Компьютерные вирусы

Классификация компьютерных вирусов

Антивирус ная профилактика

Учитель информатики Борисова Н.М.

ГБОУ СОШ №249 С-Петербург

Компьютерные вирусы, число которых в мире к настоящему времени превысило 6 000 000, представляют одну из основных угроз работоспособности компьютерных систем и безопасности данных.

Откуда берутся компьютерные вирусы?

Вирусы попадают на ПК извне в результате несоблюдения пользователями правил антивирусной защиты

(хотя возможно заражение новым, неизвестным ранее вирусом и при соблюдении этих правил).

В настоящее время во многих странах, в том числе и в России, введена уголовная ответственность за создание и распространение компьютерных вирусов (УК РФ Гл.8 ст.273 - от 3 до 7 лет).

Что такое компьютерный вирус?(стр60)

Запишите в тетрадь:

Компьютерный вирус- это специально написанная небольшая по размерам программа, действия которой в большинстве случаев направлены на разрушение или искажение данных и нарушение работоспособности ПК.

Это программа, способная к размножению, может «приписывать» себя к другим программам для выполнения каких-либо вредных действий - портит файлы, «засоряет» оперативную память и т.д.

Что может сделать компьютерный вирус?

«Засорить» оперативную память или жесткий диск :

При размножении программа-вирус может заполнить весь жесткий диск своими копиями или какими-либо символами. Кроме того, она может записывать свои копии в ОП, уменьшая тем самым ее объем.

Испортить FAT - таблицу размещения файлов:

При изменении FAT нельзя найти и прочитать каталоги и файлы с диска.

Испортить содержимое загрузочного сектора:

Загрузочный сектор - это специальная программа на диске, при повреждении которой диск становится неработоспособным.

- **Отформатировать диск;**
- **Вывести сообщение на экран или сыграть мелодию;**
- **Перезагрузить ПК:**

  Перезагрузка происходит либо после нажатия комбинации каких-либо клавиш, либо без видимых причин.
- **Заблокировать клавиатуру:**

  В результате разрушения таблицы кодов клавиш работа на ПК будет невозможна.
- **Изменить содержимое файлов с программами и данными:**

  Программа-вирус произвольным образом перемешивает данные, например, в базе данных, вносит ошибки в сложные расчеты и т.д.

Первая «эпидемия» компьютерного вируса произошла в 1986 году, когда вирус по имени Brain (англ. «мозг») заражал дискеты персональных компьютеров.

В настоящее время известно более 6 млн вирусов, заражающих компьютеры и распространяющихся по компьютерным сетям.

Активизация вируса может быть связана с различными событиями:

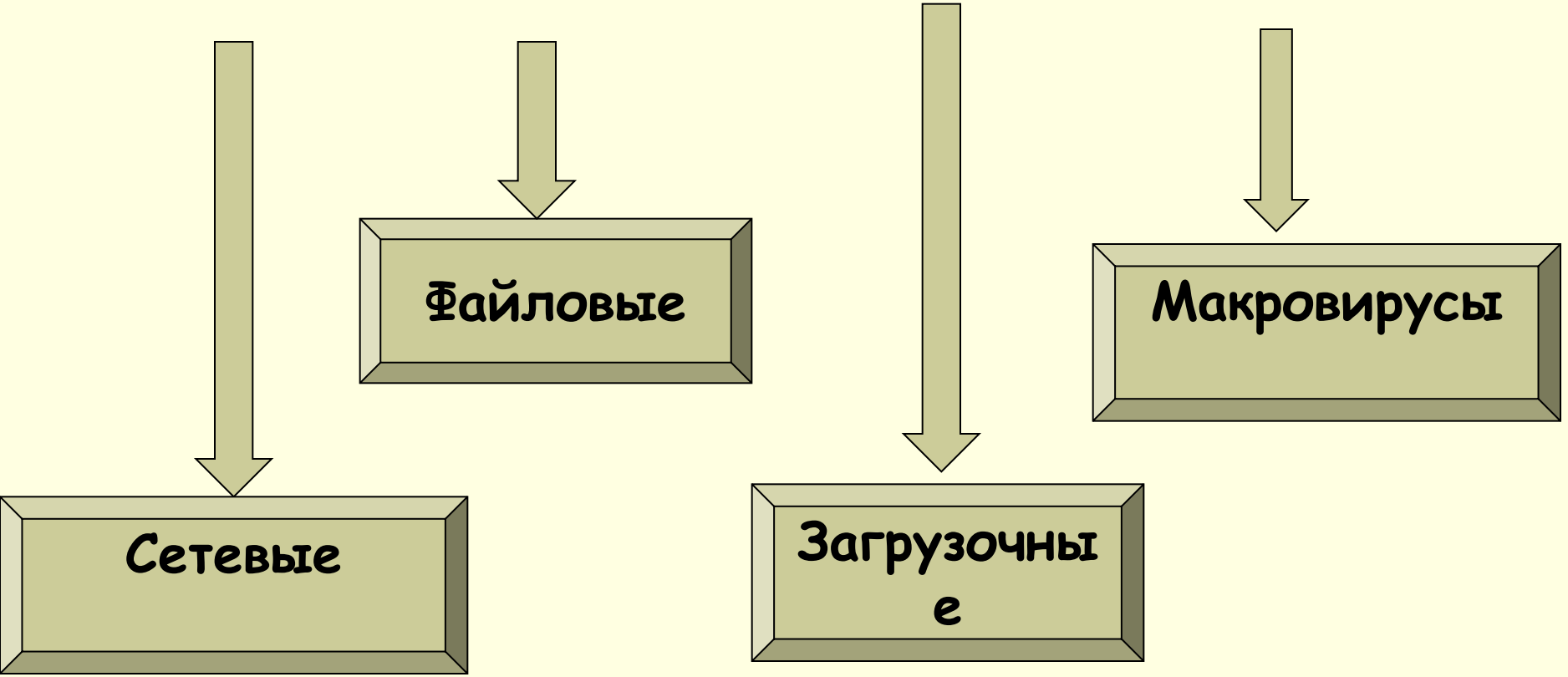
- **Наступлением определённой даты или дня недели;**
- **Запуском программы;**
- **Открытием документа и т.д.**

Классификация компьютерных вирусов

Имеются несколько признаков классификации существующих вирусов:

- **по среде обитания;**
- **по способу заражения;**
- **по деструктивным возможностям;**
- **по особенности алгоритма.**

По «среде обитания» вирусы делятся на:



Сетевые вирусы

Могут передавать по компьютерным сетям свой программный код и запускать его на компьютерах, подключенных к этой сети.

Заражение сетевым вирусом может произойти при работе с электронной почтой или при «путешествиях» по Всемирной паутине.

Файловые вирусы

Внедряются в программы и активизируются при их запуске.

После запуска заражённой программы вирусы находятся в оперативной памяти компьютера и могут заражать другие файлы до момента выключения компьютера или перезагрузки операционной системы.

Загрузочные вирусы

Загрузочные вирусы записывают себя *в загрузочный сектор* диска или в *сектор системного загрузчика* жесткого диска.

Начинают работу при загрузке ПК и обычно становятся *резидентными*.

Макровирусы

Заражают файлы документов, например, текстовых документов.

После загрузки заражённого документа в текстовый редактор макровирус постоянно присутствует в ОП и может заражать другие документы.

