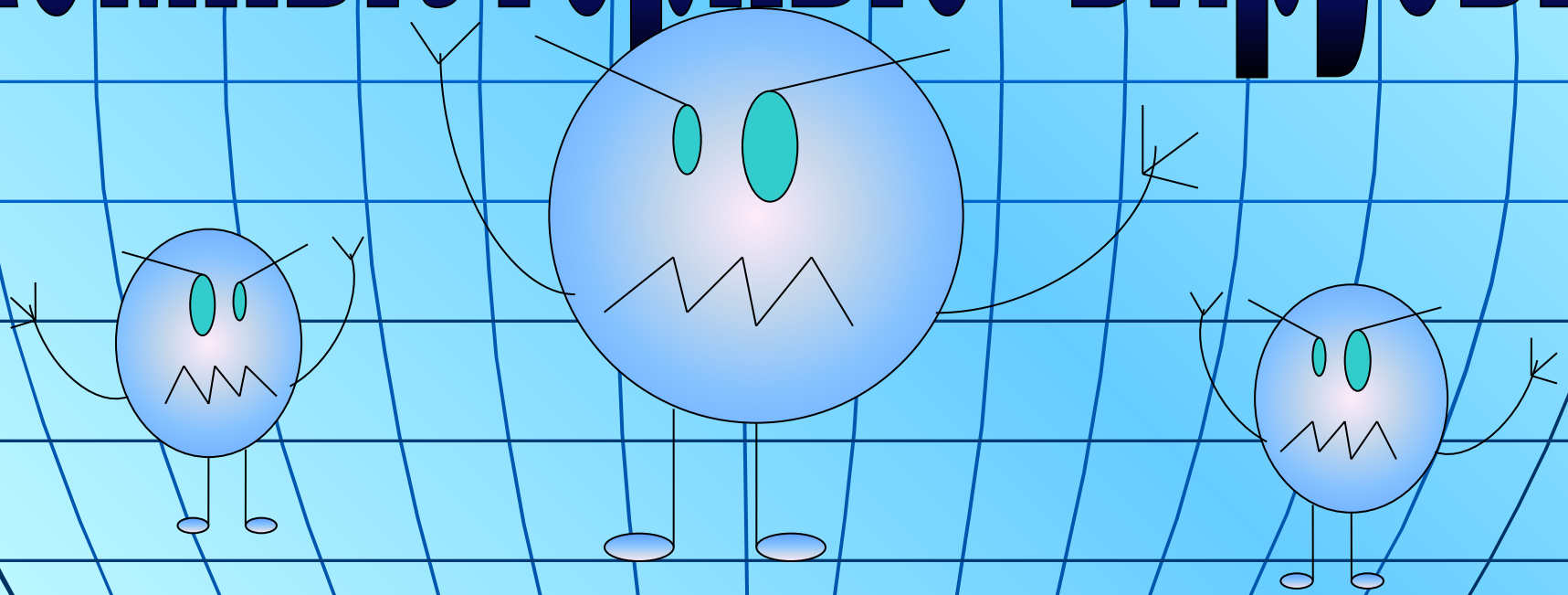
Компьютерные вирусы



Что такое вирус?

***Компьютерный вирус*- это специально написанная, небольшая по размерам программа, имеющая 2 отличительных признака**

1. Она может приписывать себя к другим программам (т.е. заражать их).

