Чем может «заболеть» компьютер?

Возникновение вирусов связано с идеей создания самовоспроизводящихся программ.

Началось всё в 50-е годы 20 века.

Сначала это были вирусоподобные программы.

В 1983 году появился первый, получивший распространение вирус на ПВЭМ Apple II.

Первый вирус назывался Elk Cloner

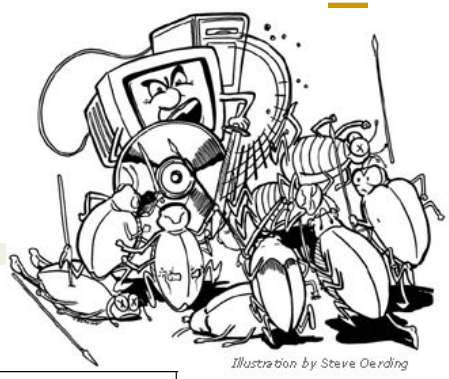
Вирус был написан в 1981 году 15-летним школьником Ричардом Скрента для компьютеров Apple II.

Компьютерные вирусы

программы, которые могут “размножаться” и скрыто внедрять свои копии в файлы, загрузочные секторы дисков и документы.

Признаки, указывающие на поражение программ вирусом:

- Неправильная работа программ
- Медленная работа компьютера
- Невозможность загрузки операционной системы
- Исчезновение файлов
- Изменение даты, времени создания файла или его размера
- Вывод на экран непредусмотренных сообщений или изображений
- Частые зависания компьютера и т.д.



Степень воздействия	Действие
Неопасные	Уменьшение свободной памяти на диске, графические, звуковые и другие внешние эффекты
Опасные	Сбой и зависание работы компьютера
Очень опасные	Потеря программ и данных, форматирование винчестера и т.д.

Компьютерные вирусы (по "среде обитания")

- Файловые
- Загрузочные
- Макровирусы
- Сетевые

Файловые вирусы

Действие	Профилактика
Внедряются в исполнимые файлы (программы) и обычно активизируются при запуске. Не могут заразить файлы данных (файлы, содержащие изображение и звук).	Не рекомендуется запускать на выполнение файлы, полученные из сомнительного источника и предварительно не проверенные антивирусными программами.

Загрузочные вирусы

Действие	Профилактика
Записывают себя в загрузочный сектор диска. При загрузке ОС с зараженного диска вирусы внедряются в ОП компьютера. В дальнейшем загрузочный вирус ведет себя как файловый, т.е. может заражать файлы при обращении к ним компьютера.	Отказ от загрузки операционной системы с гибких дисков и установка в BIOS компьютера защиты загрузочного сектора от изменений.

Макровирусы

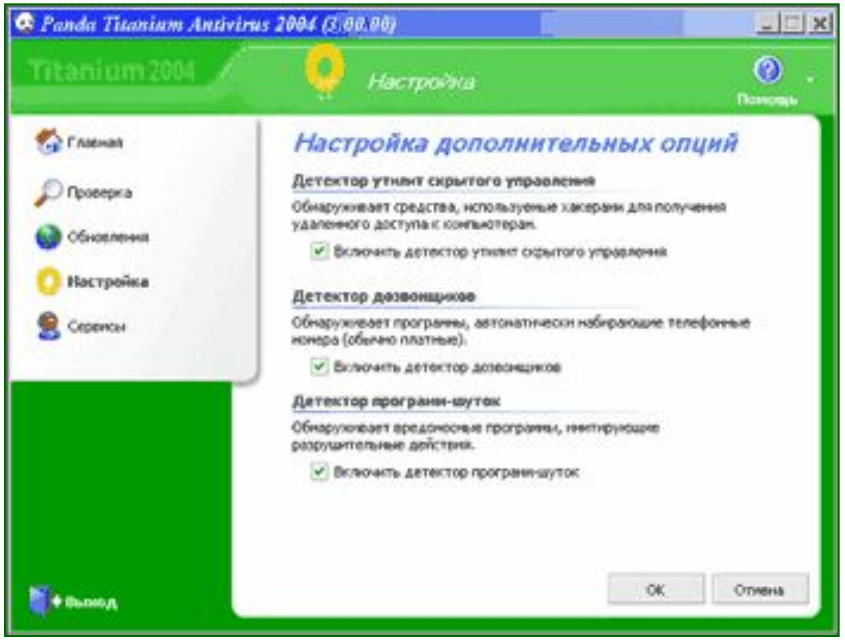
Действие	Профилактика
Заражают файлы документов Word и электронных таблиц Excel. Макровирусы являются фактически макрокомандами (макросами), которые встраиваются в документ. После загрузки зараженного документа в приложение макровирусы постоянно присутствуют в памяти компьютера и могут заражать другие документы. Угроза заражения прекращается только после закрытия приложения.	Предотвращение запуска вируса. При открытии документа в приложениях Word и Excel сообщается о присутствии в них макросов (потенциальных вирусов) и предлагается запретить их загрузку.

