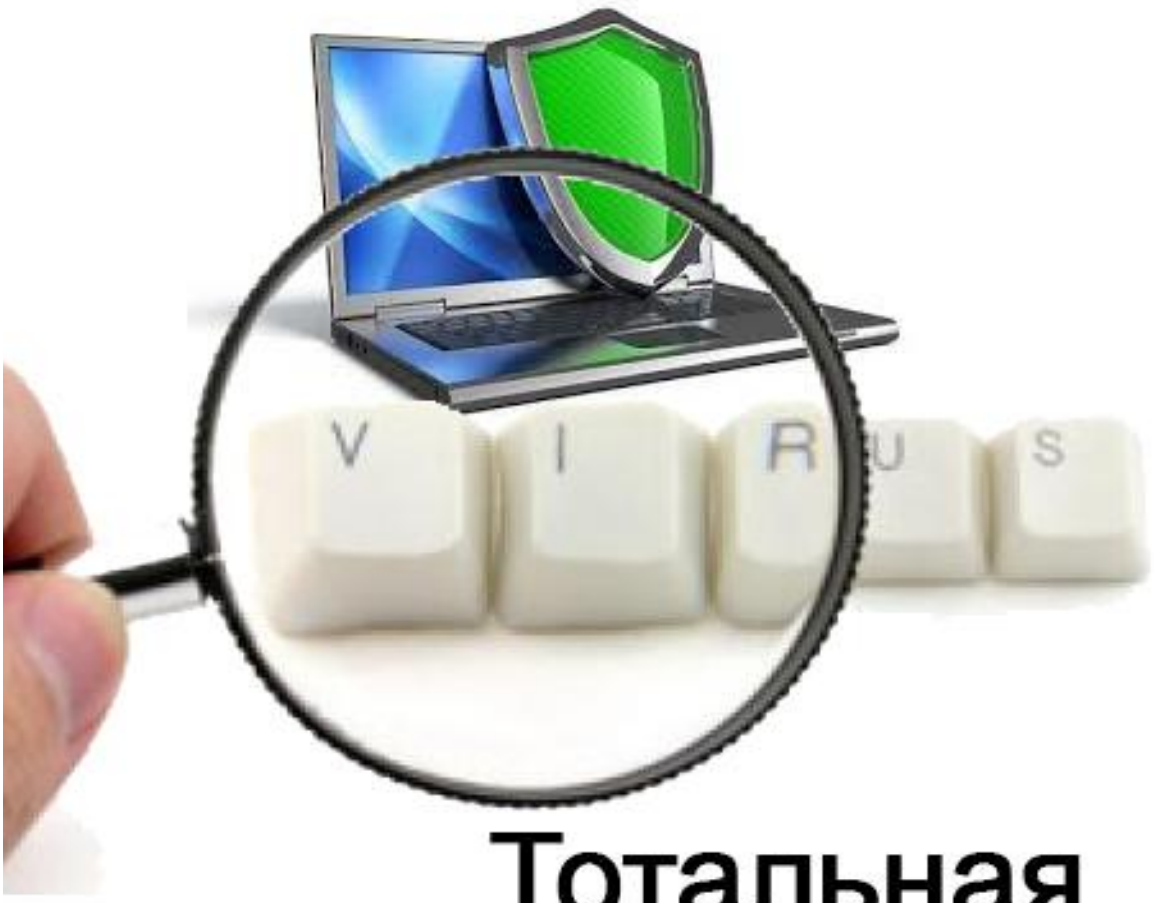


Тотальная защита компьютера от вирусов

Базовый курс

Автор книги: Сидоров Игорь
Сайт: http://webtreveller.ru

Здравствуй, дорогой друг!

С вами Сидоров Игорь.

Если вы читаете эти строки, значит, вас заинтересовал наш бесплатный продукт “Тотальная защита компьютера от вирусов: базовый курс”.

Данная книга представляет собой базовый курс защиты компьютера от вирусов.

Мы рассмотрим в данной книге все базовые понятия. Но не думайте, что здесь голая теория. В этой книге мы будем двигаться от самых основ теории до практики, которую должен знать каждый пользователь компьютера.

После прочтения данной книги вы сможете своими силами удалить вирусы и предотвратить заражение вашего компьютера в будущем.

В интернете много информации на данную тему, но эту информацию дают люди, которые просто пользуются программами и рекомендуют их другим.

Полную информацию о защите компьютера трудно найти в интернете. Поэтому мы готовим полный видео-курс “Тотальная защита компьютера”.

Что войдет в данный курс?

1. Базовый курс, т.е. данная книга, но в видео формате.
2. Практика пользования антивирусами.
3. Практика пользования интернетом.
4. Практика пользования браузерами.
5. Хранение информации.
6. Практические советы, если вы подхватили вирус.

Данный курс еще на стадии разработки и планы могут меняться.

Но пока все готовится вы сможете прочитать данный «Базовый курс».

Содержание:

Статья 1. От чего или кого стоит защищаться в Интернете?

Первая наша тема называется "От чего или кого стоит защищаться в Интернете?" или "Внешние угрозы безопасности"

Мошенники были всегда и везде. Они каждый раз придумывали новые способы вытягивания денег у простых людей. В интернете таких людей прозвали "Хакеры".

Хакеры используют вирусы, чтобы проникнуть на ваш компьютер и получить доступ к вашей личной информации.

Что я имею в виду под личной информацией?

1. логины и пароли от социальных сетей и от электронного почтового ящика;
2. пароли от электронных кошельков;
3. банковские реквизиты;
4. пароли от интернета.

Вся эта информация нужна хакерам для распространения своего вируса вашим знакомым и друзьям, ну и естественно для того, чтобы обогатиться.

Какими способами пользуются хакеры?

1. Заражение вирусами. Благодаря вирусу мошенник может проникнуть в ваш компьютер и украсть всю вашу личную информацию с него.
2. Кейлоггер (англ. keylogger) – представляет из себя маленькую программу,которая способна считывать нажатие клавиш и после передавать собранную информацию о логинах и паролях хакеру.
3. Радмин (англ. Radmin) или неправомерный доступ. Ну тут как говорится, смотря в чьи руки он попадет. Если программа попала в добрые руки, то с ее

помощью людям оказывают удаленную техническую поддержку, администрирование компьютером. В злых руках она работает как вирус т.е. ищет нужную мошенникам информацию.

Кстати вот ссылка на официальный сайт Radmin http://www.radmin.ru/. Если перейдете по ссылке, то можете увидеть, что данная программа создана для удаленной технической поддержки сотрудников. Те, кого заинтересовала эта программа могут её скачать и не бояться, что вас взломают.

Radmin работает в режиме защиты данных, при котором все передаваемые данные, изображения экрана, перемещение курсора и сигналы клавиатуры надёжно защищены. Секретный ключ генерируется случайным образом для каждого подключения.

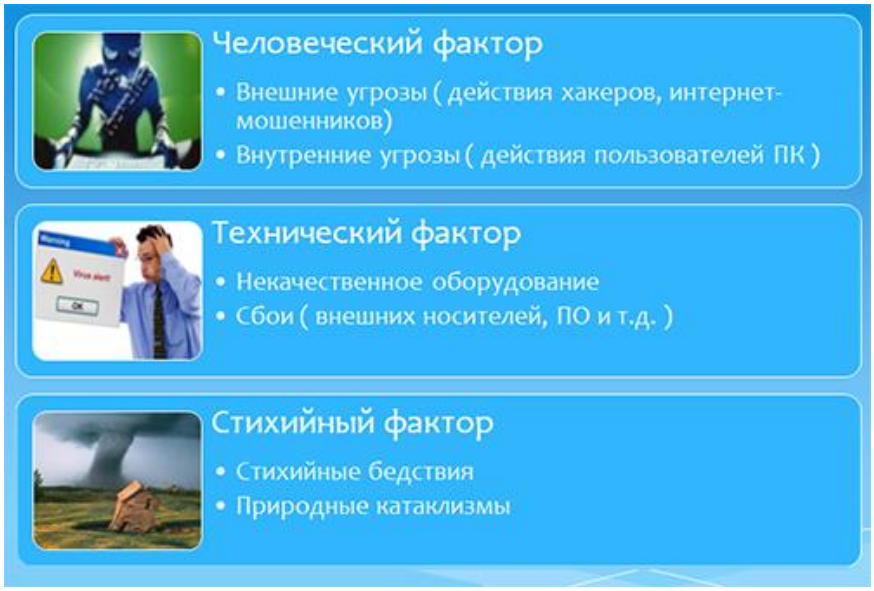
4. Мошенничество. Когда под видом одного сайта вы попадаете на сайт мошенников, и там вас просят отослать СМС на короткий номер. Или, допустим, устанавливаете приложение для сотового, а после этого деньги начинают исчезать с вашего счета.

Вот такими приёмами и уловками пользуются хакеры в наше время.

Итак, мы познакомились с нашим противником, и узнали, чем он вооружен. А, значит, вооружились сами. Ведь как говорится: "Предупреждён – значит вооружён".

Статья 2. Источники угроз информационной безопасности.

Сначала приведу вам примерную схему источников угроз информационной безопасности.



Все угрозы компьютерной безопасности делятся на три основных пункта.

1. Человеческий фактор.

Как видно из названия, речь будет идти о людях, которые каким-либо образом могут повлиять на информационную безопасность.

Человеческий фактор делится на внешние угрозы и внутренние угрозы.

