ПРАКТИЧЕСКОЕ РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

КОМПЬЮТЕРНЫЙ ДОКТОР

Надежная и бесплатная защита вашего компьютера

Василий ХАЛЯВИН www.internethalyava.ru

КОМПЬЮТЕРНЫЙ ДОКТОР

- ✓ *Хотите иметь надёжную защиту от вирусов?*
- ✓ *Надоели всплывающие окна и баннеры с голыми тётями, и рекламой?*
- ✓ *Мечтаете оградить ребёнка от посещения опасных сайтов?*
- ✓ *Что делать, если вымогатели заблокировали компьютер, выход в Интернет, вашу страничку в социальных сетях и требуют за разблокировку денег?*
- ✓ *Хотите продолжать скачивать контент с торрент-трекеров, но делать это анонимно?*
- ✓ *Есть желание зашифровать информацию на компьютере, чтобы она была доступна только вам?*
- ✓ *Нужно гарантировано удалить файл или документ с жёсткого диска, а также надёжно затереть следы его присутствия?*
- ✓ *Как всё это сделать абсолютно бесплатно?*

Решения этих проблем и ответы на все вопросы вы найдёте в новой книге Василия Халявина (Евгения Хохрякова), автора легендарной серии книг «Халява в Интернете».

Василий Халявин

ПРАКТИЧЕСКОЕ РУКОВОДСТВО
ПОЛЬЗОВАТЕЛЯ

КОМПЬЮТЕРНЫЙ ДОКТОР

Надежная и бесплатная защита вашего компьютера

Ленинградское издательство
2011

ББК 32.81
Х17

Художественное оформление
К. Долговой

Халявин В.
Х 17 Компьютерный доктор (Компьютеру не пипец!) Надежная и бесплатная защита Вашего компьютера. Практическое руководство пользователя / В. Халявин. – СПб.: «Ленинградское издательство», 2011. – 96 с.

ISBN 978-5-9942-0724-6

Новая книга «Компьютерный доктор (Компьютеру не пипец!)» В. Халявина (Евгения Хохрякова), более известного широкому кругу читателей как Плюшев (легендарная серия книг «Халява в Интернете»), посвящена актуальным вопросам обеспечения безопасности и анонимности при работе на компьютере и использовании Интернета.

Автор рассказывает и показывает, как обеспечить надежную комплексную защиту от вирусов, используя бесплатные антивирусные программы, утилиты и «облачные» сервисы безопасности. Вы узнаете, как заблокировать всплывающие окна с рекламой и порнобаннеры. Научитесь блокировать посещение опасных и нежелательных сайтов (порно, насилие, казино и т.д.). Эпидемия заражения компьютеров вирусами-вымогателями продолжается и даже нарастает! В книге даны пошаговые инструкции, как разблокировать компьютер, выход в Интернет, страницы в социальных сетях, не платя денег мошенникам. В последнее время актуальна тема скрытного скачивания контента (фильмов, музыки, программ, книг и т.д.). Книга научит, как достигнуть анонимности в этом вопросе!

Мало незаметно для посторонних скачать контент, желательно еще, чтобы доступ к нему имели только Вы. Как надежно зашифровать данные на компьютере очень подробно изложено в новой книге. Вы также узнаете, как при необходимости быстро и полностью без следов удалить («затереть») с компьютера информацию и файлы, да так надежно, что ее будет невозможно прочитать, даже используя специальные программы. Как всегда подача материала в книге рассчитана на обычного пользователя. АКТУАЛЬНОСТЬ, ПРОСТОЙ ПОНЯТНЫЙ ЯЗЫК, ИЛЛЮСТРАЦИЯ КАЖДОГО ШАГА – ЭТО ОСНОВА ПОПУЛЯРНОСТИ КНИГ ВАСИЛИЯ ХАЛЯВИНА!

ББК 32.81

ISBN 978-5-9942-0724-6

Эффективная схема бесплатной защиты компьютера

В этом разделе книги я ознакомлю Вас с эффективной схемой защиты компьютера при помощи бесплатных антивирусных и антишпионских программ, «облачных» сервисов, межсетевых экранов и различных антивирусных утилит.

Существует мнение, что бесплатная защита уступает по эффективности платной. Это не так!

Приведу пример тестирования ряда популярных антивирусных программ как платных, так и бесплатных. Для эксперимента были выбраны следующие антивирусные программы:

1. **Microsoft Security Essentials (бесплатная);**
2. **Avira AntiVir Personal (бесплатная);**
3. **Avast! Home Antivirus (бесплатная);**
4. **Kaspersky Anti-Virus 2010 (платная);**
5. **ESET NOD32 (платная).**

Для тестирования эффективности защиты использовалась база из более 16 тысяч вредоносных кодов (трояны, бэкдоры, эксплоиты, шпионские программы, черви и др.). Результаты доказали, что хорошая антивирусная программа не обязательно должна быть платной.

1. **Microsoft Security Essentials**, обнаружил 14 тысяч образцов.

2. **Avira AntiVir Personal**, обнаружил 15 тысяч образцов.

3. **Kaspersky Anti-Virus 2010**, обнаружил чуть менее 15 тысяч образцов, при этом сканирование заняло около 4 часов!

4. **Avast! Home Antivirus**, показал самые лучшие результаты. Сканирование заняло всего 8 минут, и при этом он обнаружил 15 305 образцов.

5. **ESET NOD32**, у этой антивирусной программы самые плачевные результаты. Он обнаружил всего 7600 образцов. Справедливости ради нужно сказать, что после перенастройки образцов на мгновенное инфицирование операционной системы его эф-

фективность повысилась в разы. Но скорость сканирования катастрофически упала.

Вы можете возразить, что многие бесплатные антивирусные программы не могут похвастаться дополнительными опциями, обеспечивающими защиту от угроз, которые могут попасть на ваш компьютер другими путями – с помощью скрытой загрузки файлов, электронной почты или скриптов и т.д. Но дело в том, что защиту от данных угроз можно обеспечить другими дополнительными бесплатными программами. Плюс, я намеренно оставил на «сладкое» информацию о новом революционном направлении в вопросе защиты компьютера – «облачных» антивирусных сервисах.

«Облачные» антивирусные сервисы – это то, что в конце концов заменит антивирусное программное обеспечение. И вот почему. В последнее время идет непрерывное и стремительное увеличение количества вредоносных программ. Об этом убедительно говорит отчет **«Лаборатории Касперского»**. За 15 лет (1992– 2007 годы) сотрудники «лаборатории» обнаружили около двух миллионов вирусных программ. За один только 2008 год было обнаружено уже 15 миллионов, а в 2009 году, страшно даже представить, почти 34 миллиона! Геометрическая прогрессия. При таком росте «вредоносов» не за горами критическая *временна́я* точка, когда компьютер просто «захлебнется», его вычислительных ресурсов просто не хватит для работы антивирусной программы, использующей синатурный анализ. Лет через пять вирусная база любой традиционной программы будет занимать объем около 1 гигабайта! Каждый раз при обновлении вирусной базы (а это у хорошей антивирусной программы происходит 3–4 раза в день) нужно будет скачивать сотни мегабайт новых антивирусных синатур!

Как Вы понимаете, дальнейшее развитие традиционных антивирусных программ – это тупик. Выходом из этой тупиковой ситуации является использование для защиты компьютера «облачных» антивирусных сервисов.

Как это работает? Идея очень проста и чрезвычайно эффективна. «Облачный» антивирус состоит из двух частей – клиентской и серверной. Клиентская часть установлена на компьютере пользователя и имеет минимальный размер. Эта часть содержит движок. Движок сканирует данные и отправляет для анализа, причем не сами файлы, а лишь контрольные суммы файлов (так называемый хеш) на сервер. На сервере (а не на компьютере пользователя!) содержится база синатур (вирусная база). Сер-

вер, получив хеши файлов, ищет аналоги в своей вирусной базе. Если вредные программы будут обнаружены, то сервер отправляет на компьютер пользователя скрипты (специальные команды), при выполнении которых компьютер очищается от «зловредов». Использование «облачного» антивируса:

1. Сильно разгружает процессор компьютера.

2. Дает возможность не обновлять вирусную базу (она находится на сервере).

3. Обеспечивает наилучшую защиту, основанную на так называемом коллективном разуме. Миллионы компьютеров, подключенных к «облачному» антивирусу, ежесекундно отправляют информацию о новых угрозах для автоматического обнаружения и классификации новых видов вредоносных программ.

Кстати, плюсы «облачных» антивирусов прекрасно понимают и уже, правда лишь частично, используют для своих продуктов компании разработчики «Лаборатория Касперского», ESET, Symantec, Agnitum, F-Secure, Alwil Software и другие.

Полностью «заточены» под «облака» пока лишь три сервиса: Panda Security, Immunet, фирма Prevx. Продукты двух последних пока в зачаточном состоянии и интересны лишь для тестирования. Panda Security продвинулась в этом вопросе дальше других. И на сегодняшний день является самой надежной. Мой личный опыт пользования Panda Cloud Antivirus, бесплатного продукта этой компании, уже полгода. При совместном пользовании с другими дублирующими программами (например, использование дополнительного, не конфликтующего с ним антивируса) и дополняющих бесплатных антивирусных сервисов и утилит результат просто впечатляет, ни одного прокола!

Ну вот мы и подошли к главному, списку бесплатных программ и «облачных» сервисов, которые я рекомендую использовать для комплексной и эффективной защиты Вашего компьютера.

Комплексная бесплатная защита Вашего компьютера

1. Прежде всего, нужно установить основную антивирусную программу. Надеюсь, я убедил Вас в том, что за «облачной» антивирусной защитой будущее. Так что выбираем действительно лучшее на данный момент – «облачный» антивирус Panda Cloud Antivirus.

2. Как бы ни был хорош антивирус Panda Cloud Antivirus, всегда есть угроза все-таки пропустить на компьютер какого-нибудь «представителя» вредоносного ПО. Снизить угрозу можно, установив на компьютер вторую антивирусную программу, которая не будет конфликтовать с основной. Рекомендую антивирус **IObit Security 360**. Он защищает компьютер от различного вредоносного ПО (шпионов, кейлоггеров, рекламного ПО, троянов, червей и т.п.), обнаруживает и удаляет его.

В **IObit Security 360** используется «Dual-Core» – движок с эвристическим анализатором. Крайне положительным качеством **IObit Security 360** является то, что программа не конфликтует с другими установленными в системе антивирусами. Его можно установить, не удаляя уже установленный. Зачем это нужно? У антивирусных программ различные принципы поиска вредоносных программ. Если пропустит один, то второй может их обнаружить. Например, при тестировании IObit Security обнаружил целых 84 шпиона, трояна и т.д., которые пропустил установленный Avast Home.

3. Межсетевой экран, его еще называют брандмауэр или firewall («огненная стена») – это такая система, которая предназначена для защиты компьютера или сети компьютеров, подключенных к Интернету, от несанкционированного доступа, а также для блокирования опасного входящего или исходящего трафика. Перевод слова firewall – капитальная стена, разделяющая разные здания или одно здание для предотвращения распространения пожара. Межсетевой экран представляет собой специальное программное обеспечение. Оно фильтрует данные, проходящие из Интернета и в обратном направлении. Например, межсетевой экран блокирует трафик от вредоносных программ (вирусов, троянских программ, программ Backdoor). Межсетевой экран может фильтровать или отслеживать содержимое передаваемых данных.

Брандмауэр – это необходимый элемент в комплексной защите Вашего компьютера.

Операционная система Windows уже имеет встроенный межсетевой экран. Но при тестировании независимыми экспертами он показал не очень хорошие результаты. Так какой выбрать? Не рекомендую платные, парадокс заключается в том, что они показали при тестировании худшие результаты, чем бесплат-

ные. А лучшие показатели – у бесплатной **PC Tools Firewall Plus**. Вот ее-то я и рекомендую.

4. Еще одним обязательным приложением, которое необходимо иметь на компьютере, является так называемая антишпионская программа.

Люди, думающие, что у них нет секретов на компьютере и что они неинтересны другим, глубоко ошибаются! Возможно, вы действительно неинтересны силовым структурам или крупным мошенникам. Но только представьте, сколько в Интернете молодых и не очень «дебилов-псевдохакеров», которых хлебом не корми – дай «полазить» по чужим компьютерам, чтобы заполучить хранящуюся у Вас на компьютере информацию, например хранящиеся у вас логин и пароль того же сайта «Одноклассники» или «ВКонтакте». Не установив антишпионскую программу, потом не удивляйтесь тому, что какой-то «хрен» («сорри» за грубость, по-другому его и не назовешь) от Вашего имени отправляет друзьям сообщения типа «пришли СМС-ку на номер такой-то. Там для тебя "супер-пупер"! Не отправишь – утоплюсь!». Грешим на ненадежность сайта и продажность модераторов и в последнюю очередь виним «себя любимого». А утечка информации могла произойти из-за Вашей беспечности и потому, что не установили в свое время на компьютер антишпионскую программу. Ведь попадают они на ваш компьютер посредством шпионских программ. Шпионское программное обеспечение (spyware) – это программы-шпионы, которые незаметно для вас размещаются на вашем же компьютере, чтобы контролировать и сообщать о действиях пользователя. Они стали настоящим бичом Интернета. Учитывая, какой вред хакеры могут нанести компьютерам и безопасности данных пользователя, вопрос о том, есть ли необходимость в использовании антишпионского ПО, уже не стоит. Важно получить по возможности максимальную защиту.

Рекомендую использовать бесплатное антишпионское программное обеспечение, возможностей которого для обычного пользователя вполне достаточно! Таких программ много. Это, например, всем известная программа **Ad-Aware** или тоже хорошая и стабильная **Spybot – Search and Destroy**. Если выберите их, информацию об установке, настройке и пользовании найдете на моем сайте **http://internethalyava.ru** в разделе «Безопасность компьютера». В книге же рассмотрим лучшую, на мой взгляд, программу **Spyware Terminator**. Она нравится

мне тем, что имеет резидентный монитор, который в реальном времени проводит мониторинг системы и предотвращает попытки проникновения на компьютер вредоносного программного обеспечения. Имеющийся в программе сканер поможет отыскать и поместить в «каратин» или удалить уже внедренные объекты. В программу также включен модуль защиты от вирусов (ClamAV). Кроме того, работает программа очень быстро.