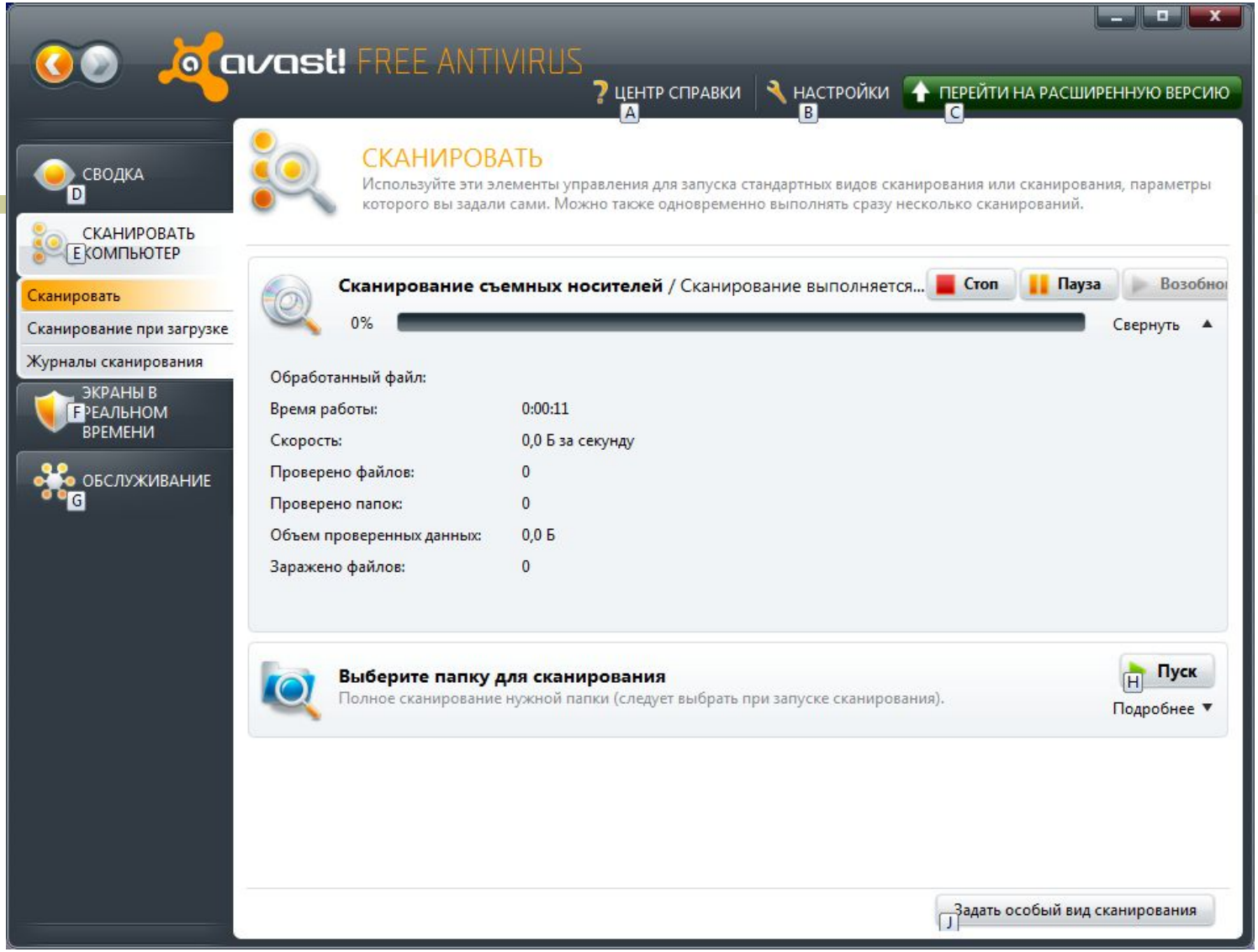
Сетевые вирусы

Действие	Профилактика
Распространяются по компьютерной сети. Заражение может происходить при получении зараженных файлов с серверов файловых архивов. **Интернет-черви** – это вирусы, которые распространяются в компьютерной сети во вложенных в почтовое сообщение файлах. По определенным датам они активизируются и уничтожают файлы на дисках зараженного компьютера. часто «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. Вирус после заражения компьютера начинает рассылать себя по всем адресам электронной почты, которые имеются в адресной книге пользователя.	Не рекомендуется открывать вложенные в почтовые сообщения файлы, полученные из сомнительных источников.

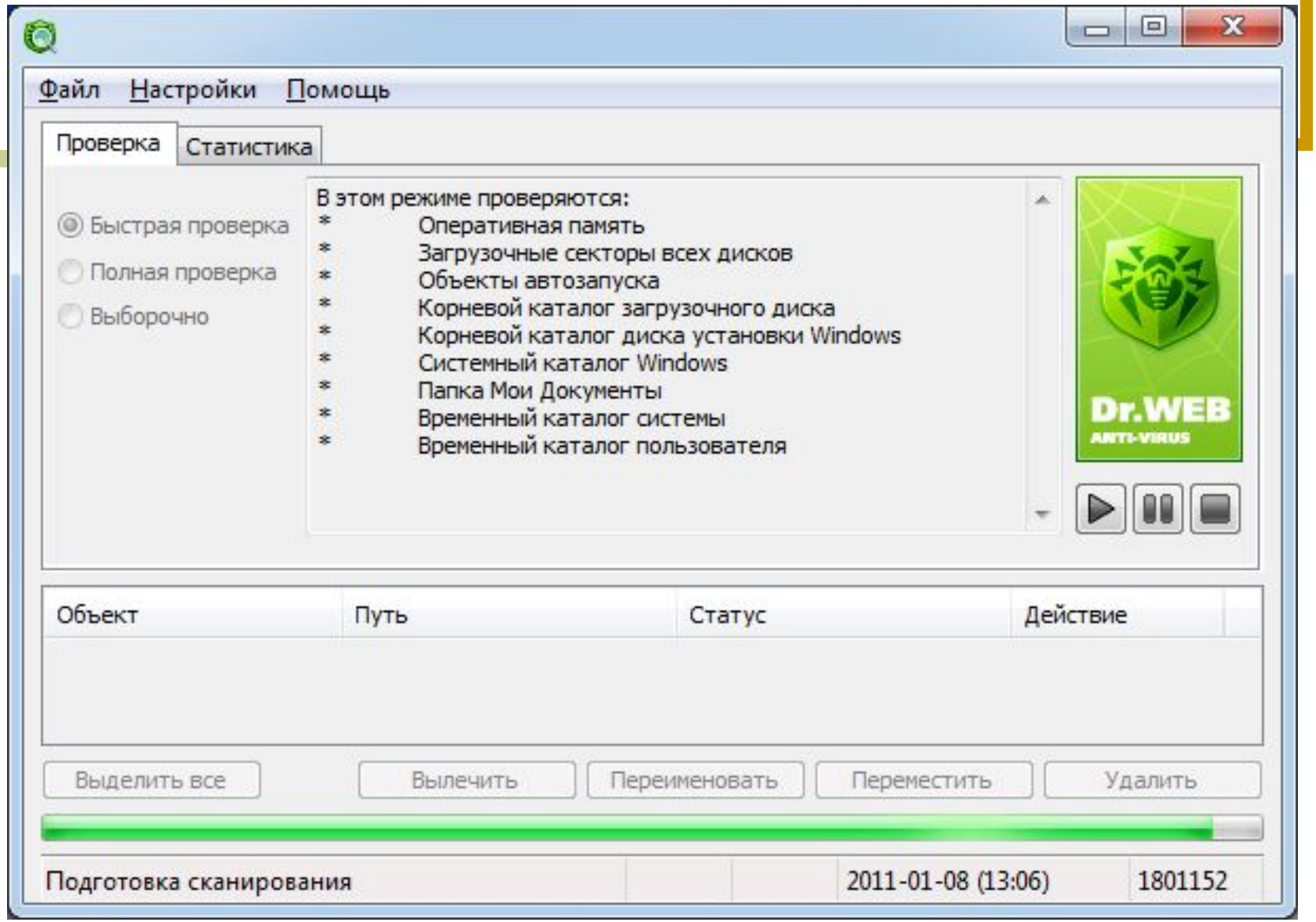
Для поиска и «лечения» заражённых файлов используются антивирусные Программы.
Это:

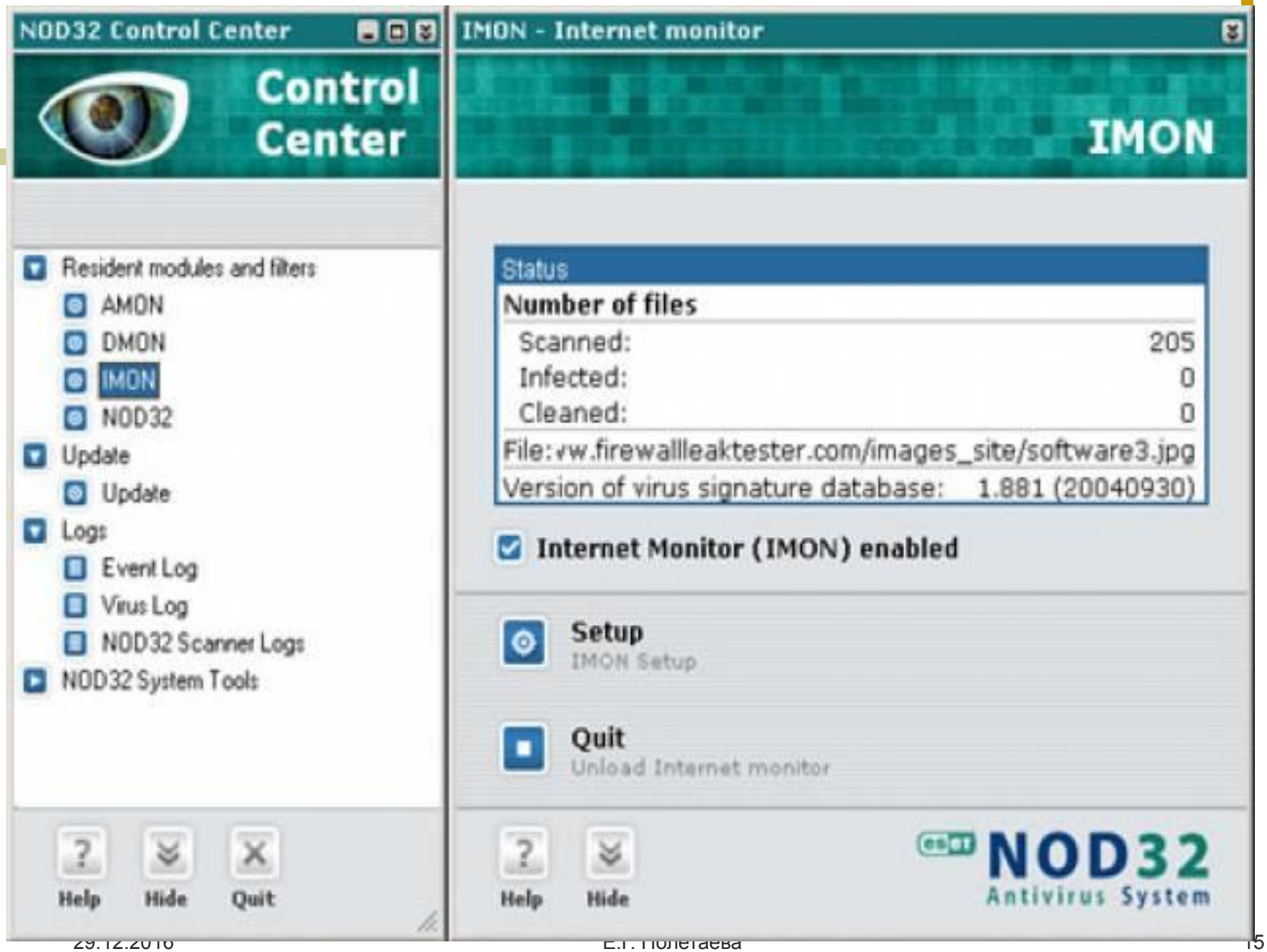
Kaspersky Anti-Virus,
Panda Titanium Antivirus





