
Комплексная защита от вирусов
Автор: Alexfedoruk
2011 год

ПРЕДИСЛОВИЕ

Приветствую всех, кто читает данную книгу.Обычно само ПРЕДИСЛОВИЕ никто не читает, но в нашем случае его лучше прочитать, чтобы понять хотя бы о чём книга на первом этапе.

В этой книге я – **Alexfedoruk** - попытаюсь Вам рассказать ПРОСТЫМИ словами и «с нуля» о настройках безопасности вашего компьютера. Попытаюсь довести до Вашего ведома как правильно настроить, как использовать, что скачать касательно повышения вирусной безопасности вашего железного зверя, а также затронуть несколько полезных оптимизационных настроек ПК. Решил написать в простом стиле, без сложных терминов, что и ученик 2-А класса поймет...

Почему вообще я решил написать? Многие даже не задумываются, что у них сидит «кто-то» в компе, а они радуются и думают,что у них «никого» нет...А когда уличили злодея в своем компьютере и сами же способствовали этому,то кидаются налево и направо в поисках удаления вируса, но бывает,что уже поздно и как всегда нас «выручает» форматирование, при котором мы теряем всё нажитое непосильным трудом – программы (будь-то платные или бесплатные, но обидно...согласитесь), но и не факт, что это поможет.... Поэтому, моя задача состоит в том,что бы Вы использовали компьютер и интернет максимально безопасно,не боясь,что у вас уведут аккаунт от соц.сети,от «мыла» (e-mail – электронный ящик) и электронного кошелька, прочей ерунды виртуальной! :)

Хочу также заметить,что ВСЕ ПРОГРАММЫ,ЧТО Я БУДУ ПРЕДЛАГАТЬ И ОПИСЫВАТЬ В КНИГЕ НЕ КОНФЛИКТУЮТ МЕЖДУ СОБОЙ!!! И будут работать отлаженно, как одно целое!

ВАЖНО: я буду рассказывать о настройках своей операционной системы *Windows Vista , но данные тонкости настройки и программы также применимы любой версии Windows, особенно к* ***Windows 7****!!!*

РАЗДЕЛ 1.0

От чего и кого нам стоит защищаться?

От кого нам защищаться – это понятно уже - конечно, от ХАКЕРА.

А вот от чего нам защищаться – это от инструментов хакера!

Эти, так назвываемые, инструменты хакера есть всё то «доброе и светлое», которое ему поможет проникнуть в ваш компьютер, заразить его вирусом или внедрить программу хакерского характера... ну и, конечно, доступ к информации. Под «вашей информацией» я имею ввиду:

- пароли /логины на ваши социальные сети и электронные ящики;
- интернетные пароли вашего сайта,или других сайтов вцелом,включая ICQ , Skype и другие средства связи;
- пароль на ваш электронный кошелек;
- хищение с вашего компьютера ценной информации, а это может быть какие-то банковские реквизиты,любая информация, которая связана с валютно-финансовой деятельностью;
- и если еще больше повезет,то хакер может найти на вашем ПК компромат,который, вследствии,может вас затем шантажировать (громко я сказал,но всё возможно);
- узнать ваш пароль/логин точки входа в интернет,т.е. возможность использования Вашего интернета (правда,порядочные провайдеры сейчас более менее за этим следят).

Как мы видим цель хакера – это информация, которую затем он использует с целью финансовой наживы!...Вобщем, в наше время кто как может «крутится», как это не звучит парадоксально....

Теперь вернемся к инструментам хакера. К **<u>инструментам хакера</u>** мы будем относить следующее:

1. **ВИРУС** - самая большая группа в инструментарии хакера, которая занимает более 90% всего «доброго и светлого» :) Вирусов,а точнее их подразделений и категорий, много (останавливаться на этом не будем), но благодаря им хакер может очень много сделать с вашим ПК, включая проникновение и хищение вашей информации.
2. **КЕЙЛОГГЕР** (англ. *keylogger) – такая себе маленькая программка,которая считывает нажатие клавиш,т.е. всё,что вы наживаете на клавиатуре отправляется хакеру(смотря,как настроен кейлоггер). Отсюда также легко и воруются пароли,логины.*
3. **РАДМИН***(англ. Radmin) – сказать, что это хакерская программа нельзя,т.к. Радмин создается для:*

   - Удаленно администрировать компьютеры локальной сети и серверы;
   - Оказывать техническую поддержку сотрудникам компании.

   И есть также официальный сайт - http://www.radmin.ru/

   Но мы понимаем,что Радмин в руках хакера является мощным средством и явно не для добрых дел.

Итак,мы уже осознаем,чего и кого нам следует стерегтись. Но бояться, значить иметь страх перед врагом, а врага нужно либо уничтожить, либо от него защититься (так сказать иметь броню).....и вот поэтому поводу есть, что рассказать – как защититься от вирусов; как найти и уничтожить вредоносное ПО; найти и обезвредить

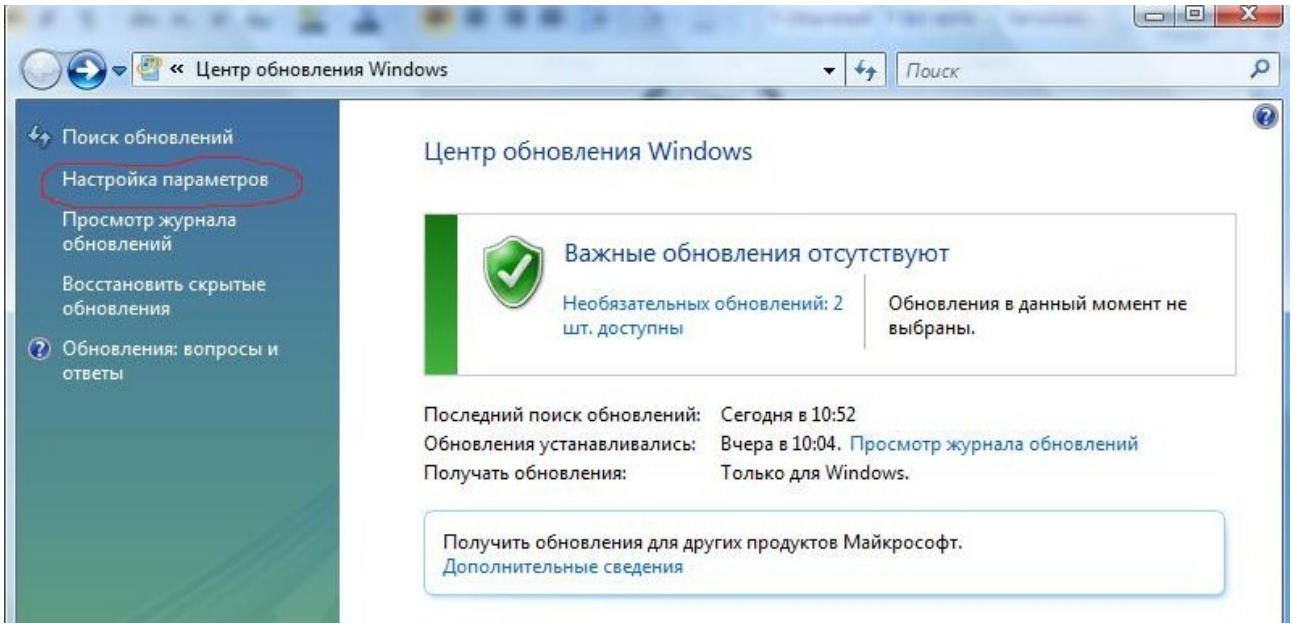
скрытые Радмин и кейлоггер; простые советы, которые вас оградят от хакерских инструментов, а также оптимизационные настройки и программы в целом, которые повлияют в хорошую сторону для вашей системы...

Обновления *Windows: быть или не быть?*

И всё-таки – БЫТЬ!!!

Заходим в: **ПУСК – Все программы – Центр обновления *Windows*** *или же:* ***ПУСК – Панель управления – Безопасность – Центр обновления Windows.***

Итак перед нами появилось панель обновлений.Мы уже обрадовались,что мы хоть их нашли :) Далее мы слева видим ***Настройка параметров:***



Заходим в ***Настройка параметров*** *и в графе* ***Важные обновления*** *ставим на* ***Устанавливать обновления автоматически (рекомендуется)*** *. Далее выбираем любой удобный день недели и время обновления и* ***ОК.***

Зачем это всё нам нужно? Обновления - это как витамины для человеческого организма! Что дают обновления для вашей системы:

- исправление ошибок внутри системы;
- загрузка драйверов;
- закрузка программ по удалению шпионского ПО, вирусов и прочей нечести. После загрузки она работает невидимо от пользователя (фоновый режим), но одноразово,т.е. сканирует ПК 1 раз после загрузки очередного обновления;
- «латание дыр» - т.е. выпускаются патчи (1 раз в месяц), которые исправляют уязвимости. Эти уязвимости используют вирусы,поэтому нам нужно их закрывать в своей системе. Вспомним,к примеру,нашумевший вирус Stuxnet ,который использовал сразу 4 «дыры» *Windows;*
- *общая оптимизация.*

Думаю над этом не стоит не стоит зацикливаться и расписывать тома по поводу обновлений. Всё и так понятно....Это только капля в море!

Брандмауэр или фаервол?

По сути это почти одно и тоже...А может и не одно и тоже?!..Ты сомневаешься уже?

Фаервол более динамичен в планах настройки, более функционален. Брандмауэр же более легок в использовании, минимум настроек. Зачем нам нужен брандмауэр/фаервол :

- Контроль за приложениями, использующими порты (в случае изменения приложения вирусами или троянами,

устанавливающимися в качестве плагинов, сетевая активность приложения блокируется);

- Назначение раздельных правил разным пользователям без дополнительной сетевой авторизации;
- В фаерволе режим обучения, когда при первом обращении программы к сетевым ресурсам пользователю выдаётся запрос (обычно вида «запретить всегда, запретить однократно, всегда разрешить, разрешить однократно, создать правило»).В брандмауэре проставляются исключения для программ;
- Режим смешанной фильтрации (при которой проверяются различные параметры на различных уровнях сетевых протоколов — от второго (проверка на фальсификацию MAC-адреса) до 4 (фильтрация портов)...простыми словами - контроль всего входящего из интернета посредством портов.Это очень важно!
- *ПРИМЕЧАНИЕ*: при установке фаервола отключаем родной брандмауэр *Windows и наоборот – это делается во избежании конфликта между ними.*

Что же вам выбрать?

Мой вам совет – если у вас на компьютере имеется ценная информация (например,пароли банковских счетов или ваш ПК учавствует в каких-то валютно-финансовых операциях и т.д.), то можно утверждать, что вам необходим фаервол. Если у вас в ПК имеется из самого ценного это пароли на Вконтакте и Одноклассники, то вам с головой хватит и родного ПРАВИЛЬНО НАСТРОЕННОГО родного брандмауэра *Windows* Vista и *Windows* 7, *т.е. для домашнего пользования. Однако, хочу заметить, что и в первом случае (когда ваш компьютер есть «денежным мешком») можно использовать родной брандмауэр*

Windows, но при условии, у вас есть голова на плечах и вы всё сделаете так,что написано в этой книге. Но мировой опыт подсказывает, что «круче» всё-таки фаервол.

Если вы заинтересовались фаерволами,то тройка лучших из лучших это:

- **COMODO Firewall** Free -http://soft.oszone.net/program/1985/Comodo_Firewall/
- **ZoneAlarm Firewall Free - http://www.zonealarm.com/security/de/zonealarm-pc-security-free-firewall.htm**
- **Agnitum Outpost Firewall Free - http://soft.oszone.net/program/10558/Outpost_Firewall_Free_2009/**

Все три фаервола вышеперечисленные я выбрал бесплатные (Free-версия), т.е. в них отсутствуют некоторые модули, чем в платных версиях (Pro-версия). Если всё-таки захотите платную версию фаервола,то вам данную версию придется или купить, или скачать, а затем искать ключи в интернете...именно ключи, а не кряки, кейгены... т.к. само понятие «кряк» (англ.Crack) или «кейген» (англ. keygen, key generator**) весьма опасно для вашего компьютера в плане вирусов, потому что именно в них часто встречаются вирусы! Поэтому, если уж не можете жить без кряка или кейгена, то лучше скачивайте их с торрент-трекеров...Но настоятельно не советую их использовать.... Для вашего же блага!**

Но хочу заметить,что **COMODO Firewall** Free из бесплатных фаерволов более-менее хорош, но выбор всегда за вами! Кроме того данный фаервол может конкурировать с платными версиями других фаерволов. Также присутствует в настройках русский язык. Поэтому, чтобы не искать ключи и ничего не тратить из денег, советую COMODO Firewall **Free** – просто, бесплатно, надёжно!

Кроме того в COMODO Firewall встроена «песочница» **sandbox,** в которой мы можем тестировать программы без вреда от того, что в программе имеется вирусы!

Безусловно, **Pro-версии фаерволов (платные) улучшены в плане безопасности за счет дополнительных функций. Но всё в ваших руках – можете скачать платную версию,но затем заняться поиском ключей. И одним из лучших платных фаерволов безусловно является** Agnitum Outpost Firewall Pro - http://soft.oszone.net/program/16/Agnitum_Outpost_Firewall_Pro/ **Вам только необходимо найти ключи в интернете...или покупайте.**

Установка и настройка фаерволов:

- Установка и настройка Agnitum Outpost Firewall - http://2ip.ru/article/outpost/
- Установка и настройка Comodo Firewall - http://2ip.ru/article/comodo/
- Установка и настройка ZoneAlarm - http://www.windowsfaq.ru/content/view/328/46/1/1/

ВНИМАНИЕ! После установки любого фаервола обязательно выставите в параметрах Режим обучения.

Однако мой выбор пал на родной брандмауэр *Windows при условии,что у меня Windows Vista. Хочу заметить, что Windows Vista и Windows 7 имеют практически индиетичные брандмауэры, но в Windows 7 идет уже более «навороченей».*

****Также хочу сказать,что именно на Windows Vista и Windows 7 брандмауэры более-менее из семейства Windows, в остальных версиях Windows они на порядок ниже идут, чем в Vista и 7. Поэтому если у вас другой Windows , то советую ставить фаервол.*

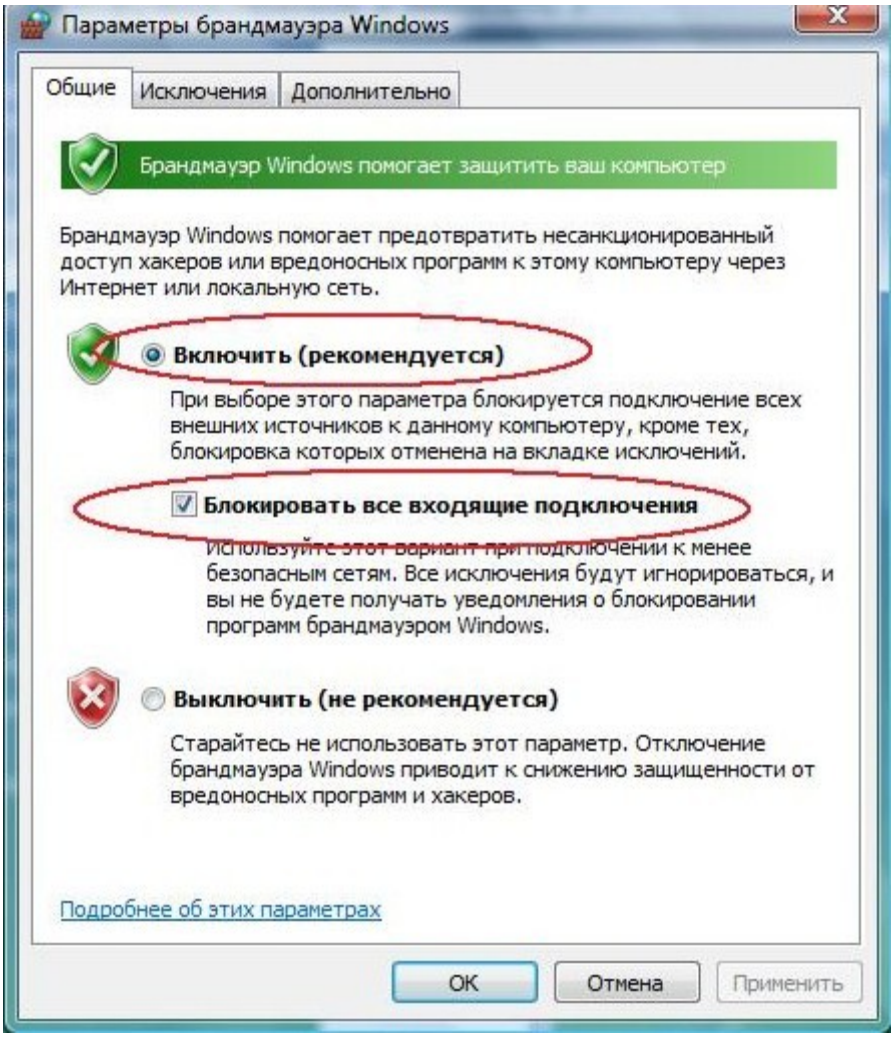
Почему я выбираю брандмауэр Windows Vista?

- *удобно;*
- *минимум настроек;*
- *вполне удовлетворяет безопасность моего компьютера.*

Однако...*В тоже время брандмауэр Windows слабо конкурирует с брандмауэрами (фаерволами) сторонних производителей. И если сравнить тестирования среди них, то продукт Windows отстает от фаерволов сторонних производителей* – Comodo, ZoneAlarm и Agnitum Outpost. Но не стоит отчаиваться! Попробуйте для начала родной брандмауэр *Windows... если не устроит вас, то вам ничего не мешает уже поставить сторонний фаервол. Лично я использую уже 3 года родной брандмауэр Windows – хочу сказать, что не так он и плох, как пишут, и пока он меня вполне устраивает. Но также не маловажен фактор лично вашей осторожности в плане вирусной безопасности! Если вы станете, например, качать программы из неизвестных источников, а также предварительно не проверив программу на вирусы перед установкой, то вас никакой фаервол и антивирус не спасет!....Главное – это иметь голову, а в голове должен быть мозг, который должен думать, что загружать, что скачивать, что устанавливать...*

Если вы решились на родной брандмауэр, то логично было бы для начала его включить :)

Пуск – Панель управления – Безопасность – Брандмауэр Windows – Изменить параметры *– ставим галочку на* ***Включить (рекомендуется)*** *и* ***Блокировать все входящие подключения – ОК:***



Включить (рекомендуется) *– это понятно – мы включили сам Брандмауэр, а вот* ***Блокировать все входящие подключения*** *– это мы включили наивысший уровень безопасности, который закрывает ВСЕ порты (на работе компьютера это не отразится).*

ВНИМАНИЕ! Если у вас двойной интернет, т.е. вы используете 2 и более компьютера (через ваш ПК подсоединен еще один и более ПК), то возможно, что на втором ПК может исчезнуть интернет! Если это произошло, то галочку тогда снимаем с Блокировать все входящие подключения. Также это касается если вдруг и на вашем компьютере исчезнет интернет – делаем по аналогии (однако это маловероятно и замечено такого не было). Также это касается, если вы используете локальную сеть – при её использовании данную опцию НЕ ВКЛЮЧАТЬ!

Если что-то не можете найти или не получается, то смотрим сюда - http://windows.microsoft.com/ru-RU/windows7/Understanding-Windows-Firewall-settings

Проведем эксперимент!

Снимите галочку в Брандмауэре с ***Блокировать все входящие подключения***.

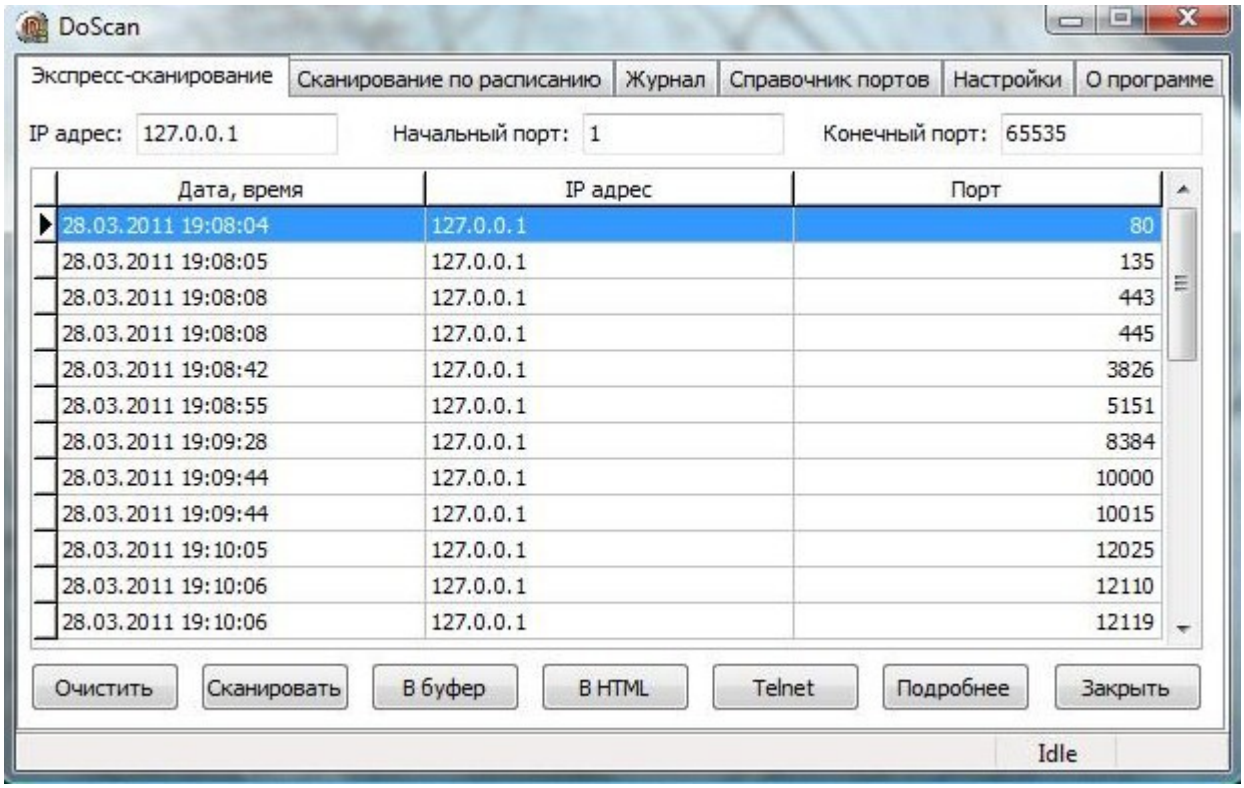
Рассмотрим метод сканирования «снаружи»,т.е. как ваши порты видит виртуальный мир. Заходим на эти сайты:

1) http://smart-ip.net/tools/ports-scan (выбираем НАЧАТЬ СКАНИРОВАНИЕ)
2) http://2ip.ru/port-scaner/ (выбираем ПРОВЕРИТЬ)
3) http://tools-on.net/privacy.shtml?2 (выбираем по очередности все три теста)
4) http://www.windowsfaq.ru/content/view/451/82/ - **самый «реальный» сканер портов:** ставим сканирование от 1 до 65535 портов. Должны понимать, что на Vista всегда будет открыт порт 21 и его никак не закрыть. Сканирование проводим в несколько заходов – за один заход сканируется 1-9572 порты, затем заново выставляем скан уже с **9572**-65535 и т.д.

Однако не исключено, что сканирование возможно будет проводиться вашего провайдера, поэтому если вы не уверены в вышеуказанных онлайн-сервисах, то вы можете просканировать уже со 100%-й уверенностью, что сканирование будет именно ваших портов,т.е. метод сканирования портов «изнутри», благодаря программе Сканер портов - http://www.softportal.com/software-4285-skaner-portov.html

Или можно использовать портабельную (без установки) версию сканера TCP портов DoScan - http://www.windowsfaq.ru/content/view/687/92/

Однако, я решил просканировать порты «изнутри» программой DoScan и я ужаснулся:



Не может же быть столько открытых портов?! ...Мы помним, что данной программой мы сканировали «изнутри» системы, а не «снаружи». Пришлось «поднять на уши» весь интернет и вот, что я любопытное нашел – отвечает **Олег Зайцев** (разработчик AVZ), цитирую: «Нельзя "сканировать на открытость порты изнутри" - понять, можно ли подключиться по порту Y можно только просканировав ПК "снаружи", причем нужно еще понимать, что в того-же KIS есть понятие локальной сети и Интернет - для локальной сети правила более мягкие, и сканируя свой компьютер с ПК соседа я могу получить совершенно иную картину, чем при сканировании портов с какого-то ПК в Инет...»
Источник: http://virusinfo.info/showthread.php?t=62567

При сканировании «снаружи»(например, из сайтов онлайн-скана) – вот, что самое основное, так нас видит Интернет, грубо говоря...и если порты открыты «извне», значит из этой же области к нам могут подключиться или послать пакет данных, в котором могут быть

вирусы. А это значит, что порты должны быть под защитой фаервола или брандмауэра, т.е. должен быть контроль над портами, особенно «снаружи». Да и порты закрыть в настройках фаервола никто не отменял – см. ниже по тексту.

Если будет хоть один порт открыт при сканировании «снаружи», то это есть плохо! А если 2 и более, то ваша система очень даже уязвима!!!

Если вы увидите, что порты закрыты, то поздравляю вас!

Также на этом сайте можете пройти 1,2,4,5 и 6 тесты:

5) http://www.pcflank.com/

С результатами,полагаю,разберетесь :)

А теперь попробуйте пройти тесты методов сканирования «снаружи» заново на предложенных четырех сайтах при включенной опции в брандмауэре ***Блокировать все входящие подключения***! Если порты были до этого открыты,то они теперь закрыты (либо под защитой), если в тестах четвертого сайта вы где-то провалили тест, то теперь ваша система их прошла! Чувствуете разницу?

С точки зрения брандмауэра и ряда онлайн-тестов сетевой порт может иметь три состояния: open (открыт), closed (закрыт) и stealthed (скрыт). «Открытым» называется порт, который виден извне, отвечает на запросы и принимает подключения(самое опасное); «закрытым» - порт, который виден извне, но не отвечает на запросы и не принимает подключения; «скрытым» - порт, который не виден извне, и, таким образом, невозможно определить, каков его статус.

Однако, если вы используете нужный вам порт, то его не следует закрывать, это и так логично! В фаерволе и брандмауэре можно ставить исключения, как на порты, так и на программы, которые могут использовать порты.

Как правильно закрывать порты в фаерволах?

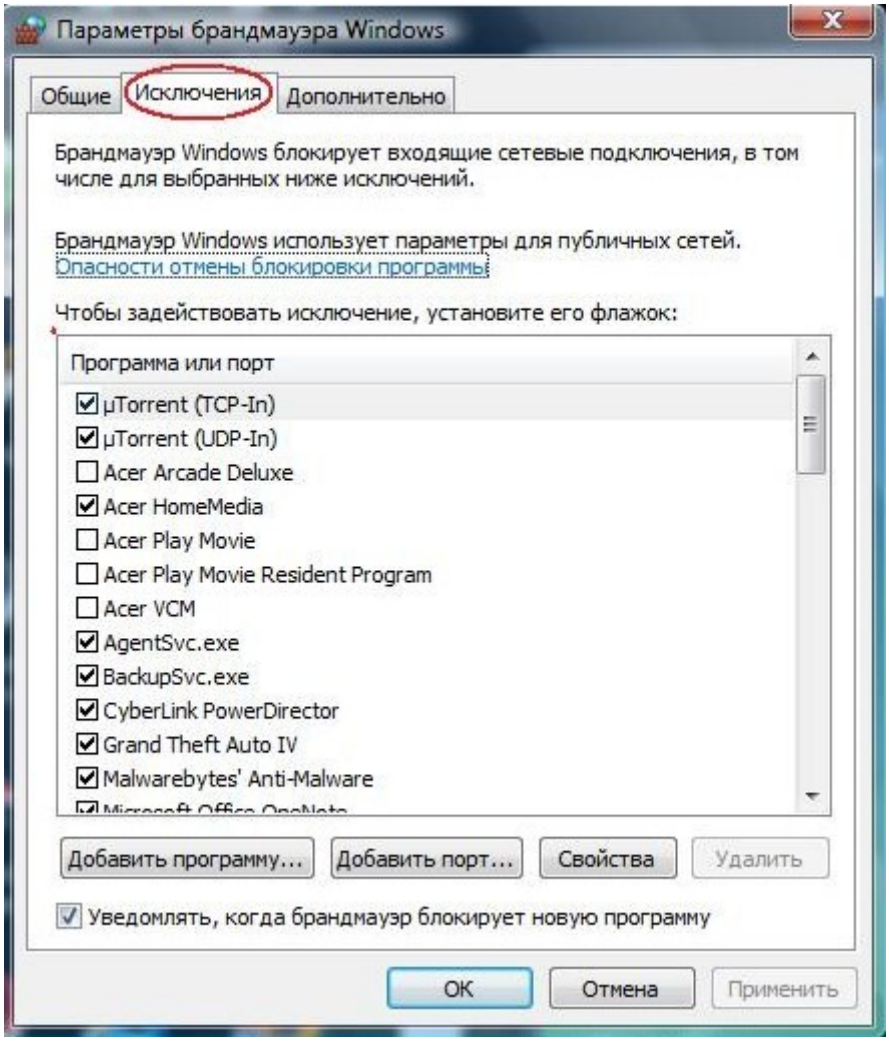
- Как закрыть порты в Outpost Firewall - http://2ip.ru/article/ruleoutpost/
- Как закрыть порты в ZoneAlarm PRO - http://2ip.ru/article/rulezonealarm/
- Как закрыть порты в Comodo Firewall - http://2ip.ru/article/rulecomodo/
- Как закрыть порты в Kaspersky Internet Security - http://2ip.ru/article/rulekis/

Если по каким-то причинам вы не можете закрыть тот или иной порт (порты), то вам в этом поможет программа **Windows Worms Doors Cleaner** - http://2ip.ru/article/portsrule/

ВНИМАНИЕ! Не забудьте поставить во вкладке Исключения в брандмауэре те программы (FTP, P2P, ICQ-клиентов и т.д.), которые могут выходить в интернет и которые вам нужны! Кратчайший путь:

Пуск – Панель управления – Безопасность – Разрешение запуска программы через брандмауэр *Windows*

... или смотрим в настройках Брандмауэра:

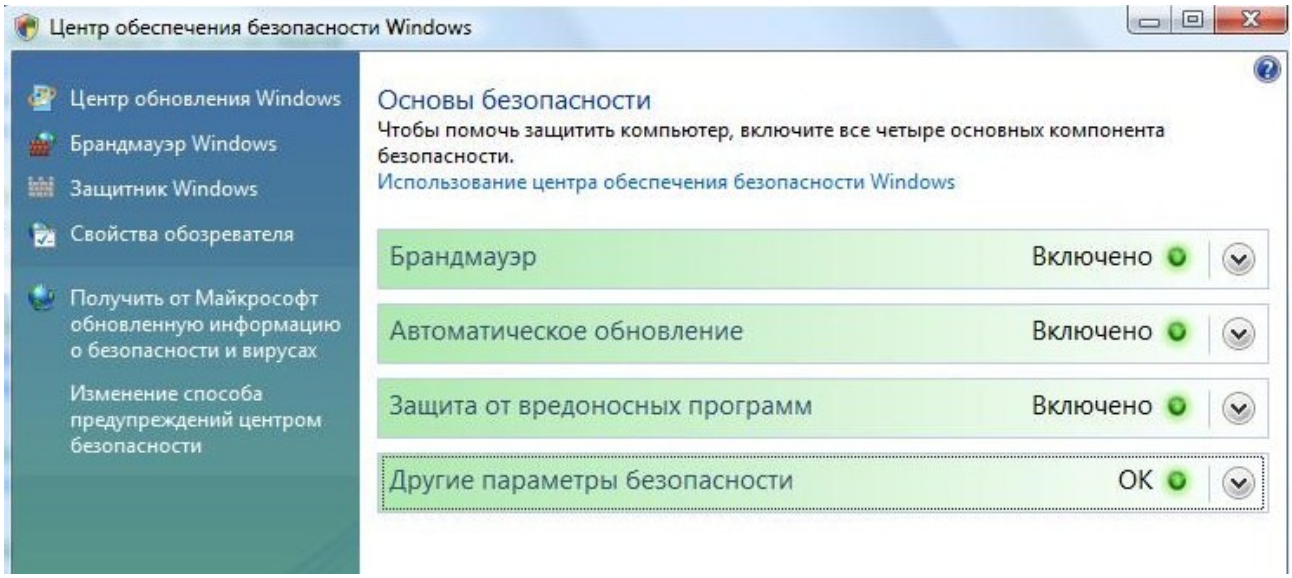


ВЫВОД: Брандмауэр представляет собой программный или аппаратный комплекс, который проверяет данные, входящие через Интернет или сеть, и в зависимости от параметров брандмауэра блокирует или разрешает их передачу на компьютер.Брандмауэр поможет предотвратить проникновение хакеров или вредоносного программного обеспечения (такого как черви) в ваш компьютер через сеть или Интернет. Брандмауэр также помогает предотвратить отправку вредоносных программ на другие компьютеры....По крайней мере нам это обещает сам Microsoft!!!

