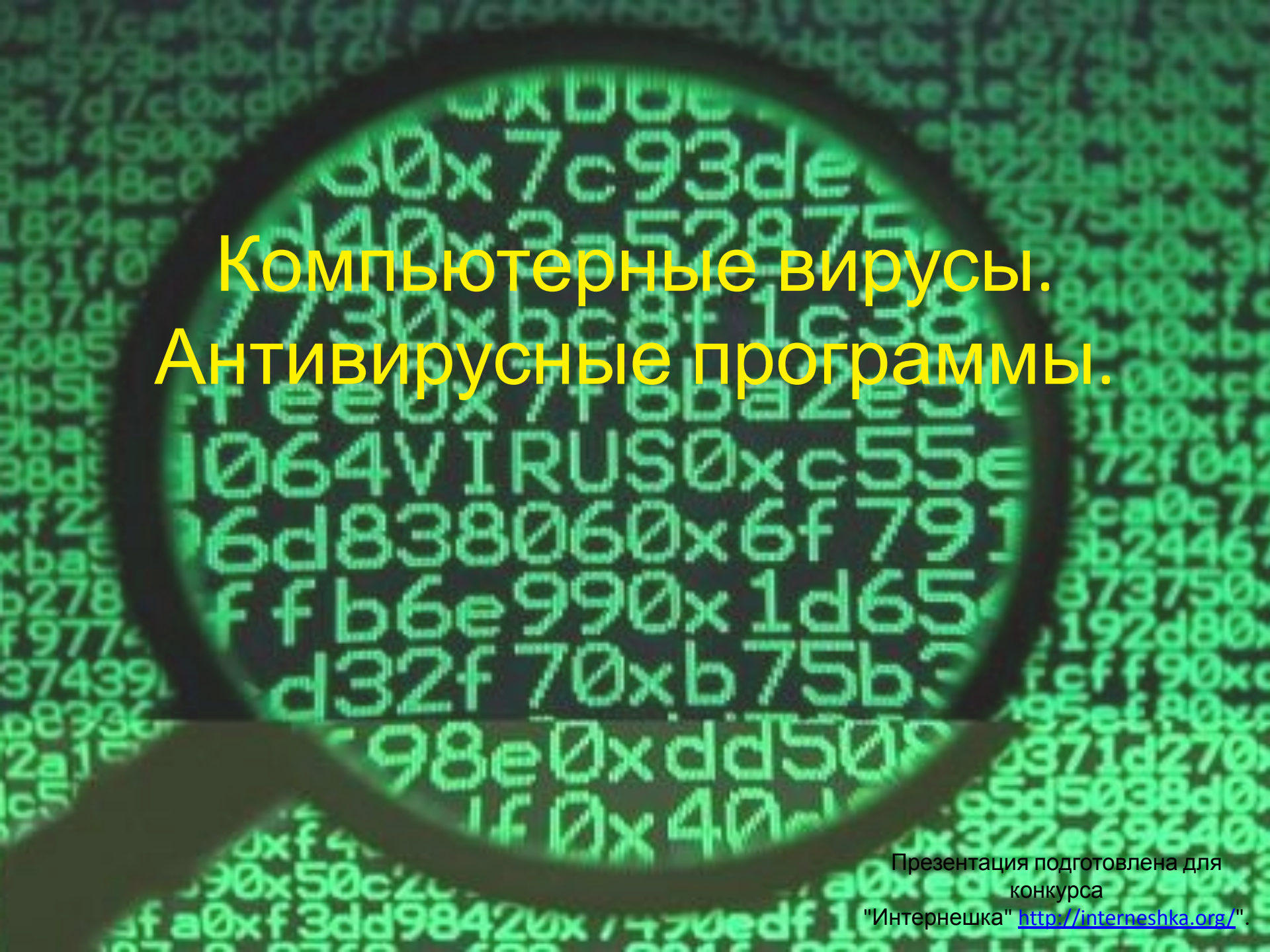


Компьютерные вирусы. Антивирусные программы.

Презентация подготовлена для конкурса "Интернешка" http://interneshka.org/".

Что такое компьютерные вирусы?

- ***Компьютерные вирусы*** *являются программами, которые могут "размножаться" и скрытно внедрять свои копии в файлы, загрузочные секторы дисков и документы. Активизация компьютерного вируса может вызывать уничтожение программ и данных.*

Разнообразны последствия действия вирусов; по величине вредных воздействий вирусы можно разделить на:

- ***Неопасные*, влияние которых ограничивается уменьшением свободной памяти на диске, графическими, звуковыми и другими внешними эффектами;**

- ***Опасные*, которые могут привести к сбоям и зависаниям при работе компьютера;**