- Внешние угрозы. Мы рассмотрели в предыдущей статье "От чего или кого стоит защищаться в Интернете?".
- Внутренние угрозы.

Что относится к внутренним угрозам? Действия всех остальных людей, включая вас самих! Вы скажете, что это не так?

Объясню на собственном примере. Я не люблю долго ждать, пока программа установится. Однажды, когда я решил обновить MicrosoftWord, у меня завис компьютер. Мне пришлось перезагружать компьютер. После того как я зашел, у меня перестал работать Word. Соответственно я потерял доступ к личной информации в виде документов в формате Word. Вот такой пример.

Или взять в пример компьютер со множеством пользователей. Другие пользователи могут каким-либо случайным образом взять и изменить, или того хуже - удалить информацию, важную для вас.

2. Технический фактор.

Вы купили компьютер. Пользуетесь им уже почти год. И вдруг он просто перестал включаться. Вы потеряли доступ к личной информации. А причина - некачественное оборудование.

Также опасность представляют "сбои". Сбои могут быть электрические - это когда вы работаете без безперебойника за компьютером и вдруг отключают свет. Сбои внешних носителей (когда вы отключаете внешний носитель не через безопасный режим. Сбои программного обеспечения - когда программа повисла, перезагрузилась и не сохранила ваш документ. И тому подобное...

3. Стихийный фактор.

Думаю, этот пункт в особых комментариях не нуждается. Этот фактор непредсказуем и может застигнуть вас врасплох.

Вот эти факторы (Человеческий, Технический, Стихийный) являются основными источниками угроз информационной безопасности.

Статья 3. Виды угроз компьютерной безопасности.

Если вы помните, когда мой сайт запускался, я написал статьи под названием Компьютерные вирусы, в которых описал каждый вид вирусов.

Теперь, подготовив данный курс, я собрал все статьи воедино и представляю вашему вниманию "пирамиду угроз".

Что представляет собой "пирамида угроз"?

Это своего рода рейтинг вирусов, которые сейчас можно подхватить в интернете.

Вот так выглядит эта пирамида.

Рассмотрим ее подробней.

Топ-3 у нас занимают:

1. Черви
2. Вирусы
3. Трояны

Червь использует уязвимости операционной системы и программ для самораспространения на другие компьютеры. Поэтому у него и такое название "Червь", что он переползает с компьютера на компьютер. Он использует сети,

электронную почту и т.д., вследствие чего обладает высокой скоростью распространения. Черви иногда создают рабочие файлы, но и могут вообще не использовать ресурсы компьютера, за исключением оперативной памяти.

Вирусы проникают в программы и изменяют их исходный код, добавляя свой, чтобы получить управление при запуске данной программы.

Трояны способны выполнять какие-либо действия без участия пользователя компьютера, например, удалять файлы, воровать личную информацию и т.д. Их действия способны привести к зависанию компьютера. Чаще всего мошенники распространяют трояны под видом полезного ПО.

В настоящее время очень часто хакеры начали комбинировать эти три вида вредоносных программ. Соответственно увеличились последствия хакерских атак. Будьте осторожны! Не забывайте обновлять базы своего антивируса!

Следующие типы вредоносных программ менее распространены в Рунете, но вы должны о них знать.

Баннерная реклама - я подразделяю ее на 2 вида.

1. Баннерная реклама, которая появляется в браузере при пользовании интернетом или распространяется встроенной в ПО. Данный баннер использует огромное количество трафика.

2. Баннерная реклама, которая встраивается в операционную систему и при запуске пользователь видит баннер с требованием заплатить деньги, чтобы разблокировать баннер.

Как правило, все эти баннеры собирают информацию о пользователе и передают ее своему разработчику.

Программы-шпионы, как видно из названия, собирают всю информацию о пользователе. Обычно целью программ-шпионов является отслеживание действий пользователя на компьютере, информации о программном обеспечении установленном на компьютере, о способе подключения к интернету и т.д.

Потенциально опасные приложения - это программы, которые содержат бреши и ошибки в безопасности. Злоумышленники способны воспользоваться

этими ошибками и проникнуть на ваш компьютер с целью получить вашу индивидуальную информацию.

Программы-шутки в свое время были популярны. Их использовали не только хакеры, но и обычные пользователи забавы ради. Однако и эти программы-шутки представляют опасность в руках хакера. Одной из таких шуток был постоянно открывающийся привод CD/DVD ROM Однажды я сам так прикололся над другом. Поставил эту программу-шутку и наблюдал его действия. Мне было весело, ему – не очень .

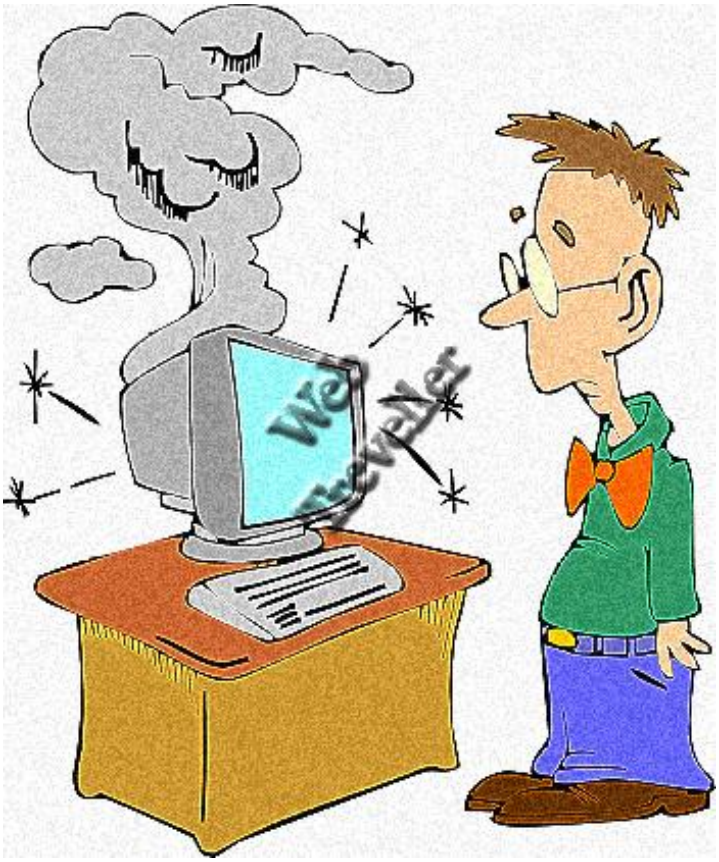
Еще одна интересная программа-шутка сообщает о форматировании диска, хотя никакого форматирования не будет.

Программы-маскировщики мешают антивирусным программам определять вредоносные программы. Также эти программы изменяют операционную систему, чтобы скрыть свое собственное присутствие.

К прочим опасным программам относятся программы взлома паролей, конструкторы вирусов, программы взлома сетевых ресурсов и т.д.

Вот примерно так выглядит "пирамида угроз".

Статья 4. Признаки заражения компьютера вирусом



В этой статье мы рассмотрим ряд признаков, которые могут свидетельствовать о заражении вирусом вашего компьютера.

Если в один прекрасный день вы включили компьютер и заметили, что на нем начались "глюки", такие как:

- На экране начали выплывать странные тексты, изображения или звучат какие-либо странные звуки;
- Привод CD/DVD начал открываться и закрываться сам по себе;
- Программы начали запускаться сами по себе;
- Появились сообщения о попытке программы выйти в интернет.
- Появляются системные ошибки при запуске Windows.

Если у вас есть хотя бы один из этих признаков то, возможно ваш компьютер подвергся заражению вирусом и его стоит проверить антивирусом.

Если

- ваши друзья, знакомые, родня говорят, что вы им присылали сообщения с просьбой пройти по ссылке, хотя вы таких сообщений не отсылали;
- в вашем почтовом ящике есть сообщения с подозрительным обратным адресом или вообще без него;
- вам на сотовый или на почту приходит сообщение об изменении пароля или каких либо данных;

то возможно ваш аккаунт взломал вирус, который находится на вашем компьютере.

Есть признаки, которые указывают на наличие вируса, но тут может сыграть свою роль и человеческий фактор:

- частые зависания во время работы компьютера и сбои в работе программного обеспечения;
- очень медленная работа компьютера при запуске программ, в отличие от прежнего состояния компьютера;
- сбои при загрузке операционной системы и невозможность загрузить Windows;
- исчезновение файлов, папок, искажение содержимого файлов, появление новых файлов и папок;
- медленная работа веб-браузера, отказ грузить интернет-страницы или переадресация на сторонние сайты.
- На всякий случай проверяем компьютер антивирусом.

Примеры, описанные в данной статье, взяты из личного опыта и опыта моих знакомых.

Статья 5. Вирус-вымогатель и борьба с ним.

Что такое вирус-вымогатель?

Вирус-вымогатель – это программа-троян, которая способна заблокировать работу вашего компьютера до тех пор, пока вы не отправите SMS на короткий номер. Чаще всего, даже если вы отправите SMS на короткий номер, работа компьютера не восстановится и вы потратите за SMS гораздо больше денег, чем указано в сообщении.

Вирусы-вымогатели могут:

- Существенно ограничить и даже полностью заблокировать работу интернет-браузера.
- Шифровать файлы пользователя.
- Блокировать доступ к операционной системе.

Вирусы вымогатели имеют расширения типа zip, rar, exe, bat, com.

