

Всё о компьютерных вирусах

Анастасия Метелюк
190(3)

Компьютерный вирус

- ◆ Компьютерный вирус — разновидность компьютерных программ, отличительной особенностью которых является способность к размножению.



Компьютерный вирус

- ◆ **Компьютерный вирус** - специально написанная программа, способная самопроизвольно присоединяться к другим программам, создавать свои копии и внедрять их в файлы, системные области компьютера и в вычислительные сети с целью нарушения работы программ, порчи файлов и каталогов, создания всевозможных помех в работе компьютера. В настоящее время известно более 50000 программных вирусов, число которых непрерывно растет.

Основные источники вирусов

- ◆ дискета, на которой находятся зараженные вирусом файлы;
- ◆ компьютерная сеть, в том числе система электронной почты и Internet;
- ◆ жесткий диск, на который попал вирус в результате работы с зараженными программами;
- ◆ вирус, оставшийся в оперативной памяти после предшествующего пользователя.

Основные ранние признаки заражения компьютера вирусом:

- ◆ уменьшение объема свободной оперативной памяти;
- ◆ замедление загрузки и работы компьютера;
- ◆ непонятные (без причин) изменения в файлах, а также изменения размеров и даты последней модификации файлов;
- ◆ ошибки при загрузке операционной системы;
- ◆ невозможность сохранять файлы в нужных каталогах;
- ◆ непонятные системные сообщения, музыкальные и визуальные эффекты и т.д.

Признаки активной фазы вируса:

- ◆ исчезновение файлов;
- ◆ форматирование жесткого диска;
- ◆ невозможность загрузки файлов или операционной системы.



Виды вирусов

1) загрузочные вирусы или ВООТвирусы -заражают boot-секторы дисков. Очень опасные, могут привести к полной потере всей информации, хранящейся на диске;

2) **файловые вирусы заражают файлы.**

Делятся на:

- ◆ вирусы, заражающие программы (файлы с расширением .EXE и .COM);
- ◆ макровирусы вирусы, заражающие файлы данных, например, документы Word или рабочие книги Excel;
- ◆ вирусы-спутники используют имена других файлов;
- ◆ вирусы семейства DIR искажают системную информацию о файловых структурах;

Виды вирусов

- 3) **загрузочно-файловые вирусы** способны поражать как код boot-секторов, так и код файлов;
- 4) **вирусы-невидимки или STEALTH-вирусы** фальсифицируют информацию прочитанную из диска так, что программа, какой предназначена эта информация получает неверные данные. Эта технология, которую, иногда, так и называют Stealth-технологией, может использоваться как в BOOT-вирусах, так и в файловых вирусах;
- 5) **ретровирусы** заражают антивирусные программы, стараясь уничтожить их или сделать нетрудоспособными;

Виды вирусов

б) **вирусы-черви** снабжают небольшие сообщения электронной почты, так называемым заголовком, который по своей сути есть Web-адресом местонахождения самого вируса. При попытке прочитать такое сообщение вирус начинает считывать через глобальную сеть Internet свое 'тело' и после загрузки начинает деструктивное действие. Очень опасные, так как обнаружить их очень тяжело, в связи с тем, что зараженный файл фактически не содержит кода вируса.

