***Лабораторная работа №7***

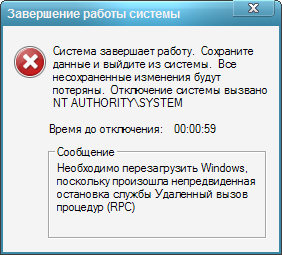
**Тема: Основные признаки присутствия на компьютере вредоносных программ**

***Цель работы:*** *получение практических навыков по выявлению* *вредоносных программ на локальном компьютере под управлением Microsoft* *Windows XP.*

**Задание 1. Изучение настроек браузера (Internet Explorer)**

Действия вредоносных программ бывают явными, косвенными и скрытыми. Если первые можно заметить сразу, то косвенные и тем более скрытые требуют от пользователя определенной квалификации - необходимо знать что, где и как нужно искать.

Не все вредоносные программы стремятся спрятаться – многие из них ведут себя весьма активно, то есть явно проявляют себя. Это характерно для троянских и , так называемых, рекламных программ. Явные проявления наиболее часто выражаются в неожиданно появляющихся рекламных баннерах, в изменении домашней страницы в браузере или появляющихся на рабочем столе окнах, как показано на [рис. 1](http://www.intuit.ru/studies/courses/2291/591/lecture/7620?page=1#image.19.1).



**Рис. 1.**

Некоторые рекламные вредоносные программы являются по сути безвредными, так как их основная цель – привлечь внимание к определенному товару или услуге.

Вредоносными программами с косвенными признаками называются программы, которые пытаются отключить или полностью удалить антивирус, блокировать обновление антивирусных баз. Соответственно, если антивирус вдруг ни с того, ни с сего перестал запускаться, либо перестали открываться сайты антивирусных компаний при том, что в целом доступ в Интернет работает нормально, это могут быть проявления вирусов. Вредоносные программы, которые никак не выдают себя, называются скрытыми. Обнаружить их можно только по подозрительным процессам в памяти компьютера, в нестандартной сетевой активности, в изменениях системного реестра.

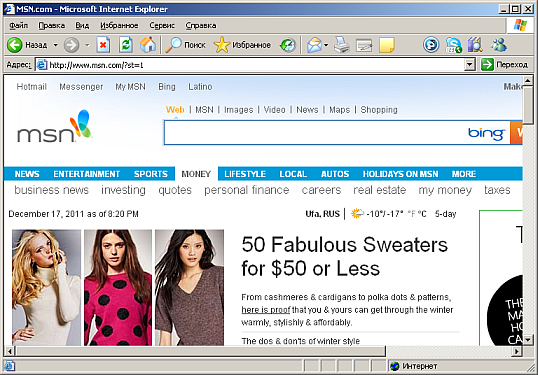
В этом задании предлагается исследовать явные проявления вирусной активности на примере несанкционированного изменения настроек браузера. Этот механизм используется для того, чтобы вынудить пользователей зайти на определенный сайт. Для этого меняется адрес домашней страницы, то есть адрес сайта, который автоматически загружается при каждом открытии браузера.

1. Откройте браузер **Internet Explorer**, воспользовавшись одноименным ярлыком на рабочем столе или в системном меню **Пуск / Программы**



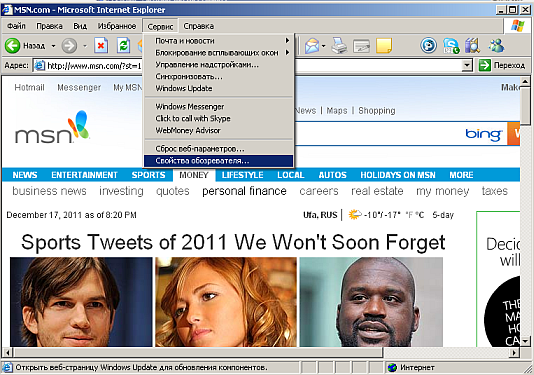
**Рис. 2.**

1. Если у Вас открыт и настроен доступ в Интернет и после установки операционной системы стартовая страница изменена не была, должна открыться страница по умолчанию - [http://www.msn.com](http://www.intuit.ru/studies/courses/2291/591/lecture/19.http:/www.msn.com).



