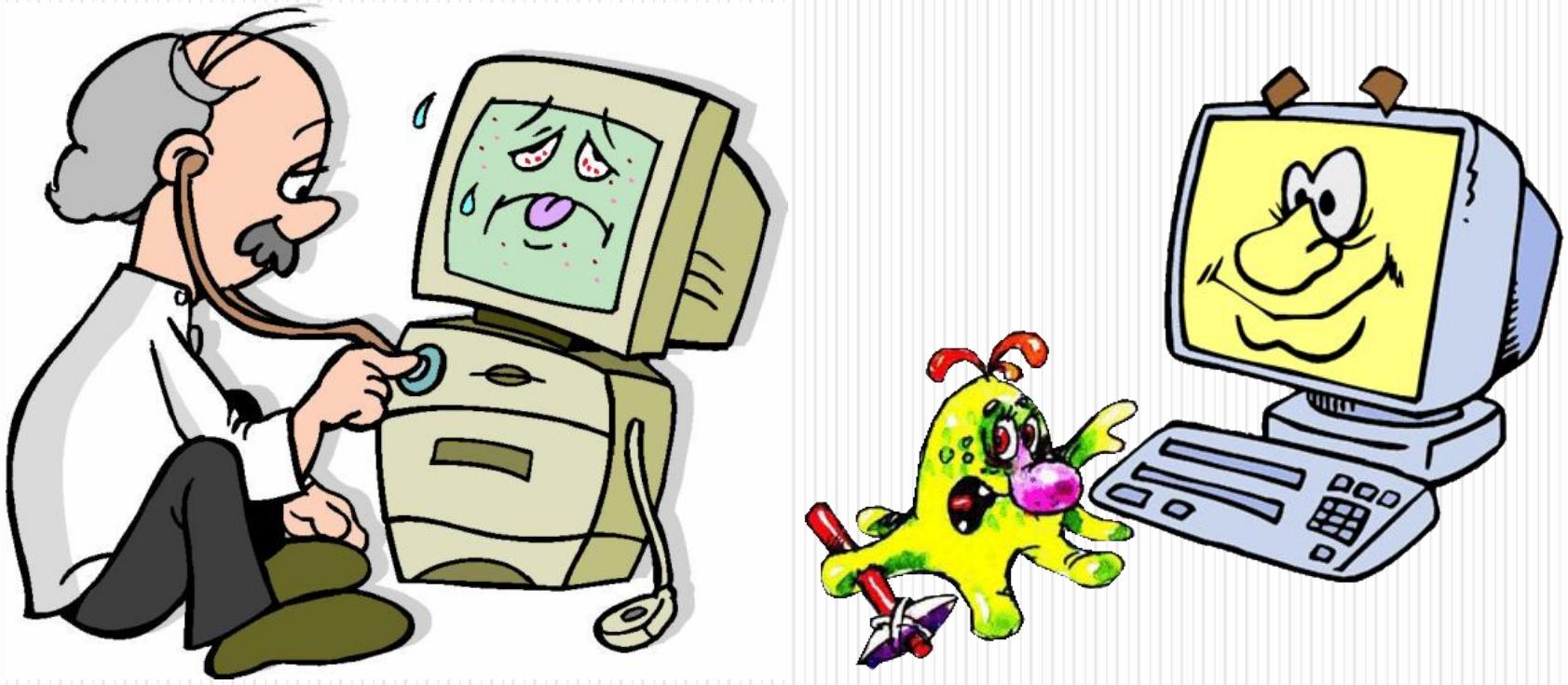
Компьютерные вирусы и антивирусные программы



Компьютерный вирус – специально созданная небольшая программа, способная к саморазмножению, засорению компьютера и выполнению других нежелательных действий.

Энциклопедия вирусов
«Лаборатории Касперского
http://www.viruslist.com/ru/viruses/encyclopedia

ИСТОРИЯ КОМПЬЮТЕРНЫХ ВИРУСОВ

Первый прототип вируса появился еще в 1971г..

Программист Боб Томас, пытаясь решить задачу передачи информации с одного компьютера на другой, создал программу Creeper, самопроизвольно «перепрыгивавшую» с одной машины на другую в сети компьютерного центра.

