

# Компьютерные вирусы

Автор :  
Шестакова Марина  
Вячеславовна  
учитель информатики  
МБОУ Лицей № 7



**Компьютерный вирус** – разновидность компьютерных программ, отличительной особенностью которых является способность к **РАЗМНОЖЕНИЮ** (саморепликация). В дополнение к этому вирусы могут без ведома пользователя выполнять прочие произвольные действия, в том числе наносящие вред пользователю и/или компьютеру. По этой причине вирусы относят к вредоносным программам.



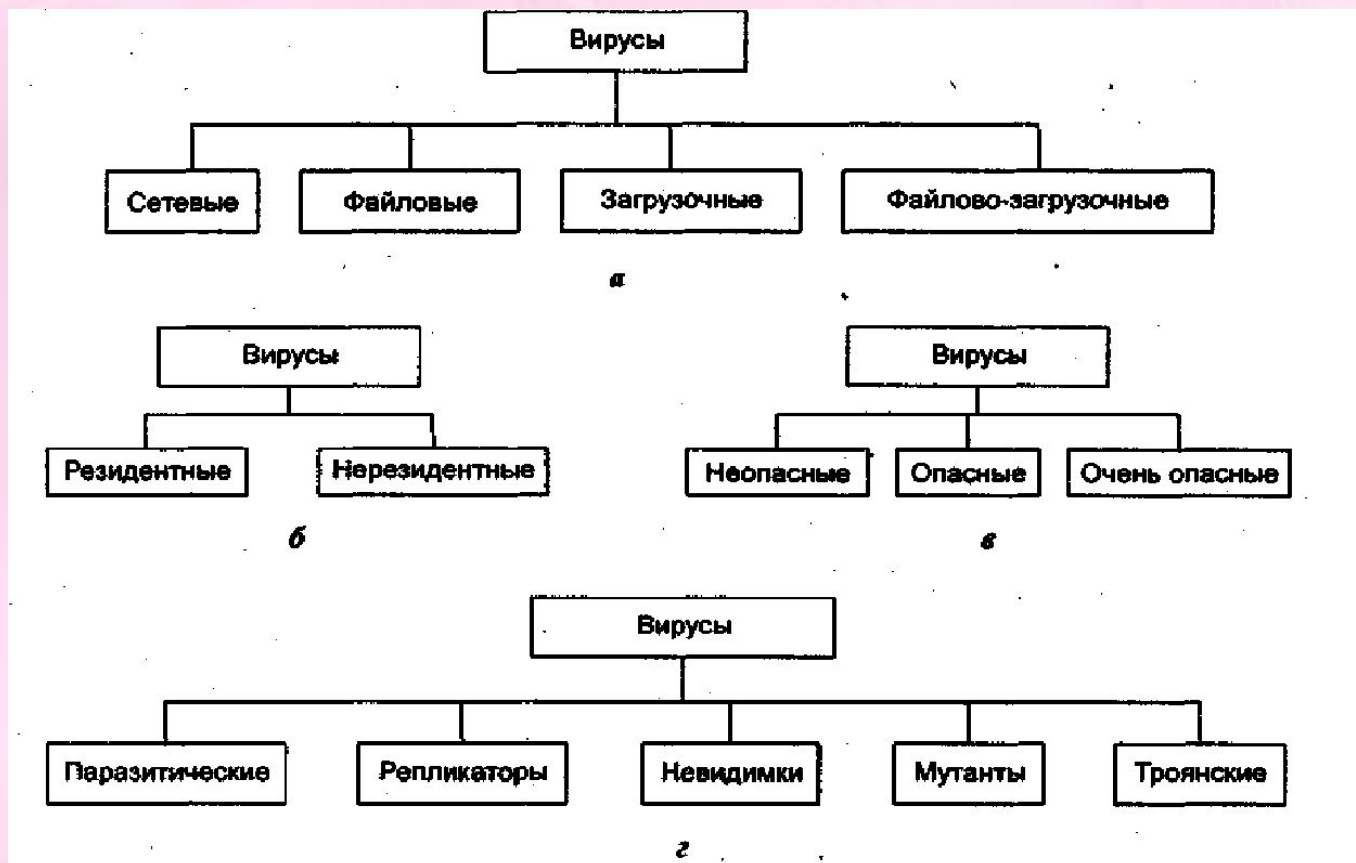
# ОСНОВНЫЕ ПРИЗНАКИ ПРОЯВЛЕНИЯ ВИРУСОВ

- ✓ 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
- ✓ Частые зависания и сбои в работе компьютера
- ✓ 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
- ✓ Частые зависания и сбои в работе компьютера



# Классификация компьютерных вирусов

- ❖ По среде обитания.
- ❖ По способу заражения.
- ❖ По степени воздействия.
- ❖ По особенностям алгоритмов.



# Пути проникновения вирусов

- Глобальная сеть Глобальная сеть Internet
- Электронная почта
- Локальная сеть
- Компьютеры «Общего назначения»
- Пиратское программное обеспечение
- Съёмные накопители



# Windows заблокирован!

Microsoft Security обнаружил нарушения использования сети интернет.  
Причина: Просмотр нелегального ГЕИ и ДЕТСКОГО порно.

## Для разблокировки Windows необходимо:

Пополнить номер абонента Киевстар: +380976674804 на сумму 100 грн.  
Оплатить можно через терминал для оплаты сотовой связи.  
После оплаты, на выданном терминалом чеке, Вы найдёте Ваш  
персональный код разблокировки, который необходимо ввести ниже.

0 1 2 3 4 5 6 7 8 9

Ваш код:

Если в течении 12 часов с момента появления данного сообщения, не будет введён код,  
все данные, включая Windows и bios будут БЕЗВОЗВРАТНО УДАЛЕНЫ! Попытка  
переустановить систему приведёт к нарушениям работы компьютера. Microsoft Corporation.