Центр обеспечения безопасности Windows

Звучит серьезно!...

Открываем: **Пуск – Панель управления – Безопасность - *Центр обеспечения безопасности.*** *Мы видим,что напротив Брандмауэра и Автоматическое обновление уже горит зеленый свет,что уже радует! А вот в разделе* ***Защита от вредоносных программ*** *у нас должно стоять* ***Защита от вирусов*** *(антивирус) и* ***Защита от шпионских и других вредоносных программ*** *(Защитник Windows), примерно так:*

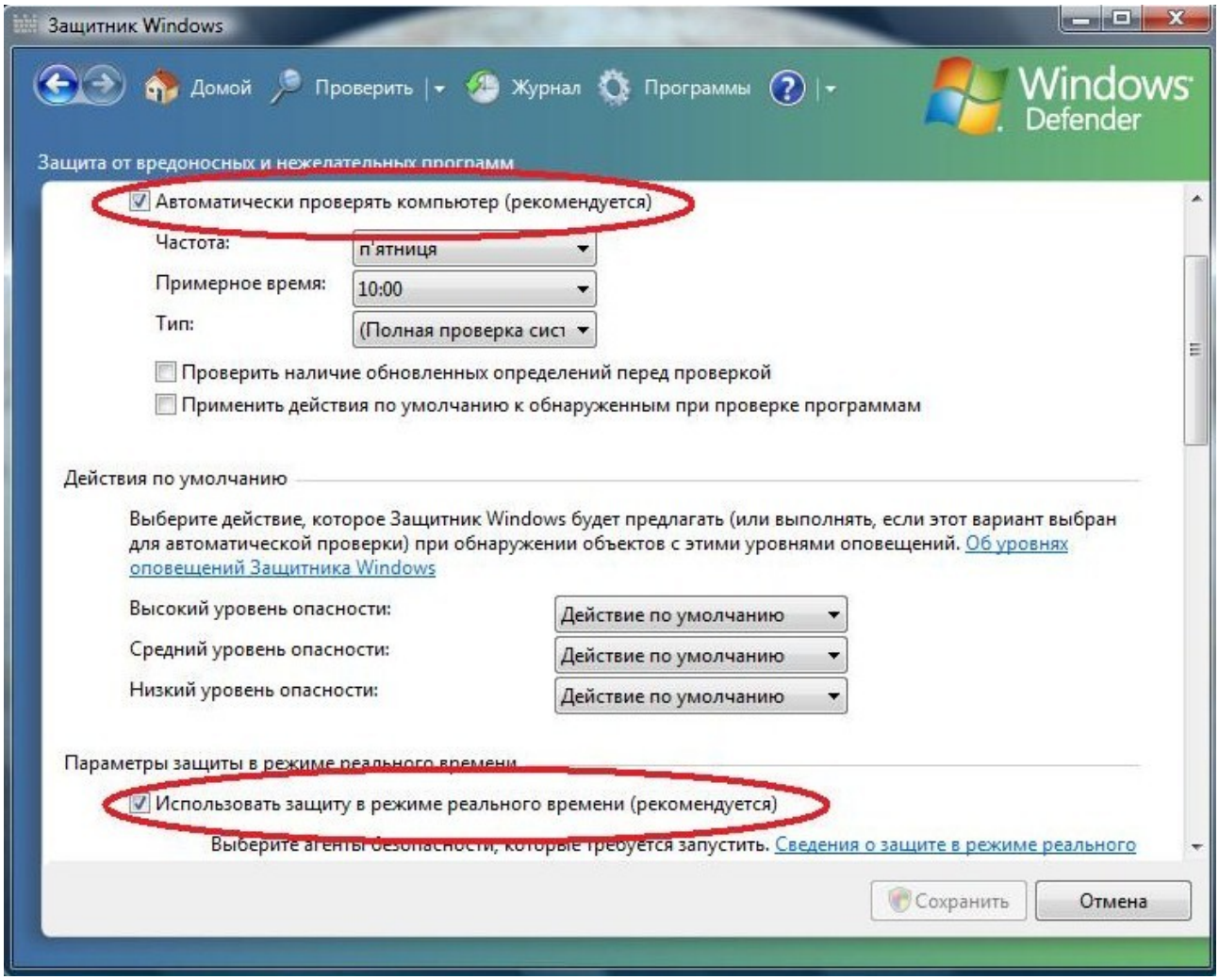


По поводу антивируса я позже напишу,а пока разберемся с Защитником Windows (Windows Defender). В этом же окне слева вы увидите ***Защитник Windows,*** *кликаем на него и в новом окне ищем вверху* ***Программы.*** *В этом разделе выбираем* ***Параметры.*** *Здесь мы ставим галочку на* ***Автоматически проверять компьютер (рекомендуется),*** *а также* ***Использовать защиту в режиме реального времени (рекомендуется),*** *далее:*

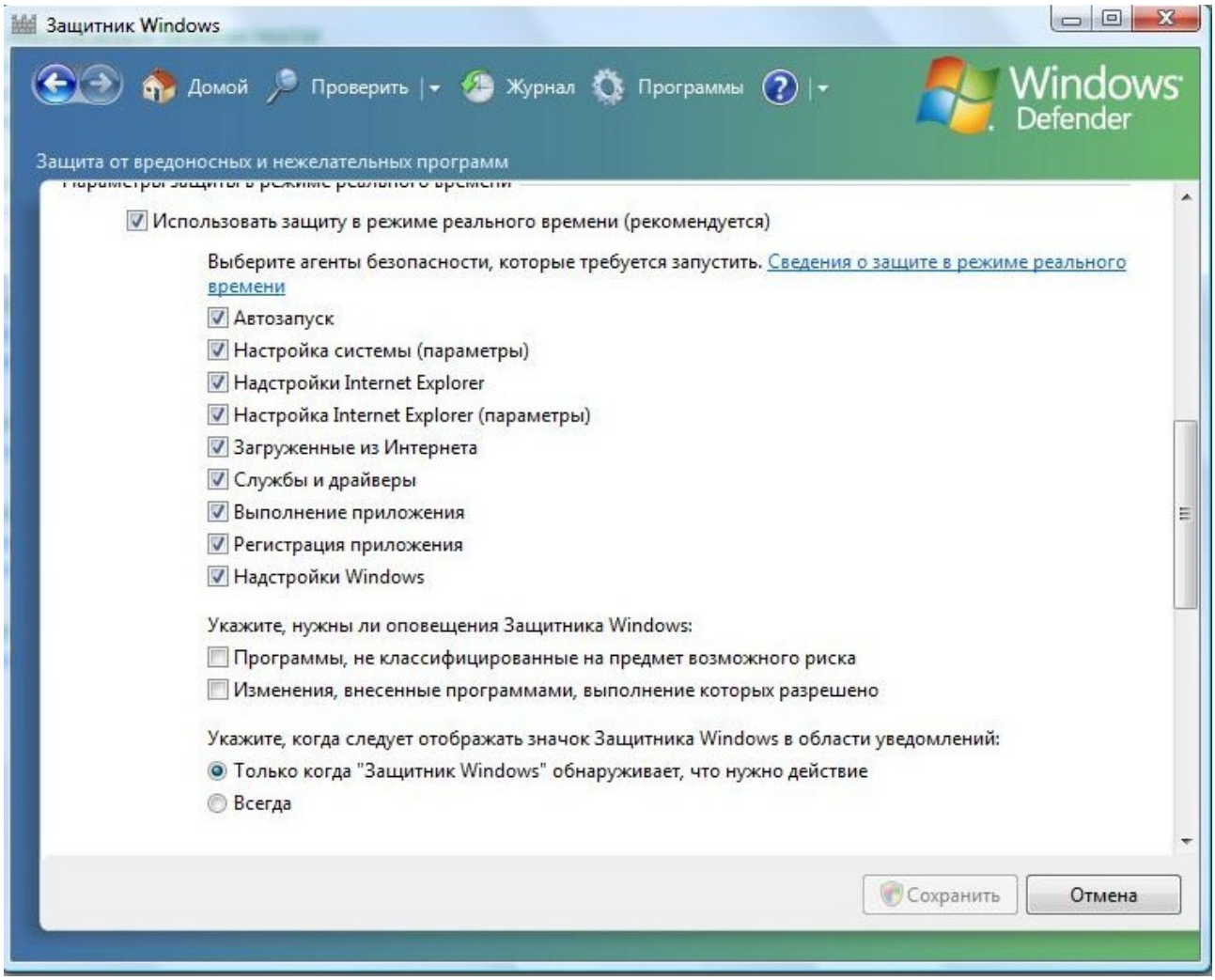
- **Частота:** выбираем любой день, какой вам удобно;
- **Примерное время:** желательно в утреннее, когда вы включаете компьютер;
- **Тип:** ставим на Полная проверка системы.

- Далее на **Высокий - , Средний - , Низкий уровень опасности** ставим По умолчанию.

Это будет выглядеть следующим образом:



Далее проставляем галочки также, как и на рисунке ниже:



Далее проставляем везде галочки и кликаем на Сохранить.
Что мы запустили?

Windows Defender (*Защитник Windows*), ранее известный как Microsoft AntiSpyware — программный продукт компании Microsoft, созданный для того, чтобы удалять, помещать в карантин или предотвращать появление spyware-модулей в операционных системах Microsoft Windows. Windows Defender по умолчанию встроен в операционные системы Windows Vista и Windows 7, и бесплатно доступен для скачивания при использовании Windows XP и Windows Server 2003.

Защитник Windows призван защищать систему от руткитов, кейлоггеров, шпионов и другого подобного вредоносного программного обеспечения; по своей сущности этот компонент относится скорее к антишпионским, чем к антивирусным решениям, поскольку неспособен к противодействию классическим вирусам. Его

задача состоит в отслеживании автозагрузки, настроек безопасности системы, дополнений и настроек IE, загрузок IE (прежде всего ActiveX). Также отслеживается работа служб, драйверов, выполнение приложений, регистрация приложений для автозагрузки, работа утилит операционной системы. При обнаружении подозрительных моментов Защитник сообщает об этом пользователю. Имеет собственную обновляемую раз в неделю базу.

Как видим не так уж и плохо звучит!..Однако, более продвинутые пользователи скажут,что Защитник *Windows неэффективен и что он может только удалить «детские» вирусы. Допустим,что это так, но если он будет ловить хоть что-то из шпионов и вирусов, то разве это нам помешает? Что-то словит Защитник* Windows*,что-то Антивирус, что-то другие программы и в итоге мы имеем неплохие результаты.*

Восстановление системы

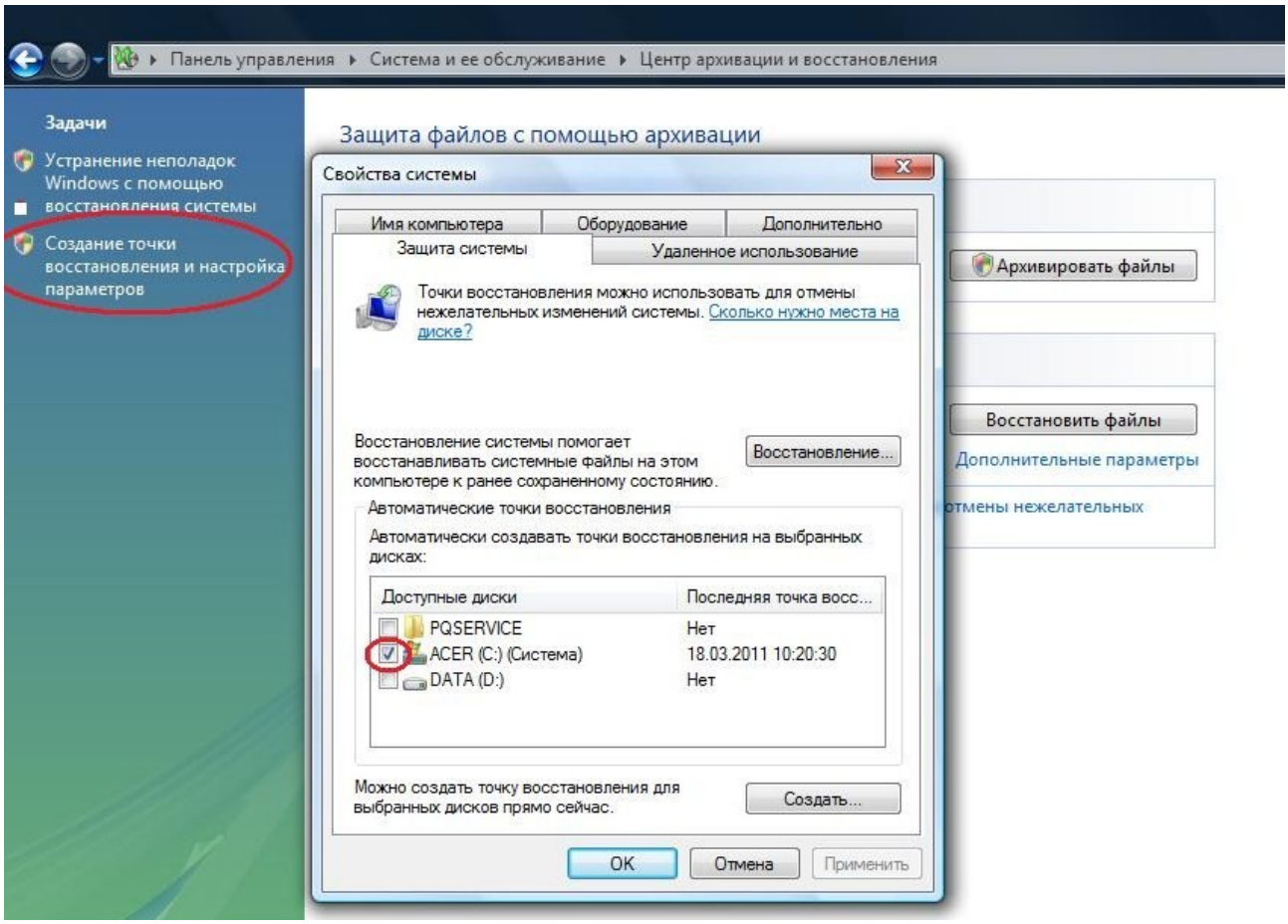
Восстановление системы позволяет восстановить состояние системных файлов компьютера на предшествующий моменту времени. Это позволяет отменить изменения, внесенные в систему компьютера, не затрагивая личные файлы, такие как электронная почта, документы или фотографии.

Иногда в результате установки программы или драйвера возникают неожиданные изменения (в том числе и отрицательные) в компьютере или наблюдается непредсказуемое поведение ОС Windows. Обычно удаление программы или драйвера позволяет устранить проблему. Но если удаление не привело к устранению проблемы, то можно попробовать восстановить состояние системы компьютера на момент времени в прошлом, когда все работало надлежащим образом. Также в некоторых случаях это касается, если ваша система была заражена вирусом и именно восстановление

системы может помочь, однако не во всех случаях это эффективно. Но мы не можем это сбрасывать со счетов, пусть будет....

Восстановление системы использует функцию, называемую защита системы, для регулярного создания и сохранения на компьютере точек восстановления. В точках восстановления содержатся сведения о параметрах реестра и другие сведения о системе, используемые ОС Windows. Точки восстановления также можно создавать вручную, но мы поступим следующим образом - поставим на автоматическую точку восстановления в Windows Vista:

Пуск – Панель управления – Система и её обслуживание – Центр архивации и восстановления – слева в колонке **Создание точки восстановления и настройка параметров –** вкладка **Защита системы -** ставим галочку на диске (С) – **Применить:**



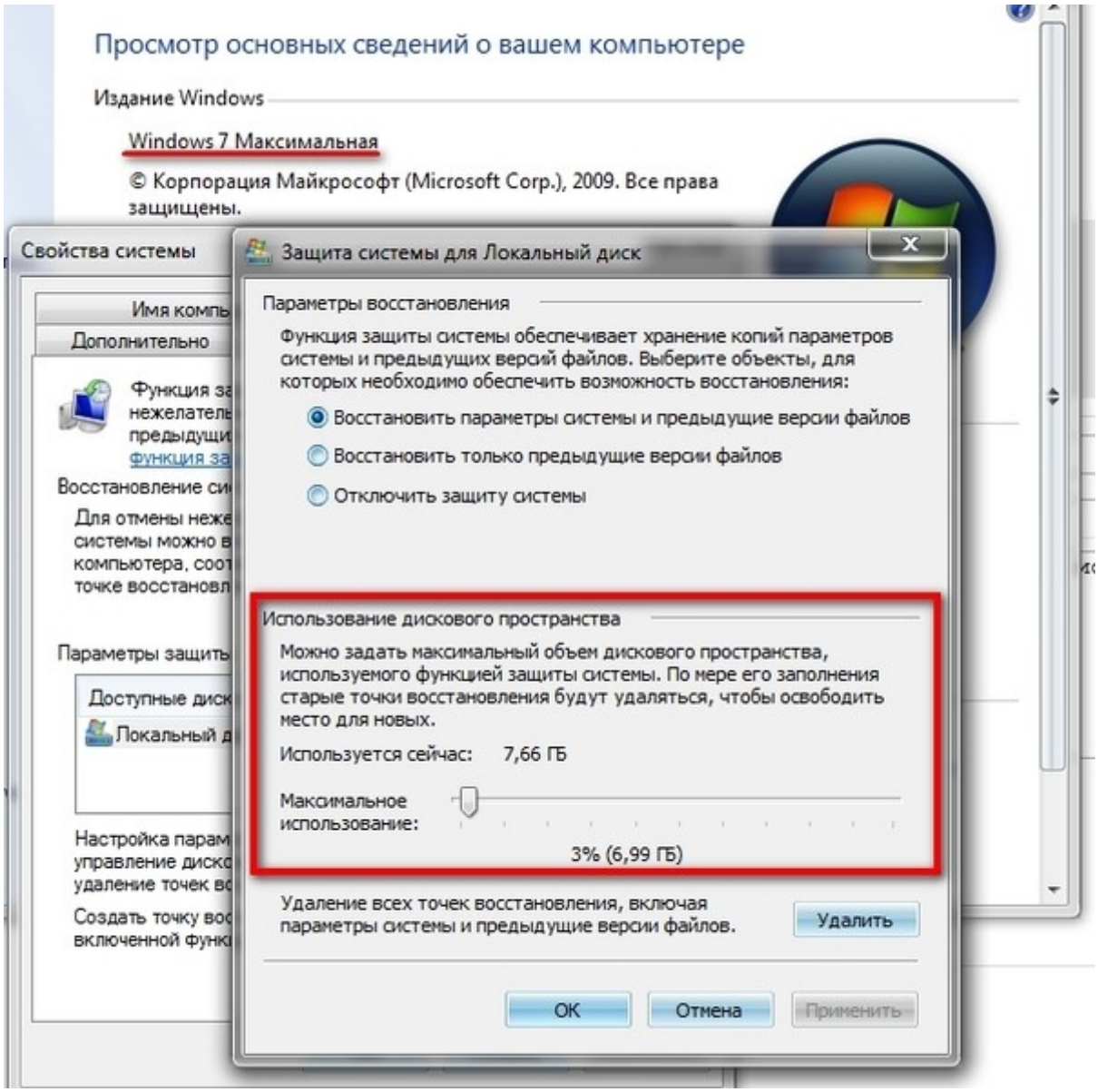
Также вы сами можете создать вручную точку восстановления в этом же разделе, как вам будет удобно...

По своему опыту хочу сказать, что восстановление системы меня спасло один раз – по спешке я установил антивирус предварительно не удалив старый антивирус, возник конфликт программ и система не могла загружаться при включении. Решение проблемы – при загрузке Windows жмём клавишу **F8** и выбираем **Восстановление последней удачной конфигурации**. Это как пример вам на будущее, в случае невозможного нормального запуска Windows.

Хочу сказать, что восстановление системы – это очень важная опция и зачастую она почему-то у многих отключена, а затем когда проблемы с системой, то тут возникает проблема восстановления, т.к. она отключена. Вполне закономерно, что многие её отключают, потому что сама точка восстановления занимает некий объём (гигабайты) вашего жесткого диска, который вы могли бы «забить» более «ценной» информацией – музыка, фильмы и т.д. И вот поэтому, когда нагрянет беда вы начинаете себя укорять, что отключили восстановление системы и, как говорится, после боя кулаками не машут. Поэтому включаем данную опцию и радуемся.

Кстати, в Windows 7 проблема места для выделения точки восстановления существенно изменилась в лучшую сторону – теперь мы можем сами выбирать количество гигабайт на жестком диске для точки восстановления. В Windows 7 это так:

Пуск - Панель управления - Система - Дополнительные параметры:



Ограничения по локальной сети

Локальная сеть - компьютерная сеть, покрывающая обычно относительно небольшую территорию или небольшую группу зданий (дом, офис, фирму, институт). Локальных сетей много видов: где-то локальная сеть представляется как выделенный сервер с которого мы скачиваем с огромной скоростью фильмы,музыку и т.д.,что есть очень даже прекрасно...а где-то компьютеры могут соединяться между собой, используя различные среды доступа и это должно нас пугать в некой степени! Ведь между компьютерами есть СВЯЗЬ, а если есть связь, то и недалеко до несанкционированного доступа к вашему ПК.

Чего нам следует бояться?

Опять же - хакера со своими хакерскими инструментами. Приведу пример: у меня есть локальная сеть, я вижу других пользователей, а значит и меня видно. И вот ваш сосед по локальной сети подцепил вирус (какой-нибудь червь с непонятным названием). Этот червь конечно же не упустит такой возможности, как «залезть» в локальную сеть. Что происходит? Данный вирус будет «бомбить» порты ВСЕХ пользователей локалки! Какой именно порт ему бомбить, это будет зависить от того, как его запраграммировал хакер.....не думаю, что он запраграммировал червяка с добрыми намерениями. Очень часто «бомбежкам» вируса подвергается 135 порт и многие другие. Видите гремучую смесь - вы видны в локальной сети + у вас возможно данный порт открыт + нет надлежащей защиты = вам капец! :) В ваш компьютер хакер «зальёт» какую-нибудь гадость и от этого, поверьте, вам не станет лучше!

Хочу заметить, что добросовестный провайдер вирус сразу же ликвидирует, а тот провайдер, которому и дела нет, что творится в локальной сети, особо не станет переживать....Такова реальность!

Что делать? Как защититься?

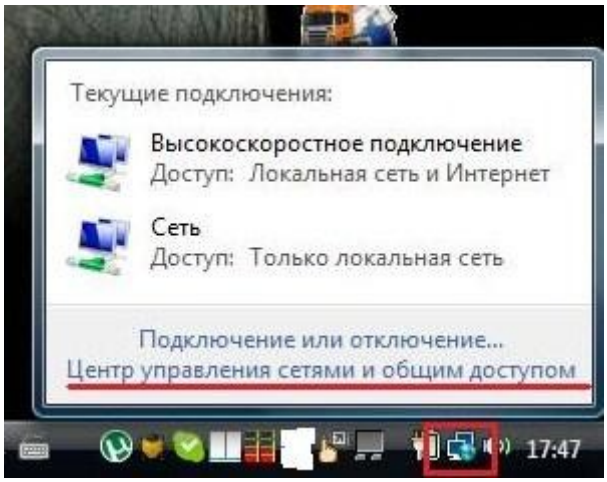
Если вы внимательно читали, что выше написано, то часть проблем уже решена. Чтобы все порты были закрыты и чтобы черви и вирусы в них не ломились, то мы их закрыли брандмауэром (или же фаерволом). Напомню,что в брандмауэре ***Windows*** :

Пуск – Панель управления – Безопасность – Брандмауэр Windows – Изменить параметры – *ставим галочку на* ***Включить (рекомендуется)*** *и* ***Блокировать все входящие подключения – ОК****.*

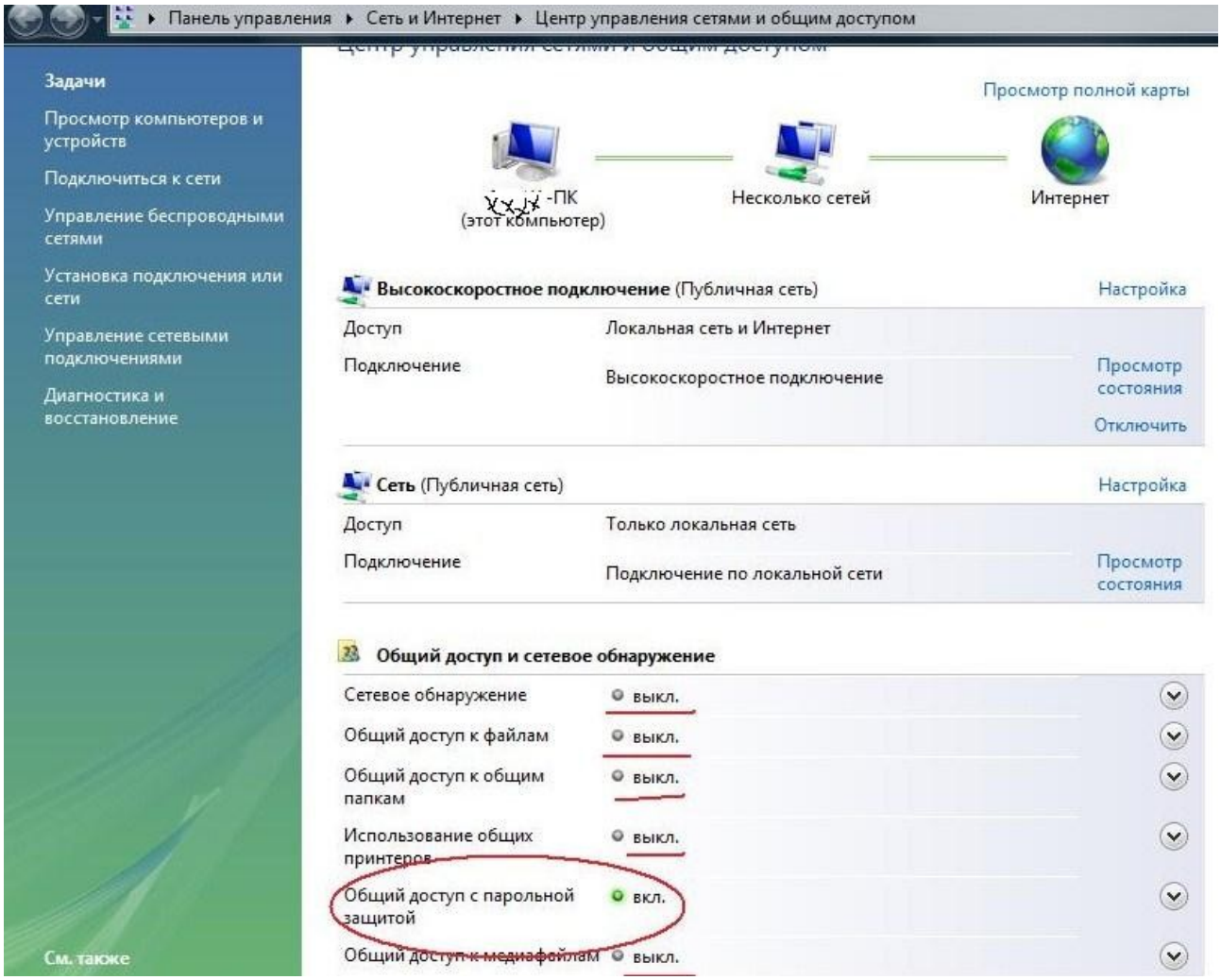
Именно опция Блокировать все входящие подключения и закрывает открытые порты снаружи.

