

Компьютерные вирусы и антивирусные программы

Михлякова Е.А. – учитель
информатики и ИКТ МОУ СОШ с
углублённым изучением отдельных
предметов д. Стулово

2009

900igr.net

КОМПЬЮТЕРНЫЕ ВИРУСЫ -

*это программы, которые могут
«размножаться» и скрытно
внедрять свои копии:
в файлы, загрузочные секторы
дисков, документы.*

Немного истории

- Писатель- фантаст Т. Дж. Райн в одной из своих книг, опубликованной в США в 1977 г., описал эпидемию, за короткое время поразившую более 7000 компьютеров.
- 1986 год - первая глобальная эпидемия вируса для IBM-совместимых компьютеров. Вирус Brain, заражающий загрузочные сектора дискет, в течение нескольких месяцев распространился практически по всему миру. Причина - полная неподготовленность к встрече с компьютерным вирусом.
- 1988 г. - глобальная эпидемия вируса Suriv-3, более известного как Jerusalem. Вирус обнаружился сам: в пятницу, 13-го, он уничтожал все запускаемые на зараженном компьютере файлы. В 1988 г. этой черной датой стало 13 мая. Именно в этот день сообщения о тысячах инцидентах с участием Jerusalem поступили со всех концов планеты, в первую очередь из Америки, Европы и с Ближнего Востока.
- Сейчас известно несколько десятков тысяч вирусов.
- Название «**вирус**» пришло из биологии по признаку его способности к саморазмножению.

По степени воздействия

- **неопасные**, *действие которых приводит к:*
 - ❑ уменьшению свободной памяти на диске,
 - ❑ графическим и звуковым эффектам;
- **опасные**, *действие которых приводит к:*
 - ❑ сбоям и зависанию компьютера;
- **очень опасные**, *действие которых приводит к:*
 - ❑ потере программ и данных (изменению или удалению файлов и каталогов)
 - ❑ форматированию винчестера и т.д.

По «среде обитания»

- **файловые** - внедряются в исполняемые файлы, создают свои копии в различных каталогах, наиболее распространенный тип вирусов;
- **загрузочные** - записывают себя в загрузочный сектор диска (boot-сектор), либо в сектор, содержащий системный загрузчик винчестера (Master Boot Record); были достаточно распространены в 1990-х, но практически исчезли с переходом на 32-битные операционные системы и отказом от использования дискет как основного способа обмена информацией;
- **макровирусы** - заражают файлы документов Word и электронных таблиц Excel; являются программами на макро-языках, встроенных в системы обработки данных;
- **сетевые** – передаются по сети: **обычные** (описаны выше), **Интернет-черви, троянские программы** (передаются во вложенных в почтовые сообщения файлах) и **скрипт-вирусы** (передаются через программы на языках JavaScript, VBScript).

По алгоритмам

- **Вирусы-черви** – в компьютерных сетях
- **Вирусы-невидимки** – перехватывают обращения ОС к поражённым файлам и секторам и подставляют незаражённые объекты
- **Вирусы-мутанты** – при самовоспроизведении создают копии, отличающиеся от оригинала
- **«Троянский конь»** - программа, которая маскируясь под полезную программу, выполняет дополнительные функции, о которых пользователь не догадывается

По способу заражения

- **перезаписывающие** - вирус записывает свой код вместо кода заражаемого файла, уничтожая его содержимое;
- **паразитические** - при распространении своих копий обязательно изменяют содержимое файлов, оставляя сами файлы при этом полностью или частично работоспособными;
- **вирусы-компаньоны** - вирусы, не изменяющие заражаемых файлов: для заражаемого файла создается файл-двойник, причем при запуске зараженного файла управление получает именно этот двойник, т. е. вирус.
- **вирусы-ссылки** - не изменяют физического содержимого файлов, однако при запуске зараженного файла «заставляют» ОС выполнить свой код;
- **вирусы, заражающие исходные тексты программ;**
- **прочие способы заражения:** существуют вирусы, которые не связывают свое присутствие с каким-либо выполняемым файлом. При размножении они копируют свой код в какие-либо каталоги дисков в надежде, что новые копии будут когда-либо запущены пользователем.

Стадии вируса

- **Пассивная стадия**

Вирус практически не проявляет себя, стараясь оставаться незаметным. Получая управление на этой стадии, вирус отыскивает на других дисках компьютера системные или прикладные программы и внедряется в них.

Продолжительность: от нескольких минут до нескольких лет.

