



**Руководство по**  
**Безопасности**  
**ПК**

**Ваше информационное руководство  
по усилению безопасности вашего  
персонального компьютера  
от вредоносных угроз!**

**[www.ebooksxe.ru](http://www.ebooksxe.ru)**

## **Руководство по безопасности ПК**

### **«Ваше руководство по улучшению производительности вашего персонального компьютера» Безопасность от вредоносных угроз!»**

#### **ЮРИДИЧЕСКОЕ УВЕДОМЛЕНИЕ**

Издатель стремился быть максимально точным и полным при создании этого отчета, несмотря на тот факт, что он не гарантирует и не заявляет в какой-либо момент, что его содержимое является точным из-за быстро меняющегося характера Интернет.

Хотя были предприняты все попытки проверить информацию, представленную в данной публикации, Издатель не несет ответственности за ошибки, упущения или противоположное толкование предмета настоящего документа. Любые предполагаемые неуважения к конкретным лицам, народам или организациям являются непреднамеренными.

В книгах с практическими советами, как и во всем остальном в жизни, не дается никаких гарантий дохода. Читателям рекомендуется отвечать на основе собственного суждения о своих индивидуальных обстоятельствах, чтобы действовать соответственно.

Эта книга не предназначена для использования в качестве источника юридических, деловых, бухгалтерских или финансовых консультаций. Всем читателям рекомендуется обратиться за услугами к компетентным профессионалам в области права, бизнеса, бухгалтерского учета и финансов.

Для удобства чтения рекомендуем вам распечатать эту книгу.

## Оглавление

Защита системы вашего компьютера  
Борьба со спамом  
Шпионское и рекламное ПО  
Фишинг и кража личных данных  
Компьютерные вирусы... и антивирусы  
Защита, которую вы можете себе позволить  
Рекомендуемые ресурсы

## Защита системы вашего компьютера

Сегодня все больше людей используют свои компьютеры для самых разных целей: от общения до онлайн-банкинга, от инвестиций до покупок.

Поскольку мы делаем это на более регулярной основе, мы открываем себя потенциальным хакерам, злоумышленникам и взломщикам. В то время как некоторые могут искать Ваши личные данные и личность для перепродажи, другие просто хотят использовать ваш компьютер как платформу для атак на другие ничего не подозревающие цели.

Ниже приведено несколько простых и экономически эффективных шагов, которые вы можете предпринять, чтобы сделать свой компьютер более безопасным для начала:

**1.** Всегда делайте резервные копии важной информации и храните ее в надежном месте отдельно от компьютера.

**2.** Регулярно обновляйте и устанавливайте исправления для вашей операционной системы, веб-браузера и программного обеспечения. Если у вас операционная система Windows, начните с перехода на страницу [www.windowsupdate.microsoft.com](http://www.windowsupdate.microsoft.com). и запуск мастера обновления. Эта программа поможет вам найти последние исправления для вашего компьютера Windows. Также перейдите на [www.officeupdate.microsoft.com](http://www.officeupdate.microsoft.com). и найдите возможные исправления для ваших программ Office.

**3.** Установите брандмауэр. Без хорошего брандмауэра вирусы, черви, трояны, вредоносное и рекламное ПО могут легко получить доступ к вашему компьютеру из Интернета. Следует рассмотреть преимущества и различия между аппаратными и программными брандмауэрами.

**4.** Проверьте настройки браузера и электронной почты для обеспечения оптимальной безопасности. Зачем вам это делать? Active-X и JavaScript часто используются хакерами для внедрения вредоносных программ в ваши компьютеры. Хотя файлы cookie относительно безвредны с точки зрения безопасности, они все равно отслеживают ваши перемещения в Интернете, чтобы создать Ваш профиль. Как минимум установите настройки безопасности для «зоны Интернета» на Высокий, а для «зоны доверенных сайтов» на Средний Низкий.

**5.** Установите антивирусное программное обеспечение и настройте его на автоматическое обновление, чтобы вы получали самые последние версии.

**6.** Не открывайте неизвестные вложения электронной почты.

Недостаточно просто узнать адрес, с которого он пришел, поскольку многие вирусы могут распространяться со знакомого адреса.

**7.** Не запускайте программы неизвестного происхождения. Также не отправляйте эти типы программ друзьям и коллегам, потому что они содержат забавные истории или шутки. Они могут содержать троянского коня, ожидающего заражения компьютера.

**8.** Отключить скрытые расширения файлов. По умолчанию операционная система Windows настроена на «скрытие файла расширения для известных типов файлов». Отключите эту опцию, чтобы расширения файлов отображались в Windows. Некоторые расширения файлов по умолчанию будут оставаться скрытыми, но вы с большей вероятностью увидите любые необычные расширения файлов, которые не относятся к ним.

**9.** Выключать ваш компьютер и отключайте его от сети, когда вы им не пользуетесь. Хакер не сможет атаковать ваш компьютер, если вы отключены от сети или компьютер выключен.

**10.** Рассмотрите возможность создания загрузочного диска на дискете на случай, если ваш компьютер повредится, взломан или скомпрометирован вредоносной программой. Очевидно, вам необходимо предпринять этот шаг до того, как вы столкнетесь с враждебным проникновением в вашу систему.



## **Быстрый компьютер за один день**

- Как всего за один день привести свой компьютер в порядок и ускорить его работу до 30-ти раз;
- Что скрывает Microsoft от нас, а также, как сделать любой компьютер Windows быстрым и полностью избавиться от системных сбоев и замедления работы;
- Как защитить свой компьютер от любых вирусов на 100%, даже если он без антивируса!