Меры предосторожности:

1. Установите хороший антивирус, с постоянно обновляемыми базами. Вы можете выбрать платный или бесплатный антивирус, но помните, что экономить на защите компьютера – это не самый лучший вариант. Подробнее о вирусах мы расскажем в следующей статье.
2. Проверяйте ваш компьютер антивирусной программой на наличие вирусов, с периодичностью раз в 1-2 недели.

3. Пользуйтесь браузерами Firefox, Chrome, Yandex, Mail, Safari и установите в них расширение AdBlock, блокирующее всплывающие окна и рекламу на сайтах.

4. Если есть подозрения на наличие в файле вируса, вы можете этот файл проверить онлайн на сайтах производителей антивирусов:

Онлайн-сканер Dr.Web:

http://vms.drweb.com/online/

Kaspersky Online Scanner:

http://www.kaspersky.ru/scanforvirus

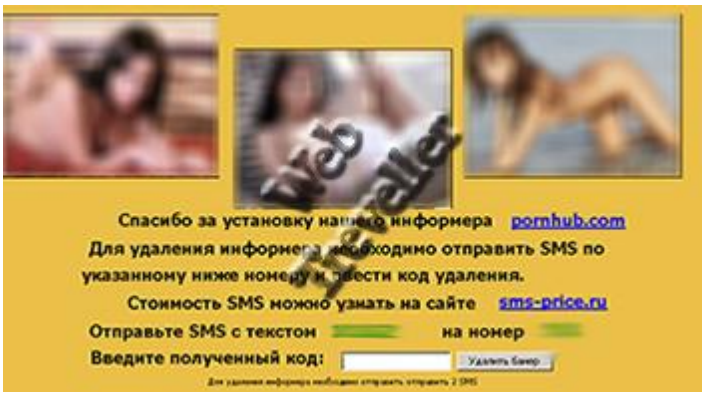
Компания Dr.Web создала помощника, который может подсказать вам, стоит ли заходить на сайт или нет, это - Dr.WebLinkChecker.

Dr.WebLinkChecker это набор плагинов для браузеров (MozillaFirefox, Chrome, Opera и InternetExplorer), после установки которых все открываемые вами страницы и файлы, скачиваемые из интернета, будут проверяться на наличие вредоносных программ заранее, т.е. до того, как вы что-то откроете или скачаете.

5. Не открывайте электронные письма от незнакомых людей, в них могут содержаться вирусы.

6. Все пароли рекомендую хранить в письменном виде, ибо на переносных электронных носителях (флешки, винчестеры и т.д.) могут быть вирусы. Поэтому сразу проверяйте переносные электронные носители на вирусы, прежде чем с ними работать.

Статья 6. Как разблокировать и удалить вирус вымогатель?



Как обычно говорят многие психологи:

Не паникуйте!..

Первое, что вам надо сделать, чтобы разблокировать и удалить вирус вымогатель, это узнать какой из вирусов-вымогателей у вас поселился.

Вирус блокирующий доступ в интернет.

Как видно из названия он блокирует выход в интернет и вы видите перед собой баннер с требованием отправить SMS, если это так, то будьте уверены вас посетил вирус блокирующий доступ в интернет. Вирус меняет файл Hosts который находится в папке C:\Windows\System32\drivers\etc (если у вас Windows NT/2000/XP/Vista/7/8).

Метод лечения:

1. Открываете файл Hosts блокнотом. (правой кнопкой мыши по файлу, открыть или открыть с помощью и выбираем блокнот)
2. Удаляем все строки кроме **127.0.0.1 localhost**.

Для примера у меня в файле Hosts написано:

```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
```

```
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
# 102.54.94.97 rhino.acme.com # source server
# 38.25.63.10 x.acme.com # x client host
# localhost name resolution is handled within DNS itself.
# 127.0.0.1 localhost
# ::1 localhost
127.0.0.1 localhost
```

3. Не забываем сохранить изменение.
4. Проверяем полной проверкой компьютер антивирусом.
5. Перезагружаем компьютер.

Проблема должна исчезнуть, если это не так - то вы сделали где-то ошибку или у вас другой вид вируса.

Вирусы вымогатели могут маскироваться под **легальные программы.**

Итак, перед вами висит ненавистное окошко с требованием выкупа за восстановление работоспособности вашего компьютера. И если вы не глупый человек, вы не станете платить этим вымогателям деньги, ведь не факт что вам придет SMS с действующим кодом деактивации вируса и не факт, что вы заплатите именно ту сумму, которая написана в сообщении. Поэтому способ лечения у нас будет такой:

1. С помощью другого компьютера зайдите на сайты производителей антивирусов и найдите там сервис деактивации вирусов-вымогателей (он поможет вам разблокировать вирус вымогатель)

Сервис деактивации вирусов-вымогателей лаборатории Касперского
Техподдержка ESET NOD32: Разблокировка Windows
Dr.Web: Разблокировка Windows от Trojan.Winlock

2. Вводим полученный нами код.
3. Проверяем полной проверкой компьютер на наличие вирусов.
4. Перезагружаем компьютер.

Если ни один код не подошел, то качаем специальные программы Лаборатории Касперского (**Digita_Cure**) или Dr.Web (CureIt), которые помогут удалить вирус вымогатель:

- Утилита Digita_Cure страница программы
- Ссылка для скачивания Digita_Cure архив

- Страница программы CureIt
- Ссылка для скачивания CureIt

Перед тем, как начать лечение от вируса, нужно закрыть доступ в интернет и перезагрузить компьютер в безопасном режиме, нажав кнопку F8 сразу после включения и выбрав пункт «Загрузка в безопасном режиме». Затем необходимо будет запустить флешку или диск с утилитой **Digita_Cure (или CureIt)** и провести полную проверку компьютера. После лечения компьютер включаем в нормальном режиме.

Вирусы, блокирующие браузер

Если вы, путешествуя в интернете, все время в своем браузере видите картинки откровенного содержания с требованием отправить SMS на короткий номер, знайте вы подхватили вирус-вымогатель.

Метод решения - это залезть в настройки браузера и отключить те настройки, в которых в графе "Издатель" написано "не проверено".

Но если это для вас составляет сложность, можно пойти другим путем.

Нам помогут такие программы как:

AVPTool от лаборатории Касперского
или
программа CureIt

Вирусы, блокирующие доступ к операционной системе.

Этот вид вируса выскакивает сразу после загрузки Windows и полностью перекрывает собой все и ничего не дает вам делать. Ну и естественно просит денег иначе он просто удалит все файлы на компьютере.

Что нужно делать чтобы разблокировать и удалить вирус-вымогатель?

1. Можно воспользоваться помощью уже знакомых нам «Касперского всемогущего» или «Dr.Weba непобедимого» и подобрать пароль к вашему баннеру.
2. Можно воспользоваться "живым диском" **Dr.Web® LiveCD**

Страница программы Dr.Web® LiveCD
Ссылка для скачивания образа Dr.Web® LiveCD

Подробнее как пользоваться Dr.Web® LiveCD мы рассмотрим в следующей статье

Вирусы-шифровальщики.

Этот вирус шифрует данные с расширением txt, xls, doc. Узнать о том, что ваш компьютер заражен, вы сможете, благодаря отсутствию доступа к информации и окошку на рабочем столе или текстовому документу, вложенному в каталог с зашифрованными файлами. Сегодня самым лучшим в борьбе с вирусами-шифровальщиками является Dr.Web, однако даже он не может дать стопроцентную гарантию, что вы восстановите все свои документы.

Ссылка на утилиту Dr.Web для борьбы с вирусами-шифровальщиками.

Если ни один из приведенных выше способов вам не помог, придется обращаться к специалистам технической поддержки сайта производителя вашего антивирусного ПО.

Статья 7. Служебная программа для поиска строк (qgrep) не работает.

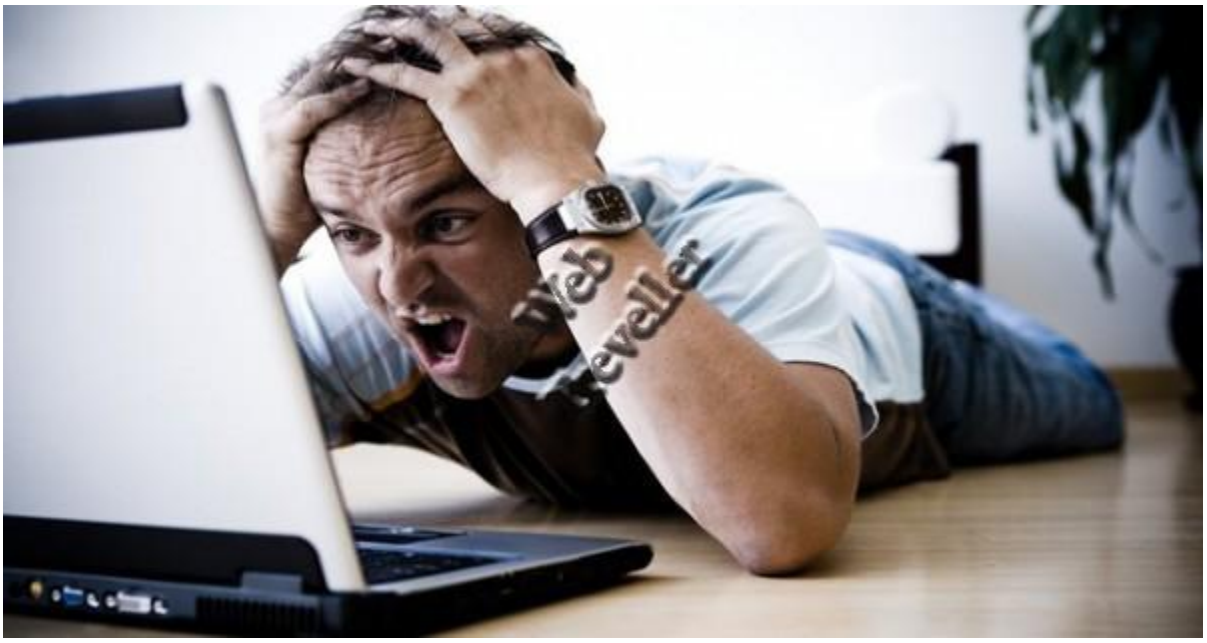
Qgrep.exe это процесс, с **Microsoft Corporation**, однако в данной ошибке может скрываться **троян**. Для вашей безопасности, если при загрузке Windows появляется данное сообщение:

Служебная программа для поиска строк (qgrep) не работает.

