Абсолютный минимум

Антивирусная программа
Своевременно обновляйте антивирусный продукт и регулярно выполняйте проверки, в том числе входящих сообщений. Без этого избежать заражения компьютера практически невозможно.

Программа антишпионажа
Такая программа может поставляться вместе с антивирусным продуктом; своевременно обновляйте ее и время от времени проводите с ее помощью проверки. Полезно установить две программы антишпионажа, например Windows Defender (поставляется вместе с Vista) и Spy Sweeper.

Двунаправленный брандмауэр
Блокируйте нежелательный входящий и исходящий трафик компьютера. Двунаправленный брандмауэр поставляется в составе Mac OS и Windows Vista. Пользователям старых версий Windows следует приобрести брандмауэр стороннего поставщика, например ZoneAlarm компании CheckPoint.

Не устанавливайте несколько разных брандмауэров и антивирусных программ
На первый взгляд, два брандмауэра обеспечивают двойную защиту, но в действительности они могут лишь удвоить неприятности. То же касается использования двух антивирусных программ. (Программы антишпионажа — другое дело.)

Разрешите автоматическое обновление
Настройте Windows и Mac OS на автоматическое обновление, так как Microsoft и Apple постоянно латают бреши, обнаруженные в программах.

Не принимайте EXE-файлы
Трудно совершенно отказаться от загрузки исполнимых файлов (с расширениями .exe, .com, .bat и .scr), но остерегайтесь подобных файлов, вложенных в сообщения электронной почты. То же относится и к файлам .doc и .xls; в них могут содержаться вирусы на основе макрокоманд.

Маршрутизация трафика
Пользователям широкополосных служб необходим маршрутизатор. Цена как беспроводных, так и проводных моделей невысока.

Аппаратный брандмауэр
Маршрутизатор должен обеспечивать преобразование сетевых адресов (NAT), чтобы злоумышленники из Интернета, занимающиеся поиском открытых портов, не могли увидеть ваши компьютеры. Чтобы отличить полезный сетевой трафик от вредного, брандмауэр должен также проверять содержимое индивидуальных пакетов (Stateful Packet Inspection, SPI). Не отключайте эти функции.

Борьба с вирусами и вредными программами

Проверка одиночных файлов
Похоже, вы обнаружили зараженный файл? Разобраться в ситуации поможет VirusTotal.com. Передайте файл на этот Web-узел или перешлите его как вложение по адресу *scan@virustotal.com* со словом SCAN в строке «Тема». Файл будет проверен с использованием 32 баз данных поставщиков антивирусного ПО, и вы получите отчет о результатах.

Искореняем компоненты rootkit
Хотя компьютер может быть чистым, постоянно следите за информацией о новых компонентах rootkit; это одни из самых трудно удаляемых вредителей. В случае заражения попробуйте применить бесплатную программу RootkitRevealer компании Sysinternals, которую можно получить по адресу *www.microsoft.com/technet/sysinternals/utilities/RootkitRevealer.mspx*.

