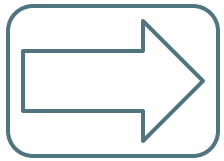
Осторожно, вирусы!

Содержание:

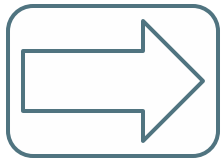


Что такое компьютерные вирусы???

- Компьютерные вирусы – это вид вредоносного программного обеспечения, способного создавать копии самого себя и внедряться в код других программ, системные области памяти, загрузочные секторы, а также распространять свои копии по разнообразным каналам связи.

Классификация вирусов

- В настоящее время не существует единой системы классификации и именования вирусов принято разделять вирусы:
  - по поражаемым объектам.
  - по механизму заражения.
  - по поражаемым операционным системам и платформам.
  - по технологиям, используемым вирусом.
  - по языку, на котором написан вирус.
  - по дополнительной вредоносной функциональности.



Как вирусы попадают в компьютер???

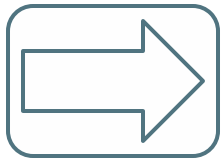
- Вирус не может просто так появиться на компьютере. Когда незараженный компьютер полностью изолирован от внешнего мира – от него отключены дисководы, он не подключен к локальной сети и в нем не установлен модем, вирус не может попасть в такой компьютер. Чтобы вирус проник на компьютер, необходимо, чтобы последний выполнил зараженную программу или загрузился с зараженной дискеты. Наиболее часто вирусы попадают в компьютер вместе с пиратским программным обеспечением, программами Freeware и Shareware.

Способы заражения вирусами

- Вот основные пути, по которым вирусы проникают в компьютер:
  - ❖ Получение программ с электронной доски объявлений и через глобальные сети;
  - ❖ Обмен дискетами и программами;
  - ❖ Проникновение вируса из локальной сети.

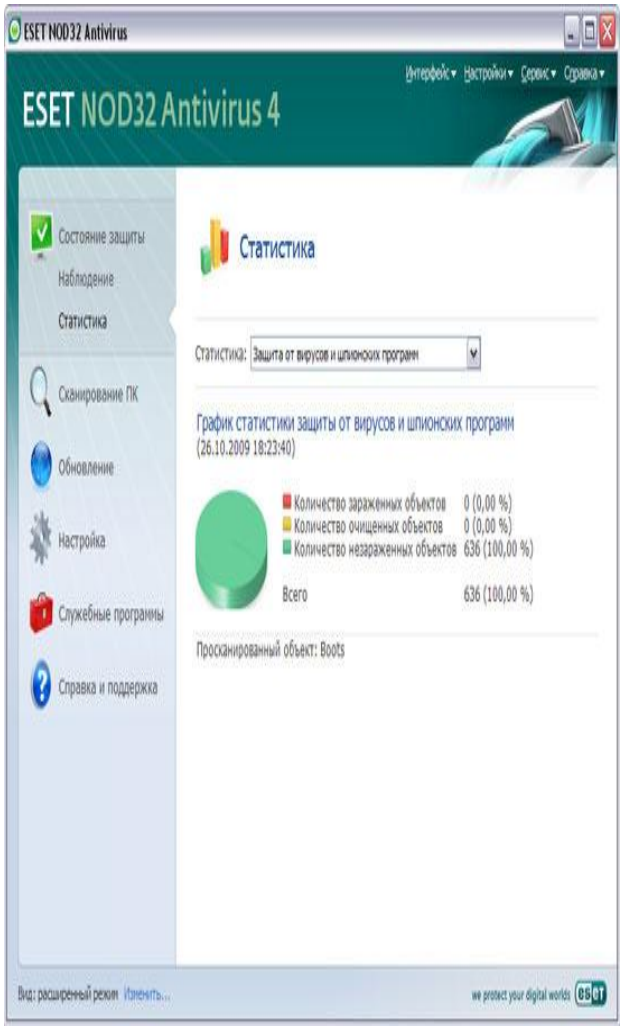
Способы защиты от вирусов

- 1. Программно-технические методы обнаружения вирусов:
  - 1.1 Сканирование
  - 1.2 Эвристический анализ
  - 1.3 Антивирусные мониторы
  - 1.4 Защита, встроенная в BIOS компьютера
- 2. Установка персональных брандмауэров:
  - 2.1 Брандмауэры