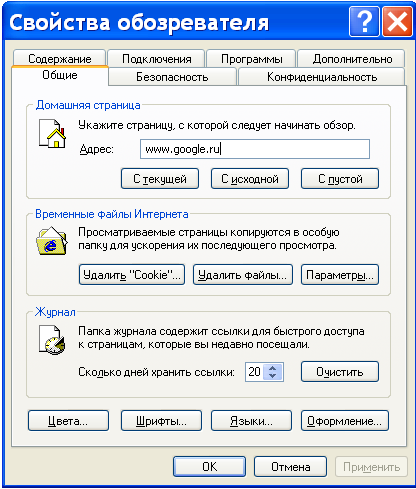
**Рис. 3.**

1. Для того чтобы проверить настройку стартовой страницы воспользуйтесь в меню **Сервис** пунктом **Свойства обозревателя**.



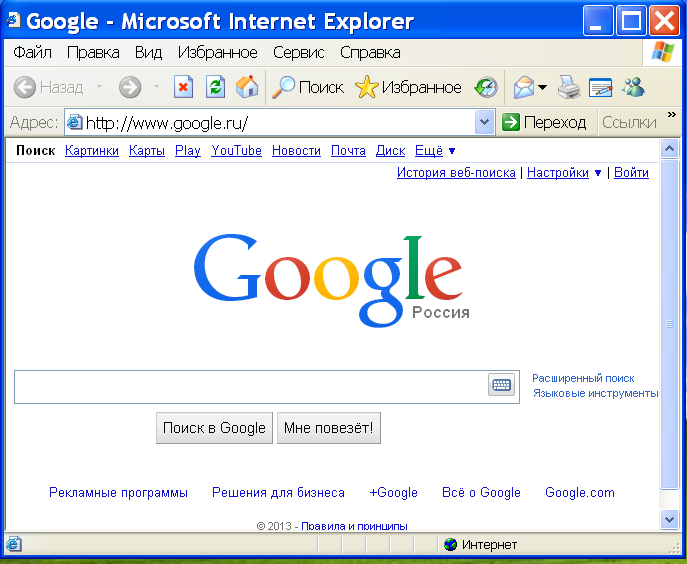
**Рис. 4.**

1. В открывшемся окне **Свойства обозревателя** на закладке **Общие** в поле **Адрес** указан адрес стартовой страницы. Измените поле, введя любой другой адрес, например,<http://www.google.ru>, и нажмите ОК. Закройте и снова откройте Internet Explorer.



**Рис. 5.**

1. Убедитесь, что теперь первым делом была загружена страница <http://www.google.ru>



**Рис. 6.**

Если Ваш браузер самостоятельно стал при запуске загружать посторонний сайт, проверьте его настройки: какой адрес выставлен в качестве домашней страницы. Некоторые вредоносные программы ограничиваются изменением настройки стартовой страницы, и для устранения последствий их действия необходимо только изменить страницу на желаемую. Однако следует иметь ввиду, что это может быть только частью вредоносной нагрузки. Поэтому при выявлении несанкционированной смены адреса домашней страницы проверьте свой компьютер с помощью антивирусной программы.

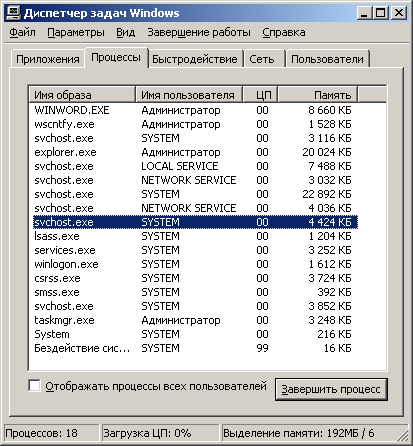
**Задание 2. Подозрительные процессы**

Основным проявлением вредоносной программы является наличие подозрительного процесса в списке запущенных процессов(программ). Имея достаточную квалификацию можно проанализировать список вручную и выявить вредоносную программу вручную. Этот способ является одним из наиболее эффективных для выявления вредоносных программ, имеющих только косвенные или скрытые признаки.

Естественно необходимо четко понимать и уметь отличать легальные процессы (например, системные или запущенные программы) от подозрительных. Для того чтобы посмотреть список запущенных на данный момент программ необходимо воспользоваться **Диспетчером задач Windows**.

**Диспетчер задач Windows** - это стандартная утилита, входящая в любую версию Microsoft Windows. C ее помощью можно в режиме реального времени отслеживать выполняющиеся приложения и запущенные процессы, оценивать загруженность системных ресурсов компьютера и использование сети.