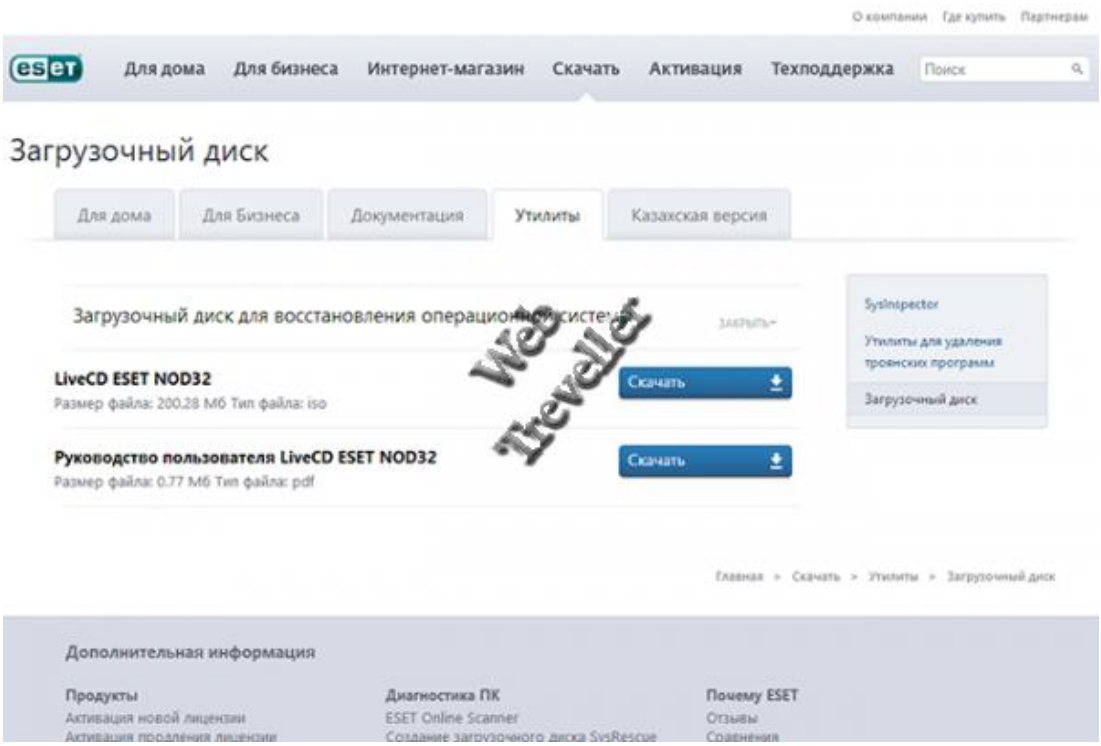
скачайте Dr.Web CureIt и проверьте компьютер на наличие вирусов. Подробнее как проверить компьютер Dr.WebCureIt описано в этой статье http://webtreveller.ru/page/proverka-kompjutera-na-virusy-pri-pomoshhi-drweb-cureit

Лично у меня после проверки, которая длилась всего 11 минут, было обнаружено и удалено 3 трояна.

Статья 8. Как удалить порно-баннер с помощью LiveCD ESET NOD32.



В борьбе с порно баннером может помочь **LiveCD ESET NOD32**. **LiveCD ESET NOD32** представляет собой загрузочный диск, при помощи которого Вы сможете быстро запустить компьютер и восстановить работоспособность выведенной из строя операционной системы, удалив все вредоносные программы.



Первое, что вам необходимо, это скачать ISO-образ диска с сервера NOD32 по адресу http://www.esetnod32.ru/download/utilities/livecd/ и записать его на CD(DVD)-диск или USB flash-накопитель.

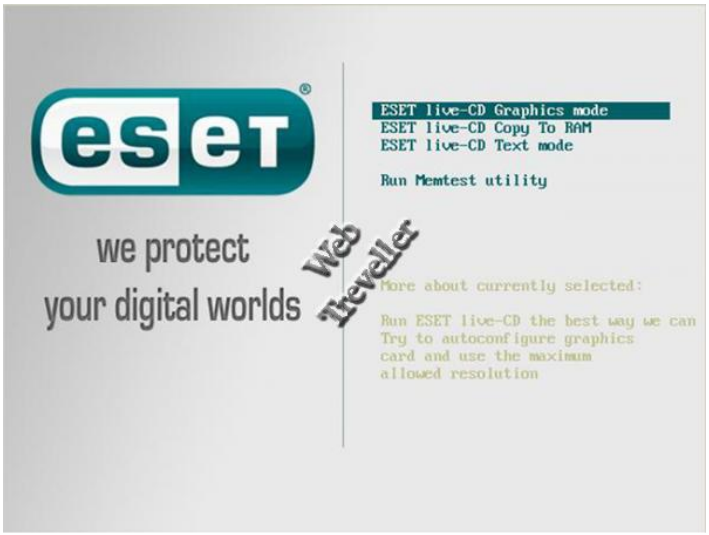
Если вы используете операционную систему Windows 7 или Windows 8, то для записи ISO-образа на CD(DVD)-диск вам необходимо:

1. Правой кнопкой мыши кликаете на файле с расширением .iso, который вы должны были скачать с официального сайта NOD32 по адресу http://www.esetnod32.ru/download/utilities/livecd/ и выбираете пункт "Открыть с помощью", после выбираете пункт "Средство записи образов дисков Windows";
2. Должен открыться диалог записи дисков, где вам потребуется выбрать привод для записи образа и вставить в него диск;
3. Кликаете на кнопку "Записать" и через несколько минут диск с образом будет записан.

Замечу в скобках, что пункты 1, 2 и 3 желательно выполнить заранее и хранить загрузочный диск или флешку на полочке, как вы храните лекарства в домашней аптечке.

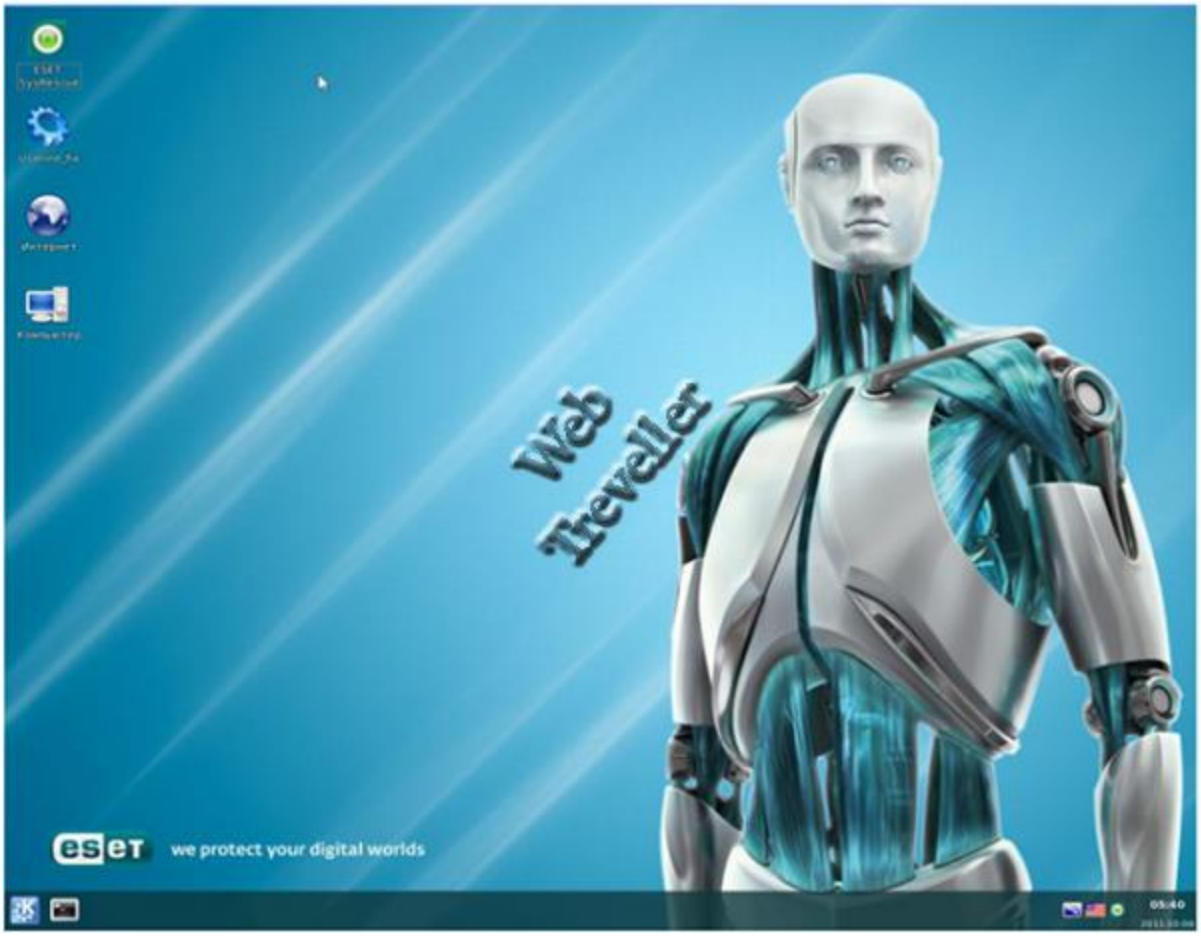
Для загрузки компьютера при помощи "загрузочного диска ESET" необходимо установить CD(DVD)-диск, с записанным на него образом "загрузочного диска ESET", и произвести перезагрузку компьютера, предварительно включив в настройках BIOS загрузку с CD(DVD)-диска. Подробнее как это сделать можно прочесть в статье Как запустить DVD или CD привод первым?