[\*\*Получить бесплатно >>\*\*](#)

## Борьба со спамом

Насколько распространен спам? По словам Скотта МакАдамса, отдела по связям с общественностью и коммуникациям ОМА ([www.oma.org](http://www.oma.org)):

«Исследования показывают, что нежелательная или «мусорная» электронная почта, известная как спам, составляет примерно половину всех электронных писем, полученных почтовых сообщений. Хотя когда-то спам считался не более чем неприятностью, его распространенность возросла до такой степени, что многие пользователи начали выражать общее недоверие к эффективности передачи электронной почты и увеличилась обеспокоенность по поводу распространения компьютерных вирусов через нежелательные сообщения».

В 2003 году президент Буш подписал законопроект «Can Spam», который стал первым национальным стандартом в отношении массовой коммерческой электронной почты, не запрашиваемой электронной почтой. Законопроект, одобренный Сенатом 97 голосами против 0, запрещает отправителям не запрашиваемой коммерческой электронной почты использовать ложные обратные адреса для сокрытия своей личности (спуфинг) и использовать словари для создания таких почтовых рассылок.

Кроме того, он запрещает использование вводящих в заблуждение тем и требует, чтобы электронные письма включали механизм отказа. Законодательство также запрещает отправителям собирать адреса с веб-сайтов.

Нарушения представляют собой правонарушение, караемое лишением свободы на срок до одного года.

В связи с этим необходимо обсудить один важный момент: спам теперь приходит из других стран во все больших количествах. С этими электронными письмами сложнее бороться, потому что они приходят из-за пределов законов и правил нашей страны. Поскольку Интернет открывает границы и мыслит глобально, эти законы хороши, но не решают проблему.

Так что же с этим делать??

Вот 5 основных правил, которые следует соблюдать для защиты от спама:

**Номер 1:** Сделайте все возможное, чтобы ваш адрес электронной почты не был опубликован в сети.

Есть программы, которые называются «спам-пауки», которые ищут в Интернете адреса электронной почты для отправки электронной почты. Если вам интересно, выполните поиск по «спам-паук» и вы будете

поражены тем, что вы получите обратно. Интересно, что есть сайт, WebPoison.org, который является проектом с открытым исходным кодом, направленным на борьбу с Интернет-спамботами и "спам-пауками", предоставляя им поддельные HTML-страницы, содержащие поддельные адреса электронной почты.

Предложения для вас:

**А)** Используйте формы электронных писем, которые могут скрывать адреса или также

**В)** Используйте такие адреса, как продажи@company.com вместо вашего полного адреса, чтобы помочь справиться с проблемой.

**С)** Существуют также программы, которые кодируют вашу электронную почту, например jsGuard, который кодирует ваш адрес электронной почты на веб-страницах таким образом, что спам-паукам становится трудно или невозможно прочитать ваш адрес электронной почты.

**Номер 2:** Установите программное обеспечение для блокировки спама.

Для этого существует множество программ. (Перейдите на [www.cloudmark.com](http://www.cloudmark.com) или [www.mailwasher.net](http://www.mailwasher.net) например). Вы также можете купить профессиональную версию. Что бы вы ни делали, приобретите программное обеспечение. Это сэкономит вам время. Программное обеспечение не является полностью надежным, но оно действительно помогает. Обычно вам приходится выполнять некоторые ручные настройки, чтобы заблокировать определенные типы электронной почты.

**Номер 3:** Используйте подход с несколькими адресами электронной почты.

Есть много бесплатных адресов электронной почты, которые можно иметь. Если вы должны подписываться на рассылки, то заведите «запасной» адрес электронной почты. Это было бы похоже на то, как если бы вы давали свой номер телефона продавцу лучшим друзьям, а рабочий номер — всем остальным.

**Номер 4:** Приложение энты от людей, которых вы не знаете, ПЛОХИЕ, ПЛОХИЕ, ПЛОХИЕ.

Распространенная проблема со спамом заключается в том, что у них есть вложения, а вложения могут содержать вирусы. Корпорации часто используют фильтры, которые не пропускают такие вещи к вам. Личная электронная почта — гораздо более «открытая страна» для спамеров. Общее правило: если вы не знаете, кто вам что-то отправляет, НЕ ОТКРЫВАЙТЕ ВЛОЖЕНИЕ. Во-вторых, ищите сервисы, которые предлагают фильтрацию. Поставщики брандмауэров также предлагают этот тип услуг.

[Бесплатные электронные книги для заработка в интернет](#)

**Номер 5:** Теперь у служб электронной почты есть корзины для «массовой почты».

Если то, что вы используете в настоящее время, не поддерживает это, подумайте о переходе к новому поставщику. Концепция проста. Если вы знаете кого-то, он может отправлять вам электронные письма. Если вы их не знаете, поместите их в стопку массовых рассылок, а затем «выберите» впустите их в свой круг. Программное обеспечение для блокировки спама также имеет эту концепцию, но наличие дополнительных слоев кажется критически важным в наши дни, поэтому стоит рассмотреть этот вариант.



## Свободный Интернет за один час

**Как обеспечить безопасность и анонимность в сети,  
а также получить доступ ко-всем ресурсам уже  
сегодня...**



Видеокурс "Свободный Интернет" состоит из 9 разделов, общей продолжительностью 1 час 16 минут + бонусные разделы, которые пополняются постоянно новыми уроками! Просмотрев этот курс, Вы уже сегодня будете знать всё, что необходимо для доступа к любому заблокированному ресурсу и обеспечения конфиденциального использования сети Интернет.

[Узнать подробнее>>](#)



## Шпионское и рекламное ПО

Шпионское и рекламное ПО — это не только постоянно растущее неудобство для пользователей компьютеров по всему миру, но также и бурно развивающаяся отрасль.

По данным Webroot Software, Inc., распространение онлайн-рекламы с помощью шпионского и рекламного ПО стало колоссальной проблемой.