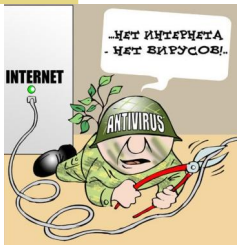


Сканирование

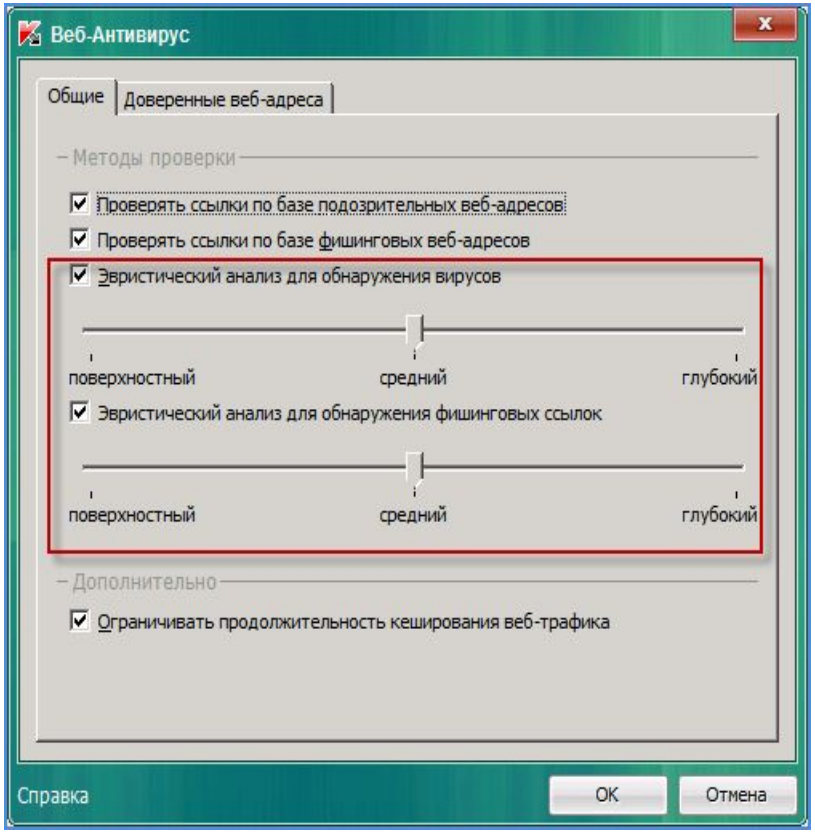
- Самая простая методика поиска вирусов заключается в том, что антивирусная программа последовательно просматривает проверяемые файлы в поиске сигнатур известных вирусов. Под сигнатурой понимается уникальная последовательность байт, принадлежащая вирусу, и не встречающаяся в других программах.
- Антивирусные программы-сканеры способны найти только уже известные и изученные вирусы, для которых была определена сигнатура. Применение простых программ-сканеров не защищает Ваш компьютер от проникновения новых вирусов.



Эвристический анализ



- Эвристический анализ позволяет обнаруживать ранее неизвестные вирусы, причем для этого не надо предварительно собирать данные о файловой системе, как этого требует, например, рассмотренный ниже метод обнаружения изменений.

