ИНФОРМАТИКА

8 класс

Компьютерные вирусы и антивирусные программы

учитель информатики
МБОУ СОШ № 42 г.Ставрополя
Кузьминых Ольга Валерьевна

Компьютерные вирусы

Компьютерные вирусы – это вредоносные программы, которые могут «размножаться» и скрытно внедрять свои копии в файлы, загрузочные секторы дисков и документы. Активизация компьютерного вируса может вызывать уничтожение программ и данных.

При заражении компьютера вирусом очень важно своевременно его обнаружить.

Основные признаки проявления вирусов:

- прекращение работы или неправильная работа ранее успешно функционировавших программ;
- медленная работа компьютера;
- невозможность загрузки операционной системы;
- исчезновение файлов и каталогов или искажение их содержимого;
- изменение даты и времени модификации файлов;
- изменение размеров файлов;
- неожиданное значительное увеличение количества файлов на диске;
- существенное уменьшение размера свободной оперативной памяти;
- вывод на экран непредусмотренных сообщений или изображений;
- подача непредусмотренных звуковых сигналов;
- частые зависания и сбои в работе компьютера.

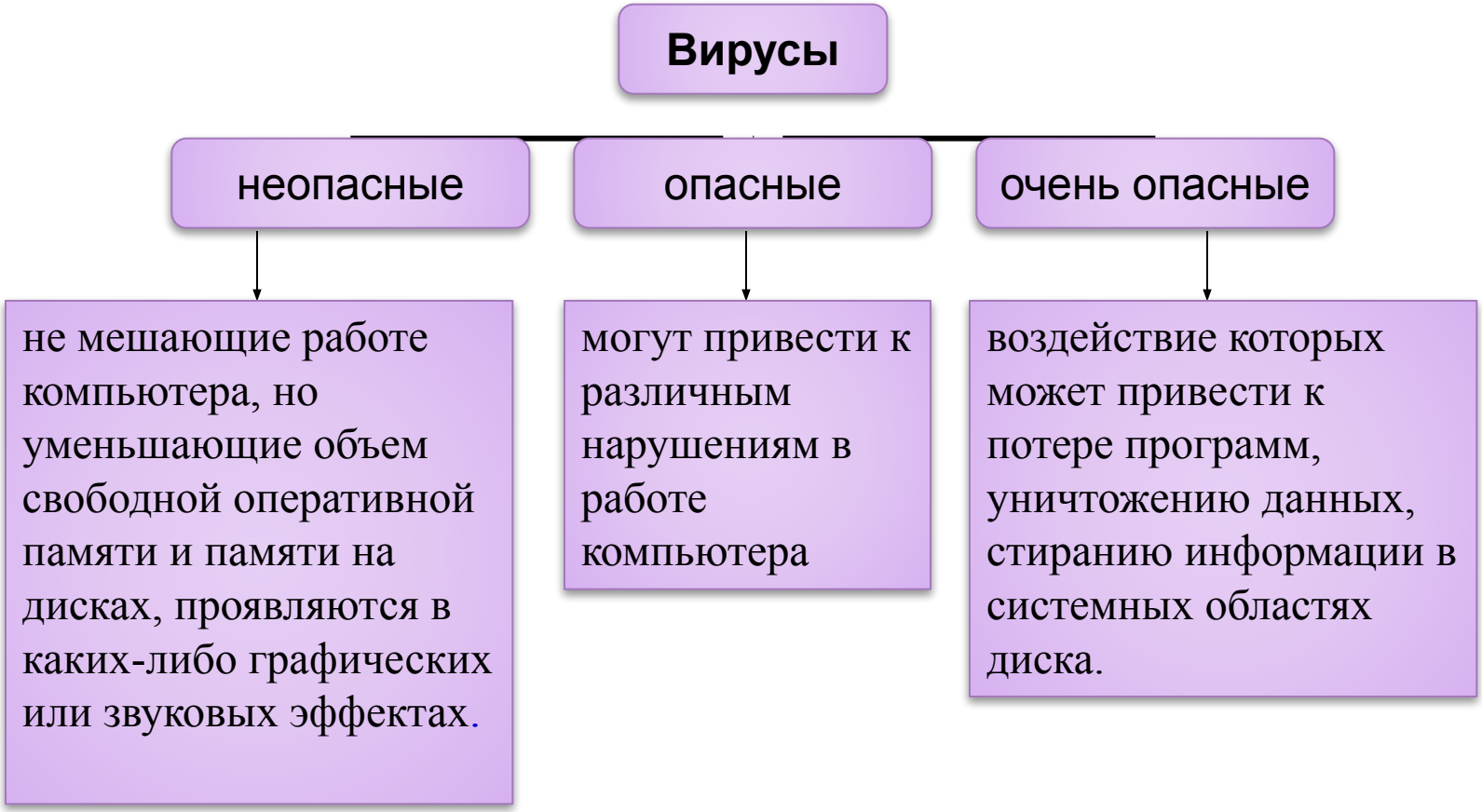
Основные виды вирусов

В настоящее время известно несколько десятков тысяч вирусов, их можно классифицировать по ***следующим признакам:***

- ***воздействию*** (неопасные, опасные, очень опасные);
- ***среде обитания*** (сетевые, файловые, загрузочные, макровирусы);
- ***способу заражения среды обитания*** (резидентные, нерезидентные);
- ***особенностям алгоритма*** (паразитические, репликаторы, невидимки, мутанты, троянские, вирусы-спутники).

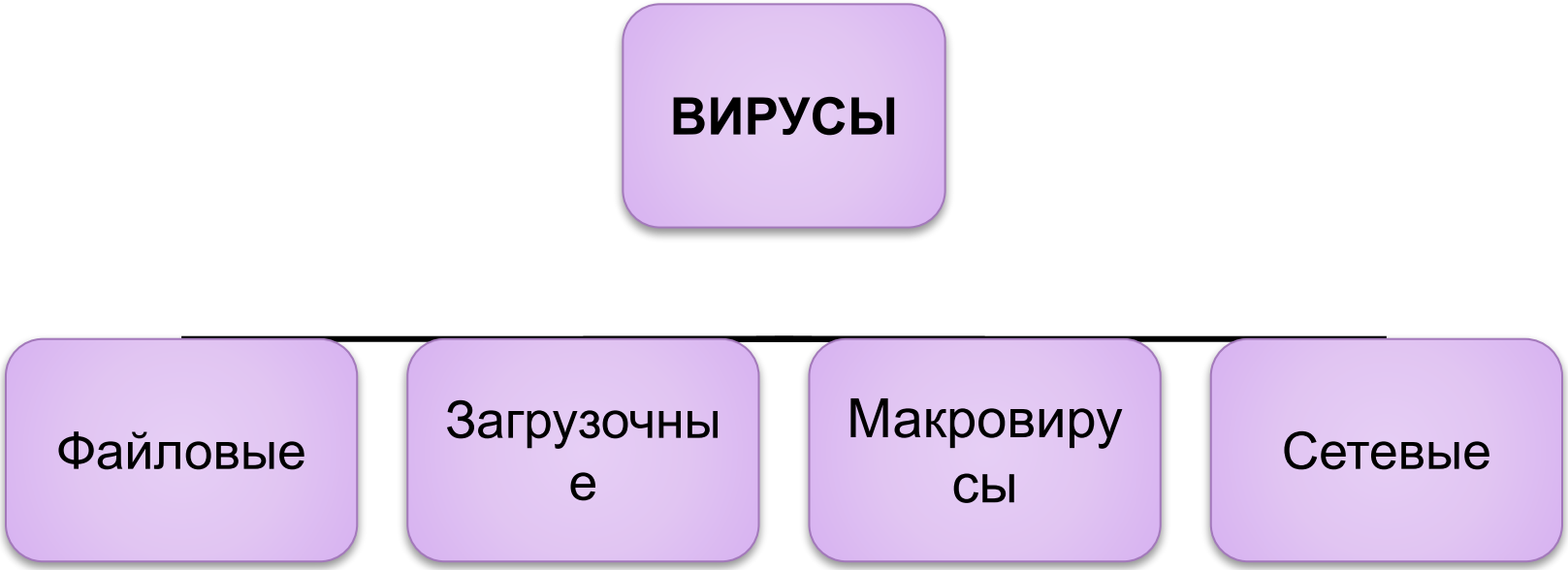
Виды компьютерных вирусов

по величине вредных воздействий



Виды компьютерных вирусов

ПО «СРЕДЕ ОБИТАНИЯ»