Угроза заражения прекращается только после закрытия текстового документа.

Запишите: СРЕДА ОБИТАНИЯ

По среде обитания вирусы можно разделить на

- ***Сетевые*** **вирусы - распространяются по компьютерной сети;**
- ***Файловые*** **вирусы - поражают исполняемые файлы программ (exe-файлы, com-файлы);**
- ***Загрузочные*** **- внедряются в загрузочный сектор диска (Boot- сектор) или в сектор, содержащий системный загрузчик винчестера (Master Boot record). Начинают работу при загрузке компьютера и обычно становятся резидентными.**
- ***Макро-*** **вирусы, заражают файлы широко используемых пакетов обработки данных.**

  Наибольшее распространение получили макровирусы для приложений Microsoft Office.

СПОСОБЫ ЗАРАЖЕНИЯ

Способы заражения делятся на резидентный и нерезидентный.

Резидентный **вирус при инфицировании компьютера оставляет в оперативной памяти свою резидентную часть, которая затем перехватывает обращения ОС к объектам заражения и внедряется в них.**

- ***Нерезидентные*** **вирусы не заражают память компьютера и являются активными в ограниченное время**

! К разновидности **резидентных** вирусов следует отнести также **макровирусы,** поскольку они постоянно присутствуют в памяти компьютера во время работы зараженного редактора.

Резидентные вирусы

способны оставлять свои копии в ОП, перехватывать обработку событий (например, обращение к файлам или дискам) и вызывать при этом процедуры заражения объектов (файлов или секторов).

Эти вирусы активны в памяти не только в момент работы зараженной программы, но и после.

Резидентные копии таких вирусов жизнеспособны до перезагрузки ОС, даже если на диске уничтожены все зараженные файлы.

Если резидентный вирус является также загрузочным и активизируется при загрузке ОС, т даже форматирование диска при наличии в памяти этого вируса его не удаляет.

По способу заражения различают

- троянские программы,
- утилиты скрытого администрирования,
- Intended-вирусы и т. д.

Троянские программы

получили свое название по аналогии с троянским конем.

относятся к самым опасным вирусам, т.к. они, маскируясь под полезную программу разрушают загрузочный сектор и файловую систему дисков

Назначение этих программ — имитация каких-либо полезных программ, новых версий популярных утилит или дополнений к ним.

При их записи пользователем на свой компьютер троянские программы активизируются и выполняют нежелательные действия.

ДЕСТРУКТИВНЫЕ ВОЗМОЖНОСТИ

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, графическими, звуковыми и прочими эффектами;*
- ***опасные вирусы**, которые могут привести к серьёзным сбоям в работе компьютера;*
- ***очень опасные**, которые могут привести к потере программ, уничтожить данные, стереть необходимую для работы компьютера информацию, записанную в системных областях.*

ОСОБЕННОСТИ АЛГОРИТМА

По особенностям алгоритма можно выделить следующие группы вирусов:

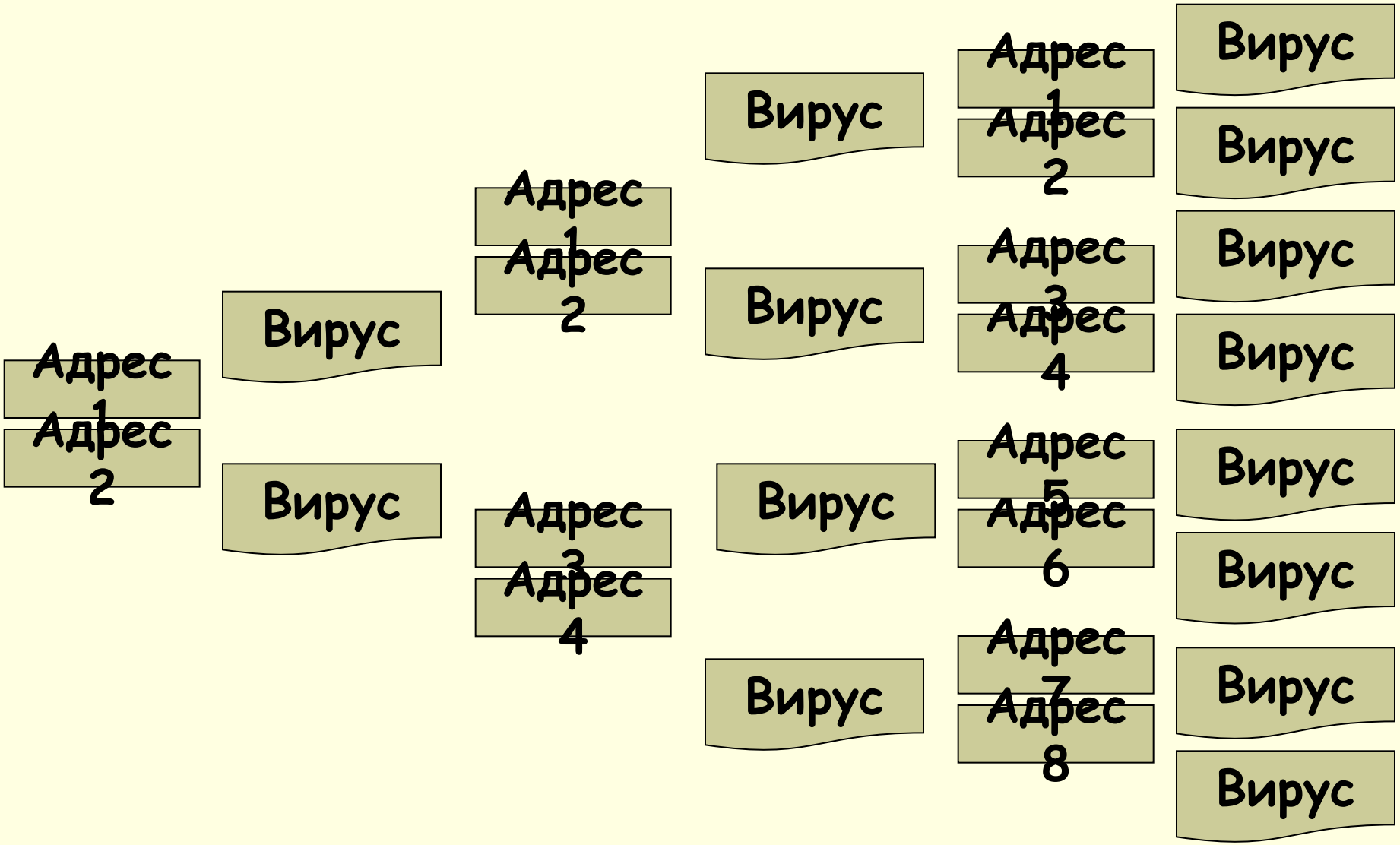
- ***вирусы-«спутники»(compаnion) - это вирусы, не изменяющие файлы. Алгоритм работы этих вирусов состоит в том, что они создают для EXE-файлов файлы-спутники, имеющие то же самое имя, но с расширением COM. При запуске система ищет сначала файл с расширением COM, запускает его, вирус выполняет все свои действия и затем запускает настоящую программу с расширением EXE;***
- ***вирусы-«черви»(worm)- вирусы, которые распространяются в компьютерной сети. Они проникают в память компьютера по сети, вычисляют адреса других компьютеров и рассылаются по этим адресам;***

