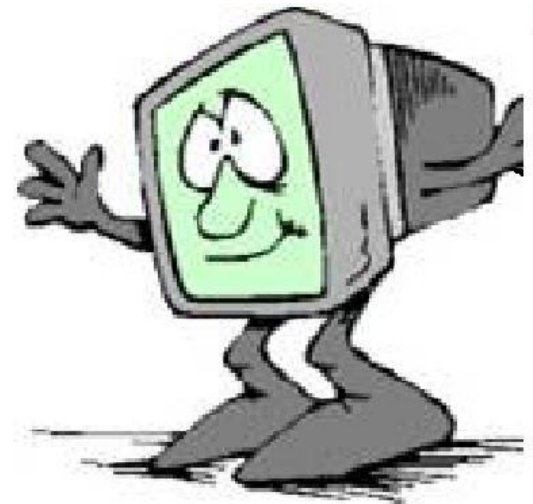


Компьютерные вирусы



Цель работы:

- Ознакомление с таким понятием, как вирусы;
- Способы борьбы с вирусами.

Достижение поставленной цели реализуется через выполнение следующих задач:

- Узнать, что такое компьютерный вирус;
- Проследить историю возникновения вирусов;
- Познакомиться с антивирусными программами;
- Узнать, что предпринять, если компьютер заражен;
- Сделать выводы и узнать, как человек сам может обезопасить свой компьютер.

Вирус – едва ли не самый главный враг компьютера. Крохотные зловредные программки могут в одночасье испортить плоды вашего многомесячного труда, уничтожить текстовые файлы и электронные таблицы, а то и вообще испортить файловую систему на жестком диске...

Вирус – это фрагмент программного кода, который может «размножаться» путем присоединения к другому объекту. Вирусная программа может производить самые разнообразные действия (в зависимости от мастерства злого гения, создавшего эту программу).

Результат воздействия вирусов:

- Повреждаются или уничтожаются файлы данных;
- Удаляются ранее установленные прикладные программы;
- Нарушается работа операционных систем;
- Возможно повреждение некоторых аппаратных компонентов ПК (например, уничтожается информация, которая хранится в микросхеме BIOS).



Описание вредоносных компьютерных программ

Вредоносное программное обеспечение

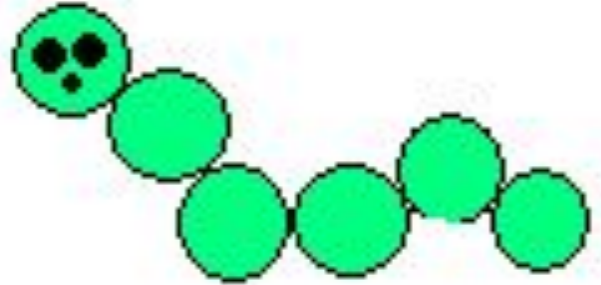
Классические компьютерные вирусы

Сетевые черви

Скрипты – убийцы

Троянские программы

Сетевые черви



К данной категории относятся программы распространяющие свои копии по локальным сетям с целью:

- проникновения на удаленные компьютеры;
- запуска своей копии на удаленном компьютере
- дальнейшего распространения на другие компьютеры в сети.

Некоторые черви обладают также свойствами других разновидностей вредоносного программного обеспечения. Например, некоторые черви содержат троянские функции или способны заражать выполняемые файлы на локальном диске, т. е. имеют свойство троянской программы и/или компьютерного вируса.

Троянские программы

В данную категорию входят программы, осуществляющие различные несанкционированные пользователем действия: сбор информации и ее передачу злоумышленнику, ее разрушение или злонамеренную модификацию, нарушение работоспособности компьютера, использование ресурсов компьютера в неблагоприятных целях.

Скрипты-убийцы

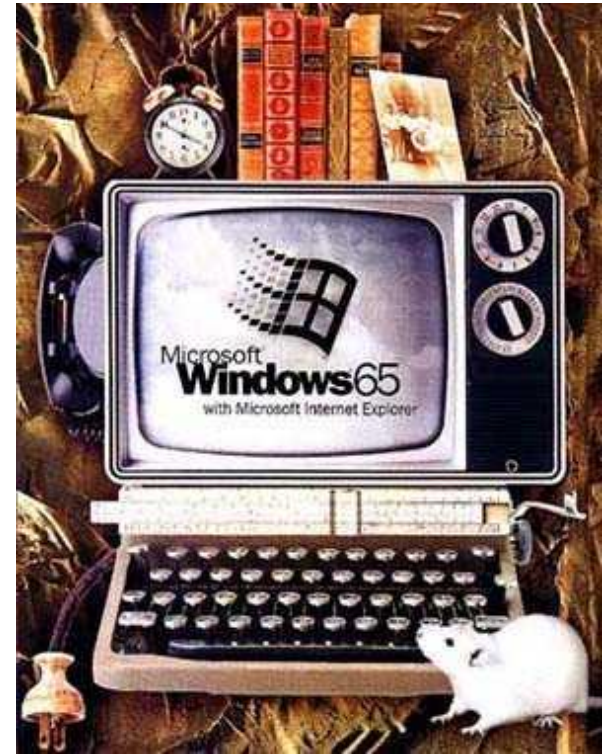


Речь идет о созданных хакерами микропрограммы, которые запускаются вместе с открываемыми страницами. Большинство из них мирно трудятся, делая страничку более привлекательной для глаза и более удобной. Но скрипты – самые настоящие полноценные программы. Причем многие из них запускаются именно на ваших компьютерах! И, встроив в них вредоносную начинку, создатели страницы могут получить доступ к содержимому вашего жесткого диска.