## КОМПЬЮТЕР ЗАБЛОКИРОВАН!

Ваш компьютер заблокирован за просмотр, копирование и тиражирование видеоматериалов содержащих элементы педофилии и насилия над детьми. Для снятия блокировки Вам необходимо оплатить штраф в размере 500 рублей на номер Билайн 8-965-347-15-40. В случае оплаты суммы равной штрафу либо превышающей ее на фискальном чеке терминала будет напечатан код разблокировки. Его нужно ввести в поле в нижней части окна и нажать кнопку "Разблокировать". После снятия блокировки Вы должны удалить все материалы содержащие элементы насилия и педофилии. Если в течение 12 часов штраф не будет оплачен, все данные на Вашем персональном компьютере будут безвозвратно удалены, а дело будет передано в суд для разбирательства по статье 242 ч.1 УК РФ.

Перезагрузка или выключение компьютера приведет к незамедлительному удалению ВРЕМЕННЫХ данных, включая код операционной системы и BIOS, с невозможностью дальнейшего восстановления.

Статья 242.1. Изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних.  
Изготовление, хранение или перемещение через Государственную границу Российской Федерации в целях распространения, публичной демонстрации или рекламирования либо распространения, публичная демонстрация или рекламирование материалов или предметов с порнографическими изображениями несовершеннолетних, а равно привлечение несовершеннолетних в качестве исполнителей для участия в трансляции, маркировке, порнографического характера лицом, достигшим восемнадцатилетнего возраста, - наказываются лишением свободы на срок от двух до восьми лет с ограничением свободы на срок до одного года либо без такового.

## Windows заблокирован

Для разблокировки необходимо отправить смс с текстом

t7580620000 на номер 3649

введите полученный код

для разблокировки у вас есть

02:59:41

\*Попытка перезагрузить систему может повлечь за собой потерю важной информации и нарушение работы компьютера.



