

# Компьютерные вирусы и антивирусные программы



**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.

Компьютерные вирусы, как таковые, впервые появились в 1986 году, хотя исторически возникновение вирусов тесно связано с идеей создания самовоспроизводящихся программ. Одним из "пионеров" среди компьютерных вирусов считается вирус "Brain", созданный пакистанским программистом по фамилии Алви. Только в США этот вирус поразил свыше 18 тыс. компьютеров. В начале эпохи компьютерных вирусов разработка вирусоподобных программ носила чисто исследовательский характер, постепенно превращаясь на откровенно вражеское отношение к пользователям безответственных, и даже криминальных "элементов".

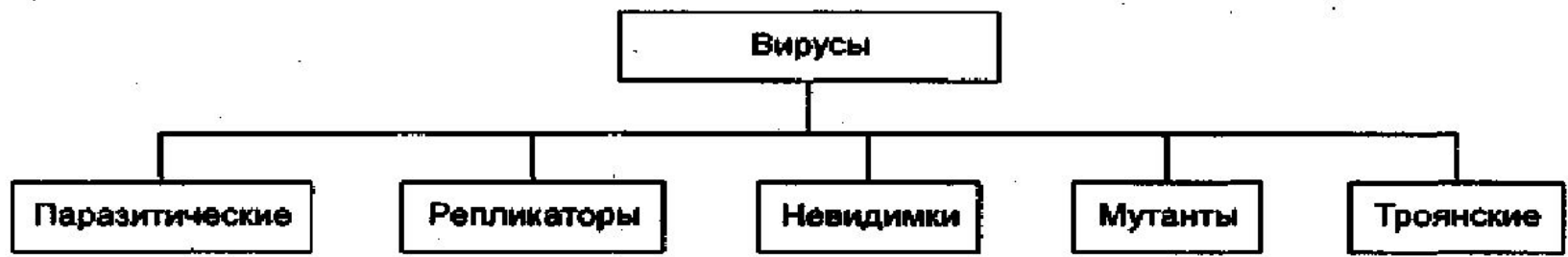
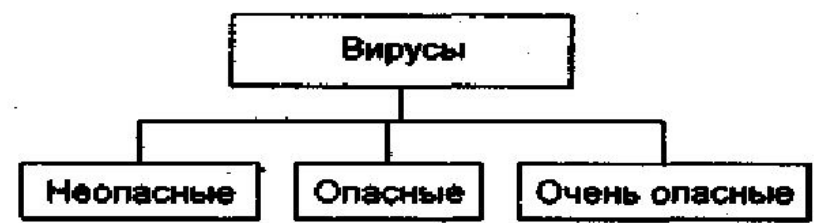


# Основные признаки проявления вирусов

- 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
- Неожиданное значительное увеличение количества файлов на диске
- Существенное уменьшение размера свободной оперативной памяти
- Вывод на экран непредусмотренных сообщений или изображений
- Подача непредусмотренных звуковых сигналов

# Классификация компьютерных вирусов

а - по среде обитания;      б - по способу заражения;  
в - по степени воздействия;      г - по особенностям алгоритмов



## 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.

# ПУТИ ПРОНИКНОВЕНИЯ ВИРУСОВ

---

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

# ПУТИ ПРОНИКНОВЕНИЯ ВИРУСОВ

## Глобальная сеть Интернет

Основным источником вирусов на сегодняшний день является глобальная сеть Internet.

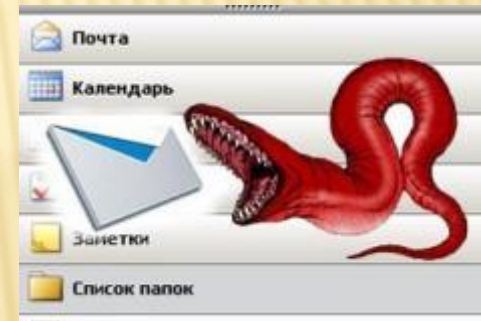
Возможно заражение через страницы Интернет ввиду наличия на страницах всемирной паутины различного «активного» содержимого: скриптов, ActiveX-компоненты, Java-апплетов. В этом случае используются уязвимости программного обеспечения, установленного на компьютере пользователя, либо уязвимости в ПО владельца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



# ПУТИ ПРОНИКНОВЕНИЯ ВИРУСОВ

## 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.

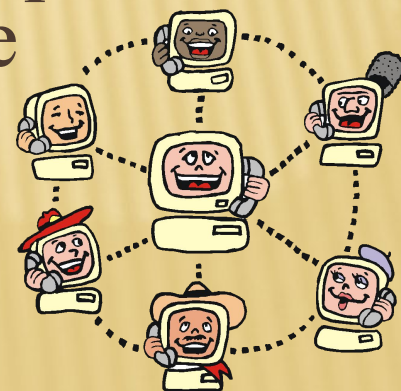


# ПУТИ ПРОНИКНОВЕНИЯ ВИРУСОВ

## 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

## **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» получают и носители всех остальных учащихся, работающих на этом компьютере.