После проделанных манипуляций с BIOS, если вы все сделали правильно, то ваш компьютер перезагрузится и появится следующее окно с выбором способов загрузки:



Теперь подробнее о способах загрузки:

1. ESET live-CD Graphicsmode – данный способ загрузки показывает полноценный рабочий стол, где вы можете запустить сканирование компьютера, выйти в интернет и осуществить другие действия;
2. ESET live-CD Copyto RAM – данный способ загрузки сначала копирует все файлы диска в оперативную память, а затем производит загрузку в 1-ом режиме, работая без CD(DVD)-диска или USB flash-накопителя;
3. ESET live-CD Textmode – данный способ загрузки позволяет работать через командную строку;
4. RunMemtestutility – данный способ загрузки производит запуск проверки оперативной памяти компьютера на наличие ошибок.

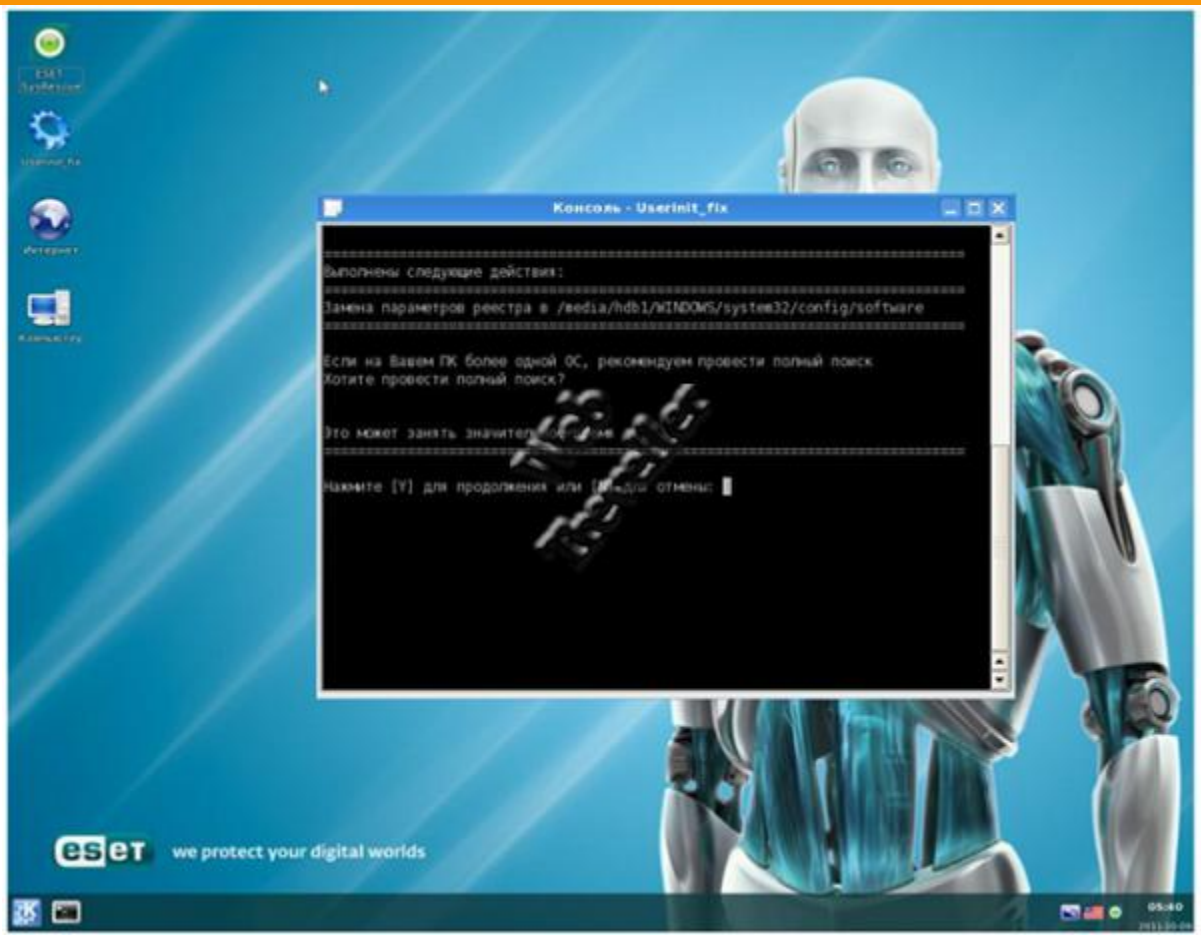


Самый оптимальный, на мой взгляд вариант, это - **ESET live-CD Graphicsmode**.

А теперь по теме!

Если Ваш компьютер заражен баннером вымогателем (или порно-баннером), который препятствует загрузке операционной системы, то просто запустите файл Userinit_fix, который находится на рабочем столе, после чего следуйте простым указаниям в появившемся черном окне. И

также для вашей безопасности рекомендую запустить сканирование компьютера двойным нажатием на значек антивируса, который находится на рабочем столе.



Для запуска сканирования компьютера при помощи антивируса нажмите на значок "ESET NOD32Antivirus" в правом верхнем углу экрана. При запуске сканирования, проверяется весь компьютер и обнаруженные угрозы удаляются автоматически.

После всех проверок перезагрузите компьютер, вытащите диск и не забудьте изменить в BIOS порядок загрузки (сделать HDD первым вместо CD/DVD). После того как вы войдете в операционную систему обновите ваш антивирус и снова проверьте ваш компьютер на вирусы.

Статья 9. Как удалить вирус в процессе svchost.exe.

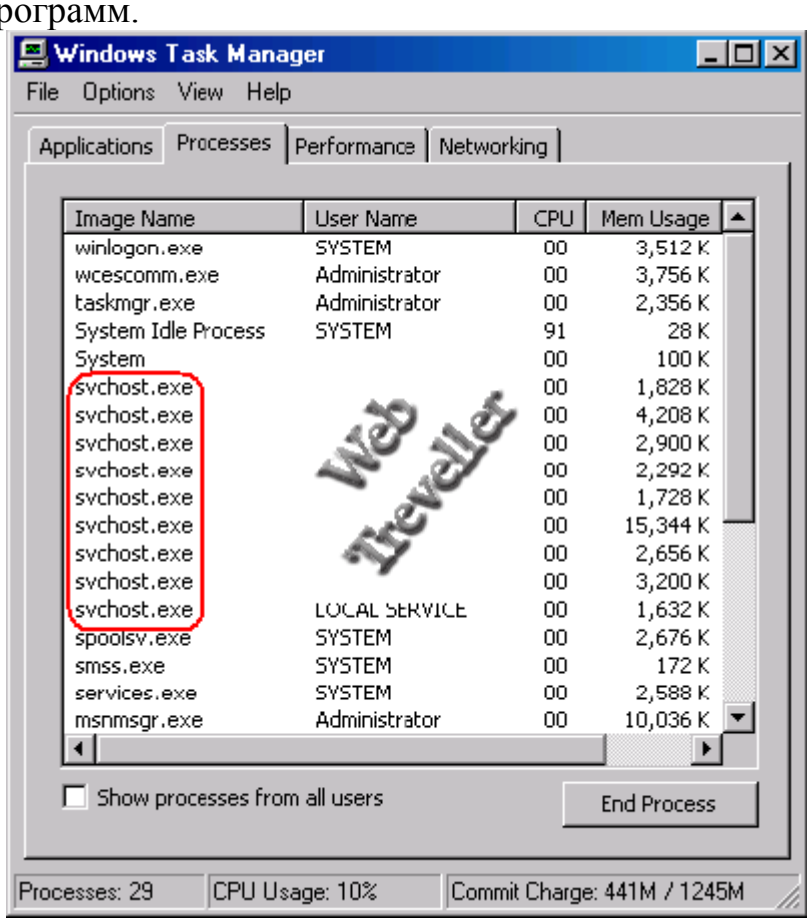
Начнем с определения, что такое svchost.exe.