Файловые вирусы

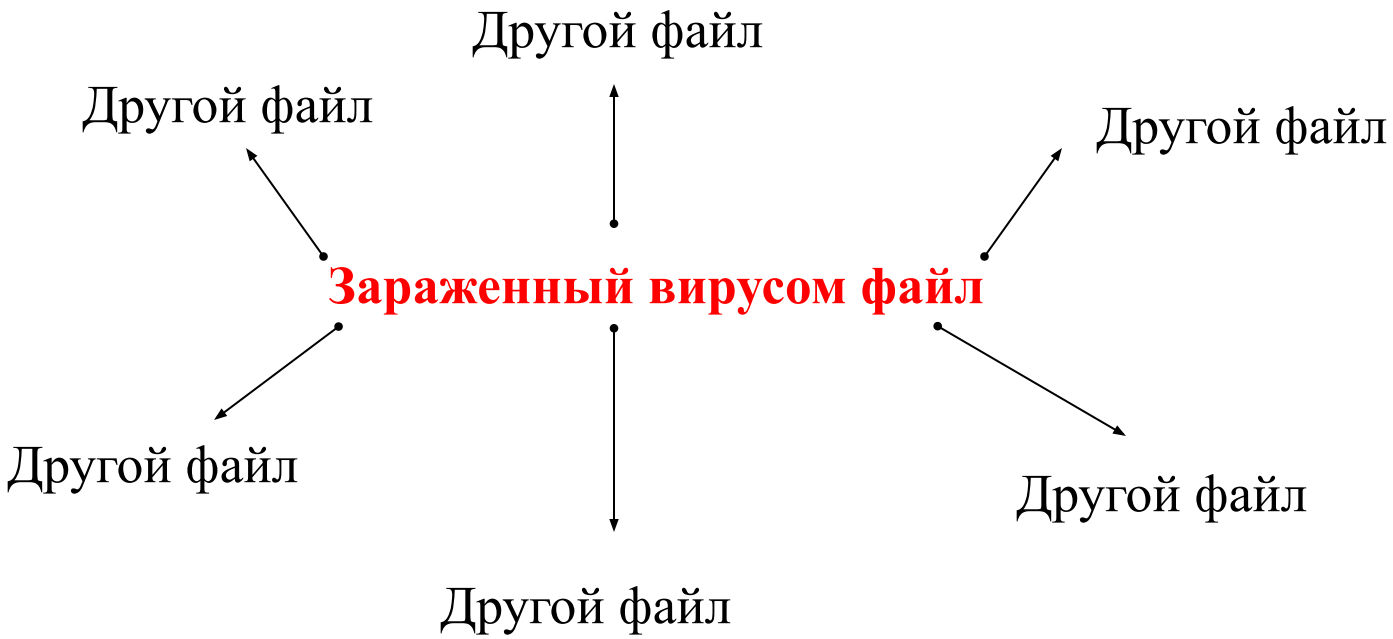
Файловые вирусы внедряются главным образом в исполняемые модули, т. е. файлы с расширением **com** и **exe.**

Обычно файловые вирусы активизируются при запуске файлов программы.

Файловые вирусы не могут заразить файлы данных (изображение, звук).

Файловые вирусы

1. Вирус внедряется в файлы программ, активизируется при их запуске.
2. После запуска зараженной программы вирус находится в оперативной памяти и может активно заражать другие файлы.



3. При отключении компьютера или перезагрузке операционной системы вирус становится неактивным.

Загрузочные вирусы

Загрузочные вирусы записывают себя в загрузочный сектор диска. При загрузке операционной системы с заражённого диска вирусы внедряются в оперативную память компьютера. В дальнейшем загрузочный вирус ведёт себя так же, как файловый, то есть может заражать файлы при обращении к ним компьютера.

Макровирусы

Макровирусы заражают файлы-документы и шаблоны документов Word и Excel и т.д.