Агрессивная реклама и шпионская тактика, продемонстрированная некоторыми из этих программ, требуют столь же агрессивного ответа от опытного искоренителя. Sunbelt Software — именно такая компания. Лидер в области антишпионского ПО, антиспама, сетевой безопасности и инструментов управления системами, они неизменно оставались на

[Бесплатные электронные книги для заработка в интернет](#)

переднем крае антишпионского программирования с 1994 года.

Итак, вы можете спросить:

«Почему у меня такое чувство, будто за мной кто-то наблюдает?»

По данным Национального альянса по кибербезопасности, шпионское ПО заражает более 90% из всех ПК сегодня. Эти незаметные вредоносные программы предназначены для скрытного обхода брандмауэров и антивирусного ПО без ведома пользователя.

После внедрения в компьютер он может нанести ущерб производительности системы, собирая ваши персональные данные. К счастью, в отличие от вирусов и червей, программы-шпионы обычно не самовоспроизводятся.

### **Откуда это взялось?**

Обычно шпионское ПО появляется тремя способами. Первый и наиболее распространенный способ — когда его устанавливает пользователь. В этом сценарии шпионское ПО встраивается, прикрепляется или связывается с бесплатной или условно-бесплатной программой без ведома пользователя. Пользователь загружает программу на свой компьютер.

После загрузки программа-шпион начинает собирать данные для личного использования автором программы-шпиона или для продажи третьей стороне. Остерегайтесь многих программ обмена файлами P2P. Они печально известны загрузками, содержащими программы-шпионы.

Пользователь загружаемой программы должен обратить особое внимание на сопровождающее лицензионное соглашение. Часто издатель программного обеспечения предупреждает пользователя о том, что вместе с запрашиваемой программой будет установлена шпионская программа.

К сожалению, мы не все способны уделить время чтению мелкого шрифта.

Некоторые соглашения могут предусматривать специальные поля «отказа», которые пользователь может нажать, чтобы остановить включение шпионского ПО в загрузку. Обязательно ознакомьтесь с документом, прежде чем подписывать загрузку.

Другой способ, которым шпионское ПО может получить доступ к вашему компьютеру, — это обманом заставить вас манипулировать функциями безопасности, разработанными для предотвращения любых нежелательных установок. Веб-браузер Internet Explorer был разработан так, чтобы не позволять веб-сайтам начинать любые нежелательные

загрузки. Вот почему пользователь должен инициировать загрузку, нажав на ссылку. Эти ссылки могут оказаться обманчивыми.

Например: на экране может появиться всплывающее окно, смоделированное по образцу стандартного диалогового окна Windows. В сообщении может быть задан вопрос, хотите ли вы оптимизировать свой доступ в Интернет. Оно предоставляет кнопки ответа «да» или «нет», но, независимо от того, какую кнопку вы нажмете, начнется загрузка, содержащая шпионскую программу. Новые версии Internet Explorer теперь немного усложняют этот путь шпионского ПО.

Наконец, некоторые шпионские приложения заражают систему, атакуя уязвимости в веб-браузере или другом программном обеспечении. Когда пользователь переходит на веб-страницу, контролируруемую автором шпионского ПО, эта страница содержит код, предназначенный для атаки на браузер и принудительно установить шпионскую программу.

### **Что могут делать программы-шпионы?**

Программы-шпионы могут выполнять множество вредоносных задач. Некоторые их действия просто раздражают пользователя, другие могут стать откровенно агрессивными по своей природе.

#### **Шпионское ПО может:**

- ⇒Отслеживать нажатия клавиш для составления отчетов.
- ⇒Сканировать файлы, расположенные на жестком диске.
- ⇒Просматривать приложения на нашем рабочем столе.
- ⇒Устанавливать на свой компьютер другие шпионские программы.
- ⇒Прочитать ваши куки.
- ⇒Кража номеров кредитных карт, паролей и другой личной информации.
- ⇒Изменить настройки по умолчанию на домашней странице веб-браузера.
- ⇒Мутировать во второе поколение шпионского ПО, что затрудняет его искоренение.
- ⇒Заставить ваш компьютер работать медленнее.
- ⇒Показывать раздражающую всплывающую рекламу.
- ⇒Добавлять рекламные ссылки на веб-страницы, за которые автор не получает оплату. Вместо этого оплата направляется программисту шпионского ПО, который изменил исходные настройки партнера.
- ⇒Не предоставлять пользователю возможности удаления и размещается в неожиданных или скрытых местах вашего компьютера, что затрудняет его удаление.

### **Примеры шпионского ПО**

Вот несколько примеров часто встречающихся программ-шпионов:

[Бесплатные электронные книги для заработка в интернет](#)

(Обратите внимание, что хотя исследователи часто дают названия шпионским программам, они могут не совпадать с названиями, которые используют авторы шпионских программ.)

CoolWebSearch, группа программ, которые устанавливаются через «дыры» в Internet Explorer. Эти программы направляют трафик на рекламу на веб-сайтах, включая coolwebsearch.com. Эта шпионская программа-вредительница отображает всплывающую рекламу, переписывает результаты поисковой системы и изменяет файл хоста компьютера, чтобы указать системе доменных имен (DNS) искать предварительно выбранные сайты.

Интернет-оптимизатор (а/к/а DyFuCa), любит перенаправлять страницы ошибок Internet Explorer на рекламу. Когда пользователь переходит по неработающей ссылке или вводит ошибочный URL, всплывает страница с рекламой.

180 Решений сообщает обширную информацию рекламодателям о веб-сайтах, которые вы посещаете. Он также изменяет HTTP-запросы для филиала рекламных объявлений, связанных с веб-сайтом. Таким образом, компания 180 Solutions получает незаработанную прибыль от кликов по измененным ими рекламным объявлениям.

HuntBar (также известный как WinTools) или Рекламное ПО. Веб-поиск, распространяется ТрафикСиндикат и устанавливается путем загрузки ActiveX drive-by на партнерских веб-сайтах или через рекламу, отображаемую другими программами-шпионами. Это яркий пример того, как программы-шпионы могут установить больше шпионских программ. Эти программы добавляют панели инструментов в Internet Explorer, отслеживают поведение пользователей при просмотре веб-страниц и показывают рекламу.