Svchost.exe - является безопасным системным процессом Windows. Тем не менее, мошенники, создатели вирусов, таких как черви и трояны, намеренно называют процессы таким же именем, чтобы скрыть вирус от глаз обычного пользователя.

Как определить присутствие вируса?

1. Нажатием на клавиши Ctrl-Alt-Delete(или Ctrl-Shift-Esc) вызываем диспетчер задач.

2. Переходим во вкладку «процессы» и ищем все процессы с именем "Svchost". Примерно так должен выглядеть диспетчер задач. Процессов svchost.exe у вас может быть много, ведь каждый svchost.exe обслуживает свой набор служб и программ.



3. Смотрим путь каждого svchost.exe в диспетчере задач.

Процесс svchost.exe располагается только в этих папках:

- C:\WINDOWS\system32

- C:\WINDOWS\ServicePackFiles\i386

- C:\WINDOWS\Prefetch

- C:\WINDOWS\winsxs\ (внутрипапки)

Где C - диск на котором расположен Windows.

Если процесс находится в другой папке, значит это вирус!

4. Также процесс может быть написан с ошибками (например svchoste.exe, svcshost.exe и т.д.), поэтому внимательно проверьте название процесса!

"Снятие задачи" в диспетчере задач не даст положительных результатов, т.к. при перезагрузке компьютера программа автозапуска, в которую часто поселяется вирус, запустит процесс снова.

Как вылечить svchost.exe?

1. Удаление вируса с помощью бесплатной лечащей утилиты Dr.WebCureIt. Подробнее как вылечить svchost.exe можно прочесть в статье "Проверка компьютера на вирусы с помощью Dr.WebCureIt".

Найденные инфицированные объекты (вирусы) необходимо вылечить, а неизлечимые удалить.

2. Удаление вируса с помощью LiveCD ESET NOD32. Об этом также написана подробная статья, которую можно прочесть по ссылке "LiveCD ESET NOD32"
3. Много всего полезного можно почерпнуть в статье "Как разблокировать и удалить вирус вымогатель".

Статья 10. AdBlock - полезное расширение для браузера.

AdblockPlus — расширение для браузера (MozillaFirefox, MozillaThunderbird, GoogleChrome, Opera), позволяющее блокировать загрузку и показ различных элементов страницы: чрезмерно назойливых или неприятных рекламных баннеров, всплывающих окон и других объектов, мешающих использованию сайта.

AdblockPlus блокирует коды HTML, Java скрипты, изображения и баннеры, которые мешают нормальной работе на сайте. Также AdBlock препятствует попаданию вирусов на ваш компьютер, благодаря блокировке некоторых скриптов.

Adblock, была выпущена Хенриком Соренсеном в 2002 году для браузера Firefox 1.0. В 2004 году Майкл Макдональд выпустил расширение под названием «AdblockPlus» и версией 0.5, который имел более совершенный интерфейс, поддержку централизованных списков фильтров и возможность скрытия элементов страницы.

В 2006 году Макдональд прекратил разработку и передал проект Владимиру Паланту (Wladimir Palant), который выпустил AdblockPlus 0.6 с переписанным кодом в январе 2006 года.

Журнал PC World оценил AdblockPlus как один из 100 лучших продуктов 2007 года.

В марте 2010 года на выставке CeBIT был отмечен как лучшее OpenSource дополнение для Firefox.

AdBlock и по сегодняшний день является самым распространенным расширением для браузера. По моему личному мнению, благодаря ему вы сможете посещать сайты со спокойной душой. Потому, что 90% всей гадости сайта (баннеры, навязчивая реклама, скрытые скрипты, переходы на другой сайт) это маленькое, но очень хорошее расширение уберет.

Я пользуюсь этим расширением уже 5 лет. Поверьте, это самое лучшее расширение вашего браузера.

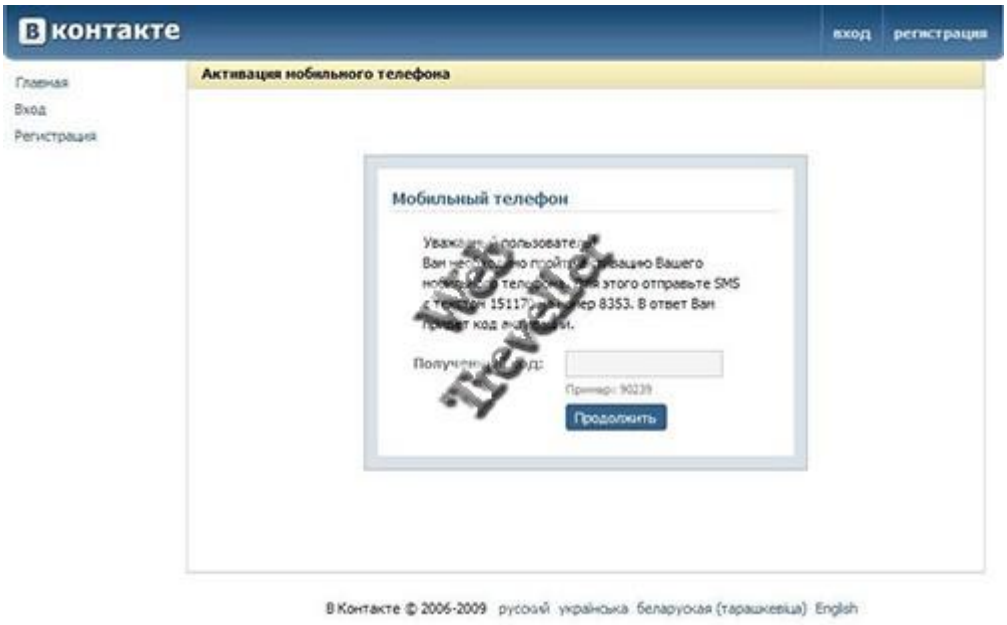
Чтобы поставить это расширение пройдите по ссылке http://adblockplus.org/ru/ (полезное расширение для вашего браузера). Сайт автоматически определит ваш браузер. Далее жмете УСТАНОВИТЬ ДЛЯ ... и жмете установить. После чего закрываем ваш браузер, снова включаем и можете спокойно плавать по просторам интернета!

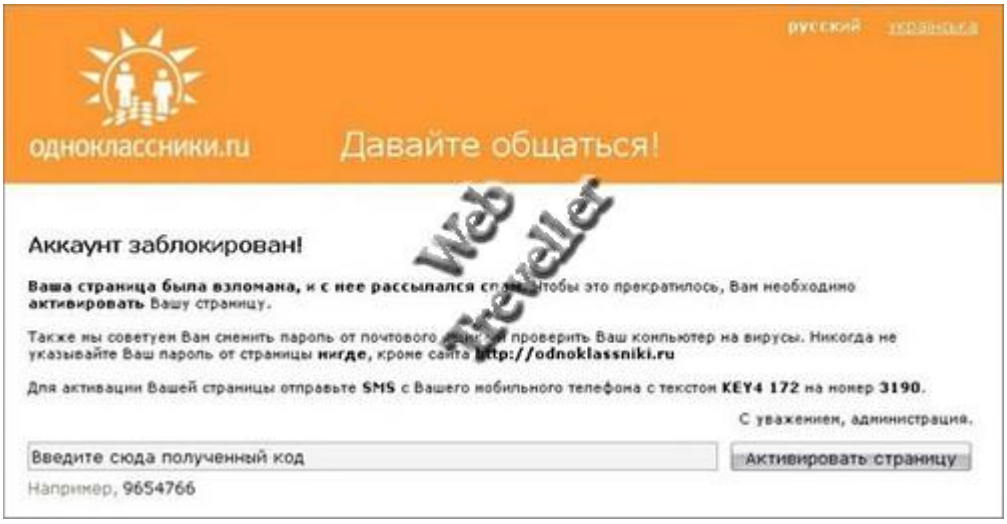
Статья 11. Как удалить вирус в Одноклассниках и Вконтакте.

Все началось как всегда. Включил компьютер, налил себе кофе, запустил браузер... Решил, что надо зайти в «Одноклассники» и проверить наличие свежих сообщений - может кто написал мне.

И тут...

Если вы читаете данную статью, вы наверное уже сталкивались с такими сообщениями, когда заходили в социальные сети:





Помните:

Администрация социальных сетей, никогда не будет просить Вас подтвердить ту или иную информацию отправкой SMS – сообщением. Максимум, что попросят - это ввести номер телефона, чтобы прислать вам СМС с кодом активации!

Статья 12. Если у вас не загружается сайт Вконтакте или Одноклассники.

1. Проблема скорее всего в вашем браузере. Поэтому попробуйте почистить компьютер с помощью программы Ccleaner (подробнее о возможностях программы в статье CCleaner - программа для ухода за компьютером.) и зайти на сайт попозже.

2. Проверьте свой компьютер на вирусы с помощью вашего антивируса, предварительно обновив его. Из своего личного опыта скажу, что после

проверки вашим антивирусом нужно еще скачать и проверить компьютер полностью с помощью Dr.WebCureIt.

3. Проверьте файл Hosts на вашем компьютере (подробности в статье Восстановление файла hosts.)

Dr.Web предупреждает!

Компания "Доктор Веб" предупреждает об опасности заражения новой версией вредоносной программы Trojan.Zekos, одна из функций которой заключается в перехвате DNS-запросов на инфицированном компьютере.

