

# **Компьютерные вирусы и антивирусные программы**

## Компьютерные вирусы и антивирусные программы



Борьбой с компьютерными вирусами профессионально занимаются сотни (или тысячи) специалистов в десятках компаний. Компьютерные вирусы были и остаются одной из наиболее распространенных причин потери информации. Известны случаи, когда вирусы блокировали работу организаций и предприятий.

Более того, был зафиксирован случай, когда компьютерный вирус стал причиной гибели человека - в одном из госпиталей Нидерландов пациент получил летальную дозу морфия по той причине, что компьютер был заражен вирусом и выдавал неверную информацию.

# Феномен компьютерных вирусов

Наше столетие, несомненно, является одним из поворотных этапов в жизни человечества.

Человечество захвачено техникой и уже вряд ли откажется от удобств, предоставляемых ею (мало кто пожелает поменять современный автомобиль на гужевую тягу). Уже забыта обычная почта с ее конвертами и почтальонами - вместо нее пришла электронная почта.

Не представляется уже существование современного общества без компьютера, способного многократно повысить производительность труда и доставить любую мыслимую информацию.

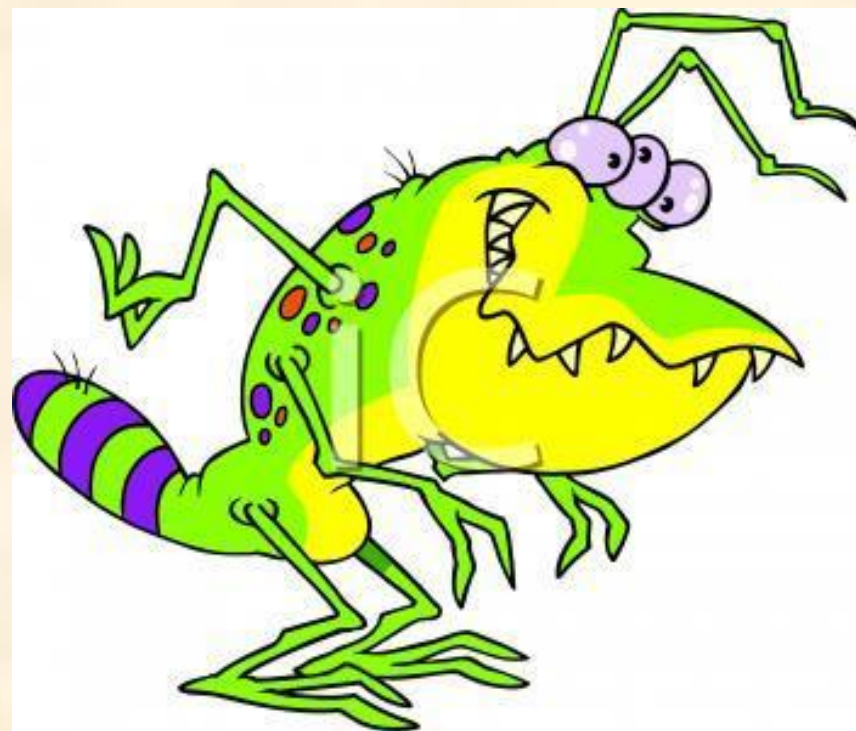
- Сегодня факт возникновения компьютерных вирусов поставлен в один ряд с исследованиями космоса, атомного ядра и развитием электроники.



- Во-первых, компьютерные вирусы - это серьезная и довольно заметная проблема, возникновения которой никто не ожидал. Даже всевидящие **фантасты-футурологи** прошлого не говорят об этом ничего, нет ни одного пророчества, посвященного компьютерным вирусам. Тема вируса в произведениях писателей появилась уже после того, как первый реальный вирус поразил свой первый компьютер.
- Во-вторых, компьютерные вирусы - это первая вполне удачная **попытка создать жизнь**. Попытка удачная, но нельзя сказать, что полезная - современные компьютерные «микроорганизмы» более всего напоминают насекомых-вредителей, приносящих только проблемы и неприятности. Но все - таки - жизнь, поскольку компьютерным вирусам присущи все атрибуты живого - способность к размножению, приспособляемости к среде, движению и т.д. (естественно, только в пределах компьютеров - так же как все вышесказанное верно для биологических вирусов в пределах клеток организма). Более того, существуют «двуполые» вирусы (вирус RMNS), а примером «многоклеточности» могут служить, например, макро-вирусы, состоящие из нескольких независимых макросов.
- И в-третьих, борьба с компьютерными вирусами является **борьбой человека с человеческим же разумом**. Эта борьба является борьбой умов, поскольку задачи, стоящие перед вирусологами, ставят такие же люди. Одни придумывают новый вирус - а другим с ним разбираться.