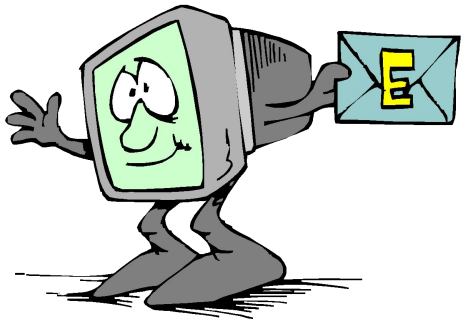
Правда эта программа не саморазмножалась, не наносила ущерба.

ЧЕМ ОПАСЕН КОМПЬЮТЕРНЫЙ ВИРУС?

После заражения компьютера вирус может активизироваться и начать выполнять вредные действия по уничтожению программ и данных.

Активизация вируса может быть связана с различными событиями:

- *наступлением определённой даты или дня недели;*
- *запуском программы;*
- *открытием документа…*



Последствия заражения

- общее замедление работы компьютера и уменьшение размера свободной оперативной памяти;
- некоторые программы перестают работать или появляются различные ошибки в программах;

- на экран выводятся посторонние символы и сообщения, появляются различные звуковые и видеоэффекты;
- размер некоторых исполнимых файлов и время их создания изменяются;
- некоторые файлы и диски оказываются испорченными;
- компьютер перестает загружаться с жесткого диска.

По способу заражения файловые вирусы разделяются на:

- Перезаписывающие вирусы.
- Вирусы-компаньоны.
- Файловые черви.
- Вирусы-звенья.
- Паразитические вирусы.
- Вирусы, поражающие исходный код программы.

ФАЙЛОВЫЕ ВИРУСЫ

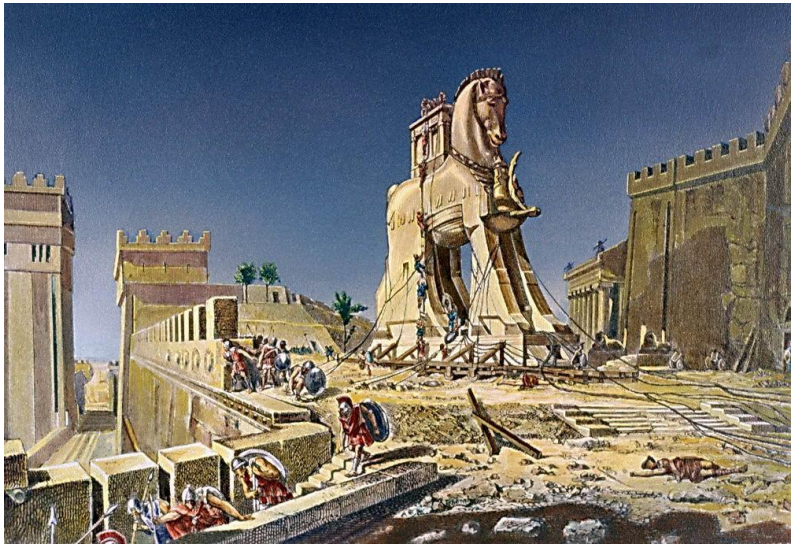
Внедряются в программы и активизируются при их запуске. После запуска заражённой программой могут заражать другие файлы до момента выключения компьютера или перезагрузки операционной системы.

МАКРОВИРУСЫ

Заражают файлы документов, например текстовых. После загрузки заражённого документа в текстовый редактор макровирус постоянно присутствует в оперативной памяти компьютера и может заражать другие документы. Угроза заражения прекращается только после закрытия текстового редактора.

