Компьютерные вирусы и антивирусные программы


My Compute
Network Neighborhoc
Recycled Bi
Internet Explorer
My Documents
Outlook Express
Start
My Computer\H
Registry Editor
9:53 PM
Please wait while your computer shuts down.
Microsoft
Windows 95

Первые вредоносные программы появились через несколько лет после появления персональных компьютеров. Это случилось в начале 80-х годов двадцатого века. К 2008 году вредоносных программ зарегистрировано уже более 200000.

Кто создает вирусы?

Студенты

Школьники

Профессиональные программисты

Классификация компьютерных вирусов

- Файловые вирусы
- Загрузочные вирусы
- Макровирусы
- Полиморфные и невидимые вирусы
- Психологические вирусы
- Почтовые черви
- Программы-шпионы (троянские кони)

Файловые вирусы

***Этап заражения*.**

Вирус, попадая в компьютер, записывает сам себя в файл, содержащий какую-либо программу. Программа, внутри которой находится вирус, в этом случае становится зараженной.

Этап размножения.

После появления в компьютере вредоносная программа никак внешне не проявляла себя, а занималась своим тиражированием или размножением.

Этап нападения.

Достаточно размножившись, вирус начинал атаковать зараженный компьютер. Проявлялось это в зависаниях, порче данных на винчестере и т. п. Приходилось переформатировать винчестер и переустанавливать ОС.

Загрузочные вирусы

При запуске компьютера операционная система начинает свою работу с чтения информации из служебного сектора диска внешней памяти (Boot–сектора). Если в этом секторе записан вирус, то он поступит в оперативную память.

Макровирусы

Макровирусы способных внедряться в файлы документов. Чаще всего они поражают документы, подготовленные в приложениях Word, Excel.

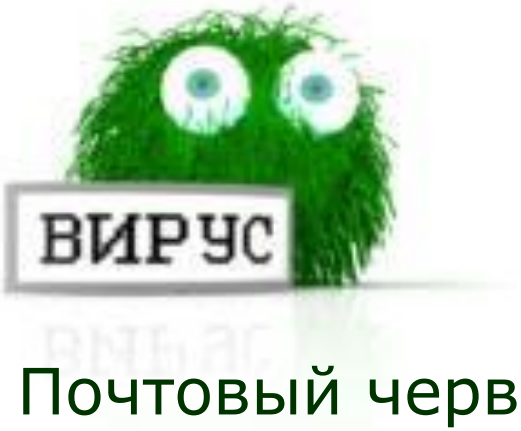
Полиморфные и невидимые вирусы

Полиморфные вирусы при размножении производят не точные свои копии, а делают каждую свою копию отличной от всех предыдущих. Таким образом они защищаются от антивирусных программ.

Вирусы-невидимки (стеллз-вирусы) перехватывают обращения операционной системы к дискам и дают искажённый ответ. Они делают таким образом свои файлы невидимыми на дисках.

Психологические вирусы

Периодически по электронной почте приходят ложные предупреждения о вирусных атаках с советами удалить один или несколько файлов на Вашем компьютере, где "прячется" вирус. Но если Вы последуете их совету, то своими руками выведете свой компьютер из строя.



Почтовые черви

Почтовый червь - это вредоносная программа, находящаяся в файле, присоединённом к электронному письму. Авторы червя всячески побуждают Вас запустить на выполнение присоединённый файл с вирусом. Его маскируют под новую игру, обновление популярных программ.

Будучи запущен на компьютере, червь первым делом рассылает свою копию по электронной почте, воспользовавшись Вашей адресной книгой. А затем делает с Вашим компьютером, что хочет: установить программу-шпиона, винчестер и т.д.

Программы-шпионы

В связи с бурным развитием сети Интернет и электронной коммерции появился новый класс вредоносных программ. Это программы-шпионы. Попадают они на компьютер с электронными червями или при посещении сайтов.

Обычно шпионские программы - это коммерческие программы очень высокого качества и большой сложности. Часто они направлены на получение секретной информации о кодах электронных банковских карточек.

Антивирусные программы

Структура и функционирование

Антивирусный монитор

Антивирусный сканер

Антивирусные базы данных

Антивирусный монитор

Постоянно отслеживает ситуации, при которых может произойти заражение компьютера вирусом: запуск программ на выполнение, обращения к дискам с целью модифицировать файлы, открытие приложений к электронным письмам, загрузка программ и файлов из сети Интернет.

Антивирусный монитор требует для своей работы большой части вычислительной мощности компьютера и обычно заметно снижает его быстродействие.

Антивирусный сканер

Антивирусный сканер проверяет оперативную память и дисков компьютера на наличие вирусов.

Сканирование винчестера занимает несколько часов. Поэтому сканирование лучше делать в обеденный перерыв или ночью.

Антивирусные базы данных

И сканер, и монитор используют общие антивирусные базы данных. В этих базах данных записана информация о вирусах. Без них антивирусная программа не может обнаруживать и обезвреживать вирусы.

Какую антивирусную программу выбрать?

Надёжными антивирусными программами считаются "Антивирус Касперского" и "Нортон Антивирус". Но эти программы очень мощные и требуют слишком больших ресурсов от компьютера.

Более экономные программы с хорошо озвучивающимся интерфейсом. Это российская программа "DrWeb" и NOD 32. Здесь нет злоупотреблений графикой и проблем с языком интерфейса.

Каждый сам принимает решение, будет ли он пользоваться антивирусом и каким.