# Что такое компьютерный вирус

Объяснений,  
что такое  
компьютерный  
вирус, можно  
привести  
несколько.



# Что такое компьютерный вирус

## Объяснение бытовое

Рассмотрим работу клерка, занимающегося исключительно с бумагами (идея такого объяснения принадлежит Д.Н.Лозинскому, одному из известнейших «докторов»). Представим себе аккуратного клерка, который приходит на работу к себе в контору и каждый день обнаруживает у себя на столе стопку листов бумаги со списком заданий, которые он должен выполнить за рабочий день.

Клерк берет верхний лист, читает указания начальства, пунктуально их выполняет, выбрасывает «отработанный» лист в мусорное ведро и переходит к следующему листу.

Предположим, что некий злоумышленник тайком прокрадывается в контору и подкладывает в стопку бумаг лист, на котором написано следующее:.....

# Объяснение бытовое

«Переписать этот лист два раза и положить копии в стопку заданий соседей»

Что сделает клерк? Дважды перепишет лист, положит его соседям на стол, уничтожит оригинал и перейдет к выполнению второго листа из стопки, т.е. продолжит выполнять свою настоящую работу.

Что сделают соседи, являясь такими же аккуратными клерками, обнаружив новое задание? То же, что и первый: перепишут его по два раза и раздадут другим клеркам.

Итого, в конторе бродят уже четыре копии первоначального документа, которые и дальше будут копироваться, и раздаваться на другие столы.

***Примерно так же работает и компьютерный вирус, только стопками бумаг-указаний являются программы, а клерком – компьютер***





# Вирус «Jerusalem»

Хорошо известен вирус «Jerusalem» (другое название - «Time»).

Кстати, на примере клерка очень хорошо видно, почему в большинстве случаев нельзя точно определить, откуда в компьютере появился вирус. Все клерки имеют одинаковые (с точностью до почерка) КОПИИ, но оригинал-то с почерком злоумышленника уже давно в корзине!

# Научное определение

Первые исследования саморазмножающихся искусственных конструкций проводились в середине нынешнего столетия. В работах фон Неймана, Винера и других авторов дано определение и проведен их математический анализ.

Термин «компьютерный вирус» впервые употребил сотрудник Лехайского университета (США) **Ф.Козн** в **1984 г.** на 7-й конференции по безопасности информации, проходившей в США.

С тех пор прошло немало времени, однако строгого определения, что же такое компьютерный вирус, так и не дано, несмотря на то, что попытки дать такое определение предпринимались неоднократно.

# Три аксиомы:

Во-первых, **вирусы не возникают сами собой** - их создают нехорошие программисты-хакеры и рассылают по сети передачи данных или подкидывают на компьютеры знакомых.

Во-вторых: **вирус не может сам собой появиться на Вашем компьютере** - либо его подсунули на дискетах или даже на компакт-диске, либо Вы его случайно скачали из компьютерной сети, либо вирус жил у Вас в компьютере с самого начала, либо (что самое ужасное) программист-хакер живет у Вас в доме.

В третьих: **компьютерные вирусы заражают только компьютер** и ничего больше, поэтому не надо бояться - через клавиатуру и мышь они не передаются.



# **Компьютерные вирусы**

**- это класс программ способных к саморазмножению и самомодификации в работающей вычислительной среде и вызывающих нежелательные для пользователей действия.**

*Действия могут выражаться в нарушении работы программ, выводе на экран посторонних сообщений или изображений, порче записей, файлов, дисков, замедлении работы ЭВМ и др.*

## Основная трудность, возникающая при попытках дать строгое определение вируса заключается

**В том что** практически все отличительные черты вируса (внедрение в другие объекты, скрытность, потенциальная опасность и проч.) либо присущи другим программам, которые никоим образом вирусами не являются, либо существуют вирусы, которые не содержат указанных выше отличительных черт (за исключением возможности распространения).

# Классификация компьютерных вирусов

Вирусы можно разделить на классы по следующим основным признакам:

- среда обитания;
- операционная система (ОС);
- особенности алгоритма работы;
- деструктивные возможности.

