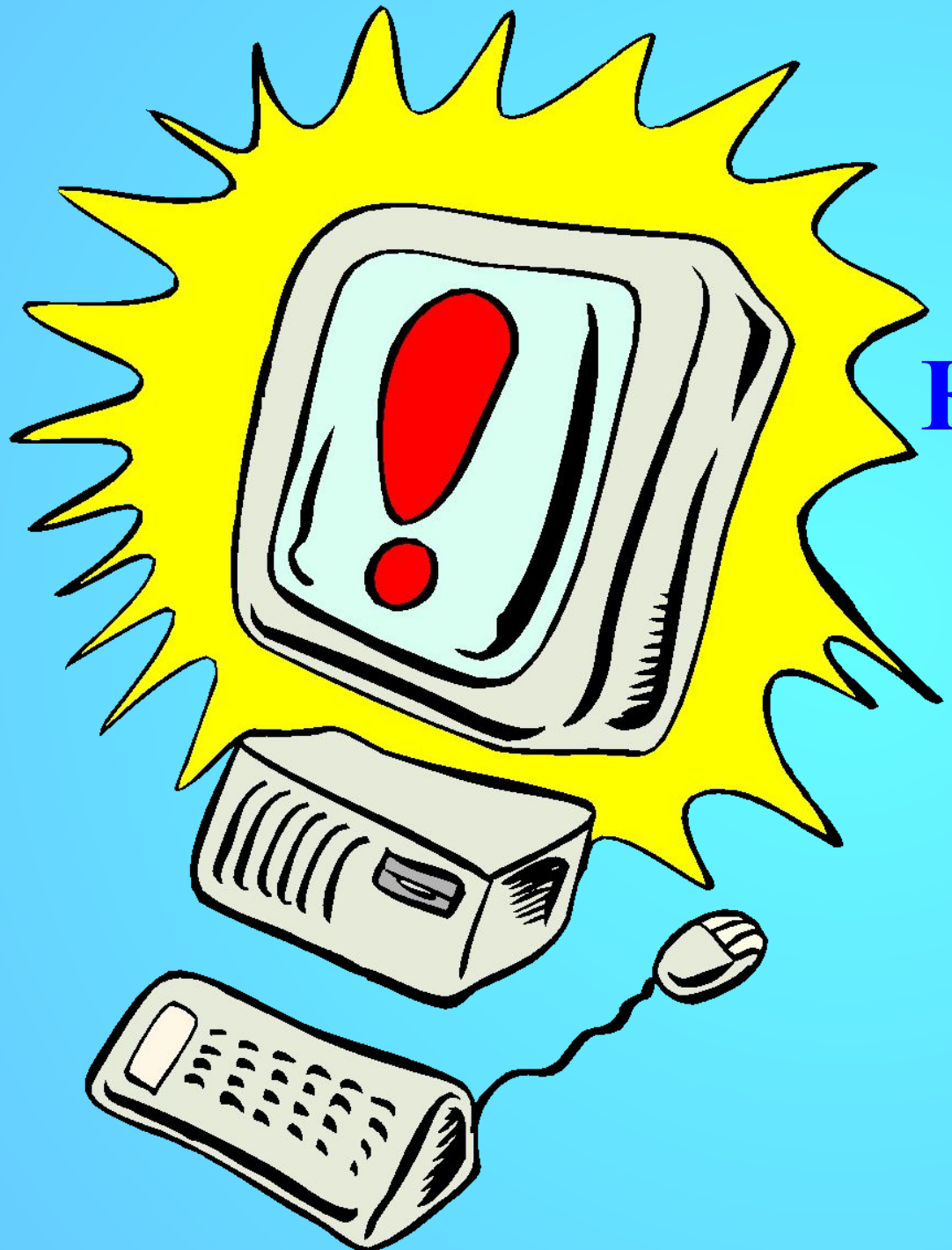


Компьютерные вирусы

Муллабаев Р.Ю.

Что такое компьютерный вирус?

Объяснений, что такое компьютерный вирус, можно привести несколько. Самое простое дадим на примере клерка, работающего исключительно с бумагами. Представим себе аккуратного клерка, который приходит на работу в контору и каждый день обнаруживает у себя на столе стопку листов бумаги со списком заданий на день. Клерк берёт верхний лист, читает указания начальства, пунктуально их выполняет, выбрасывает в корзину для бумаг "отработанный" лист и переходит к следующему листу.

Предположим, что некий злоумышленник тайком прокрадывается в контору и подкладывает в стопку с заданиями лист, на котором написано следующее: "***Переписать этот лист два раза и положить копии в стопку заданий соседей***". Что сделает клерк? Дважды перепишет лист, положит его соседям на стол, уничтожит оригинал и перейдёт к выполнению следующего листа из стопки, т.е. продолжит выполнять свою настоящую работу. Что сделают соседи, являясь такими же аккуратными клерками, обнаружив новое задание? То же, что и первый: перепишут его по два раза и раздадут другим клеркам. Итого в конторе бродят уже четыре копии первоначального документа, которые и дальше будут копироваться и передаваться на другие столы.