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

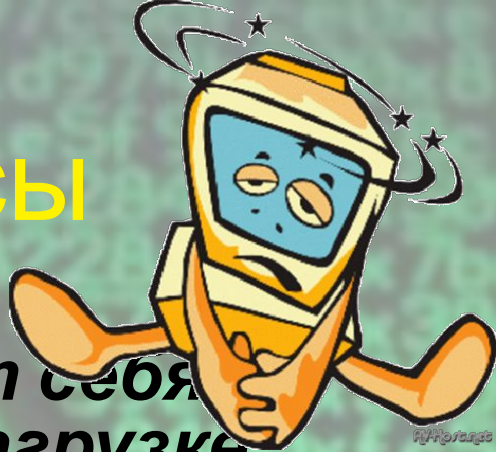
Дополнительно:

По "среде обитания" вирусы можно разделить на *файловые*,

Файловые вирусы

- ***Файловые вирусы различными способами внедряются в исполнимые файлы (программы) и обычно активизируются при их запуске. После запуска зараженной программы вирус находится в оперативной памяти компьютера и является активным (то есть может заражать другие файлы) вплоть до момента выключения компьютера или перезагрузки операционной системы.***
- ***При этом файловые вирусы не могут заразить файлы данных (например, файлы, содержащие изображение или звук).***
- ***Профилактическая защита от файловых вирусов состоит в том, что не рекомендуется запускать на выполнение файлы, полученные из сомнительного источника и предварительно не проверенные антивирусными программами.***

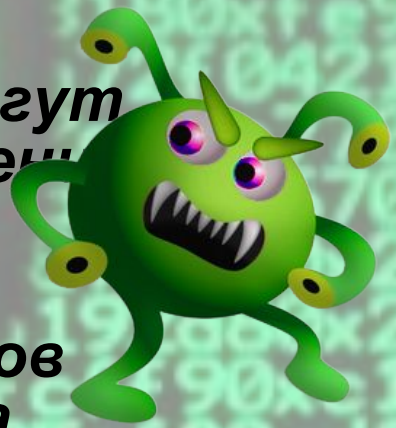
Загрузочные вирусы



- ***Загрузочные вирусы записывают себя в загрузочный сектор диска. При загрузке операционной системы с зараженного диска вирусы внедряются в оперативную память компьютера. В дальнейшем загрузочный вирус ведет себя так же, как файловый, то есть может заражать файлы при обращении к ним компьютера.***
- ***Профилактическая защита от таких вирусов состоит в отказе от загрузки операционной системы с гибких дисков и установке в BIOS вашего компьютера защиты загрузочного сектора от изменений.***

Макровирусы

- ***Макровирусы заражают файлы документов Word и электронных таблиц Excel. Макровирусы являются фактически макрокомандами (макросами), которые встраиваются в документ.***
- ***После загрузки зараженного документа в приложение макровирусы постоянно присутствуют в памяти компьютера и могут заражать другие документы. Угроза заражения прекращается только после закрытия приложения.***
- ***Профилактическая защита от макровирусов состоит в предотвращении запуска вируса. При открытии документа в приложениях Word и Excel сообщается о присутствии в них макросов (потенциальных вирусов) и предлагается запретить их загрузку. Выбор запрета на загрузку макросов надежно защитит ваш компьютер от заражения макровирусами,***

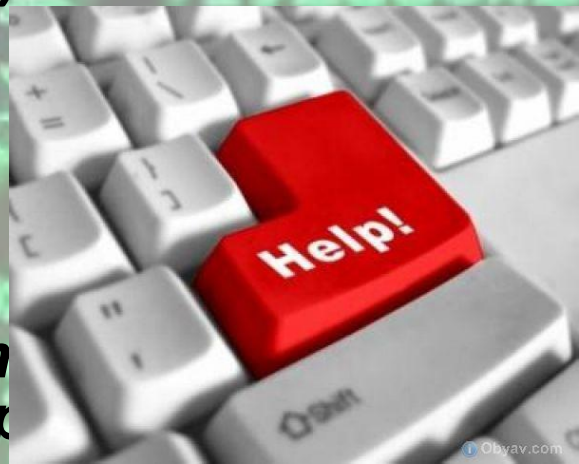


Сетевые вирусы

- *По компьютерной сети могут распространяться и заражать компьютеры любые обычные вирусы. Это может происходить, например, при получении зараженных файлов с серверов файловых архивов. Однако существуют и специфические сетевые вирусы, которые используют для своего распространения электронную почту и Всемирную паутину.*
- *Интернет-черви (worm) - это вирусы, которые распространяются в компьютерной сети во вложенных в почтовое сообщение файлах. Автоматическая активизация червя и заражение компьютера могут произойти при обычном просмотре сообщения. Опасность таких вирусов состоит в том, что они по определенным датам активизируются и уничтожают файлы на дисках зараженного компьютера.*
- *Кроме того, интернет-черви часто являются троянами, выполняя роль "троянского коня", внедренного в операционную систему. Такие вирусы "похищают" идентификатор и пароль пользователя для доступа в Интернет и передают их на определенный почтовый адрес. В результате злоумышленники получают возможность доступа в Интернет за деньги ничего не подозревающих пользователей.*
- *Лавинообразная цепная реакция распространения вируса базируется на том, что вирус после заражения компьютера начинает рассылать себя по всем адресам электронной почты, которые имеются в адресной книге пользователя. Кроме того, может происходить заражение и по локальной сети, так как червь перебирает все локальные диски и сетевые диски с правом доступа и копируется туда под случайным*