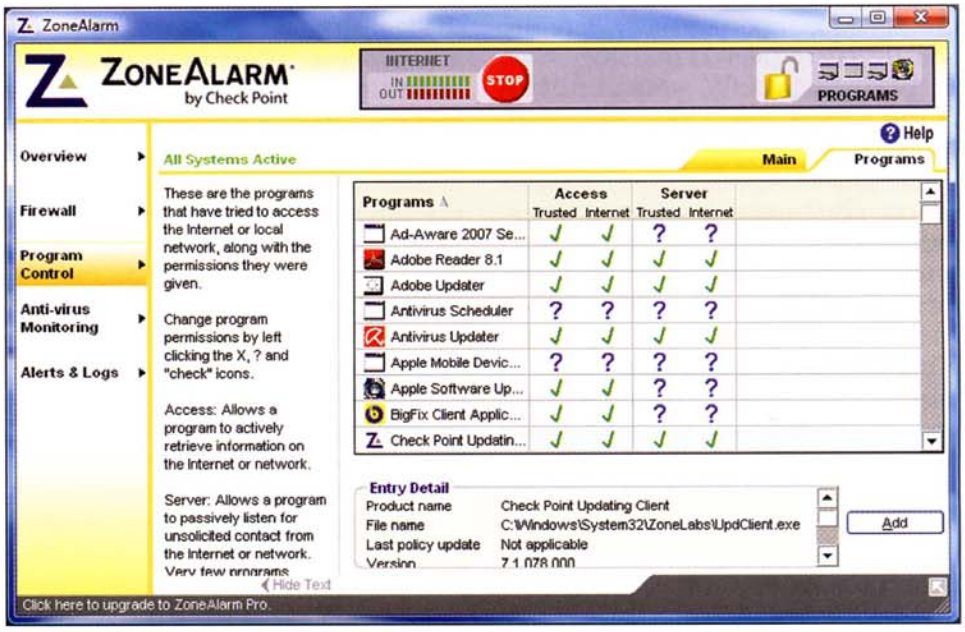
Защита Mac
Точно так же, как Firefox — менее заметная мишень для вирусов, чем Internet Explorer, компьютеры Mac реже подвергаются атакам, чем PC. Но и их владельцам не следует терять бдительность.

Специально для Windows

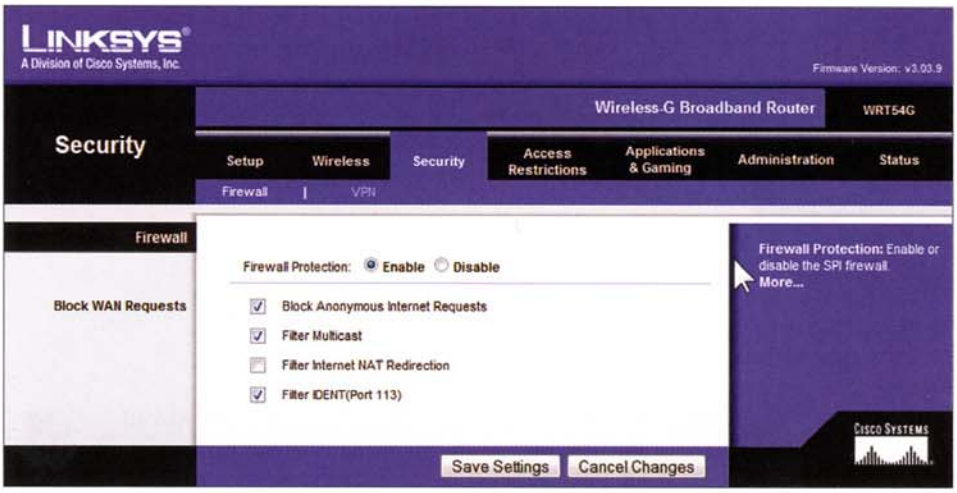
Отключите Autorun
Эта функция автоматически запускает вставленный в накопитель диск CD-ROM, но с него могут быть установлены нежелательные программы, в частности компоненты rootkit (см. выше). В XP для отмены этой функции нужно редактировать Реестр; процедура подробно описана в электронных пособиях (*go.pcmag.com/disableautorun*).

Отключите AutoPlay
Не путайте Autorun с AutoPlay, диалоговым окном с вопросом, какие действия нужно совершить с материалами, записанными на CD или флэш-накопителе. Чтобы отключить функцию в XP, используйте программу Tweak UI (*www.microsoft.com/windowsxp*). В Vista это можно сделать из панели управления AutoPlay.

Сведения об активных программах
В Windows множество программ выполняется в фоновом режиме, незаметно для пользователя. Увидеть



Тревога. С брандмауэром ZoneAlarm только указанные пользователем программы смогут отправлять данные из компьютера



Параметры маршрутизатора. Не забудьте активизировать аппаратный брандмауэр

их можно в диспетчере задач (вызывается комбинацией клавиш Ctrl-Alt-Del), но более подробные сведения предоставляются бесплатной программой Process Explorer *(www.microsoft.com/technet/sysinternals)*. Информация о процессах XP и Vista изложена на обычном английском языке.

