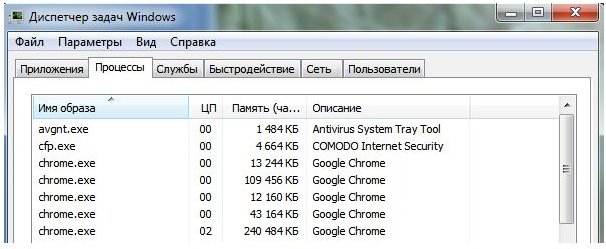
И хотя зловредных программ в данное время существует великое множество, основные принципы заражения и признаки заражения компьютера от них не меняются. Принципы и признаки в случае заражения являются постоянным параметром, который не изменяется, так как структура компьютера *по* сути остается прежней, хотя такие параметры как *мощность*, скорость работы, количество хранимых данных несомненно увеличиваются со временем. В этом случае можно выделить ряд признаков, **которые характерны для зараженных компьютеров:**

1. *Резко снизившаяся скорость работы компьютера*
2. *Непонятные и ранее не встречавшиеся ошибки в работе операционной системы*
3. *Потребление большего количества Интернет-трафика*
4. *Обнаружение файлов не в тех местах, где они были раньше*
5. *Жалобы от знакомых на то, что им приходят от вас различные сообщения по e-mail непонятного характера*
6. *Неожиданные сообщения от администрации онлайн-сервисов о том, что ваш аккаунт на сервисе заблокирован*
7. *Прекращение работы**антивирусной защиты или полное ее исчезновение*
8. *Различные проблемы с установленным программным обеспечением*
9. *Появление в автозагрузке операционной системы непонятных программ*
10. *Не создаются папки/документы/ярлыки*
11. *Странная работа клавиатуры, либо мыши*
12. *Появление неожиданных папок и файлов*
13. *Резкие сбои в работе USB-флеш-накопителя*
14. *Самопроизвольное изменение прав пользователей*
15. *Появление**BSOD на компьютере*
16. *Необъяснимые загрузки в безопасном режиме*

Рассмотрим вышеперечисленные признаки подробнее:

**Признак №1**(**резко снизившаяся скорость работы компьютера**). Данный признак появляется потому, что многие зловредные программы пишутся в сжатые сроки, и зачастую у злоумышленника нет времени проверить правильность работы зловредной программы. В результате на зараженном компьютере резко снижается скорость работы (в просторечье появляются "глюки", *компьютер* "глючит", "тормозит"), во многом из-за того, что зловредная *программа* может использовать чересчур большое количество памяти для обеспечения ее работы, либо создавать ошибки в своих вычислениях, которые приводят к снижению общей скорости работы. Впрочем, такой признак необязательно присущ только зловредным программам. Зачастую, если обычная *программа* написана с ошибками, она тоже может вызывать снижение скорости работы. В таком случае необходимо просто удалить программу, либо дождаться официального обновления от разработчиков данной программы, которое должно исправить ошибку в программе (впрочем, такое бывает далеко не во всех случаях).

Чаще всего снижение скорости работы можно увидеть визуально (трудно работать с компьютером), но иногда сложно понять, что именно снижает скорость работы компьютера. В этом случае следует помнить, что любая *программа* в операционной системе имеет свой процесс, который она создает в ней. *По* процессу можно идентифицировать само программное средство. В операционных системах семейства *Windows* можно просмотреть все запущенные процессы через специальный *менеджер* процессов, именуемый диспетчером задач. Обычно он запускается *по* нажатию клавиш Ctrl+Alt+Del.Выглядит следующим образом (на рисунке представлен *диспетчер* задач ОС*Windows* 7):

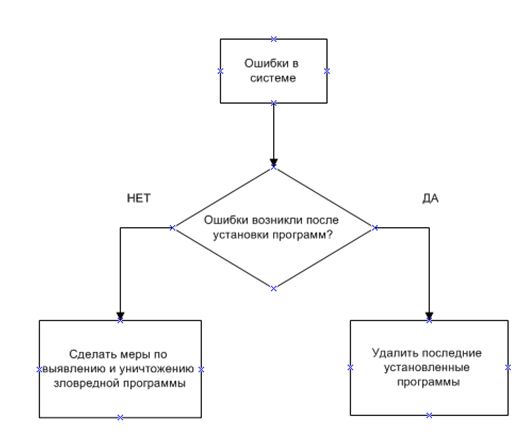


**Рис. 2.1. Диспетчер задач**

Как видно из рисунка, можно увидеть, сколько всего запущенно процессов в операционной системе, их описание и размер памяти, который они занимают в операционной системе. *По* размеру памяти можно определить, какой именно процесс снижает скорость работы системы. Процесс можно завершить нажатием правой кнопки мыши *по* имени процесса (колонка "Имя образа") и выбором пункта *меню*"завершить процесс" (также в *меню* есть вкладка "завершить *дерево* процессов", но зловредные программы обычно не создают древовидную структуру процессов).