5. Все пользователи Интернета сталкиваются с таким раздражающим фактором, как всплывающие окна (баннеры) и навязчивая реклама. Баннеры, вызывающие самопроизвольное открытие порносайтов, могут повредить вашей репутации на работе или оказать негативное влияние на детей дома. Подобная реклама зачастую используется для мошенничества и распространения вирусов и вредоносных программ. Например, последняя волна заражения компьютеров троянцами-вымогателями, требующими для разблокировки входа в систему отправить мошенникам платное СМС-сообщение, происходило при попытке закрыть порнобаннер. Нажимая на крестик закрытия окна, пользователи запускают установку троянца на компьютер. Существует возможность блокировки баннеров. Это можно сделать настройкой браузера. Но самый простой способ, особенно для простых пользователей, которым некогда разбираться с настройками, это установить замечательную бесплатную программу **AdGuard**. Программа блокирует бóльшую часть порнорекламы и рекламы сайтов сомнительного содержания. Программа не требует дополнительных настроек. Просто скачайте и установите программу – все остальное будет настроено автоматически. Программа работает в Opera, Internet Explorer, Firefox и других браузерах. Программа адаптирована под русскую часть Интернета (Рунет).

6. Еще одним отличным инструментом защиты Вашего компьютера является «облачный» сервис **SkyDNS** от компании «Айдеко».

Предназначение сервиса – защитить пользователей Интернета от посещения опасных и нежелательных сайтов, ведь самая лучшая гарантия того, что вы ничего не «подхватите» – это просто не посещать опасные сайты. Сервис автоматически блокирует сайты, содержащие вирусы, угрозы безопасности. Также блокируются фишинговые сайты. Фи́шинг (англ. phishing, от fishing – рыбная ловля, выуживание) – вид интернет-моше-

ничества, целью которого является получение доступа к конфиденциальным данным пользователей – логинам и паролям. Раньше задачу блокировки нежелательных сайтов решало специализированное ПО, за которое нужно было платить. SkyDNS – это совершенно бесплатное решение данных задач! Кроме того, за счет того, что это «облачный» сервис, хранится рабочая база опасных ресурсов не у Вас на компьютере, а на сервисе. Причем рабочие базы опасных ресурсов обновляются в режиме реального времени – это позволяет повысить уровень защиты от новых угроз.

На сегодняшний день это единственный в России (аналогов в мире много) бесплатный «облачный» сервис фильтрации Интернета.

Конечно, например, можно заблокировать вручную посещение того или иного сайта прямо в браузере, но, к сожалению, опасных ресурсов миллионы! В поисковиках в строке ссылки на сайт тоже можно найти предупреждение об опасности посещения. Ну, а если Вы просто кликнули ссылку на каком-нибудь форуме? Где гарантия, что человек, разместивший ее, не «редиска»? То-то и оно...

Так что советую использовать возможности SkyDNS.

7. Ну и последним средством эффективной и при этом абсолютно бесплатной защиты Вашего компьютера станет антивирусная утилита **AVZ**. Многим опытным пользователям известна эта антивирусная утилита. Разработана программа Олегом Зайцевым, программистом от бога. Он создавал ее по принципу «если хочешь, чтобы что-то было сделано хорошо – сделай это сам». Олег изначально создавал AVZ для выявления вредных программ (вирусов) в корпоративной сети одной крупной компании. В ходе работ он решил сделать алгоритм выявления вредоносных программ более универсальным. И ему это удалось!

Оговорюсь сразу, AVZ не является полноценной антивирусной программой, заменой вашему основному антивирусу она не станет (утилита не лечит сами программы, зараженные компьютерными вирусами). AVZ «заточена» в основном на исследование и восстановление системы, а также на поиск и удаление (есть и ручное и автоматическое): spyware, adware – программ и модулей (это одно из основных назначений утилиты), руткитов и вредоносных программ, маскирующих свои процессы, сетевых и почтовых червей, троянских программ (включая все их разновидности, в частности Trojan-PSW, Trojan-Downloader, Trojan-Spy) и Backdoor (программ

для скрытного удаленного управления компьютером), троянских программ-звонилок (Dialer, Trojan.Dialer, Porn-Dialer), клавиатурных шпионов и прочих программ, которые могут применяться для слежения за пользователем. И справляется с этими задачами на пять баллов!

Итак, для полной комплексной и эффективной защиты компьютера рекомендую следующие бесплатные программы и сервисы:

1. «Облачный» антивирус **Panda Cloud Antivirus**.
2. Второй дополнительный антивирус **IObit Security 360**.
3. Межсетевой экран **Jetico Personal Firewall**.
4. Антишпионская программа **Spybot – Search and Destroy**.
5. Блокировщик баннеров и рекламы **Нетчарт Фильтр**.
6. Блокировщик посещения нежелательных сайтов «облачный» сервис **SkyDNS**.
7. Антивирусная утилита **AVZ**.

В следующих главах этого раздела перейдем к более подробному знакомству с данными программами и сервисами. Как всегда подойдем к этому вопросу основательно. Популярность моих книг и основывается на этом – доступно и поэтапно, с иллюстрацией каждого шага, показать пользователям, как скачать, установить, настроить и пользоваться предложенными сервисами и программами.

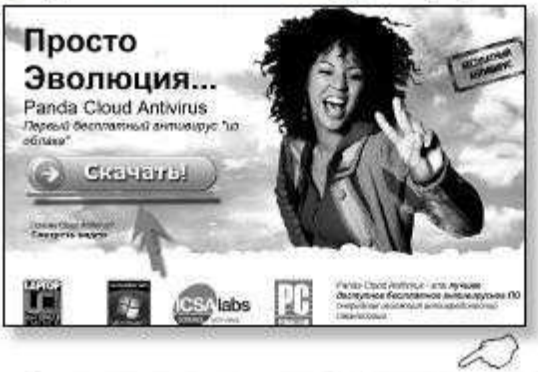
Panda Cloud Antivirus – первый в мире бесплатный «облачный» антивирус

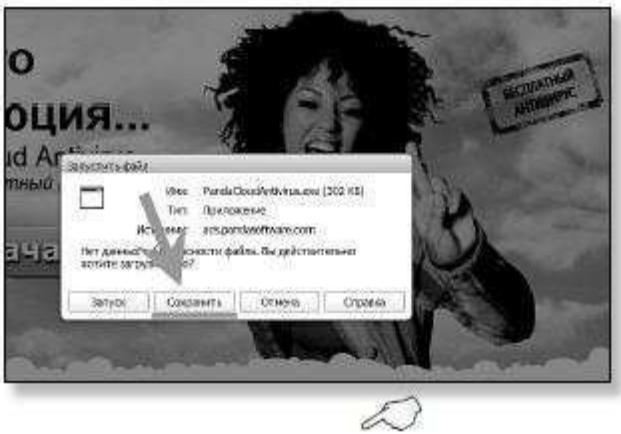
Panda Cloud Antivirus – это революция в области антивирусной защиты. Работа этого антивируса основана на защите компьютера с сервера Panda в режиме реального времени. Panda Cloud Antivirus имеет бóльшие преимущества по сравнению с традиционными антивирусными программами. Он загружает процессор на 50 процентов меньше, чем обычный антивирусник. Panda Cloud Antivirus объединяет локальный и удаленный антивирус, антишпион, антируткит, эвристическую проверку и хэширование невредоносного ПО (goodware), при этом использует всего 17 МБ оперативной памяти.

Сервис Panda Cloud Antivirus сочетает локальные технологии обнаружения вредоносных программ с проверкой объектов

на удаленных серверах. В результате «коллективный разум» имеет возможность использовать информацию, которую серверы получают от миллионов пользователей продуктов Panda Security по всему миру, что делает процесс автоматического обнаружения и классификации новых видов вредоносных программ более эффективным.

Для скачивания Panda Cloud Antivirus заходим на сайт **http://internethalyava.ru/** в раздел «Безопасность компьютера», далее – «Бесплатные антивирусные программы».





Запускаем установку антивируса.

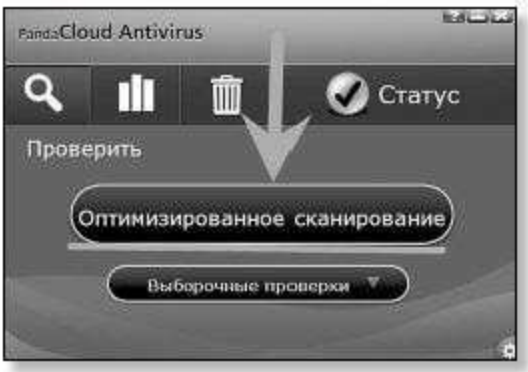
Антивирус установлен. Перезагружаем компьютер.

В процессе использования антивируса может появиться окно с предложением перейти на новую профессиональную версию. Откажитесь (просто закройте окно с предложением). Бесплатной версии вполне достаточно для защиты Вашего компьютера.

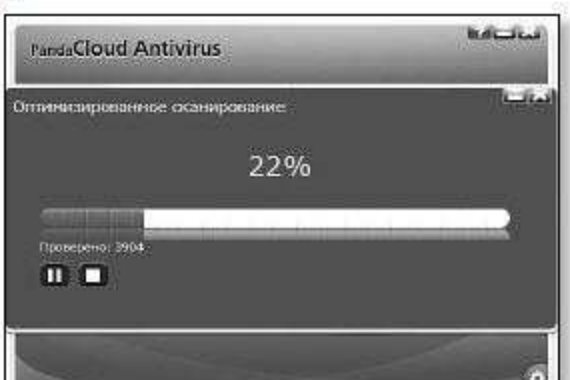
В правом нижнем углу экрана рядом с часами появилась иконка – голова медвежонка панды. Работает антивирус по принципу «установил и забыл». Защита происходит автоматически.

Можно просканировать компьютер для выявления угроз, которые могли возникнуть до его установки. Для этого кликните левой кнопкой мышки по значку программы в правом нижнем углу экрана монитора (рядом с часами). Откроется окно антивируса. Затем кликните по значку в виде лупы.

Далее кликайте «Оптимизированное сканирование».



Антивирус просканирует компьютер и устранит угрозы без Вашего участия. После сканирования Вы увидите отчет с результатами.



Panda Cloud Antivirus – это действительно лучшее решение по защите Вашего компьютера. Для двойной защиты устанавливаем дополнительную, и тоже бесплатную антивирусную программу **IObit Security 360**, подробней об этом в следующей главе.

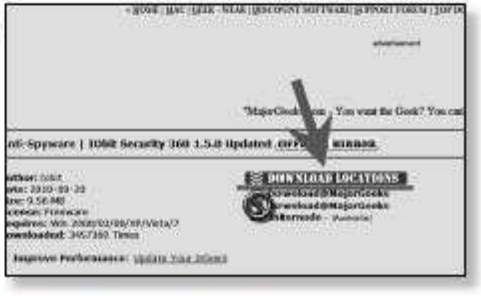
IObit Security 360 – второй дополнительный антивирус

IObit Security защищает компьютер от различного вредоносного ПО (шпионов, кейлоггеров, рекламного ПО, троянов, червей и т.п.). Обнаруживает и удаляет его.

В IObit Security используется «Dual-Core» – движок с эвристическим анализатором. Эвристический анализатор позволяет обнаруживать вредоносные коды в исполняемых файлах, секторах и памяти, а также новые скрипт-вирусы и вредоносные программы для Microsoft Office и других программ, использующих VBA, и, наконец, вредоносный код, написанный на языках высокого уровня.

Еще одним положительным качеством IObit Security 360 является то, что программа не конфликтует с другими установленными в системе антивирусами (вот это качество мы и будем использовать для усиления защищенности нашего компьютера). Зачем это нужно? У антивирусных программ различные принципы поиска вредоносных программ. Если пропустит один, то второй может их обнаружить. Например, при тестировании IObit Security обнаружил целых 84 шпиона, трояна и т.д., которые пропустил неплохой основной Avast Home.

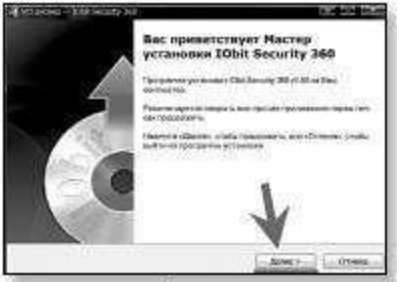
Скачиваем установочный файл на сайте **www.halyavin.ru** в разделе «Бесплатные программы».



Запускаем установку антивирусной программы.

1

2


Вас приветствует Мастер
установки IObit Security 360
Далее >
Отмена

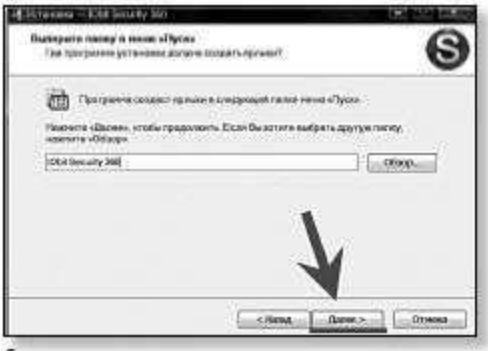
3


Лицензионное Соглашение
END-USER LICENSE AGREEMENT FOR IObit Security 360
IMPORTANT PLEASE READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE CONTINUING WITH THIS PROGRAM INSTALL: IObit End-User License Agreement ("EULA") is a legal agreement between you (either an individual or a single entity) and IObit. for the IObit software product(s) identified above which may include associated software components, media, printed materials, and "online" or
< Назад
Далее >
Отмена

4


Выбор папки установки
Программа установит IObit Security 360 в следующую папку.
C:\Program Files\IObit\IObit Security 360
Обзор...
< Назад
Далее >
Отмена

5


Выберите папку в меню «Пуск»
Где программа установки должна создать ярлыки?
Программа создаст ярлыки в следующей папке меню «Пуск».
Нажмите «Далее», чтобы продолжить. Если Вы хотите выбрать другую папку, нажмите «Обзор».
IObit Security 360
Обзор...
< Назад
Далее >
Отмена

6


Выберите дополнительные задачи
Какие дополнительные задачи необходимо выполнить?
Выберите дополнительные задачи, которые должны выполняться при установке IObit Security 360, после этого нажмите «Далее».
Дополнительные значки:
Создать значок на Рабочем столе
Add IObit to My Favorites
< Назад
Далее >
Отмена

7


Всё готово к установке
Программа установки готова начать установку IObit Security 360 на Ваш компьютер.
Нажмите «Установить», чтобы продолжить, или «Назад», если Вы хотите просмотреть или изменить опции установки.
Папка установки:
C:\Program Files\IObit\IObit Security 360
Папка в меню «Пуск»:
IObit Security 360
Дополнительные задачи:
Дополнительные значки:
Создать значок на Рабочем столе
Add IObit to My Favorites
< Назад
Установить
Отмена

8

9

Программа установлена.