Теперь идём сюда:

Пуск – Панель управления – Сеть и Интернет – Центр управления сетями и общим доступом или же кликнуть мышкой по соединению 1 раз:



В подразделе <u>*Общий доступ и сетевое обнаружение*</u> *у нас должна быть ВКЛЮЧЕНА только одна опция* ***– Общий доступ с парольной защитой.*** *Всё остальное должно быть выключено в этом* ***(****Общий доступ и сетевое обнаружение****)*** *разделе:*



Если всё это выполнено, то вы более-менее защищены от проникновения со стороны локальной сети!

UAC для повышения безопасности или...?

User Account Control, UAC (средство контроля пользовательских учетных записей) — компонент Microsoft Windows, впервые появившийся в Windows Vista,а затем и Windows 7. Этот компонент запрашивает подтверждение действий, требующих прав администратора, в целях защиты от несанкционированного использования компьютера.

Прошу заметить,что Контроль учетных записей требует права Администратора, т.е. если вы устанавливаете программу не дай Бог с вирусом, то и вирус получает автоматически права Админа, т.е. высший приоритет! Многие эту функцию отключают, т.к. при любой установке программ, запуске программ всегда запрашивается подтверждение в виде всплывающего окна,что большинство пользователей просто раздражает! Но в этом есть и плюс – без вашего ведома (вашего подтверждения) никто за запустит программу дистанционно на вашем компьютере (теоретически). Но минус в том, как я написал выше - требует права Администратора. Медаль двух сторон.

***Мой вам совет – её нужно отключить*!** Но лично у меня она включена и я работаю на правах Администратора, (т.к. я знаю с какими программами я работаю и что запускаю или загружаю), хотя знаю, что это не совсем правильно...

Заходим сюда:
Пуск – Панель управления – Учетные записи пользователей и семейнай безопасность – Учетные записи пользователей – Включение или выключения контроля учетных записей (UAC) И снимаем (или ставим если уверенны в себе на все 100%) галочку на Используйте контроль учетных записей (UAC) для защиты компьютера и ОК.

В Windows Vista контроль учетных записей можно отключить, однако уровень обеспечения конфиденциальности и целостности программ и данных существенно снизится.

В Windows 7 UAC был доработан, в частности, в панели управления вместо единственной настройки либо включавшей UAC, либо выключавшей его появились четыре режима работы:

- всегда уведомлять;
- уведомлять только при попытках программ внести изменения в компьютер;
- уведомлять только при попытках программ внести изменения в компьютер (не затемнять рабочий стол);
- никогда не уведомлять.

ВНИМАНИЕ! Если всё-таки вы включили UAC и работаете под Администратором, то вам очень даже не лишним будет поставить пароль на вашу учетную запись! Пароль всегда будет при включении компьютера запрашиваться, т.е. компьютер «думает», что зашел Админ. Пароль мы ставим в этом разделе:

Пуск – Панель управления – Учетные записи пользователей и семейнай безопасность – Учетные записи пользователей

Пароль ставим не типа: 1111 или 1q2w3e и т.д., а ставим сложный пароль.

Как это реализовать и в тоже время легко запомнить?

Выберите одно слово, но не простое, а к примеру, как ваш(ваша) друг, жена или подруга вас называет, какое-нибудь слово неповторимое, оригинальное...подумайте....И к этому слову добавьте цыфры, например год рождения, или номер телефона, или индекс города... что вам легче запомнить. А между словом и цыфрами настоятельно рекомендую использовать спецсимволы типа **!»№;%:? *()_+/,** Учтите, что **русский алфавит** предпочтительнее латинского! А также пароль должен состоять **не менее из 10 знаков** по возможности!

<u>В любом случае пароль не будет лишним, поверьте!</u>

<u>Работаем под обычным пользователем</u>

Если вы не желаете работать под Администратором по каким-то причинам, то проходим сюда:

Пуск – Панель управления – Учетные записи пользователей и семейнай безопасность – Учетные записи пользователей – Изменение типа своей учетной записи – выбираем **Обычный доступ – ОК**

Что это нам даст я уже чуть выше написал!

Раз мы уж тут в этом разделе, то советую отключить Учетную запись Гостя, если, конечно, вы её не используйте :

Пуск – Панель управления – Учетные записи пользователей и семейнай безопасность – Учетные записи пользователей – Управление учетными записями.

Удаленное управление

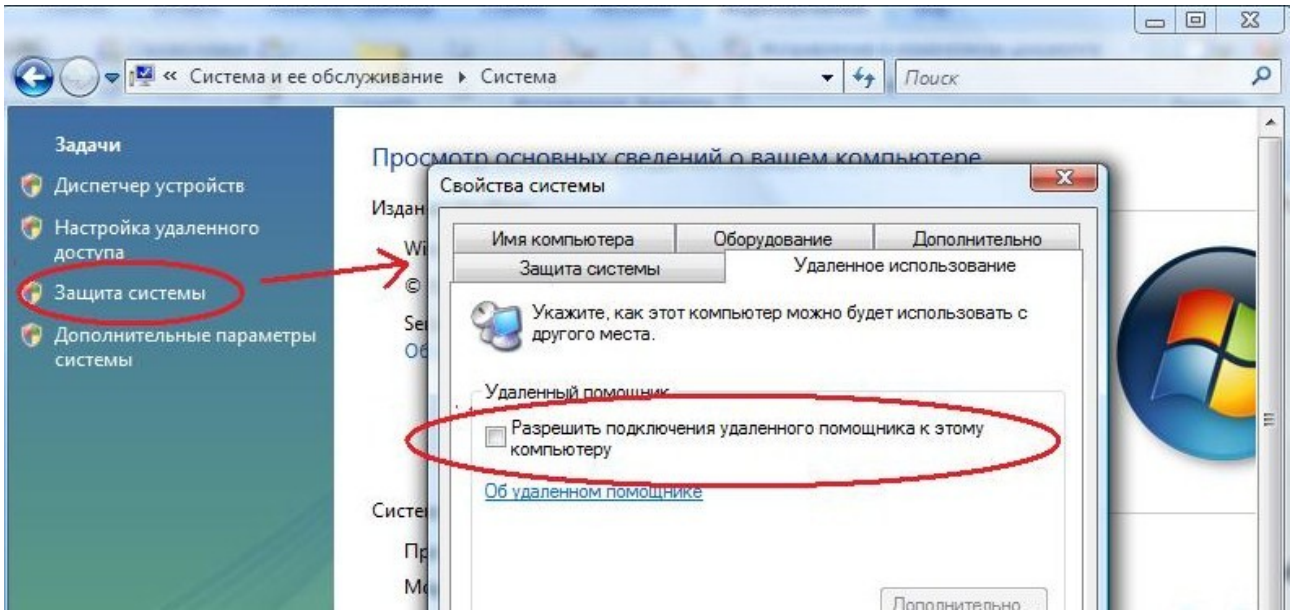
Рекомендуется отключить системные возможности удаленного управления. Для чего это делается, думаю,не стоит вам рассказывать.

Делается это следующим образом:

Пуск - Панель управления – слева увидите **Классический вид – Система –** вкладка **Удаленное использование -** снять галочку **Разрешить отправку приглашения удаленному помощнику – ОК.**

Также элемент удаленного управления снимаем тут:

Мой компьютер – Свойство системы – слева ищем **Защита системы – Удаленное использование –** снять галочку с **Разрешить подключения удаленного помощника к этому компьютеру – ОК:**



Автозапуск

Отключение автозапуска приводов CD/DVD-ROM и Flash-Drive рекомендуют многие специалисты.

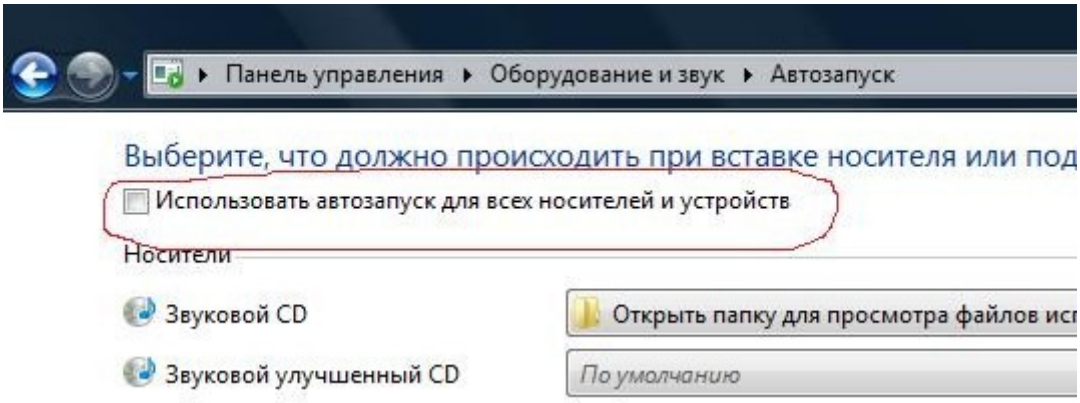
Зачем нам это, ведь это так удобно?

В настоящее время файлы **autorun.inf** и **autorun.ini** широко используются для распространения компьютерных вирусов через flash-накопители и сетевые диски. Для этого авторы вирусов прописывают имя исполняемого файла с вредоносным кодом в параметр «open». При подключении заражённого flash-накопителя Windows запускает записанный в параметре «open» файл на исполнение, в результате чего происходит заражение компьютера.

Находящийся в оперативной памяти заражённого компьютера вирус периодически сканирует систему с целью поиска новых дисков, и при их обнаружении (при подключении другого flash-накопителя или сетевого диска) создаёт на них autorun.inf со ссылкой на копию своего исполняемого файла, обеспечивая таким образом своё дальнейшее распространение.

Из этого всего понятно уже,что нам нужно отключить Автозапуск всех носителей и устройств:

Пуск – Панель управления – Оборудование и звук – Автозапуск – снимите галочку с **Использовать автозапуск всех носителей и устройств – Сохранить:**



Но для полной уверенности советую установить крошечную утилитку USBGuard , которая мало того, что не пустит вирус в компьютер,так еще и вирус уничтожит (хотя если у вас антивирус будет «нормальный», то и он это сможет сделать).

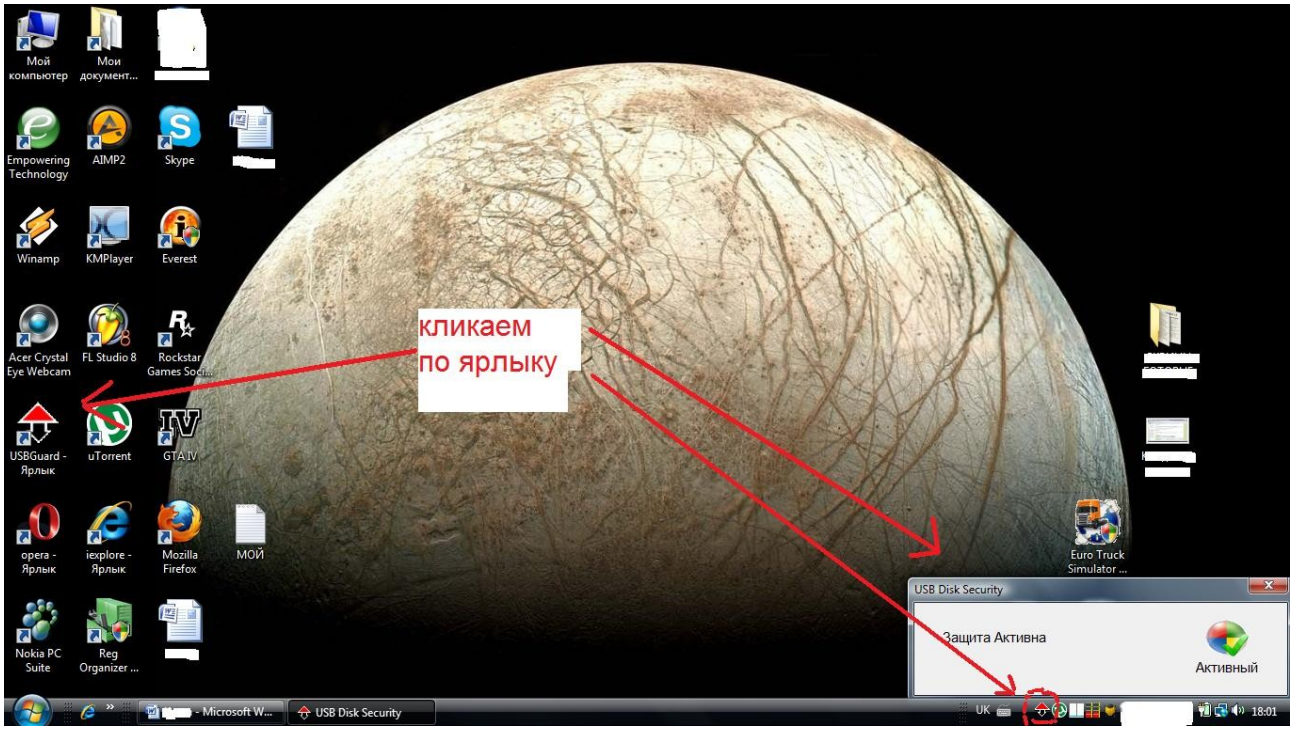
ВНИМАНИЕ! Однако даже если функция автозапуска отключена, заражение происходит при попытке пользователя открыть подключённый диск (флешку) для просмотра и тут нам не обойтись без стороннего софта или этой статьи - http://support.microsoft.com/kb/967715/KB967715 ,

в которой полностью решают данную проблему. Что касается сторонней программы, то тут выступает антивирус, но и лишней никак не будет и специализированный софт по отлову «авторанов».

Предлагаю скачать и установить **USBGuard** сам пользуюсь и доволен. Ссылка на скачивание - http://rusprogram.3dn.ru/cload/files-iW8vRVQppY.rar

Работает на платформе: Windows 95, Windows 98, Windows 2000, Windows XP, Windows NT 4.0, Windows ME, Windows Vista.
После установки на рабочем столе появится ярлык программы.

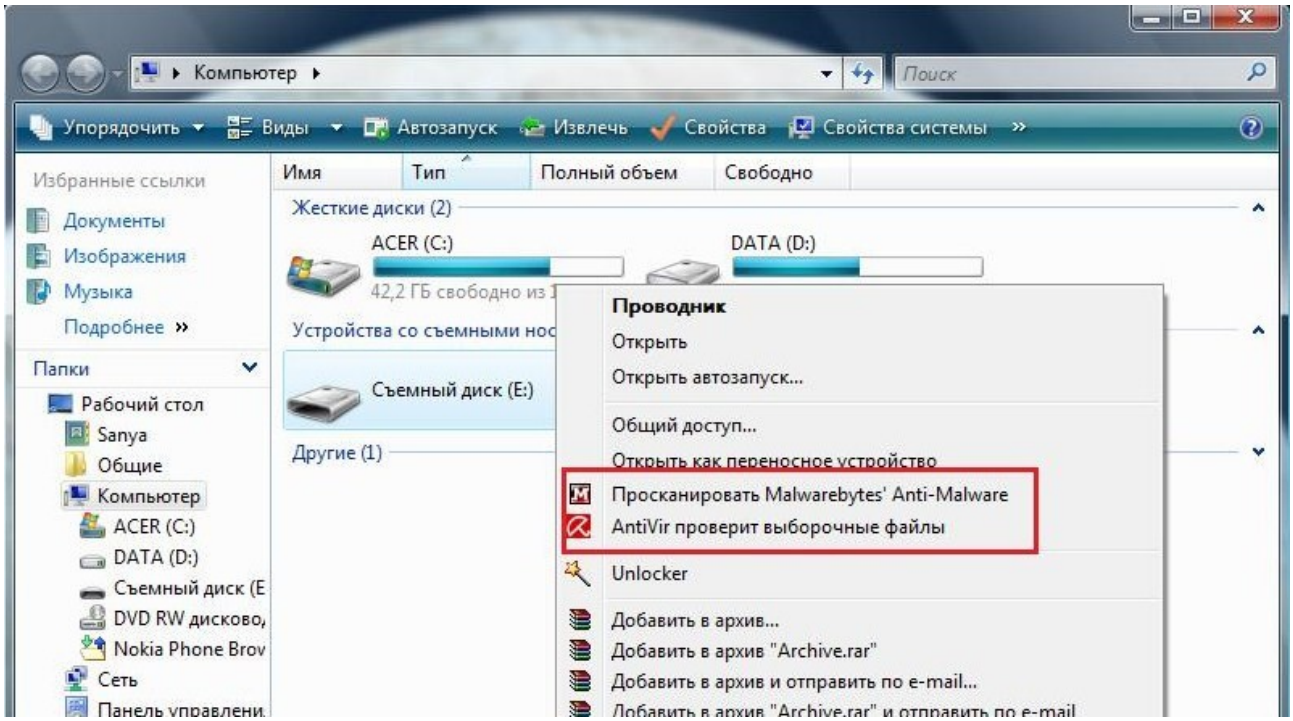
Теперь каждый раз до того, как вставить флешку, запускайте эту утилиту (клик по ярлыку), или добавьте ее запуск в автозагрузку. Если на флешке будут вирусы, программа вам это сообщит, и вы сможете безболезненно удалить и **autorun.inf** и **autorun.ini** и сам **файл вируса.**



Как успели заметить USBGuard не работает на **Windows 7** (по крайней мере я не нашел его в списке)...Однако не растраивайтесь – имеется аналог, который будет работать на платформе Windows 7. Вы можете установить программу **Зоркий глаз** - бесплатный антивирус типа anti autorun, который находит и изолирует 100% вирусов, распространяющихся на флешках (по файлу автозапуска Autorun.inf). Не требует никаких обновлений вирусных баз. Может работать параллельно с любым другим антивирусом.
Платформа: Windows 7, Vista, XP
Скачиваем здесь:
http://www.softportal.com/software-16221-zorkij-glaz.html

Однако хочу заметить, что две вышеуказанные программы (USBGuard и Зоркий глаз) узкоспекиализированы, т.е. «ловят» лишь **autorun и вирус, который он несет**, но конкретно вирус, что в самой флешке данный софт может и «не заметить». Поэтому после

сканирования флешки таким софтом нам необходимо также проканировать её и вашим антивирусом и, например, Malwarebytes' Anti-Malware (о котором речь пойдет в Разделе 3.0):



Браузер...Какой?

Спросите 10 человек: какой браузер они используют? В ответ вы услышите разные ответы, что тот или иной браузер лучше всех, безопасней всех и быстрее всех....Мнения разные будут! А некоторые просто в поисковике Google наберут ЛУЧШИЙ БРАУЗЕР и им в ответ будет свыше 49 000 000 ответов и вы их перечитаете и еще больше запутаетесь. Раньше лично я использовал Internet Explorer - остался недоволен,т.к. постоянные зависания и «быстродействие» его уж сильно раздражали...к тому же, как оказалось большинство хакеров (если рассматривать в глобальном масштабе) нацелены на поиск его уязвимостей, чтобы, используя их, с легкостью использовать свои инструменты,т.е. проникнуть в вашу систему. Поэтому мой выбор пал на **Mozilla Firefox.**

Хочу заметить, что на момент написания статьи у меня была версия 3.6 браузера Mozilla Firefox, но поскольку мне лично версия 4.0

внешне не понравилась, я всё-равно затрону внутренние настройки 3.6 надеясь, что они индиетичны с настройками версии 4.0.

Почему Mozilla Firefox ?

Он быстрее, более динамичен, но наиболее его плюсом является плагины (или же аддоны), благодаря которым мы можем данный браузер настроить под себя. Расписывать можно много,но перейдем сразу к делу и по ходу описаний вы поймёте, почему именно Mozilla Firefox может удовлетворить наши потребности с точки зрения вирусной безопасности.

Да,безусловно, Internet Explorer нам может быть полезен, но только для того, чтобы скачать Mozilla Firefox... :)

Переходим на официальный сайт Mozilla Firefox - http://www.mozilla.com/ru/firefox/ и скачиваем для своей операционной системы. Далее скачиваем ВСЕ плагины здесь - https://addons.mozilla.org/ru/firefox/browse/type:7 (это для нормального отображения страниц Интернета), в необходимые плагины входят:

- Adobe Reader
- Adobe Flash Player
- Java
- QuickTime
- RealPlayer
- Shockwave
- Windows Media Player.

Итак, установив необходимые плагины, нам необходимо перенести старые закладки любимых сайтов из старого браузера. Для этого после установки Mozilla Firefox вверху слева смотрим **Файл** далее **Импорт** и там выбираем браузер, из которого нужно импортировать

(к сожалению это применимо к Internet Explorer и Opera). После этого наши любимые старые закладки будут здесь: **Закладки – Из Internet Explorer.**

Теперь всё готово!..Можно использовать браузер.....Хм...а нееет!!! Еще рано радоваться! Нам нужно максимум «выжать» из браузера с точки зрения безопасности.

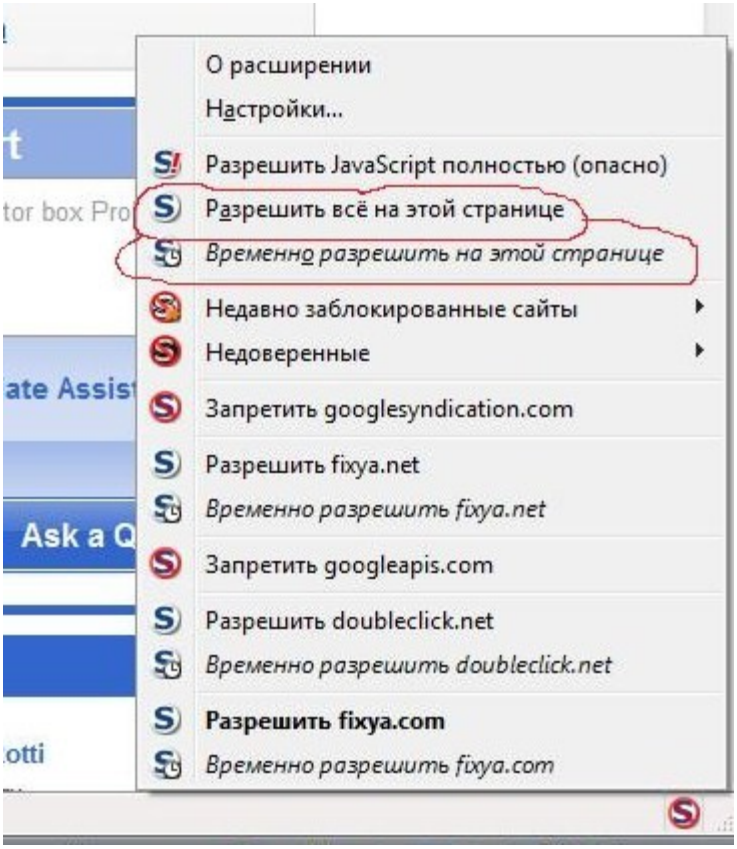
Все аддоны (плагины) касательно безопасности можно найти здесь - https://addons.mozilla.org/ru/firefox/search/?q=&cat=1%2C12 Согласитесь, есть где разогнаться! Глаза разбегаются, ведь их там сотни! Но нам нужно основное, я советую установить следующие дополнительные плагины, а остальное, если на то воля ваша, смотрите сами, что вам еще устанавливать по мере ваших желаний. И хочу добавить, что все плагины от сторонних производителей, что очень даже немаловажно! Итак, что еще необходимо:

- Adblock Plus - блокирует ненужную рекламу, что позволяет быстрее загружать странички. После утановки в правом верхнем углу появится красный значек ABP. Если вам что-то не видно на сайте (напр. фото заблокировал),то достаточно кликнуть на красный значек ABP (верхний правый угол) и выбрать Открыть список элементов и выбрав, что нужно открыть, в появившемся окне кликаем правой кнопкой на мышке и выбираем Открыть в новой вкладке:

https://addons.mozilla.org/ru/firefox/addon/adblock-plus/

- NoScript - блокирует исполнение JavaScript, апплетов Java, Flash и и других потенциально опасных компонент HTML-страниц до тех пор, пока пользователь не разрешит их исполнение на данном узле или глобально,а также защищает пользователя от XSS атак. Очень нужный плагин! После установки в браузере в нижнем правм углу появится голубая буква **S** – наведите просто мышку на него и панель управления откроется. Если вы зашли на сайт и вы в нём уверенны (для уверенности используем WOT

(см.ниже)), но некоторые компоненты странички не работают или сам сайт оповещает, что для нормальной работы нужно включить JavaScript , то достаточно в меню выбрать Разрешить всё на этой странице (это будет работать на постоянной основе) или же Временно разрешить на этой странице (временно разрешаются скрипты):



Приведу небольшой пример: вы зашли на сайт, «покопались» в нём и вышли. На следующий день у вас стали появляться всплывающие окна в браузере или более тяжелый случай – блокировка браузера, а то и рабочего стола. Это означает,что хакер взломал данный сайт и разместил вредоносный скрипт, который, используя уязвимости вашего браузера, с легкостью загрузился на ваш компьютер (XSS атака – это называется). Но если мы установили NoScript , то с высокой степенью вероятности этого бы не произошло. Данный плагин вас уведомил бы (в верхней части браузера), что с данного сайта осуществляется XSS атака и заблокировал бы это:

https://addons.mozilla.org/ru/firefox/addon/noscript/

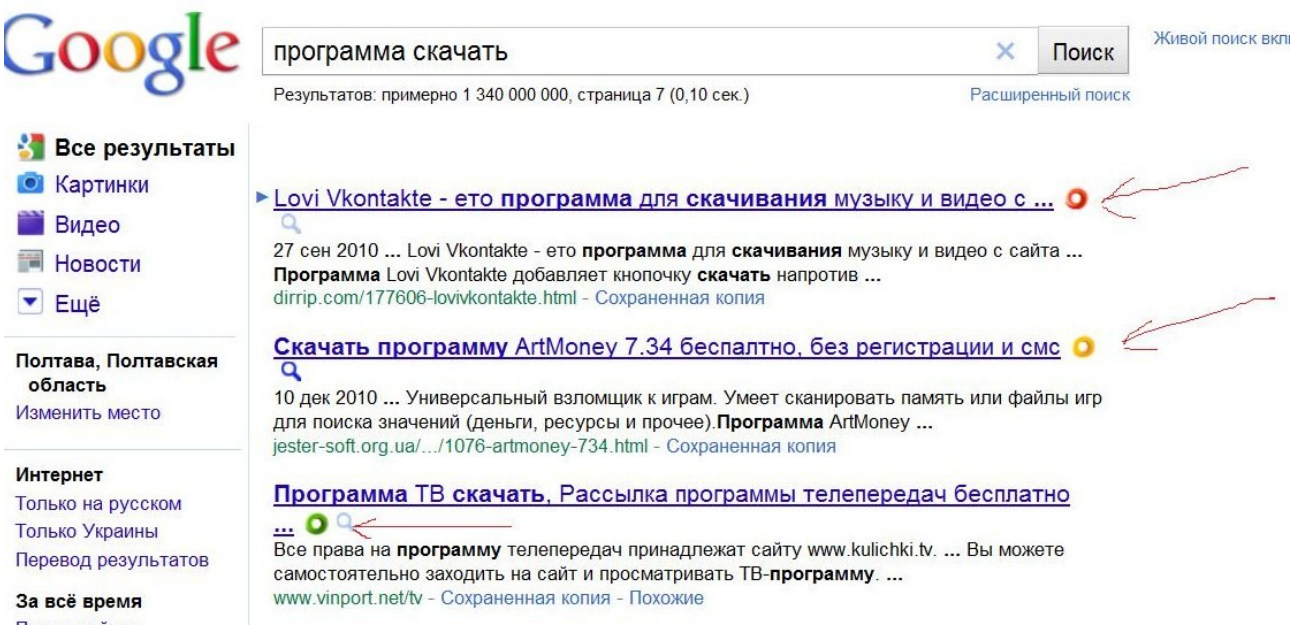
- WOT – плагин вам покажет насколько опасным является тот или иной сайт. Само понятие «опасный сайт» индексируется по многим понятиям, например, сайт распространяет вирусы, мошеннический сайт.....иначе говоря:

  1.Можно ли доверять? ; 2. Надежность продавца; 3.Конфиденциальность; 4.Безопасность для детей.

  Установите плагин WOT и сразу же слева от адресной строки вы увидите круг, который может иметь несколько цветов. Цвет круга зависит от надежности сайта, также эти кружки появляются в поисковике Google.

  Что означает цвет круга?