Управление начальной загрузкой

Установите порядок и приоритетность программ, загружаемых в память в ходе запуска ПК, с помощью утилиты WinPatrol Plus (29,95 долл., *www.winpatrol.com*).

Неотложная помощь

Компания Microsoft предоставляет бесплатные технические консультации, если речь идет о вирусах или шпионских программах. Звоните 866-PCSafety (866-727-2338).

Надежные пароли

Используйте «крепкие» словечки

«Надежный» пароль представляет собой комбинацию цифр и букв, расположенных не в алфавитной или порядковой последовательности («abcd1234» — не «надежное» сочетание). Применяйте строчные и прописные буквы в сочетании со знаками препинания. Если есть место, используйте целую фразу; чем длиннее, тем лучше. Можно заимствовать надежные пароли, формируемые методом случайного подбора, на сайте PassPub.com.

Не используйте легко отгадываемые слова

Никогда не используйте слова, которые есть в словаре, и имена собственные. Имена детей и супругов, клички домашних животных — плохие пароли. Не используйте дату изменения пароля («jan23»). Ради всего цифрового: не используйте в качестве пароля слово «password».

Меняйте пароль

Регулярно меняйте пароли, чтобы опередить злоумышленников, которые не прочь воспользоваться ими.

Будьте непоследовательны

Не используйте один и тот же пароль на всех своих компьютерах или посещаемых Web-узлах. Иначе злоумышленнику достаточно проникнуть в одно место, чтобы получить доступ ко всем вашим учетным записям.

Создайте главный пароль

Людям со слабой памятью полезно подготовить и запомнить один надежный пароль, а затем менять его с учетом имени сайта или службы. Например, для портала MySpace пароль «Blg1225» превращается в «MyspBlg1225». Задачу можно облегчить с помощью одного из нескольких модулей расширения Firefox, объединяющих пароль с именем сайта, чтобы создать новый пароль для каждого Web-узла.

Позаботьтесь о Firefox

В браузере Firefox можно назначить мастер-пароль, который необходимо ввести, прежде чем будет предоставлен доступ к любому из сохраненных паролей сайтов. При этом каждый раз приходится вводить два пароля. В операционной системе Mac OS есть компонент Keychain для хранения паролей Web-узлов, прикладных программ и других. Его можно найти в папке Utilities.

Отмените функцию автоматического завершения ввода паролей

Браузеры не только хранят пароли, но и вводят их за пользователя. Использовать эту функцию на общедоступном или офисном компьютере не рекомендуется. В Firefox используйте мастер-пароль. В IE перейдите к *Internet Options* (Свойства обозревателя), щелкните на вкладке *Content* (Содержание), а затем на кнопке *AutoComplete* (Автозаполнение) и отключите режим автозаполнения.

Используйте RoboForm

Давно известная программа RoboForm (29,95 долл., *www.roboform.com*) для Windows заполняет Web-формы и генерирует сверхсложные пароли, надежно сохраняя их, чтобы избавить пользователя от необходимости запоминать какие-либо данные. Программа RoboForm2Go

Слушайся мастера. В браузере Firefox можно назначить надежный мастер-пароль для дополнительной защиты в сети

(19,95 долл.) запускается с флэш-накопителя USB и позволяет безопасно работать на любом ПК.

Зашифруйте список

Если необходимо составить список паролей, зашифруйте его. Замените типичный пароль обычным словом. Еще лучше сохранить пароли в программе диспетчера паролей (например, KeePass Password Safe по адресу *keepass.info*) или на таком сайте, как Clipperz *(www.clipperz.com)*, на котором они шифруются.

Фишинг

Не щелкайте

Если нет уверенности на 110%, не щелкайте на ссылках в сообщениях электронной почты. Сообщение может выглядеть так, словно оно поступило от службы электронных платежей PayPal, из банка или даже от друга, но, если есть подозрения, прислушайтесь к ним. Ссылка под URL *www.paypal.com* может указывать совсем на другой сайт. Если сообщение не вызывает подозрений, введите URL-адрес банка, PayPal или любой другой непосредственно в браузер с клавиатуры. Настоящие финансовые учреждения не будут (по крайней мере, не должны) запрашивать подтверждения по электронной почте.