# КАК ЗАЩИТИТЬСЯ ОТ ВИРУСОВ

1. установите на свой ПК современную антивирусную программу.
2. перед просмотром информации принесенной на флэш-карте (дискете) с другого компьютера проверьте носитель антивирусом;
3. после разархивирования архивных файлов сразу проверьте их на вирусы (не все антивирусные программы могут искать вредоносный код в архивах или могут делать это не корректно);
4. периодически проверяйте компьютер на вирусы (если активно пользуетесь Интернетом – запускайте раз в неделю, а то и чаще);
5. как можно чаще делайте резервные копии важной информации (backup);
6. используйте совместно с антивирусной программой файервол (firewall) если компьютер подключен к Интернет;
7. настройте браузер (программа просмотра Интернет страниц – IE, Opera и т.д.) для запрета запуска активного содержимого html-страниц.



# Рынок антивирусных программ очень разнообразен





# Практическая работа.

**Задание №1.** Запустить антивирусную программу на компьютере.

**Задание № 2.** Определить наличие вирусов на компьютере.

**Задание № 3.** Если есть вирусы, определить тип вирусы и способ борьбы с ним.



**СПАСИБО ЗА  
ВНИМАНИЕ**



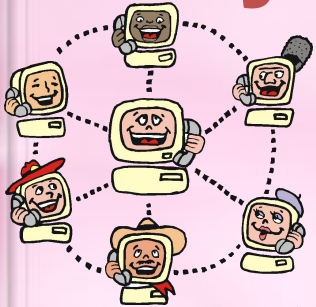
# Пути проникновения вирусов

## Глобальная сеть Интернет

Основным источником вирусов на сегодняшний день является глобальная сеть Internet. Возможно заражение через страницы Интернет ввиду наличия на страницах всемирной паутины различного «активного» содержимого: скриптов, ActiveX-компоненты, Java-апплетов. В этом случае используются уязвимости программного обеспечения установленного на компьютере пользователя, либо уязвимости в ПО владельца сайта, а ничего не подозревающие пользователи зайдя на такой сайт рискуют заразить свой компьютер.



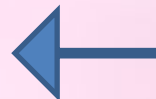
# Пути проникновения вирусов



## Локальные сети

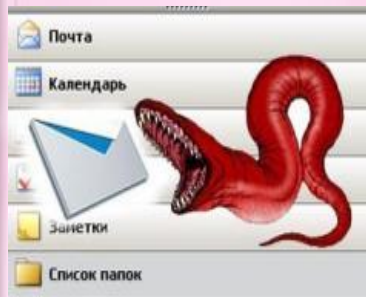
Третий путь «быстрого заражения» — локальные сети. Если не принимать необходимых мер защиты, то зараженная рабочая станция при входе в сеть заражает один или несколько служебных файлов на сервере

На следующий день пользователи при входе в сеть запускают зараженные файлы с сервера, и вирус, таким образом, получает доступ на компьютеры пользователей.



# Пути проникновения вирусов

## Электронная почта



Сейчас один из основных каналов распространения вирусов. Обычно вирусы в письмах электронной почты маскируются под безобидные вложения: картинки, документы, музыку, ссылки на сайты. В некоторых письмах могут содержаться действительно только ссылки, то есть в самих письмах может и не быть вредоносного кода, но если открыть такую ссылку, то можно попасть на специально созданный веб-сайт, содержащий вирусный код. Многие почтовые вирусы, попав на компьютер пользователя, затем используют адресную книгу из установленных почтовых клиентов типа Outlook для рассылки самого себя дальше.



# Пути проникновения вирусов

## Персональные компьютеры «общего пользования»

Опасность представляют также компьютеры, установленные в учебных заведениях. Если один из учащихся принес на своих носителях вирус и заразил какой-либо учебный компьютер, то очередную «заразу» получат и носители всех остальных учащихся, работающих на этом компьютере.

То же относится и к домашним компьютерам, если на них работает более одного человека.