Значки рейтинга, похожие на светофор, понятны на интуитивном уровне: зеленый свет – «идите», желтый – «будьте осторожны», красный – «стойте»:



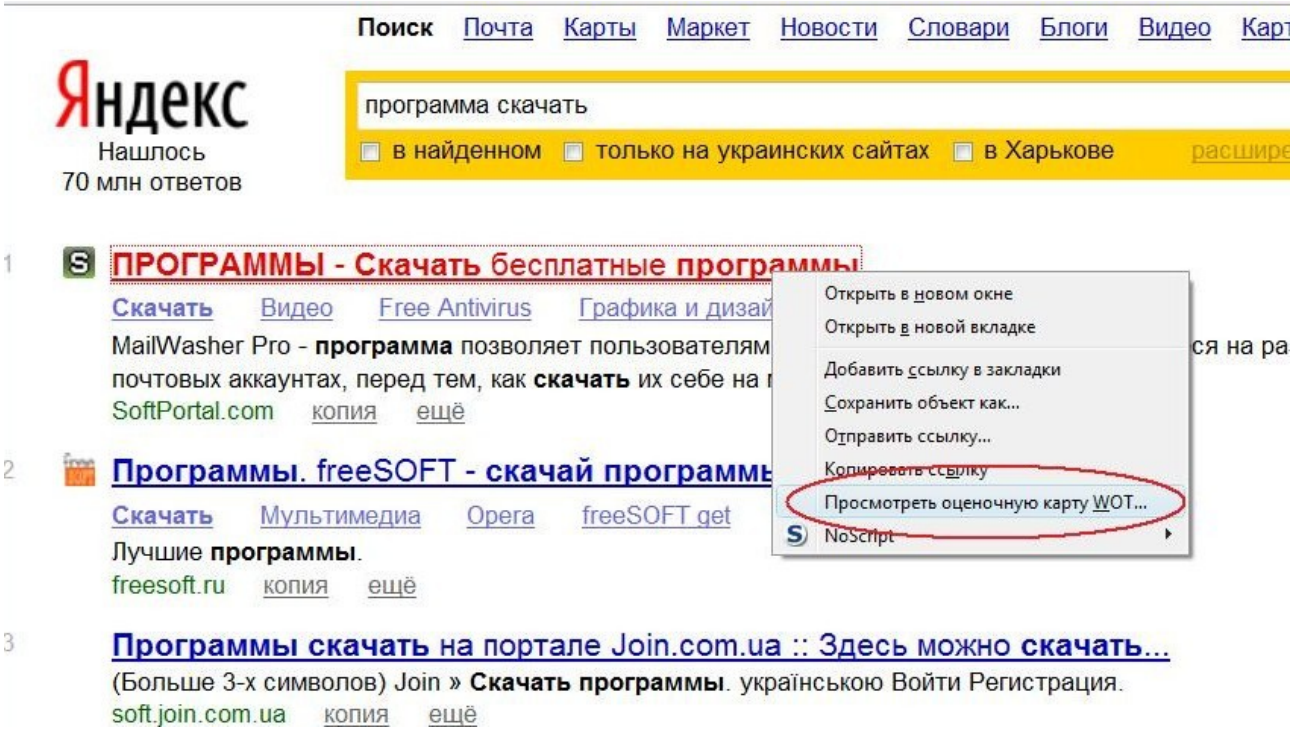
Т.е. мы, как «виртуальные пешеходы», должны идти на зеленый цвет, который может быть светло-зеленым - оценка «Хорошо», и темно-зеленым – оценка «Превосходно». Кроме того данный плагин дает нам красный цвет на фишинговые сайты, фальшивые интернет-

магазины и сайты, которые имеют плохую репутацию....И обратно - зеленый цвет на сайты с положительной репутацией. Это нас оградит от «развода» со стороны мошенников.

Если кружок бесцветный, то этот сайт, скорей всего, новый и на него нет еще рейтингов.Но подобным сайтам я бы не доверял!

Кроме того мы можем читать отзывы об определённом сайте: если в поисковике Google – кликаем на кружок и читаем (можем и свой отзыв оставить), а если загрузили сайт – слева от адресной строки браузера кликаем на кружок и выбираем Просмотр подробных данных о рейтингах.

***Следует заметить, что НЕ все поисковики поддержуют WOT, т.е. при поиске не выводятся кружки по рейтингам. Это всё решается: нашли в поисковике сайт – наводим курсор на название – кликаем правой кнопкой мышки – в меню выбираем Посмотреть оценочную карту WOT. Например, как на рисунке:

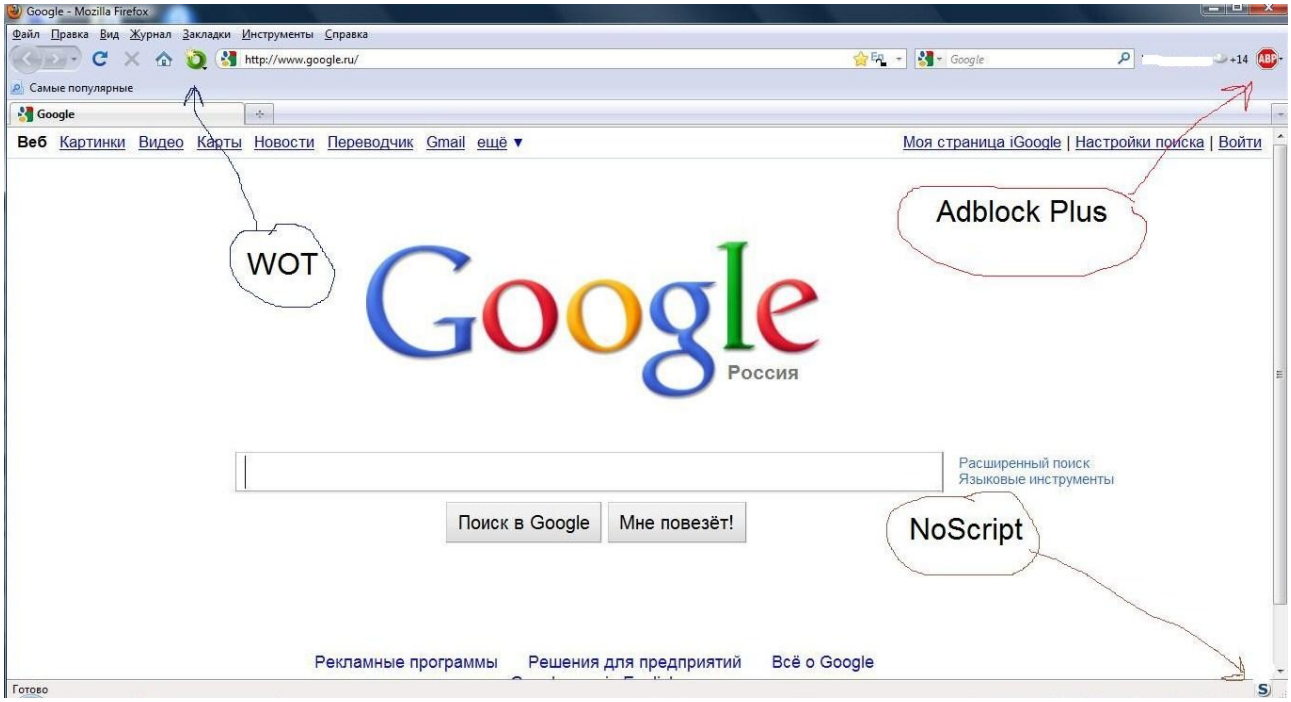


https://addons.mozilla.org/ru/firefox/addon/wot-safe-browsing-tool/

- Другое - https://addons.mozilla.org/ru/firefox/search/?q=&cat=1%2C12

  Тут вы уже сами смотрите по вашим потребностям и нуждам!

Чтобы взглянуть местоположение вышеуказанных плагинов смотрим ниже рисунок:



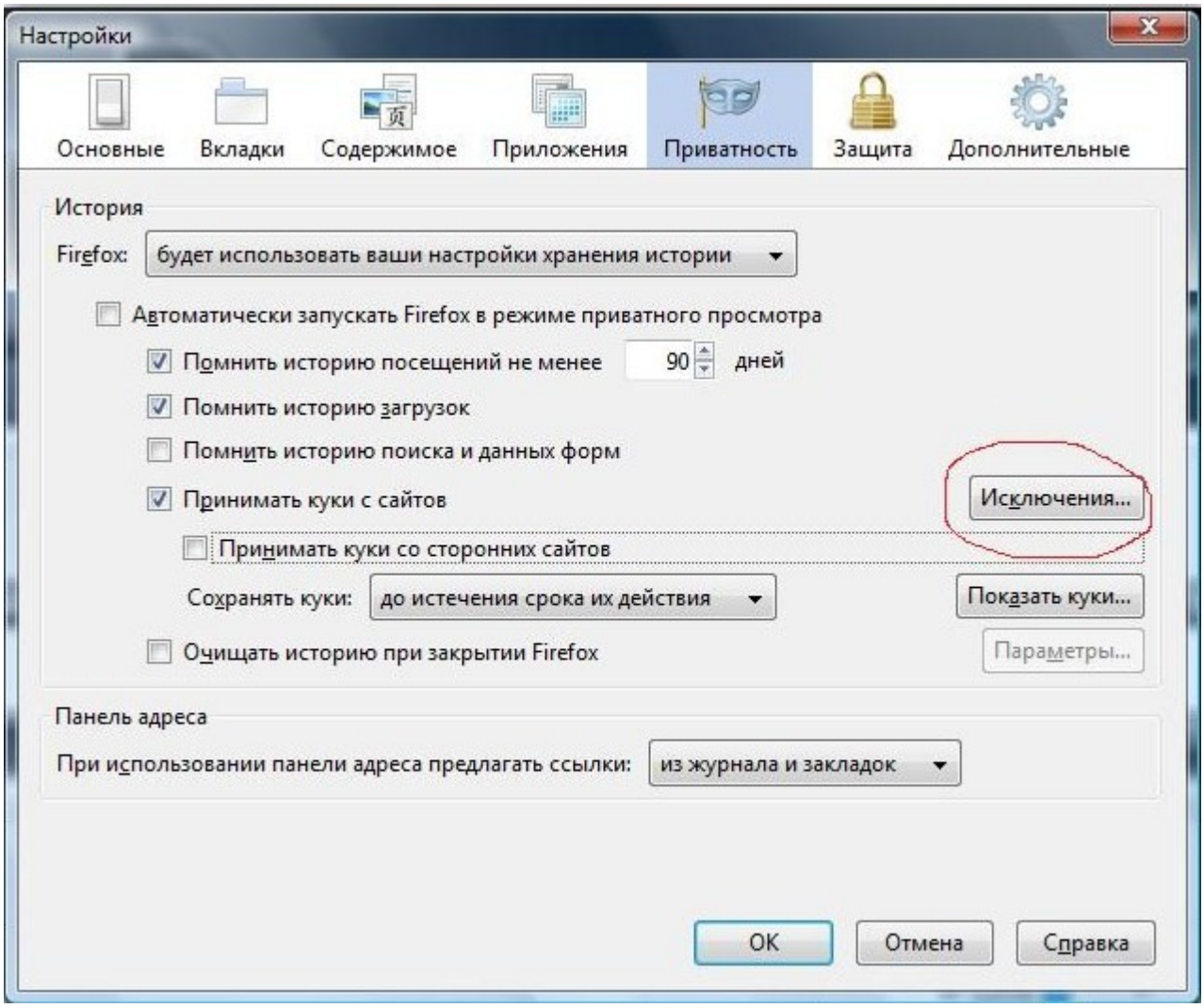
Это мы рассмотрели плагиновые методы защиты Mozilla Firefox. Теперь рассмотрим **внутренние настройки**:

Инструменты – Настройки – Приватность: тут если желаете можно выставить так, что бы куки не сохранялись, не принимались, не регестрировалась история загрузок. Куки — это простые текстовые данные, и они не могут выполнять какие-либо действия самостоятельно. В частности, куки не могут быть ни вирусами, ни шпионскими программами. Но тут есть одно НО - если ваши куки попадут к хакеру (не важно каким путем – дистанционно или физическим доступом), то это есть для вас не хорошо... Куки могут быть,например,украдены с помощью анализа трафика — это называется взломом сессии. Сетевой трафик может быть перехвачен и прочитан не только его отправителем и получателем (особенно в

публичных сетях Wi-Fi). Этот трафик включает в себя и куки, передаваемые через незашифрованные HTTP-сессии. Там, где сетевой трафик не шифруется, злоумышленники могут прочесть сообщения пользователей сети, в том числе их куки, используя программы, называемые сниферами.....Вобщем примеров масса можно привести.... Более подробно о куках и методах использования хакером ваших кук смотрим здесь - http://ru.wikipedia.org/wiki/HTTP_cookie

Но очевидно одно, что при ежедневном посещении сайтов, где нужно вводить логин и пароль, то придется каждый раз вводить логин/пароль заново – это при «выключенных» куках. Если куки «включены», т.е. стоит сохранение кук, то вводить каждый раз не нужно их, например, Вконтакте, Одноклассники и т.д.

Так что смотрите сами, что делать в этом разделе: **Инструменты – Настройки – Приватность.** Но ведущие специалисты всё-таки советуют куки не сохранять и не принимать! Также можете сохранить исключения по приёму кук лишь тех сайтов, которым доверяете (Вконтакте и т.п.):



Инструменты – Настройки – Защита : ставим галочки на следующих позициях –

1. Предупреждать при попытке веб-сайтов установить дополнения;
2. Блокировать сайты, подозреваемые в атаках;
3. Блокировать сайты, подозреваемые в мошенничестве.

Инструменты – Настройки – Дополнительное - Обновления: тут ставим везде галочки, кроме Предоставлять выбор действия пользователю . Не стоит пугаться – это касается только Дополнений и Плагинов, а также автообновления Mozilla Firefox, т.е. у вас всегда будет последняя версия браузера. Кроме того не будут постоянные

запросы – Устанавливать или нет? – касательно обновлений браузера.

Инструменты – Настройки – Дополнительное – Шифрование: тут галочки должны стоять на обоих протоколах (их там всего два), а также Когда сервер запрашивает мой личный сертификат галочка должна стоять на Запрашивать каждый раз.

Инструменты – Настройки – Содержимое : удостоверьтесь, что галочка стоит на Блокировать всплывающие окна.

Всё остальное на ваше усмотрение....Впринципе браузер Mozilla Firefox готов к использованию. Вполне возможно, что большинство вышеуказаных настроек уже установлены по умолчанию, но проверить всё же стоит.

... или Google Chrome ?

Да, пользователи есть разные и кого-то может Mozilla Firefox может не устраивать, или дизайн не нравится, или медленно грузится (хотя это не так), или просто он не может покинуть свой любимый браузер Google Chrome. Это дело лично каждого, его выбор. Я свой выбор уже описал. Многие полюбили браузер Google Chrome...спорить не стану. И поэтому хочу посоветовать некие расширения для него касательно всё той же безопасности. Впринципе, что для Mozilla Firefox и Google Chrome аддоны (расширения) во многом одинаковы.

Для начала скачайте с официального сайта браузер - http://www.google.com/chrome/?hl=ru

Если есть вопросы или что-то не получается, сюда - http://www.google.com/support/chrome/?hl=ru

Расширения для Google Chrome , советую:

- AdBlock - Блокирует рекламу по всему Интернету. https://chrome.google.com/extensions/detail/gighmmpiobklfepjocnamgkkbiglidom
- или же Adblock Plus for Google Chrome™ (Beta) – Блокирует рекламу с помощью фильтра, основанного на Firefox Adblock Plus. https://chrome.google.com/extensions/detail/cfhdojbkjhnklbpkdaibdccddilifddb
- WOT - аналог плагина Mozilla Firefox - https://chrome.google.com/extensions/detail/bhmmomiinigofkjcapegjjndpbikblnp
- KB SSL Enforcer - если к определенным сайтам или предлагают услуги слой Secure Sockets Логин или доступ вариант, KB SSL Enforcer автоматически выберет, что HTTPS: / / URL. Дней после начала использования излишне незашифрованном виде веб-адреса закончились. https://chrome.google.com/extensions/detail/flcpelgcagfhfoegekianiofphddckof?hl=ru
- NoScript - расширение для контроля JavaScript'ами, например зашита от XSS, как и в Mozilla Firefox: https://chrome.google.com/extensions/detail/odjhifogjcknibkahlpidmdajjpkkcfn?hl=en
- Better Pop Up Blocker - расширение для блокировки всплывающих окон: https://chrome.google.com/extensions/detail/nmpeeekfhbmikbdhlpjbfmnpgcbeggic?hl=en
- Proxy Switchy! - позволяет быстро и удобно переключатся между прокси-серверами. Прокси-сервер позволяет нам находится в сети анонимно, а значит наш IP и другие данные о нашем компьютере будут идти с подменой.

Зачем это нужно?

Если хакер имеет наш IP, то он может сканировать наши порты на открытость, что будет если порты открыты – я писал выше. Это как один из вариантов. https://chrome.google.com/extensions/detail/caehdcpeofiiigpdhbabniblemipncjj

- Flashblock - расширение блокирует загрузку ВСЕХ флеш-роликов с веб-страниц, оставляя вместо них пустую рамку с кнопкой. Щелкнув мышью по этой кнопке вы можете просмотреть данный флеш-ролик. Быстрее загружается страничка: https://chrome.google.com/extensions/detail/gofhjkjmkpinhpoiabjplobcaignabnl

- PasswordFail Extension - для уменьшения дополнительной параноидальности для вас было создано расширение PasswordFail Chrome предупреждающее вас с любого веб-сайта, на которых хранятся или отправляются логин/пароль в открытом виде. В общем, если один из этих сайтов взломан, ваш неприкрытый пароль открыт в базе данных, готов быть судимым на все ваши другие счета в режиме онлайн. PasswordFail дает вам знать, если ваш пароль взломан или является мишенью веб-сайтов: https://chrome.google.com/extensions/detail/ockgeenjbijlgilppfieaklfopnbdpge?hl=ru

- Credit Card Nanny - это расширение Chrome, которое отвечает за сохранность правильного направления ваших кредитных счетов, а точнее безопасность ввода номера кредитной карточки и секретного номера карты, который находится на обратной стороне кредитной карточки владельца. На сегодняшний день существует много услуг в Интернете, позволяющих получить их с помощью кредитки,

поэтому наличие расширения защиты Credit Card Nanny просто обязательно в вашем браузере GoogleChrome. Для Интернет воров не составит труда украсть ваш пин и номер кредитной карты в отсутствии именно этого расширения, поэтому если вы оплачиваете услуги в Интернете задумайтесь и незамедлительно установите себе одно из самых надёжных расширений современности CreditCardNanny: https://chrome.google.com/extensions/detail/lfmmjpapolbaaddobpnlcjkgchmhhoog?hl=ru

Пожалуй этого хватит вам для Google Chrome, есть из чего выбрать. Все остальные внутренние настройки (стандартные) вполне удовлетворяют нашим потребностям, касающимся безопасности.

Антивирус

Это, пожалуй, самый проблемный и наболевший вопрос – какой выбрать антивирус?

Опять же, кого не спроси – все будут советовать то, что у него стоит на компьютере из антивирусов. Кто-то скажет что NOD32 лучше всех, а для кого-то Бог и царь Avast, который, кстати, очень популярен в Европе....Мнений ровно столько же,сколько и людей и антивирусов...

Но давайте для начала определимся – что мы хотим получить от антивируса?...хм...понятное дело – защиту от вирусов! А если взглянуть глубже, немного познакомиться, то мы узнаем и обратную сторону медали, что тот или иной антивирус имеет свои плюсы, но и не лишен и недостатков.

Давайте откроем поисковик Google и наберем ЛУЧШИЙ АНТИВИРУС... из несколько попавшихся вам сайтов сразу станет понятно, что **Антивирус Касперского** есть лидером! Пожалуй, с этим можно согласиться. Но как бывает в жизни всё хорошее стоит денег....И Антивирус Касперского, к нашему сожалению, не есть исключение. Безусловно, можно его купить (Лицензию) и радоваться жизни, но не у всех есть деньги, что бы еще тратиться и на антивирус... Это первый недостаток его – платность.

Идем дальше в корень проблемы Антивируса Касперского.... Вы скажете, что можно найти ключи в интернете! Это разумно, но вам нужно будет помучаться, потому что если вы найдете ключи не факт, что они вам прослужат долго...Потому как специалисты Касперского также следят за «разгулом» ключей в интернете и потихоньку их «банят» и вам снова приходится искать ключи, «перекапывать» интернет и т.п. Это второй недостаток – проблемы с поиском ключей. Однако ключи можно поискать, например, здесь: https://hacker-pro.net/showthread.php?t=13728

Хорошая защита требует хороших ресурсов – в случае с Касперским. Многие жаловались, что после установки Антивируса Касперского у них начинались «подтормаживания» системы, медленее стал работать компьютер. Как оказалось для работы Касперского нужны объемные ресурсы вашего компьютера! Отсюда следует, что у «пострадавших» от данного антивируса была «слабенькая» конфигурация компьютера, т.е. маломощный процессор, «слабая» видеокарта и т.д. Отсюда вытекает третий недостаток – требовательность к ресурсам.

Однако, если у вас комьютер достаточно современный с более-менее «мощной» конфигурацией, то Антивирус Касперского его не станет «тормозить» и будет нормально работать компьютер без «глюков».

Безусловно, Антивирус Касперского, а также Kaspersky Internet Security или Kaspersky CRYSTAL заслуживают наивысшую оценку и

внимание пользователей! Если у вас современный компьютер и есть возможность приобрести продукт Касперского, то даже не задумываясь приобретайте... и радуйтесь виртуальной жизни!

Официальный сайт - http://www.kaspersky.ru/index.html

Но что делать тем, кто не может позволить себе приобрести за деньги антивирус, а также тем, которые имеют старенькие компьютеры или новые, но со «слабой» конфигурацией?

Предлагаю вам сразу два решения касательно одного антивируса -платный и бесплатный!

Хочу представить вам надежный антивирус - **Avira AntiVir**.

Почему Avira AntiVir ?

Дело в том, что данный антивирус не «грузит» систему, т.е. не требователен к конфигурации компьютера, а значит его можно ставить на старые компьютеры и любые «слабые». Кроме того есть бесплатная версия данного антивируса, а также есть и платная, но у платной версии не так остро стоит вопрос с ключами. Также хочу заметить, что Avira AntiVir будет прекрасно защищать ваш компьютер от хакерских инструментов, что должно быть на первом месте как для антивируса....особенно, когда мы имеем дело с немецким качеством!

Итак, если вы не хотите заморачивать себе голову поисками ключей, но в тоже время хотите практичный, современный и бесплатный антивирус, то ваши потребности вполне удовлетворит **Avira AntiVir Personal** - это надежная бесплатная антивирусная программа, постоянно и быстро защищающая компьютер от такого вредоносного ПО, как вирусы, трояны, Backdoor-программы, мистификаторы, черви, диалеры и т.п. Она контролирует все действия пользователя и

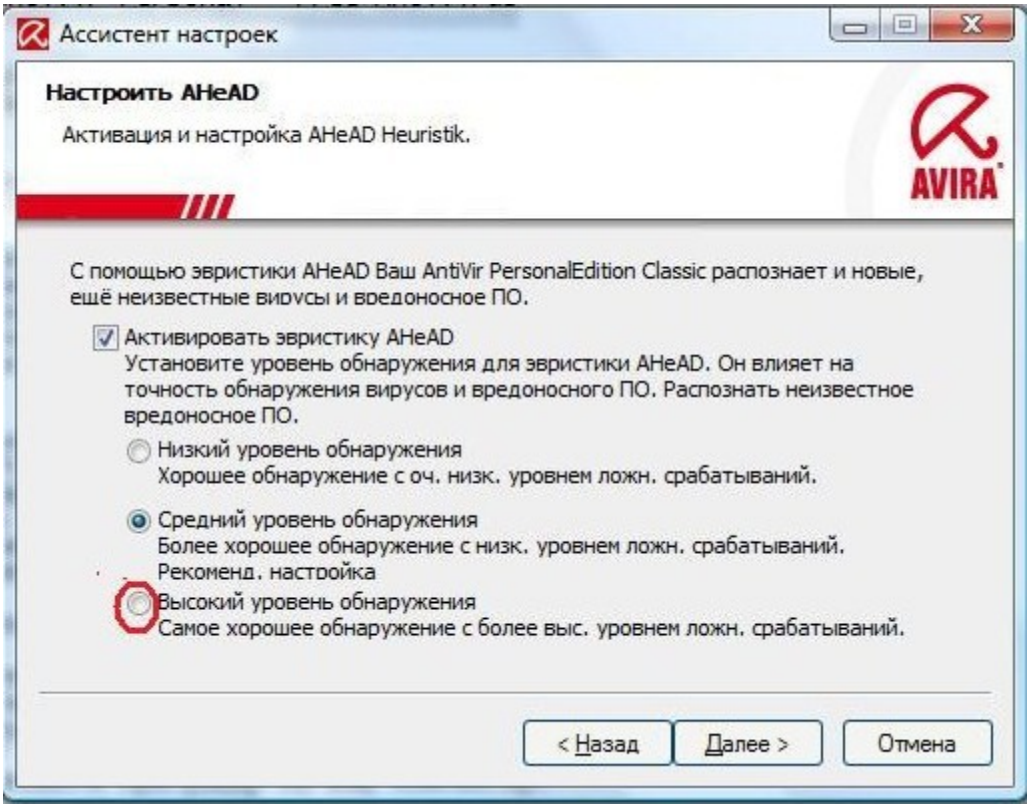
операционной системы и реагирует сразу же после обнаружения вируса. Применение эвристики.

Вобщем из бесплатных антивирусов это самый, пожалуй, надежный из всех!

Получить больше информации, а также скачать Avira AntiVir Personal на русском языке можно здесь - http://soft.oszone.net/program/9563/Avira_AntiVir_Personal_RU/

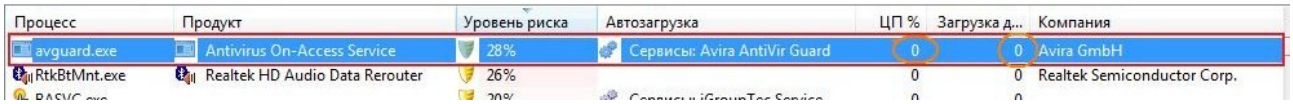
...или здесь: http://www.avira.com/ru/avira-free-antivirus

Немного информации о работе и настройке Avira AntiVir Personal. После скачивания антивируса и запуска его установочного файла в диалоговом окне будут открываться несколько ручных настроек. Впринципе там ничего сложного нет. Единственное, что когда откроется окно с настройками эвристики, то желательно поставить на Высокий уровень обнаружения:

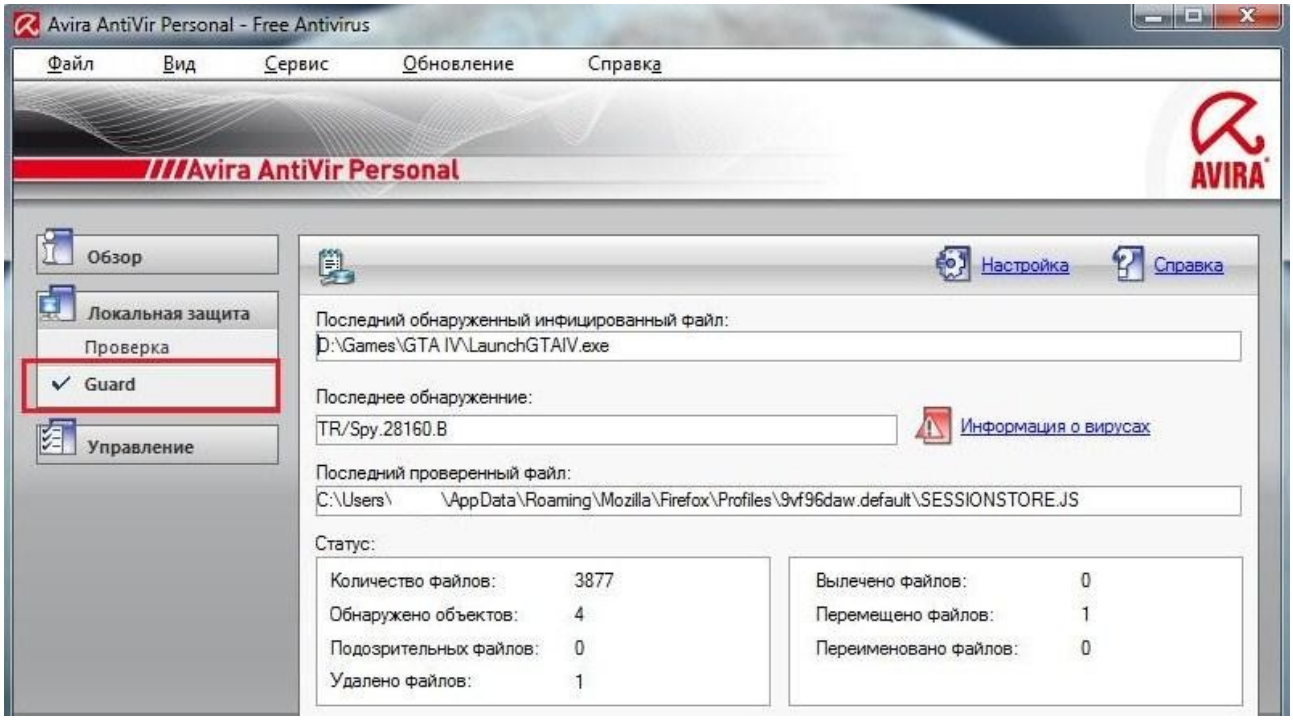


Дальше можно использовать предложенные стандартные настройки при установке.

Убедитесь, что опция AntiVir Guard была включена. Кстати, AntiVir Guard очень даже интересный модуль – он постоянно сканирует систему и при этом практически не загружает работу процессора:



Иными словами AntiVir Guard – это постоянный мониторинг системы на вирусы, при обнаружении которых вы будете уведомлены. За ходом работы AntiVir Guard мы можем наблюдать во вкладке Локальная защита:



Мы рассмотрели бесплатную версию Avira AntiVir. Но если вы хотите чего-то большего по функционалу, то есть и платная версия - **Avira AntiVir Premium.**

Avira AntiVir Premium обеспечивает профессиональную защиту от вирусов, червей, троянов, рекламных программ, шпионского ПО и фишинга. Разница между платной (Avira AntiVir Premium) и бесплатной (Avira AntiVir Personal) версиями так это то, что у платной имеются дополнительные модули защиты от вирусов, а также обновления идут от отдельного сервера обновлений. Именно за счет

дополнительных модулей Avira AntiVir Premium превосходит Avira AntiVir Personal, такие модули как AntiAd/Spyware (защищает от шпионских и рекламных рассылок), AntiPhishing (защищает от фишинговых атак), AntiRootkit (защищает от скрытого вредоносного ПО), AntiVir ProActiv (распознает неизвестные вирусы по модели поведения), WebGuard (проверяет отсутствие вирусов в загружаемых файлах), AntiDrive-by (предотвращает загрузку вирусов при интернет-серфинге).