Рекомендую для удобства установить русский язык интерфейса. Для этого в окне программы кликаем кнопку «Настройки».

Далее – «User Interface».

И выбираем в меню русский язык.

Пользоваться программой очень просто. Помимо постоянной защиты можно также делать ручное сканирование. В программе предусмотрены дополнительные инструменты. Все интуитивно понятно, а это еще один немаловажный плюс для пользователей, особенно для начинающих.

PC Tools Firewall Plus – отличный и бесплатный межсетевой экран

PC Tools Firewall Plus занимает первые места по скорости работы и степени защиты, обгоняя таких известных конкурентов, как Outpost, Look'n'Stop, Zone Alarm Pro, Norton, KIS6, Kerio.

Контролируя работу различных приложений, Firewall Plus пресекает попытки троянов, бэкдоров, клавиатурных шпионов и прочих вредоносных программ нанести ущерб компьютеру и похитить вашу конфиденциальную информацию.

Передовая технология PC Tools Firewall Plus была специально разработана таким образом, чтобы программой могли пользоваться не только специалисты, но и рядовые пользователи. Мощная защита от атак и вредоносных программ активируется по умолчанию. Все, что вам нужно сделать – это инсталлировать программу, и ваш компьютер немедленно окажется под постоянной защитой. Опытные пользователи могут также создавать свои собственные усложненные правила фильтрации пакетов, включая поддержку IPv6, чтобы настроить сетевую защиту по своему усмотрению.

Но, внимание! Если Вы абсолютный новичок и не особо разбираетесь в основах работы с протоколами, портами и т.д., советую все-таки отказаться от самостоятельных настроек правил.

Приступаем к установке PC Tools Firewall Plus. Скачиваем программу в разделе «Бесплатные программы» на сайте **http://halyavin.ru/**.

Программа скачана. Запускаем установку программы.

1

2

3

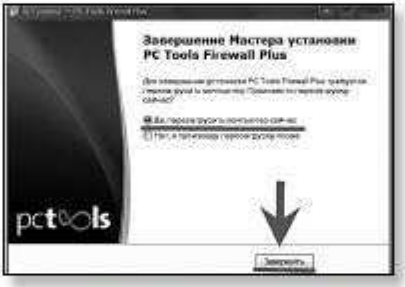
4

5

Отказываемся от установки Spyware Doctor. Программа хоть и хорошая, но платная. Установим другую, не менее эффективную, но бесплатную (об этом в следующей главе).

Выбираем режим для обыкновенного пользователя.

Программа установлена. Перезагружаем компьютер.



После перезагрузки и при первом автоматическом включении межсетевого экрана начнут появляться окна с предупреждениями о подключении тех или иных программ к Интернету. Если вы неопытный пользователь, разрешите подключение всем программам. В дальнейшем при появлении таких окон анализируйте по названию новой программы, не является ли она вредоносной. Если не уверены, совет: забейте название неизвестной программы в любой поисковик и наверняка найдете о ней всю информацию.

Бесплатная антишпионская программа Spyware Terminator

Spyware Terminator – программа для защиты компьютера от различных вредоносных программ – spyware, adware, кейлоггеров и других троянов.

Программа имеет резидентный монитор, который в реальном времени проводит мониторинг системы и предотвращает попытки проникновения на компьютер вредоносного программного обеспечения. Имеющийся в программе сканер поможет отыскать и поместить в «карантин» или удалить уже внедренные объекты. Кроме этого в программу включен модуль защиты от вирусов (ClamAV). Работает программа очень быстро.

Основные особенности Spyware Terminator:

1. Расширенная локальная база данных – обнаруживается в 3 раза больше шпионских программ.

2. Повышенная скорость работы.

3. Добавлены расширения InternetExplorer & FileExtensionShield.

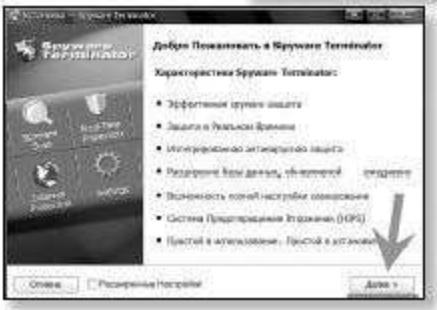
4. Улучшенный интерфейс.

Скачиваем программу в разделе «Бесплатные программы» на сайте **http://halyavin.ru/**. Новичкам – не пугаться, что ссылка там на англоязычный сайт, «скачается по-русски».

Программа скачана. Запускаем установку программы.

1

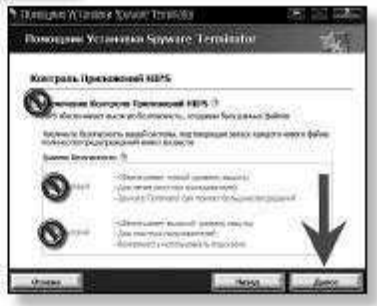
2



3

4

5



6

Начнется загрузка компонентов программы. Процесс длительный. Запаситесь терпением. После загрузки кликаем кнопку «Далее».

Программа установлена. Переходим к настройкам. При первом запуске откроется окно, где выбираем второй пункт.

После настроек откроется основное окно программы. Вам будет предложено просканировать компьютер на наличие вредоносных программ, – соглашайтесь. Причем сканирование будет происходить потом ежедневно.

Вот мы и ознакомились с еще одной программой в системной бесплатной защите вашего компьютера.

Программа AdGuard: забудь про порнобаннеры и рекламу!

Вас еще не достали при посещении сайтов всплываю щие окна с голыми тетями и другой гадостью? Нет? Тогда не читайте эту главу.

Для всех остальных рекомендую внимательно отнестись к программе, предлагаемой к установке на персональный компьютер. Программа называется **AdGuard**.

Предназначение программы AdGuard – блокировка всплывающих окон (баннеров) и другой навязчивой рекламы.

Программа блокирует большую часть порнорекламы и рекламы сайтов сомнительного содержания. Баннеры, вызывающие самопроизвольное открытие порносайтов, могут повредить вашей репутации на работе или оказать негативное влияние на детей дома. Подобная реклама зачастую используется для мошенничества и распространения вирусов и вредоносных программ.

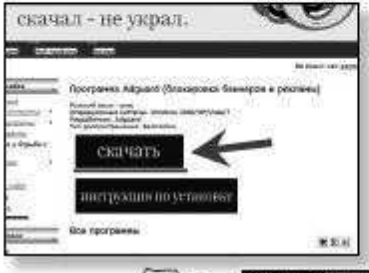
Программа имеет ряд преимуществ перед подобными программами.

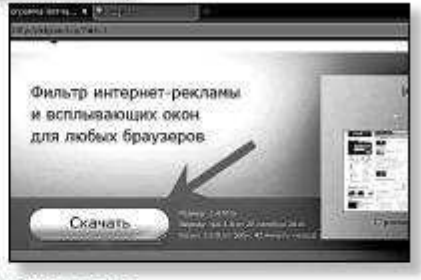
1. Программа не требует дополнительных настроек. Просто скачайте и установите программу – все остальное будет настроено автоматически.

2. Программа работает в Opera, Internet Explorer, Firefox и других браузерах.

3. Программа адаптирована под русскую часть Интернета (Рунет).

Скачать программу можно в разделе «Бесплатные программы» на сайте **http://halyavin.ru/**.



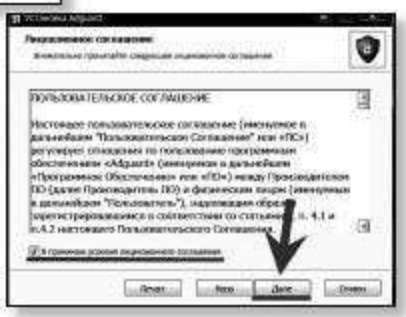


Запускаем установку программы.

Дождитесь загрузки установщика программы.

Далее действуйте, как показано на скриншотах (фотографиях экрана) ниже.

1



2

3

4

5

Программа установлена. Это бесплатная программа из категории «установил и забыл». Работает без участия пользователя, блокируя большинство баннеров и навязчивой рекламы. После установки программы Вы реально увидите результат (а точнее, не увидите всплывающие окна). Вот, например, результат работы программы – всего за 2 часа работы в Интернете было заблокировано **915** (девятьсот пятнадцать!) рекламных сообщений и всплывающих окон.

Еще одним плюсом программы является ее ежедневное обновление!

Бесплатный пробный период программы (14 дней) легко продлить, получив бесплатный ключ, – для этого нужно подключить четырех друзей. Более подробно – на сайте программы. Даже если не успеете за пробный период подключить четырех друзей, просто удалите программу и установите вновь. Можно в принципе и обойтись без этой программы, а активировать функцию блокировки баннеров в уникальном «облачном» сервисе SkyDNS, о котором в следующей статье.

«Облачный» сервис SkyDNS – блокировщик посещения нежелательных сайтов

Компания «Айдеко» открыла «облачный» сервис SkyDNS. Предназначение сервиса – защитить пользователей Интернета от посещения опасных и нежелательных (категории можно самостоятельно задать в настройках) сайтов. Сервис автоматически блокирует сайты, содержащие вирусы, угрозы безопасности. Также блокируются фишинговые сайты. Фи́шинг (англ. phishing, от fishing – рыбная ловля, выуживание) – вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей – логинам и паролям.

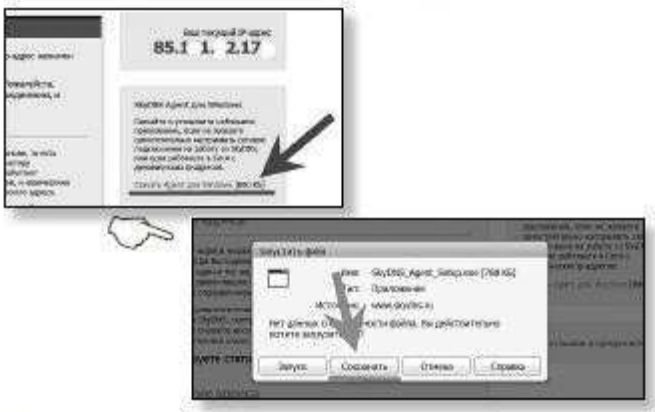
Это уникальный фильтр сайтов! Его можно настроить под индивидуальные запросы любого пользователя. Существуют специальные платные программы, которые предназначены для выполнения этой задачи. SkyDNS – «облачный» сервис, выполняющий эту работу совершенно бесплатно. Сервис делает пользование Интернетом гораздо безопаснее. Причем рабочие базы опасных ресурсов обновляются в режиме реального времени – это позволяет повысить уровень защиты от новых угроз.

На сегодняшний день это единственный в России (аналоги в мире есть, например OpenDNS **http://www.opendns.com/**) бесплатный «облачный» сервис фильтрации Интернета.

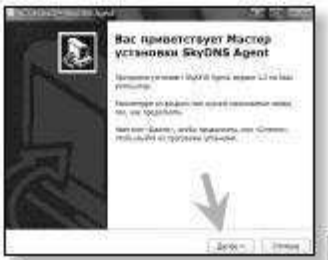
Подключиться к сервису можно на официальном сайте **www.skydns.ru/**.

Проходим регистрацию на сервисе.

После регистрации нужно настроить сетевое подключение на работу с сервисом. Можно это сделать вручную, но, если Вы недостаточно опытный пользователь или вам лениво самостоятельно заниматься настройками, советую скачать небольшую утилиту, которая автоматом перенастроит подключение.



Запускаем установку утилиты.



2

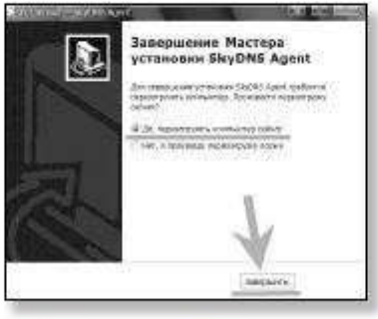
3

4

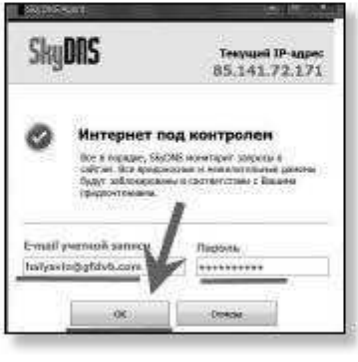
5

б

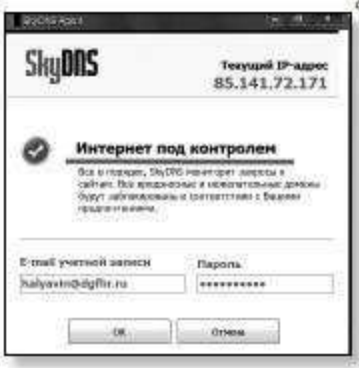
После этого перезагружаем компьютер.



При первом включении нужно будет заполнить таблицу данными, которые вы давали при регистрации.



После этого проверьте правильность работы сервиса.

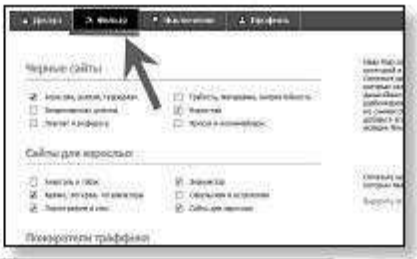


Вы самостоятельно можете изменить настройки блокировки нежелательных сайтов. Для этого заходим на сервис **www.skydns.ru/**. Заполняем форму входа в личный кабинет. Делаем индивидуальные настройки.