- ***«паразитические»*** ***- все вирусы, при распространении своих копий изменяют содержимое дисковых секторов и файлов. В эту группу входят все вирусы, которые не являются «спутниками» и «червями»;***

- ***«стелс»-вирусы*** ***(вирусы-невидимки, stealth) - это очень совершенные программы, которые перехватывают обращения DOS к пораженным файлам или секторам диска и «подставляют» вместо себя незараженные участки;***

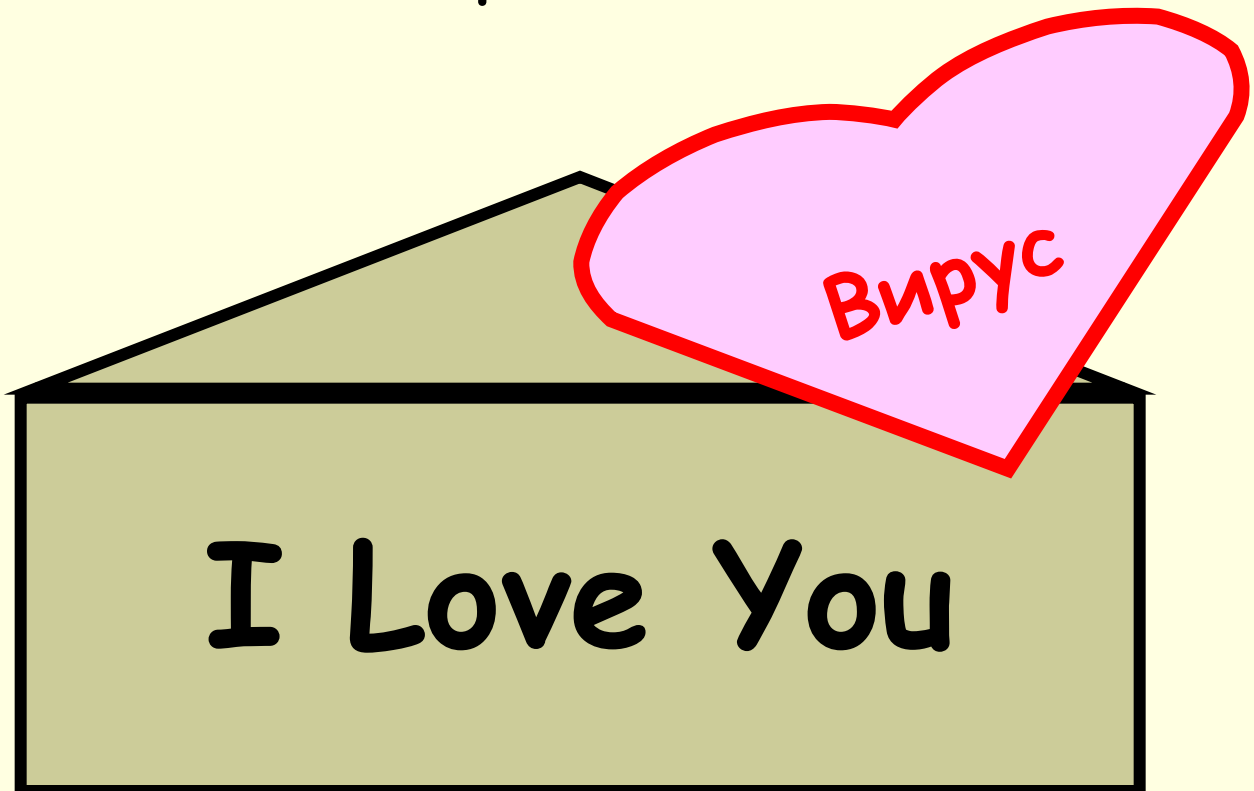
- ***вирусы-«призраки»*** ***- достаточно трудно обнаружимые вирусы, не имеющие ни одного постоянного участка кода. Вирус шифрует свой код. При шифровке каждый раз используются разные ключи. Кроме того, модифицируется и программа-расшифровщик. Таким образом, код вируса в разных случаях заражения будет разный.***

Лавинообразное заражение компьютеров почтовым вирусом:



5 мая 2000 года

Началась всемирная эпидемия заражения почтовым вирусом, когда десятки миллионов, подключенных к сети Интернет, получили почтовое сообщение:



Антивирусная лаборатория "Доктор Веб" классифицирует компьютерные вредоносные программы следующим образом:

Атаки методом подбора пароля (Brute force attacks)
Бомбы с часовыми механизмами (Time bombs)
Вишинг (Vishing)
Дифейсмент (Defacement)
DoS-атаки (DoS-attacks)
Зомби (Zombies)
Клавиатурные перехватчики (Keyloggers)
Логические бомбы (Logic bombs)
Люки (Backdoors)
Почтовые бомбы (Mail bombs)
Руткит (Rootkit)
Скамминг (Scamming)
Сниффинг (Sniffing)
Спуфинг (Spoofing)
Троянские кони (Троянцы) (Trojan Horses)
Фишинг (Phishing)
Фарминг (Pharming)

Домашнее задание: **Что такое:**

Вишинг (Vishing)

Дифейсмент (Defacement)

Зомби (Zombies)

Скамминг (Scamming)

Сниффинг (Sniffing)

Спуфинг (Spoofing)

Фишинг (Phishing)

Фарминг (Pharming)

Нежелательные программы:

Аплеты (applets)
Веб-жучки (Web bugs)
Вирусные мистификаторы (Hoaxes)
Всплывающие окна (pop-ups)
"Горшочки с медом" (honey pots)
Дозвонщики (Dialers)
Зомби (Zombies)
Перехватчики страниц (highjackers)
Технологии социальной инженерии
Технология ActiveX
Утилиты удаленного администрирования
Уязвимость (Vulnerability)
Файлы cookies
Шпионские модули-роботы (spybots)
Шпионское ПО (spyware)

Признаки, указывающие на поражение программ вирусом:

Запишите в тетрадь:

- **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.**

Первые признаки вируса в компьютере

- вывод на экран непредусмотренных сообщений или изображений,
- подача непредусмотренных звуковых сигналов,
- неожиданное открытие и закрытие лотка дисковода,
- самопроизвольный запуск каких-либо программ,
- самопроизвольные попытки ПК выйти в интернет.

Характерные признаки вируса, заражающего компьютеры через электронную почту:

- друзья и знакомые сообщают о письмах от вас, хотя вы им ничего не отправляли,
- в почтовом ящике находится большое количество сообщений без обратного адреса и заголовка.

АНТИВИРУСНАЯ ПРОФИЛАКТИКА

Для защиты ПК от компьютерных вирусов используются средства профилактики, позволяющие не допустить попадания вируса в систему, а также программные средства диагностики и лечения.

