

# Проектная работа на тему Вирусы антивирусы



# Содержание

1. Что называют компьютерным вирусом?
2. Защищайтесь от вирусов.
3. Как заражаются компьютеры?
3. Как обеспечить надёжную антивирусную защиту?
4. Что такое качественный антивирус?
5. Антивирусные программы.
6. Настройка антивирусных программ.
  - Как правильно настроить.
  - Важнейшие настройки антивирусного ПО.



## **Что называют компьютерным вирусом?**

**Компьютерным вирусом** называется программа, способная создавать свои копии и внедрять их в различные объекты или ресурсы компьютерных систем, сетей и так далее без ведома пользователя. При этом копии сохраняют способность дальнейшего распространения. На сегодняшний день известно 6 основных типов вирусов:

- **файловые**
- **загрузочные**
- **призраки (полиморфные)**
- **невидимки**
- **скрипт-вирусы**
- **макро-вирусы.**

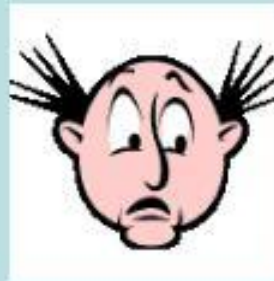
Следует отличать вирусы от вредоносных кодов. К ним относятся Интернет-черви и программы, получившие название «Троянские кони».

*По величине вредных воздействий вирусы можно разделить на:*

• **Неопасные**



• **Опасные**



• **Очень опасные**



*Это вирусы влияние  
которых ограничивается  
уменьшением свободной  
памяти на диске,  
графическими,  
звуковыми и другими  
внешними эффектами.*



*Это вирусы  
которые могут  
привести к сбоям  
и зависаниям при  
работе  
компьютера.*



*Это вирусы активизация которых может привести к потере программ и данных( изменению или удалению файлов или каталогов), форматированию винчестера и так далее.*



## *Защищайтесь от вирусов!*

Вряд ли во всем мире найдется хоть один компьютер, который не получал бы время от времени данные из "внешнего мира": из Интернета, по электронной почте, локальной сети, с CD, с дискет, побывавших на другом компьютере и т.п. Во всех этих случаях существует опасность заражения компьютера вирусом.





## Как заражаются компьютеры?



Хитрые и умные вирусописатели постоянно ищут и находят все новые и новые способы внедрения вредоносных программ на наши компьютеры. Если когда-то вы могли заполучить вирус только одним способом: скопировав через дискету инфицированную программу, то сейчас основной путь распространения вирусов - через Интернет и электронную почту.



## Как заражаются компьютеры?



Хитрые и умные вирусописатели постоянно ищут и находят все новые и новые способы внедрения вредоносных программ на наши компьютеры. Если когда-то вы могли заполучить вирус только одним способом: скопировав через дискету инфицированную программу, то сейчас основной путь распространения вирусов - через Интернет и электронную почту.



# *Как обеспечить надежную антивирусную защиту?*

Защитить компьютер от вирусов может только сам пользователь. Предотвратить заражение компьютера или минимизировать ущерб, если заражение все-таки произошло, можно только правильно и своевременно применяя антивирусные программы. Для надежной защиты своего компьютера выполняйте определённые [правила](#).

- Проверяйте на вирусы все дискеты, CD-RW, ZIP-диски, побывавшие на другом компьютере, все приобретенные CD (особенно и обязательно - с играми!)
- Используйте антивирусные программы известных проверенных фирм, регулярно (в идеале - ежедневно!) обновляйте их базы
- Не выгружайте резидентную часть (монитор) антивирусной программы из оперативной памяти вашего компьютера
- Используйте только программы и данные, полученные из надежных источников. Чаще всего вирусами бывают заражены пиратские копии программ, особенно игр
- Никогда не открывайте файлы, прикрепленные к электронным письмам, пришедшим от неизвестных вам отправителей, и не заходите на сайты, рекламируемые через спам-рассылки (по данным лаборатории Касперского, в настоящее время около 90% вирусов распространяются именно таким образом)



## *Что такое качественный антивирус?*

Хорошая антивирусная программа должна:

- Обеспечивать эффективную защиту в режиме реального времени.
- Позволять проверять все содержимое локальных дисков "по требованию", запуская проверку вручную или автоматически по расписанию.
- Защищать ваш компьютер даже от неизвестных вирусов. Уметь проверять и лечить архивированные файлы.
- Давать возможность регулярно (ежедневно!) обновлять антивирусные базы (через Интернет, с дискет или CD - как вам удобнее).