# По **СРЕДЕ ОБИТАНИЯ** вирусы можно разделить на:

- файловые;
- загрузочные;
- макро;
- сетевые.



- **Файловые вирусы** заражают выполняемые файлы (это наиболее распространенный тип вирусов), либо создают файлы-двойники (компаньон - вирусы), либо используют особенности организации файловой системы (link-вирусы).
- **Загрузочные вирусы** заражают загрузочные сектора дисков (boot-сектор), либо главную загрузочную запись (Master Boot Record), либо меняют указатель на активный boot-сектор.
- **Макро-вирусы** - разновидность файловых вирусов встраивающиеся в документы и электронные таблицы популярных редакторов.
- **Сетевые вирусы** используют для своего распространения протоколы или команды компьютерных сетей и электронной почты.

Существует большое количество сочетаний - например, файлово-загрузочные вирусы, заражающие как файлы, так и загрузочные сектора дисков. Такие вирусы, как правило, имеют довольно сложный алгоритм работы, часто применяют оригинальные методы проникновения в систему. Другой пример такого сочетания - сетевой макро-вирус, который не только заражает редактируемые документы, но и рассылает свои копии по электронной почте.



# Заражаемая ОПЕРАЦИОННАЯ СИСТЕМА

вернее, ОС, объекты которой подвержены заражению, является вторым уровнем деления вирусов на классы.

Каждый файловый или сетевой вирус заражает файлы какой-либо одной или нескольких ОС - DOS, Windows, Win/NT, OS/2 и т.д. Макровирусы заражают файлы форматов Word, Excel, Office.

Загрузочные вирусы также ориентированы на конкретные форматы расположения системных данных в загрузочных секторах дисков.

Среди  
**ОСОБЕННОСТЕЙ АЛГОРИТМА РАБОТЫ**  
**ВИРУСОВ ВЫДЕЛЯЮТСЯ СЛЕДУЮЩИЕ ПУНКТЫ:**

- резидентность;
- использование стелс - алгоритмов;
- самошифрование и полиморфичность;
- использование нестандартных приемов.



# По ДЕСТРУКТИВНЫМ ВОЗМОЖНОСТЯМ

## вирусы можно разделить на

- **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 и графическими, звуковыми и пр. эффектами;
- **опасные вирусы**, которые могут привести к серьезным сбоям в работе компьютера;
- **очень опасные**, в алгоритм работы которых заведомо заложены процедуры, которые могут привести к потере программ, уничтожить данные, стереть необходимую для работы компьютера информацию, записанную в системных областях памяти

# Защита от компьютерных вирусов



**резервирование** (копирование FAT, ежедневное ведение архивов измененных файлов);

**профилактика** (раздельное хранение вновь полученных программ и эксплуатирующихся, хранение неиспользуемых программ в архивах, использование специального диска для записи новых программ);

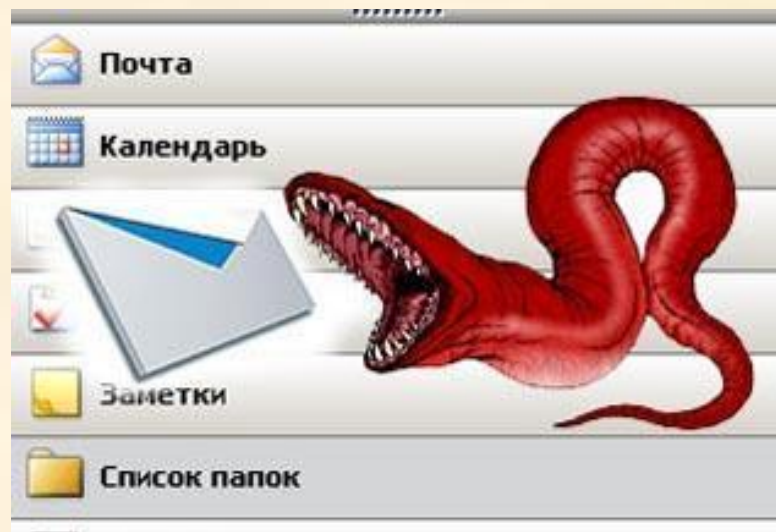
**ревизия** (анализ вновь полученных программ специальными средствами и их запуск в контролируемой среде, систематическая проверка *BOOT*-сектора используемых дискет и содержимого системных файлов (прежде всего *command.com*) и др.);

**фильтрация** (использование специальных сервисных программ для разбиения диска на зоны с установленным атрибутом *read only*);

**вакцинация** (специальная обработка файлов, дисков, каталогов, запуск специальных резидентных программ-вакцин, имитирующих сочетание условий, которые используются данным типом вируса для определения, заражена уже программа, диск, ЭВМ или нет, т.е. обманывающих вирус);

**лечение** (дезактивацию конкретного вируса с помощью специальной программы или восстановление первоначального состояния программ путем удаления всех экземпляров вируса в каждом из зараженных файлов или дисков).