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

## **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.



# ПУТИ ПРОНИКНОВЕНИЯ ВИРУСОВ

---

## Ремонтные службы

Достаточно редко, но до сих пор вполне реально заражение компьютера вирусом при его ремонте или профилактическом осмотре. Ремонтники — тоже люди, и некоторым из них свойственно наплевательское отношение к элементарным правилам компьютерной безопасности.

## Съемные накопители

В настоящее время большое количество вирусов распространяется через съёмные накопители, включая цифровые фотоаппараты, цифровые видеокамеры, цифровые плееры (MP3-плееры), сотовые телефоны.

**Троянский конь** - это вредоносное программное обеспечение, которое, без ведома владельца персонального компьютера может предоставить доступ к его данным или по определенному адресу выслать вашу персональную информацию. Кроме этого, вы даже себе и подумать не можете, что эта программа является "трояном" подобного рода законспирированы под приложения.





**Trojan.Winlock (Винлокер)** — семейство вредоносных программ блокирующих или затрудняющих работу с операционной системой, и требующих перечисление денег злоумышленникам за восстановление работоспособности компьютера. Впервые появились в конце 2007 года. Широкое распространение вирусы-вымогатели получили зимой 2009—2010 года, по некоторым данным оказались заражены миллионы компьютеров, преимущественно среди пользователей русскоязычного Интернета. Второй всплеск активности такого вредоносного ПО пришелся на май 2010 года.

---

# Windows заблокирован!

Microsoft Security обнаружил нарушения использования сети интернет.  
Причина: Просмотр нелицензионного ГЕЙ 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	очистить
Ваш код:										ВХОД В СИСТЕМУ

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 ВСЕХ данных, включая код операционной системы и BIOS, с невозможностью дальнейшего восстановления.

Разблокировать

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 распространение, публичная демонстрация или рекламирование материалов или предметов с порнографическими изображениями несовершеннолетних, а равно привлечение несовершеннолетних в качестве исполнителей для участия в зрелищных мероприятиях 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

т7580620000 на номер 3649

введите полученный код

Активация

для разблокировки у вас есть

02:59:41

\*Попытка переустановить систему может привести к потере важной информации  
и нарушению работы компьютера.

**Trojan.Winlock** условно можно разделить на 3 типа, в зависимости от того, насколько они затрудняют работу для пользователя.

**1 тип** — это баннеры или порноинформеры, появляющиеся только в окне браузера. Наиболее легко удаляемый тип. Обычно они выдают себя за дополнительные плагины или надстройки для браузера.

**2 тип** — это баннеры, которые остаются на рабочем столе после закрытия браузера и при этом закрывают большую его часть. Но у пользователей обычно остаётся возможность открывать другие программы, в том числе диспетчер задач и редактор реестра.

**3 тип** — это наиболее трудноудаляемый тип баннеров, которые закрывают практически весь рабочий стол, блокируют запуск диспетчера задач, редактора реестра, а также загрузку в безопасном режиме. Некоторые разновидности полностью блокируют клавиатуру, предоставляя пользователю лишь цифровые клавиши из своего «интерфейса», и рабочую мышь для ввода кода.

Троянец заблокировал Windows и требует отправить SMS? Не надо платить преступнику!  
Используйте **бесплатно** разблокировщик **Dr.Web от Trojan.Winlock**

### Если Ваш компьютер инфицирован

Компания «Доктор Веб» не несет ответственности за моральный, а также иной вред, (в т.ч. причиненный чести, достоинству и деловой репутации) причиненный просмотром, либо использованием материалов (текстовых или изобразительных) размещенных в данном разделе.

Если **Вам** точно известно имя троянской программы, которой инфицирован Ваш ПК. Попробуйте получить код разблокировки, выбрав название троянца.

Trojan.Winlock 87 Win+D to unlock



Введите номер и текст сообщения, которое предлагается отправить:

Номер:  Текст:

Найти код

Если **Вы не знаете точное имя троянской программы**, попробуйте найти похожий скриншот. Под скриншотом будет написано название троянца.

**Внимание!** Некоторые варианты вируса проявляются одинаково, так что, если указанный код разблокировки не подошел, попробуйте поискать похожие изображения.