# АНТИВИРУСНЫЕ ПРОГРАММЫ

- *Полифаги*
- *Ревизоры*
- *Блокировщики*



*Принцип работы полифагов основан на проверке файлов, загрузочных секторов дисков и оперативной памяти и поиске в них известных и новых вирусов.*

*Полифаги могут обеспечивать проверку файлов в процессе их загрузки в оперативную память. Такие программы называются антивирусными мониторами.*

*К достоинствам полифагов относится их универсальность. К недостаткам можно отнести большие размеры используемых ими антивирусных баз данных.*



*Принцип работы ревизоров основан на подсчете контрольных сумм для присутствующих на диске файлов.*

*Недостаток ревизор состоит в том, что они не могут обнаружить вирус новых файлов, поскольку в их базах данных отсутствует информация об этих файлах.*





*Антивирусные Блокировщики – это программы, перехватывающие «вирусоопасные» ситуации и сообщающие об этом пользователю. Наибольшее распространение получили антивирусные блокировщики в BIOS компьютера. К достоинствам блокировщикам относится их способность обнаружить и останавливать вирус на самой ранней стадии его размножения.*



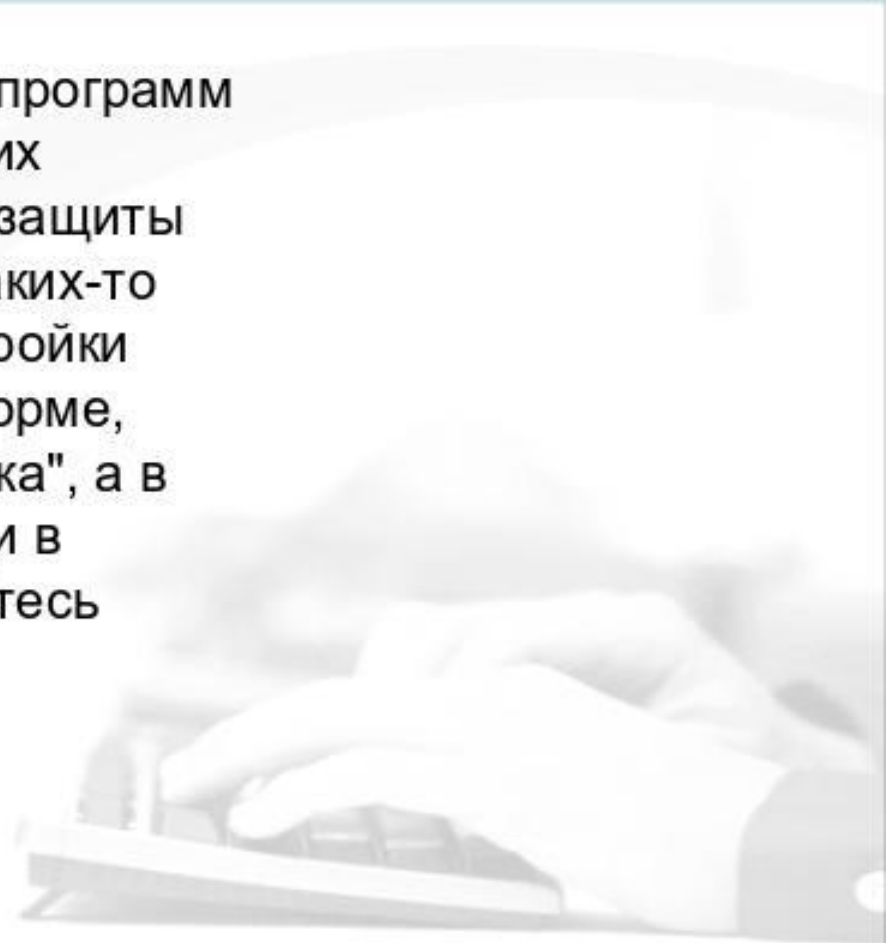
## *Настройка антивирусных программ*

Итак, вы приобрели и установили на свой компьютер хорошую антивирусную программу. Но успокаиваться еще рано - надо ее правильно настроить. Предлагаемые производителями антивирусов настройки по умолчанию далеко не всегда бывают оптимальны.



# Настраиваем антивирусные программы

У каждой из серьезных антивирусных программ есть множество настроек, позволяющих изменять ее режим работы и уровень защиты вашего компьютера. Заметим, что в каких-то программах все описанные ниже настройки удобно собраны на одной экранной форме, вызываемой по пункту меню "Настройка", а в других могут быть запрятаны глубоко и в разных местах интерфейса. Постарайтесь отыскать и проверить их все.



# важнейшие Настройки антивирусного ПО.

**Постоянная защита.** Обычно постоянная защита бывает включена по умолчанию. Проверьте это и без крайней необходимости не выключайте этот режим.