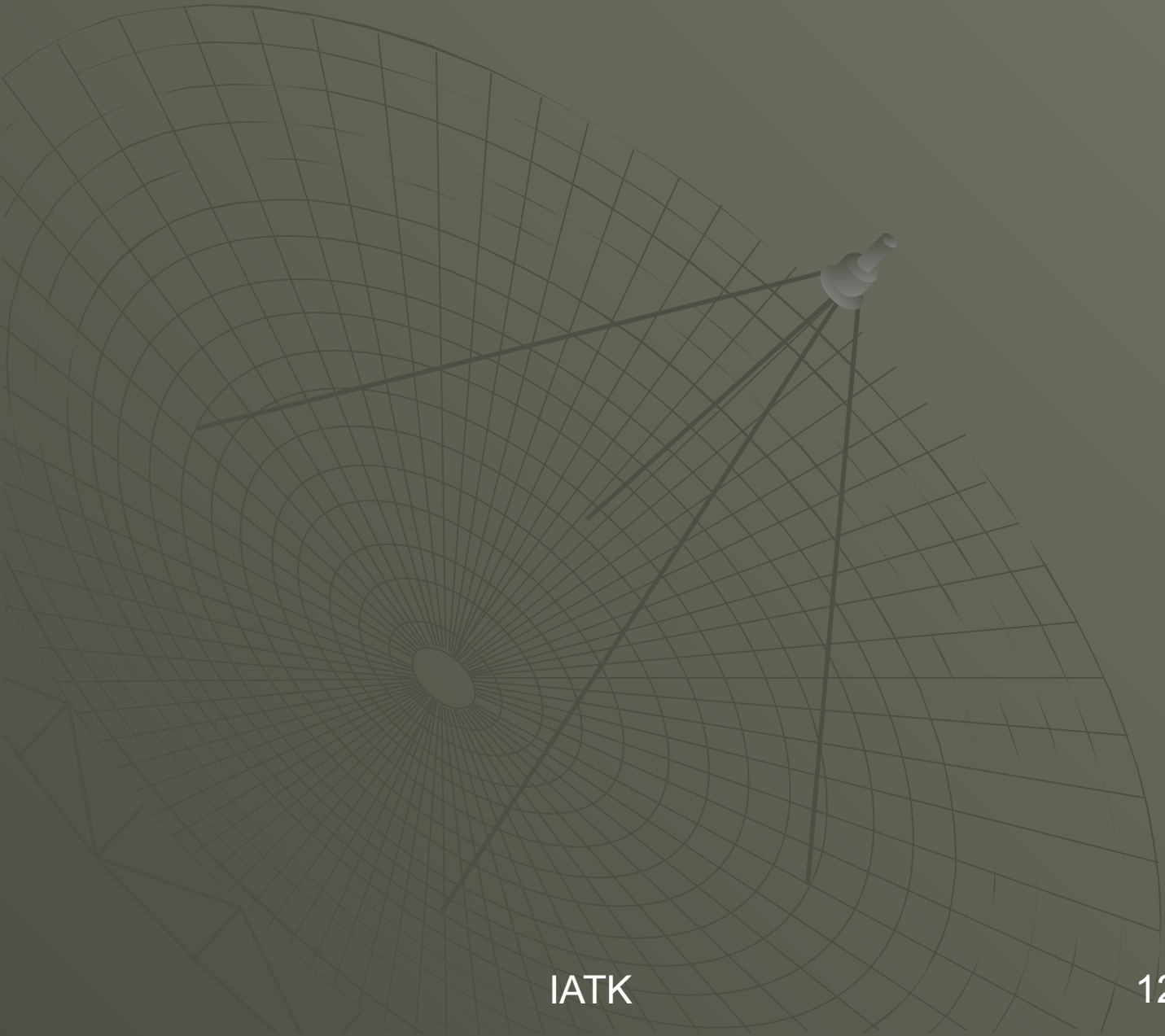
Советы

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

- оснастить компьютер современными антивирусными программами, например AVP, Aidstest, Doctor Web, и постоянно обновлять их версии;
- перед считыванием с дисков информации, записанной на других компьютерах, всегда проверять эти диски на наличие вирусов, запуская антивирусные программы;
- при переносе на компьютер файлов в архивированном виде проверять их сразу же после разархивации на жестком диске, ограничивая область проверки только вновь записанными файлами;

Советы

- ◆ периодически проверять на наличие вирусов жесткие диски компьютера, запуская антивирусные программы для тестирования файлов, памяти и системных областей дисков;
- ◆ обязательно делать архивные копии на дисках ценной информации;
- ◆ использовать антивирусные программы для входного контроля всех исполняемых файлов, получаемых из компьютерных сетей;
- ◆ для обеспечения большей безопасности применения Aidstest и Doctor Web необходимо сочетать с повседневным использованием ревизора диска Adinf, либо использовать полный комплект антивируса AVP.



IATK

12