- [Бесплатная разблокировка Windows](#)
- [Инструкция по разблокировке Windows](#)
- [Пришлите код разблокировки ИМХО](#)
- [Ты можешь помочь](#)
- [Правовой уголок](#)
- [Горячая лента угроз](#)
- [Бесплатная лечащая утилита Dr.Web CureIt!](#)  
Даже если систему удалось разблокировать, необходимо удалить из нее следы пребывания троянца. Это можно сделать с помощью Dr.Web CureIt! В противном случае сохранится вероятность блокировки работы отдельных программ.
- [Сказочка](#)


# СЛУЖБА ТЕХНИЧЕСКОЙ ПОДДЕРЖКИ

Лаборатории Касперского

Выберите язык:  

[Начало](#) / [Борьба с вредоносными программами](#) / [Удаление баннера с рабочего стола, разблокировка Windows](#)

-  **Защита для домашних пользователей**  
1 - 5 компьютеров
-  **Защита для малого офиса**  
5 - 10 компьютеров
-  **Защита для корпоративных пользователей**  
5 - 1000+ рабочих станций
-  **Борьба с вредоносными программами**  
Как выключить компьютер...
  - [Kaspersky Virus Removal Tool 2011](#)
  - [Удаление баннера с рабочего стола, разблокировка Windows](#)
  - [Утилиты для удаления вирусов](#)
  - [Компьютерная безопасность](#)
  - [Способы удаления вирусов](#)
  - [Rogue security software](#)
  - [Kaspersky Rescue Disk 10](#)

 **Вспомогательные сервисы**  
Дополнительная онлайн помощь

 **Обучение в Лаборатории Касперского**  
Пройдите обучение и получите сертификат специалиста в области антивирусной защиты

 **О поддержке продуктов Лаборатории Касперского**  
Дополнительная информация о поддержке продуктов



Предлагаем вам подписаться на рассылку новостей о публикации новых статей в Базе знаний.

[Выбрать рассылки](#)

 **Поиск:**

[Как искать?](#) **Номер статьи:**  [Найти](#)



## Удаление баннера с рабочего стола, разблокировка Windows

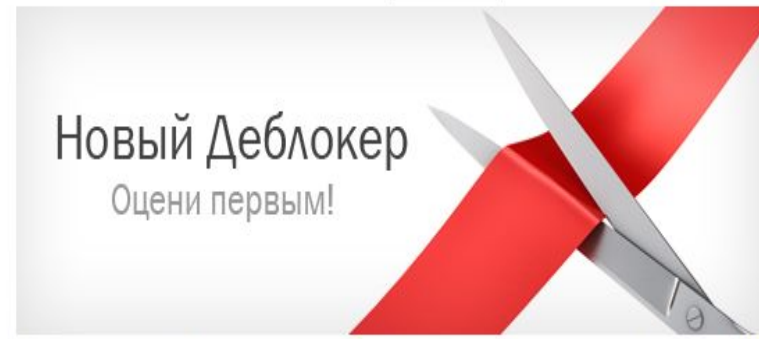
Номер телефона или счета

[Получить код разблокировки](#)



Доступно в **App Store**

Бесплатно



Бесплатный сервис Deblocator поможет **убрать баннер с рабочего стола, разблокировать Windows** без перевода денег на счет, вернуть зашифрованные вирусом файлы.

Чтобы удалить баннер, введите номер телефона (например, 89854120769, 3116) или счета (например, 9636256259). [Подробная инструкция.](#)

После удаления баннера проверьте компьютер на наличие вирусов с помощью бесплатной утилиты [Kaspersky Virus Removal Tool](#).

Для предотвращения заражения вашего компьютера рекомендуем установить Kaspersky Internet Security 2012. [Скачать бесплатную 30-дневную версию.](#)

**Лаборатория Касперского предупреждает:** в данном разделе публикуется информация третьих лиц (коды разблокировки, скриншоты и прочее), которая может содержать неформативную лексику, оскорбительные или иные выражения, противоречащие общественным интересам, принципам гуманности и морали. Вы

**Полезные ссылки**

- [Как использовать Deblocator](#)
- [Задать вопрос на форуме](#)
- [Deblocator на вашем сайте](#)
- [Обратиться за помощью в Вирусную лабораторию](#)
- [Скачать Kaspersky Internet Security 2012 \(бесплатная 30-дневная версия\)](#)

## 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.





Microsoft<sup>®</sup>  
Security Essentials



**СПАСИБО ЗА  
ВНИМАНИЕ**

---