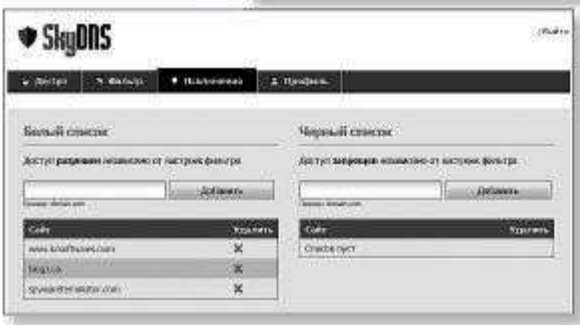
1


Настройки
Защита от фишинга
Закрыть доступ к вредоносным сайтам
Блокировать баннеры
Сохранить

2


Черные сайты
Сайты для взрослых

3


SkyDNS
Белый список
Черный список
Добавить
Удалить
Список пуст

4

При посещении нежелательных сайтов вместо их открытия появится примерно такая таблица.

Сервис действительно повышает безопасность работы в Интернете. Ведь согласитесь, что лучшая защита – это просто не посещать опасные сайты.

В дальнейшем, по словам авторов проекта, возможности сервиса будут улучшаться. Появится и форма платного обслуживания (я думаю, платная форма будет востребована организациями, она будет иметь расширенные возможности), но для обычных пользователей обещают оставить бесплатное обслуживание.

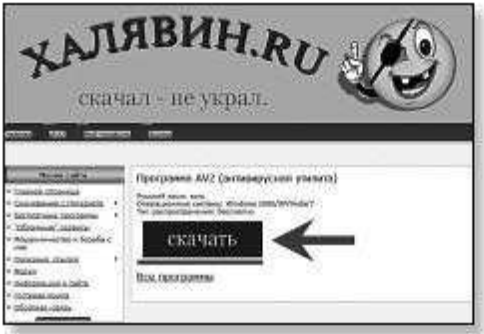
Антивирусная утилита AVZ – эффективная и надежная как танк

Многим опытным пользователям известна эта антивирусная утилита. Разработана программа Олегом Зайцевым, программистом от бога. Он создавал ее по принципу «если хочешь, чтобы что-то было сделано хорошо – сделай это сам». Олег изначально создавал AVZ для выявления вредных программ (вирусов) в корпоративной сети одной крупной компании. В ходе работы он решил сделать алгоритм выявления вредоносных программ более универсальным. И ему это удалось.

Оговорюсь сразу, AVZ не является полноценной антивирусной программой, заменой вашему основному антивирусу она не станет (утилита не лечит сами программы, зараженные компьютерными вирусами). AVZ «заточена» в основном на исследование и восстановление системы (необходима для чистки компьютера после разблокировки, например), а также на поиск и удале-

ние (есть и ручное и автоматическое): spyware, adware– программ и модулей (это одно из основных назначений утилиты), руткитов и вредоносных программ, маскирующих свои процессы, сетевых и почтовых червей, троянских программ (включая все их разновидности, в частности Trojan-PSW, Trojan-Downloader, Trojan-Spy) и Backdoor (программ для скрытного удаленного управления компьютером), троянских программ-звонилок (Dialer, Trojan.Dialer, Porn-Dialer), клавиатурных шпионов и прочих программ, которые могут применяться для слежения за пользователем. И справляется с этими задачами быстрей и лучше по сравнению с другими антишпионскими программами, например она эффективней популярной программы **Ad-Aware**.

Скачать последнюю, самую свежую версию AVZ рекомендую с сайта **http://halyavin.ru/** в разделе «Бесплатные программы».



1

2

3

Программа не требует установки. Работать с ней несложно. Со всеми возможностями можно ознакомиться на официальном сайте разработчика утилиты AVZ в разделе «Документация по работе с AVZ». Вот адрес: **http://www.z-oleg.com/secur/avz_doc/**.

Рассмотрим, как сделать общую автоматическую проверку компьютера на наличие вредоносных программ. Для начала распаковываем папку с программой (она в архиве) на рабочий стол.

В папке выбираем значок в виде меча со щитом, названный «Антивирусная утилита AVZ», и запускаем программу.

В окне программы выбираем (ставим галочки) места поиска вредоносных программ, галочку напротив «Выполнять лечение» и запускаем сканирование, кликнув на кнопку «Пуск».

После сканирования будет выведен отчет о проделанной работе: выявленных вредных процессах, а также эффективности лечения.

Это одна из лучших в своей категории программ, которую я настоятельно рекомендую иметь в арсенале всем пользователям.

Вот мы и ознакомились с комплексом бесплатных антивирусных программ и сервисов, которые дают практически стопроцентную гарантию безопасности. Перед тем как прийти к этому оптимальному комплексу мер безопасности я протестировал огромное количество программ и сервисов. Долгое время использовал (и продолжаю использовать) эту систему. Я убежден, бесплатная комплексная защита компьютера ничем не хуже платной. Но еще раз повторюсь, использовать ее нужно не частично, а применяя весь предложенный комплекс программ и сервисов.

Лечение компьютера от вирусов и разблокировка входа в социальные сети

Пошаговая инструкция восстановления, лечения компьютера от вирусов и способы разблокировки

Для начала, что такое вирус? Так уж сложилось, что вирусом называют все программы, которые заражают файлы (объектные или выполняемые) на компьютере. Вирус помещает себя в программный файл и начинает «работать» сразу, как только вы запустите зараженную программу. В настоящее время почти 100 процентов вирусов мы «ловим» в Интернете. Хотя иногда можно «поймать» его и с зараженного диска или флешки.

Разновидностей вирусов много. С большинством из них справляется хороший антивирус. А хороший – не значит платный. Существует много отличных бесплатных антивирусных программ. Из личного опыта рекомендую «облачный» антивирус Panda Cloud Antivirus Подробную информацию о нем найдете в первой части книги.

Panda Cloud Antivirus – это революция в области антивирусной защиты. Работа этого антивируса основана на защите компьютера с сервера Panda в режиме реального времени. Panda Cloud Antivirus имеет преимущество по сравнению с традиционными антивирусными программами. Он загружает процессор на 50 процентов меньше, чем обычный антивирусник. Panda Cloud Antivirus объединяет локальный и удаленный антивирус, антишпион, антируткит, эвристическую проверку и хэширование невредоносного ПО (goodware), при этом использует всего 17 МБ оперативной памяти.

Сервис Panda Cloud Antivirus сочетает в себе локальные технологии обнаружения вредоносных программ с проверкой объектов на удаленных серверах. В результате «коллектив-

ный разум» имеет возможность использовать информацию, которую сервера получают от миллионов пользователей продуктов Panda Security по всему миру, что делает процесс автоматического обнаружения и классификации новых видов вредоносных программ более эффективным.

Panda Cloud Antivirus также недавно завоевал награду от PC Magazine в категории «Выбор редактора» за Лучший бесплатный антивирус и удостоился звания лучшего антивируса для обнаружения вредоносного ПО в сравнительном обзоре PCWorld.

Но каким бы хорошим ни был антивирус, угроза заражения существует всегда. И в первую очередь это связано с отставанием разработчиков традиционных антивирусов от интернет-преступников. Известная аналитическая компания Cyveillance недавно провела тестирование самых популярных (основанных на принципе синатурного анализа) антивирусов. Тестирование показало, что они выявляют менее 20 процентов новых вредоносных программ. После месяца с момента появления новых вирусов показатель выявления и блокировки повышается до 61,7 процента. Операционный директор Cyveillance Панос Анастассиадис отмечает: «Даже спустя месяц многие разработчики не могут научить свои антивирусы обнаруживать известные атаки, что делает внедрение упреждающего подхода к обеспечению безопасности критически важным для снижения риска возможного заражения».

Всего было испытано тринадцать самых популярных традиционных антивирусов. Вот их средние показатели:

1. Новые угрозы – обнаружено 18,9 процента.

2. Через 8 дней после появления вируса – обнаружено 45,7 процента.

3. через 15 дней – обнаружено 56 процентов.

4. Через 30 дней – обнаружено 61,7 процента.

А в целом разработчикам популярных (читай – лучших) антивирусных программ требовалось для добавления нового вируса в базу в среднем 11,6 дня! При этом некоторые вредоносные приложения вообще не добавлялись в базу данных многие недели.

В данной ситуации пришло время протестировать «облачный» антивирус Panda. Несмотря на то что ему только чуть

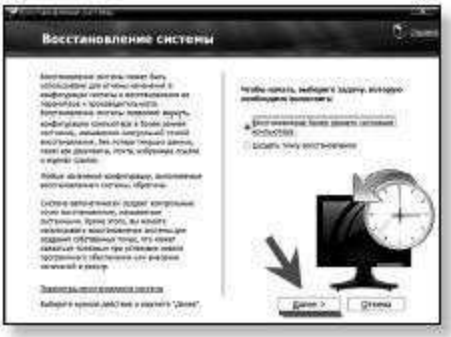
больше года, он уверенно догнал по надежности самые лучшие антивирусы. А функция обновления вирусной базы в реальном времени в связи с активизацией киберпреступников выводит его, по моему мнению, вообще на первое место. Кстати, версия для домашнего пользователя совершенно бесплатная.

Итак, что же делать, если на компьютер все-таки попал вирус? Прежде всего, не паниковать. Статистика показывает, что лишь 5 процентов разновидностей вируса несут серьезную угрозу вашему компьютеру, операционной системе. Многие вы можете месяцами просто не замечать. Для выявления и удаления большинства вирусов достаточно проводить периодически сканирование компьютера установленной антивирусной программой, причем всего компьютера, всех жестких дисков. Процесс этот, иногда очень длительный, находится в зависимости от количества файлов хранящихся на винчестере (жестком диске). Рекомендую: проводить сканирование в ночное время, когда вы спите. С утра просто удалите выявленные угрозы.

В тех случаях, когда вирус реально мешает работе компьютера (блокировка операционной системы или отдельных программ, порнобаннеры, блокировка доступа в Интернет или на определенный сайт, например в социальную сеть) нужно действовать немедленно. Рассмотрим ваши действия, начиная с самого простого. Если не помогает, переходите к следующим.

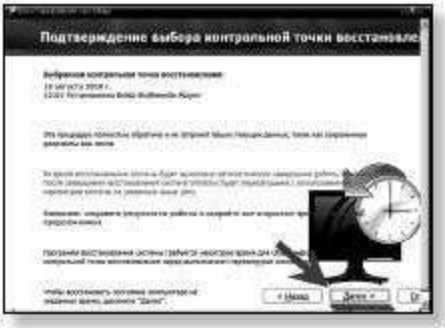
Итак, первым делом попробуйте сделать «откат» операционной системы. Вирус, как вы поняли, – это программа. Операционная система Windows имеет полезную функцию восстановления более раннего состояния компьютера. «Операционка» периодически и после установки новой программы создает точки восстановления. Можно восстановить работоспособность компьютера на период создания точки восстановления, то есть вернуться к состоянию компьютера, когда проблем не было.

Заходим в меню «ПУСК» (нижний левый угол экрана монитора). Далее – «ПРОГРАММЫ», где выбираем «СТАНДАРТНЫЕ» и затем «СЛУЖЕБНЫЕ». Из служебных программ выбираем «ВОССТАНОВЛЕНИЕ СИСТЕМЫ». В открывшемся окне ставим точку напротив пункта «Восстановление более раннего состояния компьютера» и кликаем кнопку «Далее».



Выбираем точку восстановления на период, когда с компьютером было все в порядке (точки восстановления выделены жирным шрифтом) и кликаем «Далее».

В следующем окне кликаем «Далее». Начнется процесс восстановления.



После восстановления компьютер автоматически перезагрузится. Во многих случаях этот простой способ очень эффективен. После восстановления обязательно просканируйте компьютер антивирусом.

В случаях когда вирус блокирует вход в операционную систему, попробуйте загрузить Windows в Безопасном режиме.

Что такое Безопасный режим?

Безопасный режим (Safe Mode) – это диагностический режим (иногда его еще называют режимом защиты от сбоев), позволяющий выявить неполадки, вызванные некорректной работой (или неправильной настройкой) программной или аппаратной части ПК.

В Безопасном режиме Windows использует настройки по умолчанию (минимальный набор драйверов устройств, необходимых для запуска Windows: драйверы мыши, монитора, клавиатуры, дисков, видеоадаптера; стандартные системные службы; поддержка сети отсутствует).

Как загрузить Windows в Безопасном режиме:

1. Перезагрузите компьютер.

2. При загрузке нажмите на клавиатуре кнопку «F8» (если появится окно выбора Boot Device, выберите жесткий диск, на котором установлена ОС, нажмите «Enter», потом «F8»).

3. В Меню дополнительных вариантов загрузки Windows при помощи клавиш со стрелками выберите Безопасный режим.

4. Выберите нужную учетную запись.

5. В окне Рабочий стол с сообщением, что Windows работает в Безопасном режиме, нажмите «Да» (если вы нажмете кнопку «Нет», запустится программа восстановления системы).

После сканируйте компьютер своей антивирусной программой.

Иногда безопасный вход заблокирован вирусом, а этим в последнее время «грешат» так называемые вирусы-вымогатели. Они блокируют компьютер и выводят на экран монитора баннер с требованием для разблокировки отправить платное СМС-сообщение или пополнить счет мобильного телефона через терминал, чего делать категорически нельзя! Никакого кода разблокировки вы, естественно, не получите.

Для того чтобы помочь пользователям, попавшимся на удочку мошенников компания «Доктор Веб» создала специальный раздел на своем официальном сайте, где собрала всю информацию об этих вирусах. В разделе, например, дана фор-

ма разблокировки, которая помогает бесплатно найти необходимый код. Если на ваш компьютер попал троянец и заблокировал его, нужно сделать следующее.