Остерегайтесь мошенничества с поздравлениями

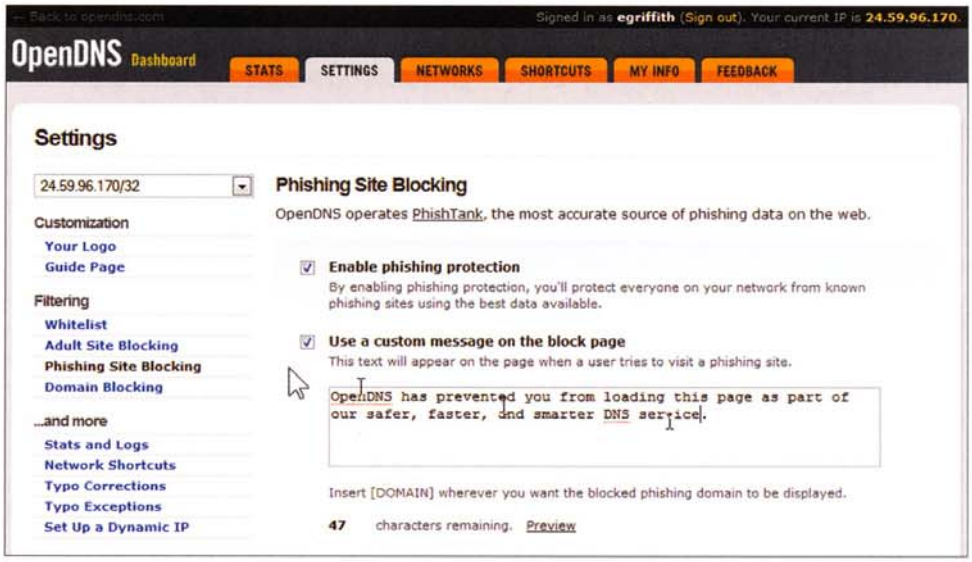
Электронные поздравительные открытки — чрезвычайно удобное орудие мошенников. Такие сайты могут собирать сведения от людей, отправляющих открытки, а затем от получателей, щелкнувших, чтобы посмотреть открытку. Пользуйтесь только услугами магазина Hallmark. Или просто отправьте жуликам деньги.

Остерегайтесь ложных всплывающих предупреждений о безопасности

Возможно, вам приходилось встречать в Интернете всплывающие окна с предложением провести проверку на наличие вредителей или удалить их и рекламой соответствующего продукта. Слишком заманчиво, чтобы быть правдой, — это просто вредная реклама.

Firefox как щит

Как Firefox, так и IE располагают дополнительными фильтрами фишинга, цель которых — отсеять сайты, владельцы которых пытаются украсть личную информацию. В окне Firefox Options (Настройки) перейдите на вкладку *Security* (Защита), установите флажок Tell me if the site I'm visiting is a suspected forgery (Информировать, не подозревается ли посещаемый Web-сайт в имитации другого Web-сайта) и не поленитесь установить второй флажок — Check by asking Google (Проверять, запрашивая Google), чтобы получать свежие списки сайтов фишинга.



DNS без фишинга. С помощью OpenDNS можно защитить всю сеть от сайтов фишинга

IE как щит

Internet Explorer 7 поставляется со встроенным фильтром фишинга, который необходимо активизировать через меню *Tools* (Сервис), из него же можно сообщать о сайтах, подозреваемых в фишинге. Пользователи IE6 могут установить панель инструментов Windows Live Toolbar и модуль расширения Windows Live OneCare Advisor для борьбы с фишингом.

Защита службы Skype

Кражи информации происходят не только через Web и электронную почту. Они случаются и при использовании других программ, таких, как VoIP-служба Skype. Был случай, когда «троянский конь» имитировал Skype, чтобы красть имена пользователей и пароли. Решение: обновите антивирусную программу.