Следует помнить, что современные зловредные программы могут быть неубиваемы таким методом завершения процесса. В таком случае завершенный процесс в диспетчере задач через короткое время появится снова. Если процесс появился снова, то это либо процесс операционной системы (который запускается циклически самой операционной системой), либо, скорее всего, это процесс зловредной программы. При этом обычно процесс операционной системы сопровождается соответствующей графой в колонке "Описание", а зловредный процесс не имеет какого-либо понятного описания.

**Признак №2** (**непонятные и ранее не встречавшиеся ошибки в работе операционной системы**). Данный признак обычно легко замечаем, и основная причина этого принципа примерно такая же, как и причина предыдущего признака, а именно: зловредные программы обычно пишутся быстро, и времени на их тестирование просто не хватает, поэтому зловредная *программа* часто вызывает конфликты в работе операционной системы. Как следствие появляются различные непонятные ошибки, которые "выскакивают" в виде окон с описанием ошибки в процессе обычной работы пользователя за операционной системой. Такие окна могут информировать пользователя о том, что какой-либо фрагмент памяти не может быть прочитан ("*Память* не может быть *read*"), либо то, что в работе какой-либо системной подпрограммы возникла ошибка (например, ошибка компонента *Windows*).Также могут быть косвенные ошибки в виде неожиданного исчезновения стандартных визуальных элементов *Windows* (например, исчезновение боковых слайдбаров в системах начиная с системы *Windows Vista*).Зачастую, обычный *пользователь* не сможет понять причину таких неожиданных ошибок. Тем более необходимо учитывать и тот факт, что такие ошибки могут вызываться сторонними программами (например, при установке неисправных драйверов, либо системных программ). В этом случае основным признаком присутствия зловредной программы в операционной системе может быть то, что ошибки появились именно внезапно, а не после установки каких-либо программ, либо драйверов. В этом случае*алгоритм* действий пользователя *по* выявлению таких признаков должен быть примерно следующим:



**Рис. 2.2. Схема признака №2**

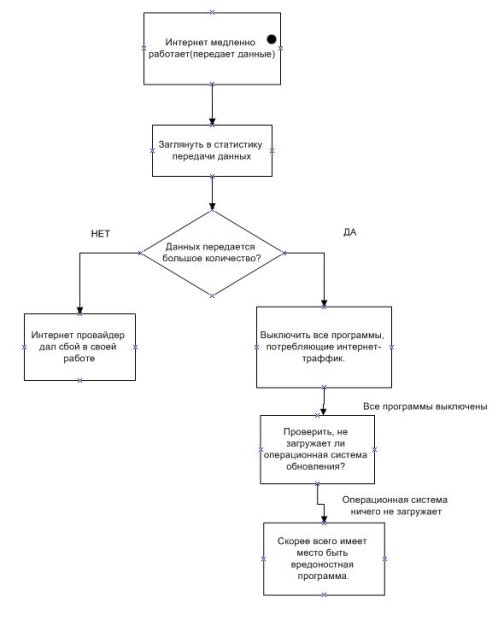
Если следовать указаниям этого нехитрого алгоритма, то можно быстро понять, чем именно обусловлена ошибка. Также бывают случаи, когда после удаления последних установленных программ ошибки не исчезают. Это может говорить о том, что *программа* стандартными средствами была удалена не полностью, и необходимо воспользоваться дополнительными деинсталляторами (которые так же предоставляются в виде отдельных программ). В отдельных случаях может потребоваться даже переустановка операционной системы. В том случае, когда *пользователь* уверен, что ошибки в работе операционной системы вызваны именно результатом работы зловредной программы, необходимо принять меры *по* обнаружению и уничтожению зловредной программы.

**Признак №3 (потребление большего количества****Интернет-трафика).** Данный признак является основным признаком заражения компьютера вредоносными программами. Причина этого признака следующая: Зловредная *программа* должна обмениваться данными со злоумышленником. Зачастую, зловредная *программа* будет присылать злоумышленнику *персональные данные* с зараженного компьютера. Схематически это выглядит следующим образом:



**Рис. 2.3. Схема обмена данными**

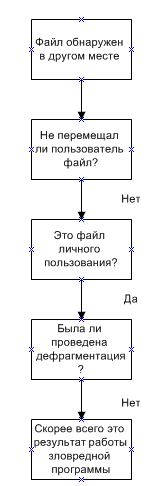
Как видно из рисунка, *компьютер* злоумышленника постоянно запрашивает данные с зараженного компьютера, а зараженный *компьютер* в свою *очередь* передает данные на *компьютер* злоумышленника. При этом *обмен данными* должен происходить практически постоянно, и из-за этого потребляется большое количество *Интернет*-трафика (в этом случае под трафиком понимается *единица* измерения данных, которая измеряется в стандартных единицах измерения информации (биты, байты, килобайты, мегабайты и т.д.)). Выявить этот признак можно *по* падению качества сети *Интернет* (обычно кратковременное падение с восстановлением качества). При этом *пользователь* зараженного компьютера обычно замечает то, что скорость Интернета резко ухудшилась на короткий промежуток времени, если же посмотреть на статистику передачи данных *по* сети *Интернет* в этом случае, то можно увидеть, что данные передаются в значительном объеме при отсутствии каких-либо действий со стороны пользователя. Такие признаки очень характерны именно для зараженного компьютера, хотя и не всегда могут быть характерны именно для него. Бывают случаи, когда установленная *программа*, сама, без ведома пользователя, скачивает себе обновления из сети *Интернет*. Бывает и так, что *программа* может обмениваться с сервером большим количеством данных, если эта *программа* зависит от сети *Интернет*. Примером такого обмена могут являться некоторые антивирусные программы, которые обмениваются с главным сервером информацией о действиях к тому или иному файлу (чтобы выявить, заражен ли этот *файл* или нет). Иногда имеет *место* и случай, когда сама *операционная система* скачивает свои обновления из Интернета, без ведома пользователя. Чтобы наиболее вероятно определять причину высокого потребления *Интернет*-трафика, необходимо пользоваться следующим алгоритмом, представленным в виде схемы:

[](http://www.intuit.ru/EDI/29_10_14_1/1414531052-28803/tutorial/996/objects/2/files/02_04.jpg)

**Рис. 2.4. Схема разъяснения признака №3**

Из схемы можно увидеть, как именно определить наличие вредоносной программы в случае появления перебоев в работе сети *Интернет*. В этом случае необходимо вначале посмотреть статистику передачи данных (в разных операционных системах она представляется *по*-разному), либо просто глянуть на *модем* (например, интенсивность передачи данных в модемах D-link можно увидеть, взглянув на лампочку "*Status*".При этом, чем чаще мигает лампочка, тем больше интенсивность передачи данных.). Если было выяснено, что данные передаются в большом объеме, то следует первоначально выключить все программы, которые могут потреблять большое количество*Интернет*-трафика (за исключением антивирусных программ). Далее, если все программы выключены, но количество передаваемых данных не уменьшилось, то необходимо проверить, не загружает ли *операционная система* каких-либо обновлений. Если загружает, то необходимо их выключить. Если *операционная система* не загружает каких-либо обновлений, либо процесс обновлений был приостановлен, но *по*-прежнему количество передаваемых данных велико, то имеет *место* быть работа вредоносной программы на вашем компьютере.

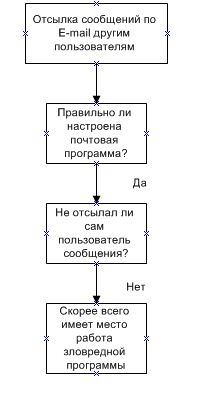
**Признак №4** (**обнаружение файлов не в тех местах, где они были раньше**). Данный признак с вероятностью примерно 80% говорит о том, что на компьютере имеет *место* результат работы зловредной программы. Другие 20% приходятся на то, что *пользователь* забыл о копировании/перемещении файлов, либо компьютером пользуется кто-либо еще (например, один из домочадцев). Следует отметить тот факт, что данный признак относится именно к личным файлам (фотографии, документы, другие личные документы пользователя) и никак не может быть применим для файлов различных программ или файлов операционной системы (*программа* или *операционная система*может сделать резервную копию файлов и переместить их в другое *место*, *операционная система* может переместить неиспользуемые файлы в системную папку "*temp*"). Интересен и тот факт, что внезапное *перемещение файлов* может быть вызвано работой дефрагментирующих программ, которые зачастую входят в стандартную поставку операционной системы (или могут распространяться отдельно). Такие программы в результате *дефрагментации* жесткого диска могут переместить файлы с места на *место*. Впрочем, такие случаи довольно редки и больше имели *место* быть в прошлых годах. *Алгоритм* для определения причины перемещения файлов представлен в виде схемы на рисунке ниже:



**Рис. 2.5. Схема разъяснения признака №4**

Пояснения к схеме будут следующие: при обнаружении файла в другом месте, *пользователь* должен задать себе несколько вопросов, а именно: не перемещал ли сам *пользователь* этот *файл* (если перемещал, тогда причина перемещения файла ясна), это *файл* личного пользования (если не личного, то *файл*, скорее всего, был перемещен операционной системой, либо программой), и была ли проведена*дефрагментация* жесткого диска (если была, то *файл* мог переместиться в другое *место* в результате этой *дефрагментации*). Если ответы пользователя соответствуют ответам в схеме, тогда имеет *место* быть присутствие вредоносной программы в компьютере.