Для уменьшения вероятности заражения ПК вирусом необходимо:

- **Установить на ПК антивирусный комплект;**
- **Не запускать программы, назначение которых вы не знаете.**
- **Проверять на вирус все архивы**
- **!!! Электронная почта**

Правила защиты от компьютерных вирусов:

- Регулярно тестируйте компьютер на наличие вирусов с помощью антивирусных программ
- Делайте архивные копии ценной для вас информации
- Не используйте программы, поведение которых непонятно
- Регулярно обновляйте антивирусные программы

! Принимая электронную почту

не вскрывайте вложения, если отправитель вам неизвестен;

! Подключаясь к Internet,

настройте свой обозреватель,

выбрав в главном меню Internet Explorer команду Вид | Свойства обозревателя

и выбрав

высокий уровень безопасности

Для борьбы с вирусами существуют программы, которые можно разбить на основные группы:

- **мониторы,**
- **детекторы,**
- **доктора,**
- **ревизоры**
- **вакцины.**

Программы-мониторы (программы-фильтры)

- располагаются резидентно в ОП компьютера, перехватывают и сообщают пользователю об обращениях ОС, которые используются вирусами для размножения и нанесения ущерба.
- Пользователь имеет возможность разрешить или запретить выполнение этих обращений.
- К преимуществу таких программ относится возможность обнаружения неизвестных вирусов.
- Использование программ-фильтров позволяет обнаруживать вирусы на ранней стадии заражения компьютера.
- Недостатками программ являются невозможность отслеживания вирусов, обращающихся непосредственно к BIOS, а также загрузочных вирусов, активизирующихся до запуска антивируса при загрузке DOS, и частая выдача запросов на выполнение операций.

Программы-детекторы

Проверяют, имеется ли в файлах и на дисках специфическая для данного вируса комбинация байтов. При ее обнаружении выводится соответствующее сообщение. Недостаток — возможность защиты только от известных вирусов.

Программы-доктора

восстанавливают зараженные программы путем удаления из них тела вируса.

Обычно эти программы рассчитаны на конкретные типы вирусов и основаны на сравнении последовательности кодов, содержащихся в теле вируса, с кодами проверяемых программ.

Программы-доктора необходимо периодически обновлять с целью получения новых версий, обнаруживающих новые виды вирусов.

Программы-ревизоры

анализируют изменения состояния файлов и системных областей диска.

Проверяют состояние загрузочного сектора и таблицы FAT; длину, атрибуты и время создания файлов; контрольную сумму кодов.

Пользователю сообщается о выявлении несоответствий.

Программы-вакцины

Программы-вакцины модифицируют программы и риски так, что это не отражается на работе программ, но вирус, от которого производится вакцинация, считает программы или диски уже зараженными. Существующие антивирусные программы в основном относятся к классу гибридных (детекторы-доктора, доктора-ревизоры и пр.).

Антивирусные программы:

- Антивирус Касперского
- Doctor Web
- Norton AntiVirus
- NOD32
- McafeeMcafee, AviraMcafee, Avira, AvastMcafee, Avira, Avast, SophosMcafee, Avira,

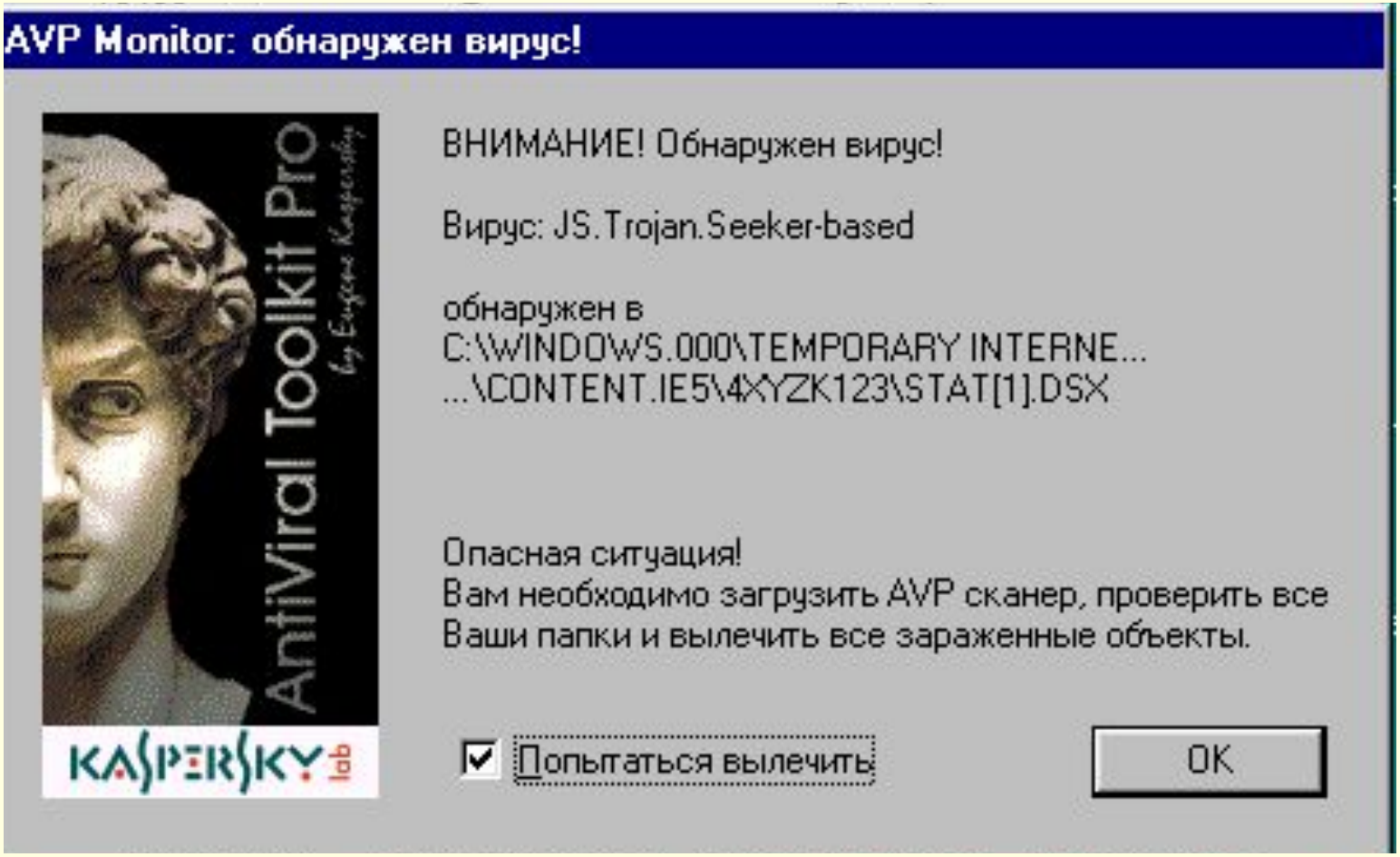
В России наибольшее распространение получили антивирусные программы

Лаборатории Касперского (Anti-IViral Toolkit Pro)