**Проверять все файлы.** Для повышения уровня защищенности лучше включить этот режим. Очень часто вирусы спокойно ждут своего часа в заархивированных файлах, нередко вредоносные программы распространяются в файлах с измененными расширениями.



Обычно имеется возможность установить один из следующих режимов:

- *только отчет;*
- *лечить зараженные файлы; если вылечить невозможно:*
  - *удалять зараженные файлы;*
  - *переименовывать, перемещать зараженные файлы;*
  - *запрашивать пользователя о дальнейших действиях*
- *сразу удалять зараженные файлы.*

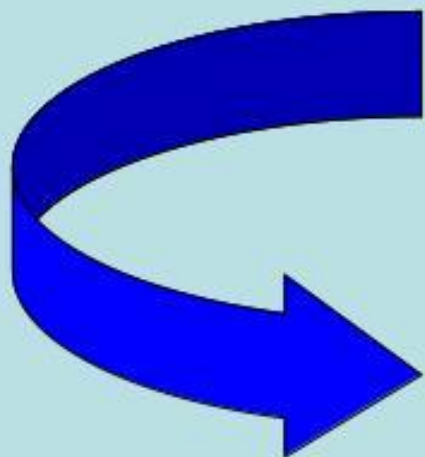
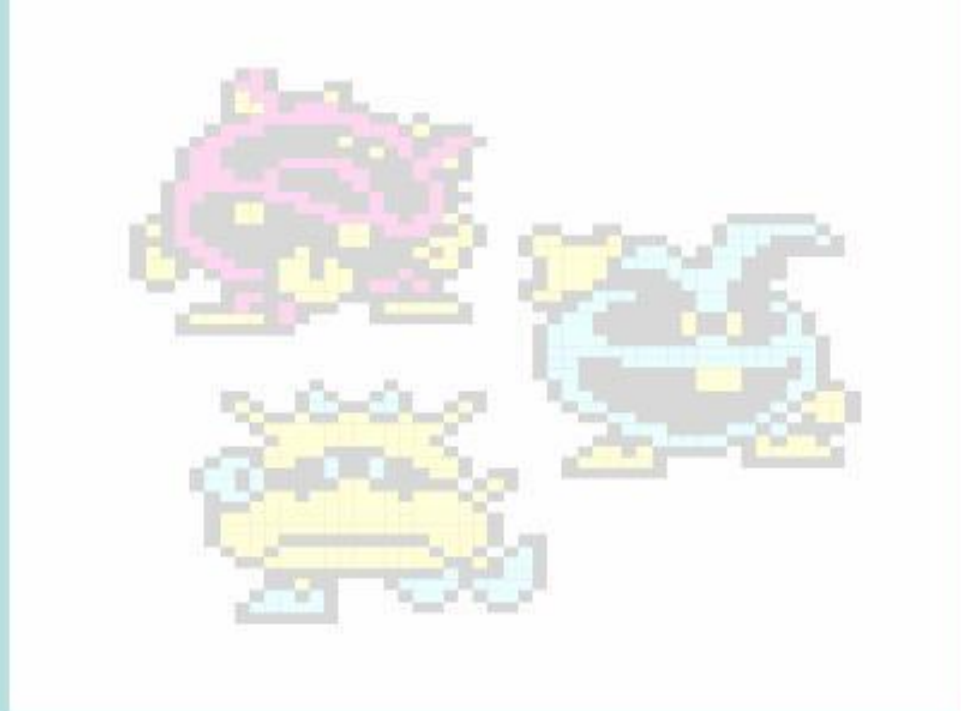


**Автоматическое сканирование.** Если ваш компьютер включен постоянно, то рекомендуется запускать ежедневно в удобное для вас время, например, ночью, сразу после обновления программы и антивирусных баз. Если же пользуетесь компьютером немного, а в Интернет заходите еще реже, достаточно запускать полное сканирование вручную раз в неделю.

**Автоматическое обновление программы и антивирусных баз.** Эта опция позволяет автоматически скачивать через Интернет с сайта разработчика все последние изменения. Рекомендуем включить и установить в расписании "ежедневно" в удобное для вас время, например, ночью.



*Если вы не будите выполнять  
этих требований, то возможно  
это.....*





Установка программы Антивирус Касперского Personal 5.0



## Добро пожаловать в мастер установки программы Антивирус Касперского Personal 5.0

Эта программа установит Антивирус Касперского Personal 5.0 на ваш компьютер.

Перед началом установки рекомендуется закрыть все работающие приложения. Это позволит программе установки обновить системные файлы без перезагрузки компьютера.

Нажмите на кнопку "Далее" для продолжения установки программы.

Далее >

Отмена