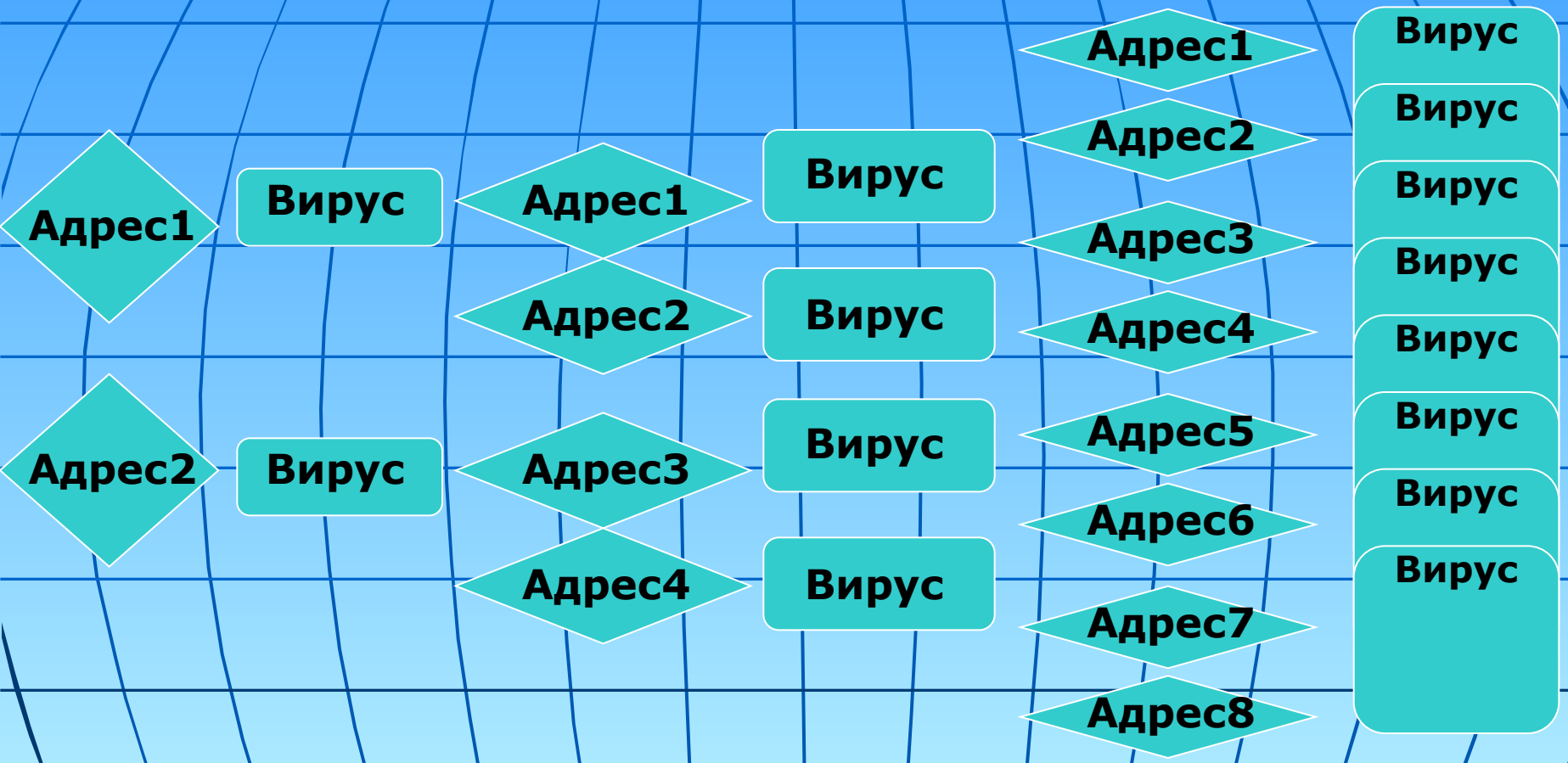
2.Может выполнять различные нежелательные и вредные действия. (портит файлы или таблицу размещения файлов на диске, засоряет оперативную память, удаляет файлы, выводит посторонние сообщения, символы и др.).

Среда обитания

- Сетевые: передают по компьютерным сетям свой программный код и запускают его на компьютере. Заражение может произойти при работе с электронной почтой или при работе в Интернете.
- Файловые: внедряются в программы и активизируются при их запуске. После запуска заражённой программы вирусы находятся в ОЗУ (оперативная память) и могут заражать другие файлы до выключения или перезагрузки ПК.
- Макровирусы (или загрузочные): заражают файлы различных документов. После загрузки заражённого документа вирус постоянно присутствует в ОЗУ и может заражать другие документы. Угроза заражения прекращается после выключения ПК.