Если говорить простым языком, то данный троян перенаправляет вас на сайт злоумышленников с целью нажиться на вас. Поэтому администрация сайта Webtreveller настоятельно рекомендует обновлять антивирусы и быть внимательными, т.к. мошенники используют идентичный настоящему дизайн сайта. Кроме того, на поддельной веб-странице демонстрировались настоящие имена пользователей, поэтому многие жертвы мошенников не замечали подмены, и думали, что их учетная запись в социальной сети действительно была взломана.

Статья 13. Как проверить компьютер на вирусы Dr.WebCureIt.

Как проверить компьютер на вирусы Dr.WebCureIt и вообще что такое Dr.WebCureIt?

Dr.WebCureIt - это бесплатная утилита, которая проверяет ваш компьютер на наличие вирусов. Если на Вашем ПК установлен другой антивирус, но вы сомневаетесь в его эффективности, то с помощью утилиты Dr.WebCureIt!® без установки Dr.Web в системе Вы можете быстро проверить Ваш компьютер и, в случае обнаружения вредоносных объектов, вылечить его.

Какие виды вредоносных программ обезвреживает Dr.WebCureIt?

- черви;
- вирусы;
- трояны;
- руткиты;
- шпионские программы;
- программы дозвона;

- рекламные программы;
- программы взлома;
- программы-шутки;
- потенциально опасные программы.

Как проверить инфицирован ли ваш компьютер вирусами?

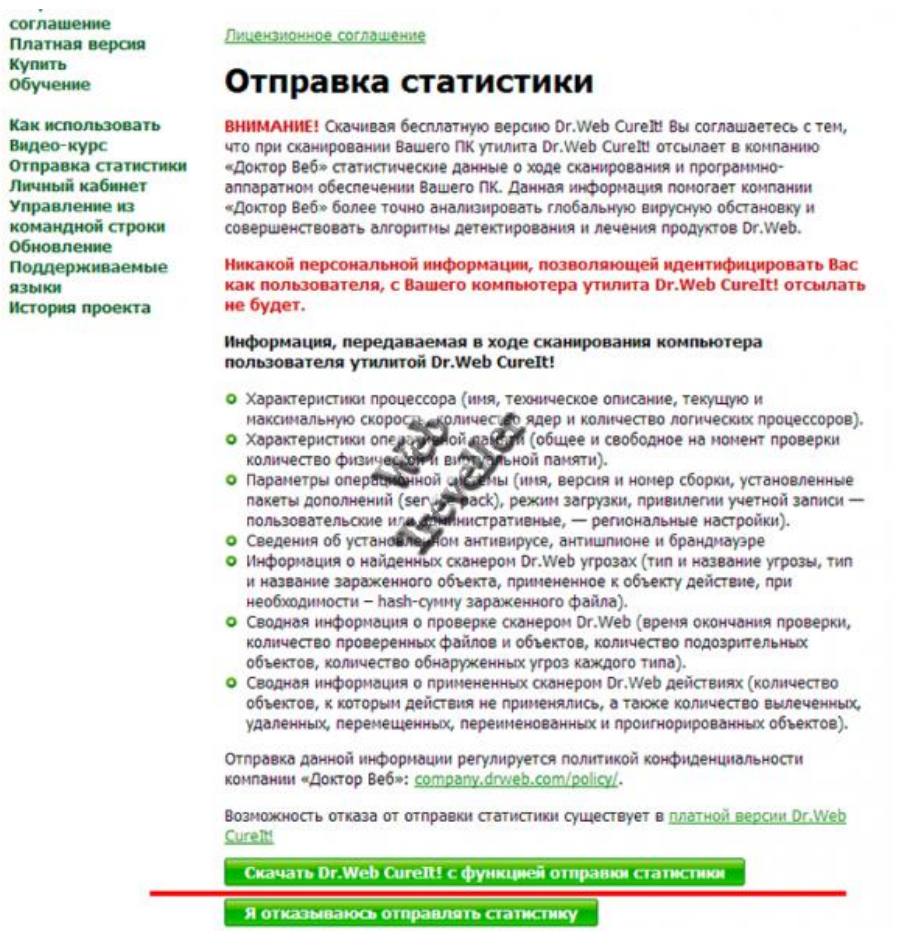
1. Скачайте Dr.WebCureIt!, сохранив утилиту на жесткий диск.
2. Запустите сохраненный файл на исполнение (дважды щелкните по нему левой кнопкой мышки).
3. Выберите режим защиты – усиленный или обычный.
4. Дождитесь окончания сканирования и изучите отчет о проверке.

Где и как скачать Dr.WebCureIt?

1. Заходим по этой ссылке https://www.freedrweb.com/download+cureit+free/?lng=ru на официальный сайт Dr.Web.
2. Нажимает на кнопочку "Далее"

3. Нажимаем на "Скачать Dr.WebCureIt! с функцией отправки статистики". Как написано на сайте:

Возможность отказа от отправки существует в платной версии Dr.WebCureIt!



4. Ставим галочку "Я принимаю условия Лицензионного Соглашения" и жмем "Продолжить"

5. После этого начинается загрузка файла Dr.WebCureIt!. (размер файла примерно от 100 до 200 Мб)

В каком режиме проводить проверку компьютера?

Dr.WebCureIt! запускается в 2 режимах:

1. **Режим усиленной защиты**. Антивирус блокирует работу компьютера и в это время работает только антивирус, который проверяет компьютер.
2. **Обычный режим**. Если вы хотите продолжать работать на компьютере, пока он проверяется антивирусом, то выбирайте **Обычный режим**. Однако советую выбирать **Режим усиленной защиты.**

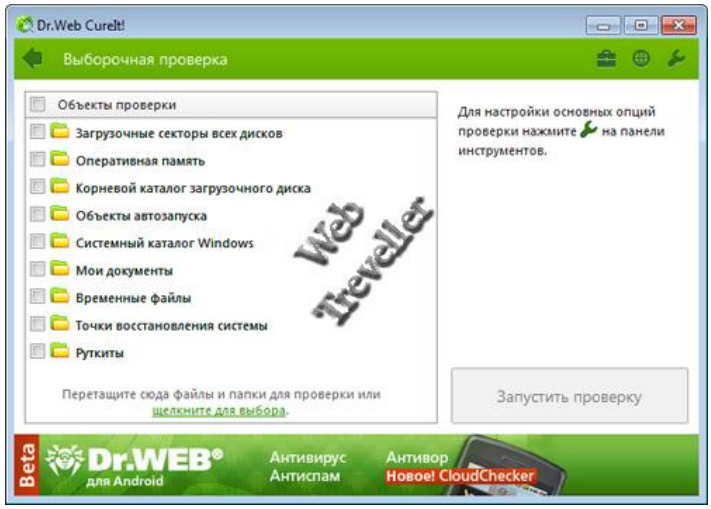
Какую проверку выбрать?

1. **Быстрая проверка** занимает несколько минут. В данном режиме производится проверка следующих объектов:
   - оперативная память;
   - загрузочные секторы всех дисков;
   - объекты автозапуска;
   - корневой каталог загрузочного диска;
   - корневой каталог диска установки Windows;
   - системный каталог Windows;
   - папка Мои Документы;
   - временный каталог системы;
   - временный каталог пользователя;
   - наличие руткитов (если процесс проверки запущен от имени администратора).

Как вы понимаете, при быстрой проверке проверяются только самые важные, в плане безопасности, объекты.

Для быстрой проверки компьютера на вирусы достаточно нажать на кнопку Начать проверку.

2. **Выборочная проверка**, как вы уже догадались позволяет выбрать объекты для проверки самим.



3. **Полная проверка компьютера на вирусы** - проверяет все файлы, находящиеся на вашем компьютере. Для полной проверки, воспользуйтесь ссылкой **"щелкните для выбора"** и в появившемся окне поставьте галочку напротив пункта **Мой компьютер**.

Если Dr.WebCureIt обнаружит вирусы, то в конце проверки появится список обнаруженных угроз.

Если хотите, вы можете изменить настройки, но я этого не советую, т.к. настройки оптимальны и менять их, нет необходимости.

Следите за вашим компьютером и старайтесь проверять его хотя бы раз в месяц на наличие вирусов.

Статья 14. Что лучше защитит компьютер, Брандмауэр или Фаерволл?

Что поставить на компьютер, Брандмауэр или фаервол?

По сути это одно и тоже. Брандмауэр и фаервол – представляют собой программно-аппаратный комплекс, который проверяет данные, входящие через Интернет или сеть, и, в зависимости от настроек, блокирует их или позволяет им пройти в компьютер.

Фаервол более динамичен в планах настройки и более функционален. Брандмауэр же более легок в использовании и содержит минимум настроек.

Зачем нам нужен брандмауэр/фаервол?

1. Контролировать приложения, использующие порты (в случае изменения приложения вирусами или троянами, устанавливающимися в качестве плагинов, сетевая активность приложения блокируется);

2. В фаерволе существует режим обучения, когда при первом обращении программы к сетевым ресурсам пользователю задаётся запрос как поступить с программой (обычно вида «запретить всегда, запретить однократно, всегда разрешить, разрешить однократно, создать правило»);
3. В брандмауэре проставляются исключения для программ;
4. Режим смешанной фильтрации (при которой осуществляется контроль всего входящего из интернета, посредством портов).

При установке фаервола отключаем родной брандмауэр Windows и наоборот – это делается во избежание конфликта между ними.