Чтобы приобрести Avira AntiVir Premium есть 2 варианта: либо купить её, например, с официального сайта - http://www.avira.com/ru/for-home-avira-antivir-premium или другого источника.....Либо скачать, а затем искать ключи активации на некий период. Мы выберем второй вариант.

Итак, скачиваем Avira AntiVir Premium с оф. сайта или отсюда - http://soft.oszone.net/program/10617/Avira_AntiVir_Premium/

И перед нами стает вопрос - где брать ключи? Ответ будет банальным – в интернете. Ключ реально найти, а если найдете, то их не так жестко «банят», как у Касперского. Ключи на Avira AntiVir Premium можно найти, например, здесь – https://hacker-pro.net/showthread.php?t=11073

https://hacker-pro.net/showthread.php?t=11495

Итак, после сравнения мы видим явные преимущества платной версии (Avira AntiVir Premium) перед бесплатной (Avira AntiVir Personal). Эти преимущества идут за счет дополнительных модулей, о которых я уже написал выше. Однако, большим минусом Premium является платность или же поиск ключей, и некоторых это может напрягать, что нужно искать ключи, которые имеют свойство, как временный фактор, т.е. нет вечного ключа. Ключи есть, как на 1 месяц, так и на 3 месяца...или на 4..5....месяца, но он «закончится» и снова нужно искать ключи. Поэтому по числу скачиваний лидирует Avira AntiVir Personal. Но ведь так хочеться иметь те дополнительные

модули, что в Avira AntiVir Premium... Но если подумать хорошо, то всё-таки выход есть – мы можем скачать бесплатную версию, но в тоже время мы можем иметь и модули с Premium версии, только немного модифицированные....Вы удивлены?!...Этого ведь не может быть?!...А если подумать, то это вполне возможно! Мы можем данные модули заменить другим. Сначала будет написан модуль из Avira AntiVir Premium, а затем – чем его можно заменить:

- AntiAd/Spyware (защищает от шпионских и рекламных рассылок) – легко заменяется программой-антишпионом, о которых я написал темой ниже. К тому же Антишпион куда более функционален и «навороченней» и его всё равно нужно будет ставить.

- AntiPhishing (защищает от фишинговых атак) – Для справки: Фишинг - вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей (логинам и паролям) – поэтому данный модуль в большей мере заменяется плагином WOT на браузер, о котором написано выше в статье о браузерах. Но что самое интересное, так это то, что в Avira AntiVir Personal имеется «Специальная функция автоматически блокирует вредоносное ПО и Фишинг (AntiDrive модуль)».Еще нам может помочь онлайн-мультисканер Urlvoid, который также определяет мошенническо-фишинговые сайты: http://www.urlvoid.com/

- AntiRootkit (защищает от скрытого вредоносного ПО) – а вот этот модуль можно скачать отдельно и сканировать компьютер - ***Avira AntiRootkit Tool*** - http://www.avira.com/ru/support-download-avira-antirootkit-tool К тому же сам производитель пишет об Avira AntiVir Personal: «Защита от руткит-программ позволяет обнаружить ПО, скрыто установленное в системе (Руткит)(только для 32-битн. системы)»

- AntiVir ProActiv (распознает неизвестные вирусы по модели поведения) – это называется эвристикой. Однако, снова в

функциях Avira AntiVir Personal прописано: «Расширенный эвристический модуль позволяет выявлять и обезвреживать». К тому же фаервол тут будет, как раз кстати, надежной защитой по неизвестным активностям в эвристике.

- WebGuard (проверяет отсутствие вирусов в загружаемых файлах) – вам никто не мешает скачать файл и вручную просканировать его антивирусом: выделяем файл полученный – клик правой кнопкой мыки – выбираем сканирование нашего файла. Этот модуль просто делает всё автоматически. Просто мы должны себе взять за правило – сканировать загружаемые (полученные) файлы антивирусом. К тому же в Avira AntiVir Personal в функциях имеется: «Распознавание всех популярных типов архивов, включая вложенные, с применением списков опасных расширений файлов» - это как дополнение.
- AntiDrive-by (предотвращает загрузку вирусов при интернет-серфинге) – сам производитель утверждает, что Avira AntiVir Personal встроен «Специальный модуль WebGuard проверяет Интернет-трафик (HTTP) на наличие вирусов и вредоносных программ», а также «Специальная функция автоматически блокирует вредоносное ПО и Фишинг (AntiDrive модуль)»... Также при серфинге в интернете вирус может «просочиться» посредством скриптов, а скрипты мы контролируем плагином NoScript на браузере, о котором я упоминал в книге несколько раз. Также в этом плане поможет AnVir Task Manager (см.тему ниже) – бывает так, что зашел на какой-либо сайт и AnVir Task Manager вас сразу уведомляет, что какой-то процесс хочет прописаться в Автозагрузке – это вирус, при условии если вам неизвестен данный процесс и вы ничего на данный момент не устанавливаете что-либо из ПО. И наконец, фаервол также контролирует любую активность, как «снаружи», так и «внутри» системы.

Кому интересно знать о всех функциях Avira AntiVir Personal - http://www.avirus.ru/content/view/30/67/

Как видим, мы можем установить Avira AntiVir Personal, которая бесплатна и не требует ключей... и в тоже время имеет возможность модифицированного функционала от Avira AntiVir Premium, что не может нас привлекать. Так что выводы делайте сами...

Также существует **AntiVir Premium Security Suite** - пакет безопасности, отличается от Premium тем, что были добавлены персональный Firewall, анти-спам, родительский контроль (блокировка сайтов, нежелательных для просмотра детьми), игровой режим. Однако хочу заметить, что Firewal AntiVir не очень надежный и практичный. У AntiVir отменный антивирус. Поэтому не советую использовать AntiVir Premium Security Suite именно из-за фаервола. Нам самое главное вынести для себя – это только антивирус!

Антишпионы...Нужны ли они?

К антишпионам относятся программы для поиска программ-шпионов (spyware), рекламных вставок (adware), программ - похитителей данных (hijackers) и прочего вредоносного ПО.

Для справки:

Spyware (**шпионское программное обеспечение**) — программа, которая скрытным образом устанавливается на компьютер с целью сбора информации о конфигурации компьютера, пользователе, пользовательской активности без согласия последнего. Также могут производить другие действия: изменение настроек, установка программ без ведома пользователя, перенаправление действий пользователя.

Adware — программное обеспечение, содержащее рекламу,т.е. вид программного обеспечения,при использовании которого пользователю принудительно показывается реклама.

О другом шпионском ПО, кому интересно, здесь – http://z-oleg.com/secur/articles/spyware.php

Но вы можете утверждать, что и антивируса хватит! Однако, ничего не может быть совершенным (я про антивирус) и как показывает практика антивирусам свойственно «пропускать» программы-шпионы: кто-то больше, кто-то меньше....Поэтому нам просто необходима программа узкоспециализированно-заточенная под данный инструмент хакера. Эти программы совершенно не конфликтуют с антивирусами.

Представляю вашему вниманию **TOP-4** самых лучших антишпионов:

1. **Spybot Search&Destroy - программа для поиска программ-шпионов (spyware), рекламных вставок (adware), программ - похитителей данных (hijackers) и прочего вредоносного ПО, а также удаление программ записи нажатий на клавиши (keylogger). Spybot - Search & Destroy сканирует жёсткий диск и реестр операционной системы, выявляя тем самым шпионские модули и вредоносные ключи. База данных программы постоянно обновляется разработчиками, её обновление происходит из соответствующего раздела, аналогично обновлению антивируса. Интерфейс прост и понятен: кнопок и управляющих меню - минимум, работать с программой не составляет труда. Перед проверкой системы на наличие в ней шпионских модулей рекомендуется сделать копию реестра. В программе также предусмотрен откат, т.е. вы всегда можете вернуть ключи и файлы, которые были удалены (если, конечно, вы их не удалили безвозвратно). Несмотря на свою бесплатность, эта программа является одним из признанных лидеров в своём классе и я с этим, пожалуй, соглашусь:**
   http://soft.oszone.net/program/3813/Spybot_Search_and_Destroy/
2. **Ad-Aware -** программа для поиска и удаления шпионских модулей и других вредоносных приложений. Ad-Aware позволяет сканировать оперативную память компьютера и файлы жёсткого диска для определения в них шпионских

модулей. Кроме того, программа может проверять реестр операционной системы, удаляя из него все записи, оставленные вредоносными программами. Работает Ad-Aware достаточно быстро, настройки просты и интуитивно понятны: http://soft.oszone.net/program/3732/AdAware/

3. **Spyware Terminator -** программа для защиты компьютера от различных вредных модулей - spyware, adware, кейлоггеров и других троянов. Имеет резидентный монитор, который в реальном времени проводит мониторинг системы и предотвращает попытки проникновения на компьютер вредоносного ПО. Имеющийся в программе сканер поможет отыскать и поместить в "каратин" или удалить уже внедренные объекты. Кроме этого, в программу включен модуль защиты от вирусов (ClamAV):

   http://soft.oszone.net/program/4143/Spyware_Terminator/

4. **SuperAntiSpyware Free -** программа для обнаружения и удаления шпионских, рекламных и вредоносных программ, червей, руткитов, паразитов и другого подозрительного софта:

   http://biblprog.org.ua/ru/superantispyware/

Хочу заметить, что все вышеперечисленные программы есть БЕСПЛАТНЫМИ, а также все на русском языке, за исключением Ad-Aware (но и без русского языка,полагаю, разберетесь).

Ставить антишпион **нужно**, и при том один, а не два...три...чтобы избежать конфликта между ними!

ВНИМАНИЕ! Сканировать антишпионом рекомендуется 1 раз в месяц для профилактики вирусов, шпионов, кейлоггеров и других инструментов хакера! Но если грызет параноя, то сколько угодно раз в месяц:)

Но в данном TOP-4 есть и свой лидер! Судя по отзывам, рейтингам и сравнительном тестировании среди антишпионов лучшим из лучших является Spybot Search&Destroy. Так что выводы делайте сами.

Если где-то затрудняетесь в установке или использовании Spybot Search&Destroy, то вот вам инструкция - http://blogs.mail.ru/bk/ste69/2AC8CCAA6BDFD4DD.html

AnVir Task Manager – контроль над процессами!

Нам необходима также программа, которая будет делать мониторинг Автозагрузки и Процессов. Если вы у себя откроете Автозагрузку программ при включении Windows, то вы увидите просто набор программ и вам это ни о чем не скажет с точки зрения безопасности...также это касается и Процессов...Нам нужна программа, которая «скажет» - опасные ли это процессы?!

Поэтому настоятельно рекомендую и советую программу AnVir Task Manager - менеджер процессов и программ автозагрузки с функциями анти-трояна, antispyware и анти-вируса. Иными словами данная программа дает возможность удалить с зараженного компьютера вирусные и вредоносные программы: троянские кони (трояны), хакерские утилиты, spyware, рекламу (adware) и вирусы, скрыто работающие на компьютере. Также дает ускорение загрузки Windows и работы компьютера. Как её использовать и что она нам дает – читаем далее...

Вобщем настоятельно советую!

Для начала заходим на официальный сайт - http://www.anvir.net/

Читаем про функциональные возможности программы AnVir Task Manager и понимаем, что это действительно шикарный софт:)

Далее смотрим на сайте **Обучающий ролик**... и скачиваем программу (кликаем на СКАЧАТЬ БЕСПЛАТНО). При установке программа запросит, чтобы в системном трее появились иконки, которые мониторят:

1. Использование процессора (со списком наиболее активных процессов)

2. Температуру и загрузку жестких дисков (со списком наиболее активных процессов)

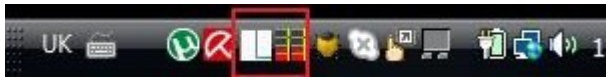
3. Сетевой трафик

4. Аккумулятор ноутбука

5. Память.

На мой взгляд, чтобы не «захламлять» трей нам хватит пунктов 1 и 5, а вообще смотрите сами по вашим потребностям. Далее при установке поставьте галочку, чтобы данная программа загружалась в Автозагрузке. Также при установке «выплывет» программа Reg Organizer - пока что мы её закрываем и никаких манипуляций с ней не предпринимаем. Дальше в книге я расскажу, как её активировать и зачем она нужна нам. Иными словами нам сначала надо разобраться с AnVir Task Manager.

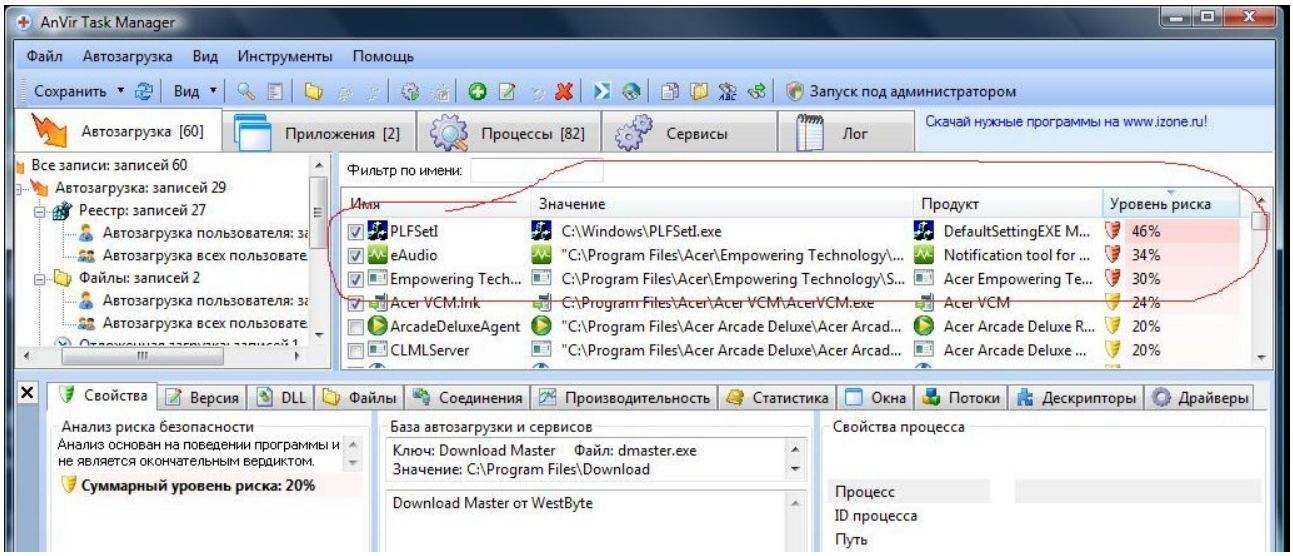
Итак, мы установили AnVir Task Manager, в трее появились 2 иконки (смотря сколько вы захотели при установке):



Кликаем по любой иконке, открылась программа. Вверху мы видим вкладки: Автозагрузка, Приложения, Процессы, Сервисы, Лог.

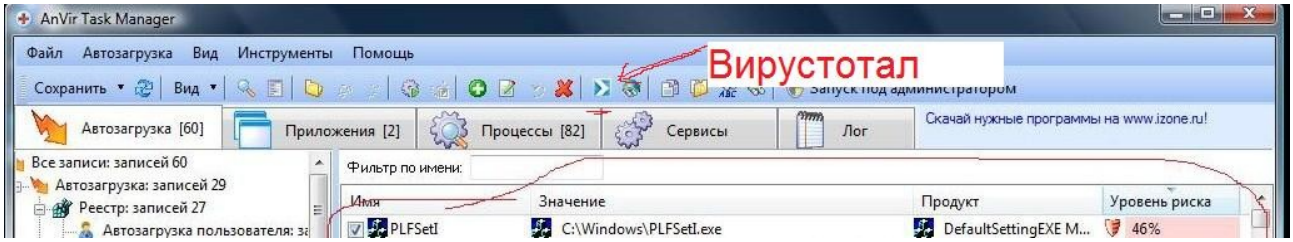
Кликаем на вкладку Автозагрузка. Видим, что в самом верху некоторые процессы(программы) выделены красным цветом, некоторые менее красным, далее желтым и зеленым. Интуитивно

понятно становится, что красным цветом выделены наиболее **опасные программы (Уровень риска в %)**, которые могут быть вирусами и прочими инструментами хакера:

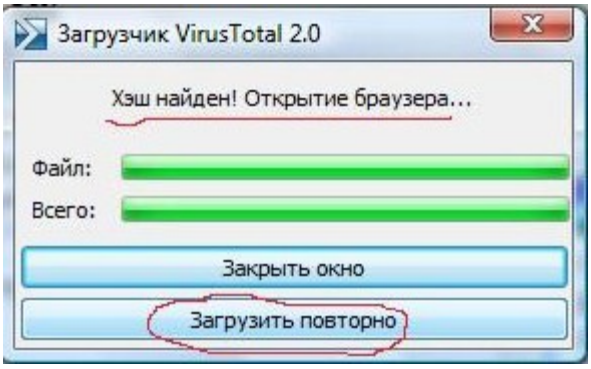


Как проверить на вирусы процесс (программу) в AnVir Task Manager?

Для этого выделяем мышкой «красный» процесс – кликаем правой кнопкой мышки – выбираем Проверить на сайте.....или еще проще: выделяем процесс и кликаем в шапке программы на значек Вирустотала:



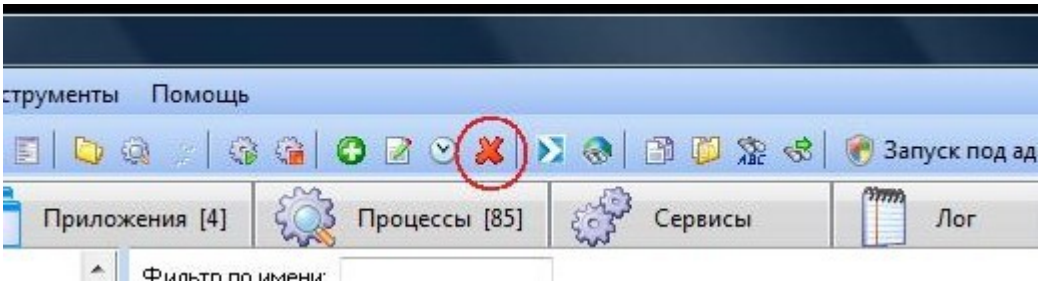
Далее по хешу находится этот процесс, который когда-то был загружен на Virustotal, но нас это не касается. Мы по окошку всплывшему Загрузчик Virustotal 2.0 кликаем на Загрузить повторно:



Этот процесс заново загружается на Вирустоал и вы получаете уже ваш результат – вирус это или не вирус. Если НЕ вирус – проходим мимо и удостоверьтесь нужен ли этот процесс вашему ПК...если не знаете нужен ли – то не трогайте! А если этот процесс действительно лишний, то он нам не нужен, т.к. он (они) грузит систему, что медлит его работу. А медленный компьютер нам нужен?

Хочу заметить, что если вы не можете посредством Загрузчика Virustotal 2.0 загрузить на Вирустотал тот или иной процесс (файл), то знайте, что что-то блокирует, а именно с уверенностью можно сказать, что это «проделки» вируса. Тогда читайте Раздел 3.0.

Если Вирустотал показал, что это вирус, то внизу программы во вкладке Свойства узнаёте где хранится исполнительный файл или же можно узнать где находится – просто наведите мышку на опасный файл. Например, файл находится: C:\Windows\ertyx.exe и мы находим этот файл ertyx.exe и удаляем. Есть и другой способ, более удобный - в верху программы AnVir Task Manager вы увидите красный крестик в виде **X –** это удаление выделенного файла и процесса:



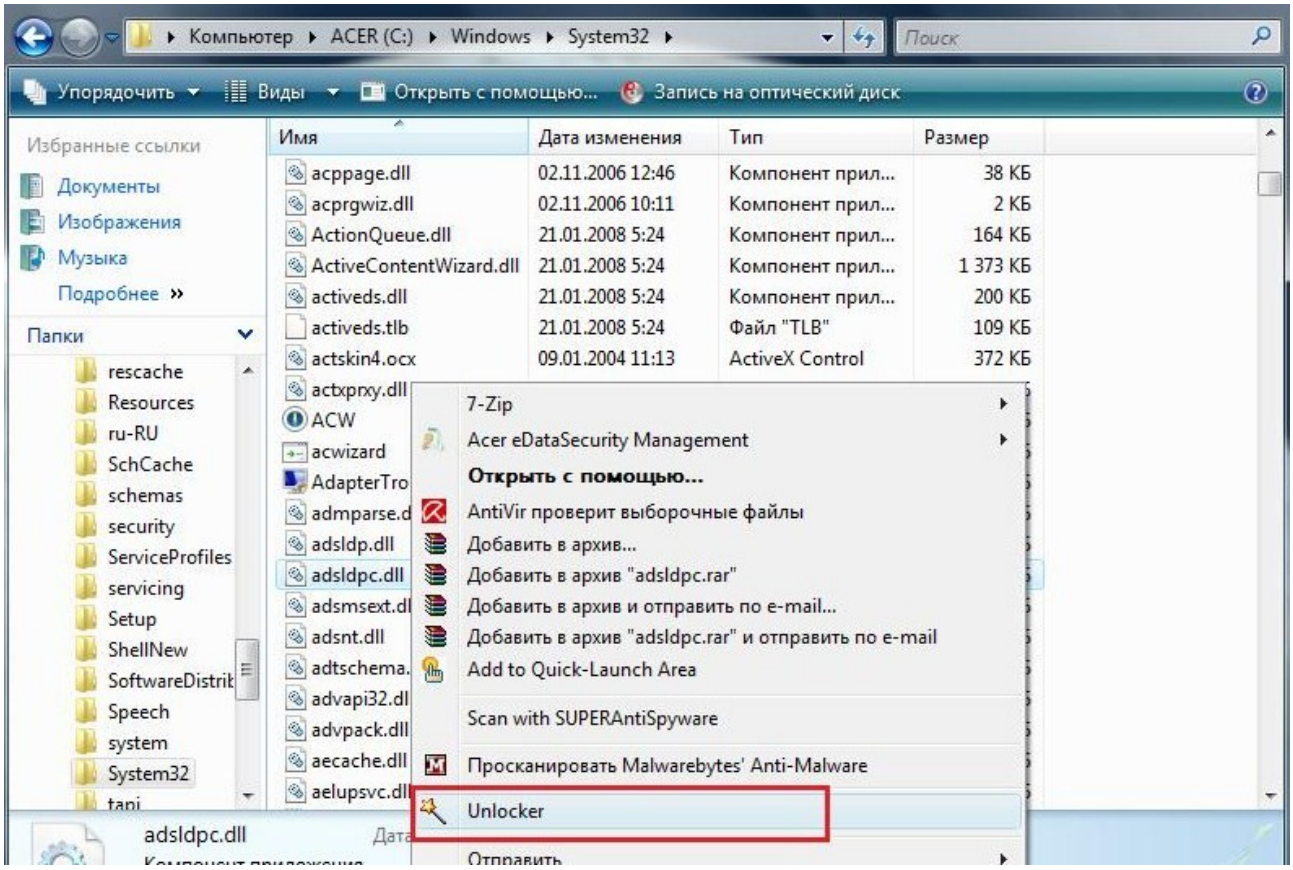
***Для справки: VirusTotal — сервис, который анализирует подозрительные файлы и облегчает быстрое обнаружение вирусов, червей, троянов и всех видов вредоносных программ, определяемых антивирусами.

Итак, мы побывали во вкладке Автозагрузка. Теперь же посетим вкладку Процессы и действуем аналогично, как написано выше.

Как видите программа предельно проста и удобна! Её козырь – показ нам опасных процессов, а также функционал их удаления!

ВНИМАНИЕ,РАДМИН!

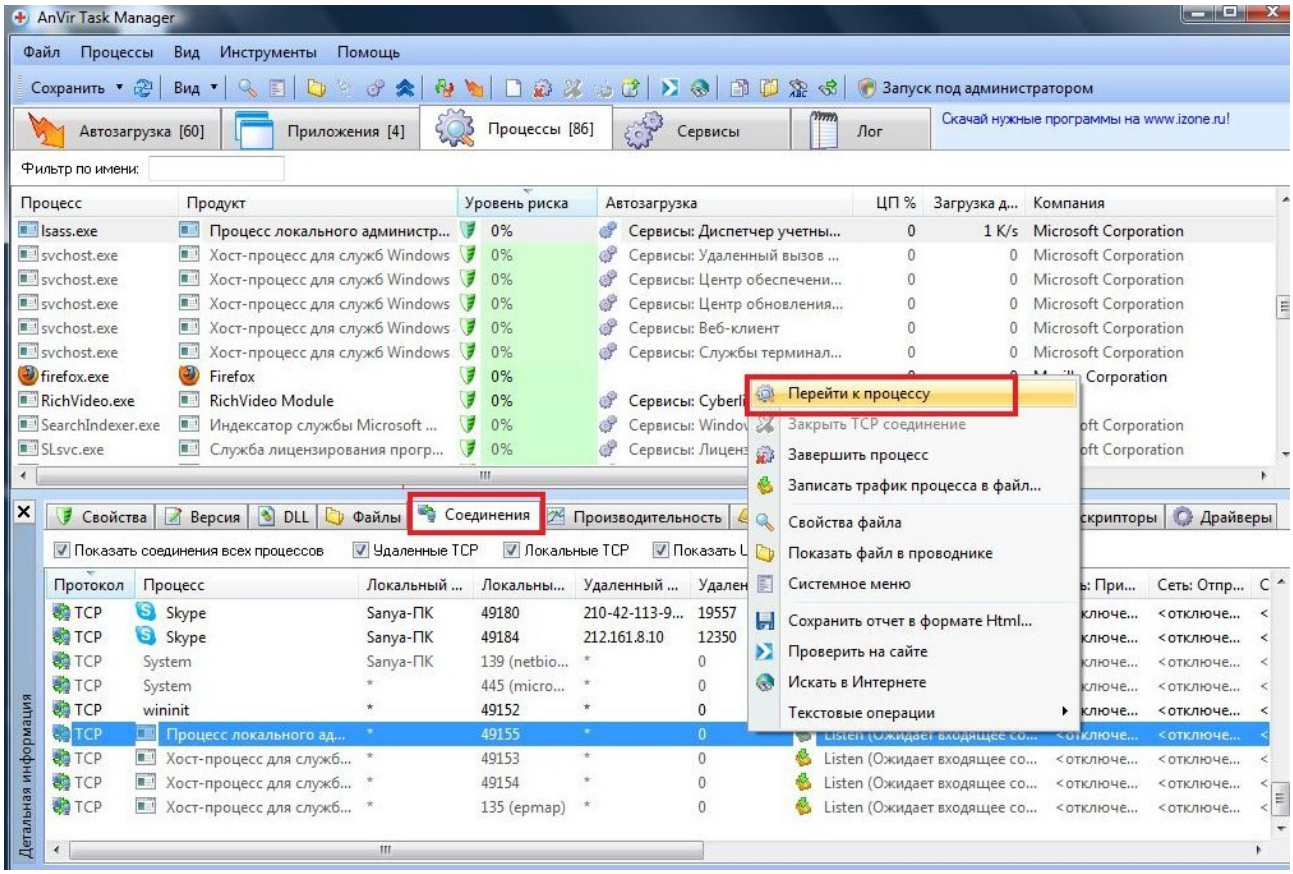
Если у вас в Автозагрузке или Процессах (см. в AnVir Task Manager) имеется **Radmin Service**, или **Remote administrator,** или **r_server.exe**, то знайте, что у вас **Радмин**!!! Что такое Радмин я писал выше, и поэтому удаляйте эту нечисть с вашего компьютера! Как удалить – смотрим чуть выше, т.е. удаляем, как вирус. Бывает так, что сам файл Радмина невозможно удалить и пишет, что невозможно удалить, т.к. занят другим процессом. Для этого попробуйте его удалить в Безопасном режиме. Если не получается, то скачайте программу Unlocker - http://soft.oszone.net/program/1773/Unlocker/ и с помощью её удалите Радмин: найдите этот файл – выделите его – клик правой кнопкой мышки – Unlocker:



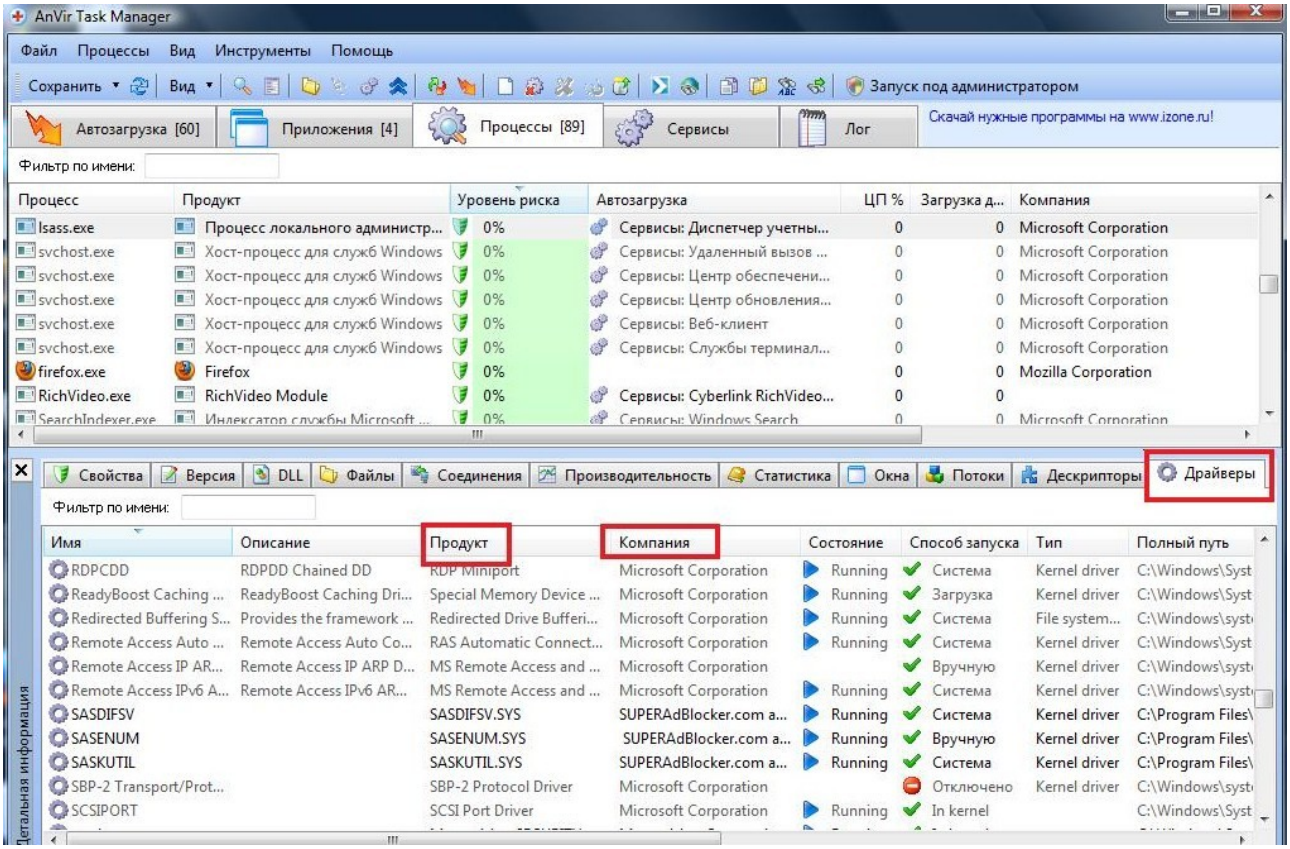
Также можно использовать Unlocker, не устанавливая её, т.е. Unlocker Portable - http://soft.oszone.net/program/10676/Unlocker_Portable/

Мы должны понимать, что Радмин будет использовать порт на вашем компьютере (очень часто 4899-й порт), поэтому в политике закрытия портов мы должны на первое место ставить фаервол или брандмауэр. Как проверить и закрыть порты я выше уже описал, повторяться нет смысла...Вот почему **очень важно иметь ВСЕ закрытые порты**!