- **Активная стадия, или вирусная атака**

Вирусная атака может начинаться одновременно на всех пораженных компьютерах или в разное время. Обычно атака начинается с выполнения некоторого общего для всех компьютеров условия.

Хакерские утилиты и вредоносные программы

- Bad-Joke, Ноах — **злые шутки**, введение пользователя в заблуждение.

Не причиняют вреда, но выводят ложные сообщения о вирусных атаках, несуществующей опасности, форматировании диска и т.д. Программы, сообщающие пользователю заведомо ложную информацию о своих действиях в системе

- Dialers — **программы дозвона на платные ресурсы**.

Непосредственного вреда системе не наносят, но могут привести к значительному финансовому ущербу для владельца телефонного номера, с которого идёт дозвон на платный ресурс.

- Downloaders — **сетевые инсталляторы**

Программы, предназначенные для скачивания из сети и установки на компьютер прочего программного обеспечения, в большинстве случаев скрытно от пользователя.

- DoS, DDoS — **сетевые атаки** на удаленные сервера, посылая на них многочисленные запросы, что приводит к отказу в обслуживании.

- Хакерские утилиты для проникновения в удаленные компьютеры с целью дальнейшего управления ими (используя методы троянских программ типа «backdoor») или для внедрения во взломанную систему других вредоносных программ.

- Flooder — **«замусоривание»** сети

- Constructor — **конструкторы вирусов и троянских программ** — утилиты, предназначенные для изготовления новых компьютерных вирусов и «троянцев».

- **Хакерские утилиты**, использующиеся для шифрования других вредоносных программ с целью скрытия их содержимого от антивирусной проверки.

Как обнаружить хакерскую атаку

- Подозрительно высокий исходящий трафик. Подобный компьютер может использоваться для скрытой рассылки спама или для размножения сетевых червей.
 - Повышенная активность жестких дисков или подозрительные файлы в корневых директориях.
 - Большое количество пакетов с одного и того же адреса, останавливаемые персональным межсетевым экраном.
 - Постоянная антивирусная защита вашего компьютера сообщает о присутствии на компьютере троянских программ, хотя в остальном все работает нормально. Если ваш антивирус сообщает о поимке подобных вредоносных программ, то это может являться признаком того, что ваш компьютер открыт для несанкционированного удаленного доступа.
-

Признаки заражения

- Замедление работы компьютера
- Невозможность загрузки ОС
- Частые зависания и сбои в работе компьютера
- Вывод на экран непредусмотренных сообщений и изображений
- Подача непредусмотренных звуковых сигналов
- Произвольный запуск каких-либо программ
- Попытка какой-либо программы выйти в сеть Интернет
- Подозрительно высокий исходящий трафик
- Увеличение количества файлов и их размеров
- Знакомые говорят о сообщении, которое вы не посылали
- В электронной почте письма без обратного адреса и заголовка

Правила компьютерной гигиены

- Не использовать сомнительные дискеты
- Ограничить доступ к файлам программ, устанавливая для них, когда возможно, статус « только для чтения»
- При работе в сети, по возможности, не вызывайте программы из памяти других компьютеров.
- Храните программы и данные на разных дискетах или в разных подкаталогах жесткого диска.
- Не копируйте программы для собственных нужд со случайных копий.
- Обязательно иметь антивирусную программу

Что делать, если компьютер заражён

- Не паниковать
 - Отключить компьютер от сети Интернет
 - Отключить компьютер от локальной сети
 - Установить антивирусную программу
 - Выполнить полную проверку компьютера
-

Антивирусные программы

- **Полифаги** (*Kaspersky Anti-Virus, Dr.Web*):
 - ❑ проверяют файлы, загрузочные секторы дисков и оперативную память и ищут известные и новые (неизвестные полифагу) вирусы;
 - ❑ могут обеспечивать проверку файлов в процессе их загрузки в оперативную память (*мониторы*)
- **Ревизоры** (*ADinf*):
 - ❑ подсчитывают контрольные суммы для файлов на диске и хранят их в базе данных ;
- **Блокировщики** (*в BIOS компьютера*):
 - ❑ перехватывают «вирусоопасные» ситуации и сообщают об этом пользователю;

Антивирус Касперского

- 1997 год
- Информационная безопасность: система защиты от вирусов, спама, хакерских атак.
- Варианты работы программы:
 - Постоянная защита компьютера
 - Проверка компьютера по требованию
- Обновление антивирусных баз каждый час
- Не проверяет повторно не изменившиеся объекты – повышается скорость работы программы

Антивирус Касперского



Обновление

Антивирус Касперского

Kaspersky Anti-Virus

Защита

Файловый
Почтовый
Веб-Антивирус
Проактивный
Анти-Шпион
Анти-Хакер
Анти-Спам

Поиск вирусов

Сервис

Информация

Выполняется

Подробнее...