Защита

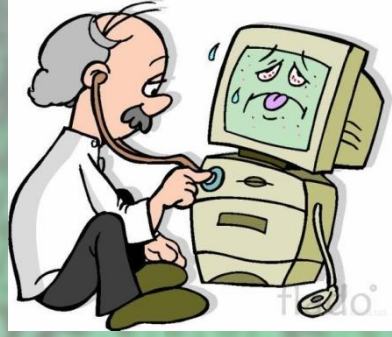
- ***Профилактическая защита от интернет-червей состоит в том, что не рекомендуется открывать вложенные в почтовые сообщения файлы, полученные из сомнительных источников.***
- ***Особой разновидностью вирусов являются активные элементы (программы) на языках JavaScript или VBScript, которые могут выполнять разрушительные действия, то есть являться вирусами (скрипт-вирусами). Такие программы передаются по Всемирной паутине в процессе загрузки Web-страниц с серверов Интернета в браузер локального компьютера.***
- ***Профилактическая защита от скрипт вирусов состоит в том, что в браузер***



Программа-детектор

- ***Программы-детекторы*** **осуществляют поиск характерной для конкретного вируса сигнатуры в оперативной памяти и в файлах и при обнаружении выдают соответствующее сообщение. Недостатком таких антивирусных программ является то, что они могут находить только те вирусы, которые известны разработчикам таких**

Программа-доктор



- ***Программы-доктора***, **или фаги, а также *программы-вакцины* не только находят зараженные вирусами файлы, но и «лечат» их, т. е. удаляют из файла тело программы-вируса, возвращая файлы в исходное состояние. В начале своей работы фаги ищут вирусы в оперативной памяти, уничтожая их, и только затем переходят к «лечению» файлов. Среди фагов выделяют *полифаги*, т. е. программы-доктора, предназначенные для поиска н уничтожения большого количества вирусов. Наиболее известные из них: Kaspersky Antivirus, Norton AntiVirus, Doctor Web.**
- **В связи с тем, что постоянно появляются новые вирусы, программы-детекторы и программы-доктора быстро устаревают, и требуется регулярное обновление версий.**

Программа-ревизор

- ***Программы-ревизоры*** **относятся к самым надежным средствам защиты от вирусов. Ревизоры запоминают исходное состояние программ, каталогов и системных областей диска тогда, когда компьютер не заражен вирусом, а затем периодически или по желанию пользователя сравнивают текущее состояние с исходным. Обнаруженные изменения выводятся на экран монитора. Как правило, сравнение состояний производят сразу после загрузки операционной системы. При сравнении проверяются длина файла, код циклического контроля (контрольная сумма файла), дата и время модификации, другие параметры. Программы-ревизоры имеют достаточно развитые алгоритмы, обнаруживают стелс-вирусы и могут даже отличить изменения версии проверяемой программы от изменений, внесенных вирусом. К числу программ-ревизоров относится широко распространенная программа Kaspersky Monitor.**

Программа-фильтр

- ***Программы-фильтры*** **или «*сторожа*» представляют собой небольшие резидентные программы, предназначенные для обнаружения подозрительных действий при работе компьютера, характерных для вирусов. Такими действиями могут являться:**
- **Попытки коррекции файлов с расширениями COM. EXE;**
- **Изменение атрибутов файла;**
- **Прямая запись на диск по абсолютному адресу;**
- **Запись в загрузочные секторы диска;**

- При попытке какой-либо программы произвести указанные действия «сторож» посылает пользователю сообщение и предлагает запретить ил разрешить соответствующее действи Программы-фильтры весьма полезны. так как способны обнаружить вирус на самой ранней стадии его существования, до размножения. Однако они не «лечат» файлы и диски.
- Для уничтожения вирусов требуется применить другие программы, например фаги. К недостаткам программ-сторожей можно отнести их «назойливость» (например, они постоянно выдают предупреждение о любой попытке копирования исполняемого файла), а также

Вакцины

- ***Вакцины или иммунизаторы*** **— это резидентные программы. предотвращающие заражение файлов. Вакцины применяют, если отсутствуют программы-доктора, «лечащие» этот вирус. Вакцинация возможна только от известных вирусов. Вакцина модифицирует программу или диск таким образом, чтобы это не отражалось на их работе, а вирус будет воспринимать их зараженными и поэтому не внедрится. В настоящее время программы-вакцины и ограниченное применение.**
- **Своевременное обнаружение зараженных вирусами файлов и дисков, полное уничтожение обнаруженных вирусов на каждом компьютере позволяют избежать**

СПАСИБО ЗА ВНИМАНИЕ!

- Сайты с которых была взята информация:
- http://5byte.ru/10/0033.php
- http://shkolo.ru/antivirusyi