Проверяйте мошеннические программы

Устанавливаемые вами программы также могут красть личную информацию — *особенно* программы, которые якобы призваны помочь в поиске программ шпионажа! Обнаружив подозрительную программу, сверьте ее со списком известных вредителей на сайте *www.spywarewarrior.com*.

Установите дополнительные фильтры

Компании McAfee и Trend Micro предлагают свои фильтры фишинга (SiteAdvisor и TrendProtect соответственно), чтобы расширить возможности браузеров. Служба OpenDNS тоже обеспечивает дополнительную защиту от фишинга. Прочитать о том, как функционирует служба, можно по адресу *go.pcmag.com/opendns*.

Безопасный Web-серфинг

Попробуйте Firefox или Opera

IE остается наиболее широко используемым браузером, соответственно и наиболее привлекательной мишенью для взломщиков. Смените браузер на Firefox или Opera. Они тоже уязвимы, но хакеры реже атакуют их из-за меньшего числа пользователей.

Отключите ActiveX

Если по каким-то причинам IE — единственный возможный вариант браузера, то можно избежать многих потенциальных опасностей, отключив элементы управления ActiveX — технологию автоматического запуска программных компонентов в браузере. Перейдите в *Internet Options* (Свойства обозревателя), затем на

вкладку *Security* (Безопасность), щелкните пиктограмму глобуса «Интернет» и следом *Custom Level* (Другой). Установите большинству элементов ActiveX значения Prompt (Предлагать) или Disable (Отключить). Если окажется, что не функционируют некоторые нужные компоненты, вернитесь в диалоговое окно и скорректируйте настройки.

Обратите внимание на «замок»

Собираясь отправить личную информацию через Web-узел, убедитесь, что сайт шифрует трафик. Обратите внимание на *https* (особенно символ «s») в URL-адресе и пиктограмму замка в адресной строке или панели состояния. Не посылайте никакой информации (такой, как номера кредитных карт), если на сайте нет шифрования. Но помните, что злоумышленники тоже могут обзавестись зашифрованным сайтом. Не доверяйте сайту только потому, что он защищен.

Активизируйте ForceField

Новый продукт ZoneAlarm ForceField (*go.pcmag.com/forcefield*) компании CheckPoint полностью предназначен обезопасить перемещения по Интернету. Он обеспечивает виртуальный слой между браузером и любыми изменениями, вносимыми через него в компьютер.

Следите за cookie-файлами

В прошлом cookie-файлы доставляли массу беспокойства. Однако в настоящее время они в основном безвредные — без них пришлось бы вводить гораздо больше паролей на часто посещаемых сайтах. Тем не менее, благодаря регулярным проверкам с помощью программы антишпионажа, можно удалить нежелательные cookie-файлы, чтобы не отслеживались перемещения пользователя по Интернету.

Анонимность и конфиденциальность

Защита папок

Пользователи Windows XP и Vista могут защитить паролем отдельные папки с помощью Folder Guard (39,95 долл. с бесплатным 30-дневным пробным периодом, *www.folderguard.com*). Можно просто сжать содержимое папки в ZIP-файл, используя такую программу, как WinZip (29,95 долл., *www.winzip.com*), и назначив ZIP-файлу пароль. При этом файлы также будут зашифрованы.

Защита папок на компьютере Mac

В операционной системе Mac OS можно сформировать защищенную паролем «папку» с использованием программы Disk Utility для создания дискового образа оригинала. Примените пароль. Полученный в результате DMG-файл содержит всю информацию, восстановить которую можно одним щелчком мыши.

Общая защита паролем

Пароль можно назначить отдельным файлам, составленным в Microsoft Office. В программе Word установите пароль для документа и зашифруйте его. Сделать это можно на вкладке *Security* (Безопасность) в разделе *Options* (Параметры); в Word 2007 — *Save As* (Сохранить как), перейдите в меню *Tools* (Сервис) и откройте *General Options* (Параметры). Можно также защитить паролем файлы Adobe Acrobat (PDF) и OpenOffice.

Не публикуйте в социальных сетях информацию о своей личной жизни.