### **Как предотвратить или бороться со шпионским ПО?**

Есть несколько вещей, которые вы можете сделать, чтобы предотвратить заражение вашего компьютера шпионским ПО компьютерную систему. Во-первых, инвестируйте в надежную коммерческую антишпионскую программу. В настоящее время на рынке представлено несколько программ, включая отдельные пакеты, такие как Ad-Aware от Lavasoft или Антишпионское ПО для Windows. Другие варианты предоставляют антишпионское программное обеспечение как часть антивирусного пакета.

Этот тип опции предлагают такие компании, как Sophos, Symantec и McAfee. Антишпионские программы могут бороться со шпионским ПО, обеспечивая защиту в реальном времени, сканирование и удаление любого найденного шпионского ПО. Как для большинства программ регулярно

обновляйте антивирусное ПО.

Как уже говорилось, Internet Explorer (IE) часто является источником проблемы шпионского ПО, поскольку шпионские программы любят прикрепляться к его функционалу. Шпионское ПО любит проникать в слабые стороны IE.

Из-за этого многие пользователи перешли на браузеры, отличные от IE. Однако, если вы предпочитаете использовать Internet Explorer, обязательно регулярно обновляйте исправления безопасности и загружайте программы только из надежных источников. Это поможет снизить вероятность проникновения шпионского ПО.

### **А когда все остальное терпит неудачу?**

Заметили, что я сказал «когда», а не «если»? Поскольку вредоносное ПО растёт и легко охватывает более 90% компьютеров (это вы и я, 9 из 10!), единственное решение вам, возможно, придется сделать резервную копию данных и выполнить полную переустановку Операционная система!



## **Быстрый браузер**



Устали искать закладки в панели браузера своего компьютера? Быстрый браузер позволяет держать открытыми множество вкладок без расходования ресурсов компьютера и значительно экономит затраты времени. Надоело устанавливать разные VPN и настраивать на нужную страну? Главное преимущество Быстрого браузера - это встроенный VPN. Для некоторых сервисов он сам настраивается на нужную страну. В этом его интеллектуальная способность.

**[Это и множество других плюшек предоставляет "Быстрый браузер">>](#)**

## Фишинг и кража личных данных

Кто не получал письмо, направляющее их на знакомый веб-сайт, где их просят обновить личную информацию? Веб-сайт требует от вас проверить или обновить ваши пароли, номера кредитных карт, номер социального страхования или даже номер вашего банковского счета. Вы узнаете название компании, поскольку вы вели с ней бизнес в прошлом.

Итак, вы нажимаете на удобную ссылку «перейти туда» и продолжаете предоставлять всю запрошенную ими информацию. К сожалению, гораздо позже выясняется, что сайт поддельный. Он был создан с единственной целью — украсть вашу личную информацию.

Тебя, мой друг, только что «обманули».

Фишинг (произносится как «рыбалка») определяется как действие по отправке электронного письма получателю с ложным указанием утверждая, что у вас есть устоявшийся, законный бизнес. Цель фишера заключается в том, чтобы обманом заставить получателя предоставить свою личную информацию, и в конечном итоге украсть вашу личность.

Это не легко как вы думаете, чтобы обнаружить фишинговое письмо с целью получения информации. На первый взгляд, письмо может выглядеть так, как будто оно от законной компании. Поле «От» электронного письма может содержать адрес .com компании, упомянутой в письме. Щелкающая ссылка даже, кажется, ведет на веб-сайт компании, когда на самом деле это поддельный сайт, созданный для копирования настоящего сайта.

Многие из этих людей — профессиональные преступники. Они потратили много времени на создание писем, которые выглядят подлинными. Пользователям необходимо внимательно просматривать все письма, запрашивающие персональные данные. При просмотре своего письма помните, что поле «От» может быть легко изменено отправителем. Хотя может показаться, что оно пришло с .com, с которым вы ведете бизнес, внешний вид может быть обманчивым.

Также имейте в виду, что фишер будет стараться изо всех сил, чтобы его электронное письмо выглядело как можно более легитимным. Они даже копируют логотипы или изображения с официального сайта, чтобы использовать их в своих электронных письмах. Наконец, они любят включать кликабельную ссылку, по которой получатель может перейти, чтобы удобно обновить свою информацию.

Отличный способ проверить легитимность ссылки — навести на нее мышью. Затем посмотрите на нижний левый экран вашего компьютера. Фактический адрес веб-сайта, на который вы направляетесь, будет показан для просмотра. Это очень быстрый и простой способ проверить,

перенаправляетесь ли вы на законный сайт.

Следуйте золотому правилу: никогда, никогда не нажимайте на ссылки в тексте электронного письма и всегда немедленно удаляйте электронное письмо. После того, как вы удалили электронное письмо, очистите также корзину в ваших учетных записях электронной почты. Если вы действительно обеспокоены тем, что вы пропустили важное уведомление относительно одной из ваших учетных записей, введите полный URL-адрес веб-сайта в ваш браузер. По крайней мере, тогда вы можете быть уверены, что вас действительно направляют на настоящий и законный веб-сайт.

## **Развитие кейлоггера**

Кейлоггер — это программа, которая работает в фоновом режиме на вашем компьютере, тайно записывает все ваши нажатия клавиш. После того, как ваши нажатия клавиш записываются, они скрываются для последующего извлечения злоумышленником. Затем злоумышленник внимательно просматривает информацию в надежде найти пароли или другую информацию, которая может оказаться ему полезной.

Например, кейлоггер может легко получить конфиденциальные электронные письма и раскрыть их любой заинтересованной сторонней стороне, готовой заплатить за эту информацию.