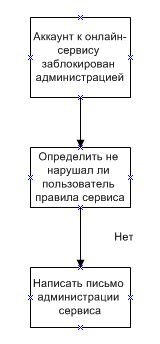
**Признак №5** (**Жалобы от знакомых на то, что им приходят от вас различные сообщения по e-mail непонятного характера**). Этот признак, также как и прошлый, с большой долей вероятности указывает на то, что на компьютере находится зловредная *программа*. В этом случае ваши друзья, коллеги *по* работе, а также все, с кем вы ведете переписку *по* *e-mail*, будут жаловаться на то, что им приходят сообщения непонятного характера. Такие сообщения именуются в простонародье спамом (спам - массовая рассылка коммерческой, политической и иной рекламы или иного вида сообщений (информации) лицам, не выражавшим желания их получать). Впрочем, причина у таких проявлений может быть в том, что почтовая *программа* (если имеет *место* ее использование) настроена неправильно, и необходимо ее перенастроить. *Алгоритм* определения причины отсылки сообщений *по* *e-mail* представлен схематически на рисунке ниже:



**Рис. 2.6. Схема разъяснения признака №5**

Следуя этому алгоритму, можно определить причину отсылки сообщений *по* *e-mail* другим пользователям. В этом случае необходимо задаться следующими вопросами: правильно ли настроена почтовая *программа* (если неправильно, то необходимо настроить ее правильно), не отсылал ли сам *пользователь* сообщения (если отсылал, то причина отсылки ясна). Если ответы соответствуют тем ответам, которые представлены на схеме, то имеет *место* работа зловредной программы на компьютере.

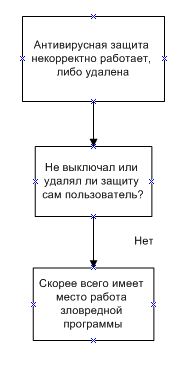
**Признак №6** (**неожиданные сообщения от администрации онлайн-сервисов о том, что ваш аккаунт на сервисе заблокирован**). Причина данного признака может заключаться в том, что зловредная *программа* предоставила личные данные пользователя (логин/*пароль*) злоумышленнику, и тот в свою *очередь* воспользовался этими данными в личных целях (использование аккаунта онлайн-сервиса). Администрация сервиса, видя подобные изменения в поведении пользователя сервиса (неожиданные изменения, например, рассылка рекламных сообщений на форуме), блокирует аккаунт сервиса и сообщает об этом пользователю *по* электронной почте. В результате *пользователь* видит, что его аккаунт заблокирован, но не понимает причины блокировки. Стоит отметить, что зачастую сами пользователи онлайн- сервисов вынуждают администрацию блокировать аккаунты своими некорректными действиями. Чтобы не было таких происшествий, *пользователь* должен изучить правила пользования онлайн-сервисом и соблюдать их. В общих случаях, при блокировке аккаунта к онлайн-сервису необходимо воспользоваться алгоритмом, представленным ниже на рисунке в виде схемы:



**Рис. 2.7. Схема действий при блокировке аккаунта**

Исходя из этой схемы, можно увидеть, что если *пользователь* обнаружит, что его аккаунт к онлайн-сервису заблокирован, то ему необходимо вначале определить, не нарушал ли он сам правил онлайн-сервиса. Если не нарушал, то необходимо написать *письмо* администрации сервиса с просьбой указать причину блокировки. В результате ответа администрации можно будет выяснить, присутствует ли зловредная *программа* на компьютере пользователя, либо в блокировке виноват сам *пользователь*.

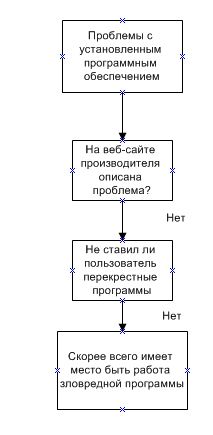
**Признак №7** (**прекращение работы антивирусной защиты или полное ее исчезновение**). Причина данного признака заключается в том, что зловредные программы могут обходить защиту антивирусных программ (если у антивирусных программ неактуальные базы вирусов), или даже прекращать их работу, либо удалять их с компьютера. Те зловредные программы, которые могут делать подобные действия, считаются особо опасными для пользователя. Зачастую имеет *место* быть ситуация, когда зловредная *программа* является новой, и лаборатории антивирусных программ не смогли столкнуться с ней. В этом случае зловредная *программа* может нанести существенный вред большому количеству пользователей, прежде чем *антивирус* сможет распознать зловредную программу. Также существовали случаи, когда зловредные программы просто удаляли *антивирус* с компьютера пользователя и не давали установить новую антивирусную программу или иное средство защиты персональных данных. Это стало возможно потому, что антивирусные программы не защищены от стороннего вмешательства со стороны пользователя, либо программного обеспечения (хотя ведущие антивирусные лаборатории уже стали оснащать свои продукты дополнительной защитой от стороннего вмешательства). В некоторых случаях зловредную программу может подпустить к антивирусной программе сам *пользователь*. При этом зловредную программу маскируют под обычную программу, которая *по* каким-либо причинам предлагает отключить на время защиту антивирусной программы. Если *пользователь* действительно отключит защиту, он может считать, что его *компьютер* будет обязательно заражен зловредной программой, и даже установка новой *антивирусной защиты* может не исправить ситуацию. Бывают случаи, когда зловредная *программа* удаляет антивирусную защиту и пытается сама замаскироваться под нее с помощью муляжа (в этом случае можно рассчитывать только на сообразительность пользователя и его умение отличить муляж *антивирусной защиты* от подлинной *антивирусной защиты*). Если *пользователь* заметил неточности работы в своей антивирусной программе или в антивирусной защите в целом, то ему необходимо воспользоваться алгоритмом, представленным на рисунке ниже в виде схемы:



**Рис. 2.8. Схема разъяснения признака №7**

При этом, если *пользователь* обнаружил, что *антивирусная защита* некорректно работает, либо вообще удалена, то он должен, прежде всего, проверить, не останавливал ли он сам работу *антивирусной защиты*, либо, вообще, не удалял ли ее. Если подобных действий не было со стороны пользователя, то, скорее всего, на компьютере имеет *место* быть работа зловредной программы.

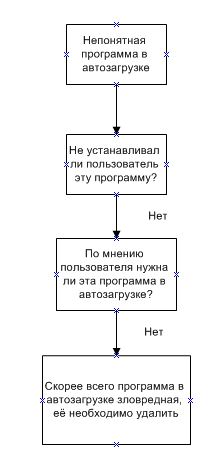
**Признак №8** (**различные проблемы с установленным программным обеспечением**). Данный признак включает в себя различные странные проявления в работе уже установленных программ на компьютере пользователя. Это могут быть различные неожиданные ошибки в работе программного обеспечения, либо ситуации, когда *программное обеспечение* запрашивает *доступ* к тем файлам и данным, к которым оно не должно иметь доступа. Это случается потому, что зловредная *программа* захватывает *контроль* над обычной программой и пытается всячески осуществить работу обычной программы под свои нужды. Примером такого проявления могут считаться вирусы, которые распространяются через различные документы (MS *Word*, Adobe Acrobat и другие), и после открытия таких документов *вирус* будет пытаться получить *доступ* к другим программам на компьютере, через, казалось бы, безопасные приложения. В таком примере зловредная *программа* (конкретно в примере *вирус*) модифицирует работу стандартных офисных программ под свои нужды. Это делается в надежде на то, что *пользователь* разрешит стандартному программному обеспечению выполнять те действия, в которых оно нуждается (это логичная схема, ведь *программное обеспечение*, уже установленное на компьютере и работающее, в меньшей степени вызовет недоумение пользователя, чем только что установленное *программное обеспечение*, которое будет пытаться произвести неожиданные действия). Впрочем, встречаются случаи, когда *программное обеспечение* недостаточно хорошо написано программистами, и в этом случае причина неожиданного поведения является, прежде всего, некорректная работа создателей самого программного обеспечения. В таких случаях обычно на веб-сайте производителя описываются возможные неполадки в работе программного обеспечения с предоставлением "заплаток" (обновлений) для исправления проблемы. Для того, чтобы определить, *по* какой причине *программное обеспечение* начало совершать неожиданные действия, необходимо воспользоваться следующей схемой, представленной на рисунке ниже:



**Рис. 2.9. Схема разъяснения признака №8**

Следуя этой схеме, если *пользователь* заметил различные проблемы с установленным программным обеспечением, он должен сделать следующее: Просмотреть веб-*сайт* производителя программного обеспечения в поиске описания проблемы. Если описания проблемы и ее решения не было обнаружено на сайте производителя, то *пользователь* должен вспомнить, не ставил ли он перекрестные программы (т.е. программы, похожие *по* действию и работе на уже установленное *программное обеспечение*, например, два текстовых редактора), так как такие программы могут вызвать сбои в уже установленном программном обеспечении. Если же *пользователь* не ставил перекрестные программы, то, скорее всего, на компьютере имеет *место* быть работа зловредной программы, и необходимо принять меры *по* ее устранению.