- Так же могут присутствовать сочетания вирусов, например: файлово- загрузочные вирусы и др.

Реакция распространения вирусов



Лавинообразная цепная реакция распространения почтовых вирусов.

Способы заражения вирусом

Способы заражения делятся на:

- **Резидентный**
- **Нерезидентный**
- *Резидентный* вирус при инфицировании компьютера оставляет в оперативной памяти свою резидентную часть, которая затем перехватывает обращение операционной системы к объектам заражения и внедряется в них.
- *Нерезидентные* вирусы не заражают память компьютера и являются активными в ограниченное время.

Деструктивность вирусов

По деструктивным возможностям (по степени разрушительности) вирусы бывают разные.

- **безвредные,** т. е. никак не влияющие на работу компьютера (кроме уменьшения свободной памяти на диске в результате своего распространения).
- **неопасные,** влияние которых ограничивается уменьшением свободной памяти на диске, графическими, звуковыми и прочими эффектами.
- **опасные вирусы,** которые могут привести к серьезным сбоям в работе компьютера.
- **очень опасные,** которые могут привести к потере программ, уничтожить данные, стереть необходимые для работы файлы.

Типы вирусов

По особенностям алгоритма можно выделить следующие группы вирусов:

- **вирусы-“спутники” *(companion)*** — это вирусы, не изменяющие файлы. Алгоритм работы этих вирусов состоит в том, что они создают для EXE- файлов файлы- спутники, имеющие то же самое имя, но с расширением COM. При запуске система ищет сначала файл с расширением COM, запускает его, вирус выполняет все свои действия и затем запускает настоящую программу, у которой расширение EXE;

- **вирусы-“черви”** *(worm)* —вирусы, которые распространяются в компьютерной сети. Они проникают в память компьютера по сети, вычисляют адреса других компьютеров и рассылаются по этим адресам.
- **“паразитические” -** все вирусы, которые при распространении своих копий изменяют содержимое дисковых секторов и файлов. В эту группу входят все вирусы, которые не являются “спутниками” и “червями”.

- **студенческие” -** крайне примитивные вирусы, часто нерезидентные и содержащие большое число ошибок.
- **вирусы- невидимки (*stealth)* —** это очень совершенные программы, которые перехватывают обращения DOS к пораженным файлам или секторам диска и “подставляют” вместо себя незараженные участки.
- **вирусы-“призраки”-** достаточно трудно обнаруживаемые вирусы, не имеющие ни одного постоянного участка кода. Вирус шифрует свой код. При шифровке каждый раз используются разные ключи. Кроме того, модифицируется и программа- расшифровщик. Таким образом, код вируса в разных случаях заражения будет другой.

Эпидемии компьютерных вирусов

- Первая эпидемия заражения компьютерным вирусом произошла в 1986 году, когда вирус по имени Brain («мозг») «заражал» дискеты ПК.

- Ещё более крупная эпидемия произошла 5 мая 2000 года. Это был почтовый вирус. Десятки миллионов ПК подключенных к глобальной сети Интернет, получили почтовое сообщение «ILOVEYOU». Это сообщение содержало вложенный файл- вирус. После его прочтения вирус заражал компьютер и разрушал файловую систему.