Кейлоггеры могут быть как программными, так и аппаратными..

Программное обеспечение Кейлоггеры легко распространять и заражать, но в то же время их легче обнаружить.

Аппаратный Кейлоггеры сложнее и их сложнее обнаружить. Насколько вам известно, на вашей клавиатуре может быть установлен чип кейлоггера, и все, что вы печатаете, записывается во флэш-память, находящуюся внутри вашей клавиатуры. Кейлоггеры стали одним из самых мощных приложений, используемых для сбора информации в мире, где зашифрованный трафик становится все более распространенным.

По мере того, как кейлоггеры становятся все более продвинутыми, их становится все сложнее обнаружить. Они могут нарушать конфиденциальность пользователя в течение месяцев или даже лет, оставаясь незамеченными. За это время кейлоггер может собрать много информации о пользователе, за которым он следит. Кейлоггер может потенциально получить не только пароли и имена для входа, но и номера кредитных карт, данные банковских счетов, контакты, интересы, привычки просмотра веб-страниц и многое другое. Вся эта собранная информация может быть использована для кражи личных документов пользователя, денег или даже его личности.

Кейлоггер может быть таким же простым, как .exe и .dll который помещается в компьютер и активируется при загрузке через запись в реестре. Или более сложные кейлоггеры, такие как Perfect Keylogger или ProBot Activity Monitor, разработали целый ряд отвратительных способностей, включая:

- ⇒ Необнаружимый в списке процессов и невидим в работе
- ⇒ Драйвер кейлоггера ядра, который фиксирует нажатия клавиш, даже если пользователь вышел из системы
- ⇒ Мастер удаленного развертывания
- ⇒ Возможность создания текстовых снимков активных приложений
- ⇒ Возможность сбора данных HTTP-постов (включая логины/пароли)
- ⇒ Возможность ставить временные метки при использовании рабочей станции
- ⇒ Экспорт файла журнала в формате HTML и текстового файла
- ⇒ Автоматическая доставка файла журнала по электронной почте

Все кейлоггеры используются в незаконных целях. Появилось множество других вариантов использования. Кейлоггеры использовались для мониторинга посещаемых веб-сайтов в качестве средства родительского контроля над детьми. Они активно использовались для предотвращения детской порнографии и предотвращения контакта детей с опасными элементами в Интернете.

### **Что такое системы обнаружения вторжений?**

Системы обнаружения вторжений (IDS) являются необходимой частью любой стратегии безопасности предприятия. Что такое системы обнаружения вторжений? CERIAS, Центр образования и исследований в области обеспечения безопасности информации, определяет это следующим образом:

Цель системы обнаружения вторжений (IDS) — обнаружение несанкционированного доступа или неправильного использования компьютерной системы. Системы обнаружения вторжений — это своего рода сигнализация для компьютеров. Они подают звуковой сигнал и иногда даже предпринимают корректирующие действия при обнаружении злоумышленника или нарушителя.

Разработано множество различных систем обнаружения вторжений, но схемы обнаружения обычно попадают в одну из двух категорий: обнаружение аномалий и обнаружение неправомерного использования.

Детекторы аномалий ищут поведение, которое отклоняется от обычного использования системы. Детекторы неправильного использования ищут поведение, которое соответствует известному сценарию атаки. В обнаружение вторжений вложено много времени и усилий, и этот список содержит ссылки на множество сайтов, где

обсуждаются некоторые из этих усилий

([http://www.cerias.purdue.edu/about/history/coast\\_resources/intrusion\\_detection/](http://www.cerias.purdue.edu/about/history/coast_resources/intrusion_detection/))

Существует подкатегория систем обнаружения вторжений, называемая сетевыми системами обнаружения вторжений (NIDS). Эти системы отслеживают пакеты на сетевом проводе и ищут подозрительную активность. Системы обнаружения сетевых вторжений могут контролировать много компьютеров одновременно по сети, в то время как другие системы обнаружения вторжений могут контролировать только один.

### **Кто взламывает вашу систему?**

Одно из распространенных заблуждений относительно хакеров программного обеспечения заключается в том, что обычно люди за пределами вашей сети взламывают ваши системы и устраивают хаос. Реальность, особенно для корпоративных работников, заключается в том, что инсайдеры могут и обычно вызывают большинство нарушений безопасности. Инсайдеры часто выдают себя за людей с большими привилегиями, чем они сами, чтобы получить доступ к конфиденциальной информации.

### **Как злоумышленники проникают в вашу систему?**

Самый простой и легкий способ взлома — предоставить кому-то физический доступ к системе. Несмотря на все усилия, часто бывает невозможно остановить кого-то, получившего физический доступ к машине.

Кроме того, если у кого-то уже есть учетная запись в системе с низким уровнем доступа, еще один способ взлома — использовать уловки, получить более высокие привилегии через дыры в вашей системе. Наконец, есть много способов получить доступ к системам, даже если один работает удаленно. Борьба с удаленными методами вторжения стало сложнее и труднее.

### **Как остановить вторжения?**

Существует несколько бесплатных/условно-бесплатных систем обнаружения вторжений, а также коммерческих систем обнаружения вторжений.

**Системы обнаружения вторжений с открытым исходным кодом**

Ниже приведены несколько систем обнаружения вторжений с открытым исходным кодом:

**ПОМОЩНИК** (<http://sourceforge.net/projects/aide>)- Описывает себя как «AIDE (Advanced Intrusion Detection Environment) — это бесплатная замена Tripwire. Она делает то же самое, что и полубесплатный Tripwire, и даже больше. Существуют и другие бесплатные замены, так зачем создавать новую? Все остальные замены не достигают уровня Tripwire. А мне нужна была программа, которая бы превзошла ограничения Tripwire».