Avast! Antivirus


Файл Настройки Помощь
Проверка
Статистика
Быстрая проверка
Полная проверка
Выборочно
В этом режиме проверяются:
* Оперативная память
* Загрузочные секторы всех дисков
* Объекты автозапуска
* Корневой каталог загрузочного диска
* Корневой каталог диска установки Windows
* Системный каталог Windows
* Папка Мои Документы
* Временный каталог системы
* Временный каталог пользователя
Dr.WEB
ANTI-VIRUS
Объект
Путь
Статус
Действие
Выделить все
Вылечить
Переименовать
Переместить
Удалить
Подготовка сканирования
2011-01-08 (13:06)
1801152


NOD32 Control Center
Control Center
Resident modules and filters
AMON
DMON
IMON
NOD32
Update
Update
Logs
Event Log
Virus Log
NOD32 Scanner Logs
NOD32 System Tools
Help
Hide
Quit
IMON - Internet monitor
IMON
Status
Number of files
Scanned: 205
Infected: 0
Cleaned: 0
File: vw.firewallleaktester.com/images_site/software3.jpg
Version of virus signature database: 1.881 (20040930)
Internet Monitor (IMON) enabled
Setup
IMON Setup
Quit
Unload Internet monitor
Help
Hide
NOD32
Antivirus System

Правила защиты от компьютерных вирусов:

- Регулярно тестируйте компьютер на наличие вирусов с помощью антивирусных программ
- Перед считыванием информации с дискет проверяйте их на наличие вирусов
- Всегда защищайте свои дискеты от записи при работе на других компьютерах
- Делайте архивные копии ценной для вас информации
- Не оставляйте дискету в дисководе
- Не используйте программы, поведение которых непонятно
- Регулярно обновляйте антивирусные программы

Защита от компьютерных вирусов

Существуют три рубежа защиты:

- предотвращение поступления вирусов;
- предотвращение вирусной атаки, если вирус поступил на ПК;
- предотвращение разрушительных последствий, если атака произошла.

Методы реализации защиты

- Программные
- Аппаратные
- Организационные

Средства антивирусной защиты

Основное средство– резервное копирование наиболее ценных данных. В случае утраты информации жесткие диски форматируют, устанавливают ОС с дистрибутивного CD-диска и все необходимые программы, а данные – с резервного носителя (который должен храниться отдельно от ПК). Все регистрационные и парольные данные для доступа в Интернет рекомендуется хранить не на ПК, а в служебном дневнике в сейфе.

- Вспомогательные средства – это антивирусные программы и аппаратные средства.
  - Аппаратное средство: отключение перемычки на материнской плате не позволит осуществить стирание микросхемы BIOS ни вирусу, ни злоумышленнику, ни неаккуратному пользователю.
  - Антивирусная программа сравнивает коды программ с известными ей вирусами, которые хранятся в ее базе данных.

Антивирусные программы

Вид	Примеры	Принцип работы	Недостатки
Полифаги			
Ревизоры			
Блокировщики			