

Презентация

выполнила

Пирожкова Анастасия

**Компьютерные
вирусы
и
борьба с ними**

Что такое компьютерный вирус

Компьютерный вирус-это программа, обычно малая по размеру (от 200 до 5000 байт), которая самостоятельно запускается, многократно копирует свой код, присоединяя его к кодам других программ («размножается») и мешает корректной работе компьютера и/или разрушает хранимую на магнитных дисках информацию (программы и данные).

Признаки проявления вируса:

- прекращение работы или неправильная работа ранее успешно функционировавших 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

Разновидности вирусов

По способу
заражения

По среде
обитания

По степени
воздействия

По
особенностям
алгоритма

по среде обитания

по среде обитания

файловы

е

загрузочны

е

драйверны

е

сетевые

загрузочно-
файловые

по способу заражения



резидентные

нерезидентные

по степени воздействия

по степени воздействия

опасные

неопасные

очень опасные



Принципы функционирования вирусов

- **файловые вирусы;**
- **загрузочные вирусы;**
- **загрузочно-файловые вирусы.**

Файловые вирусы

1. поиск подходящего для раздражения файла;
2. внедрение в него так, чтобы получить управление при запуске файла;
3. произведение эффекта(звукового или графического).

Загрузочные вирусы

- выделяют некоторую область дискеты и делают её недоступной операционной системе (помечая, например, как сбойную-bad);
- замещают программу начальной загрузки в загрузочном секторе дискеты, копируя корректную программу загрузки, а также свой код в выделенную область дискеты;
- организуют передачу управления так, чтобы вначале выполнялся бы код вируса и лишь затем - программа начальной загрузки.

Загрузочно-файловые вирусы

загрузочные вирусы

+

файловые вирусы

+

сила

=

загрузочно-файловые вирусы.

Методы защиты от компьютерных вирусов

- копирование информации - создание копий файлов и системных областей дисков;
- разграничение доступа предотвращает несанкционированное использование информации, в частности, защиту от изменений программ и данных вирусами, неправильно работающими программами и ошибочными действиями пользователей.

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.

Антивирусные средства

- Детекторы;
- Программы-доктора(фаги);
- Программы-ревизоры;
- Программы-фильтры(сторожа);
- Вакцины(иммунизаторы).

детекторы

детекторы

универсальные

полидетекторы

специализированные

Антивирусные программы

- *ДОСТОР
WEB*

- *АНТИВИРУС
КАСПЕРСКОГО
(KAV)*

DOCTOR WEB

Антивирус нового поколения, относящийся к классу детекторов-докторов.



Файл Задание Настройки Язык Помощь

Заголовок	Время запуска	Путь	Параметры	
Однократное обновле...	заблокировано	C:\Program Files\DrW...		
Ежечасное обновление	заблокировано	C:\Program Files\DrW...		
Еженедельное обновл...	заблокировано	C:\Program Files\DrW...		
Ежемесячное обновле...	заблокировано	C:\Program Files\DrW...	/GO	
Ежемесячное обновле...	заблокировано	C:\Program Files\DrW...		
Ежедневное обновлен...	18:00:00 29/05/2006	C:\Program Files\DrW...		
Ежегодное обновление	заблокировано	C:\Program Files\DrW...		
Update DrWeb	15:06:00 29/05/2006	C:\Program Files\DrW...	/GO	
Daily scan	заблокировано	C:\Program Files\DrW...	*	

OK

АНТИВИРУС КАСПЕРСКОГО (KAV)



Самый популярный и мощный из отечественных антивирусов.

Стандарт

Эксперт

Объекты

Параметры

Настройка

Статистика

- Мой компьютер
- Диск 3,5 (A:)
- Локальный диск (C:)
- CD-дисковод (D:)
- Сетевое окружение

- Действия в случае обнаружения вируса
 - Спросить пользователя
 - Только отчет
 - Лечить
 - Переименовывать объект
 - Удалять объект
- Сканировать сменные диски
- Сканировать жесткие диски
- Сканировать сетевые диски
- Сканировать файлы следующих типов
- Сканировать секторы
- Сканировать память
- Сканировать базы данных MS Outlook Express
- Сканировать объекты, исполняемые на старте системы
- Сканировать составные объекты
- Использовать эвристический анализатор кода

***Компьютерные
вирусы
и
борьба с ними***