Файловая система **Saint** (<http://sourceforge.net/projects/fss>)- Описывая себя, «File System Saint — это легкая хостовая система обнаружения вторжений, в которой основное внимание уделяется скорости и простоте использования».

**Фырканье** ([www.snort.org](http://www.snort.org))- Описывая себя как «Snort® — это система обнаружения и предотвращения сетевых вторжений с открытым исходным кодом, использующая язык правил, который сочетает в себе преимущества методов проверки на основе сигнатур, протоколов и аномалий. На сегодняшний день Snort имеет миллионы загрузок и является наиболее широко используемой технологией обнаружения и предотвращения вторжений во всем мире и стала фактическим стандартом для отрасли».

### **Коммерческие системы обнаружения вторжений**

Если вы ищете коммерческие системы обнаружения вторжений, вот несколько из них:

Растяжка  
<http://www.tripwire.com>

Touch Technology Inc (детектор вторжений POLYCENTER Security)  
<http://www.ttinet.com>

Системы безопасности в Интернете (Real Secure Server Sensor)  
<http://www.iss.net>

eEye Digital Security (защита веб-сервера SecureIIS)  
<http://www.eeye.com>

### **Анонимный веб-серфинг — вопросы, которые следует задать**

Когда вы бродите по сети, о вас могут узнать информацию, даже если вы не хотите афишировать, кто вы. Это справедливо даже в том случае, если ваша система не содержит вирусов или вредоносного программного обеспечения.

[Бесплатные электронные книги для заработка в интернет](#)

В частности, информация, которая легко доступна в сети, включает ваш IP-адрес, вашу страну (и часто дополнительную информацию о местоположении на основе IP-адреса), какую компьютерную систему вы используете, какой браузер вы используете, историю вашего браузера и другую информацию. Дальше будет еще хуже.

Люди могут узнать имя вашего компьютера и даже узнать ваше имя, если ваша машина поддерживает такие программы, как finger или identd. Кроме того, файлы cookie могут отслеживать ваши привычки, когда вы переходите с одной машины на другую.

### **Как люди получают эту базовую информацию о тебе?**

Когда вы посещаете другой веб-сайт, информация о вас может быть извлечена. По сути, информация перехватывается и используется другими для отслеживания вашей интернет-активности.

### **Как этого не допустить?**

Прежде всего, можно анонимно серфить в сети и тем самым перестать оставлять следы, которые могут найти другие. Обратите внимание, что это не является абсолютно надежным, но это значительно усложняет для людей возможность узнать, кто вы. Существуют продукты, называемые анонимными прокси-серверами, которые помогают защитить вас. Анонимный Прокси-сервер заменяет ваш интернет-адрес на свой собственный. Это скрывает ваш IP-адрес и значительно затрудняет отслеживание вас другими людьми.

### **Как получить анонимный прокси-сервер?**

Есть много поставщиков, которые продают анонимные прокси-серверы. Вам также доступны бесплатные прокси-серверы. Два таких продукта — ShadowSurf и Guardster. Guardster (<http://www.guardster.com/>) предлагает различные услуги для анонимного и безопасного доступа к сети, некоторые платные, а также бесплатный сервис. ShadowSurf (<http://www.shadowsurf.com/>) ShadowSurf предоставляет анонимный серфинг на своем сайте бесплатно. Зайдите на него и вы увидите поле для ввода URL, который вы не хотите, чтобы кто-то отслеживал. Есть много других, но вот эти два, которые часто используются.

Еще один интересный продукт, учитывая недавние новости о том, что поисковая система Google фильтрует свои результаты для китайского правительства, — это Anonymizer (<http://www.anonymizer.com>). Эта компания, среди прочих, заявила, что она «разрабатывает новое антицензурное решение, которое позволит гражданам Китая безопасно получать доступ ко всему Интернету без фильтров».

([http://www.anonymizer.com/consumer/media/press\\_releases/02012006.html](http://www.anonymizer.com/consumer/media/press_releases/02012006.html))

).

## **Обеспечивает ли анонимный прокси-сервер 100% безопасность?**

Нет. Тем не менее, вам будет гораздо лучше, если вы воспользуетесь такой технологией.

## **О чем еще мне следует беспокоиться, пытаясь сохранить конфиденциальность своей личной информации?**

Три других пункта приходят на ум, когда пытаешься сохранить конфиденциальность своей информации. Во-первых, вы можете использовать зашифрованное соединение, чтобы скрыть свой серфинг. В этой статье мы не будем вдаваться в подробности, но поищите в Интернете, и вы найдете много информации по этому поводу. Во-вторых, удаляйте файлы cookie после каждого сеанса. В-третьих, вы можете настроить свой браузер на удаление JavaScript, Java и активного контента. Это на самом деле приводит к ограничениям, поэтому вам нужно подумать о стоимости/выгоде этого курса действий.



## **Антикатастрофа**

С этого момента вы больше никогда не будете пользоваться услугами "компьютерной скорой помощи", поскольку сами сможете в автоматическом режиме восстановить свою операционную систему, установленные программы и их настройки, а также персональные файлы. Одно это сэкономит вам кучу нервов, времени и денег.

[Узнать подробнее>>](#)



## **Компьютерные вирусы... и антивирусы**

Каждый день создаются новые компьютерные вирусы, чтобы раздражать нас и сеять хаос в наших компьютерных системах. Ниже приведены десять вирусов, которые в настоящее время считаются наиболее распространенными с точки зрения их наибольшего распространения или их способности потенциально наносить ущерб.

Новые вирусы создаются ежедневно. Это далеко не полный список. Лучшее, что вы можете сделать, — это сохранять бдительность, обновлять

[Бесплатные электронные книги для заработка в интернет](#)

антивирусное программное обеспечение и быть в курсе текущих угроз компьютерных вирусов.

**Вирус: Trojan.Lodear**

Троянский конь, который пытается загрузить удаленные файлы. Он внедряет файл .dll в процесс EXPLORER.EXE, вызывая нестабильность системы.