Сетевые вирусы

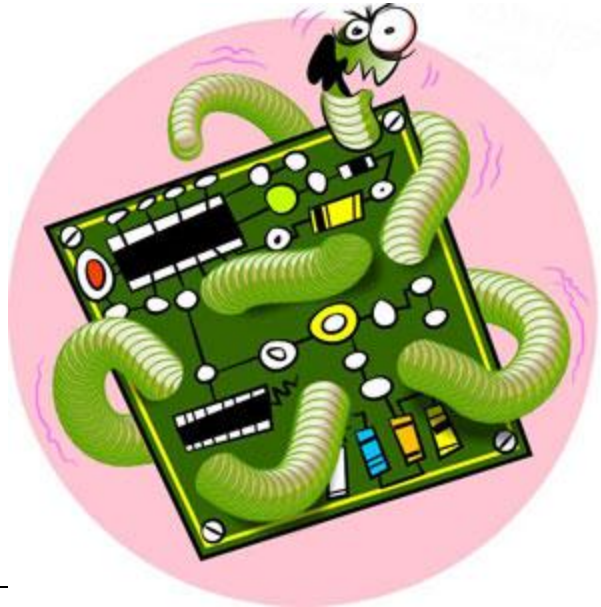
- сетевые черви
- троянские программы
- хакерские утилиты



Сетевые вирусы

Сетевые черви – программы, распространяющие свои копии по локальным или глобальным сетям с целью:

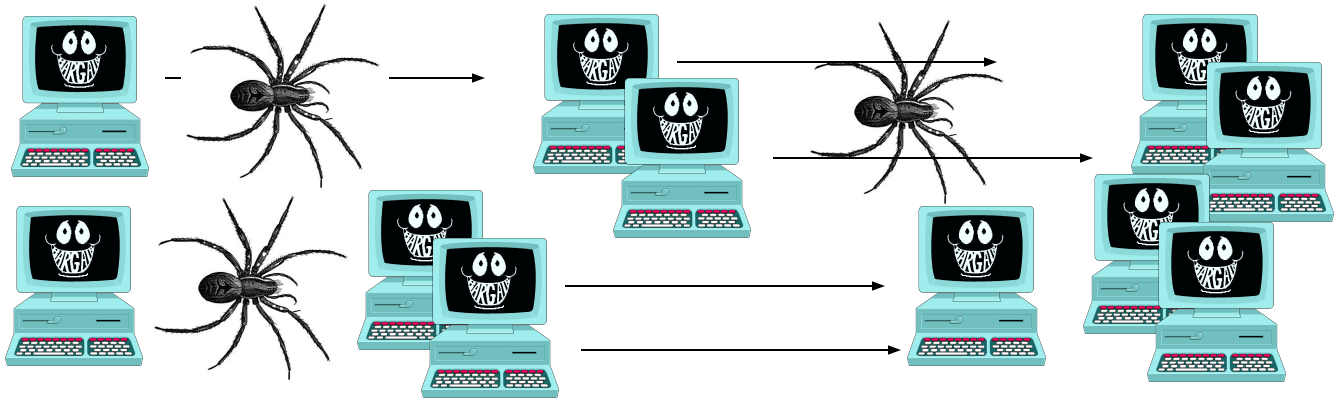
- проникновения на удаленные компьютеры;
- запуска своей копии на удаленном компьютере;
- дальнейшего распространения на другие.



Сетевые вирусы

Троянские программы. «Троянский конь» употребляется в значении: тайный, коварный замысел. Эти программы осуществляют различные несанкционированные пользователем действия:

- сбор информации и ее передача злоумышленникам;
- разрушение информации или злонамеренная модификация;
- нарушение работоспособности компьютера;
- использование ресурсов компьютера в неблаговидных целях.



По деструктивным особенностям 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 алгоритмах работы которых заведомо заложены процедуры, которые могут привести к потере программ, уничтожить данные, стереть необходимую для работы компьютера информацию, записанную в системных областях памяти, и даже, как гласит одна из непроверенных компьютерных легенд, способствовать быстрому износу движущихся частей механизмов - вводить в резонанс и разрушать головки некоторых типов винчестеров.

