • постоянная доступность службы поддержки (прозрачные расходы);
- • комфортное обслуживание.