**Вирус: W32.Beagle.CO@mm**

Червь массовой рассылки, снижающий настройки безопасности. Он может удалять подключения реестра, связанные с безопасностью, и блокировать доступ к веб-сайтам, связанным с безопасностью.

**Вирус: Backdoor.Zagaban**

Троянский конь, позволяющий использовать взломанный компьютер в качестве скрытого прокси-сервера и способный снизить производительность сети.

**Вирус: W32/Netsky-P**

Червь массовой рассылки, который распространяется посредством отправки сообщений электронной почты на адреса, созданные из файлов на локальных дисках.

**Вирус: W32/Mytob-GH**

Червь массовой рассылки и IRC-бэкдор-троян для платформы Windows. Сообщения, отправляемые этим червем, будут иметь тему, выбранную случайным образом из списка, включающего заголовки. Например: уведомление об ограничении учетной записи, приостановка действия учетной записи электронной почты, меры безопасности, поддержка участников, важное уведомление.

**Вирус: W32/Mytob-EX**

Червь массовой рассылки и IRC-бэкдор-троян, по своей природе схожий с W32-MytobGH. W32/Mytob-EX постоянно работает в фоновом режиме, предоставляя бэкдор-сервер, который позволяет удаленному злоумышленнику получить доступ и контроль над компьютером через каналы IRC. Этот вирус распространяется, отправляя себя во вложениях электронной почты, собранных с ваших адресов электронной почты.

**Вирус: W32/Mytob-AS, Mytob-BE, Mytob-C и Mytob-ER**

Это семейство разновидностей червей обладает схожими характеристиками с точки зрения того, что они могут делать. Это черви массовой рассылки с функцией бэкдора, которыми можно управлять через сеть Internet Relay Chat (IRC). Кроме того, они могут распространяться через электронную почту и различные уязвимости операционных систем, такие как LSASS (MS04-011).

**Вирус: Зафи-Д**

[Бесплатные электронные книги для заработка в интернет](#)

Червь массовой рассылки и одноранговый червь, который копирует себя в систему Windows папку с именем файла Norton Update.exe. Затем он может создать несколько файлов в системной папке Windows с именами, состоящими из 8 случайных символов и расширением DLL. W32/Zafi-D копирует себя в папки с именами, содержащими share, upload или музыку как ICQ 2005a new!.exe или winamp 5.7 new!.exe. W32/Zafi-D. Также отобразит поддельное окно сообщения об ошибке с заголовком "CRC: 04F6Bh" и текстом "Ошибка в упакованном файле!".

#### Вирус: **W32/Netsky-D**

Червь массовой рассылки с функцией бэкдора IRC, который также может заражать компьютеры, уязвимые для эксплойта LSASS (MS04-011).

#### Вирус: **W32/Zafi-B**

Червь одноранговой сети (P2P) и электронной почты, который копирует себя в системную папку Windows как файл EXE со случайным именем. Этот червь проверяет наличие интернет-соединения, пытается подключиться к [www.google.com](http://www.google.com) или [www.microsoft.com](http://www.microsoft.com). Двухязычный червь с прикрепленным текстовым сообщением на венгерском языке, которое переводится как «Мы требуем что правительство принимает бездомных, ужесточает уголовный кодекс и ГОЛОСУЕТ ЗА СМЕРТНУЮ КАЗНЬ, чтобы сократить рост преступности. Июнь 2004 г., Печ (SNAF) Команда)»

### **Троянский конь – греческий миф или компьютерный враг?**

Мы все слышали термин «троянский конь», но что это такое? Троянский конь — это разрушительная программа, которая маскируется под безвредное приложение. В отличие от вируса, Троянский Конь не воспроизводит себя, но он может быть столь же разрушительным. Один из самых опасных примеров Троян это программа, которая обещает избавить ваш компьютер от вирусов, но вместо этого вводит вирусы в ваш компьютер.

Троян может быть коварен. Кто не был в сети и не сталкивался с всплывающей рекламой, утверждающей, что может избавить ваш компьютер от какого-то неприятного вируса? Или, что еще страшнее, вы получаете электронное письмо, которое якобы предупреждает вас о новом вирусе, который может угрожать вашему компьютеру. Отправитель обещает быстро искоренить или защитить ваш компьютер от вирусов, если вы просто загрузите их «бесплатное» прилагаемое программное обеспечение на свой компьютер. Вы можете быть скептически настроены, но программное обеспечение выглядит законным, а компания кажется авторитетной. Вы продолжаете принимать их предложение и скачивать программное обеспечение. Поступая так, вы только что потенциально подвергаете себя сильной головной боли, а свой компьютер — длинному списку недугов.

При активации трояна может произойти множество вещей. Некоторые трояны скорее раздражают, чем вредоносны. Некоторые из менее раздражающих троянов могут изменить настройки вашего рабочего стола или добавить глупые значки на рабочий стол. Более серьезные трояны могут стирать или перезаписывать данные на вашем компьютере, портить файлы, распространять другие вредоносные программы, такие как вирусы, шпионить за пользователем компьютера и тайно сообщать данные, такие как привычки просмотра, другим людям, регистрировать нажатия клавиш для кражи информации, такой как пароли и номера кредитных карт, фишинговать для получения данных банковских счетов (которые могут использоваться для преступной деятельности) и даже установить бэкдор в вашей компьютерной системе, чтобы они могли приходить и уходить, когда им заблагорассудится.

Чтобы повысить свои шансы не столкнуться с трояном, следуйте следующим рекомендациям:

Оставайтесь прилежными.

Трояны могут заразить ваш компьютер через мошеннические веб-сайты, мгновенные сообщения и электронные письма с вложениями. Не загружайте ничего на свой компьютер, если вы не уверены на 100 процентов в отправителе или источнике.