Как говорят в медицине  
болезнь легче предупредить,  
чем лечить.



# Антивирусные программы

- **Антивирусные программы** предназначены для предотвращения заражения компьютера вирусом и ликвидации последствий заражения. В зависимости от назначения и принципа действия различают следующие антивирусные программы:
  - **сторожа или детекторы** – предназначены для обнаружения файлов зараженных известными вирусами, или признаков указывающих на возможность заражения.
  - **доктора** – предназначены для обнаружения и устранения известных им вирусов, удаляя их из тела программы и возвращая ее в исходное состояние. Наиболее известными представителями являются Dr.Web, AidsTest, Norton Anti Virus.
  - **ревизоры** – они контролируют уязвимые и поэтому наиболее атакуемые компоненты компьютера, запоминают состояние служебных областей и файлов, а в случае обнаружения изменений сообщают пользователю.
  - **резидентные мониторы или фильтры** – постоянно находятся в памяти компьютера для обнаружения попыток выполнить несанкционированные действия. В случае обнаружения подозрительного действия выводят запрос пользователю на подтверждение операций.
  - **вакцины** – имитируют заражение файлов вирусами. Вирус будет воспринимать их зараженными и не будет внедряться. Чаще всего используются Aidstest Лозинского, Drweb, Dr.Solomon.

# Полезные советы

1. Применение антивирусных программ
2. Необходимо периодическое обновление антивирусных программ
3. Проверка информации поступающей из вне.
4. Периодическая проверка всего компьютера.
5. Осторожность с незнакомыми файлами. Их действия могут не соответствовать названию.





Среди антивирусных программных продуктов можно отметить, прежде всего, пакеты:

- **Norton Antivirus (Symantec),**
- **Vims Scan (McAfee),**
- **Dr.Solomon AV Toolkit (S&S IntL),**
- **AntiVirus (IBM),**
- **InocuLAN (Computer Associates)**
- **Лаборатория Касперского.**

Данные программные продукты отвечают требованиям ICISA, отслеживая 300 наиболее распространённых и хотя бы 9 из каждых 10 остальных вирусов, обладают функциями проверки на вирусы и удаления их в реальном времени, отключения заражённых рабочих станций от сети, определения источника заражения, проверки сжатых файлов в режимах сканирования и реального времени.

Кроме того, эти программы позволяют проводить удаленное сканирование ПК с Windows NT и ведут единый журнал событий.

# ИСТОЧНИКИ

- <http://startnewlife.ru/wp-content/uploads/2011/09/virus.jpg>
- [http://gansik.ru/wp-content/uploads/2011/09/first\\_computer\\_virus\\_001.jpg](http://gansik.ru/wp-content/uploads/2011/09/first_computer_virus_001.jpg)
- <http://www.mobile-inform.com/phones/edneo/qxz7047/WMvirus/virus.jpg>
- <http://www.jagannath.ru/upload/iblock/fd0/virus.jpg>
- [http://sovetuyzeru.ru/wp-content/uploads/1086\\_picture\\_of\\_a\\_weird\\_looking\\_computer\\_virus\\_with\\_three\\_eyes.jpg](http://sovetuyzeru.ru/wp-content/uploads/1086_picture_of_a_weird_looking_computer_virus_with_three_eyes.jpg)
- <http://burnlife.ru/wp-content/76369ac5dc46.jpg>
- <http://img15.nnm.ru/f/7/5/8/9/ae9c1748b28121e92bc530cf4ee.jpg>
- <http://clip2net.com/clip/m10803/1275421068-clip-23kb.jpg>
- [http://sp.sz.ru/virusi\\_.html](http://sp.sz.ru/virusi_.html)
- <http://www.google.ru/url?sa=t&source=web&cd=1&ved=0CBsQFjAA&url=http>