1. Для того, чтобы открыть **Диспетчер задач Windows** нажмите одновременно клавиши **Ctrl+Alt+Delete.**



**Рис. 7.**

Открывшееся окно содержит пять закладок, отвечающих пяти видам активности, которые отслеживает Диспетчер: приложения, процессы, быстродействие (использование системных ресурсов),Сеть и Пользователи. По умолчанию открывается вторая закладка Процессы.

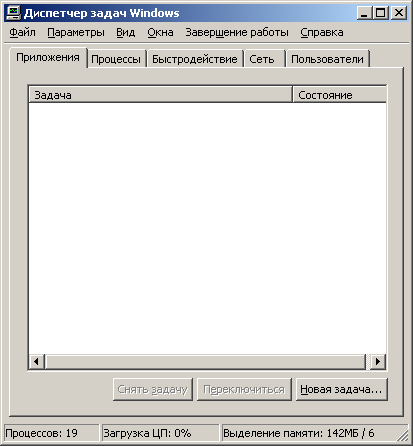
Если на компьютере не запущены никакие пользовательские программы, список текущих процессов должен содержать только служебные процессы операционной системы.

**Внимание! Эти процессы необходимы системе для стабильной работы**

|  |  |  |
| --- | --- | --- |
| Таблица 1. | | |
| **Название процесса** | **Описание** | **Возможность завершения** |
| CSRSS.EXE | Сокращение от "Client/Server Run – Time Subsystem".Процесс отвечает за окна консоли, за создание и удаление потоков, а также частично за работу 16-битной среды MS-DOS. Он относится к подсистеме Win32 пользовательского режима (WIN32.SYS же относится к ядру Kernel) и должен всегда выполняться. | - |
| EXPLORER.EXE | Пользовательская среда, содержащая такие компоненты, как Панель задач, Рабочий стол и тому подобное. Его практически всегда можно закрывать и снова открывать без каких-либо последствий. | + |
| INTERNAT.EXE | Загружает различные выбранные пользователем языки ввода, показывает на панели задач значок "RL", который позволяет переключать языки ввода. С помощью панели управления возможно без использования данного процесса безо всяких проблем переключать раскладку клавиатуры. | + |
| LSASS.EXE | Этот локальный сервер авторизации отвечает за IP-директивы безопасности (Интернет- протоколы) и загружает драйвер безопасности. Он запускает процесс, отвечающий за авторизацию пользователей. При успешной авторизации пользователя приложение создает и присваивает ему специальный протокол. Все запущенные далее процессы используют этот протокол. | - |
| MSTASK.EXE | Отвечает за службу планирования Schedule, которая предназначена для запуска различных приложений в определенное пользователем время. | - |
| SMSS.EXE | Диспетчер сеансов запускает высокоуровневые подсистемы и сервисы. Процесс отвечает за различные действия, например запуск Winlogon- и Win32-процессов, а также за операции с системными переменными. Когда Smss определяем, что Winlogon или Csrss закрыты, он автоматически выключает систему. | - |
| SPOOLSV.EXE | Обеспечивает создание очереди на печать, временно сохраняя документы и факсы в памяти. | - |
| SVCHOST.EXE | Этот всеобъемлющий процесс служит хостом для других процессов, запускаемых с помощью DLL. Поэтому иногда работают одновременно несколько Svchost. С помощью команды "tlist - s" можно вывести на экран все процессы, использующие Svchost. | - |
| SERVICES.EXE | Процесс управления системными службами. Запуск, окончание, а также все остальные действия со службами происходят через него. | - |
| SYSTEM | Этот процесс выполняет все потоки ядра Kernel. | - |
| SYSTEM IDLE PROCESS | Этот процесс выполняется на любом компьютере. Нужен он, правда, всего лишь для мониторинга процессорных ресурсов, не используемых другими программами. | - |
| TASKMGR.EXE | Процесс диспетчера задач, закрывать который крайне не рекомендуется. | + |
| WINLOGON.EXE | Отвечает за управление процессами авторизации пользователей. Он активен, только когда пользователь нажимает "Ctrl+Alt+Del". | - |
| WINMGTM.EXE | Основной компонент клиентской службы Windows. Процесс запускается одновременно с первыми клиентскими приложениями и выполняется при любом запросе служб. В XP он запускается как клиент процесса Svchost. | - |