Пути проникновения вирусов

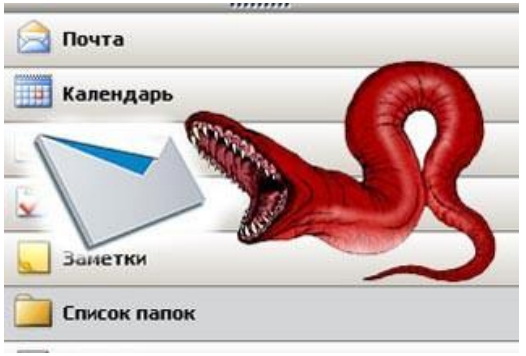
Глобальная сеть Интернет

Основным источником вирусов на сегодняшний день является глобальная сеть Internet. Возможно заражение через страницы Интернет ввиду наличия на страницах всемирной паутины различного «активного» содержимого: скриптов, ActiveX-компоненты, Java-апплетов. В этом случае используются уязвимости программного обеспечения, установленного на компьютере пользователя, либо уязвимости в ПО владельца сайта, а ничего не подозревающие пользователи зайдя на такой сайт рискуют заразить свой компьютер.

Пути проникновения вирусов

Электронная почта

Сейчас один из основных каналов распространения вирусов. Обычно вирусы в письмах электронной почты маскируются под безобидные вложения: картинки, документы, музыку, ссылки на сайты. В некоторых письмах могут содержаться действительно только ссылки, то есть в самих письмах может и не быть вредоносного кода, но если открыть такую ссылку, то можно попасть на специально созданный веб-сайт, содержащий вирусный код. Многие почтовые вирусы, попав на компьютер пользователя, затем используют адресную книгу из установленных почтовых клиентов типа Outlook для рассылки самого себя дальше.



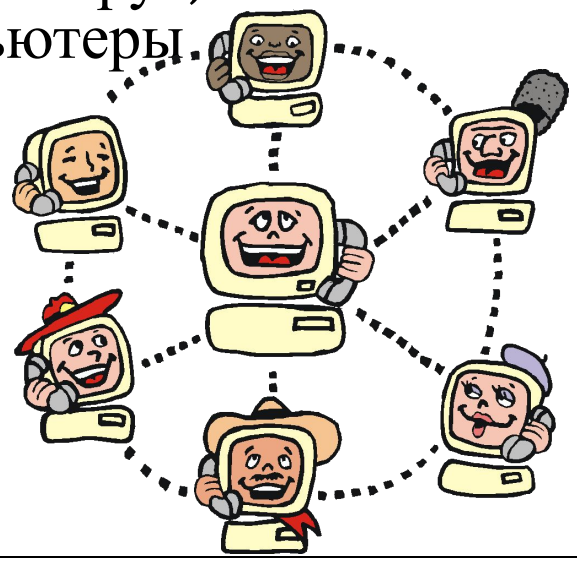
Пути проникновения вирусов

Локальные сети

Третий путь «быстрого заражения» —

локальные сети. Если не принимать необходимых мер защиты, то зараженная рабочая станция при входе в сеть заражает один или несколько служебных файлов на сервере

На следующий день пользователи при входе в сеть запускают зараженные файлы с сервера, и вирус, таким образом, получает доступ на компьютеры пользователей.



Пути проникновения вирусов

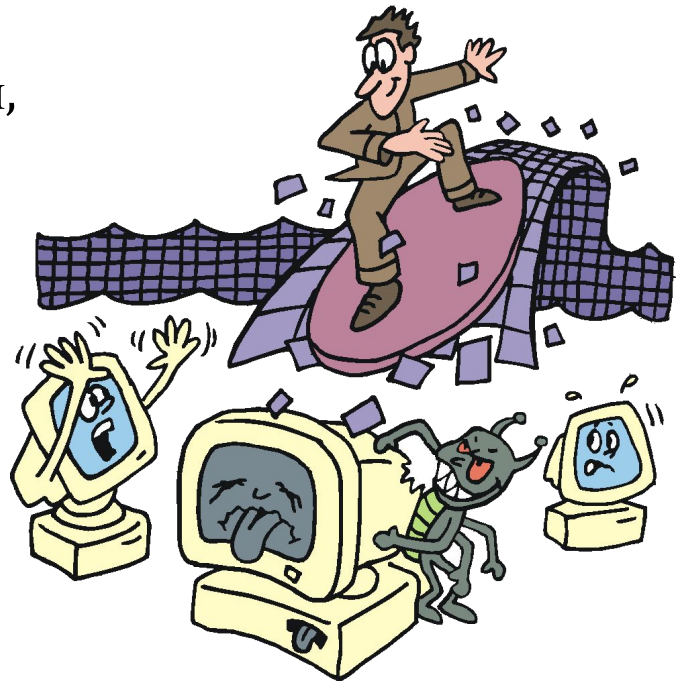
Персональные компьютеры «общего пользования»

Опасность представляют также компьютеры, установленные в учебных заведениях. Если один из учащихся принес на своих носителях вирус и заразил какой-либо учебный компьютер, то очередную «заразу» получат и носители всех остальных учащихся, работающих на этом компьютере.