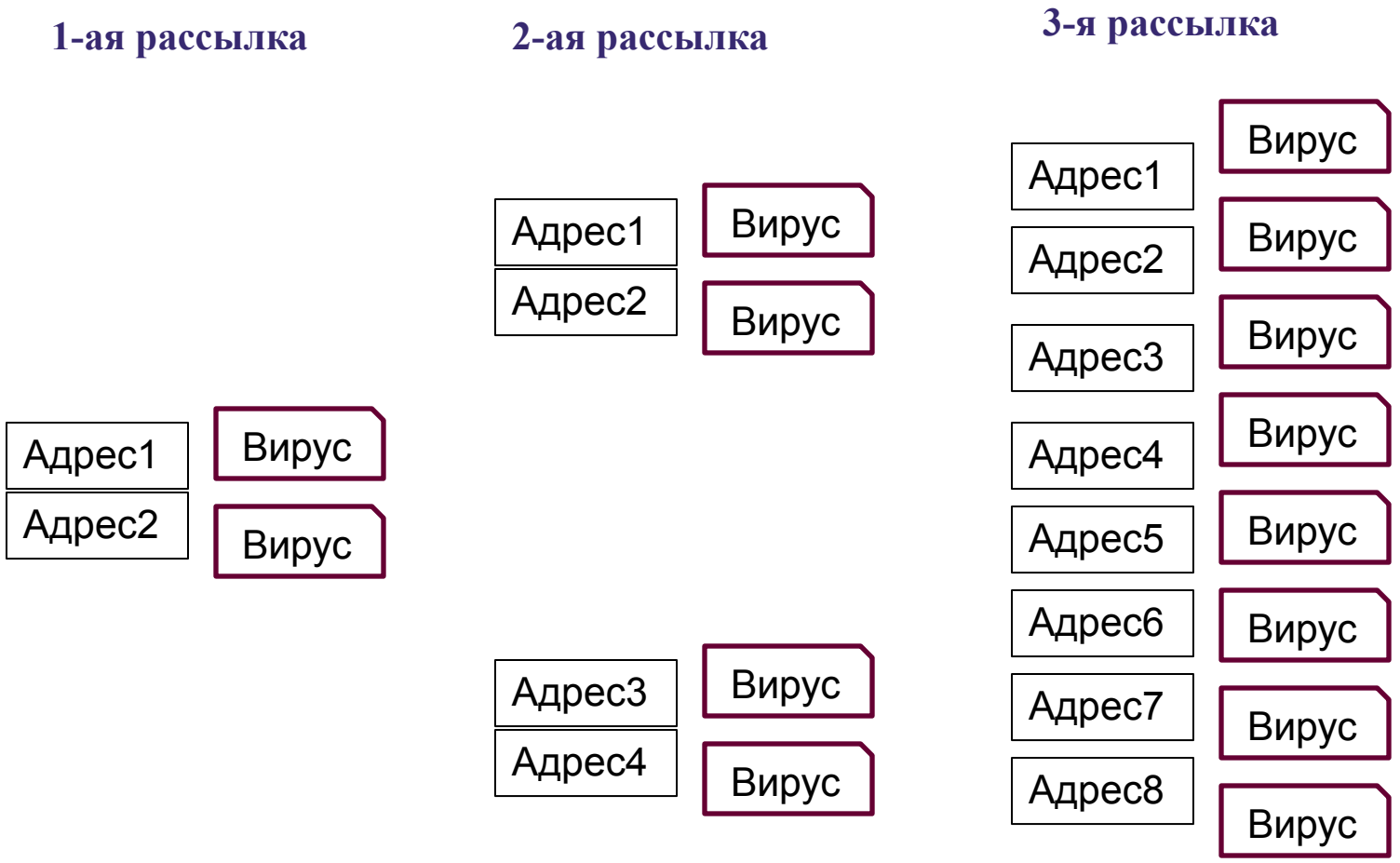
После загрузки зараженного документа и приложения макровирусы постоянно присутствуют в памяти компьютера и могут заражать другие документы.

Профилактическая защита от макровирусов состоит в предотвращении запуска вируса. При открытии документа в приложениях Word и Excel сообщается о присутствии в них макросов и предлагается запустить их загрузку. Выбор запрета на загрузку макросов надежно защитит ваш компьютер от заражения макровирусами, однако отключит и полезные макросы, содержащиеся в документе.

Сетевые вирусы

Сетевые вирусы могут передавать по компьютерным сетям свой программный код и запускать его на компьютерах, подключенных к этой сети; заражение сетевым вирусом может произойти при работе с электронной почтой или при «путешествиях» по Всемирной паутине.