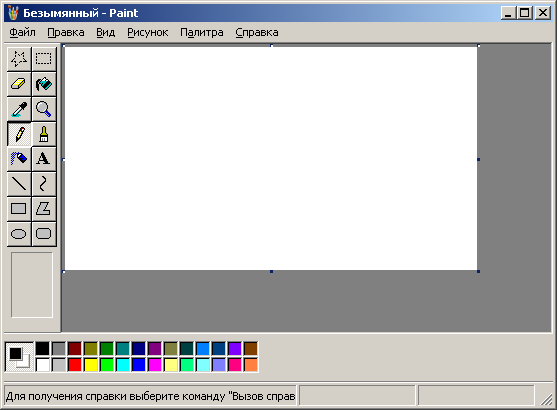
Представленные в таблице процессы необходимы для работы Windows XP. В Windows Vista,7,8 их значительно больше.

1. Для каждого процесса выводятся его параметры: имя образа, имя пользователя, от чьего имени был запущен процесс, загрузка этим процессом процессора и объем занимаемой им оперативной памяти (настраивается в меню "Вид").
2. Поскольку в данный момент не должна быть запущена ни одна пользовательская программа, процессор должен быть свободен. Следовательно, "Бездействие системы" должно оказаться внизу списка с достаточно большим процентом "использования" процессора. На рис. 7 это 99 %.
3. Если Вы обнаружили подозрительный процесс, не относящийся к системным, завершите его вручную с помощью кнопки "Завершить процесс". Естественно, это не избавляет от наличия вируса на компьютере, а только останавливает его работу в данное время. Далее следует провести проверку с помощью антивируса.
4. Выпишите все запущенные процессы на лист бумаги или в текстовый файл и перейдите к закладке **Приложения**. В данном окне отобразятся все запущенные в настоящий момент приложения. Если в настоящий момент запущенных приложений нет, появится пустое окно, показанное на рис. 8.



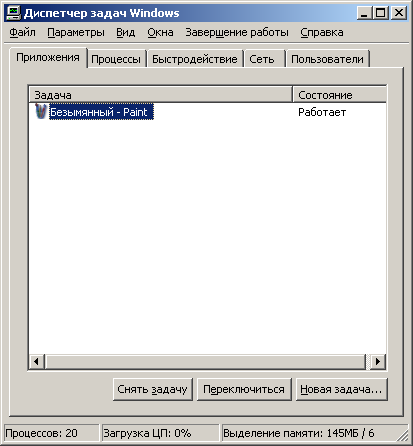
**Рис. 8.**

1. Не закрывая окна **Диспетчера задач Windows**, откройте программу **Paint**. Для этого воспользуйтесь системным меню **Пуск / Программы / Стандартные / Paint**. Дождитесь запуска **Paint**.



**Рис. 9.**

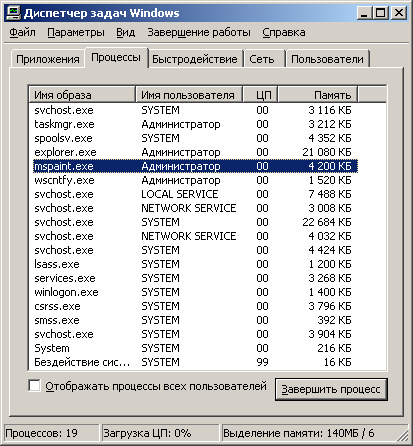
Не закрывая приложение **Paint**, вернитесь к окну **Диспетчера задач Windows** и проследите за изменениями на закладке **Приложения**. В списке запущенных приложений появился **Paint**.



**Рис. 10.**

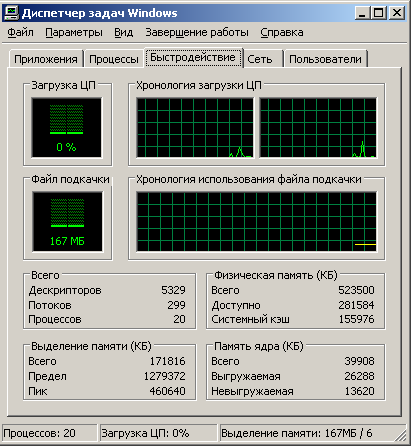
Иногда случается так, что программа вызывает ошибку - тогда в ее состоянии будет написано "Не отвечает". Если некое ранее бесперебойно работающее приложение начало часто без видимых причин переходить в состояние "Не отвечает", это может быть косвенным признаком заражения.