Так как ваш компьютер заблокирован, узнавать код разблокировки придется с другого компьютера, подключенного к Интернету. Заходим на официальный сайт разработчика антивирусных программ «Доктор Веб» в специальный раздел по решению данной проблемы по адресу: **http://www.drweb.com**. На главной странице сайта кликайте в верхней строчке меню раздел «Поддержка». В разделе поддержки в левой части страницы найдите в разделе «Сервисы» пункт «Бесплатная разблокировка Windows». Попадаете на бесплатный сервис разблокировки операционной системы.

На сайте дано несколько вариантов получения кода, который нужно ввести в окно разблокировки баннера (картинки), закрывающего рабочий стол зараженного компьютера.

Можно узнать точное имя троянской программы, найдя фотографию (скриншот экрана) баннера. Если вы нашли идентичный вашему, внизу картинки увидите название троянской программы, которую «посчастливилось» поймать.

Перепишите название программы на листок, блокнот и т.д. После этого в Меню, показанном ниже, выберите «Свой». Кликните по названию левой кнопкой мыши. В правом прямоугольнике увидите код, который необходимо ввести в окно баннера, закрывающего экран вашего монитора.

Второй способ – это узнать код по номеру и тексту сообщения, которое предлагается отправить. Перепишите код номера и текст сообщения на листок, блокнот и т.д. После этого в Меню, показанном на нижнем скриншоте, выберите идентичные. Кликните по ним левой кнопкой мыши. В правом прямоугольнике увидите код, который необходимо ввести в окно баннера, закрывающего экран вашего монитора.

Мошенники не стоят на месте, придумывая постоянно что-то новенькое. В начале июня появилась новая угроза. Новый троянец, блокируя компьютер, требует не отправки СМС-сообщения, а предлагает пополнить счет мобильного телефона мошенников через терминал. Якобы на чеке, выданном терминалом, будет напечатан код разблокировки. Смешно! Подумайте сами, это значит, что владельцы терминалов с ними в сговоре... нонсенс. Заполните в том же разделе сайта «Доктор Веб» форму (номер телефона) и вы получите код разблокировки.

После того как Вы «вылечите» свой компьютер, настоятельно рекомендую просканировать его на наличие вирусов своим антивирусником или бесплатной утилитой Dr.Web CureIt! Ее можно скачать на официальном сайте компании «Доктор Веб» в разделе «Скачайть».

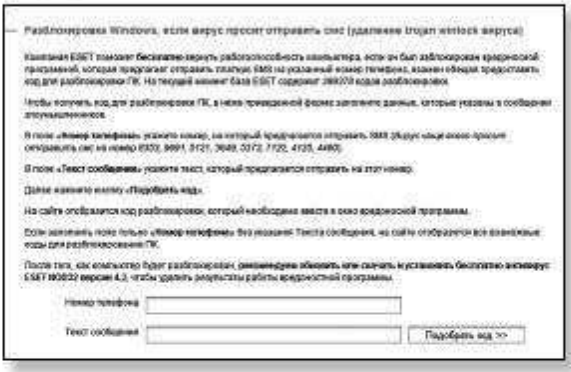
Стал доступен способ бесплатного получения номера разблокировки через браузер мобильного телефона. Выходим с мобильника в Интернет, вводим в адресную строку адрес: **http://www.drweb.com/unlocker/mobile/**. Ну а дальше все просто! Вводим короткий номер телефона, на который мошенники предлагают

отправить СМС-сообщение, выбираем текст «вашего» сообщения и получаем бесплатно код разблокировки! Советую на всякий случай иметь этот адрес, записанным в бумажный блокнот.

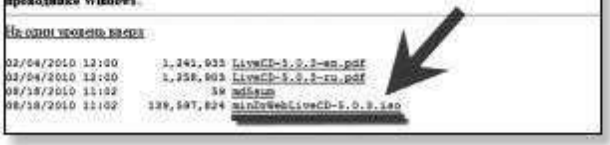
Компания «Лаборатория Касперского» тоже занимается данной проблемой. У нее тоже есть бесплатный сервис по решению этой проблемы. Сервис находится по адресу: **http://support.kaspersky.ru/viruses/deblocker**.

Компания ESET, известная всем как разработчик популярной антивирусной программы NOD32, присоединилась к решению проблемы блокировки Windows троянцами. Компания по примеру других производителей антивирусного софта открыла бесплатный онлайн-сервис. Для разблокировки компьютера необходимо зайти на страницу **http://www.esetnod32.ru/.support/**

winlock/ и заполнить данные, которые указаны в сообщении мошенников. В поле «Номер телефона» укажите номер, на который предлагается отправить SMS. В поле «Текст сообщения» укажите текст, который предлагается отправить на этот номер. Далее нажмите кнопку «Подобрать код». На сайте отобразится код разблокировки, который необходимо ввести в окно вредоносной программы.



Еще один стопроцентный способ удаления порнобаннера – иметь под рукой лечащий диск «Лайф СД от доктора Web». Скачайте бесплатно образ диска по адресу: **ftp://ftp.drweb.com/pub/drweb/livecd/**.



Запишите образ диска на болванку CD. Образ занимает всего 88 МБ, так что диска CD хватит за глаза. Инструкцию, как пользоваться диском, вы можете посмотреть в онлайн или сохранить (скачать на компьютер) на той же странице, где скачали диск.

Разработчик антивирусных программ AVG тоже выпустил бесплатный спасательный CD. AVG спасательный CD – это эффективный набор инструментов, необходимых для аварийного восстановления и ремонта зараженных компьютеров. Он включает следующие возможности:

1. Комплексный набор инструментов администрирования.
2. Восстановление системы в случае заражения вирусом или шпионским ПО.
3. Возможности для восстановления операционных систем MS Windows и Linux (файловые системы FAT32 и NTFS).
4. Возможность выполнять чистую загрузку с компакт-диска или USB-накопителя.
5. Бесплатная поддержка и обслуживание для владельцев платной лицензии любого продукта AVG.
6. Раздел «Часто задаваемые вопросы» и самостоятельное решение вопросов на форуме для пользователей AVG Free.

Скачайте образ диска по адресу: **http://www.avg.com/ru-ru/avg-rescue-cd.**

Многие пользователи «ВКонтакте» в последнее время столкнулись с проблемой входа в эту социальную сеть. При попытке входа видят надпись, что «аккаунт заблокирован». Сразу оговоримся – ваш аккаунт не заблокирован. Чтобы убедиться в этом, введите в адресной строке браузера следующие цифры: 93.186.225.211 и кликайте «Войти».

Заполняем форму входа. Без проблем попадаем на свою страничку.

Почему не удается зайти обычным способом? Дело в том, что ваш компьютер атакован вирусом. Это так называемый вирус vkontakte.exe. Он представляет из себя вредоносный код, который изменяет файл C:\WINDOWS\system32\drivers\etc\hosts. При изменении файла вы, набирая в браузере vkontakte.ru будете попадать на копию настоящего сайта, которая выглядит совершенно идентично оригиналу. Целью создавших его злоумышленников является кража паролей и получение денег наивных пользователей, которые отправляют им платные СМС-сообщения в надежде, что их разблокируют. Пароли они потом продадут другим нехорошим людям и получат еще немного денег.

Как устранить эту проблему? Открываем файл C:\WINDOWS\system32\drivers\etc\hosts. Для этого заходим в меню «ПУСК». Выбираем «МОЙ КОМПЬЮТЕР». Далее – диск с установленной операционной системой (обычно диск С). Затем выбираем папку «WINDOWS», далее – «system 32», заходим в папку «drivers», далее – в папку «etc».

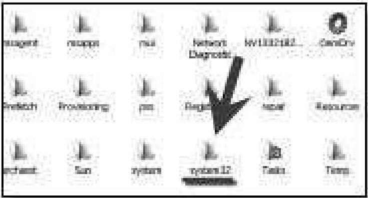
Находим в папке файл «hosts».


Локальный диск (C:)
Локальный диск (E:)
Локальный диск (F:)

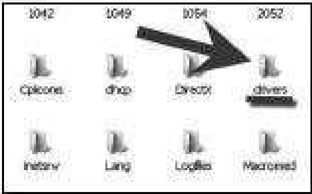
2


WINDOWS

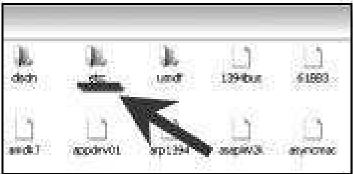
3


system32

4


1042
1049
1054
2052
drivers
Lang

5


etc

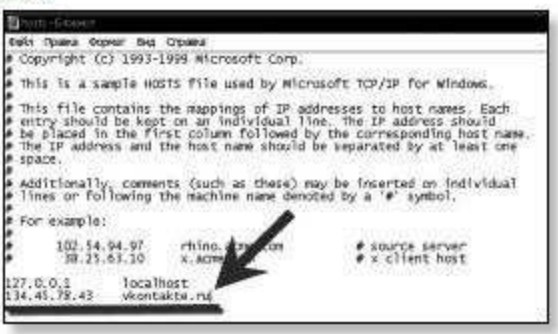
6


hosts

7

Открываем файл программой «Блокнот».

Просматриваем содержимое этого файла. Если там есть какие-либо строки, содержащие слова «vkontakte.ru», «mail.ru» или другие адреса сайтов, то вам нужно удалить эти строки и сохранить файл.



По умолчанию там есть только одна незакомментированная (закомментированные строки начинаются со знака # и не учитываются) строка –127.0.0.1 localhost , ее оставьте, а остальные удалите.

Вводим в проводнике в поиске: «vkontakte.exe» (приложение), если что-то находит, то и удаляем его.

После этого перезагружаем компьютер. Проблема решена!

Для перестраховки вводим в проводнике в поиске: «vkontakte.exe» (приложение), если что-то находит, то удаляем и его.

Если при попытке входа появляется такая надпись:

«Активируйте свою анкету.

Ваш аккаунт заблокирован.

Активация происходит в автоматическом режиме, отправьте СМС с текстом 40956 1315594 (Между 40956 и 1315594 поставьте пробел) на номер 1171. Если SMS не отправляется на номер 1171, попробуйте отправить на номер 3649 и заполните форму ниже: ...»

Для бесплатной разблокировки понадобится воспользоваться программой AVZ. Скачайте и установите самую новую версию (постоянно обновляется). Найти ее несложно через любой поисковик. Пишем в поисковике «скачать программу AVZ».

Программа не требует установки. Просто открываем ее.

Затем открываем программу «Блокнот» и пишем в нем, только строго, как показано ниже, следующий текст:

```
Begin
SearchRootkit(true, true);
SetAVZGuardStatus(True);
QuarantineFile('H:\WINDOWS\system32\vksaver.dll','');
QuarantineFile('H:\Autorun.exe','');
QuarantineFile('H:\autorun.inf','');
DeleteFile('H:\autorun.inf');
DeleteFile('H:\Autorun.exe');
ClearHostsFile;
ExecuteSysClean;
RebootWindows(true);
end.
```

Копируем текст. Вставляем скопированный текст. Для этого в программе AVZ нажимаем кнопку «Файл» (верхний левый угол окна программы), далее – «Выполнить скрипт». Вставляем в появившемся окне скопированное (правой кнопкой мыши кликаем в окне и выбираем в выпавшем меню «Вставить») и затем – «Запустить».

После выполнения скрипта компьютер перезагрузится. Эта программа отлично справляется и с другими задачами по безопасности компьютера. Советую протестировать.

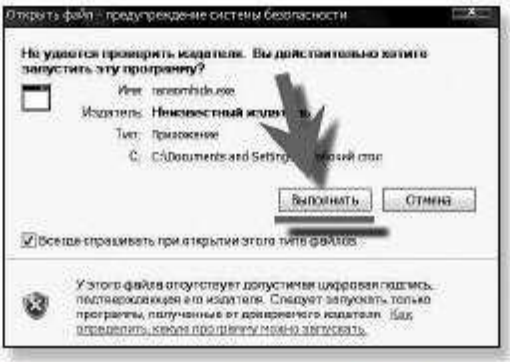
Данные способы, конечно, не панацея от всех бед. Мошенники не стоят на месте. Но в большинстве случаев они эффективны.

RansomHide – удаление порнобаннеров-вымогателей без выхода в Интернет

Бесплатная программа RansomHide предназначена для разблокировки компьютера без отправки денег мошенникам. Огромным плюсом программы является то, что выхода в Интернет не требуется. Второй плюс программы – она постоянно обновляется. Третий плюс – помимо базы кодов разблокировки программа содержит большое количество других способов разблокировки, на случай если проблема не будет решена.

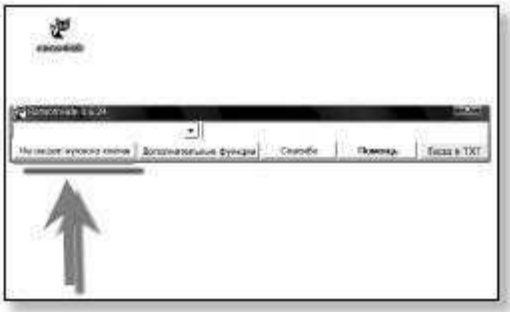
Скачиваем бесплатно программу на сайте **http://halyavin.ru/** в разделе «Бесплатные программы». Сохранить лучше на рабочий стол.

Программа не требует установки. Просто при необходимости запускаем программу, кликнув по значку программы на рабочем столе.



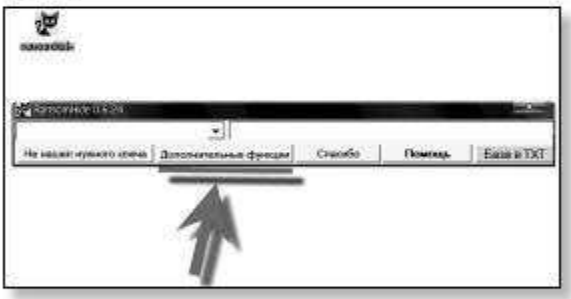
В окне программы забиваем (или находим в базе TXT) короткий номер и текст сообщения вымогателей и получаем бесплатно код разблокировки.

Если не нашли нужного ключа, кликаем кнопку «Не нашел нужного ключа».

