Ответственность за несанкционированный доступ к информации, за создание и распространение вредоносных компьютерных программ

Васильева Александра, Чванов Денис,
Иноземцев Роман 11А

Определение

- ***Вирус*** - это программный код способный к самостоятельному размножению и функционированию, и имеющий защитные механизмы от обнаружения и уничтожения.
- ***Компьютерный вирус*** - это неизменный атрибут киберпространства; это независимая от выбора пользователя программа, способная к самораспространению.

Васильева Александра, Чванов Денис,
Иноземцев Роман 11А

Интересно

- ***Вирусописатели*** - это люди, попавшие в наиболее сильные потоки водоворота киберпространства, и в моменты написания вирусов ими руководит само киберпространство, в эти моменты они полностью ощущают себя его частью, получая взамен огромные запасы духовной энергии.
- ***Антивирусники***, по большей части - бывшие вирусописатели.

Васильева Александра, Чванов Денис,
Иноземцев Роман 11А

Виды

Расшифровка значений.

"+" - поддерживается

"-" - не поддерживается

"1"- Самовыполнение

"2"- Запуск носителя вируса

"3"- Используя функции поиска файлов

"4"- Использую записи в адресной книге

"5"- Перехватывая обращения ОС к файлам

Условное название	Краткое описание	Независимость	Самораспространение	Способ заражения	Способ распространения
COM		-	-	2	3
TSR	Резидентный вирус.	-	-	2	5
EXE	Вирус заражающий EXE(cutable) файлы.	-	-	2	3
BAT	Вирус на языке batch.	-	-	2	3
SYS	Вирусы заражающие SYS(tem) файлы.	-	-	?	3
BOOT	Вирус записывающий себя в загрузочную область.	-	+	1	?
MACRO	Вирус заражающий документы MSOffice.	-	+	2	3
STEALTH	Вирус перебрасывающий себя в память после запуска жертвы и записывающийся обратно после ее выполнения.	-	+	2	3,4
POLYMORPHIC	Вирус изменяющий свое тело.	-	+	2	3
PHANTOM	?	?	?	?	3
WORM	Червяк ☺. Вирус, распространяющийся по сети.	+	+	1	4
TROJAN	Трояны, если не понятно как это почитайте о взятии города Троя... (впрочем, позже я расскажу о нем подробнее.	+	-	2	4

Васильева Александра, Чванов Денис,
Иноземцев Роман 11А

Вирусы можно разделить

- ***на классы по следующим основным признакам*:**

1. среда обитания;
2. операционная система (ОС);
3. особенности алгоритма работы;
4. деструктивные возможности.

- ***среду обитания:***
- ***файловые;***
- ***загрузочные;***
- ***макро;***
- ***сетевые.***

Существуют следующие виды компьютерных вирусов по признаку вероломности:

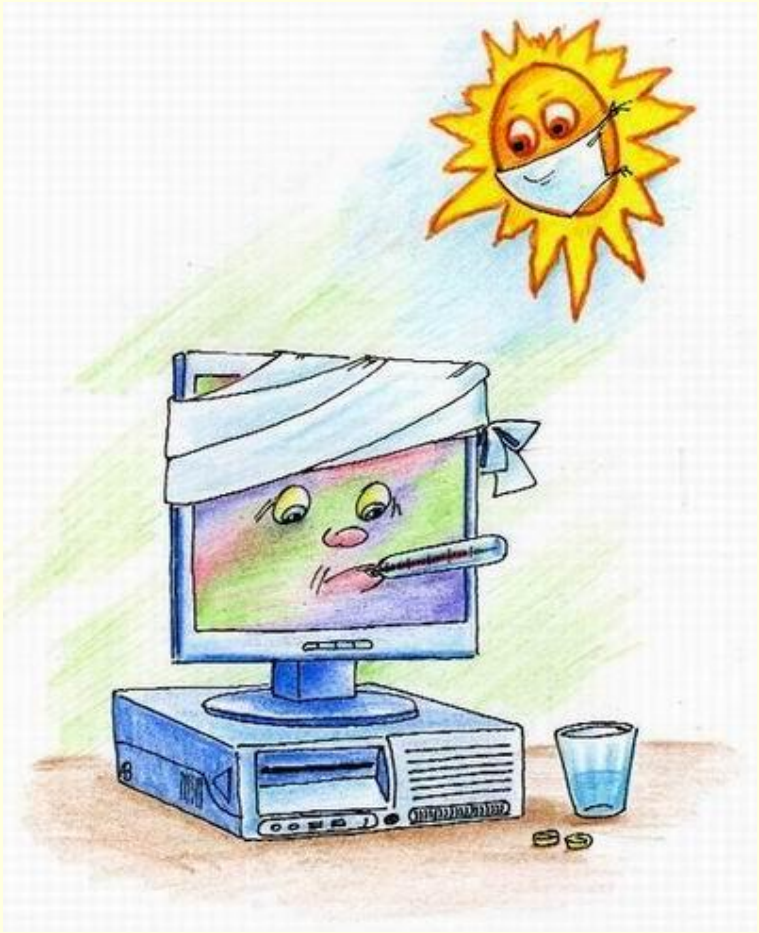
- вирусы, которые моментально поражают компьютер - они могут отформатировать жесткий диск, испортить таблицу размещения файлов, испортить загрузочные сектора, стереть BIOS.
- вирусы, действующие на компьютере продолжительно время - они постепенно заражают программы на компьютере, не выдавая своего присутствия.