1. Перейдите к закладке **Процессы** и сравните список в тем, который видели ранее. Найдите процесс, соответствующий **Paint**, - **mspaint.exe**.



**Рис. 11.**

1. Перейдите к закладке **Быстродействие**. Внимательно изучите расположенные тут графики. Всплески на графиках соответствуют по времени определенным действиям, например, запуску программы, требовательной к ресурсам. Если Вы не запускали ничего, а всплески есть, это может быть причиной для более детального исследования компьютера.

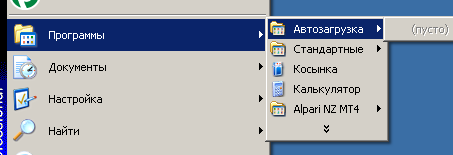


**Рис. 12.**

**Задание 3. Элементы автозапуска**

Вредоносная программа, так же как любая другая программа, для работы нуждается в запуске. При этом возможно два варианта – сделать так, чтобы пользователь сам запустил вредоносную программу, либо внедриться в конфигурационные файлы и запускаться одновременно с легитимными программами. Оптимальным вариантом для вредоносной программы является "прописывание" себя в автозагрузку при запуске операционной системы.

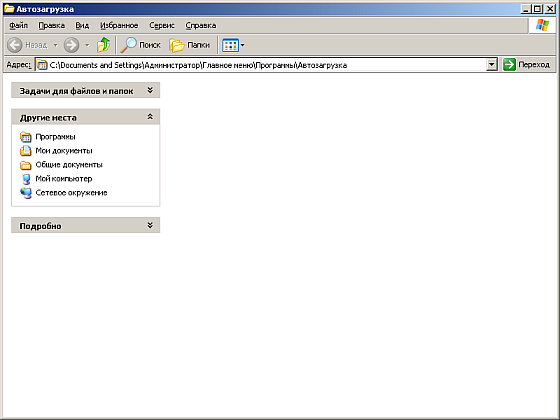
1. Самый простой способ добавить какую-либо программу в автозагрузку - это поместить ее ярлык в раздел **Автозагрузка** системного меню **Пуск / Программы**. По умолчанию, сразу после установки операционной системы этот раздел пуст.



**Рис. 13.**

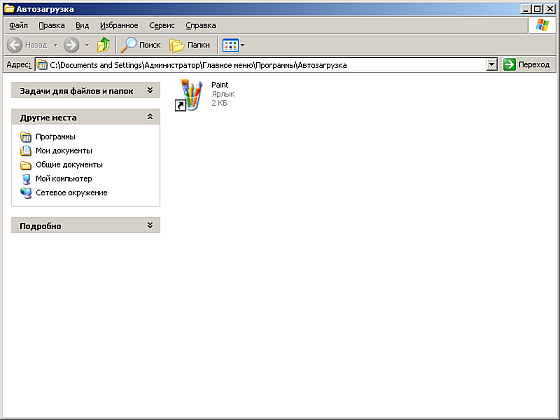
1. Добавьте в список автозагрузки свою программу (создайте ярлык на любую программу, например Калькулятор или Блокнот и поместите его в группу Автозагрузка). Для этого дважды щелкните левой клавишей мыши по названию группы **Автозагрузка**. Откроется папка автозагрузки в стандартном окне – [рис. 14](http://www.intuit.ru/studies/courses/2291/591/lecture/7620?page=3#image.19.14). По умолчанию путь к папке следующий:

**C:\Documents and Settings\Администратор\Главное меню\Программы\Автозагрузка**



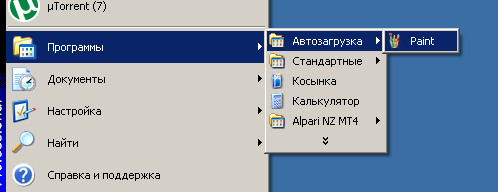
**Рис. 14.**

Всё, что нужно сделать, для того, чтобы программа запускалась автоматически при запуске операционной системы – поместить в данную папку ее ярлык.



**Рис. 15.**

1. Закройте окно и убедитесь, что теперь раздел **Автозагрузка** в меню **Пуск / Программы** содержит **Paint**.