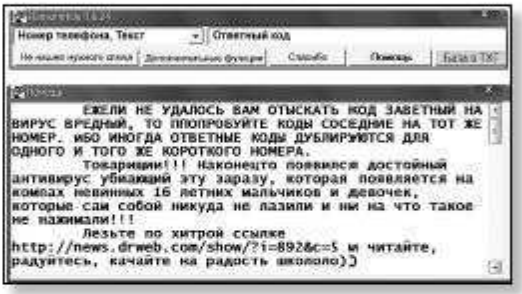


В открывшемся окне ищем по базам разработчиков антивирусных программ.

Если проблема не решена, переходим к дополнительным функциям.



Для самых сложных случаев в программе есть раздел «Помощь».



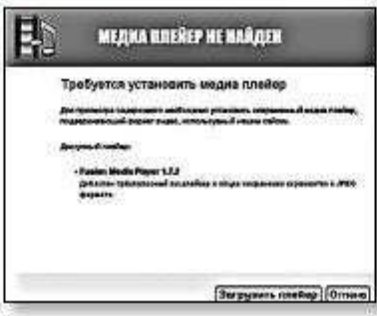
Программа действительно полезная. Советую скачать и периодически (раз в неделю) обновлять. Файл по ссылке постоянно обновляется. Внимание! При обновлении программа должна быть закрыта.

Новая угроза Вашему компьютеру – вирус Trojan.HttpBlock

В конце сентября интернет-мошенники запустили вредоносную программу, которая стала новым витком в развитии вирусов-троянцев, блокирующих вход в операционную систему или Интернет. Для получения кода разблокировки мошенники требуют отправить им платное СМС-сообщение, в последнем случае это код 6681. На данный момент эпидемия заражений достигла огромных масштабов, например доля обращений с просьбой помочь разблокировать доступ в Интернет (а именно доступ к нему и блокирует этот новый троянец) на сайте разработчика антиви-

русных программ «Доктор Web» в процентном исчислении занимает уже более 80 процентов.

«Поймать» Trojan.HttpBlock можно, открыв на каком-либо сайте (в основном это сайты, где можно скачать пиратские фильмы, программы, игры и т.д.) всплывшее окно с предложением посмотреть порноролик. При попытке просмотра ролика выскакивает предложение «скачать медиаплеер», без которого якобы просмотр невозможен. Дав согласие на загрузку плеера, Вы установите на компьютер троянца Trojan.HttpBlock! Так что самое разумное – отказаться от установки.



Ну а если вы все-таки «лоханулись» – ОТПРАВЛЯТЬ СМС-СООБЩЕНИЕ НЕЛЬЗЯ НИ В КОЕМ СЛУЧАЕ! Никакого кода разблокировки Вы не получите.

Разблокировать можно самостоятельно. Правда, при попытке проанализировать систему с помощью различных утилит могут возникнуть трудности, поскольку троянец завершает работу некоторых опасных для себя процессов в соответствии со списком, составленным авторами программы. Вредоносная программа работает и блокирует антивирусы как в 32-, так и в 64-разрядных системах – версиях Windows. В последних модификациях Trojan.HttpBlock некоторые строки зашифрованы, что затрудняет анализ вредоносных файлов.

Но не отчаивайтесь. В большинстве случаев для лечения системы достаточно просканировать систему с помощью бесплатной лечащей утилиты Dr.Web CureIt! С начала распространения Trojan.HttpBlock в вирусную базу Dr.Web было добавлено более 30 модификаций этой вредоносной программы. Также была создана запись Trojan.HttpBlock.origin, использующая техноло-

гию Origins Tracing. Эта запись позволяет определять наличие в системе неизвестных модификаций троянца. Заранее, на всякий случай, скачайте эту утилиту на сайте **http://halyavin.ru/** в разделе «Бесплатные программы».

Обман пользователей при скачивании

В последнее время участились случаи обмана пользователей, качающих фильмы, музыку, программы с сайтов, размещающих ссылки. Попадаются в основном новички. Суть «разводки» в следующем: человек, решивший скачать что-либо на подобных сайтах, на странице с информацией о файле на самом видном месте видит табличку «Скачать на большой скорости» с несколькими вариантами способов получения.

При выборе любого из данных в табличке способов вы скачиваете программу «самораспаковывающийся архив» (хотя название скачанного именно то, что вы и хотели скачать, но небольшой размер файла и окончание «exe.» выдает «разводил» с головой).

При попытке открытия скачанного файла появляется вот такое окно с пользовательским соглашением, которое обязывает вас при установке отправить ПЛАТНОЕ СМС-сообщение!

Неопытные пользователи отправляют деньги. Это чистый развод!!! Не попадайтесь. Будьте предельно внимательны. На этой же странице вы найдете и бесплатные способы скачивания. Без всякой отправки платных СМС за сомнительные программы.

Подведем итог:

1. НИКОГДА НЕ ОТКЛИКАЙТЕСЬ НА ПРЕДЛОЖЕНИЯ СКАЧАТЬ НА ВЫСОКОЙ СКОРОСТИ.

2. ОБРАЩАЙТЕ ВНИМАНИЕ НА РАЗМЕР СКАЧИВАЕМОГО ФАЙЛА. Вас должно насторожить, что, например, скачиваемый фильм «весит» всего 16 МБ. Он должен быть размером ну никак не меньше 700 МБ.

3. ОБРАЩАЙТЕ ВНИМАНИЕ НА ОКОНЧАНИЕ СКАЧИВАЕМОГО ФАЙЛА. Например, фильм ну никак не может оканчиваться на «exe». Такое окончание явно указывает на установочный файл.

Меры безопасности при скачивании и хранении контента на компьютере

Скрытное скачивание с торрентов (подмена IP-адреса, блокировка IP-адресов антипиратских организаций и т.д.)

Принятие закона **«Об Интернете»** должно произойти, скорее всего, уже в 2011 году. Этот закон установит нормы авторского права для русскоязычной части Интернета (Рунета). Проект, его основные разделы, фактически списан с американского закона **DMCA** (Digital Millenium Copyright Act). В принципе это наиболее мягкий из вариантов, которые рассматривались разработчиками. Этот закон снимает ответственность с сайтов, где пользователи размещают спорный контент. Ответственность перекладывается на физических лиц, разместивших его. То есть не случится такого, что в один прекрасный день, зайдя в Интернет, мы не обнаружим там ни одного русскоязычного файлообменника или врезного сайта.

Впрочем, простых пользователей, которые не используют скачанный контент для коммерческих целей, этот закон коснуться не должен. По словам зампредседателя Комитета Госдумы по законодательству Владимира Груздева, «Конечно, это не коснется простых людей, это будет касаться нарушителей, системных нарушителей, людей, которые занимаются этим бизнесом, потому что это действительно стало бизнесом. Речь, конечно же, не будет идти о том, что если вы вдруг запишите какую-либо передачу, то вас завтра посадят».

Но вопрос анонимного скачивания – это то, что будет актуально при любом раскладе.

Существует несколько способов скрытного скачивания с торрентов. Например, скачивание через магнитные ссылки или с открытых торрент-трекеров (там, где не нужна регистрация) дает относительную анонимность. Истории скачанного и отданного там не ведется. Но при большом желании (желание должно

быть ну о-о-очень большим) вычислить именно вас все же можно. Но вы, как в том анекдоте, должны быть «уловимым Джо».

– Почему этот Джо зовется «неуловимым?

– Да потому что он на фиг никому не нужен!

Ну а так как именно конкретно на вас не будет открыта «охота», то этих способов «шифрования» вполне достаточно. Причем, скачивая через новую версию торрент-клиента Media Get, вы увеличиваете анонимность в разы! Дело в том, что в этом клиенте есть очень полезная функция, а именно блокирование IP-адресов антипиратских организаций. Именно антипиратскими организациями во всем мире и происходит «вычисление» людей, обменивающихся между собой контентом. База состоит из нескольких миллионов таких адресов, и эта база постоянно обновляется и дополняется! О том, как установить, настроить и пользоваться этим уникальным торрент-клиентом, кстати, разработанным российскими программистами, информация ниже.

Эффективным, но, правда, платным способом скрыть свой IP-адрес является скачивание через прокси-сервисы, которые специально «заточены» под торренты. Плата за пользование этими сервисами небольшая, примерно 10 долларов в месяц. При этом стопроцентная гарантия анонимности. Из всей когорты прокси-сервисов для торрентов выделю только два, которые стабильны и безопасны (на этом рынке предложений, особенно в последнее время, появилось много мошенников).

1. **BTGuard** (http://btguard.com/) – это прокси-сервис, который позволяет скрыть ваш IP-адрес. Сервис работает на Windows, Mac, Linux, но работает он только с торрент-трафиком.

2. **TorrentPrivacy** (https://torrentprivacy.com/). Если BTGuard позволяет настроить на работу практически с любым клиентом, то TorrentPrivacy предлагает свой торрент-клиент, который работает только под Windows.

Итак, как и обещал, рассмотрим, как установить и пользоваться торрент-клиентом MediaGet.

MediaGet – торрент-клиент со встроенным поисковиком

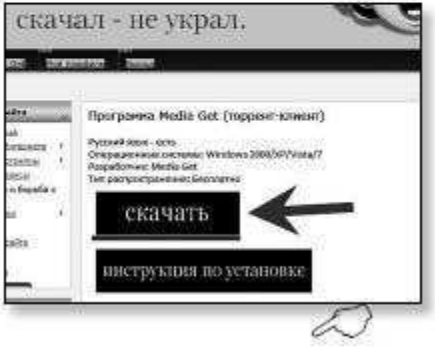
MediaGet – это торрент-клиент российских разработчиков. Все больше пользователей торрент-трекерами переходят на скачивание именно через MediaGet. И это неудивительно.

Дело в том, что в одной из последних обновленных версий добавилась функция безопасного режима. Эта функция блокирует обмен IP-адресами с антипиратскими организациями. Именно так во всем мире происходит «вычисление» качающих с торрент-трекеров. В постоянно обновляемую базу уже внесено более двух миллионов IP-адресов этих организаций.

Среди возможностей и функций торрент-клиента – прекрасная база различных фильмов, обновляющаяся регулярно, поиск, позволяющий искать информацию по открытым для доступа трекерам и многое другое. Особого внимания заслуживает возможность экспорта или импорта загрузки файлов, т.е. вы сможете начать закачку необходимой информации на одном компьютере, а закончить уже на другом. Это очень удобно, если вы начали загружать файл на работе, а закончить загрузку времени нет – просто сделайте это дома. Также, воспользовавшись поиском, вы сможете выбирать среди файлов информацию того размера, который вас устраивает.

Еще одно приятное новшество, которое предлагает торрент-клиент MediaGet – это возможность рассказать о торренте друзьям и знакомым, которые пока не освоили эту программу. С помощью функции «Поделиться» вы легко сможете переслать ссылку на закачку интересного файла: кликнув по полученной ссылке, ваш знакомый запустит установку торрент-клиента на свой компьютер, а затем начнется автоматическая закачка выбранной вами информации.

Скачиваем программу **MediaGet** на сайте **http://halyavin.ru/** в разделе «Бесплатные программы».



1

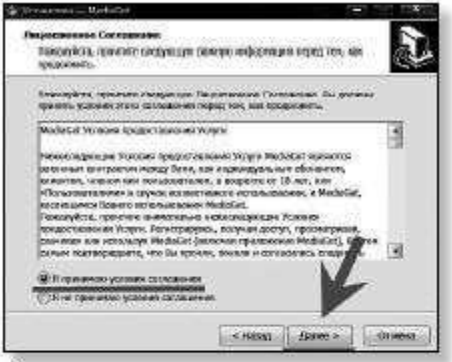
2

3

Сохранять лучше на рабочий стол. После скачивания программы запускаем установку.

1

2



3

4

5

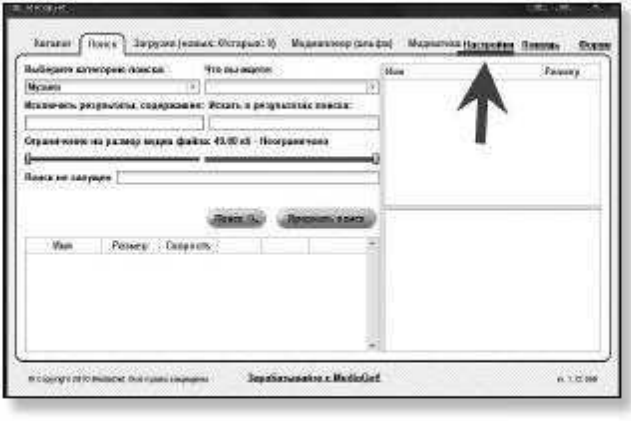
6

В следующем пункте установки выбираем не полную установку, а настройку параметров, где отказываемся от установки Ассистента с сервисами Рамблера.

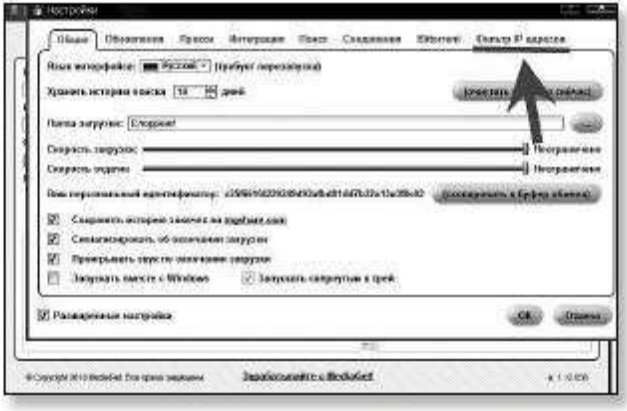
Завершаем установку.

При первом запуске вам будет предложено выбрать папку для загрузки файлов. Если у Вас уже существует папка, куда Вы загружаете файлы с торрентов, выберите ее. Если Вы новичок, советую создать папку в разделе на жестком диске, где у Вас больше всего свободного места.