Убедитесь, что ваша операционная система всегда обновлена. Если вы используете операционную систему Microsoft Windows, это необходимо.

Установите надежное антивирусное программное обеспечение. Также важно, чтобы вы часто загружали обновления, чтобы ловить все новые троянские кони, вирусы и черви. Убедитесь, что выбранная вами антивирусная программа также может сканировать электронные письма и файлы, загружаемые через Интернет.

Рассмотрите возможность установки брандмауэра.

Брандмауэр — это система, которая предотвращает несанкционированное использование и доступ к вашему компьютеру. Брандмауэр не устранит проблемы с вирусами на вашем компьютере, но при использовании в сочетании с регулярными обновлениями операционной системы и надежным антивирусным программным обеспечением он может обеспечить дополнительную безопасность и защиту для вашего компьютера.

Ничто не может гарантировать безопасность вашего компьютера на 100 процентов. Однако вы можете продолжать повышать безопасность своего компьютера и снижать вероятность заражения, последовательно следуя этим рекомендациям.

## **Кто является игроками антивирусной индустрии?**

Каждый в Соединенных Штатах слышал о ведущих поставщиках антивирусных программ. Symantec, Макафи, Компьютерные партнеры, и Тренд Микро. Эти компании занимают лидирующие позиции на рынке США.

Майкрософт также стал Ключевым игроком на этом рынке. Microsoft приобрела интеллектуальную собственность и технологии у GeCad software в 2003 году, компании из Бухареста, Румыния. Они также приобрели Pelican Software, которая имела безопасность на основе поведения, а также Giant Company Software для шпионского ПО и Sybari Software, которая управляет фильтрацией вирусов, спама и фишинга.

Много дискуссий было сосредоточено на том, сможет ли Microsoft занять доминирующее положение на рынке антивирусов, просто бесплатно связав свои технологии со своими операционными системами. Это аналогичный метод, применяемый на других рынках, таких как обработка текста и интернет-браузеры.

Конечно, есть ряд поставщиков антивирусов, которые также играют на этом рынке. Есть много компаний с большим присутствием на рынке в других странах, которые начинают становиться все более широко известными. Эти поставщики включают GriSoft из Чешской Республики, Sophos в Великобритании, Panda Software в Испании, Kaspersky в России, SoftWin в Румынии, F-Secure в Финляндии, Norman в Норвегии, Arcabit в Польше, VirusBuster в Венгрии и AhnLab в Южной Корее.

Неясно, куда движется отрасль, и все на этом рынке сталкиваются с быстро меняющейся обстановкой. Объем усилий по поиску и предоставлению исправлений для вирусов ошеломляет. Вредоносные программы становятся все более сложными, а их число растет. Многие компании могут оказаться без ресурсов, чтобы соответствовать усилиям тех, кто действительно настроен на создание хаоса.

Некоторые компании, занимающиеся вирусами, получают сотни новых образцов в день! Более того, новые вирусы становятся «умнее» в том смысле, что они быстро размножаются, часто прячутся и достаточно умны, чтобы перемещаться в системе, переименовывая себя в попытке затруднить удалите их.

## **Защита, которую вы можете себе позволить**

В общем, есть многочисленные способы, которыми вы можете потерять информацию на вашем компьютере. Ваш ребенок решает сыграть Шопена на вашей клавиатуре, скачок напряжения, молния, вирус или даже простой сбой оборудования. Поэтому резервное копирование содержимого

вашего жесткого диска является **ОБЯЗАТЕЛЬНЫМ**. Регулярно делая резервные копии ваших файлов и сохраняя их в отдельном месте, вы, как правило, можете вернуть часть, если не всю, вашу информацию в случае сбоя вашего компьютера.

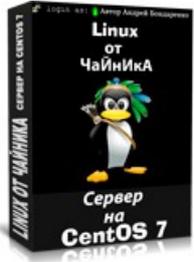
Хотя обычное резервное копирование на дискету, CD или zip-диск сохранит ваши файлы, разве не было бы здорово, если бы вы могли создать точную копию (образ диска) вашего жесткого диска? Это означает резервные копии всех ваших файлов, программ и пользовательских настроек. Это определенно сэкономит вам время, когда дело дойдет до перезагрузки. Acronis может помочь.

Acronis истинный образ 9.0 — это надежное программное обеспечение для создания образа диска, которое копирует все содержимое вашего жесткого диска, включая данные и файлы операционной системы, персонализированные настройки и многое другое, на другой диск или раздел диска. Его структура проста в использовании и навигации. Он также включает в себя мастеров, которые могут провести вас через резервное копирование и восстановление вашего компьютера. Основные функции включают в себя:

Безопасная зона — позволяет сохранять данные на специальном скрытом разделе, расположенном на жестком диске, что избавит от необходимости приобретать дополнительный жесткий диск.

Клонирование ПК — вы можете перейти на новый системный диск без необходимости переустановки операционной системы и приложений или настройки пользовательских параметров.

Восстановление Acronis Snap – молниеносное восстановление вашего ПК из образа. Вы можете начать работать за считанные секунды, пока ваша система еще восстанавливается. Acronis предоставляет бесплатный тест-драйв своего продукта и 30-дневную гарантию возврата денег. Когда вы будете готовы купить, вы можете либо загрузить за \$49.99, либо, если вы так желаете, заказывать коробочную версию за \$59.99. С Acronis True Image Home 9.0 вы можете быть спокойны, что ваши семейные фотографии, личные документы, налоговые декларации, резюме и другая важная информация не будут потеряны навсегда.



## Linux от Чайника - Сервер на CentOS 7

### Хотите научиться настраивать Linux-сервер?

Не имеете особых знаний в операционной системе Linux, и хотите с нуля, и за короткий срок, освоиться и научиться конфигурировать сервер-Linux?

**[Тогда Вы на правильном пути>>](#)**