Также нам не помешает просмотреть в программе AnVir Task Manager вкладку Соединения, которое вам покажет какая программа использует тот или иной **порт**. Если вас насторожил какой-то процесс, то чтобы его выявить кликните по процессу правой кнопкой мышки и Перейти к процессу, далее можете его проверить посредством Загрузчика Вирустотал 2.0 или же можете завершить/удалить процесс – это при условии, что процесс есть вредоносным:



Также было бы неплохо заглянуть и во вкладку Драйверы. Идеально если столбики Продукт и Компания заполнены теми названиями, которые вам хоть немного знакомы:



Данные меры помогут нам найти не только Радмин, но и кейлоггер, а также другие вредоносные программы и процессы.

Также мы должны осознавать, как Радмин может проникнуть в нашу систему. Обычно его мы можем получить вместе с принятой картинкой, программой...вообще с любым файлом, который мы открываем или запускаем. По поводу проверок на Радмин и другие хакерские инструменты в принятых или скачанных файлах я написал в Разделе 2.0 – Рекомедации by Alexfedoruk.

Кроме того меры по выявлению и удалению Радмина нам может помочь Раздел 3.0 – Реанимация.

Но на этом приятные сюрпризы от AnVir Task Manager не заканчиваются....

Reg Organizer – чистим компьютер!

AnVir Task Manager нам дарит прекраснейшую программу Reg Organizer - менеджер системного реестра Windows. Основным её

достоинством являются: 1) автоматическая и ручная очистка (с помощью инструментов очистки Reg Organizer может обнаружить и удалить ненужные элементы системного реестра); в автоматическом режиме программа сама удалит «мусор и хлам». 2) Оптимизация реестра – удалит ненужные записи....

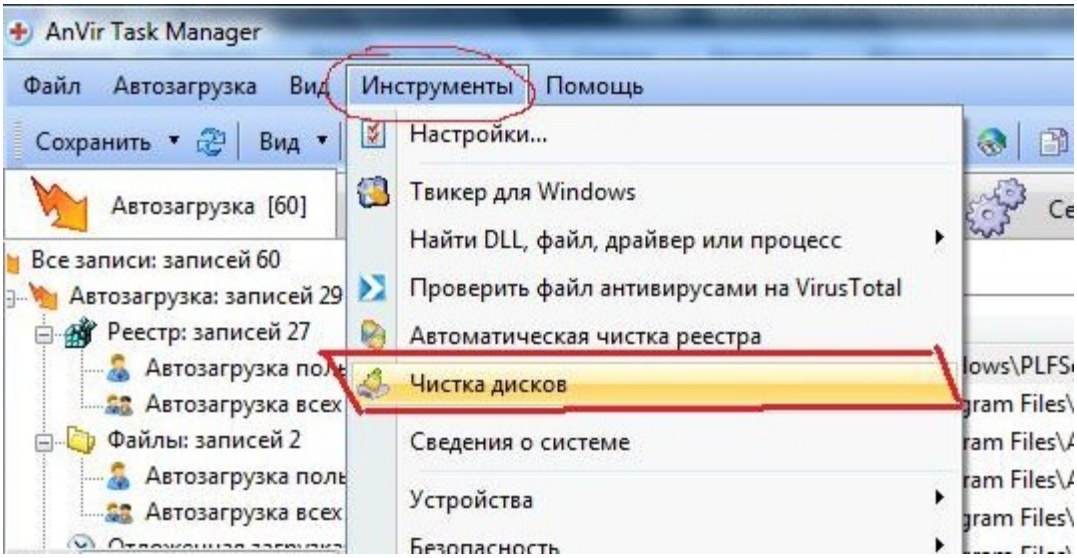
Более подробно о функционале программы вы можете прочитать на официальном сайте разработчика Reg Organizer: http://www.chemtable.com/ru/organizer.htm

Если не чистить систему от ненужных файлов и от ненужных записей в реестре, то со временем этот «мусор» накапливается и системе становится тяжелее «дышать», т.е. медленнее работает, тормозит, медленно запускаются приложения и программы, что приводит к неудобству, к нервам пользователя и психически тяжело работать за компьютером...согласитесь?!

Но проблема в том, что данная программа **платная**, и она расчитана на 30 дней,т.е. это пробная версия. Если вы купите программу, то вам предоставят ключ активации для полной работоспособности Reg Organizer. Но не растраивайтесь, я вам постараюсь помочь и платить не нужно.

Как я упоминал выше AnVir Task Manager дарит программу Reg Organizer, но дарит её как и официальный сайт – на 30 дней, но не стоит торопить события:)

Открываем AnVir Task Manager – Инструменты – Чистка дисков:



Далее программа начнет устанавливаться, если вы её не устанавливали совместно с AnVir Task Manager (выше я советовал НЕ устанавливать пока что). Итак, при установке ставим галочку в нужном месте, чтобы создался ярлык на Рабочем столе (как вам удобней). И тут мы подходим к тому, что программа вас уведомит, что Reg Organizer на 30 дней и т.д. Найдите где-то в настройках (точно не могу сказать,т.к. не помню), куда можно ввести ключ активации. Когда найдете, то вот вам сразу три ключа активации, но нам нужен один ключ... так что на ваш выбор:

1. Регистрационный ключ: BPQYWX-9GQAL-ZSTGN-8TGGV-H4XHP-9THYZ

   Регистрационное имя: Vladislav

2. Регистрационный ключ: B552AA-TNTQX-VP3JM-ZUZMH-MCWKC-BP3MC

   Регистрационное имя: Admin

3. Регистрационный ключ: BK3GVB-GGS4C-DJNS7-UDC2L-X6YFA-NU48G

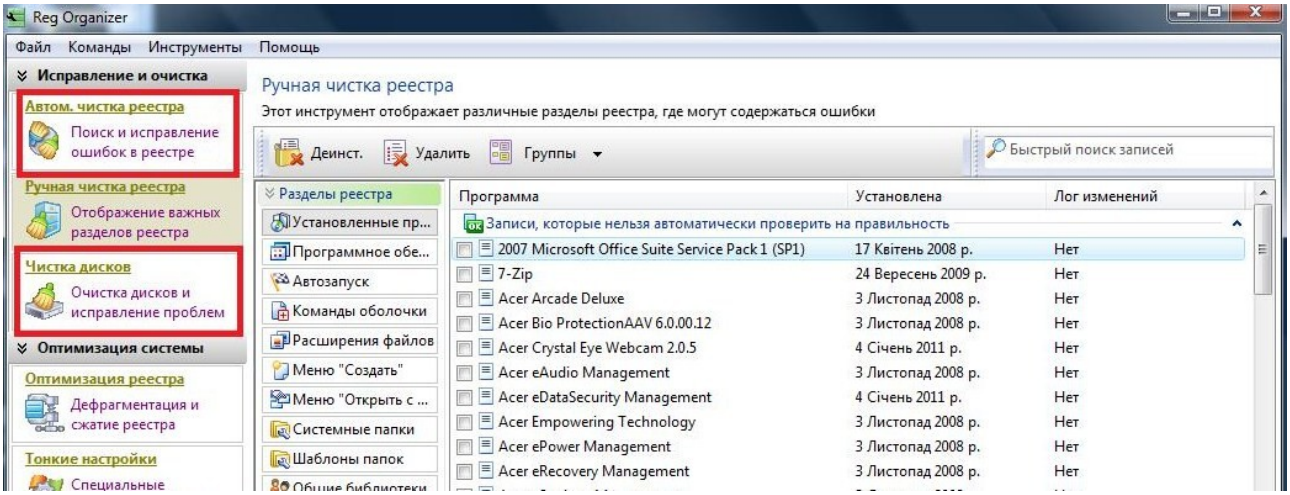
   Регистрационное имя: User

На момент написания книги все ключи были рабочими!

Итак, мы активировали программу Reg Organizer и теперь ей можно полноценно пользоваться. Открываем программу и нас будут интересовать такие 2 опции, смотрим в левой колонке программы:

- Автом.чистка реестра: Поиск и исправление ошибок в реестре;
- Чистка дисков: Очистка дисков и исправление проблем.

О местоположении этих двух опций смотрите на рисунке:



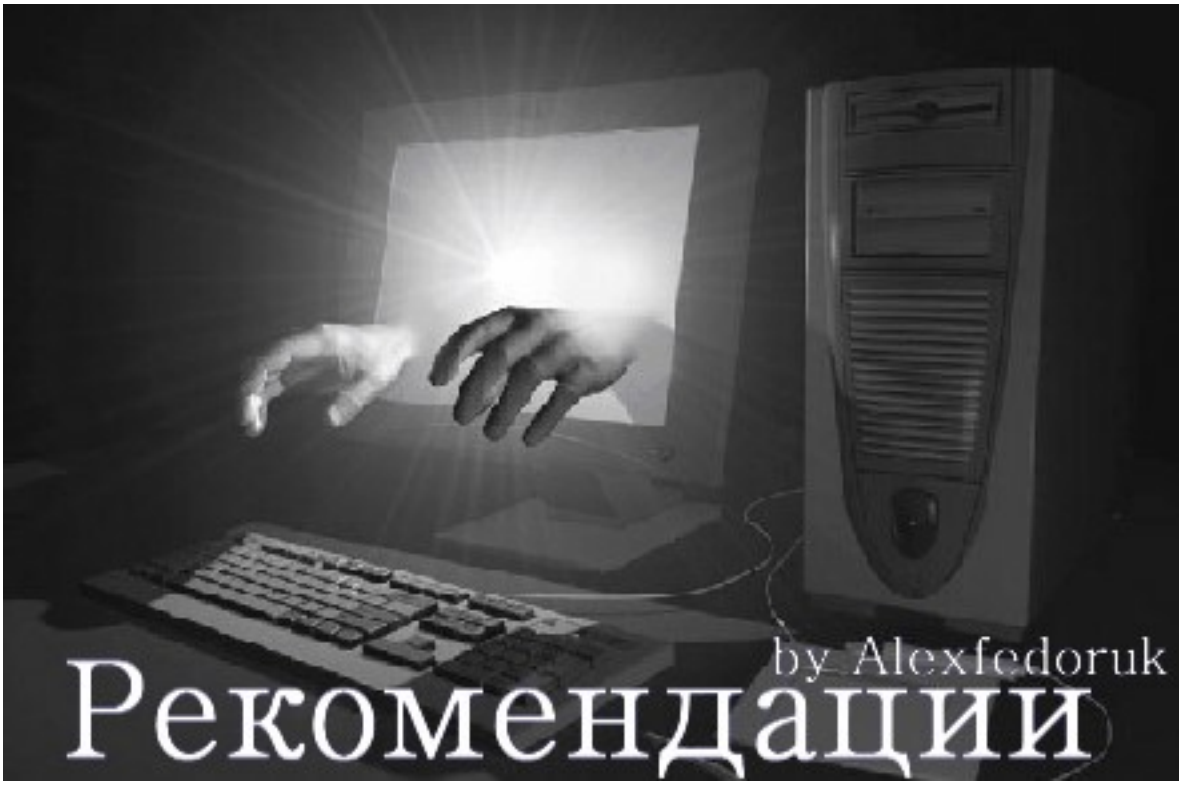
Кликаем по ним и очищаем компьютер от «мусора и хлама», который тормозит вашу систему *Windows. После очистки вы увидите, что памяти на жестких дисках станет больше (в зависимости от забитости), что придаст скорости вашему компьютеру.*

Чистить диск - 1 раз в месяц, а реестр – 1 раз в 3-6 месяца...Это будет оптимальным «очищением».

Не так давно запустил на одном компьютере Reg Organizer. Компьютер не чистился ни разу за 4 года его работы! После чистки было обнаружено – свыше 17800 ненужных файлов и около 1400 проблем в реестре, следовательно около 6-7 гигабайт освободилось с жестких дисков! Так что задумайтесь – нужна ли такая программа?!

Также в данной программе есть ряд других функций, но это вы уже сами разберетесь, т.к. книга всё-таки о безопасности, а не о «хламе» в вашем компьютере.

РАЗДЕЛ 2.0



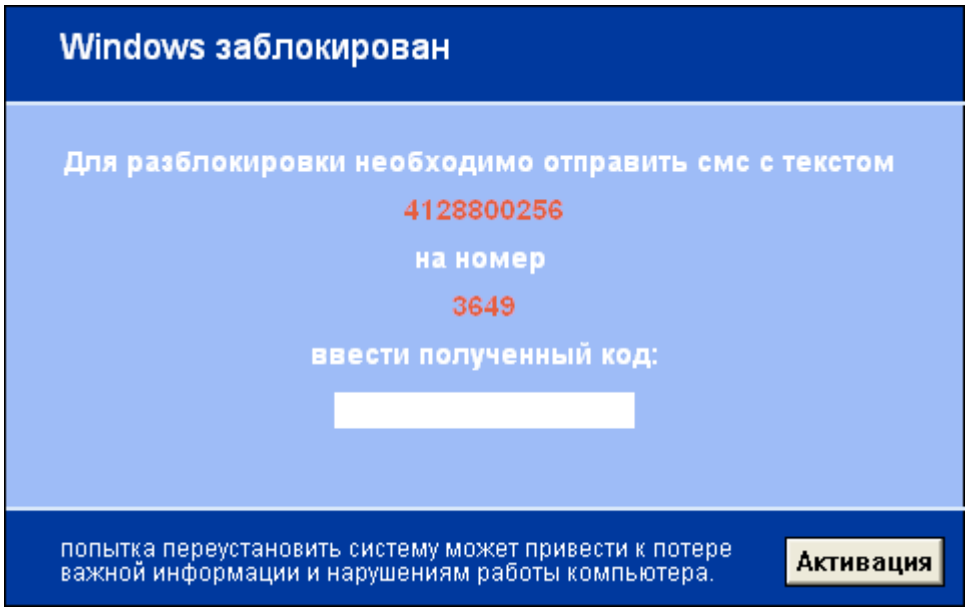
Задача: Скачать что-либо и без вирусов!

Задача не из простых! Ведь большинство вирусов и прочей гадости мы устанавливаем сами же!

Как мы способствуем тому, что мы сами себе вредим?

Итак, классический вариант – обычный пользователь хочет скачать и установить какую-либо программу. Он набирает в поисковике, например Google, название программы и на первых ссылках он её находит, скачивает, устанавливает и вроде программа работает, пользователь радуется.... Утром включает компьютер, а тут у нас на весь экран голая тетя с большими.....эээээ...ммм...ГЛАЗАМИ и требует отправить СМС на короткий номер. Он в панике бъётся об стену, пытаетется зайти в Диспетчер задач или Пуск, но всё безрезультатно, пытается другие методы...и затем ему ничто не остается, как

форматирование и переустановка *Windows*..... – это один из «жестких» вариантов...Возможны и другие варианты – вирусы с различными функциями, кейлоггер, радмин, черви и т.д. и т.п.



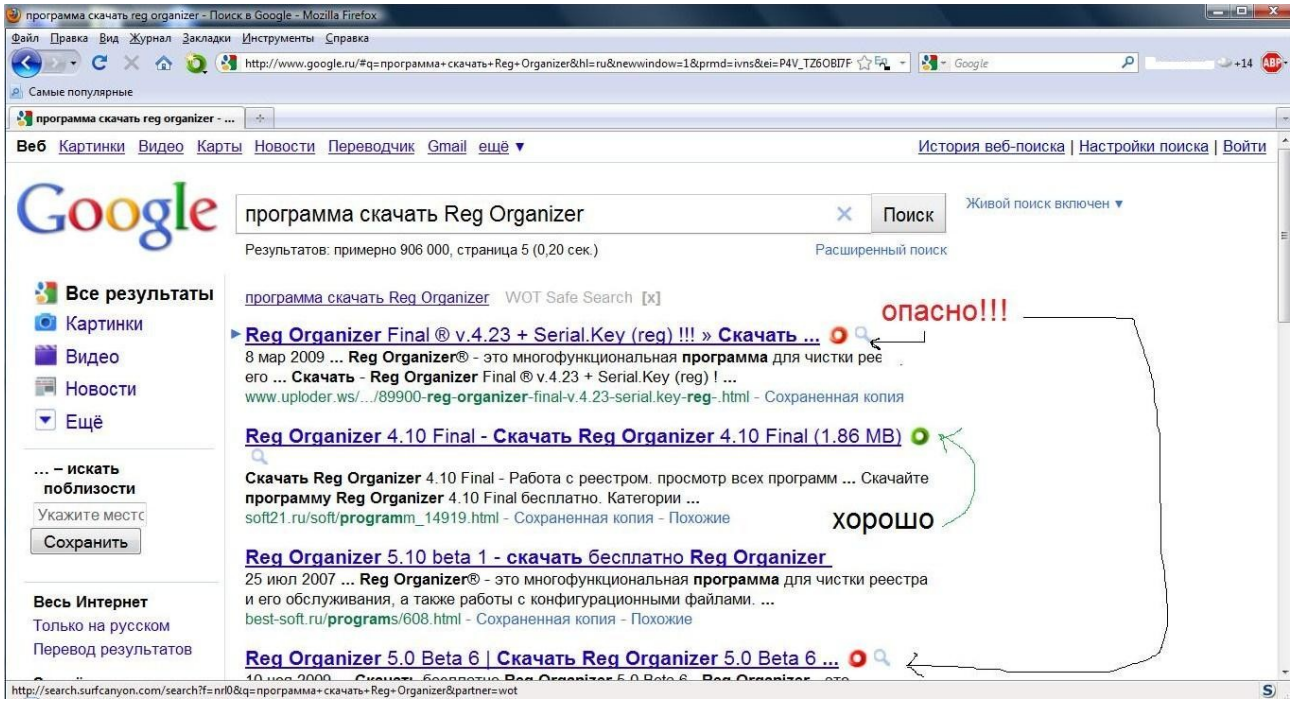
Что произошло в классическом варианте? Пользователь загрузил «склееный» файл: его интересующая программа + вирус. Конечно, в описании программы, откуда он скачивал, ни слова о вирусе...это и так понятно.

Вобщем, примеров масса – это может быть программа или музыкальный файл....а также архивные файлы. И мы понимаем, что классический вариант может нам испортить настроение и *Windows.*

*Предлагаю вам свой - вариант от **Alexfedoruk**. Вообще я не любитель загружать софт, чтобы проверить другой софт, поэтому обойдемся самым легким и в тоже время надежным способом. К тому же Америку я ни для кого не открою, всё это вы знаете или хотя бы «краем уха» слышали о чём далее пойдет речь...*

Итак, нам нужна какая-нибудь программа,чтобы впоследствии её установить на компьютер. Мой метод предусматривает фильтрацию программ по трём разным направлениям (этапам).

Заходим в любимый наш поисковик Google (www.google.ru). Вводим название нашей программы. Появилась масса ссылок. И тут начинается **первый этап** - фильтрация ссылок. В фильтрации ссылок участвует плагин **WOT** – я писал уже выше, что это плагин на браузер, который нам показывает «хорошие»(зеленый кружок) и «плохие»(красный кружок) сайты. Более подробно об этом плагине читаем выше, повторяться не буду, и данный плагин вам подскажет хорошие и плохие сайты:

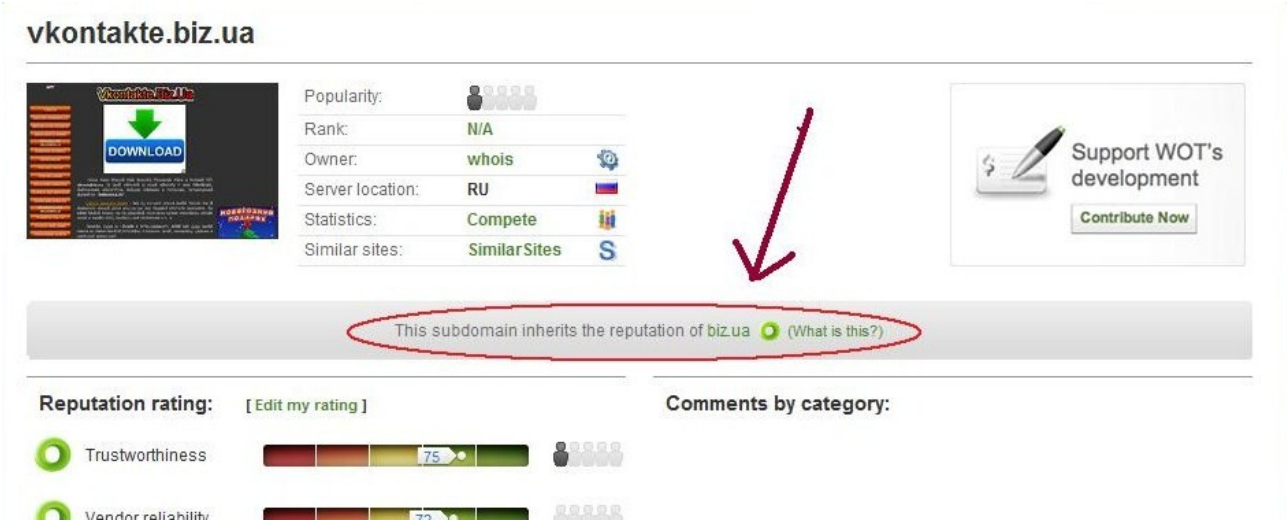


Итак уже какой-то процент сайтов отсеялись и мы с них не будем скачивать программу – это и так понятно!

Заходим на сайты, которые обозначены WOT темно-зеленым цветом. Если на данном сайте нас удовлетворяет наше требование (скачать программу) и мы её скачиваем. Если есть там комментарии скачавших пользователей по программе - обязательно прочитайте. А также прочитайте комментарии в WOT по данному сайту.

Хочу заметить, что сайты, куда размещают все кто хочет свои файлы (файлообменники) нельзя принимать за надёжный сайт, даже если WOT будет зеленым цветом. Это касается и субдоменов, т.е. если видите название сайта, состоящее из более 3 частей (но не

обязательно), то **возможно** WOT может оценивать только субдомен, а не сам сайт, а значит на саму оценку не стоит расчитывать. Поэтому смотрим WOT-рейтинг сайта более внимательней.... WOT вас об этом уведомит, что оценка идет субдомена:



Итак, мы уже скачали нужную нам программу, но не торопитесь её устанавливать. Хорошо, если мы скачивали с официального сайта разработчика данный софт, но в большинстве случаев мы качаем не с оф.сайтов. Ну да ладно!...Когда скачали программу, то мы её «заливаем» на следующие онлайн-сервисы по проверке на вирусы – это я называю **второй этап** - фильтрация программ по «начинке» :

- http://www.virustotal.com/index.html
- http://www.virscan.org/

Эти два сайта практически индиетичны по функциям, но проверяйте программу на обоих сайтах-сканерах! Данные сканеры содержат несколько десятков антивирусов, которые будут сканировать на предмет вируса в вашей программе, что в свою очередь нам дает уверенности в том, что программа безопасна для использования! Но недостатком данных онлайн-сканеров является то, что более 20 мегабайт невозможно проверить, а также отсутствие поведенческого анализа внутри системы (но об этом в третьем этапе).

Но сканировать это одно, а вот понять результат сканирования – это другое.

Если при анализе файла (программы) вы увидите такие слова,как «**Heur**», «**Heuristic**», «**Gen**», «**Generic**», «**Suspicious**» и т.п.), следует помнить, что объект лишь подозревается как возможно вредоносный и не обязательно является вирусом – это как рулетка: 50/50...может есть вирус, а может и нет. Тут уже вам решать.

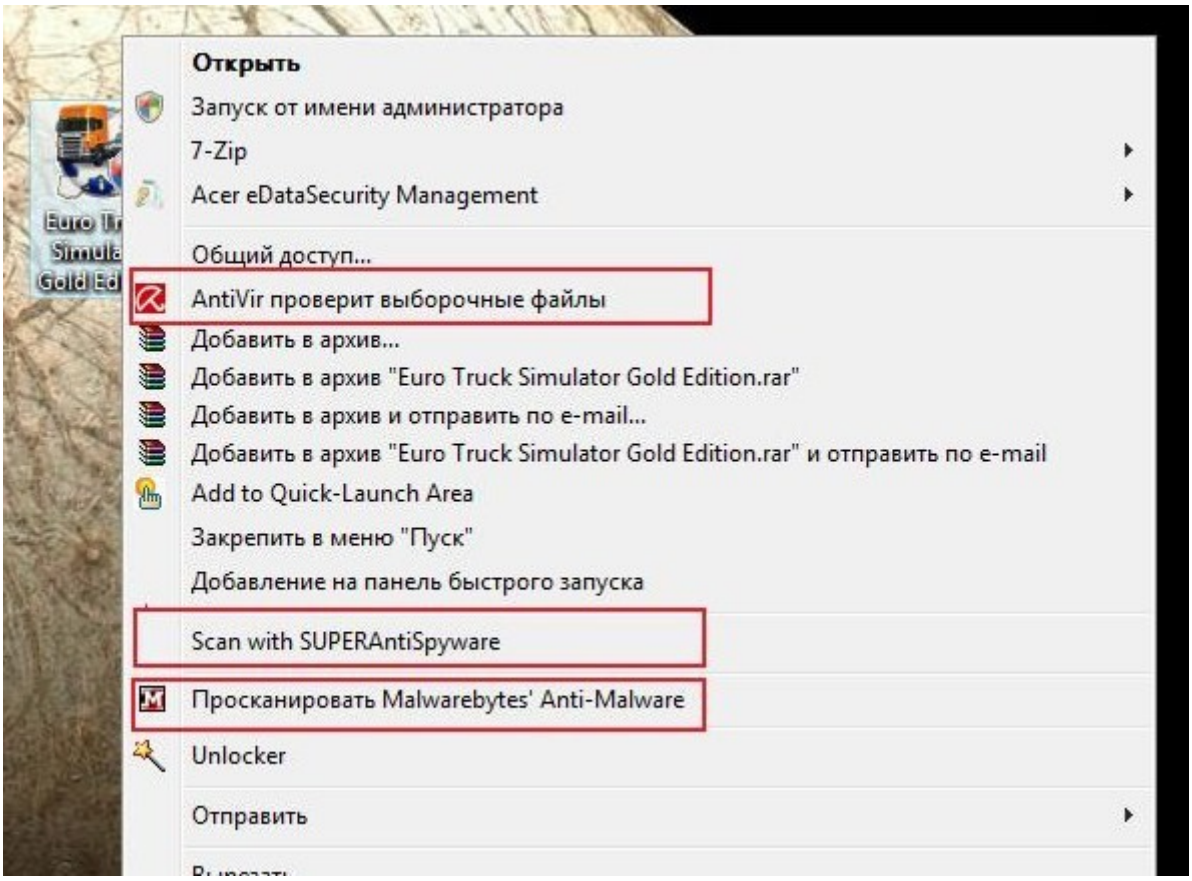
Если программа имеет, кроме установочного файла .exe , и другие компоненты, то их также следует проверить на сканерах второго этапа!

Если вам непонятно, что нашел сканер, то просто введите это название в Google.

На втором этате фильтрация программ по «начинке» обычно большинство программ отсеиваются.

Также незабывайте просанировать скачанный файл своим **антивирусом**, **антишпионом** и **Malwarebytes Anti-Malware** (про эту утилиту смотрите в Разделе 3.0):

Смотрим рисунок, как пример, ниже:



Если наша скачанная программа прошла второй этап, то остался третий этап, который будет для тех программ,что прошли первых два этапа. Этот **третий этап** я называю фильтрация по активности.На этом этапе мы будем использовать так называемые «песочницы», которые дают нам возможность получить полную информацию о том, что он (исполнительный файл) делает, будучи запущен в системе.

ПРИМЕЧАНИЕ: Песочница – это механизм для безопасного исполнения программ. Песочницы часто используют для запуска непротестированного кода, непроверенного кода из неизвестных источников, а также для запуска и обнаружения вирусов.