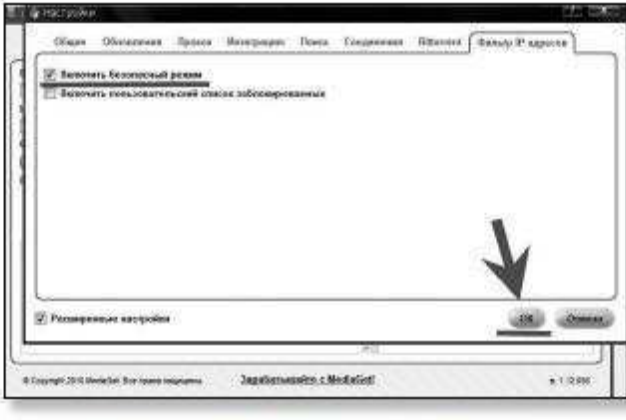
Включаем функцию блокирования IP-адресов антипиратских организаций. Для этого в окне программы кликаем кнопку «Настройки».



В следующем открывшемся окне кликаем «Фильтр IP-адресов».



Ставим галочку напротив «Включить безопасный режим». Скачиваем обновленный список антипиратских организаций и кликаем кнопку «ОК».



Функция блокировки IP-адресов активирована.

Более подробно о пользовании этим торрент-клиентом вы найдете информацию на сайте **http://halyavin.ru/**. На сайте есть даже видеоурок по освоению программы.

В следующих статьях этой главы мы научимся шифровать информацию, которая хранится у вас на компьютере и при необходимости гарантировано удалять (затирать) всю информацию без оставления следов ее присутствия на компьютере.

Шифрование данных на компьютере программой TrueCrypt

Шифрование данных, находящихся на жестком диске Вашего компьютера, становится актуальной темой. Надобности в этом еще совсем недавно обычному пользователю не было. Шифрованием своих данных занимались в основном коммерческие структуры ну и еще люди, страдающие манией преследования. Все круто изменилось в связи с усилением борьбы с «пиратством». Теперь о том, как закрыть посторонним доступ к информации на персональном компьютере стали задумываться практически все здравомыслящие люди.

Обычные средства защиты доступа к информации на компьютере, такие как пароли Windows, пароли ZIP-файлов, пароли BIOS и FTP/Web всегда при желании легко обойти даже мало-мальски грамотному специалисту. По-настоящему гарантированно можно закрыть доступ к данным только используя современные алгоритмы шифрования вкупе с использованием надежного (читай длинного) пароля.

Способов и средств шифрования и защиты информации не так уж и мало. Например, уже есть жесткие диски самошифрования. Технология Opal SSC, которая используется при их изготовлении, позволяет организовать доступ по паролю не только ко всему накопителю, но и к отдельным его разделам, причем до загрузки операционной системы. Также аутентификация возможна с применением датчиков биометрической защиты, с помощью смарт-карт или токенов (токен – это компактное устройство в виде USB-брелка, которое служит для авторизации пользователя в сети или на локальном компьютере, защиты электронной переписки, безопасного удаленного доступа к информационным ресурсам, а также надежного хранения персональных данных).

Но это не является преградой для тех, кто очень захочет узнать о том, что хранится у Вас на компьютере. Теоретически жесткий диск самошифрования можно разблокировать с помощью специальной утилиты от производителя жесткого диска.

Гарантированно защитить от посторонних информацию на компьютере способно только программное обеспечение, которое шифрует системный диск или при желании только раздел, где хранятся секретные файлы. Для этих целей идеально подходит бесплатная программа **TrueCrypt**.

TrueCrypt – компьютерная программа для шифрования «на лету» (On-the-fly encryption). Что обозначает «на лету»?

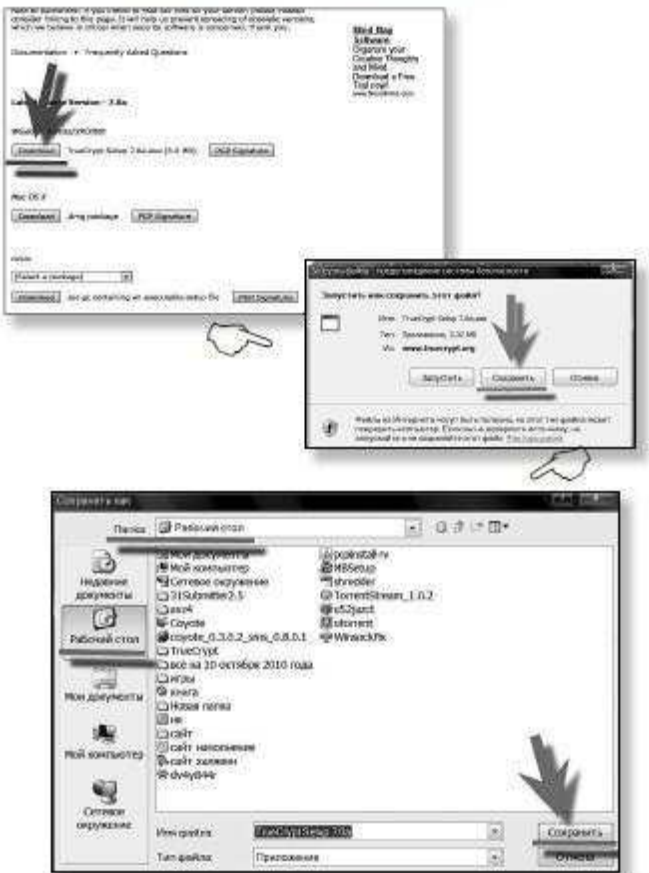
Представьте, что у вас на компьютере хранится фильм, записанный, например, в формате avi. Он хранится на томе (как создавать том рассмотрим ниже) TrueCrypt и поэтому целиком зашифрованный. Пользователь, применяя правильный пароль, подключает (открывает) том TrueCrypt. Когда пользователь дважды кликает на иконке видеофайла, операционная система запускает программу, связанную с этим типом файла – как правило, это медиаплеер. Медиаплеер начинает загружать небольшую начальную часть видеофайла с зашифрованного TrueCrypt-тома в память, чтобы проиграть его. В процессе загрузки этой небольшой части TrueCrypt автоматически дешифрует ее в памяти. Расшифрованная часть видео, хранящаяся теперь в памяти, проигрывается медиаплеером. После проигрывания этой части медиаплеер начнет загружать следующую небольшую часть видеофайла с зашифрованного тома TrueCrypt в память, и процесс повторится. Этот процесс и называется шифрованием/дешифрованием «на лету», и он работает со всеми типами файлов, а не только с видео.

Программа позволяет создавать виртуальный зашифрованный логический диск, хранящийся в виде файла. С помощью TrueCrypt также можно полностью шифровать раздел жесткого диска или иного носителя информации, такой как флоппидиск или USB флеш-память. Все сохраненные данные в томе TrueCrypt полностью шифруются, включая имена файлов и каталогов. Смонтированный том TrueCrypt подобен обычному логическому диску, поэтому с ним можно работать с помощью обычных программ проверки и дефрагментации файловой системы.

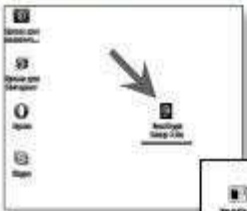
Установка и использование программы

Установка программы

Для начала скачайте последнюю версию программы на сайте **http://halyavin.ru/** в разделе «Бесплатные программы».



Запускаем установку программы.



1

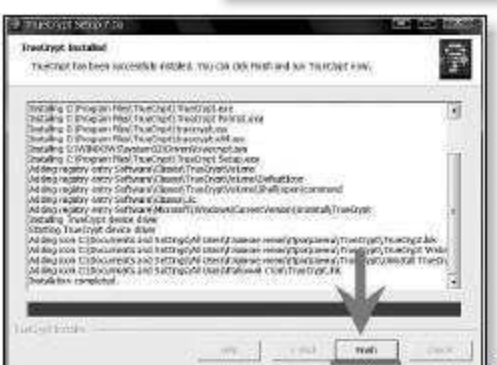
2

3

4

5

6



7

Программа установлена.

Руссификация программы

Программа изначально имеет английский интерфейс. На момент написания книги последней стабильной версией была версия программы 3.0, языкового русского пакета под эту версию еще не было. Для удобства пользования программой советую скачать (если он появился) и установить русский. Открываем окно программы. Это можно сделать, кликнув в трее (в правом нижнем углу экрана рядом с часами) по значку программы (ключ на синем фоне) или запустить программу из папки TrueCrypt, которая находится в Program Files.

В верхней строчке программы выбираем «Settings», далее – «Language» и в открывшемся окне кликаем кнопку «Download languge pack».

Вы будете перенаправлены на страницу скачивания (Интернет должен быть подключен) языкового пакета. Выбираем русский и кликаем «Download» («Скачать»).

Языковой пакет в архиве. Извлеките языковой пакет в папку, для которой установлен TrueCrypt, т.е. папке, в которой находится файл TrueCrypt.exe; например C:\Program Files\TrueCrypt. Запустите TrueCrypt. Выберите настройки -> язык, затем выберите язык и нажмите кнопку ОК.

Чтобы вернуться к «Английский», выберите параметры -> язык. Затем выберите английский язык и нажмите кнопку «ОК».

Использование программы TrueCrypt

Как я уже писал ранее, на момент написания книги, последняя версия программы еще не была руссифицирована. Поэтому все скриншоты (фотографии с экрана монитора) и названия кнопок из англоязычной версии.

Рассмотрим, как создать, подключить и использовать зашифрованный том программой TrueCrypt. Как шифровать физические разделы, то есть полностью шифровать всю информацию на жестком диске (дисках), на этом примере вы сможете разобраться самостоятельно или найдете пошаговую инструкцию, посетив мой сайт **http://halyavin.ru**.

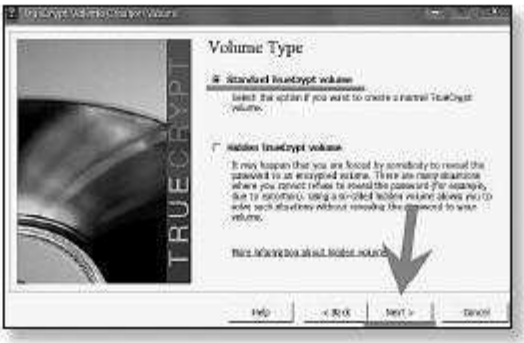
Итак, **шаг 1**: Открываем программу, кликая значок программы в трее или находим ее в папке программы (папка программы находится в Program Files и имеет название TrueCrupt). В прин-

ципе можно создать ярлык программы на рабочем столе, но в целях секретности делать этого не рекомендуется.

Шаг 2: В окне программы кликаем кнопку «Create Volume» («Создать том»).

Шаг 3: Вы должны выбрать, где вы желаете создать том TrueCrypt. Он может занимать файл (который в таком случае может называться контейнером), раздел и диск. Рассмотрим первую возможность – создание тома TrueCrypt в файле (создать файловый контейнер). Так как эта опция выбрана по умолчанию, просто кликнаем кнопку «Next» («Далее»).

Шаг 4: Вам нужно выбрать, создавать обычный или скрытый том. В этом руководстве мы пойдем простым путем и создадим обычный том.

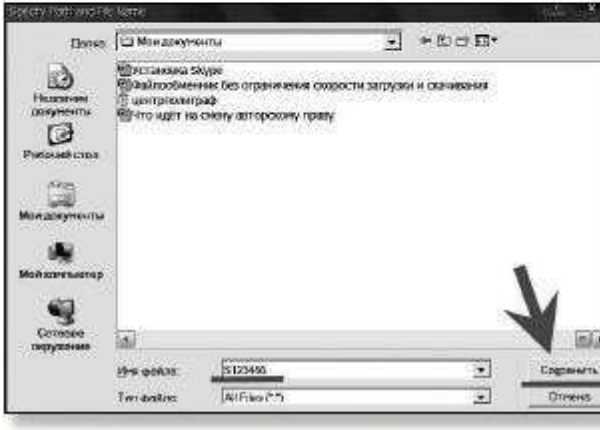


Шаг 5: Выбираем место хранения тома TrueCrypt (файловый контейнер). Учтите, что контейнер TrueCrypt выглядит как обычный файл. Его можно перемещать, копировать и удалять, как любой нормальный файл. И, конечно же, он нуждается в имени файла, которое мы сейчас и выберем.

Кликаем кнопку «Select File» («Файл»).

Появится стандартное окно Windows для выбора файла (при этом окно мастера создания тома остается открытым под ним).

Шаг 6: Создаем том в любой удобной для Вас папке (в данном случае создадим том в папке «Мои документы»). Обратите внимание, что том должен быть назван именем, не содержащим букв русского алфавита, можно использовать только цифры и английские буквы. В поле «Имя файла» пишем придуманное имя и кликаем «Сохранить».



Шаг 7: Проследите, чтобы поле нахождения тома было заполнено, и кликните «Next» («Далее»).

Шаг 8: На этом этапе вы можете выбрать алгоритмы шифрования и хэширования для тома. Если вы не знаете, что выбрать, то можете оставить настройки по умолчанию и кликнуть «Next» («Далее»).

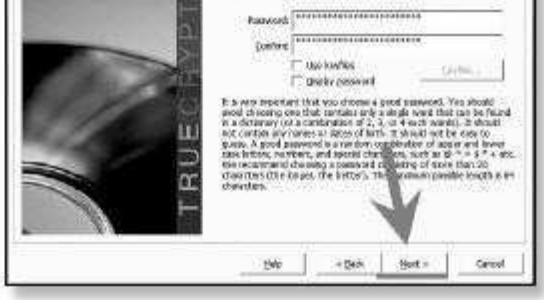
Шаг 9: Выбираем размер тома. Если Вы собираетесь хранить в нем весь скачиваемый с Интернета материал, то советую сделать его большим. Кликаем «Next» («Далее»).

Шаг 10: Внимание! Это один из самых важных шагов – выбор пароля! Очень важно выбрать хороший пароль. Избегайте указывать пароли из одного или нескольких слов, которые можно

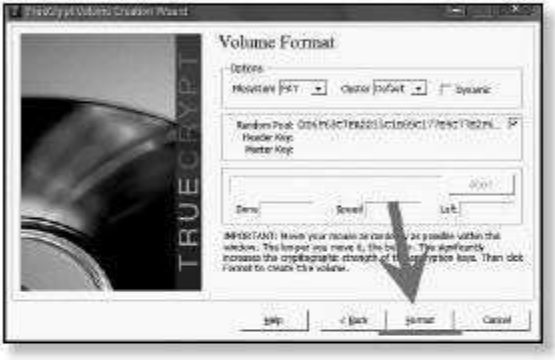
найти в словаре. Пароль не должен содержать имен или дат рождения. Он должен быть труден для угадывания.