Если вы сомневаетесь с выбором…

Если у вас на компьютере есть очень ценная информация, которая содержит в себе пароли банковских счетов, интернет кошельков и т.д. или ваш компьютер участвует в валютно-финансовых операциях, то вы можете не сомневаться, что вам необходим фаервол.

Если ваш компьютер предназначен для домашнего пользования, то вам с головой хватит встроенного стандартного брандмауэра Windows (если конечно вы не используете Windows XP и ниже).

Если вы заинтересовались фаерволами…

Предлагаю вашему вниманию три фаервола, которые должны вас заинтересовать

1. COMODO FirewallFree
2. ZoneAlarmFree
3. OutpostSecurityFree

Почему именно эти фаерволы?

Эти фаерволы бесплатные, т.к. отсутствуют некоторые модули. Конечно у них есть PRO – версия, но эту версию придется купить.

Наверняка некоторые из ваз сразу полезут искать данные фаерволы в торренте, чтобы найти их с таблэткой.

Если вы будете искать в торренте данные фаерволы, то ищите только ключи. Не кейгены или кряки, а именно ключи. Т.к. в большинстве кейгенов и кряков находятся вирусы. Крякнув фаервол вы просто построите своеобразный проход для хакера к вашим личным данным.

Мое личное мнение, что если вы хотите поставить фаервол, то ставьте COMODO. Данный фаервол вполне способен конкурировать с платными версиями других фаерволов. Также в COMODO присутствует русский язык

интерфейса (что согласитесь очень хорошо). В данный фаервол встроена “песочница”, которая позволяет запустить программу, пускай даже с вирусом, без вреда вашему компьютеру. Поэтому, если вы не хотите зря тратить деньги и рисковать безопасностью вашей личной информации, то не ставьте кряки или кейгены, а ставьте **COMODO FirewallFree**.

Если вы надумаете купить PRO-версию фаервола, то ваш выбор – AgnitumOutpostFirewallPro.

Рейтинг фаерволов июль 2013.

В июле 2013 года был проведен рейтинг фаерволов. Данный рейтинг не часто проводится, в отличие от рейтинга антивирусов.

В июльском тесте участвовала 21 программа класса InternetSecurity и фаервол. Тесты проводились на чистом компьютере с предустановленными на тот момент последними обновлениями на Windows 7 x86.

Что включал в себя тест фаерволов?

1. Проверка защиты процессов от завершения.
2. Защита от стандартных внутренних атак.
3. Тестирование защиты от нестандартных утечек.
4. Тестирование защиты от нестандартных техник проникновения в режим ядра.

Тест внутренних атак был поделен на два уровня.

1. Базовый уровень сложности (56 вариантов атак): проверка защиты процессов от завершения (41 вариант атак) и защита от стандартных внутренних атак (15 вариантов атак).
2. Повышенный уровень сложности (8 вариантов атак): тестирование защиты от нестандартных утечек (3 варианта атак) и тестирование защиты от нестандартных техник проникновения в режим ядра (5 вариантов атак).

Таблица рейтинга фаерволов на июль 2013 года.

Тестируемый продукт	Вариант настроек	Предотвращение атак [%]		Всего [%]	Награда
		Базовый уровень сложности	Повышенный уровень сложности		
Comodo	Max	100%	100%	100%	
Bitdefender	Max	100%	100%	100%	Platinum Firewall Outbound Protection Award
Online Armor	Max	95%	100%	95%	
Kaspersky	Max	95%	88%	94%	
Comodo	Standard	95%	75%	92%	
Norton	Max	90%	100%	91%	
Online Armor	Standard	89%	94%	90%	
PC Tools	Max	88%	69%	86%	
Outpost	Max	88%	69%	85%	
Eset	Max	88%	69%	85%	Gold Firewall Outbound Protection Award
Norton	Standard	80%	75%	80%	
Dr.Web	Max	83%	63%	80%	
Jetico	Max	82%	56%	79%	
Jetico	Standard	82%	56%	79%	
Outpost	Standard	80%	31%	74%	
Trend Micro	Max	77%	38%	72%	
TrustPort	Max	77%	31%	71%	
Trend Micro	Standard	75%	38%	70%	
Kaspersky	Standard	75%	31%	70%	Silver Firewall Outbound Protection Award
Dr.Web	Standard	76%	25%	70%	
G DATA	Max	75%	38%	70%	

Лучшие результаты в тесте показали фаерволы Comodo и Bitdefender, набравшие 100% баллов на максимальных настройках.

Почему стоит оставить обычный брандмауэр?

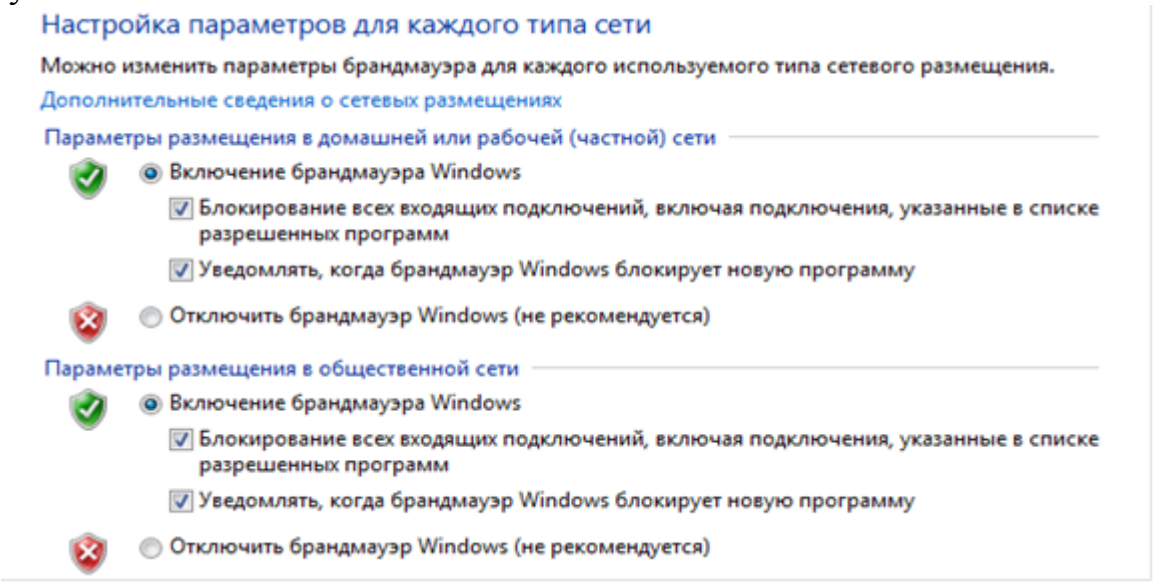
Лично я выбираю обычный брандмауэр встроенный в Windows. Однако, если у вас стоит Windows XP и менее, то лучше всего поставьте фаервол.

1. Он очень удобный. Как говорится все всегда под рукой.
2. В брандмауэре минимум настроек, с которыми сможет справиться обычный пользователь.
3. Безопасность, которую он создает, вполне меня устраивает.

Да обычный брандмауэр ругают, но если вы качаете программу с подозрительных сайтов и сразу же, не проверив ее на вирусы, запускаете, то вам никакой антивирус и фаервол не поможет!

Как включить Брандмауэр?

1. Кликаем на кнопку Пуск.
2. Заходим в Панель управления.
3. Ищем Система и безопасность.
4. Слева ищем Включение и отключение брандмауэра Windows.
5. Выбираем пункт Включение брандмауэра Windows и выставляем все как на рисунке ниже.



Что мы включили?

Ну, естественно, понятно, что Включение брандмауэра Windows – это означает, что мы включили защиту брандмауэра.

А вот блокирование всех входящих подключений – это означает то, что мы включили максимальную защиту безопасности, которая закрывает все порты.

Если оставить галочку на “Уведомлять, когда брандмауэр windows блокирует новую программу”, то будут всплывать сообщения о блокировке.

Внимание!

Если вы работаете в локальной сети, то возможно, что пропадет связь между компьютерами. Если такое случилось, то снимаем галочку с “Блокирование всех входящих подключений”.

Заключение.

Здравствуйте, дорогой друг!

Пришло время нам с вами подвести итог. Итак, что мы узнали из данного курса? Я хочу вас поздравить, ведь вы теперь знаете базовые методы защиты компьютера.

Вы даже себе не представляете, что 90% всех людей, которые приходят ко мне и говорят, чтобы я вылечил компьютер от вирусов, даже не пытаются сами вылечить их. Почему так происходит – для меня большая загадка.

Если вы читаете данные строки, значит, вы прочли книгу и сможете самостоятельно защитить свой компьютер от хакерских атак и вирусов. Теперь вы с гордостью можете сказать всем, что вы уже не “чайник”, а “юзер”!

Самое главное, что я хочу сказать – не бойтесь сломать компьютер! Пускай вы не сможете удалить вирус, и придется переустановить систему, но вскоре вы научитесь удалять вирусы самостоятельно и вам уже не понадобится данная книга.

Это всего лишь базовый курс. Полный курс “Тотальная защита компьютера” даст вам уже не теоретические, а практические знания, которые вы сможете применять в жизни. Но это будет потом…

А сейчас не забывайте практиковать свои знания… Скачайте все необходимые программы, чтобы быть уже готовым. Ведь, предупрежден – значит защищен!

На этой ноте я заканчиваю книгу.

Желаю вам удачных продаж и успеха!

С вами был, и остается, Сидоров Игорь.

Личный сайт: http://webtreveller.ru