По способам передачи и размножения существуют следующие виды компьютерных вирусов:

- Обычные вирусы - поражают только исполняемые файлы (с расширениями .com и .exe).
- Макро-вирусы - содержат скрытые команды для приложений, например для Internet Explorer, Microsoft Word.

Основные признаки проявления вирусов

- прекращение работы или неправильная работа ранее успешно функционировавших программ;
- медленная работа компьютера;
- 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;
- частые зависания и сбои в работе компьютера.



Васильева Александра, Чванов Денис,
Иноземцев Роман 11А

Последствия действий вируса

- уменьшает объем свободной памяти;
- считывает с диска свое продолжение;
- переносит себя в другую область памяти;
- устанавливает необходимые векторы прерываний;
- совершает дополнительные действия;
- копирует в память оригинальный Boot -сектор и передает на него управление.

- ***Зараженный диск*** – это диск, в загрузочном секторе которого находиться программа – вирус.
- ***Зараженная программа*** – это программа, содержащая внедренную в нее программу-вирус.

Способы защиты от вирусов

Основные методики обнаружения и защиты от вирусов:

- сканирование;
- эвристический анализ;
- использование антивирусных мониторов;
- обнаружение изменений;
- использование антивирусов, встроенных в BIOS компьютера.
- Кроме того, практически все антивирусные программы обеспечивают автоматическое восстановление зараженных программ и загрузочных секторов (конечно, если это возможно).

Васильева Александра, Чванов Денис,
Иноземцев Роман 11А

Способы защиты от вирусов

Административно-технологические методы защиты:

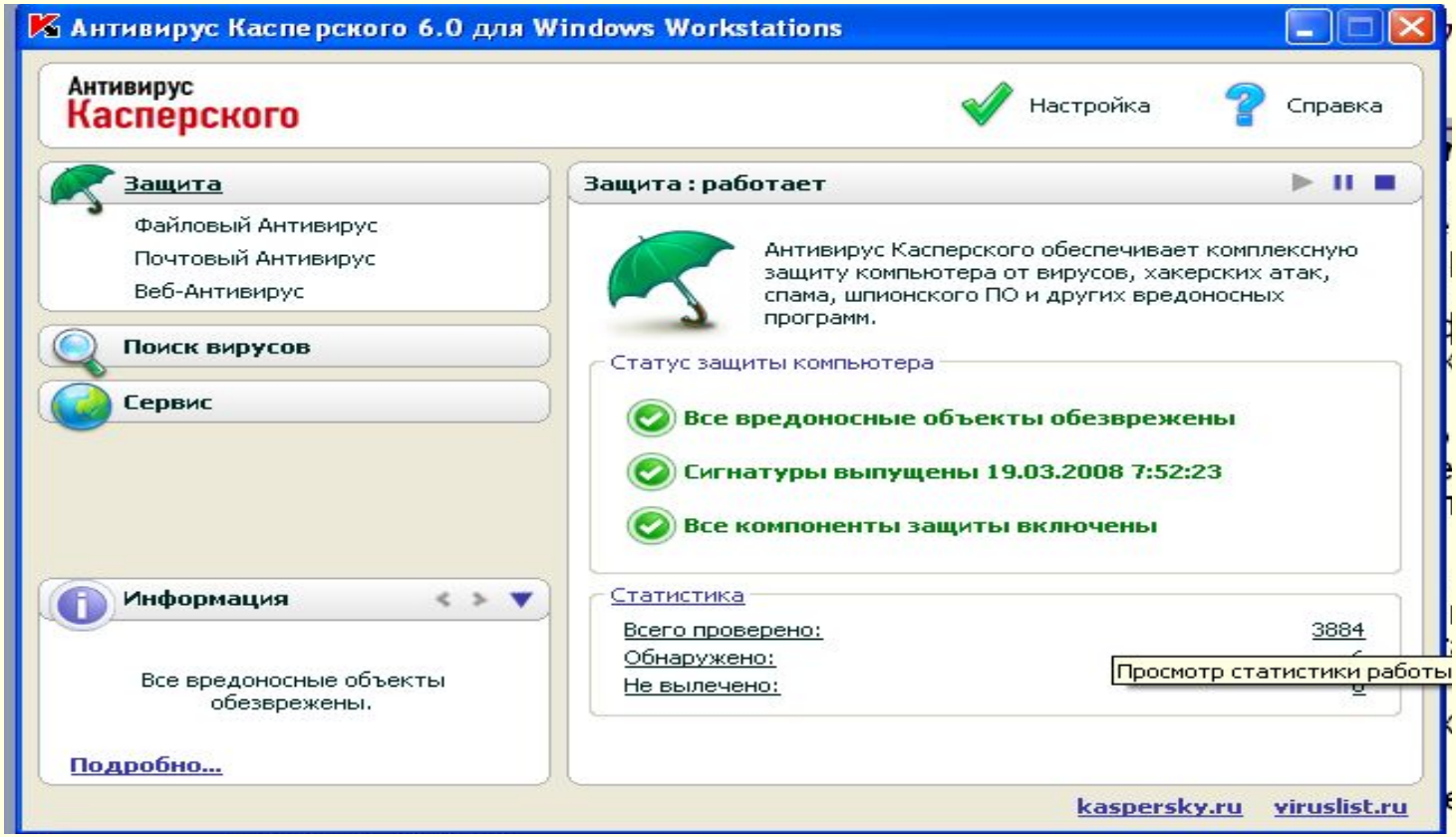
- Чтобы антивирусные программы эффективно выполняли свои функции, необходимо:

1. строго соблюдать рекомендации по их применению,
2. особое внимание следует обратить на регулярное обновление вирусных баз данных и программных компонентов антивирусов.

- Меры по предотвращению проникновения вирусов в компьютер и уменьшение вреда, который они нанесут в случае заражения:

1. Блокируйте возможные каналы проникновения вирусов: не подключайте компьютер к Интернету и локальной сети, отключите устройства внешней памяти, такие, как дисководы для дискет и устройства CD-ROM.
2. Настройте параметры BIOS таким образом, чтобы загрузка ОС выполнялась только с жесткого диска, но не с дискет.
3. Запретите программное изменение содержимого энергонезависимой памяти BIOS.

Защита школьных компьютеров



Васильева Александра, Чванов Денис,
Иноземцев Роман 11А

Способы защиты от вирусов

1. Изготовьте системную загрузочную дискету, записав на нее также антивирусы и другие системные утилиты для работы с диском, а также диск аварийного восстановления Microsoft Windows.
2. Устанавливайте ПО только с лицензионных компакт-дисков, ограничьте обмен программами и дискетами.
3. Установите на всех дискетах защиту от записи и снимайте ее только в случае необходимости.
4. Устанавливайте минимально необходимые права доступа к каталогам файлового сервера, защищайте от записи каталоги дистрибутивов и программных файлов.
5. Регулярно выполняйте резервное копирование данных.
6. Составьте для пользователей инструкцию по антивирусной защите, описав в ней правила использования антивирусов, правила работы с файлами и электронной почтой, а также опишите действия, которые следует предпринять при обнаружении вирусов.

Васильева Александра, Чванов Денис,
Иноземцев Роман 11А

Ответственность за распространение компьютерных вирусов

- Преступление, предусмотренное частью 1 ст. 273, может быть совершено только с умышленно, с сознанием того , что создание, использование или распространение вредоносных программ заведомо должно привести к нарушению неприкосновенности информации. Максимально тяжелым наказанием для преступника в этом случае будет лишение свободы до трех лет.

  Часть 2 ст. 273 в качестве дополнительного квалифицирующего признака предусматривает наступление тяжких последствий по неосторожности. По этой части суд может назначить максимальное наказание в виде семи лет лишения свободы.

- **Статья 274.** Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети (нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред).

Спасибо за внимание!
P.S. Мы следим за вами

Васильева Александра, Чванов Денис,
Иноземцев Роман 11А