Рекомендованная длина пароля 20 знаков. Максимальная длина пароля составляет 64 знака. 20 знаков запомнить, конечно, очень сложно, а вот забыть легко. Поэтому рекомендую записать его и хранить в бумажном виде, но только в таком месте, где он не будет доступен никому кроме Вас.

После того как Вы придумаете пароль, введите его в первом поле. Потом повторно введите во втором поле и кликните «Next» («Далее»). Кстати, кнопку «Next» («Далее») будет невозможно кликнуть, пока введенные в обоих полях пароли не будут совпадать.



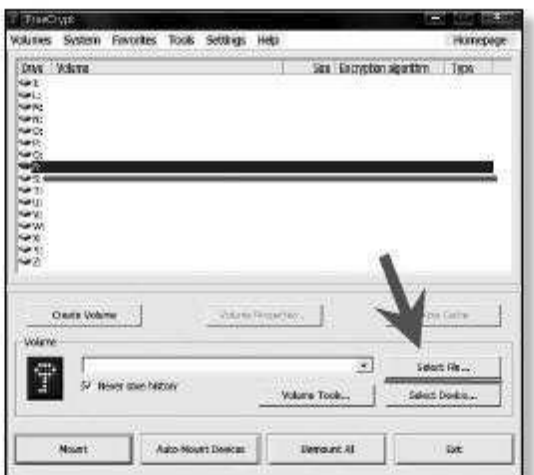
Шаг 11: Поводите вашей мышкой настолько случайно, насколько это возможно, секунд 30 или больше в этом окне мастера. Чем дольше вы это будете делать, тем лучше – это повысит криптографическую устойчивость ключей, что увеличивает безопасность. Затем кликайте кнопку «Format» («Разместить»).



Начнется создание тома. Чем больше размер тома, тем больше времени на его создание будет потрачено. После окончания операции появится следующее диалоговое окно, где кликаем «ОК».

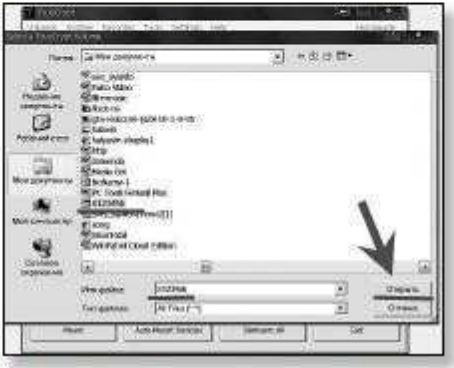
Шаг 12: Том TrueCrypt (файл контейнера) успешно создан. Кликните «Exit» («Выход») для выхода из этого окна.

Шаг 13: В следующих шагах мы подключим созданный нами том. Для этого мы вернемся в главное окно TrueCrypt. Если вы его уже закрыли, повторите шаг 1. Выберите букву диска из списка (можете выбирать любую по своему желанию). Это будет диск, под которым будет отображаться подключенный контейнер TrueCrypt. Затем кликаем кнопку «Select File» («Файл»).



Шаг 14: Появится стандартное окно Windows для выбора файла.

Шаг 15: В этом окне найдите файл контейнера, созданный нами в шагах 6–11, и выберите его. Кликните «Открыть». Окно закроется, и мы снова окажемся в основном окне TrueCrypt.



Шаг 16: В главном окне TrueCrypt кликните кнопку «Mount» («Смонтировать»).

Шаг 17: Появится окно запроса пароля. Введите пароль, придуманный вами в шаге 10, в поле ввода пароля. Кликните «OK» в окне запроса пароля.

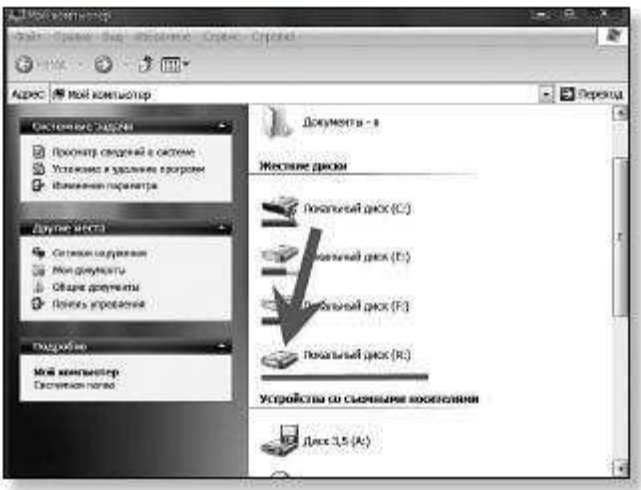
Теперь TrueCrypt попробует подключить ваш том. Если пароль был введен неправильно (например, из-за ошибки при наборе), TrueCrypt сообщит об этом и вернет вас на предыдущий шаг. В таком случае введите пароль снова и кликните «OK». Если пароль будет введен правильно, том будет подключен.

Шаг 18 (заключительный). Контейнер успешно смонтирован на виртуальный (в нашем случае) диск «R». Виртуальный диск полностью зашифрован (включая имена файлов, таблицы размещения файлов, свободное место и т.п.) и выглядит как обычный диск. Вы можете сохранять, копировать, переносить файлы на этот виртуальный диск и они будут шифроваться «на лету» во время записи.

Если вы откроете файл с тома TrueCrypt, он будет автоматически дешифрован в память «на лету» во время никогда не записывает никаких расшифрованных данных на диск – они временно хранятся только в памяти. Даже когда том подключен, хранимые на нем данные остаются зашифрованными. Когда вы перезапустите Windows или выключите компьютер, том будет отключен, и файлы станут недоступны, оставаясь при этом зашифрованными. Даже если питание компьютера неожиданно отключится (то есть стандартная процедура выключения не будет выполнена), все файлы на томе станут недоступны, оставаясь зашифрованными. Для доступа к ним необходимо будет подключить том снова (папка программы находиться в Program Files и имеет название TrueCrupt). Для этого повторите шаги 13–18.

Когда вы открываете файлы, хранимые на томе TrueCrypt (или когда вы записываете/копируете файлы), вам не надо вводить пароль каждый раз.

Вы можете открывать и просматривать подключенный том, как обычный раздел диска, имеющий букву. Например, вы можете войти в «Мой компьютер» и открыть его двойным кликом на букве диска (в нашем случае «R»).



На зашифрованный виртуальный диск советую перенести всю информацию (файлы), которую Вы хотите скрыть от посторонних глаз. Для этого кликните по переносимому файлу правой кнопкой мыши и выберите в выпавшем меню «Копировать». После этого откройте зашифрованный виртуальный диск (в нашем случае диск «R»), в любом месте открывшегося окна кликните правой кнопкой мыши. В выпавшем меню кликните «Вставить».

Внимание! Не забудьте «затереть» следы переносимого файла, которые остались на незашифрованном диске. Идеально для этого подходит программа **Shredder** (так называемый шрёдер), о которой будет рассказано далее.

Кстати, с помощью этой программы можно зашифровать вообще все данные, находящиеся на вашем компьютере!

Совет: установите две операционные системы на ваш компьютер. Первая будет «белая и пушистая». Устанавливайте на нее только лицензионные и бесплатные программы. На вторую устанавливайте и храните все что вам хочется. Зашифруйте обе под разными паролями. При включении компьютера в окне ввода пароля в зависимости от ситуации вводите пароль нужной операционной системы. Вторая просто не будет отображаться, как будто ее нет вовсе.

И еще, повторюсь, если жесткий диск будет снят с вашего компьютера, прочитать зашифрованные данные, подключив его к другому компьютеру, будет просто невозможно!

Бесплатная программа Shredder – полное уничтожение файлов

В последнее время, а также в связи со скорым принятием так называемого закона «Об Интернете», стал очень актуален вопрос защиты информации, хранящейся на компьютере от постороннего доступа.

Одним из самых эффективных способов является, в случае опасности досмотра ПК, мгновенное удаление всех данных на жестком диске компьютера. Но за считанные секунды это возможно сделать, только используя специальные аппаратные шрёдеры. Цена вопроса очень высокая, минимум 1000 долларов! Такова цена самого дешевого из них. Такой вариант мгновенного уничтожения данных доступен только супербогатым

людям и организациям (но там они используются совсем для других целей).

Для обычного пользователя оптимальным вариантом станет использование для удаления данных специального программного обеспечения. Почему нельзя использовать обычное удаление или форматирование жесткого диска? Дело в том, что обычное форматирование не полностью удаляет информацию. Ее можно восстановить при помощи специальных программ.

Для гарантированного стирания нужны программы, так называемые программные шрёдеры.

Для программного уничтожения информации на рынке предлагается огромное количество шрёдеров, использующих разные алгоритмы стирания данных и характеризующихся различной надежностью (уровнем секретности) и быстродействием. Все алгоритмы удаления информации основываются на многократной перезаписи информации в секторах жесткого диска и предусматривают запись в каждый байт каждого сектора жесткого диска неких фиксированных значений или случайных чисел.

Лучшей программой данной категории, на мой взгляд, является программа **Acronis Privacy Expert Suite**. Это целый пакет программ. Основное назначение пакета Acronis Privacy Expert Suite – обеспечение безопасности и конфиденциальности работы на компьютере, а возможность уничтожения информации – лишь одна из его дополнительных функций. Программа подкупает простотой в использовании. С ней справится даже новичок. На каждое действие есть подробная подсказка. Но, к сожалению, она платная. Так что рассмотрим другую программу – Shredder. Программа бесплатная. Но это не значит, что она плохая.

Назначение программы состоит в безвозвратном удалении файлов и папок с жесткого диска компьютера путем затирания исходных данных нулями. Программа быстрая в работе, работает с любой операционной системой Windows.

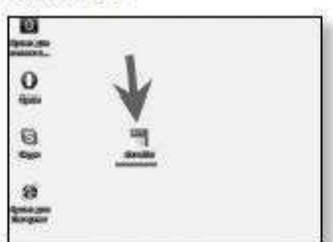
Сразу хочу предупредить.

Внимание! При обработке ярлыка Shredder, вызванный из контекстного меню Проводника, уничтожает объект, на который ссылается ярлык. Будьте внимательны. Уничтожая ярлык, Вы автоматически уничтожаете и файл, на который он ссылается!

Скачать программу можно на сайте **http://halyavin.ru/** в разделе «Бесплатные программы».

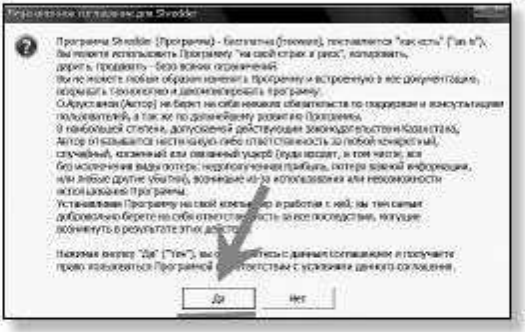
Программа в архиве. Распакуйте ее на рабочий стол. В архиве собственно сама программа и инструкция пользователя. Вариантов использования два.

1. Без установки и интеграции в оболочку Windows. При этом способе просто перетягивайте мышкой в папку программы файл, который Вы хотите удалить.

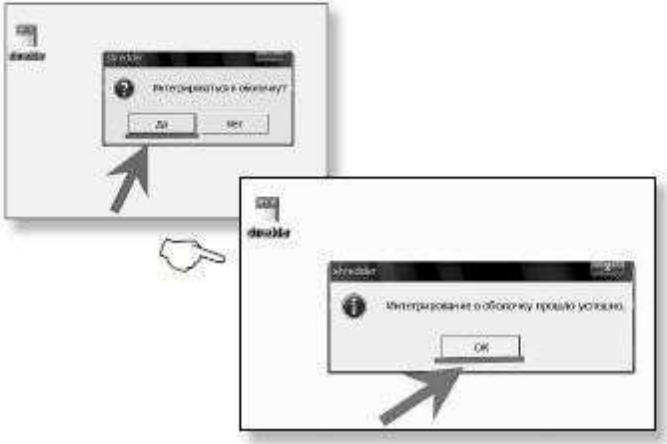


2. С установкой и интеграцией в оболочку Windows. Способ наиболее удобный и предпочтительный. Так как при интеграции в оболочку Windows упрощается процедура удаления и полного стирания файлов. При этом способе просто кликайте правой кнопкой мыши по удаляемому файлу и в выпавшем контекстном меню выбирайте пункт «Shredder».

Для установки и интеграции в оболочку программы Shredder необходимо кликнуть по значку программы на рабочем столе. Согласиться с пользовательским соглашением.



В следующем окне кликните кнопку «Да».



Программа интегрирована. Можно пользоваться.

Как видим, комплекс мер, предложенный мной для анонимного скачивания, безопасного хранения и в случае опасности гарантированного полного удаления (затирания) контента (и не только) совсем несложно применить на практике. Тем более что все эти меры абсолютно бесплатны! Совсем скоро наступят времена (если они уже не наступили к моменту, когда вы читаете эту книгу), когда эти меры безопасности будут совсем не лишними.

СОДЕРЖАНИЕ

Практическое руководство пользователя

Василий Халявин

КОМПЬЮТЕРНЫЙ ДОКТОР

Надежная и бесплатная защита вашего компьютера

Редактор
Н. Торгашова
Корректор
О. Ковальчук
Разработка макета и верстка
Н. Привезенцевой

Подписано в печать 26.11.10.
Формат 60×90 $^{1}/_{16}$. Гарнитура SchoolBookC.
Печать офсетная. Усл. печ. л. 6,00. Уч.-изд. л. 4,68.
Тираж 50 000 экз. Заказ

«Ленинградское издательство»
191023, Санкт-Петербург,
пер. Апраксин, д. 4, лит. А, пом. 15Н
Телефон/факс: (812) 363-42-72

Отпечатано по технологии CTP
в ИПК ООО «Ленинградское издательство»
195009, Санкт-Петербург, ул. Арсенальная, д. 21/1
Телефон/факс: (812) 495-56-10