Будьте благоразумны в социальных сетях

Не публикуйте личную информацию в социальных сетях и не облегчайте посторонним сбор подробных сведений о своей личной жизни. Не публикуйте свои компрометирующие фотографии. Информация в Web имеет свойство становиться постоянно доступной. Вспомните о Wayback Machine на сайте *www.archive.org*.

Уничтожайте следы

Уничтожьте журнал посещений в браузере после работы на общем ПК. В Firefox перейдите в раздел *Options* (Настройки), затем *Privacy* (Приватность) и щелкните на кнопке Clear Now (Очистить сейчас) в области *Private Data* (Личные данные). В качестве дополнительной меры можно установить флажок Always clear my private data when I close Firefox (При закрытии Firefox всегда удалять мои личные данные). В браузере IE7 выберите пункт *Delete Browsing History* после нажатия кнопки *Tools*. При щелчке на кнопке *Delete All* удаляются все сохраненные данные: предыстория, cookie-файлы, временные файлы и пароли.

Откажитесь от сохранения пароля

При работе на общедоступном ПК отклоняйте предложения сохранить пароль. Еще важнее завершать сеансы (log out) на сайтах, чтобы не оставить файлы электронной почты или другие файлы открытыми для посторонних.

Спрячьтесь за посредником

Использование службы-посредника позволяет скрыть IP-адрес своего компьютера или сети. Примеры бесплатных служб — Mproxy (*mproxy.info*) и Megaproxy (*megaproxy.com*). Служба Anonymizer Anonymous Surfing (29,99 долл./год, *www.anonymizer.com*) обеспечивает те же услуги и дополнительные возможности.

Сохраните в тайне адрес электронной почты

Почти каждая Web-служба запрашивает адрес электронной почты посетителя. Если он требуется только для передачи подтверждения, сообщите временный адрес. Служба 10 Minute Mail (*10minutemail.com*) предоставляет потребителям временный адрес, который работает в течение 10 мин.

Заведите второй адрес электронной почты

Благодаря широкому распространению бесплатных Web-служб электронной почты Google, Yahoo!, Microsoft и других, нет никаких оснований сообщать свой основной адрес электронной почты кому-то, кроме друзей.

Спам и спим

Не отвечайте

Никогда и ни при каких обстоятельствах не отвечайте на спам. Даже если это реклама полезного продукта. Ответ подтверждает, что сообщение прочитано, и ваш адрес будет навечно внесен в список автора спама.

Блокируйте «маяки»
Настройте программу электронной почты так, чтобы она не показывала изображений. Это надежная мера защиты от Web-маяков, изображений размером всего 1×1 пиксел, с помощью которых авторы спама узнают, что получатель посмотрел сообщение, а значит, адрес — действительный.

Избегайте «пауков»
Если вы публикуете свой адрес в Интернете, представьте его в виде «имя_домена точка com», чтобы помешать его обнаружению «пауками». Люди, неспособные догадаться, что эта запись соответствует адресу имя@домен.com, недостойны направлять вам свои послания.

Фильтруйте спам
Используйте электронную почту с фильтром спама. Встроенный блокировщик спама есть в программе Thunderbird, а в Outlook 2003 и 2007 для анализа сообщений и выявления спама используется Microsoft SmartScreen. Механизм Gmail почти безупречен. Фильтры спама обычно входят в состав комплексов безопасности.

Усложните адрес
Чем сложнее адрес почты, тем труднее отгадать его спамерам. Сравните: *ba3jacks59@gmail.com* и *bsmith@gmail.com*.

Избегайте спима
Спам в системах мгновенного обмена сообщениями называется спимом (spim). Избегайте его, используя необычные имена пользователя (например, ba3jacks56), а главное, не публикуйте свои координаты в общедоступном каталоге службы мгновенного обмена сообщениями. (Это относится и к службе Skype.)

Избегайте спима, совет 2
В некоторых продуктах приняты меры для борьбы со спимом, но они действуют только с определенными программными клиентами. Web-службы мгновенного обмена сообщениями, такие, как Yahoo! и Google, пока не защищены.

Дети и компьютер

Доступное размещение
ПК, которым пользуются дети, необходимо разместить так, чтобы они всегда были под присмотром.