Обновление

Обновление : завершено

**Обновление завершено успешно**

Размер обновлений: 98.6 КБ

Трафик: 29.4 КБ

Скорость: 0.59 КБ/сек

Запуск: 1/15/2009 2:45:21 PM

Длительность: 00:01:17

Завершение: 1/15/2009 2:46:38 PM

События

Параметры

Событие	Имя объекта	Время	Трафик
✓ Выбран источник обновления	http://dnl-01.geo.kaspersky.com/	1/15/2009 2:45:24 PM	
✓ Файл загружен	index/6/u0607g.xml.dif	1/15/2009 2:45:24 PM	449 6
i Формируется список файлов для загрузки		1/15/2009 2:45:24 PM	
✓ Файл загружен	bases/aspy/aspy-0607g.xml.dif	1/15/2009 2:45:49 PM	850 6
✓ Файл загружен	bases/as/pas/pas-0607g.xml.dif	1/15/2009 2:45:52 PM	684 6
✓ Файл загружен	bases/av/avc/i386/av-i386-0607g.xml.dif	1/15/2009 2:45:55 PM	577 6
✓ Файл загружен	diffs/bases/aspy/aphish.dat.hqx	1/15/2009 2:46:26 PM	2.9 КБ
✓ Файл загружен	diffs/bases/as/pas/cfbase-s.gsg.nmw	1/15/2009 2:46:26 PM	1.2 КБ
✓ Файл загружен	diffs/bases/av/avc/i386/dailyec.avc.r9h	1/15/2009 2:46:31 PM	20.4 КБ
✓ Файл загружен	diffs/bases/av/avc/i386/daily-ec.avc.cqz	1/15/2009 2:46:32 PM	1.8 КБ
✓ Файл загружен	diffs/bases/av/avc/i386/daily.avc.l6q	1/15/2009 2:46:33 PM	622 6
i Файл обновлен	C:/Documents and Settings/All Users.WINDOWS/Application Data/Kaspe...	1/15/2009 2:46:33 PM	
i Файл обновлен	C:/Documents and Settings/All Users.WINDOWS/Application Data/Kaspe...	1/15/2009 2:46:34 PM	
i Файл обновлен	C:/Documents and Settings/All Users.WINDOWS/Application Data/Kaspe...	1/15/2009 2:46:34 PM	
i Файл обновлен	C:/Documents and Settings/All Users.WINDOWS/Application Data/Kaspe...	1/15/2009 2:46:34 PM	
i Файл обновлен	C:/Documents and Settings/All Users.WINDOWS/Application Data/Kaspe...	1/15/2009 2:46:34 PM	
i Файл обновлен	C:/Documents and Settings/All Users.WINDOWS/Application Data/Kaspe...	1/15/2009 2:46:34 PM	
i Файл обновлен	C:/Documents and Settings/All Users.WINDOWS/Application Data/Kaspe...	1/15/2009 2:46:34 PM	
i Файл обновлен	C:/Documents and Settings/All Users.WINDOWS/Application Data/Kaspe...	1/15/2009 2:46:34 PM	
i Файл обновлен	C:/Documents and Settings/All Users.WINDOWS/Application Data/Kaspe...	1/15/2009 2:46:34 PM	
i Файл обновлен	C:/Documents and Settings/All Users.WINDOWS/Application Data/Kaspe...	1/15/2009 2:46:35 PM	
i Файл обновлен	C:/Documents and Settings/All Users.WINDOWS/Application Data/Kaspe...	1/15/2009 2:46:35 PM	
i Файл обновлен	C:/Documents and Settings/All Users.WINDOWS/Application Data/Kaspe...	1/15/2009 2:46:35 PM	
i Файл обновлен	C:/Documents and Settings/All Users.WINDOWS/Application Data/Kaspe...	1/15/2009 2:46:35 PM	
i Задача завершена		1/15/2009 2:46:38 PM	

☐ Показывать все события

Действия...

Справка

Все отчеты

< Назад

Далее >

Сохранить как...