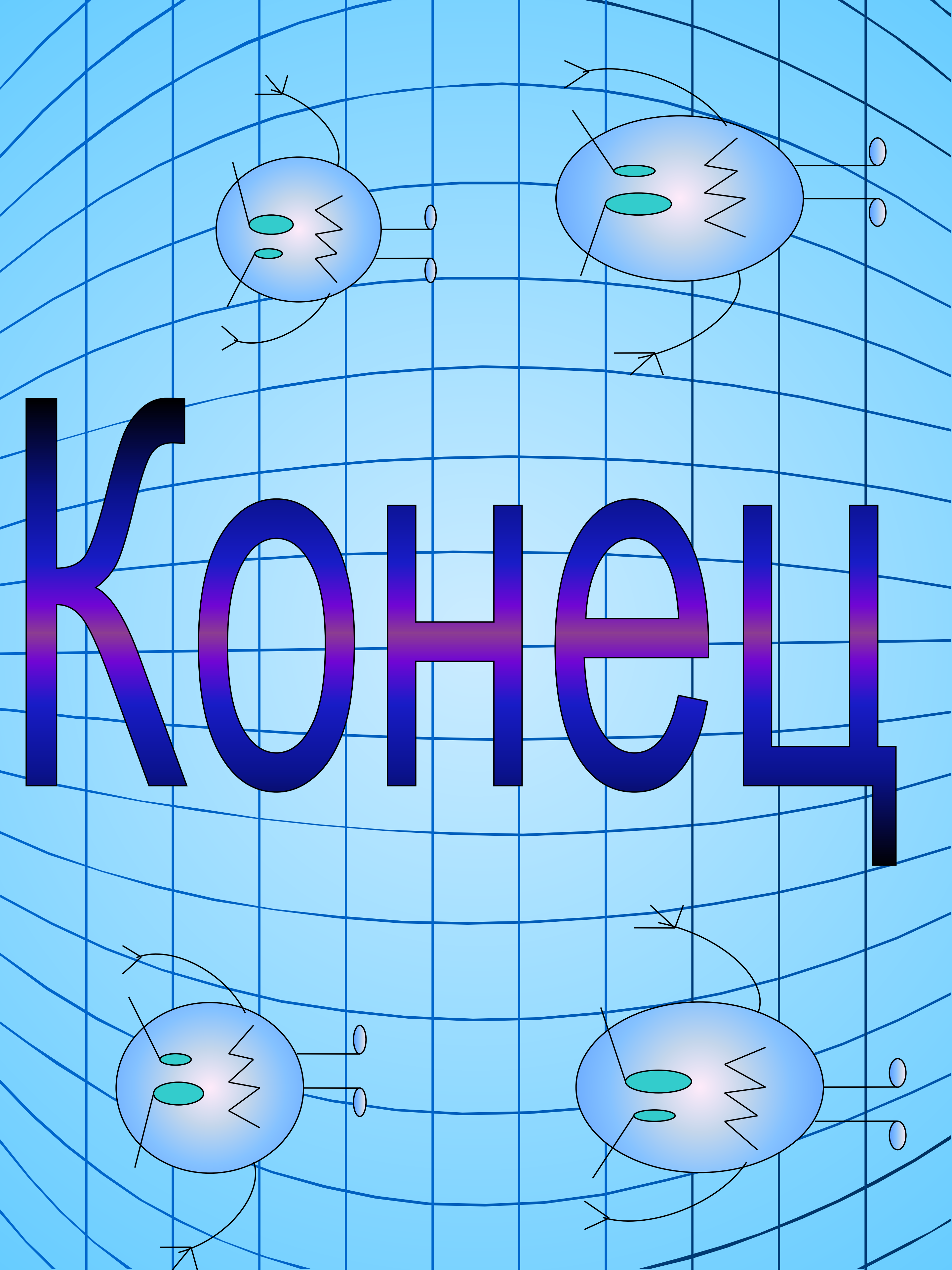
Если вы обнаружили опасный вирус

Необходимо:

- Отключить зараженный вирусом ПК.
- Запустить систему, используя специальную загрузочную дискету, защищенную от записи.
- Запустить антивирусную программу.
- Возможно форматирование жесткого диска.

Подразделение антивирусных программ

- Сканеры (доктора) - сканируют и лечат по запросу пользователя (требуют обновления антивирусных баз).
- Ревизоры (создают базу контрольных кодов всех файлов и в дальнейшем их сравнивают).
- Мониторы или фильтры - постоянно находятся в памяти ПК и проверяют файлы в процессе работы.
- Антивирусные программы: DR WEB, Антивирус Касперского, Nod32, Norton-антивирус и др.


Конец