Примерно также работает и компьютерный вирус, только стопками бумаг-указаний являются **программы**, а клерком - **компьютер**. Как и клерк, компьютер аккуратно выполняет все команды программы (листы заданий), начиная с первой. Если же первая команда звучит как - "***скопируй меня в две другие программы***", то компьютер так и сделает, и команда-вирус попадёт в две другие программы. Когда компьютер перейдёт к выполнению этих заражённых программ, вирус тем же способом будет расходиться всё дальше и дальше по всему компьютеру.

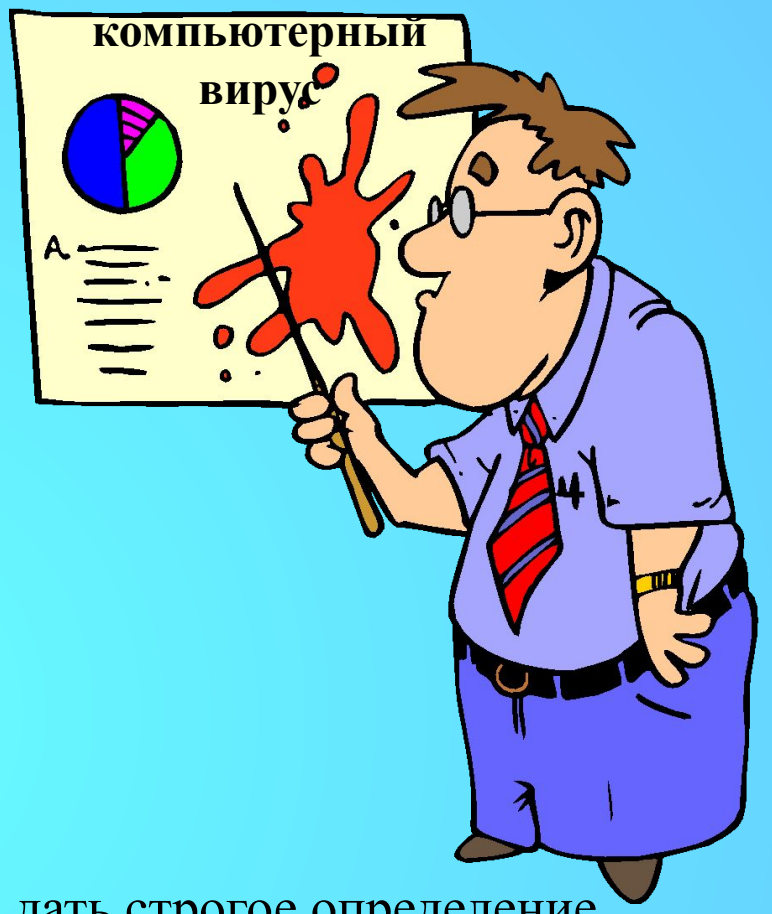
Как это не смешно (хотя участникам этого инцидента было совсем не смешно), именно такой случай произошёл в 1988 г. в Америке: несколько глобальных сетей передачи информации оказались переполненными копиями сетевого вируса (вирус Морриса), который рассылал себя от компьютера к компьютеру. Поэтому "правильные" вирусы делают так: "***Переписать этот лист два раза и положить копии в стопку заданий соседей, если у них ещё нет этого листа***".
Проблема решена - "перенаселения" нет, но каждая стопка содержит по копии вируса, при этом клерки ещё успевают справляться и с обычной работой.

Вот такое простое объяснение работы вируса. Плюс к нему хотелось бы привести две **аксиомы**, которые, как это ни странно, не для всех являются очевидными.

Во-первых: вирусы не возникают сами собой - их создают очень злые и нехорошие программисты-хакеры и рассылают затем по сети передачи данных или подкидывают на компьютеры знакомых. Вирус не может сам собой появиться на вашем компьютере: либо его подсунули на дискетах или на компакт-диске, либо вы его случайно "скачали" из компьютерной сети передачи данных.

Во-вторых: компьютерные вирусы заражают только компьютер и ничего больше, поэтому не надо бояться - через клавиатуру и мышь они не передаются.