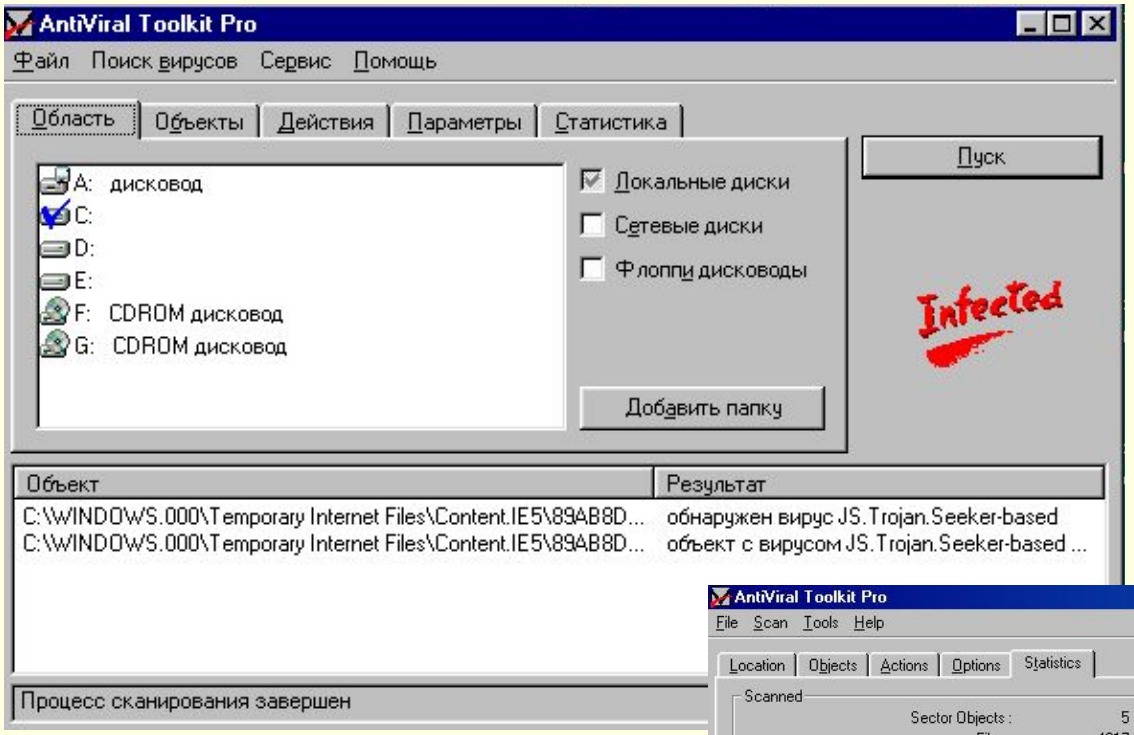
ДиалогНаука (Adinf,Dr.Web)

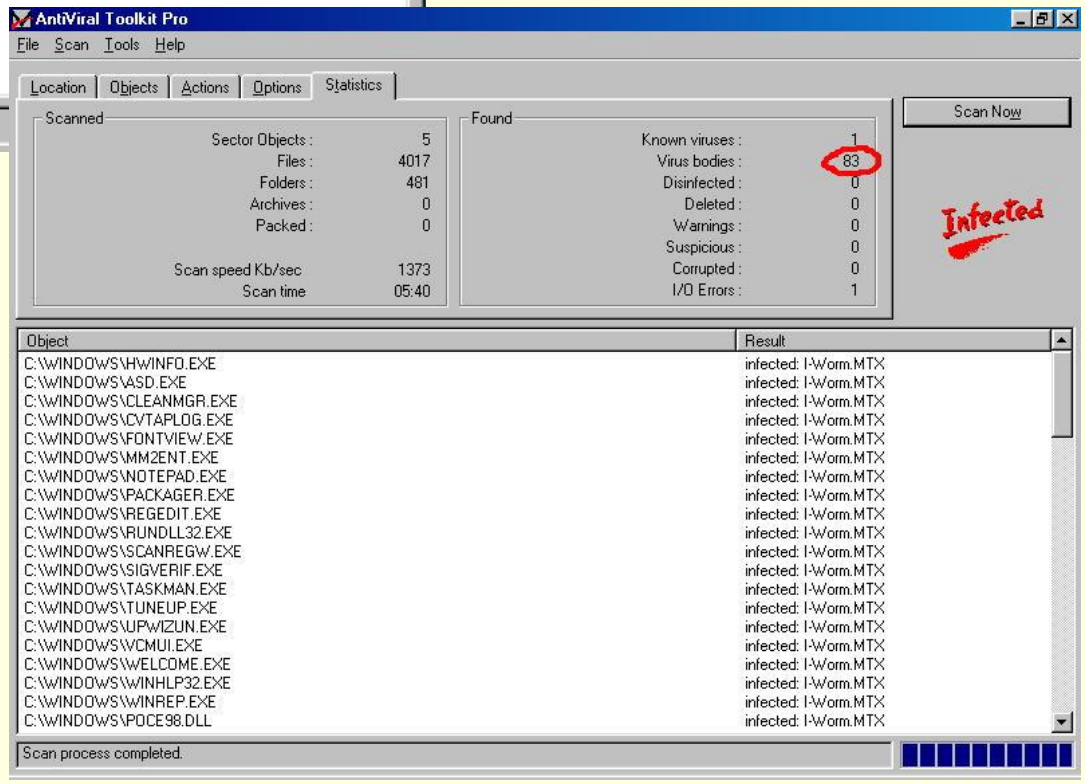
NOD32

Так выглядит сообщение программы-сторожа при обнаружении вируса. При его появлении нужно немедленно выполнить то, что сказано в сообщении.



Так выглядит окно антивирусной программы при обнаружении вируса.





Dr.Web для Windows включает в себя :

- Dr.Web Сканер для Windows ;
- SplDer Guard для Windows;
- SplDer Mail;
- Dr.Web Модуль автоматического обновления для Windows;
- Планировщик_заданий для Windows;

сканер для среды DOS

и ряд вспомогательных программ.

Dr.Web Сканер для Windows – антивирусный сканер с графическим интерфейсом.

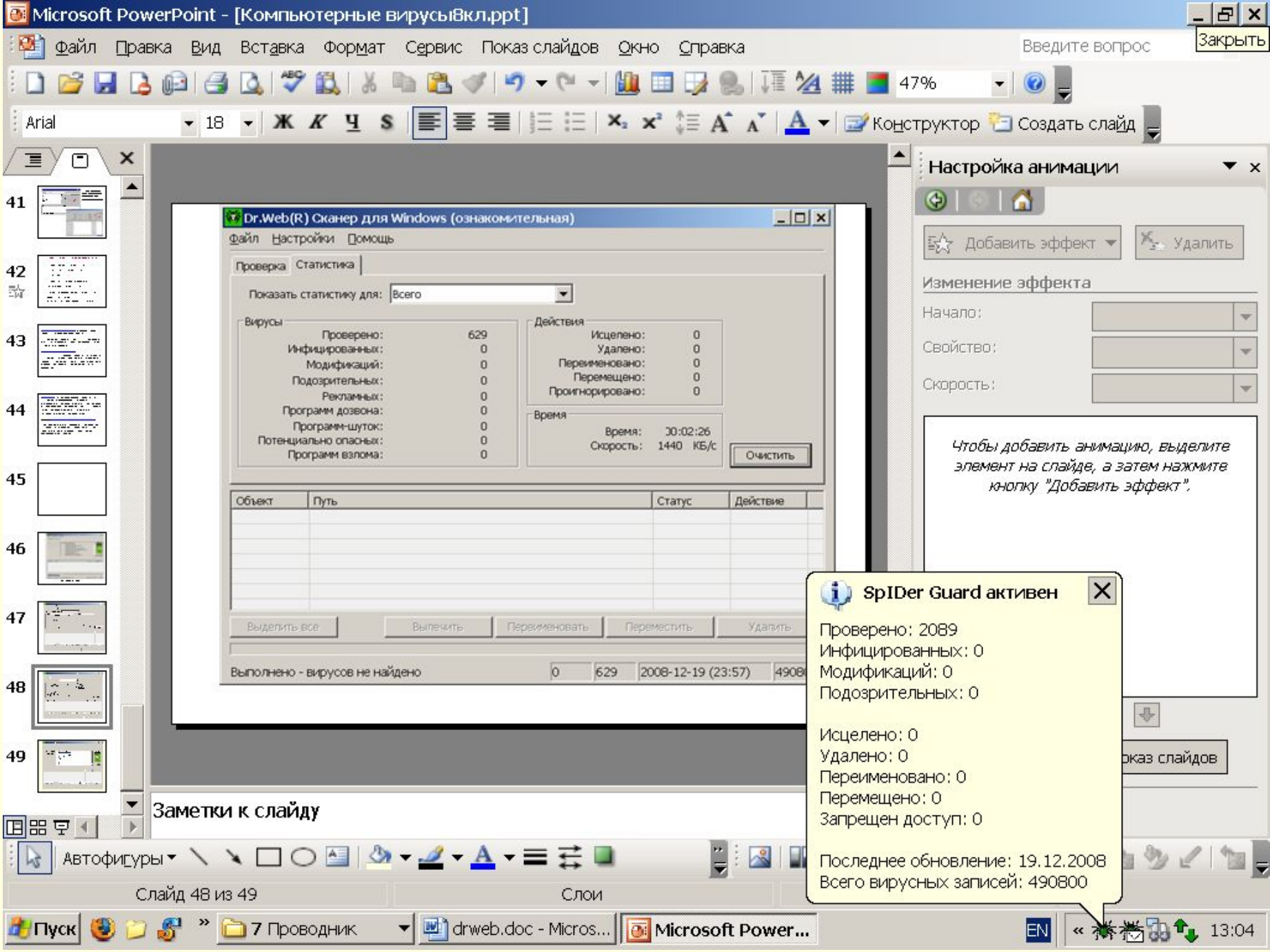
Программа запускается по запросу пользователя или по расписанию и производит антивирусную проверку компьютера.