Еще одно разнообразие скриптов – многочисленные рекламные окна, которые заполняют экран вашего монитора после открытия одной единственной странички. Таким образом создатель сайта зарабатывает деньги за счет вашего времени и нервов.

История вредоносных программ

Идея компьютерных вирусов появилась давно. Отправной точкой можно считать труды Джона фон Неймана по изучению самовоспроизводящихся математических автоматов. Эти труды стали известны в 1940-х годах. А в 1951 г. знаменитый ученый предложил метод, который демонстрировал возможность создания таких автоматов.



Необходимо отметить, что с самого начала эти исследования были направлены не на создание теоретической основы для будущего развития компьютерных вирусов. Наоборот, ученые стремились усовершенствовать мир, сделать его более приспособленным для жизни человека. Ведь именно эти труды легли в основу многих более поздних работ по робототехнике и искусственному интеллекту. И в том, что последующие поколения злоупотребили плодами технического прогресса, нет вины этих печальных ученых.



Антивирусные программы

Полностью «отсечь» вирусы от вашего компьютера, разве что вы удалите дисковод, перестанете работать в Интернет и будете пользоваться только легальным программным обеспечением. Но есть еще один способ: снабдить вашу ОС антивирусными программами.

Многие белорусские пользователи останавливают выбор лишь на двух – **Norton Antivirus** от Symantec и **Антивирус Касперского (AVP)**. Обе эти программы достойны всяческих похвал, хотя, вне всякого сомнения у
обоих есть и минусы.

Norton Antivirus

Из под контроля этой программы не уйдет ни один запущенный на компьютере процесс. После установки Norton Antivirus о ней можно вообще забыть – NAV сама проконтролирует все, что нужно. Привлекать ваше внимание программа будет лишь в момент обнаружения нового вируса или при необходимости обновить антивирусные базы через Интернет. Вирусная база NAV, пожалуй, не имеет конкурентов по числу распознаваемых вирусов – около 50000! Однако NAV – громоздкая программа для большинства домашних компьютеров, размеры ее установочного комплекта оставляют желать лучшего, да и скорость работы не утешает.



Антивирус Касперского

Многие сделали свой выбор в пользу антивируса Kaspersky.

По сравнению со своими конкурентами «Касперский» компактен и быстр. В его архитектуре выдержан необходимый баланс между интеллектуальностью самой программы и возможностью контроля над ее действиями со стороны пользователя. Кроме того, программа «подстроена» под российскую и белорусскую «вирусную атмосферу» и способна дать отпор вирусам отечественного производства.



Признаки заражения компьютера

Есть ряд признаков, свидетельствующих о заражении компьютера:

- вывод на экран непредусмотренных сообщений или изображений;
- подача непредусмотренных звуковых сигналов;
- неожиданное открытие и закрытие лотка CD-ROM-устройства;
- произвольный, без вашего участия, запуск на компьютере каких-либо программ;
- при наличии на вашем компьютере межсетевого экрана, появление предупреждений о попытке какой-либо из программ вашего компьютера выйти в Интернет, хотя вы это никак не инициировали.

Если вы замечаете, что с компьютером происходит подобное, то с большой степенью вероятности можно предположить, что ваш компьютер поражен вирусом.

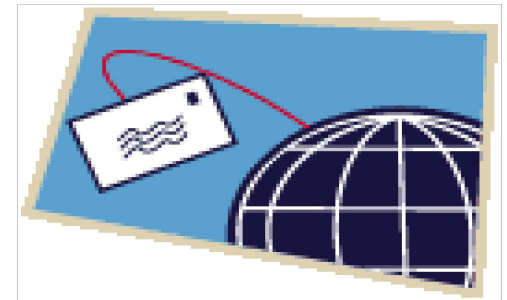


Характерные признаки поражения вирусом через электронную почту

Кроме того, есть некоторые характерные

признаки поражения вирусом
Через электронную почту:

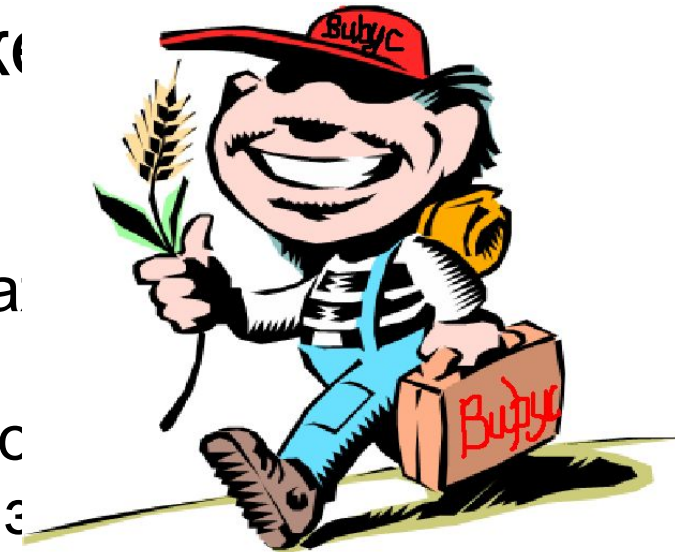
- друзья или знакомые говорят вам о сообщениях от вас, которые вы не отправляли;
- в вашем почтовом ящике находится большое количество сообщений без обратного адреса и заголовка.



Косвенные признаки заражения компьютера

Есть также косвенные признаки заражения компьютера:

- частые зависания и сбои в работе компьютера;
- медленная работа компьютера при выполнении операций;
- невозможность загрузки операционной системы;
- исчезновение файлов и каталогов или искажение их содержимого;
- частое обращение к жесткому диску (часто мигает лампочка на системном блоке);
- Интернет-браузер «зависает» или ведет себя неожиданным образом (например, окно программы невозможно закрыть).



Что делать, если компьютер заражен?

Если вы заметили, что ваш компьютер ведет себя «подозрительно»:

1. Не паникуйте! Не поддаваться панике — золотое правило, которое может избавить вас от потери важных данных и лишних переживаний.
2. Отключите компьютер от Интернета.
3. Отключите компьютер от локальной сети, если он к ней был подключен.
4. Если симптом заражения состоит в том, что вы не можете загрузиться с жесткого диска компьютера (компьютер выдает ошибку, когда вы его включаете), попробуйте загрузиться в режиме защиты от сбоев или с диска аварийной загрузки Windows, который вы создавали при установке операционной системы на компьютер.

5. Прежде чем предпринимать какие-либо действия, сохраните результаты вашей работы на внешний носитель (дискету, CD-диск, флэш-карту и пр.).
6. Установите антивирусную программу, если вы этого еще не сделали.
7. Получите последние обновления антивирусных баз. Если это возможно, лучше воспользоваться другим компьютером, поскольку при подключении к Интернету с зараженного компьютера есть вероятность отправки вирусом важной информации злоумышленникам или распространения вируса по адресам вашей адресной книги. Именно поэтому при подозрении на заражение лучше всего сразу отключиться от Интернета. Установите рекомендуемый уровень настроек антивирусной программы.
8. Запустите полную проверку компьютера.



Как обезопасить свой компьютер

Известно, что удовольствия от общения с вирусами не много. Так каким же образом можно остановить компьютерные вирусы и черви на начальном этапе, не допустив фатального повреждения данных и программ, установленных на компьютере или в сети? Для этого следует выполнять следующие рекомендации.



- ❖ Обращайте внимание на признаки, «говорящие» о появлении новых вирусов. Придерживаться подобной тактики особенно важно на протяжении первых нескольких часов или дней после того, как появилась информация о появлении нового вируса или червя (ведь в это время еще отсутствуют обновления антивирусных программ, направленные на выявление и ликвидацию новой вредоносной программы). Файлы, присоединенные к электронным сообщениям, которые присылаются вашими знакомыми, должны восприниматься настороженно.



- ❖ Установите антивирусные программы, которые следует своевременно обновлять. Желательно выполнять обновления еженедельно, поскольку в противном случае пользы от подобных программ будет немного... Идентификация инфицированных файлов грамотно спроектированной антивирусной программой осуществляется путем отслеживания загружаемых файлов, а так же файлов почтовых вложений в режиме реального времени.
- ❖ Регулярно проверяйте все сменные носители информации (CD –диски, флэш-карты, дискеты, цифровые фотоаппараты и др.).

❖ Обучайте других сетевых пользователей методикам, позволяющим предотвратить инфицирование вирусными программами. Удостоверьтесь в том, что пользователи, работающие совместно с вами в сети, не склонны посещать «подозрительные» Web-узлы, а так же открывать файлы, вложенные в почтовые сообщения. Рассказывайте им о важности своевременного обновления антивирусных программ...



Использованная литература

1. А. П. Сергеев. Офисные локальные сети. Самоучитель. М., 2003.
2. В. П. Леонтьев. Новейшая энциклопедия Интернет. М., 2003.
3. В. П. Леонтьев. Новейшая энциклопедия персонального компьютера 2003. М., 2003.
4. <http://www.kaspersky.ru>