То же относится и к домашним компьютерам, если на них работает более одного человека.

Пиратское программное обеспечение

Нелегальные копии программного обеспечения, как это было всегда, являются одной из основных «зон риска». Часто пиратские копии на дисках содержат файлы, зараженные самыми разнообразными типами вирусов.



Пути проникновения вирусов

Ремонтные службы

Достаточно редко, но до сих пор вполне реально заражение компьютера вирусом при его ремонте или профилактическом осмотре. Ремонтники — тоже люди, и некоторым из них свойственно наплевательское отношение к элементарным правилам компьютерной безопасности.

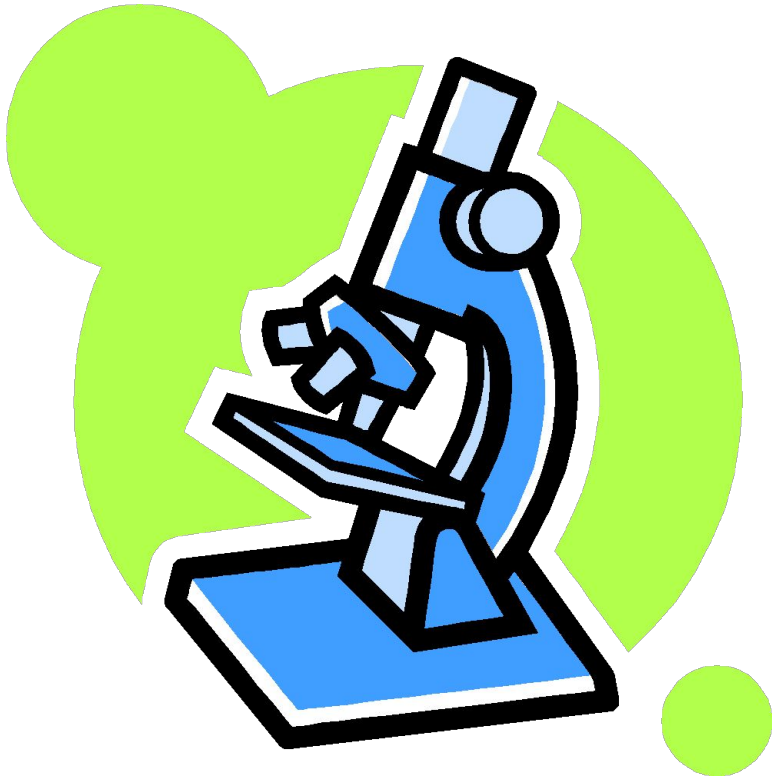
Съемные накопители

В настоящее время большое количество вирусов распространяется через съёмные накопители, включая цифровые фотоаппараты, цифровые видеокамеры, цифровые плееры (MP3-плееры), сотовые телефоны.