Используйте таймер
Используйте правила на основе расписания, чтобы запретить работу в Интернете (или с компьютером) в неурочные часы. Они встроены в учетные записи пользователей Vista (и даже формируют отчеты об активности пользователей) и в большинство программ родительского контроля. Даже в некоторых сетевых маршрутизаторах есть соответствующие настройки.

Ограничьте игры
Контролируйте действия детей не только на ПК, но и за игровыми консолями. В Xbox 360 и Nintendo Wii есть возможность ограничить доступ детей на основе ESRB-рейтинга игр. В Xbox также устанавливаются ограничения по MPAA-рейтингу DVD-фильмов. В PlayStation 3 применяются иные уровни ограничений. (Измените выбираемый по умолчанию пароль 0000, или ребенок изменит его за вас.) В службе Xbox Live появился семейный счетчик времени, проводимого за играми в день или в неделю.

Остерегайтесь новых программ
Дети быстро обнаруживают, что родительский контроль распространяется лишь на очередной тип браузера или других программ, и просто загружают что-то новое. Купите программу контроля, которая действует в масштабах всей системы. Net Nanny Home Suite (49,99 долл., *www.netnanny.com*) — самая зрелая из программ родительского контроля.

Домашние сети

Измените заводские настройки
Большинство маршрутизаторов поставляются с таким именем пользователя, как admin, и без пароля. Если не изменить заводские настройки, то любой пользователь сети сможет управлять устройством как администратор.

Отключите широковещательную передачу
Имя беспроводной сети, SSID (service set identifier — идентификатор набора служб), передается широковещательно, чтобы облегчить устройствам доступ к ней. Отключите режим широковещательной передачи. Метод нельзя назвать полностью неуязвимым, но соседи, не

Фильтрация MAC-адресов. Разрешите подключение к маршрутизатору только устройствам с указанными вами MAC-адресами

имеющие технической подготовки, не смогут подключиться к вашей локальной сети.

Фильтруйте MAC-адреса
У каждого сетевого устройства есть MAC-адрес (media access control — управление доступом к среде). Маршрутизатор можно настроить на подключение только указанных устройств. Эта мера тоже не абсолютно надежна, но никогда не помешает.

Применяйте шифрование WPA
WiFi Protected Access (WPA) — лучший алгоритм шифрования для защиты WiFi-соединений. Еще лучше обзавестись маршрутизатором и устройством, совместимым со спецификацией WiFi Protected Setup (WPS), в котором ключи шифрования формируются автоматически.

Туннель к безопасности
Продукт независимого поставщика, такой, как Hotspot Helper (бесплатный пробный 10-дневный период, 24,95 долл./год) компании JiWire, устанавливает VPN-соединение между ноутбуком и Интернетом при использовании общедоступной сети WiFi, и злоумышленники не смогут похитить ваши данные во время передачи.

Физическая безопасность

Биометрические пароли
Будущее — за паролями на основе биометрических данных: отпечатков пальцев, сетчатки глаза и даже формы лица. Существует множество сканеров отпечатков пальцев,

встроенных в ноутбуки и в мыши. Программа Banana Screen (бесплатно, *www.bananasecurity.com*) дополняет Windows XP функциями распознавания лица, и компьютер просто блокируется, если владелец отсутствует в поле зрения Web-камеры.

Замок для ноутбука

В большинстве ноутбуков есть гнездо Kensington Security Slot (или K-Slot) для замка. Купите замок и используйте его, когда находитесь в офисе или кафе. Он может пригодиться даже дома, если пришел кто-то незнакомый. Начальная цена замка — 25 долл.

Приготовьтесь к краже

Нельзя полностью исключить вероятность кражи, поэтому запишите все номера модели и серийные номера своих устройств. Внимательно прочтите условия страховки домовладельца, чтобы выяснить, удастся ли вернуть деньги, даже если ноутбук украден из дома в ваше отсутствие. Если нельзя, то поменяйте страховку.