Закрыть

Настройка: Антивирус Касперского



Настройка

Защита

- Файловый Антивирус
- Почтовый Антивирус
- Веб-Антивирус
- Проактивная защита
- Анти-Шпион
- Анти-Хакер
- Анти-Спам

Поиск вирусов

- Критические области
- Мой Компьютер
- Объекты автозапуска

Сервис

- Обновление
- Файлы данных
- Настройка сети
- Вид



Защита

Общие

- ☒ Включить защиту
- ☒ Запускать приложение при включении компьютера

Доверенная зона...

Категории вредоносного ПО

- ☒ Вирусы, черви, троянские и хакерские программы
- ☒ Шпионское, рекламное ПО, программы скрытого дозвона
- ☒ Потенциально опасное ПО (riskware)

Я согласен, что некоторые легальные программы могут быть классифицированы как потенциально-опасные, и хочу, чтобы они воспринимались как угроза на этом компьютере.

Дополнительно

- ☒ Применять технологию лечения активного заражения
- ☒ Не запускать задачи по расписанию при работе от батареи
- ☒ Уступать ресурсы другим приложениям

Справка

OK

Закреть

Применить

slist.ru

Kaspersky
Anti-Virus



Настройка



Справка



Защита



Поиск вирусов

Критические области

Мой Компьютер

Объекты автозапуска



Сервис



Информация

Проверка Моего Компьютера:
выполняется

[Подробнее...](#)

Поиск вирусов : прервана



- ☒ F:\{вирус.ppt
- ☐ Мои документы
- ☐ Почтовые ящики
- ☐ Диск 3,5 (A:)
- ☒ Локальный диск (C:)
- ☐ DVD-RAM дисковод (D:)
- ☐ Съемный диск (F:)

Добавить...

Удалить

Действия...

Поиск вирусов

Настройка

Уровень безопасности:

Рекомендуемый

Действие:

Запросить по окончании проверки

Статистика

Проверено:

797

Обнаружено:

0

Последний запуск:

1/15/2009 2:40:17 PM

Проверка Моего Компьютера : работает



Проверяется: SCDWriter.exe

Расположение: C:\1\администрация\Новая папка\24 мар 2006 (D)\!!! По... \Запись CD_DVD\

Проверено: 25670 Запуск: 1/15/2009 2:42:53 PM
Обнаружено: 0 Длительность: 00:10:16
Не обработано: 0 Завершение: 1/15/2009 5:02:43 PM
Дата выпуска баз: 1/15/2009 6:02:32 AM

Обнаружено

События

Статистика

Параметры

Время	Имя	Статус	Причина
1/15/2009 2:53:08 PM	Файл: C:\1\администрация\Новая папка\24 мар 2006 (D)...	ok	проверен
1/15/2009 2:53:08 PM	Файл: C:\1\администрация\Новая папка\24 мар 2006 (D)...	ok	проверен
1/15/2009 2:53:08 PM	Файл: C:\1\администрация\Новая папка\24 мар 2006 (D)...	ok	iChecker
1/15/2009 2:53:08 PM	Файл: C:\1\администрация\Новая папка\24 мар 2006 (D)...	ok	проверен
1/15/2009 2:53:08 PM	Файл: C:\1\администрация\Новая папка\24 мар 2006 (D)...	ok	iChecker
1/15/2009 2:53:08 PM	Файл: C:\1\администрация\Новая папка\24 мар 2006 (D)...	ok	iChecker
1/15/2009 2:53:08 PM	Файл: C:\1\администрация\Новая папка\24 мар 2006 (D)...	ok	iChecker
1/15/2009 2:53:08 PM	Файл: C:\1\администрация\Новая папка\24 мар 2006 (D)...	ok	iChecker
1/15/2009 2:53:08 PM	Файл: C:\1\администрация\Новая папка\24 мар 2006 (D)...	упакованны...	
1/15/2009 2:53:08 PM	Файл: C:\1\администрация\Новая папка\24 мар 2006 (D)...	ok	проверен
1/15/2009 2:53:08 PM	Файл: C:\1\администрация\Новая папка\24 мар 2006 (D)...	ok	проверен

☒ Показывать все события

Действия...

Справка

Все отчеты

< Назад Далее >

Сохранить как...

Закреть

Литература

- Н. Угринович Информатика и информационные технологии. 10-11 класс
- Презентация «Компьютерные вирусы»
Мисюк А.В. г. Макеевка
 - Коляда М.Г. « Информатика и компьютерные технологии»
 - Гаевский « Информатика 7-11 класс»
 - Диск « 6 семестров»
- Viruslist.com