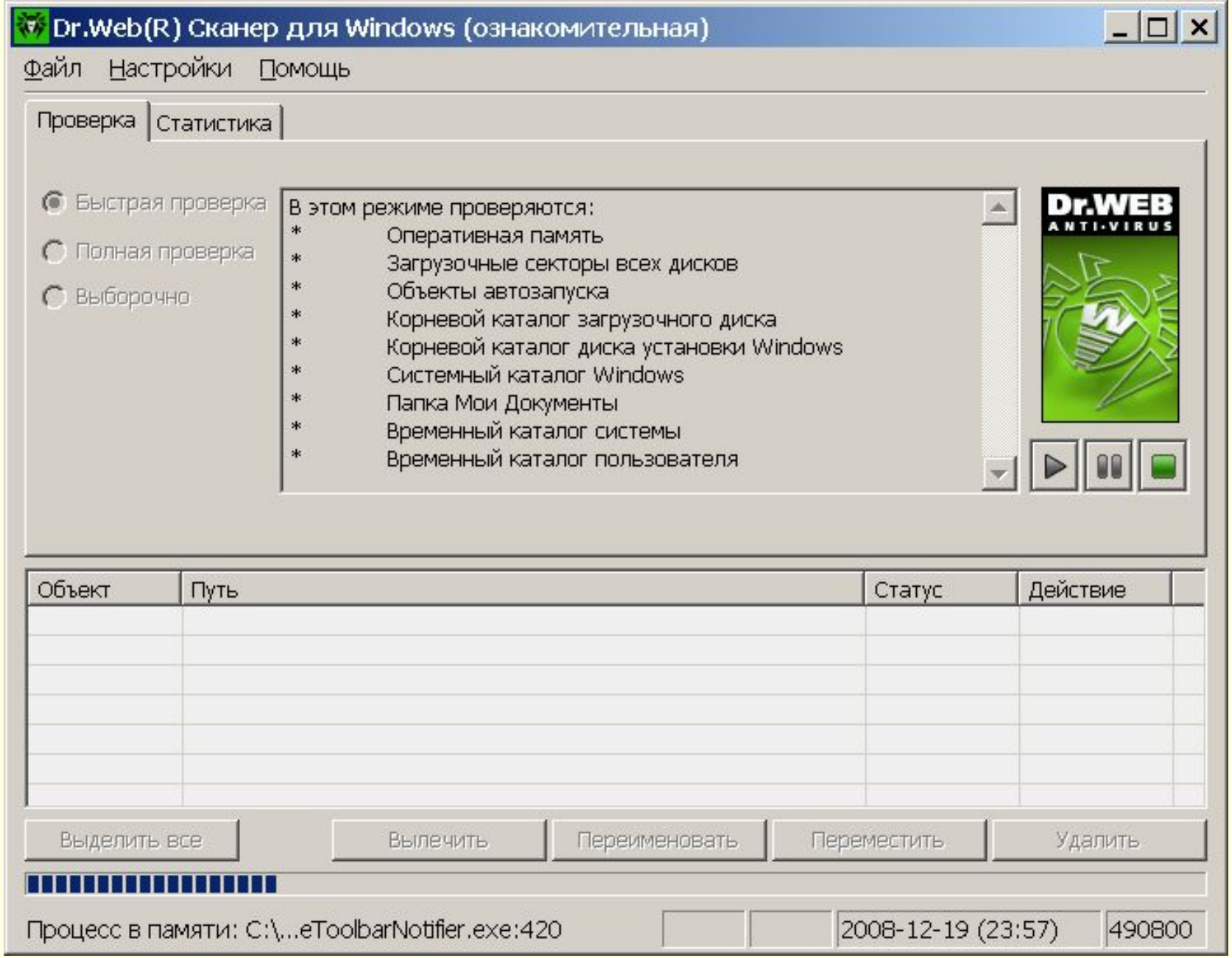
SpIDer Guard для Windows – антивирусный сторож (монитор). Программа постоянно находится в оперативной памяти, осуществляя проверку файлов «на лету», а также обнаруживая проявления вирусной активности.

SpIDer Mail – почтовый антивирусный сторож. Программа перехватывает обращения компьютера к почтовым серверам, обнаруживает и обезвреживает почтовые вирусы до получения писем почтовым клиентом с сервера или до отправки письма на почтовый сервер.