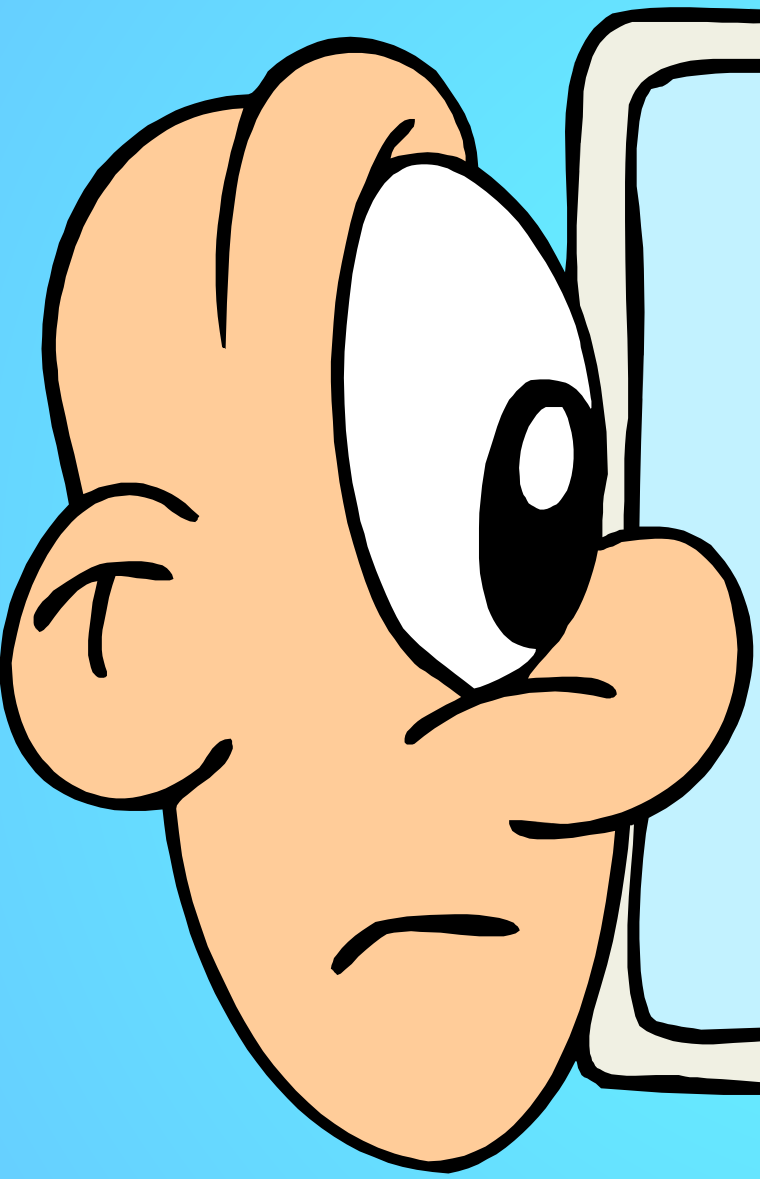
Термин "**компьютерный вирус**" появился позднее, официально считается, что его впервые употребил сотрудник Лехайского университета (США) Ф.Коэн в **1984 г**. на 7***-й конференции по безопасности информации***, проходившей в США. С тех пор прошло немало времени, острота проблемы вирусов многократно возросла, однако строгого определения, что же такое компьютерный вирус, так и не дано, несмотря на то что многие пытались это сделать неоднократно.



Основная трудность, возникающая при попытках дать строгое определение вируса, заключается в том, что практически все отличительные черты вируса (внедрение в другие объекты, скрытность, потенциальная опасность и пр.) либо присущи другим программам, которые никоим образом вирусами не являются, либо существуют вирусы, которые не содержат указанных выше отличительных черт (за исключением возможности распространения).

Поэтому представляется возможным сформулировать только обязательное условие для того, чтобы некоторая последовательность выполняемого кода являлась вирусом.

Обязательное (необходимое) свойство компьютерного вируса - возможность создавать свои дубликаты (не всегда совпадающие с оригиналом) и внедрять их в вычислительные сети и/или файлы, системные области компьютера и прочие выполняемые объекты. При этом дубликаты сохраняют способность к дальнейшему распространению.



Макровирусы

заражают файлы-документы и электронные таблицы нескольких популярных редакторов.

Сетевые вирусы

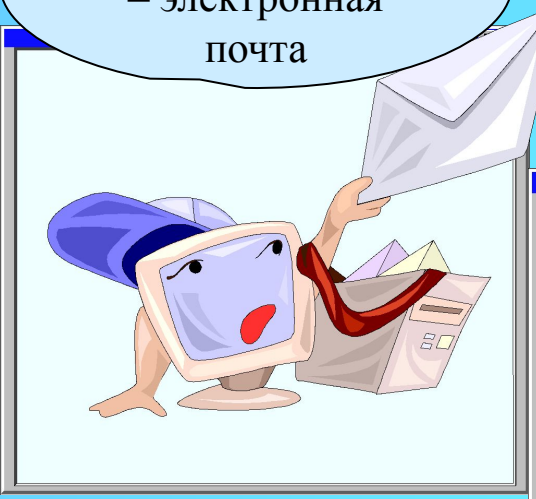
используют для своего распространения протоколы или команды компьютерных сетей и электронной почты.