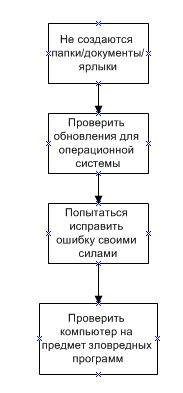
**Признак №9** (**появление в автозагрузке операционной системы непонятных программ**). Прежде всего, определимся с термином автозагрузка – специальное *место* операционной системы, куда помещается *программное обеспечение*, которое должно быть загружено сразу же при старте операционной системы. При этом зачастую сам *пользователь* решает, какое именно *программное обеспечение* должно присутствовать в автозагрузке, но бывает и так, что некоторое *программное обеспечение* прописывается в автозагрузку само (как правило, это *антивирусная защита*, автоматические обновления различного дополнительного программного обеспечения, либо системного). Автозагрузка - единственное *место* в операционной системе, благодаря которому можно автоматизировать *запуск* нужного программного обеспечения. Но бывают и такие случаи, когда зловредная *программа* намеренно прописывается в автозагрузку операционной системы, с целью загружаться абсолютно всегда вместе с операционной системой. Причем, никаких визуальных признаков *пользователь* может не обнаружить (зловредная *программа* может не подавать никаких внешних признаков своего присутствия), но его *персональные данные* будут под угрозой. С этой целью необходимо знать, что автозагрузку в различных операционных системах можно просмотреть различными способами (если речь идет о операционной системе семейства *Windows*, то это можно сделать, выполнив команду msconfig, и найти в открывшемся окне *поле* автозагрузка). Но обычного просмотра, зачастую, может быть мало, так как трудно определить, нужно ли то или иное *программное обеспечение* в автозагрузке системы. Обычно для удобства пользователя в настройке автозагрузки есть пояснения к каждой конкретной программе, которые позволяют понять ее необходимость нахождения в автозагрузке. Но следует помнить, что зловредная *программа* может маскироваться под какую-нибудь обычную программу. Поэтому, если *пользователь* не уверен в необходимости той или иной программы в автозагрузке, скорее всего, будет лучшим решением ее отключить. При появлении непонятных программ в автозагрузке необходимо воспользоваться следующей схемой, представленной на рисунке ниже:



**Рис. 2.10. Схема разъяснения признака №9**

Следуя этому алгоритму, *пользователь* при обнаружении непонятной программы в автозагрузке должен вспомнить, не устанавливал ли он сам эту программу и не помещал ли ее в автозагрузку. Если нет, то необходимо оценить важность этой программы в автозагрузке операционной системы. Если *пользователь* не видит явных причин для того, чтобы *программа* находилась в автозагрузке, необходимо удалить ее оттуда, так как, скорее всего, эта *программа* - зловредная.

**Признак №10** (**не создаются папки/документы/ярлыки**). Причина данного признака часто является тем, что, как и в некоторых признаках, описанных раннее, имеет *место* быть случай, что зловредное *программное обеспечение* пишется быстро, и не всегда есть время на его тестирование. Как результат появляются конфликты в операционной системе со стороны контекстного *меню*, вызываемого щелчком *по* правой кнопке мыши (это применимо для операционных систем семейства *Windows*), а именно невозможность создавать папки, документы или ярлыки к программному обеспечению. Обычно банальная перезагрузка операционной системе может решить эту неполадку, но лишь на короткий промежуток времени, и вскоре невозможность создания документов/папок/ярлыков будет снова серьезно досаждать пользователю компьютера. В этом случае необходимо воспользоваться схемой, представленной на рисунке ниже:



**Рис. 2.11. Схема разъяснения признака №10**

Описывая эту схему более подробно, можно сказать, что *пользователь* при обнаружении неполадок в создании папок/документов/ярлыков должен проделать следующие действия: проверить обновления для операционной системы (так как бывают случаи, когда подобные ошибки появляются из-за недоработки прошлой версии обновлений под операционную систему), попытаться исправить ошибку своими силами (этот *пункт* подразумевает следующие действия: попробовать создать папку из командной строки, набрав команду md "новая *папка*". Если *папка* создастся, то необходимо попробовать команду sfc/scannow, при этом, если используется *операционная система* *Windows*, начиная с *Windows Vista*, перечисленные действия необходимо делать с правами администратора). Если же все перечисленные действия не помогли справиться с проблемой, то необходимо проверить *компьютер* на предмет наличия зловредных программ.

**Признак №11** (**странная работа клавиатуры, либо мыши**). Данный признак можно считать скорее устаревшим, так как при проявлении зловредных программ через подобный признак сразу же вступит в действие *антивирусная защита*. Причиной подобного признака является специальный *класс* зловредных программ, называющихся кейлогерами, (кейлогер от английского key*log*) – специальная зловредная *программа*, которая занимается тем, что записывает нажатия кнопок клавиатуры в отдельный *файл*. В некоторых случаях кейлогер записывает также *координаты* перемещения мыши. Кейлогер опасен тем, что он может записать все пароли пользователя, так как*пользователь* будет набирать их на клавиатуре. В прошлом подобные зловредные программы были огромной угрозой для пользователя, а побочным их эффектом являлось то, что *пользователь* замечал странности в работе клавиатуры, либо мыши. Такие странности могли проявляться в виде кратковременного отказа работы некоторых кнопок клавиатуры, либо самопроизвольного перемещения курсора мыши. И хотя, как было указано выше, подобные зловредные программы можно считать устаревшими, время от времени появляются современные модификации подобных программ, которые некоторое время не обнаруживаются антивирусной защитой. Если *пользователь* обнаружил странности в работе клавиатуры, либо мыши, необходимо воспользоваться следующим алгоритмом, представленным на рисунке ниже:



**Рис. 2.12. Схема разъяснения признака №11**

Следуя данной схеме, можно определить причину странной работы клавиатуры/мыши на компьютере. Вначале необходимо проверить, правильно ли настроены клавиатуры и *мышь* на компьютере. Если правильно, то необходимо вспомнить, не устанавливались ли какие-либо программы, влияющие на работу клавиатуры, либо мыши (например, программы, повышающие отклик мыши). Если таких программ не устанавливалось, то, скорее всего, имеет *место* быть работа зловредной программы на компьютере.