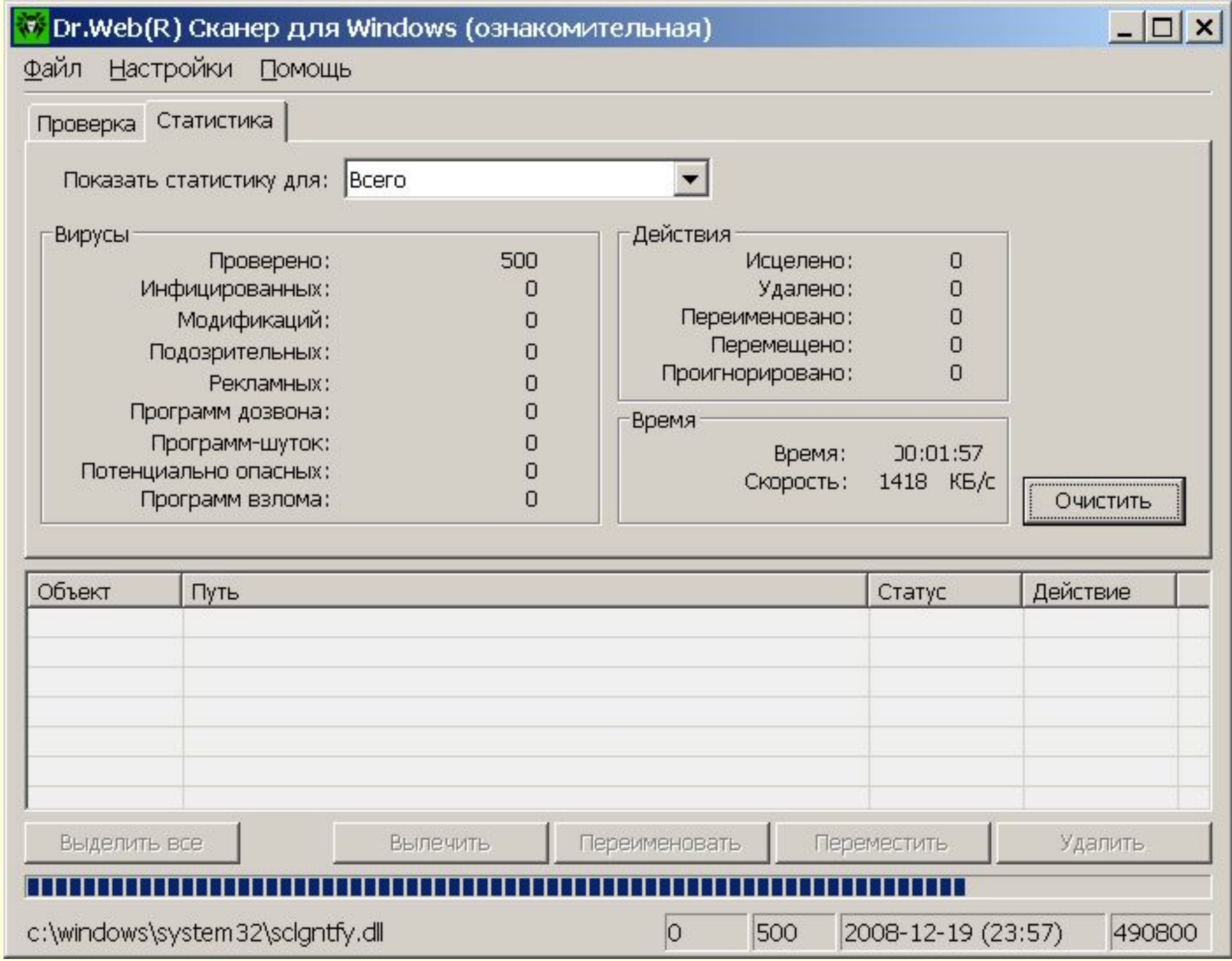
Dr.Web Модуль автоматического обновления–

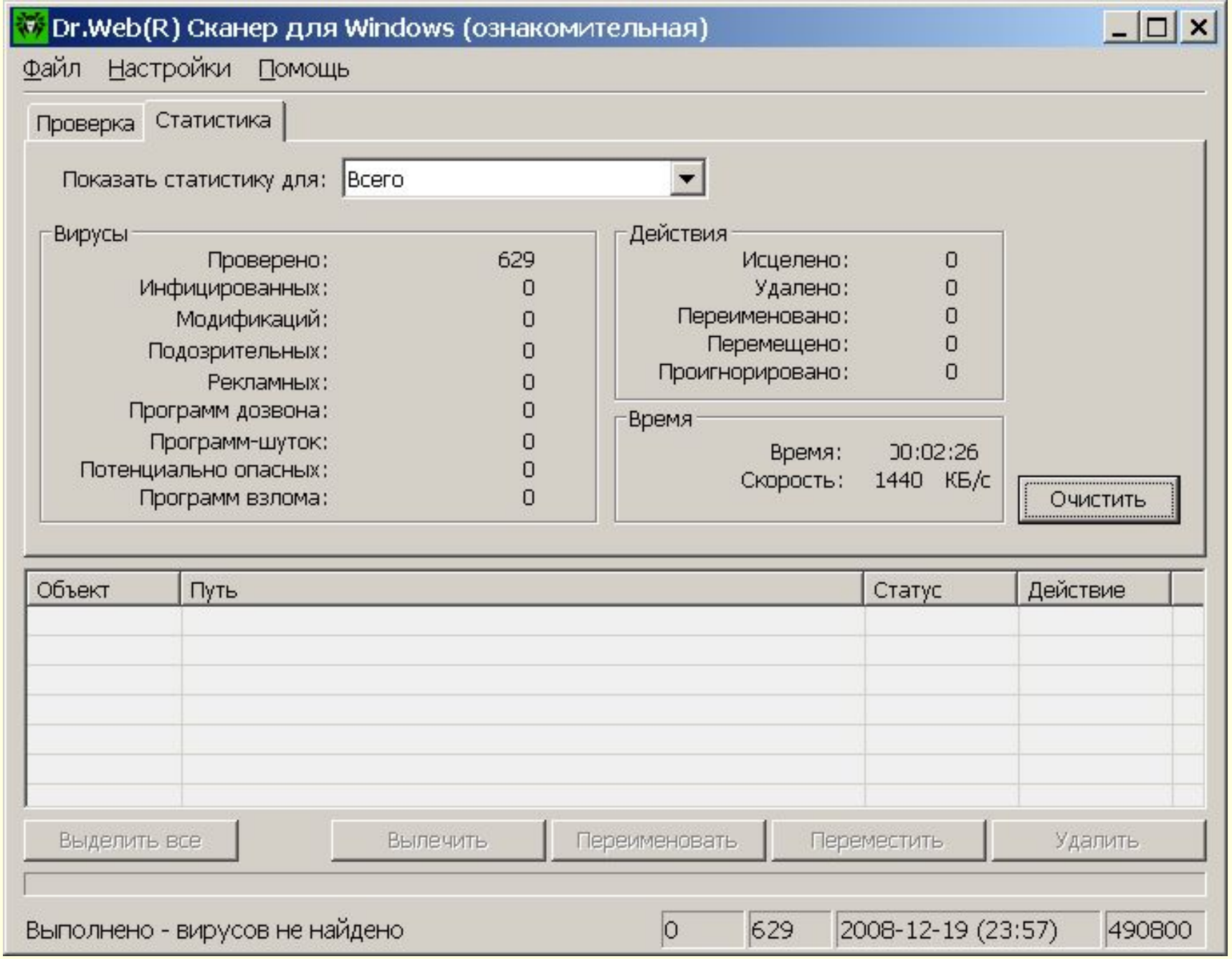
позволяет зарегистрированным пользователям получать обновления вирусных баз и других файлов комплекса, а также производит их автоматическую установку.