***Но у вас возникнет вполне естественный вопрос – **зачем тестировать в песочнице на вирусы, если десятки антивирусов во втором этапе их не обнаружили?** Ответ будет очень прост: есть такое понятие, как криптовать файл и если эту фразу перевести простым языком, то криптование делает вирус (склееный с нашей программой) невидимым для антивирусов (для второго этапа) и

чтобы выявить этот вирус, то наш установочный файл программы нужно запустить либо на нашем компьютере (не рекомендуется), либо в песочнице (рекомендуется).

Учтите, что в песочнице запускается установочный файл формата **.exe ,** а не **.rar** или другие форматы.

С теорией разобрались, теперь к практике!

К вашему вниманию онлайн-песочницы, куда мы «заливаем» установочный файл программы:

http://www.threatexpert.com/submit.aspx

http://www.sunbeltsecurity.com/sandbox/

http://anubis.iseclab.org/

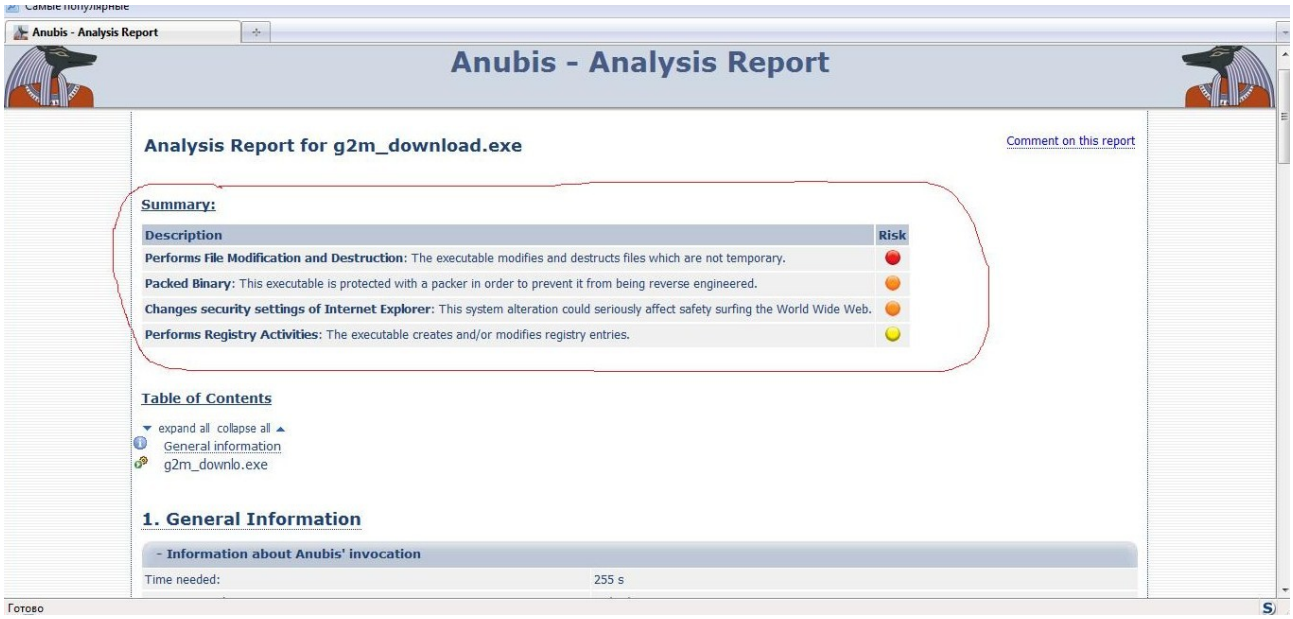
http://www.joesecurity.org/service.php

http://eureka.cyber-ta.org/

http://www.norman.com/security_center/security_tools/

Можете хоть на всех перечисленных песочницах проверять, но лично мне по душе песочница **anubis** (третья ссылка), в котором вердикт анализа всегда вверху странички публикуются (красный круг – плохо и т.д.), а также не поленитесь просмотреть полностью анализ на страничке. Но нужно еще перевести с английского языка и красный цвет – это еще не означает, что файл вредоносный.

Как пример результата песочницы anubis, смотрим на рисунке:



Кстати, в anubis, если программа будет устанавливаться на компьютер, то результат типа: «**Performs File Modification and Destruction:** The executable modifies and destructs files which are not temporary.» - будет практически всегда красным выделяться, как на рисунке выше.Это нормально.

Вобщем выбор песочниц есть и выбрать есть из чего!

Единственный минус онлайн-песочниц – это ограничение по файлам в мегабайтах, которые можно проверить в данных песочницах.

Конечно, результаты будут на английском языке, поэтому для облегчения понятия воспользуйтесь любым онлайн-переводчиком.

И только после третьего этапа, при условии, что результат нас удовлетворил,т.е. отсутствие вирусов, можно приступать к установке и использованию данного софта.

Однако, мы рассмотрели в третьем этапе онлайн-песочницы.Есть также и оффлайн-песочницы, т.е. это уже программа-песочница, которую нужно установить на ваш компьютер. Лично я ими не пользовался, но хочу сказать, что они выгодны тем, что они могут проверить большие установочные файлы программ в отличие от онлайн-песочниц, которые ограничены по приёму файла в мегабайтах (у каждой песочницы по разному).

Одна из самых распространенных песочниц является Sandbox, о которой вы больше узнаете здесь:
http://habrahabr.ru/blogs/virus/114450/

Более навороченной песочницей является виртуальная машина. Одна из самых известных является VirtualBox, которая имеет официальный сайт - http://www.virtualbox.org/wiki/Downloads ...а также инструкцию и детали - http://softobzor.ru/softreview/virtualbox/index.html

..или же Microsoft Virtual PC 2007 - http://www.windowsfaq.ru/content/view/566/46/

ВАЖНО! Однако, если у вас **COMODO Firewall (**или любой другой фаервол, но в случае предусмотренном разработчиком) , хочу заметить, что песочница имеется и в фаерволе COMODO Firewall - изолированная операционная среда для тестирования неизвестных приложений, которым недоверяют. Запуск приложения в песочнице означает, что приложение не может произвести постоянные изменения в других процессах, программах или данных в Вашей «реальной» системе. Comodo объединили **sandboxing** технологию непосредственно в архитектуру интернет-безопасности Comodo, чтобы служить дополнением и усилить фаервол.

Кстати, у хакеров есть очень интересная фишка – это подделывание иконки (сложенные папки) архивных файлов (.rar или .zip) под исполнительный файл (.exe) это называется **маскировка файла**. Например, вы скачали архив, который имеет стандартный вид:

Но всё дело в том, что это НЕ архив, а исполнительный файл (.exe). Есть такой особый контингент пользователей, которые любят на архиве сделать двойной клик, чтобы просмотреть, что запаковано. Вот как раз и этот контингент больше всего и страдает. Или вы видите, что кликнув правой кнопкой мышки на архивном файле мы не видим в меню Извлечь файлы... Если сделать двойной клик мышкой по псевдоархиву (иконка от архива, но сам файл с расширением .exe), то запустится вирус или смотря тем, чем его «начинили». Поэтому проверяйте, так сказать, на «архивность», чтобы они не оказались исполнительным файлом. Проверить легко - на файле с иконкой архива кликаем правой кнопкой мышки и выбираем **Свойства** и смотрим, чтобы расширение архивного файла соответствовало иконке,т.е. в нашем случае имел формат .rar или .zip. Если вы сталкнетесь с подобным случаем, то знайте, что в данном псевдоархиве вас хорошего ничего не ждет...Не зря же его так замаскировали под архив. Только не стоит путать с такой иконкой установочного exe-файла, что ниже...это совсем другое:

Вот впринципе и весь мой «простенький» метод поиска нужной программы:)

«Фильтруем» всё подряд!

Всё, что вам приходит, даже от друзей или еще от кого-то, то проверяйте их на сайтах:

- http://www.virustotal.com/index.html
- http://www.virscan.org/

Это могут быть абсолютно любые файлы: фотографии, музыкальный файл, программы, текстовый документ и т.д... и независимо от

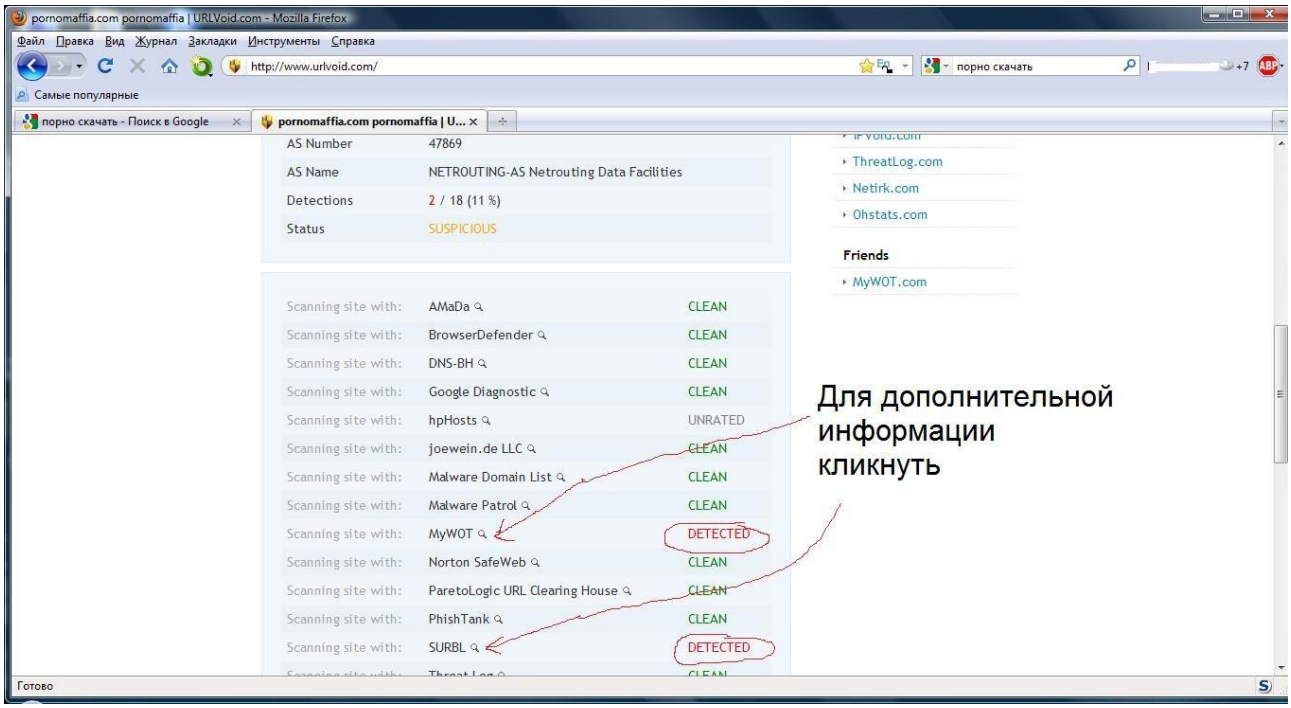
расширения файла – будь-то .exe или .pdf... Этот «фильтр» должен быть всегда с вами рядом и под рукой! И помним, что сканеры принимают файлы не более 20 мегабайт! Если даже вам друг прислал файл, то он и сам может не подозревать, что там вирус, т.к. его система заражена уже!

Проверяем ссылки!

Все ссылки, которые вам приходят самыми различными путями, нужно проверять на специальных сканерах. Эти сканеры вам сразу поведают – опасный ли это сайт, содержит ли вирусы, какая репутация у данного сайта, использует ли агрессивную атаку на браузер, присутствует ли какой-либо вредоносный код, замечен ли сайт в мошенничестве (особенно это касается интернет-магазинов и т.д.) и фишинге, распространяет ли вредоносные программы и т.д...

Вот эти два сканера, которыми нужно пользоваться одновременно:

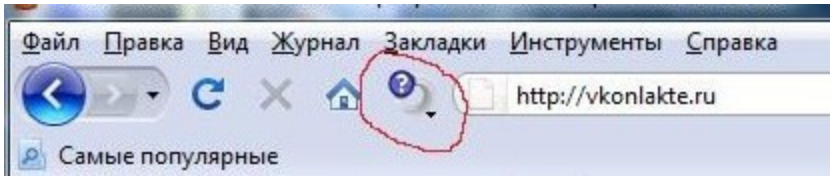
- http://www.urlvoid.com/ - самый мощный мультисканер; сканирует сайт одновременно 18 сканеров! Если результат CLEAN – это хорошо, если DETECTED – это плохо. Чтобы прочитать, что сканер нашел (в случае DETECTED), то кликните возле названия сканера на маленькую лупу:

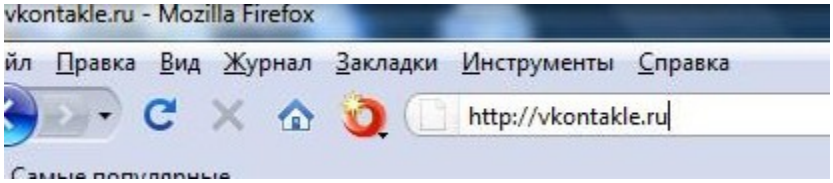


- http://vms.drweb.com/online/ - как сам сканер тянет на оценку 4- , но этот сканер хорош тем, что показывает переадресацию (в отличие от первого сканера).

Поэтому можно с уверенностью сказать, что эти оба сканера дополняют друг друга. Ну и не забывем о плагине WOT на браузер.

Кстати, хочу заметить,что бывает такое – вы заходите, например, в социальную сеть Вконтакте, вам откроется окно Введите Логин/Пароль, но WOT показывает **бесцветный** или **красный круг!!!** Это означает, что вы попали на фейк или псевдосайт и если введете свои Логин/Пароль, то можно сказать, что ваша страничка уже взломана, т.к. ваши данные отправились уже хакеру. Поэтому поглядывайте на кружок (слева от адресной строки) и название сайта (чтобы правильно писался), когда вводите ваши данные:





Это на примере социальной сети Вконтакте. Кроме того если WOT показывает красный цвет, то часто всплывает большое предупреждение на весь браузер, что данный сайт есть опасным.

ДЛЯ СПРАВКИ: **Фейком** (веб-страницы) называется страница или сайт, где находится точная копия какого-либо веб-сайта, для просмотра которого нужна обязательная авторизация. Используется для кражи логинов и паролей у пользователей. Принцип действия: жертва получает ссылку на сайт, авторизуется с настоящим логином, данные отправляются в файл на сайте, злоумышленник получает логин и пароль жертвы и входит на сайт.

Но мой вам совет!!! Не переходите на сомнительные ссылки, что приходят от неизвесных личностей, спама, а также даже если от друзей (лучше у них лично спросите – присылали ли они ссылку или нет).

Как хранить ценную информацию?

Понятие «ценная информация» для каждого разная. Для кого-то это пароли и логины от Вкотнакте или какого-либо форума....а для кого-то это номера кредитных карт с логинами или информация в электронном виде, касающаяся финансовых операций.Но в любом случае у каждого есть что-то, что нужно скрыть от посторонних глаз. особенно от хакерского глаза.Тем более, что благодаря хакерским инструментам украсть ваши пароли из текстового (или любого другого) незащищенного файла ничего не стоит! Есть специальные программы, налаживающие пароль на определенный диск или папку, но мы пойдем более простым, без «заморочек» и в тоже

время надежным способом, при котором ничего не нужно будет устанавливать из программ.

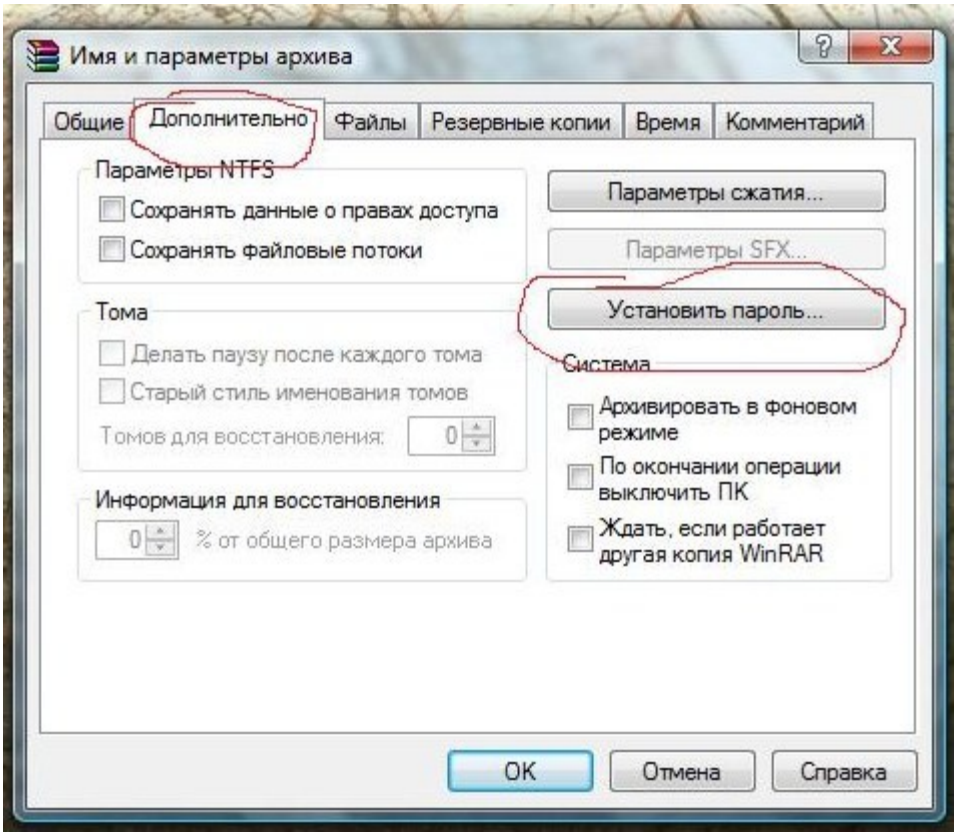
Немного теории. Пароли на всех веб-ресурсах, где вы зарегистрированы, нужно ставить разные и сложные. Чем больше вы всюду регистрируетесь, тем больше нужно запомнить паролей и логинов – это логично. Поэтому нам нужно ЧТО-ТО, что бы мы всегда их помнили....Конечно, вы можете написать на бумажке все ваши пароли и логины, но это неудобно...согласитесь?!..каждый раз перепечатывать...

Если у нас пароли/логины (т.е. текстовая информация), то создайте текстовый документ и занесите туда всё, что необходимо.

Мы будем работать с очень нужной программой **WinRar**,если таковой нет у вас программы, то это есть странно, что у вас её нет. Поэтому, если нет её - скачайте, пригодится и в будущем:

http://soft.oszone.net/program/83/WinRAR/

Далее кликаем правой кнопкой мышки на документе – Добавить в архив. Мы создаем архивный файл, но мы на него поставим пароль: во вкладке Дополнительно выбираем Установить пароль. Как оказалось – всё гениальное просто:



Пароль ставим сложный! Если одни цыфры, то можете считать, что вы пароль не ставили! Нам нужно поставить пароль, состоящий из букв и цыфр, а если еще хотя бы один спецсимвол, то взломать (брутить) практически невозможно! К спецсимволам относим всё то, что не является буквой и цыфрой,а именно «.№;%:?*()_+/, и т.д. Например, пароль на архив: иванов*25 или сергей!1980, или (сергей1980) и т.д. и т.п. Главное, чтобы вы его помнили и для вас этот пароль был **запоминающимся**.

Полученный архивный файл (.RAR) называем любым словом, но чтобы это слово не было связано с тем, что вы там храните! Иными словами ПАРОЛИ или PASSWORD - не катит, а нужно что-то типа СОБАКА, ЦВЕТЫ, ФОТО, СЕМЬЯ и т.д.....Т.е., называем чем-то отдаленным от внутренности архива полученного.

Данным действием мы сразу убиваем двух зайцев: во-первых, физически (у компьютера) никто, кроме вас, теперь не сможет читать то, что вы спрятали.....а во-вторых, скрыли информацию от хакера, который дистанционно,например, через Радмин может их заполучить. Пусть даже хакер заполучит ваш архивный файл с

паролями, но он его замучается брутить (взламывать). Поэтому, **чем сложнее пароль, тем труднее его взломать!**

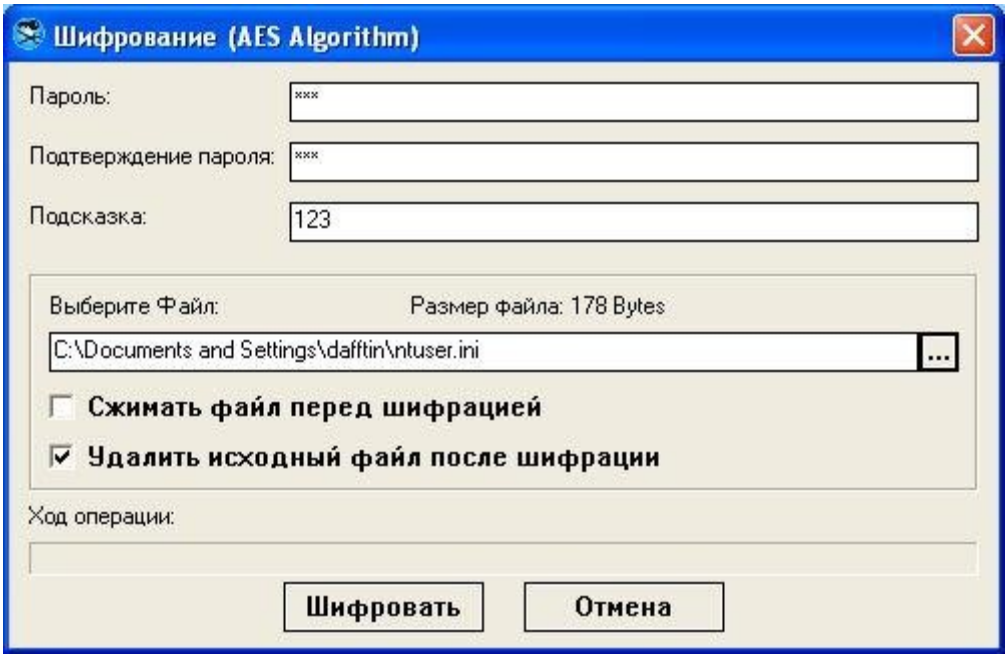
Кстати, есть интересный онлайн-сервис, который определяет (теоретически) то количество времени, которое потребуется хакеру, чтобы взломать ваш пароль. Вы вводите на сайте свой пароль – внизу отображается время, чтобы его взломать . Так что делайте выводы сами:
http://howsecureismypassword.net/

Естественно, мы можем так хранить не только пароли/логины, но и всё, что вам нужно спрятать от чужих глаз и рук!

Но есть и еще один вариант – более прогрессивный метод!

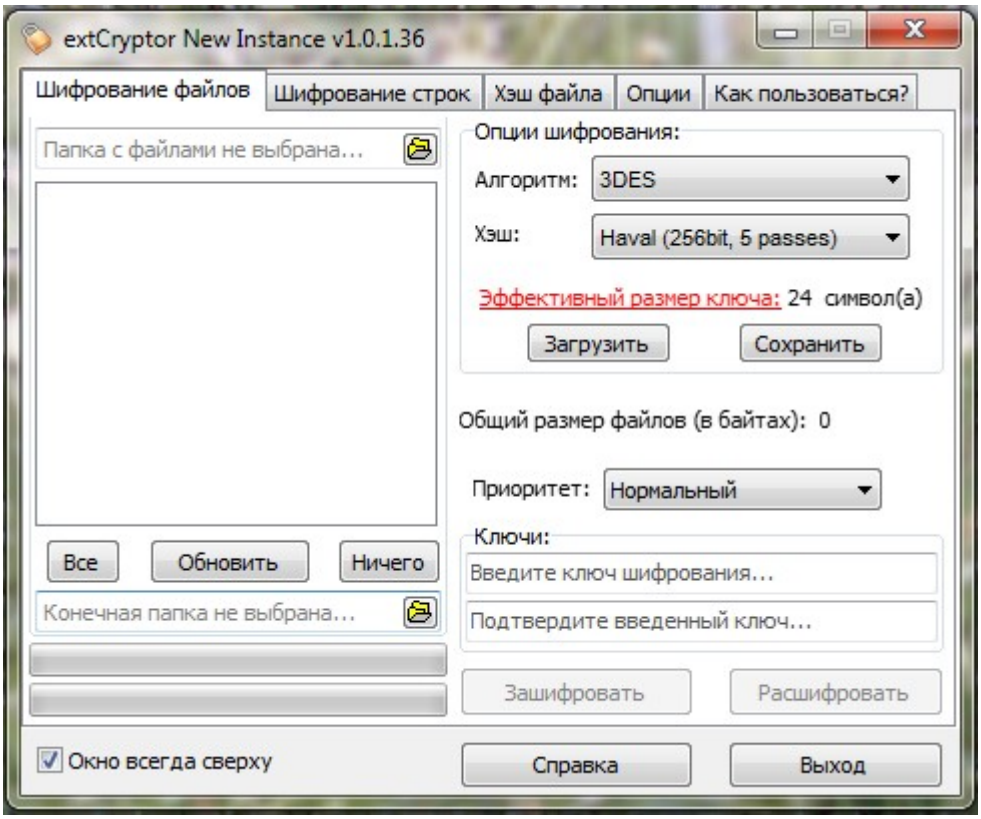
Если вышеописанный метод хранения информации не впечатляет, то тогда вам путь к **шифрованию информации**. Есть специальные программы, которые зашифруют вам нужные файлы под парольной защитой!

Одна из таких программ - **DAFFTIN Cryppie** - это небольшая, но порой очень полезная утилита, позволяющая защищать любой тип файлов полностью шифруя их содержимое по известному алгоритму BLOWFISH или AES. После этого никто не сможет расшифровать ваши файлы не зная пароль:



Кроме того язык программы DAFFTIN Cryppie русский, что не может радовать: http://soft.oszone.net/program/11310/DAFFTIN_Cryppie/

Если в вышеуказанной программе DAFFTIN Cryppie вас не устраивает только 2 вида шифрования (BLOWFISH или AES), то вот вам программа **extCryptor** - небольшая программа, предназначенная для шифрования/дешифрования любых типов файлов различными алгоритмами: программа поддерживает 17 различных алгоритмов шифрования файлов и 10 алгоритмов подсчета хэша (так же применяется при шифровании):



Язык русский. extCryptor – скачиваем здесь: http://soft.oszone.net/program/9994/extCryptor/

Определяем – есть ли у нас кейлоггер?!

В начале книги я немного упомянул про такой инструмент хакера, как кейлоггер. Теперь немного в деталях.

Кейлоггер (англ. **keylogger**) – это программа для записи нажатий на клавиши. Некоторые моменты о нём:

- кейлоггер может записать ваши коды и номера счетов в электронных платежных системах, пароли к учетным записям в online-играх, адреса, логины, пароли к системам электронной почты и т.д.;
- большинство кейлоггеров распространяются вместе с шпионским ПО (спайваре), а также с различными программами;

- кейлоггеры могут быть установлены на ваш компьютер дистанционно;
- большинство кейлоггеров незаметны, поэтому даже если ваш компьютер работает нормально, это не значит что его нет;
- все, что кейлоггер запишет, он может отправить по электронной почте; так что физический доступ к вашему компьютеру не нужен;
- часто на публичных компьютерах (компьютерные салоны, интернет-кафе, библиотеки) могут быть установлены кейлоггеры;
- кейлоггер может распространятся, как один из вариантов, с помощью скрипта на веб-страницах, который использует особенности интернет-браузеров, позволяющие программам запускаться автоматически при заходе пользователя на данные страницы. Поэтому очень важен плагин на браузер NoScript, о котором я уже писал выше в статье о браузерах.

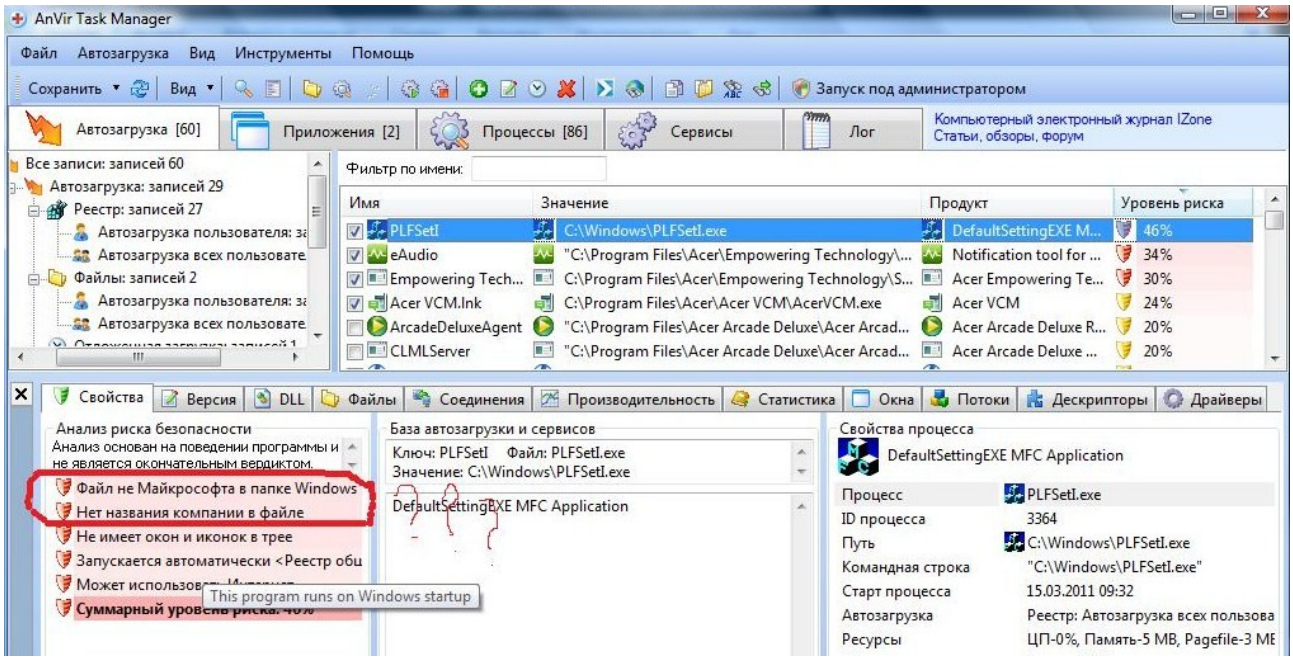
Как видим вещь эта неприятная и она нам может подпортить жизнь.