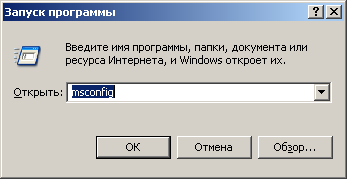


**Рис. 16.**

1. Перезагрузите компьютер. Убедитесь, что в процессе загрузки операционной системы автоматически запустился **Paint**.
2. Отсутствие подозрительных ярлыков в разделе **Автозагрузка** системного меню **Пуск / Программы**, к сожалению, не гарантирует, что ни одна вредоносная программа не запускается автоматически. Технически для автозапуска нужно добавить соответствующую запись в системный реестр операционной системы.

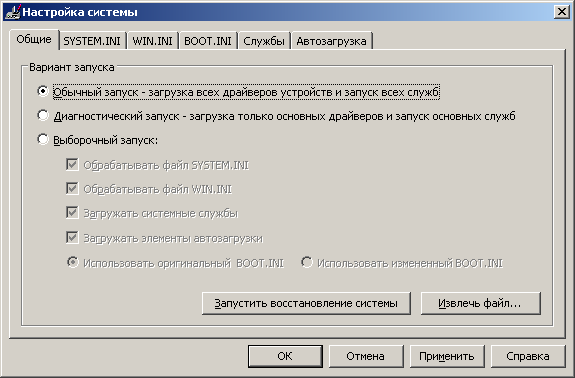
Несмотря на то, что реестр Windows очень большой, существует оболочка, позволяющая с ним работать напрямую - **regedit**. Но делать это рекомендуется только в крайнем случае. Для большинства ситуаций, связанных с автозапуском, достаточно использовать системную утилиту **Настройка системы** .

Запустите ее. Для этого откройте системное меню **Пуск** и перейдите к пункту **Выполнить** и в открывшемся окне **Запуск программы** наберите **msconfig** и нажмите OK.



**Рис. 17.**

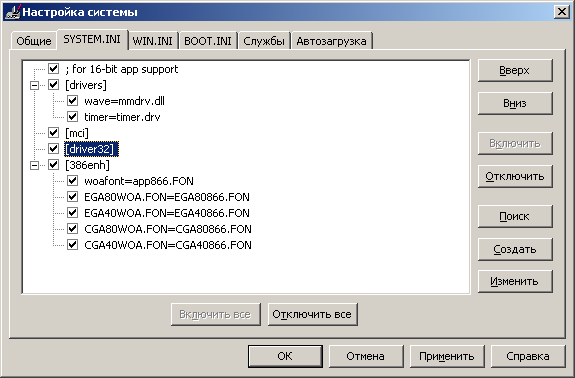
1. Ознакомьтесь с внешним видом окна утилиты **Настройка системы**. На первой закладке **Общие**, можно выбрать вариант запуска операционной системы. По умолчанию отмечен Обычный запуск. Он обеспечивает максимальную функциональность системы. Остальные два варианта запуска предназначены для диагностики.



**Рис. 18.**

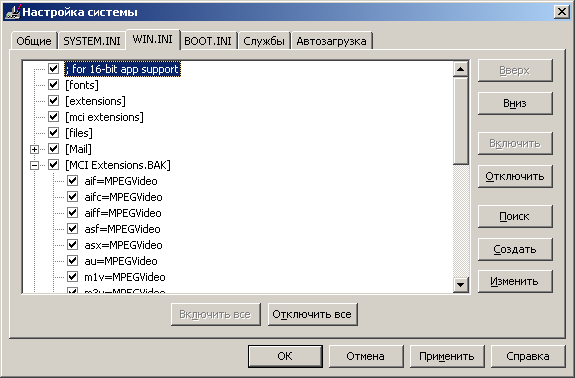
**Диагностический запуск** рекомендуется использовать также при подтвердившемся наличии вредоносной программы - если компьютер уже заражен, сразу установить антивирус в ряде случаев нельзя, например, если вирус сознательно блокирует запуск ряда антивирусных программ. Тогда, если нет возможности удалить или хотя бы временно обезвредить вирус вручную, рекомендует запустить операционную систему в безопасном режиме, инсталлировать антивирус и сразу же проверить весь жесткий диск на наличие вирусов.

1. Ознакомьтесь со списком запускаемых драйверов и других параметров операционной системы, перейдя к закладке SYSTEM.INI . Тут отображаются все ссылки, указанные в одноименном системном файле.