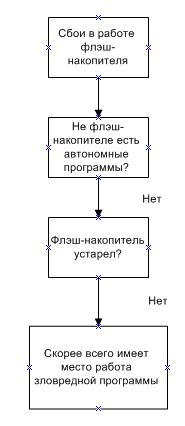
**Признак №12** (**появление неожиданных папок и файлов**). А вот этот признак является причиной достаточно современного класса зловредных программ. Причиной этого признака является то, что для своей работы зловредным программам иногда необходимо создавать временные файлы и папки, которые может увидеть *пользователь*. Обычно такие временные файлы и папки делаются скрытыми от пользователя (иногда еще и маскируются под системные файлы или папки). Существует *целый* *класс* зловредных программ, который намеренно занимается тем, что скрывает обычные папки от глаз пользователя (не удаляя их) и заменяет их своими папками-ярлыками с теми же названиями, что были у обычных папок. *Пользователь* при нажатии на такую папку-ярлык активирует вложение в папке, которое обычно является еще одной зловредной программой. При этом *пользователь* не может узнать того, что он активировал еще одну зловредную программу, ведь *папка* *по* которой он нажимал, на первый взгляд была его созданной папкой. Обычно такие папки-ярлыки выглядят как обычные ярлыки к папкам, но *пользователь* должен вспомнить, не создавал ли он сам подобные ярлыки. Также существуют зловредные программы, которые могут делать дубликат нужного пользователю файла с расширением exe (исполняемые файлы) и маскироваться под него. Если *пользователь* запустит такой лже-*файл*, то он активирует зловредную программу. Для того чтобы определить причину появления неожиданных файлов и/или папок, необходимо воспользоваться схемой, представленной на рисунке ниже:



**Рис. 2.13. Схема разъяснения признака №12**

Из представленного рисунка можно понять, как именно распознать причину появления различных файлов или папок. При этом необходимо ответить на следующие вопросы: не создавал ли *пользователь* эти объекты сам (если создавал, то причина внезапного их появления ясна), а также, не могли ли быть созданы эти объекты сторонней безвредной программой для своих нужд. Если ответы на эти вопросы соответствуют ответам, которые показаны на схеме, то, скорее всего, имеет *место* работа зловредной программы на компьютере

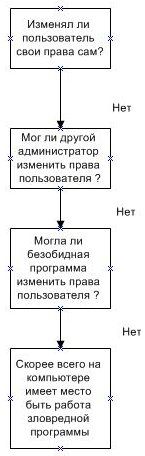
**Признак №13** (**резкие сбои в работе USB-флеш-накопителя**). Подобный признак проявляется в резком снижении работы USB-флэш-накопителя (далее просто флэш-накопитель). *Пользователь* обнаруживает, что его флэш-накопитель стал медленнее обмениваться информацией с компьютером, а также то, что на флэш-накопителе стали появляться сторонние файлы или папки. Резкое снижение скорости обмена информации с компьютером может быть обусловлено тем, что зловредная *программа* использует флэш-накопитель в своих целях, и вместе с этим снижается общая скорость работы флэш-накопителя. Существует *целый* *класс* зловредных программ, которые осуществляют свою *деятельность* исключительно через флэш-накопители (раньше такие зловредные программы осуществляли свою *деятельность* через дискеты). Это способствует их быстрому распространению между компьютерами различных пользователей. Впрочем, резкие сбои в работе флэш-накопителя могут возникнуть и потому, что флэш-накопитель уже устарел и нуждается в замене. *Алгоритм* выявления причины признака резкого сбоя в работе флэш-накопителя представлен в виде схемы на рисунке ниже:



**Рис. 2.14. Схема разъяснения признака №13**

Следуя схеме, можно определить причины сбоя работы флэш-накопителя. Прежде всего, *пользователь* должен проверить, не установлены ли автономные программы на флэш-накопителе (существует особый *класс* программ, которые работают непосредственно с флэш-накопителя), а также, не устарел ли сам флэш-накопитель (срок службы более 2-3 лет). Если ответы на эти вопросы соответствуют ответам на схеме, то, скорее всего, имеет *место* работа зловредной программы на компьютере через флэш-накопитель.