Лавинообразное заражение компьютеров почтовым вирусом



Для защиты от вирусов необходимо соблюдение следующих требований:

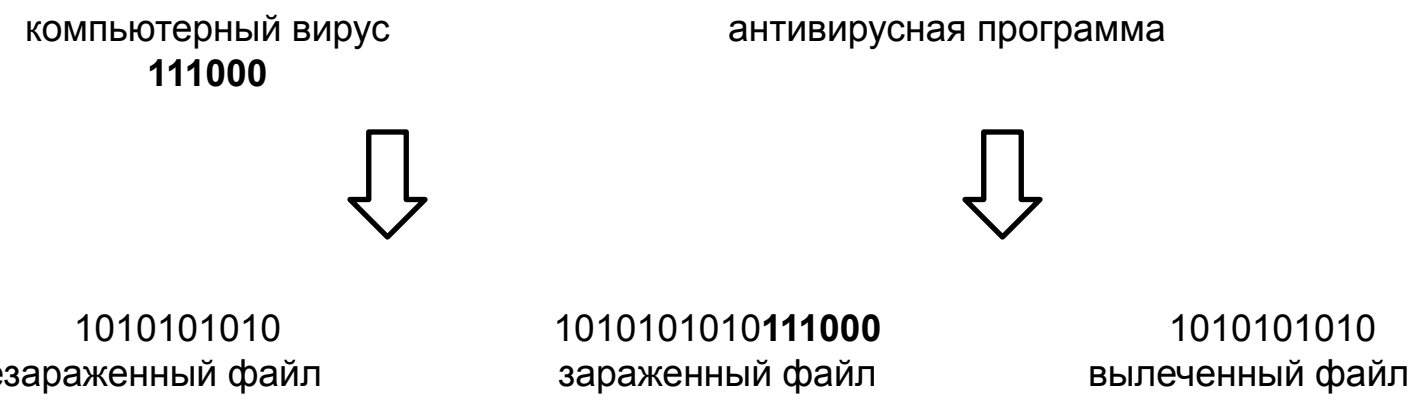
1. Нужно использовать только *лицензионные* дистрибутивные копии программных продуктов, приобретать их следует только у официальных продавцов.
2. Необходимо периодически проверять компьютер на наличие вирусов. Компьютер должен быть оснащен эффективным регулярно используемым и постоянно обновляемым пакетом *антивирусных программ.*
3. Перед считыванием с флэш-памяти и компакт-дисков информации, записанной на других компьютерах, необходимо всегда *проверять их на наличие вирусов.* При переносе на компьютер файлов в архивированном виде после распаковки их также необходимо проверять.
4. Необходимо периодически проверять *жесткие диски* компьютера, запуская антивирусные программы.
5. При работе *в сетях* необходимо использовать антивирусные программы для входного контроля всех файлов, получаемых из компьютерных сетей. Никогда не следует запускать непроверенные файлы, полученные по компьютерным сетям.
6. Необходимо делать регулярное резервное копирование и периодически сохранять файлы, с которыми ведется работа, на внешнем носителе. *Архивные копии* особенно ценной информации лучше дублировать на разных носителях.
7. *Не оставлять диски в кармане дисководов* при включении и перезагрузке операционной системы, чтобы исключить заражение компьютера загрузочными вирусами.

Антивирусные программы

Антивирусные программы используют постоянно обновляемые списки известных вирусов, которые включают название вирусов и их программные коды.

Если антивирусная программа обнаружит компьютерный код вируса в каком-либо файле, то файл считается зараженным вирусом и подлежит лечению, т.е. из него удаляется программный код вируса. Если лечение невозможно, то зараженный файл удаляется целиком.

Заражение файла компьютерным вирусом и его лечение с использованием антивирусной программы



Антивирусные программы

Большинство антивирусных программ сочетает в себе функции постоянной защиты (***антивирусный монитор***) и функции защиты по требованию пользователя (***антивирусный сканер***).

Антивирусный монитор запускается автоматически при старте операционной системы и работает в качестве фонового системного процесса, проверяя на вредоносность совершаемые другими программами действия.

Антивирусный сканер запускается по заранее выбранному расписанию или в произвольной момент пользователем, производит поиск вредоносных программ в оперативной памяти, на жестких, сетевых дисках компьютера.