# Пути проникновения вирусов

## Пиратское программное обеспечение

Нелегальные копии программного обеспечения, как это было всегда, являются одной из основных «зон риска». Часто пиратские копии на дисках содержат файлы, зараженные самыми разнообразными типами вирусов

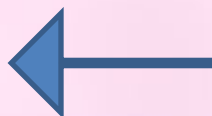


## По среде обитания:

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

**Файловые вирусы** либо различными способами внедряются в выполняемые файлы (наиболее распространенный тип вирусов), либо создают файлы-двойники (компаньон-вирусы), либо используют особенности организации файловой системы (link-вирусы)

**Загрузочные вирусы** записывают себя либо в загрузочный сектор диска (boot-сектор), либо в сектор, содержащий системный загрузчик винчестера (Master Boot Record), либо меняют указатель на активный boot-сектор.

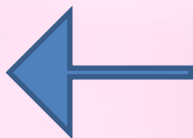




## По способу заражения:

**Резидентные** (такой вирус при инфицировании ПК оставляет в оперативной памяти свою резидентную часть, которая потом перехватывает обращение ОС к объектам заражения и поражает их. Резидентные вирусы живут до первой перезагрузки ПК)

**Нерезидентные** (не заражают оперативную память и могут быть активными ограниченное время)



## По степени воздействия:

**Неопасные** (как правило эти вирусы забивают память компьютера путем своего размножения и могут организовывать мелкие пакости – проигрывать заложенную в них мелодию или показывать картинку);

**Опасные** (эти вирусы способны создать некоторые нарушения в функционировании ПК – сбои, перезагрузки, глюки, медленная работа компьютера и т.д.);

**Очень опасные** (опасные вирусы могут уничтожить программы, стереть важные данные, убить загрузочные и системные области жесткого диска, который потом можно выбросить)



## По особенностям алгоритма:

**Паразитические** (меняют содержимое файлов и секторов диска. Такие вирусы легко вычисляются и удаляются);

**Мутанты** (их очень тяжело обнаружить из-за применения в них алгоритмов шифрования. Каждая следующая копия размножающегося вируса не будет похожа на предыдущую);

**Репликаторы** (вирусы-репликаторы, они же сетевые черви, проникают через компьютерные сети, они находят адреса компьютеров в сети и заражают их);

**Троянский конь** (один из самых опасных вирусов, так как трояны не размножаются, а воруют ценную (порой очень дорогую) информацию – пароли, банковские счета, электронные деньги и т.д.);

**Невидимки** (это трудно обнаружимые вирусы, которые перехватывают обращения ОС к зараженным файлам и секторам дисков и подставляют вместо своего незараженные участки.



## *Использованные материалы*

<http://biblprog.org.ua/ru/antivirus/>

<http://www.nosorogka.ru/antivirusy>

<http://antivibest.ru/page/vidy-computer-virus>

<http://frame3.loadup.ru/6d/1d/1080751.1.3.jpg>

[http://img-fotki.yandex.ru/get/4705/lenivova-elena.1de/0\\_762fc\\_b4656be1\\_XL](http://img-fotki.yandex.ru/get/4705/lenivova-elena.1de/0_762fc_b4656be1_XL)

[http://i.obozrevatel.ua/8/804646/gallery/126190\\_image\\_large.jpg](http://i.obozrevatel.ua/8/804646/gallery/126190_image_large.jpg)

[http://images.brighthouse.com/6b/b/6bbca6a861f8252f3f8b939c9b11b513c2508e17\\_large.jpg](http://images.brighthouse.com/6b/b/6bbca6a861f8252f3f8b939c9b11b513c2508e17_large.jpg)

<http://prosecurity.ucoz.ru/virushto.jpg>

[http://old.mr7.ru/netcat\\_files/840/629/shutterstock\\_8089942\\_\\_580\\_no.jpg](http://old.mr7.ru/netcat_files/840/629/shutterstock_8089942__580_no.jpg)

<http://stepblog.ru/wp-content/uploads/2011/03/Warfare.jpg>