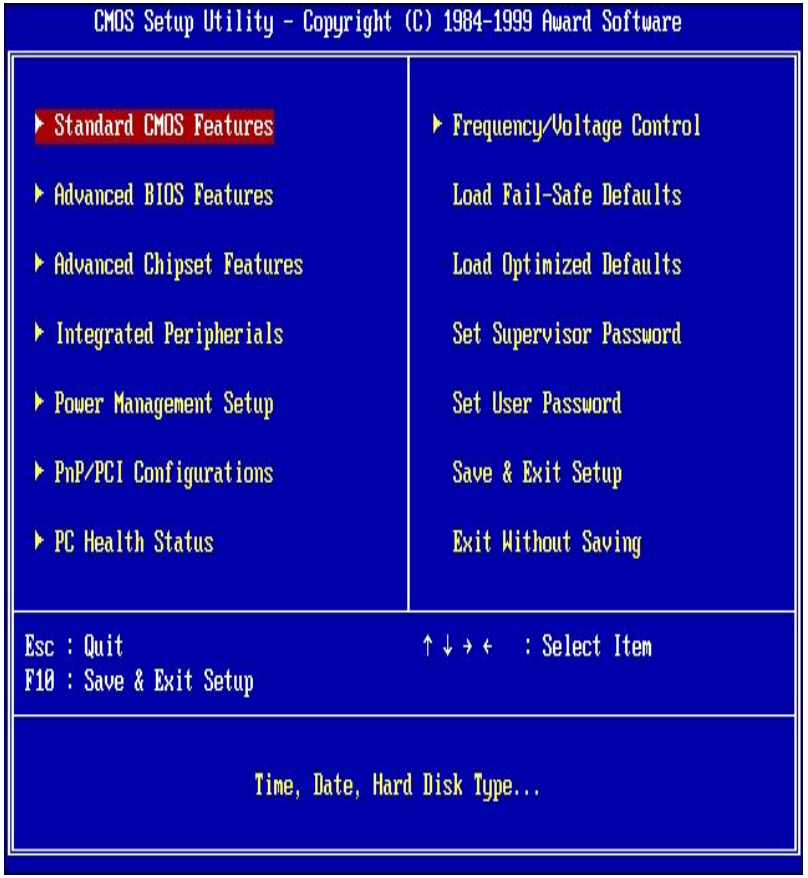


Антивирусные мониторы

- Существует еще целый класс антивирусных программ, которые постоянно находятся в памяти компьютера, и отслеживают все подозрительные действия, выполняемые другими программами. Такие программы носят название антивирусных мониторов или сторожей.
- Монитор автоматически проверяет все запускаемые программы, создаваемые, открываемые и сохраняемые документы, файлы программ и документов, полученные через Интернет или скопированные на жесткий диск с дискеты и компакт диска. Антивирусный монитор сообщит пользователю, если какая-либо программа попытается выполнить потенциально опасное действие.

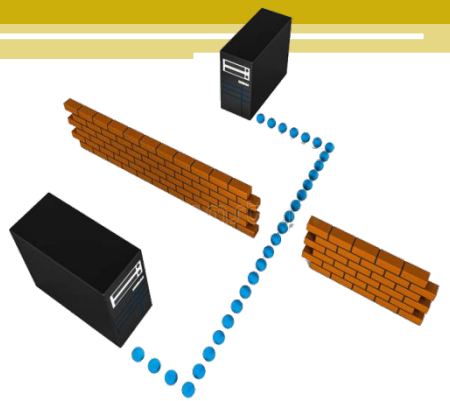
Защита, встроенная в BIOS компьютера

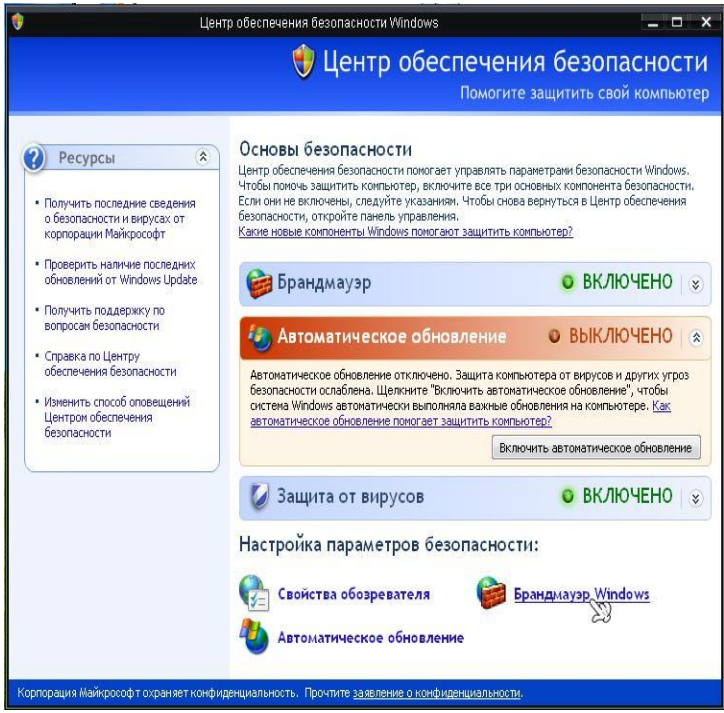
- В системные платы компьютеров тоже встраивают простейшие средства защиты от вирусов. Эти средства позволяют контролировать все обращения к главной загрузочной записи жестких дисков, а также к загрузочным секторам дисков и дискет. Если какая-либо программа попытается изменить содержимое загрузочных секторов, срабатывает защита и пользователь получает соответствующее предупреждение. Однако важно помнить, что такая защита не очень надёжна.



Брандмауэры

- Корпоративная сеть, подключенная к Интернету, должна быть защищена от атак хакеров при помощи брандмауэра. Однако помимо этого можно дополнительно защитить рабочие станции и серверы сети, установив на них персональные брандмауэры, такие как AtGuard





Спасибо за внимание!

- В ходе создания презентации использовались следующие ресурсы:

1. https://ru.wikipedia.org
2. http://www.frolov-lib.ru
3. http://teralex.ru
4. http://www.lessons-tva.info
5. https://sites.google.com