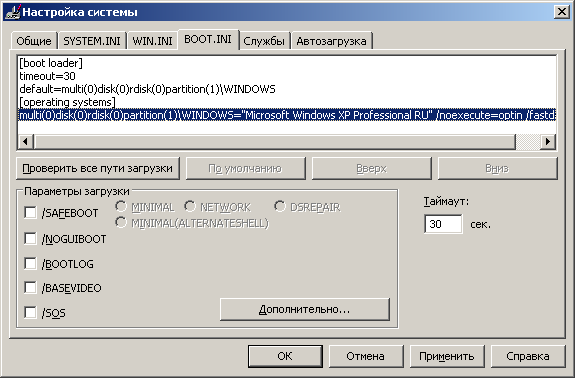
**Рис.**

1. Перейдите к аналогичной закладке **WIN.INI** и ознакомьтесь с ее содержимым.



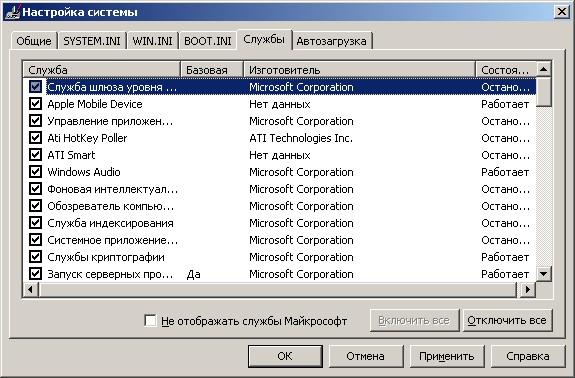
**Рис. 20.**

1. Следующая закладка **BOOT.INI** также отображает данные из одноименного файла. Как и предыдущие две, она также содержит системную информацию. Изменять ее можно только обладая соответствующими знаниями!



**Рис. 21.**

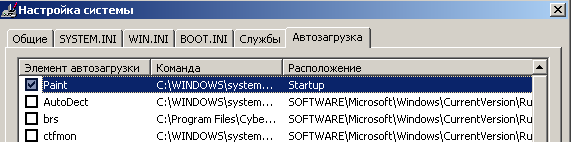
1. Перейдите на закладку **Службы**. Здесь представлен список всех служб, установленных в системе. Каждая служба представляет собой некое приложение, работающее в фоновом режиме. Например, антивирусный комплекс, обеспечивающий постоянную защиту, также встраивает свою службу, следовательно, она должна присутствовать в этом перечне. Так же и вирус может установить свою службу в системе.



**Рис. 22.**

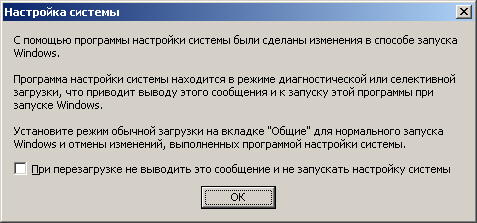
Определить, какие службы запущены и какую функцию они выполняют. Отключить на ваш взгляд ненужные в данной конфигурации службы, перезапустить систему и убедиться в правильности выбора.

1. Перейдите к последней закладке **Автозагрузка** и убедитесь, что в списке приложений, автоматически запускаемых при загрузке системы, есть **Paint**.



**Рис. 23.**

1. Отключите автоматическую загрузку **Paint**, убрав галочку напротив него в столбце **Элемент автозагрузки** и нажмите ОК. В открывшемся окне согласитесь на перезагрузку.
2. После того, как компьютер перезагрузится, система выведет предупреждение в виде окна, представленного на рис. 23.



**Рис. 24.**

1. Откройте окно **Настройка системы**. Обратите внимание, что теперь используется не обычный запуск, а выборочный. При этом полностью обрабатываются все элементы файлов SYSTEM.INI, WIN.INI и BOOT.INI, загружаются все службы, но флаг **Загружать элементы автозагрузки затенен**. Это означает неполную загрузку .
2. Перейдите к закладке **Автозагрузка** и убедитесь, что ее вид не изменился - **Paint** все так же присутствует в списке, но отключен.
3. Не закрывая окна **Настройка системы** проверьте, что Paint автоматически не запустился и раздел **Пуск / Программы / Автозагрузка** теперь снова пуст.
4. Необходимо учесть, что если выбрать после изменений **Обычную загрузку** – все файлы, находящиеся на вкладке **Автозагрузка** будут запускаться снова, в том числе и **Paint**.