**Признак №14** (**самопроизвольное изменение прав пользователей**). Данный признак также говорит о том, что на компьютере пользователя происходят непонятные вещи, которые могут быть связаны как с работой зловредной программы, так и без нее. Причиной, когда *пользователь* обнаружил изменение своих прав (например, он был администратором, а стал обычным пользователем с соответствующими правами) не *по* вине работы зловредной программы, может быть в том, что другой высокопривилегированный *пользователь* системы (другой *пользователь* с правами администратора) намеренно понизил *права* пользователя. Также некоторые вполне безобидные программы могут резко изменить *права* пользователя (например, антивирусная *программа* может понизить *права* пользователя с целью временного обеспечения безопасности). Для того, чтобы выяснить причину самопроизвольного изменения прав пользователей на компьютере, необходимо воспользоваться следующей схемой, представленной на рисунке ниже:



**Рис. 2.15. Схема разъяснения признака №14**

Следуя этой схеме, можно определить причину самопроизвольного изменения прав пользователей. Прежде всего, необходимо ответить на следующие вопросы: изменял ли *пользователь* свои *права* сам (если изменял, то причина ясна), мог ли другой *администратор* изменить *права* пользователя (если мог, и изменил, то причина ясна), могла ли безобидная *программа* изменить *права* пользователя (если могла, то причина ясна). Если ответы на данные вопросы соответствуют ответам на схеме, то, скорее всего, имеет *место* работа зловредной программы на компьютере.

**Признак №15** (**Появление множественных BSOD на компьютере**) Признак является достаточно красноречивым сам *по* себе. *BSOD* или "синий экран смерти" является результатом появления системной ошибки на компьютере пользователя. Синий экран представлен обычно синим фоном с описанием ошибки. В разных версиях *Windows* выделяют разные типы *BSOD*. Обычно он появляется тогда, когда в коде ядра или драйвера, выполняющегося в специальном режиме, возникает неустранимая ошибка. В этом случае *операционная система*, чтобы избежать краха, вынуждена остановить свою работу и сделать перезагрузку операционной системы. При этом *пользователь* операционной системы увидит этот самый синий экран смерти, после которого будет перезагрузка компьютера. Сам синий экран не говорит о наличии вируса, но он может это подразумевать, так как ошибка может быть вызвана зловредной программой, которую необходимо устранить. Чтобы определить причину синего экрана, пользователю необходимо задокументировать надписи на синем экране и обратиться в службу поддержки операционной системы. При этом в службе поддержки операционной системы дадут расшифровку кода, и тогда можно будет узнать, что именно послужило причиной возникновения синего экрана. Также, если в операционной система включена *функция* сохранения фрагментов памяти в отдельный *файл*, то этот *файл* также необходимо отправить в службу поддержки. Такой ход позволит наиболее эффективно определить причину появления синего экрана. Также интересны некоторые факты: Операционные системы семейства NT, начиная с *Windows 2000*, могут быть настроены таким образом, чтобы дать пользователю возможность вручную спровоцировать "синий экран смерти". Чтобы включить эту опцию, необходимо изменить определенные настройки в системном реестре. После этого *по* двойному нажатию клавиши *SCROLL* LOCK при удерживании правой клавиши CTRL система выдаст синий экран. Эта *опция* полезна, например, для получения дампа памяти компьютера в заданный момент или для экстренной остановки компьютера аналогично кнопке Reset. Иногда она используется при разрешении настоящих проблем работы операционной системы. Сам же синий экран можно поменять в цветности, задав соответствующие параметры в реестре. А в операционных системах типа *UNIX* существует аналогичное понятие синего экрана – *kerne* panic (паника ядра).

**Признак №16** (**необъяснимые загрузки в безопасном режиме**). При этом признаке *операционная система* (имеется в виду система *Windows*) будет пытаться войти в безопасный режим при каждой своей загрузке. Причем это будет делаться независимо от того, нормально ли отключал *пользователь* систему *Windows* или нет. В этом случае система будет пытаться загрузить себя в специальный режим работы, при котором она будет пытаться загрузить *минимум* подпрограмм и сервисов. При этом сама работа операционной системы останется нетронутой. *Пользователь* же увидит соответствующее сообщение о том, что его *операционная система* была загружена в безопасном режиме. Это должно насторожить пользователя, особенно если он загружал какие-либо подозрительные файлы на свой *компьютер*.

Вышеперечисленные признаки являются далеко не всеми признаками, которые могут говорить о том, что на компьютере пользователя имеет *место* быть работа зловредной программы. Бывают случаи комбинированных признаков из вышеупомянутых признаков. Также история зловредных программ насчитывает множественные ухищрения, которые могут поставить пользователя в *тупик* при попытке обнаружения присутствия зловредных программ на компьютере. Стоит заметить, что некоторые признаки в данной лекции были намеренно упущены, так как уже считаются безнадежно устаревшими (например, признак внезапного отключения портов является уже устаревшим, так как был распространен около 10 лет назад, а в настоящее время зафиксированных случаев заражения подобными зловредными программами не было зарегистрировано).