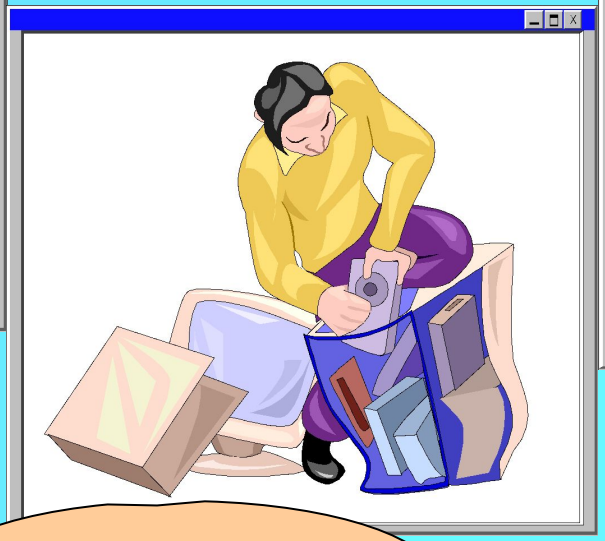
Резидентный вирус

при инфицировании компьютера оставляет в оперативной памяти свою резидентную часть, которая затем перехватывает обращения ОС к объектам заражения и внедряется в них. Эти вирусы находятся в памяти и являются активными вплоть до выключения компьютера или перезагрузки ОС.

Откуда берутся вирусы

Глобальные сети – электронная почта





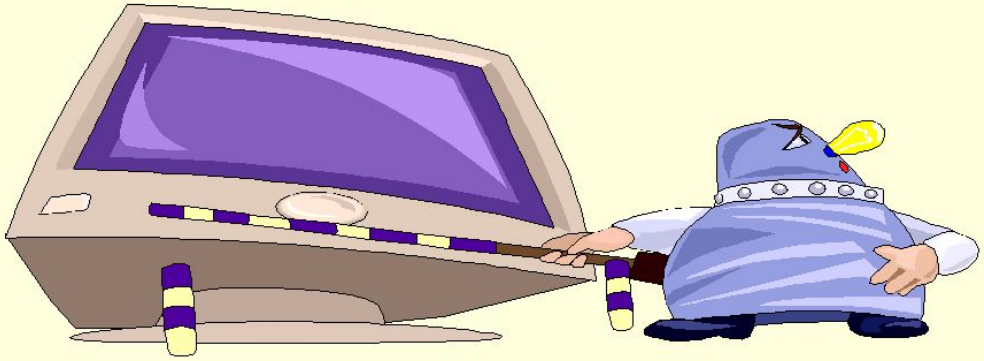
Локальные сети

Ремонтные службы

Персональный компьютер общего пользования

Пиратское программное обеспечение

Основные правила защиты

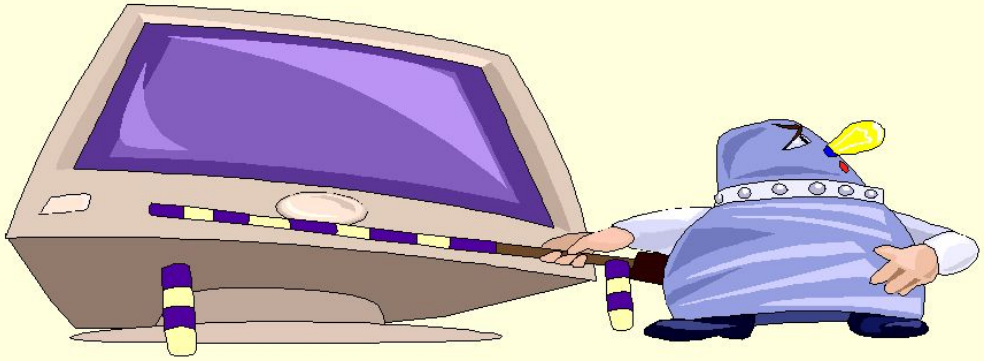


Правило первое: крайне осторожно относитесь к программам и документам Word/Excel, которые получаете из глобальных сетей. Перед тем как открыть документ обязательно проверьте его на наличие вирусов.

Правило второе: защита локальных сетей (ограничение прав пользователей, использование антивирусных программ, использование бездисковых рабочих станций.

Правило третье: используйте только хорошо зарекомендовавшие себя источники программ.

Основные правила защиты



Правило четвёртое: старайтесь не запускать не проверенные файлы. Перед запуском новых программ обязательно проверьте их одним или несколькими антивирусами.

Правило пятое: необходимо ограничивать круг лиц, допущенных к работе на конкретном компьютере. Как правило, наиболее часто подвержены заражению многопользовательские ПК.

Удачи

в борьбе с компьютерными вирусами!