Методы защиты

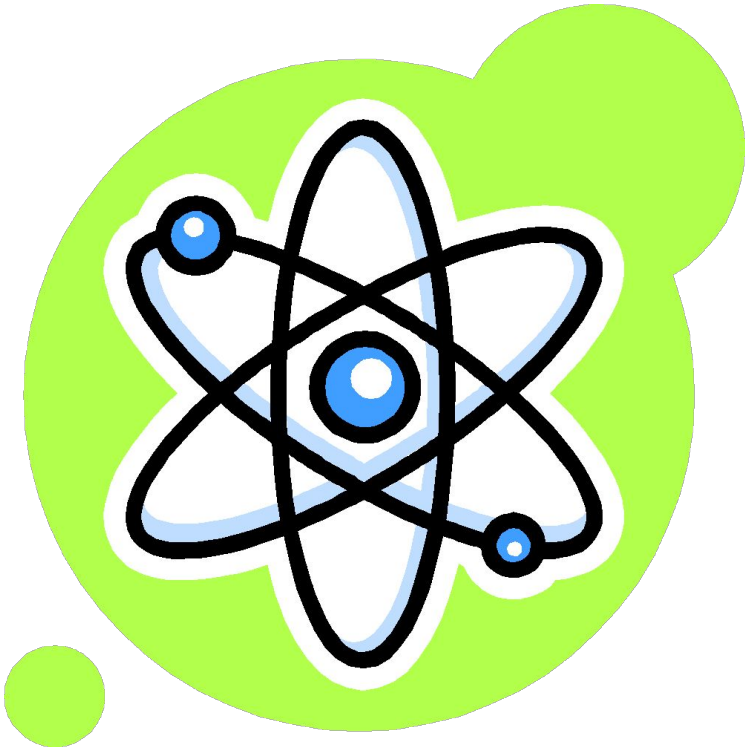
- Защита локальных сетей.
- Использование дистрибутивного ПО.
- Резервное копирование информации.
- Использование антивирусных программ.
- Не запускать непроверенные файлы.

Программы-ревизоры



Принцип их работы состоит в подсчете контрольных сумм для присутствующих на диске файлов/системных секторов. Эти суммы затем сохраняются в базе данных антивируса, как, впрочем, и некоторая другая информация: длины файлов, даты их последней модификации и т.д. При последующем запуске CRC-сканеры сверяют данные, содержащиеся в базе данных, с реально подсчитанными значениями. Если информация о файле, записанная в базе данных, не совпадает с реальными значениями, то CRC-сканеры сигнализируют о том, что файл был изменен или заражен вирусом.

Программы-фильтры



Антивирусные блокировщики — это резидентные программы, перехватывающие «вирусо-опасные» ситуации и сообщающие об этом пользователю. К «вирусо-опасным» относятся вызовы на открытие для записи в выполняемые файлы, запись в boot-сектора дисков или винчестера, попытки программ остаться резидентно и т.д., то есть вызовы, которые характерны для вирусов в моменты из размножения.

Программы-вакцины

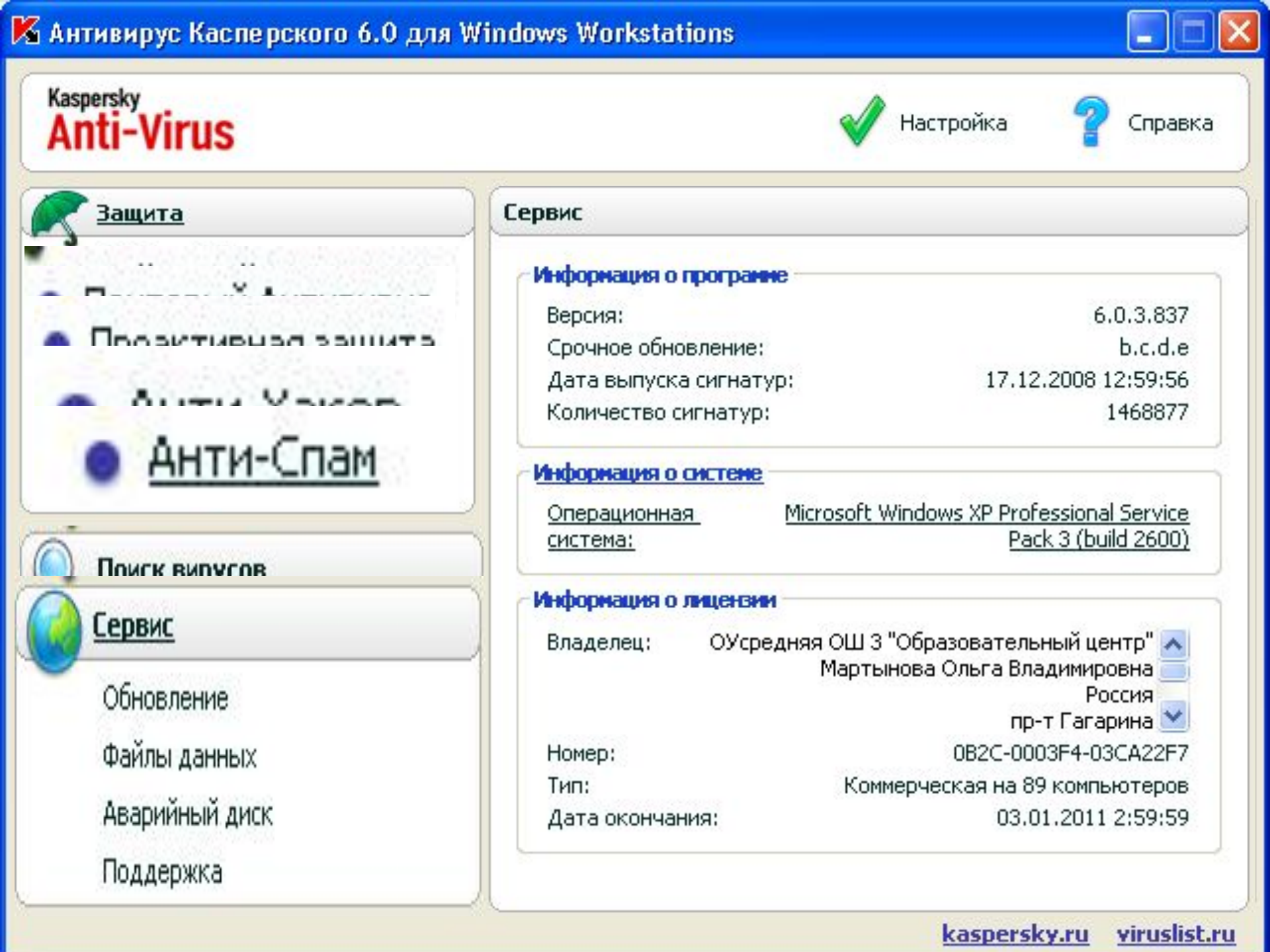
Иммунизаторы делятся на два типа:

- иммунизаторы, сообщающие о заражении;
- иммунизаторы, блокирующие заражение каким-либо типом вируса.


ADinf32 v3.02/Pro (Настройки по умолчанию)
Advanced Diskinfoscope™
Режимы
Без CRC
Не обнов.
Рабочий стол
Мой компьютер
Дискета 3,5" A:
Диск C: 20 янв 2005 г.
Диск D: 20 янв 2005 г.
http://www.adinf.com
Диски: 0
Готово 0 из 0
Настройки
Старт
Выход
Нажмите "Старт" для начала работы или F1 для помощи

Возможности программы Антивирус Касперского

- защита от вирусов, троянских программ и червей;
- защита от шпионских, рекламных и других потенциально опасных программ;
- проверка файлов, почты и интернет-трафика в реальном времени;
- проактивная защита от новых и неизвестных угроз;
- антивирусная проверка данных на любых типах съемных носителей;
- проверка и лечение архивированных файлов;
- контроль выполнения опасных макрокоманд в документах *Microsoft Office*;
- средства создания диска аварийного восстановления системы.


Антивирус Касперского 6.0 для Windows Workstations
Kaspersky
Anti-Virus
Настройка
Справка
Защита
Анти-Спам
Поиск вирусов
Сервис
Обновление
Файлы данных
Аварийный диск
Поддержка
Сервис
Информация о программе
Версия: 6.0.3.837
Срочное обновление: b.c.d.e
Дата выпуска сигнатур: 17.12.2008 12:59:56
Количество сигнатур: 1468877
Информация о системе
Операционная система: Microsoft Windows XP Professional Service Pack 3 (build 2600)
Информация о лицензии
Владелец: ОУсредняя ОШ 3 "Образовательный центр"
Мартынова Ольга Владимировна
Россия
пр-т Гагарина
Номер: 0B2C-0003F4-03CA22F7
Тип: Коммерческая на 89 компьютеров
Дата окончания: 03.01.2011 2:59:59
kaspersky.ru
viruslist.ru

СРЕДСТВА ЗАЩИТЫ ПЕРСОНАЛЬНОЙ ИНФОРМАЦИИ

- *антивирусные программы*
- *брандмауэры или файрволы*
- *антишпионы*

СПАСИБО за внимание