Мы уже понимаем, что кейлоггер мы можем «подцепить» с любой программой, особенно, если мы скачиваем и устанавливаем хакерские программы по взломам, кряки и т.п. Поэтому, я выше уже писал, как правильно скачивать «правильный» софт.

Немного забегу наперёд – есть довольно простой метод, при котором мы можем «надурить» кейлоггер,т.е. сделать так, что при вводе текста (например, логин и пароль) мы его оставим «с носом» и хакеру ничего не прийдет из ценной информации. Об этом методе написано в следующей теме.

Но чтобы удостовериться (на процентов так 90-98), что у нас нет кейлоггера, мы должны для начала заглянуть в **Автозагрузку** – в этом нам поможет программа AnVir Task Manager, о которой я уже выше писал. Изучите Автозагрузку (Автозапуск), посмотрите нет ли там чего

«лишнего» , да и еще и без сертификата (это смотрим во вкладке Свойства, внизу):



Также есть новые кейлоггеры, которые уже даже не прописуются в Автозапуск, а сразу в Процессы или Сервисы, а может ни там и ни там.... к тому же уже с подписью, что софт от Microsoft, что существенно визуально и вручную будет практически невозможно найти кейлоггер.

Поэтому нам помогут программы, которые «ловят» кейлоггеров-шпионов.

Первый, кто «заступится» за нас это антивирус, но не всегда. При условии, что имеется эвристический (поведенческий) анализ у вашего антивируса...Кстати, Avira AntiVir и Антивирус Касперского имеют эвристику.

Второй, кто нас оборонит – это фаервол или брандмауэр. **Но у фаервола будет больше преимуществ, перед брандмауэром *Windows***. *Мы должны знать, если хакер имел физический доступ к вашему компьютеру, то он, наверняка, свой кейлоггер внёс в настройки фаервола (брандмауэра) в доверенные программы (или Исключения), а это значит, что в данном случае фаервол «скажет» кейлоггеру: «Милости просим в компьютер...»*

Третий – это наша программа-антишпион. Поэтому 1 раз в месяц сканирование антишпионом очень даже кстати будет.

Четвертый, очень даже неплохой защитник, который хорошо ловит кейлоггеров – это утилита AVZ –

http://www.z-oleg.com/secur/avz/download.php

Даная антивирусная утилита AVZ распознает кейлоггеры за счет анализа системы без применения базы сигнатур, что позволяет достаточно уверенно детектировать заранее неизвестные троянские DLL и Keylogger.

Также утилита *AVZ удаляет* SpyWare и AdWare модули, Trojan-Spy, Trojan-Downloader, Trojan-Dropper и многое-многое другое... Подробней: http://www.z-oleg.com/secur/avz/

AVZ не нужно устанавливать, просто скачали, запустили и сканируем все жесткие диски, предварительно проставив галочки на них в утилите.

И наконец пятые помощники, которые «почистят» систему не только от кейлоггеров, но и помогут в обнаружении и последующим удалением с компьютера различного рода вредоносных скрытых объектов (**rootkit**).

Rootkit — программа или набор программ для скрытия следов присутствия злоумышленника или вредоносной программы в системе. Этот набор, как правило, включает в себя разнообразные утилиты для "заметания следов" вторжения в систему, сниферы, сканеры, кейлоггеры, троянские программы.

На ваш выбор по операционной системе предлагаю два варианта:

1) *Если вы установили бесплатную версию Avira AntiVir Personal, то там отсутствует (или слабо работает) опция по поиску и удалению руткитов. Но мы можем скачать отдельно эту опцию и просканировать систему. Предлагаю программу*

Avira AntiRootkit Tool -
http://www.avira.com/ru/support-download-avira-antirootkit-tool

Avira AntiRootkit Tool для Windows Vista, XP, 2000.

2) ***Sophos Anti-Rootkit -*** программа для защиты компьютера от руткитов - вредоносного софта, тщательно скрывающего свое присутствие в системе. По уверениям разработчиков, Sophos Anti-Rootkit способен обнаруживать и удалять как известные, так и неизвестные руткиты:
http://soft.oszone.net/program/1894/Sophos_AntiRootkit/

Sophos Anti-Rootkit для Windows 2000/XP/Vista/Server 2003/Server 2008/Seven. Как видим поддержка Windows 7.

ВНИМАНИЕ! *Рекомендую 1 раз в месяц сканировать утилитой AVZ для профилактики вирусов, кейлоггеров и прочих инструментов хакера! И, кстати, мы должны понимать, что если кейлоггер есть приватный (свеженаписанный и отсутствие его в сигнатурных базах антивирусного ПО), то искоренить его гораздо будет труднее, но возможно.*

Правильная виртуальная жизнь

Безусловно, в интернете мы все общаемся посредством тех возможностей, которые нам доступны – социальные сети, ICQ , Skype, электронная почта, различные форумы и т.д. И, как правило, везде нас подстерегает угроза, поэтому несколько простых правил.

В социальных сетях не нужно расписывать ваши личные данные, телефоны, ICQ, адрес проживания и, особенно, электронную почту, к которой привязана данная страничка соц.сети. «Привяжите» ваш аккаунт к мобильному телефону. Нельзя переходить на ссылки, что шлют вам, даже друзья – лучше у них переспросите – они ли вам прислали, а если это и они, то проверяйте ссылки на вирусы (выше я

написал по этому поводу).... особенно сейчас модно присылать картинки с заманчивым предложением, на которых имеется ссылка и её всего-лишь нужно вставить в адресную строку браузера – это развод и обман. По возможности сделайте ваш профиль закрытым.

Это касается ICQ, Skype , электронной почты – не принимать «левых» ссылок и файлов, особенно: «Оу..привет! Посмотри на себя. Я незнала, что ты там был..» – и ссылка прилагается. Пароли всюду ставим сложные - цыфры, буквы и !»№%:?*()_+=.... Не нужно указывать в Skype свои контактные даные и телефон. По возможности сервиса применяйте в пароле русские буквы.

Рекомендуется снимать ICQ-клиенты с автоматической загрузки, т.е. запускать их вручную, а не автоматически при старте системы. Существуют описания атак на ICQ, для реализации которых клиент должен быть запущен автоматически во время загрузки Windows.

Не создавайте основную почту, которую вы собираетесь делать привязку к социальным сетям, ICQ , Skype и т.д. на почтовом сервисе **mail.ru**, потому как данный сервис почты излюбленный хакерами-взломщиками. Такую почту не так тяжело взломать, особенно если пользователь «ламер» (неопытный пользователь) и пароль к тому же ставит типа qwerty, а также свой этот e-mail он всюду укажет среди виртуальной обественности....К тому же на mail.ru имеется опция Мой мир – социальная сеть, где вас легко вычислить и взломать. Кстати, если вы думаете, что поставив пароли на папки Входящие или Отправленные в сервисе mail.ru, вы защитите проникновение хакера в эти папки, то вы глубоко ошибаетесь – настоящий взломщик-профессионал имеет обходы этих паролей, которые ему не помехой уже будут ваши запароленные папки (сталкивался лично с этим)... Знайте, что mail.ru – это один из самых «дырявых» почтовых сервисов и не стоит возлагать на него большие надежды. Поэтому правильней и безопасней было бы иметь основной электронный ящик на почте от компании **Google.com** - http://mail.google.com/mail?hl=ru

После создания почты gmail у нас будет два преимущества:

- данный электронный ящик мы никому не показываем и не рассказываем, только вы один знаете свою почту, к которому можно привязать аккаунт от социальные сети, ICQ , Skype и т.д.
- сама почта от Google.com является более безопасней с точки зрения взлома и спама, но всё же ни при каких условиях не переходим на «левые» ссылки и не открываем «левые» файлы, что будут приходить на ящик от сторонних людей.

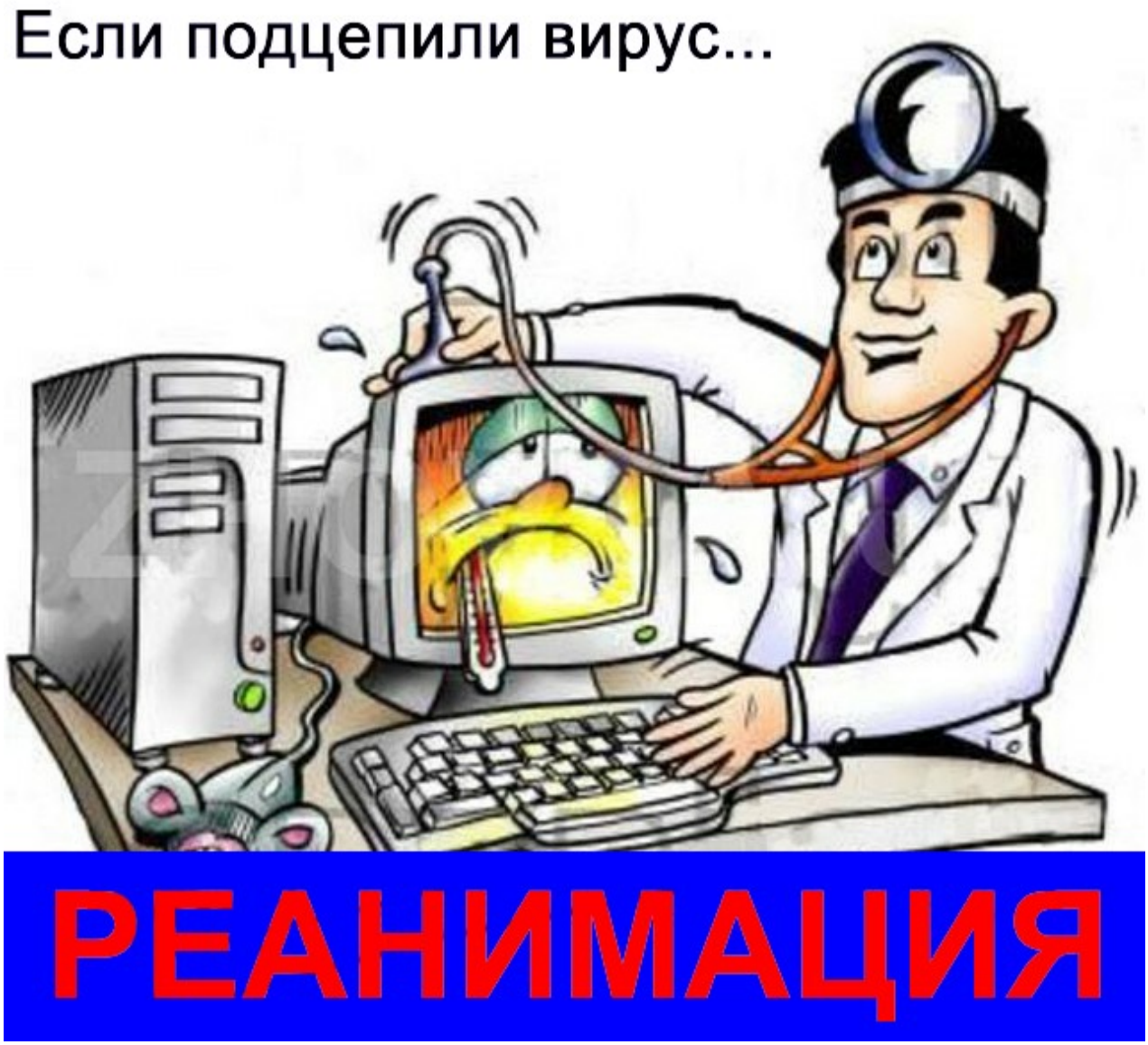
Хочу также заметить, что везде и всюду, где это возможно, делайте привязку к мобильному телефону и дополнительному электронному ящику, чтобы в случае проблем вы всегда смогли вернуть те или иные пароли через СМС на ваш номер мобильного. А дополнительная привязка к электронному ящику (e-mail от Google) будет, как своеобразной страховкой на случай, если мобильный потерялся или нет просто доступа к нему...и наоборот – если e-mail взломан или нет доступа, то восстановить пароль можно посредством СМС.

Постарайтесь обходиться без компьютера, который находится в общественном месте – интернет-кафе, библиотеки и т.д. Имеется ввиду, что как правило, в таких «злачных» местах очень возможно, что присутствуюю кейлоггеры, Радмины и вирусы, собирающие пароли и логины, которые вы введете. Поэтому не стоит в подобных местах вводить различные свои логины и пароли от той же почты или социальной сети... Но что делать тем, у кого нет своего ПК и интернета, а к другу идти и просмотреть почту как-то стыдно? Конечно остаётся, например, интернет-кафе. И тут вам совет: **если всё-таки приходиться пользоваться общественным компьютером, то вводите логин и пароль через виртуальную клавиатуру онлайн** - можете в поисковике набрать это словосочетание. Нашли, например: http://www.keyboard.su/ Далее мышкой «печатаем» логин и скопировали его в поле ЛОГИН, например, почты....также и пароль. И тогда можно с большей уверенностью сказать, что клавиатурные перехватчики (кейлоггер) вам не страшен уже. А дальше можете печатать тексты нормально – на клавиатуре...пусть читают хакеры :)

Такая клавиатура применима всюду, где есть подозрения на кейлоггер!

Знайте, чем меньше данных вы оставляете о себе в сети Интернет, тем менее вы уязвимы!

РАЗДЕЛ 3.0



Если так уж получилось, что вирус или прочая паразитирующая «нечесть» уже на вашем компьютере, то не спешите решать проблему форматированием, так сказать «снести Винду»...Это вы всегда успеете...да и не факт, что это поможет.

Есть множество признаков заражения вирусом вашего компьютера, среди которых:

**Компьютер работает медленнее, чем обычно;

**Компьютер перестает отвечать на запросы и часто блокируется;

**Каждые несколько минут происходит сбой и компьютер перезагружается;

** Компьютер самопроизвольно перезагружается и после этого работает со сбоями;

** Установленные на компьютере приложения работают неправильно;

**Диски или дисководы недоступны;

**Не удается выполнить печать;

**Появляются необычные сообщения об ошибках;

**Открываются искаженные меню и диалоговые окна;

**Исчезновение файлов и каталогов или искажение их содержимого;

**Частое обращение к жесткому диску (часто мигает лампочка на системном блоке);

**Интернет-браузер «зависает» или ведет себя неожиданным образом (например, окно программы невозможно закрыть).

***Самый явный признак вируса – это хищение всех паролей (или большинства): вы не можете зайти на сайты по вашему логину/паролю, вы не можете зайти в ICQ и Skype, а также почту, электронный кошелек и т.д.

Но в большинстве случаев наличие косвенных симптомов вызвано сбоем в аппаратном или программном обеспечении. Несмотря на то, что подобные симптомы с малой вероятностью свидетельствуют о

заражении, при их появлении рекомендуется провести полную проверку компьютера.

Простые правила:

- если нижеперечисленные программы инфицированный компьютер «отказывается» скачивать (вирус не пускает на сайт разработчика), то пойдите к другу с USB-носителем (флешка или диск можно) и скачайте всё необходимое;
- если у вас нет флешки и друга рядом с интернетом, то попытайтесь связаться с любым другом дистанционно (например,через телефон, ICQ ,Skype и т.д.), чтобы все программы, что ниже описаны он вам передал посредством связи (например, через ICQ ,Skype и т.д) или же «залил» на любой файлообменник и вам дал ссылку на скачивание, например, на http://rghost.ru/

или http://depositfiles.com/ru/ ....

Расмотрим наиболее популярные программы по удалению вирусов, которые не будут конфликтовать с вашим антивирусом!

Ваш антивирус + антишпион

Для начала просканируйте ваш компьютер уже установленными антивирусными ПО, а именно антивирусом и антишпионом. Возможно, что они вам помогут и ничего не нужно будет скачивать.

Dr.Web CureIt!

Итак,переходим по этой ссылке - http://www.freedrweb.com/
В правом верхнем углу будет Скачайте Dr.Web CureIt! бесплатно, кликаем на на эту надпись,ставите галочку на Я принимаю условия Лицензионного Соглашения и ПРОДОЛЖИТЬ. Скачали, для удобства перенесите эту утилиту на Рабочий стол. Кликните 2 раза по ней - запускаем утилиту. Сначало утилита начнет сканировать

автоматически в БЫСТРОМ РЕЖИМЕ (это займёт примерно 40 мин). Если нашёлся вирус - следуйте за указаниями утилиты (удаляем вирус).
Независимо от того, нашла ли утилита CureIt! вирусы при БЫСТРОМ РЕЖИМЕ, ставим затем на ПОЛНАЯ ПРОВЕРКА, которая может длиться 3...4....5..часов, взависимости от количества файлов на вашем компьютере. Для удобства - если вам надо отлучиться от компьютера, то ставим утилиту на ПАУЗУ , а компьютер в СПЯЩИЙ РЕЖИМ.
По окончании сканирования в ПОЛНОМ РЕЖИМЕ при нахождении вирусов - удаляем их (утилита сама вам подскажет).
Если при сканировании работа утилиты неожиданно обрывается, тухнет экран, выключаеатся компьютер самопроизвольно, то не прекращайте попытки сканировать (еще минимум три попытки), если ни в какую не сканируется, то тогда сканируйте в БЕЗОПАСНОМ РЕЖИМЕ вашего компьютера!

Как включить БЕЗОПАСНЫЙ РЕЖИМ компьютера?

Когда скачали утилиту CureIt! - выключите компьютер - подождали 3-5 минут - включаем компьютер - при загрузке компьютера жмём клавишу **F8** - выбираем БЕЗОПАСНЫЙ РЕЖИМ - запускаем CureIt! и сканируем компьютер – после сканирования и удаления вирусов перезагружаем компьютер.

Kaspersky Virus Removal Tool

Заходим сюда - http://support.kaspersky.ru/viruses/avptool2010?level=2 - знакомися, читаем про эту программу и качаем то,что написано после **Дистрибутив последней версии:**на момент написания книги было: 9.0.0.722 [EXE, 63.7 MB] - вот это мы и качаем!
Скачали,опять же двойной клик мышкой, запускаем, сканируем, удаляем вирусы.
Я не стану расписывать её использование, т.к. данная утилита интуитивно понятна!

Если при сканировании работа утилиты неожиданно обрывается, тухнет экран, выключаеатся компьютер самопроизвольно, то тогда сканируйте в БЕЗОПАСНОМ РЕЖИМЕ вашего компьютера!

AVZ

О данной утилите AVZ уже писал выше, поэтому прямая ссылка на скачивание - **http://z-oleg.com/avz4.zip** **Скачали, запустили, просканировали, вирусы удалили...радуемся.**

«Откат» *Windows*

Как это банально не звучит, но вам может помочь обычный **откат системы** или же **Восстановление системы.**

Откат системы можно сделать двумя путями:

1. при загрузке компьютера жмём **F8** и выбираем **Последняя удачная конфигурация**;

2. заходим в ***пуск => все программы => стандартные => служебные => восстановление системы***.Если там появится календарь,то ставим дату на несколько дней назад или на месяц.

Если **Windows 7**: ***пуск-все программы-обслуживание-архивация и восстановление.***

AnVir Task Manager

О программе AnVir Task Manager я уже писал выше. Если вы давно не заглядывали в Автозагрузку и Процессы, то сейчас самое время туда посмотреть.

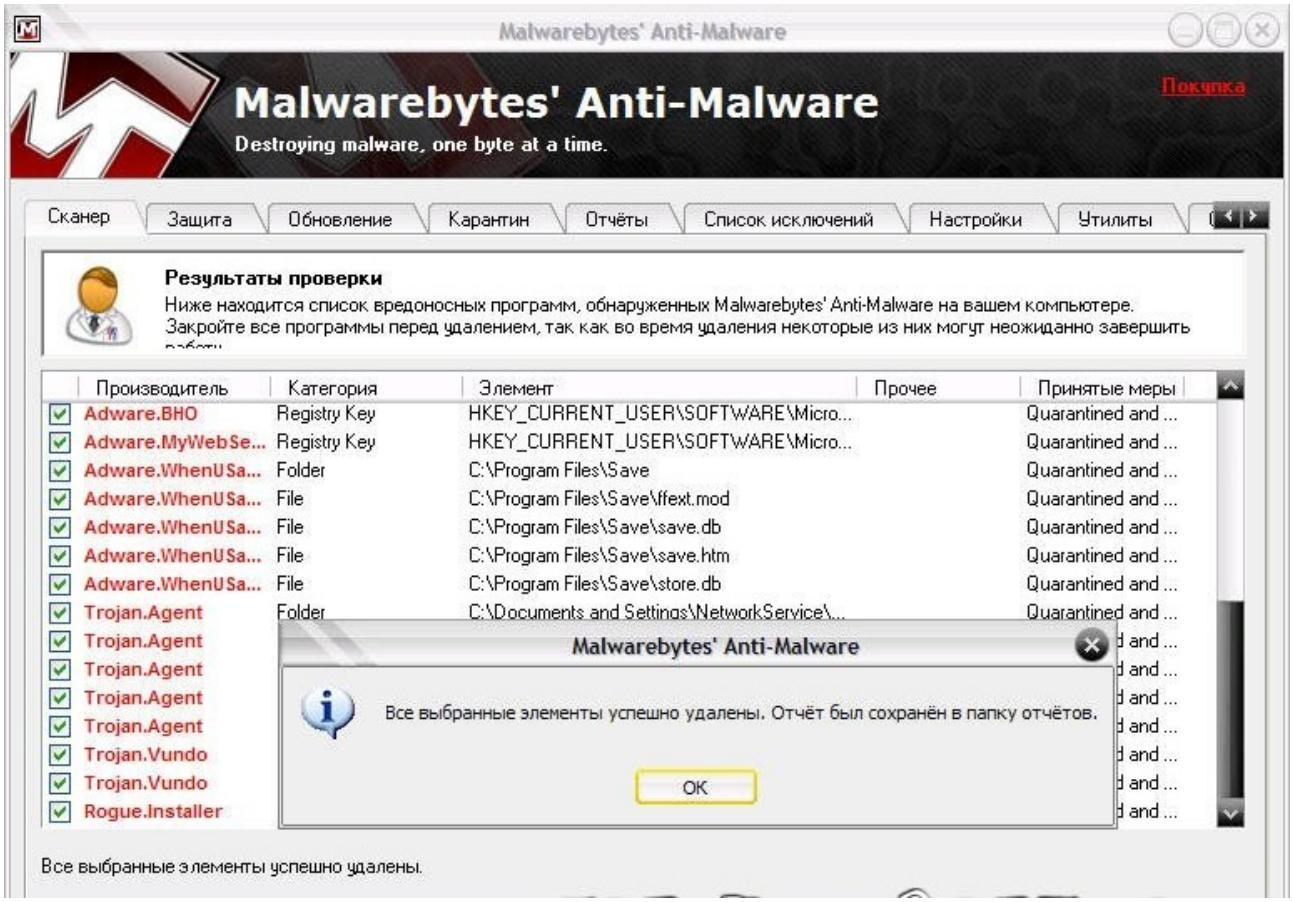
Если вы не устанавливали AnVir Task Manager, то советую установить.

О принципе работы данного софта, как «распознать» вирусы и их удаление – читаем в Разделе 1.0

Malwarebytes Anti-Malware

Одна из самых лучших убийц вирусов!
Программа очень мощная, имеет множество плюсов, но и не лишена минусов.
Объясню - программа детектит ВСЁ ПОДРЯД,ЧТО ЕСТЬ ПОДОЗРИТЕЛЬНЫМ, т.е. видит то, что не увидят антивирусы, а значит не лишена и **ложных срабатываний**!
Но, повторюсь, программа действительно уникальная и если запустите её на инфицированом ПК,то положительный результат будет на 90% в вашу пользу!...Поэтому из-за ложных срабатываний этот софт в какой-то мере есть для профессионалов, чтобы лишнее не удалить на своем ПК, в то время, как данный софт будет распознавать, что это вирусы!
Однако, ложные срабатывания примерно составляет 6-7 из 100 случаев! Как бы много, но она этого стоит!
Представляю вам программу **Malwarebytes Anti-Malware** - http://www.techspot.com/downloads/4716-malwarebytes-anti-malware.html

Скачиваем, при установке ставим на **русский язык**. Ставим сразу на **Полное сканирование**.Процесс может длиться около 40 мин (у всех будет по разному). Далее, после сканирования вам откроется окно, где **ВАМ решать,что удалять,а что оставлять!**



Тут очень важен момент - не удалить лишнее! Если будет очевидно, что это вирус и будет написано, например, Trojan-Downloader, Trojan Backdoor... или Adware и т.д., то галочку с них **не** снимаем (или же с очевидных других названий вирусов). Если вам непонятно,что хочет удалить данная программа, то «спросите» это лучше в поисковиках – просто наберите найденный результат.

Очень опасно, если предлагает что-то с реестра - но в 97% случаев программа предлагает дельное и по существу, как и по найденным угрозам.

Конечно, программа распознает все кряки ваших программ, поэтому мы их не трогаем (снимаем галочку).

После того, как мы уже определились (сняли/не сняли галочки) мы удаляем вирусы!

Если предложит перезагрузить компьютер - перезапускаем!

Кстати, если желаете можно активировать Malwarebytes Anti-Malware. Для этого нам необходим ключ. Разника между активированной и не активированной программой будет защита в

реальном времени. Но не советую вам его активировать, т.к. у вас и так неплохой арсенал уже имеется, а также многие пользователи жаловались, что программа сильно грузит систему. От вас всего лишь требуется её установить и она всегда будет под рукой – в любой момент мы кликаем правой кнопкой мышки и в меню она уже будет, и таким образом мы можем проверить файл... или кликнув на ярлыке программы (или в Пуск-Все программы-Malwarebytes Anti-Malware) – мы можем просканировать компьютер на наличие угроз...предварительно обновив базы во вкладке Обновления. Но ключ активации я всё-таки выложу...вдруг пригодится кому-то:

1FF37
EA31-QN1N-XCR4-TLTK

На момент написания книги ключ был действительным!!!

Помните, что если решитесь активировать программу и она будет работать в режиме онлайн-защиты, то возможны конфликты с другими программмами по защите от вирусов. Точно не могу сказать будет ли конфликт программ,т.к. сам лично не активировал.

Спасательный диск

Когда ничего уже не помогает....когда вирус блокирует входы на сайты, где мы можем скачать ту или иную утилиту, ...когда вирус не дает запустить антивирусную утилиту..... то нам не обойтись без стороннего компьютера с интернетом.

Попросите друга или найдите компьютер с интернетом и скачайте загрузочный диск, из под которого можно будет просканировать инфицированный компьютер.

Загрузочных дисков я выбрал два, но вам нужен один из двух...или если первый не помог, то воспользуйтесь вторым. Эти загрузочные диски Dr.Web LiveCD и Kaspersky Rescue Disk.

Dr.Web LiveCD - если действия вредоносных программ сделали невозможной загрузку компьютера под управлением Windows или Unix, восстановите работоспособность пораженной системы бесплатно с помощью Dr.Web LiveCD, который поможет не только очистить компьютер от инфицированных и подозрительных файлов, но и скопировать важную информацию на сменные носители или другой компьютер, а также попытается вылечить зараженные объекты: http://www.freedrweb.com/livecd/how_it_works/

Kaspersky Rescue Disk - предназначен для проверки и лечения зараженных x86 и x64-совместимых компьютеров. Программа применяется при такой степени заражения, когда не представляется возможным вылечить компьютер с помощью антивирусных программ или утилит лечения (например, Kaspersky Virus Removal Tool), запускаемых под управлением операционной системы. При этом эффективность лечения повышается за счет того, что находящиеся в системе вредоносные программы не получают управления во время загрузки операционной системы:
http://support.kaspersky.ru/viruses/rescuedisk?level=2
если возникли трудности, то смотрим сюда:
http://support.kaspersky.ru/viruses/rescuedisk

ВНИМАНИЕ!!! Если по каким-то причинам (поломка CD/DVD-привода или вирус не «пускает») вы не можете загрузить загрузочный диск CD/DVD , то попробуйте записать Kaspersky Rescue Disk на USB-носитель и загрузить с него компьютер:
http://support.kaspersky.ru/faq/?qid=208638405

Если ничего не помогает, то попробуйте «спросить» у поисковика Google о своей проблеме, например, какае-то ошибка (номер ошибки) или появились файлы с определенным названием.....

Для большей безопасности сканируйте 1 раз в месяц компьютер антивирусными утилитами AVZ или Malwarebytes Anti-Malware, а также не забываем про свой антивирус и антишпион!!!

Делаем выводы...

Вот, собственно, что я и хотел вам рассказать...Как видите ничего сверхсложного нет – вам только нужно это всё «добро» настроить, а также знать несколько правил и ваша система будет в «чистоте» и порядке, а значит целы нервы и, возможно, кошелек.

Хочу еще сказать, что я нигде не видел книги типа «Безопасность для чайников», где бы по молекулам расписывалось о том, что ставить и как настраивать.Поэтому этот фактор и побудил меня написать эту книгу... а может и к лучшему, что нигде не видел подобную книгу.

Пусть я не всё написал, но, поверьте, это есть самое основное...по крайней мере я так считаю..... Затронул действительно проблемные вопросы и кратко их разложил, без лишнего текста и отступлений, чтобы вас не томить чтением.

При копировании текста из данной книги прошу указывать источник – **«Комплексная защита от вирусов»** и автора – **Alexfedoruk**.

Все указанные ссылки не есть рекламой.

И помните, что самое главное оружие против хакеров – это ваша голова, которая должна думать, а всё остальное (антивирус, фаервол и т.д.) – это дополнительные аксессуары!

Будьте здоровы Вы и Ваш компьютер!!!

Автор: Alexfedoruk

2011

*