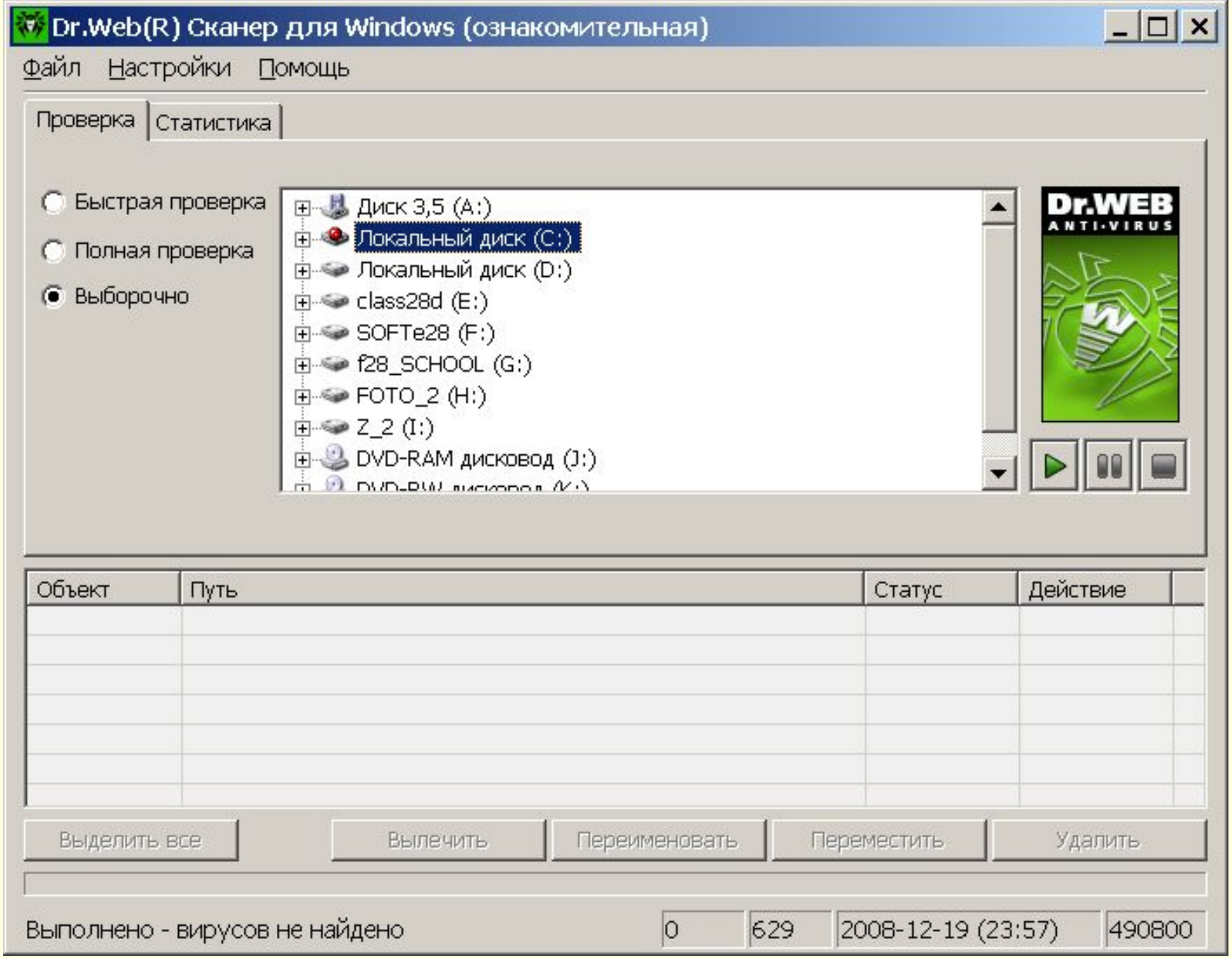

Microsoft PowerPoint - [Компьютерные вирусы8кл.ppt]
Файл Правка Вид Вставка Формат Сервис Показ слайдов Окно Справка
Введите вопрос
Закрыть
Конструктор
Создать слайд
Настройка анимации
Добавить эффект
Удалить
Изменение эффекта
Начало:
Свойство:
Скорость:
Чтобы добавить анимацию, выделите элемент на слайде, а затем нажмите кнопку "Добавить эффект".
Dr.Web(R) Сканер для Windows (ознакомительная)
Файл Настройки Помощь
Проверка Статистика
Показать статистику для: Всего
Вирусы
Проверено: 629
Инфицированных: 0
Модификаций: 0
Подозрительных: 0
Рекламных: 0
Программ дозвона: 0
Программ-шуток: 0
Потенциально опасных: 0
Программ взлома: 0
Действия
Исцелено: 0
Удалено: 0
Переименовано: 0
Перемещено: 0
Проигнорировано: 0
Время
Время: 30:02:26
Скорость: 1440 КБ/с
Очистить
Объект
Путь
Статус
Действие
Выделить все
Вылечить
Переименовать
Переместить
Удалить
Выполнено - вирусов не найдено
0
629
2008-12-19 (23:57)
SpIDer Guard активен
Проверено: 2089
Инфицированных: 0
Модификаций: 0
Подозрительных: 0
Исцелено: 0
Удалено: 0
Переименовано: 0
Перемещено: 0
Запрещен доступ: 0
Последнее обновление: 19.12.2008
Всего вирусных записей: 490800
Заметки к слайду
Автофигуры
Слайд 48 из 49
Слои
Пуск
7 Проводник
drweb.doc - Micros...
Microsoft Power...
EN
13:04



Окно сканера DrWeb


Dr.Web(R) Сканер для Windows (ознакомительная)
Файл Настройки Помощь
Проверка Статистика
Показать статистику для: Всего
Вирусы
Проверено: 500
Инфицированных: 0
Модификаций: 0
Подозрительных: 0
Рекламных: 0
Программ дозвона: 0
Программ-шуток: 0
Потенциально опасных: 0
Программ взлома: 0
Действия
Исцелено: 0
Удалено: 0
Переименовано: 0
Перемещено: 0
Проигнорировано: 0
Время
Время: 00:01:57
Скорость: 1418 КБ/с
Очистить
Объект
Путь
Статус
Действие
Выделить все
Вылечить
Переименовать
Переместить
Удалить
c:\windows\system32\sclgntfy.dll
0
500
2008-12-19 (23:57)
490800


Dr.Web(R) Сканер для Windows (ознакомительная)
Файл Настройки Помощь
Проверка Статистика
Показать статистику для: Всего
Вирусы
Проверено: 629
Инфицированных: 0
Модификаций: 0
Подозрительных: 0
Рекламных: 0
Программ дозвона: 0
Программ-шуток: 0
Потенциально опасных: 0
Программ взлома: 0
Действия
Исцелено: 0
Удалено: 0
Переименовано: 0
Перемещено: 0
Проигнорировано: 0
Время
Время: 00:02:26
Скорость: 1440 КБ/с
Очистить
Объект
Путь
Статус
Действие
Выделить все
Вылечить
Переименовать
Переместить
Удалить
Выполнено - вирусов не найдено
0
629
2008-12-19 (23:57)
490800


Dr.Web(R) Сканер для Windows (ознакомительная)
Файл Настройки Помощь
Проверка Статистика
Быстрая проверка
Полная проверка
Выборочно
Диск 3,5 (A:)
Локальный диск (C:)
Локальный диск (D:)
class28d (E:)
SOFTe28 (F:)
f28_SCHOOL (G:)
FOTO_2 (H:)
Z_2 (I:)
DVD-RAM дисковод (J:)
Dr.WEB
ANTI-VIRUS
Объект
Путь
Статус
Действие
Выделить все
Вылечить
Переименовать
Переместить
Удалить
Выполнено - вирусов не найдено
0
629
2008-12-19 (23:57)
490800