Звуковая сигнализация для ноутбука

Laptop Alarm *(www.syfer.nl)* — программа, которая подает звуковой сигнал, если кто-то отключает шнур питания, мышь или закрывает ноутбук без разрешения. Программа может даже отправить уведомление на ваш телефон.

Полезное устройство. SecureSpot останавливает вирусы на подступах к маршрутизатору

Слежение с использованием LoJack

Теперь не только для автомобилей. Программа с маркой LoJack для Windows или Mac от компании Computrace (49,95 долл., *www.lojack-forlaptops.com*) регулярно посылает сигналы на серверы этой компании. Если ПК или ноутбук украден, то Computrace может информировать полицию, где искать его.

Защита сети

Устройство SecureSpot компании D-Link располагается между кабельным модемом и маршрутизатором и защищает до четырех компьютеров в домашней сети с использованием антивирусной программы McAfee. Имеются функции родительского контроля.

Слежка с помощью Skype

Ловите злоумышленников в офисе на месте преступления с помощью службы Skype и Web-камеры. Настройте ПК, чтобы он автоматически передавал видеосигнал в ответ на вызовы, а затем обратитесь к нему из второй учетной записи Skype. При отключенном мониторе и звуке воры не заметят слежки.

Записывайте движение

Если вы не можете отлучиться, чтобы поймать взломщиков, то поможет программа Yawcam. Бесплатная программа для Windows обнаруживает движение и передает снятые изображения на сервер или по электронной почте.

Знайте свои права

Никто не читает лицензионных соглашений (EULA) — юридических текстов, выводимых на экран при установке программы, — но делать это нужно. Проверьте его с помощью бесплатной программы EULAlyzer *(www.javacoolsoftware.com)*. Она анализирует текст и отыскивает фрагменты, касающиеся потенциальных проблем. ≡

с 15 по 15

Безопасность

Компания BioLink *(www.biolink.ru)* объявила о выпуске новой версии биометрической системы BioTime. В BioTime 4.3 расширена номенклатура функций управления и контроля. Появилась специальная утилита для дистанционной регистрации персональных (в том числе биометрических) данных сотрудников (ранее работникам филиалов приходилось приезжать в центральный офис для регистрации в системе). Улучшена подсистема отчетов, их также можно экспортировать в формате XML. Реализована диагностическая подсистема (предоставляет информацию о текущей конфигурации системы BioTime и ее внешнем окружении, включая номенклатуру лицензий, сетевые настройки, адреса задействованных серверов и т. д. Обеспечена интеграция BioTime с платформой «1С:Предприятие 8.1», из BioTime в «1С» экспортируются сведения об отработанном времени, а из «1С» — персональные данные сотрудника (фамилия, имя, отчество, должность, отдел). Импорт выполняется с учетом иерархии организационных единиц (департаментов, управлений, отделов и т. д.), уже отраженной в «1С». Подсистема контроля физического доступа дополнена режимом запрета «повторного прохода». Не зарегистрировав свой уход из помещения, защищенного биометрическими терминалами BioLink FingerPass IC, сотрудник не получит права на вход (и наоборот). Тем самым предотвращаются попытки «обмануть» замок, турникет или шлюз, которым управляет биометрический терминал.

Принтеры

Компания Xerox *(www.xerox.ru)* объявила о начале продаж Phaser 6110MFP/B. Это цветной лазерный принт-комбайн, рассчитанный на формат A4 и адресованный небольшим рабочим группам, а также домашним пользователям. Он компактен (41×35×35 см, 16,5 кг), в устройстве используется система пассивного охлаждения, существенно снижающая шум — при печати до 49 дБ, при копировании до 52 дБ. Скорость печати — до 16 стр./мин в монохромном режиме и до 4 стр./мин — в цветном. На передней панели имеется порт USB. В комплект поставки входит программа ABBYY Fine Reader 7.0 Sprint Edition.

Периферия

Компания Genius *(www.genius.ru)* объявила о выпуске мыши Net Scroll 220 Laser. Эта модель рассчитана на мобильных пользователей, имеет черный симметричный корпус, переключаемое разрешение 800 или 1600 точка/дюйм.