- Nokia 6600 FOLD
- Sony Ericsson T700
- Motorola MOTOZINE ZN5
- Samsung L700
- Samsung i8510 INNOV8
- Sony Ericsson W902

ТЕСТЫ GSM-ТЕЛЕФОНОВ

Мир связи

hi-Tech

www.hi-tech.ua

№3 2009
март

Проект под ключ
Комплектуем нетбук

Как стать
невидимкой в Сети

Платежные карты
Кинет? Не кинет?

ТВОЯ ДОМАШНЯЯ СЕТЬ

Практический подход

Читай полную версию журнала в формате PDF!

Более 40 интересных публикаций, более 50 протестированных устройств, более 100 тестов и обзоров программного обеспечения! Смотрите самую полную версию 150-страничного журнала в формате PDF* на hi-Tech DVD. Подробнее о содержании журнала и диска — на с. 4.

* Для просмотра и распечатки электронных публикаций вы можете использовать Adobe Reader 9, который размещен на диске в разделе hi-Tech Toolbox

Лицензионный софт: полные версии!
- Alpha Five V9
- RecentX 2.0
- Webroot Window Washer 6.5
- Персональный поиск Яндекса 2.6.0

Домашний видеоархив
- AVIedit 3.38
- iuVCR 4.17.0.408
- Burn4Free 4.6
- Easy Burning 2.03a
- Speed DVD Creator 4.0.46
- SearchMyDiscs 3.7
- CDDataBase 4.00
- Camel Disc Catalog 2.2.1
- Sur Video Catalog 5.5.4
- Картотека видеофильмов 1.4.1
- Movienizer 1.9
- Media Catalog Studio 5.9 Lite
- iPod Video Converter 3.6

Чистильщики реестра
- WinASO Registry Optimizer 4.2
- Reg Organizer 4.22
- SBMAV Disk 2.88 Cleaner Lite
- Registry Trash Keys Finder 3.8.1
- Vit Registry Fix 9.3

Анонимный серфинг
- Anonymity 4 Proxy 2.8
- MultiProxy 1.2
- Proxy Checker Lite 1.1
- Hide IP NG 1.44
- Delete Cookie 1.01

Программы-шутки к 1 апреля
- CleverSpeaker 6.0
- SOUP 1.25
- IconMove 1.0
- Летающий «Пуск»
- Adrenaliner 1.139
- Face4Fun 1.0
- WinJoke 1.0
- Болтун 3.0

Игры
- Герои Мальгримии II: Победить дракона
- Переполох на ранчо
- Веселая ферма. Печем пиццу
- Охотники за привидениями. Призраки в поместье Мажести
- Тайна замка Единорога
- Лара Джонс. Находка профессора
- Официальный ролик к игре "Даша Васильева: Личное дело Женщины-кошки"

Киноафиша
- Рестлер
- Знамение
- Монстры против пришельцев
- Драконий жемчуг: Эволюция

Creative Commons: свободное творчество
- Big Buck Bunny
- Elephants Dream

Каталоги
- Цифровые фотокамеры
- Ноутбуки
- Мобильные телефоны
- КПК
- Тарифы

Свежие драйверы
- видеокарты (ATI-AMD, nVidia)

hi-Tech Toolbox
- Mozilla Firefox 3.1 Beta 2 (украинская версия)
- OpenOffice.org 3.0.1
- ICQ 6.50 (украинская версия)
- Mozilla Thunderbird 2.0.0.19
- Яндекс.Бар
- Українські мАксими 2008
- Adobe Reader 9
- Picasa 2
- IrfanView 4.23 P
- PDFCreator 0.9.6
- Opera 9.63 P
- Free Download Manager 3.0 P
- Media Player Classic 6.4.9.0
- WinRAR 3.80 (русская версия)
- FastStone Image Viewer 3.7
- AVS DVD Player 2.4.3.128
- Winamp 5.54
- Skype 3.8
- pMetro 1.26
- Miranda@HotCoffee 1.5.1
- Маршрут 1.0
- Comodo Firewall 3.0
- VirtualDub 1.8.8
- AnVir Task Manager 5.4.1
- K-Lite Codec Pack 4.6.2
- GOM Media Player 2.1.15
- Keyboard Ninja 2.1
- CDBurnerXP 4.2.4
- Paint.NET 3.36
- Dicto 2.7
- Unreal Commander 0.95

Мир связи

Украина, 03005, г. Киев-5, а/я 5
e-mail: MC@softpress.kiev.ua
homepage: www.ht.ua

Адрес редакции и издателя:
г. Киев, ул. Героев Севастополя, 10

тел.: (044) 585-82-82
факс: (044) 585-82-85

Издатель в Украине –
ООО «СофтПресс»

Учредитель журнала –
ООО «СофтПресс»

Тираж – 12 000 экземпляров
Цена договорная

Издание зарегистрировано в Министерстве информации Украины. Свидетельство о регистрации КВ № 6651 от 29.10.2002 г.

Подписной индекс в каталоге «Укрпошта»:
с CD – 45687,
с DVD – 98555.

Издатель: Эллина Шнурко-Табакова

Редакционный директор: Владимир Табаков

Шеф редактор: Владимир Куковский

Главный редактор: Евгений Высокович

Редакторы: Инна Иванова, Евгений Барилюк

Тестовая лаборатория: Константин Гончаров

Ответственный секретарь: Ирина Семенюк

Макетирование, графика, дизайн: Дмитрий Берестян, Вита Слюсаренко, Иван Таран

Фотохудожник: Александр Зенич

Директор по маркетингу и рекламе: Евгений Шнурко

Руководитель отдела маркетинга: Ирина Савиченко

Руководитель отдела рекламы: Нина Вертебная

Региональные представительства:
Днепропетровск: Игорь Малахов, тел. (056) 233-52-68, 724-72-42
e-mail: malakhov@softpress.com.ua
Донецк: Begemot Systems, Олег Калашник, тел.: (062) 345-06-26, 345-06-25
e-mail: edit@begemot.donetsk.ua
Львов: Андрей Мандич, тел.: (032) 295-64-10
e-mail: push@mail.lviv.ua

Отпечатано:
ООО «Имидж Принт»,
г. Киев, ул. Нововокзальная, 8

Панорама

Мобильный мир

ОФИС НА СВЯЗИ

Интернет

Телескоп

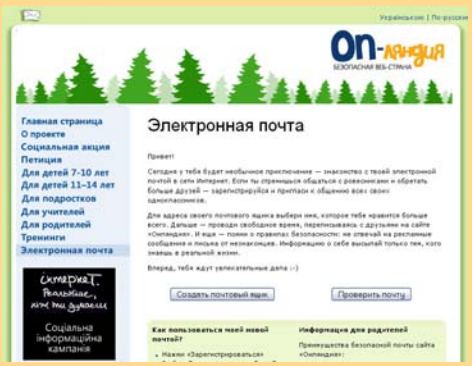
НОВОСТИ КОРОТКО

Программа «Trade-in» от NATEC

С 15.02.09 по 31.12.09 компания «Национальные Электронные Коммуникации» (NATEC), официальный партнер NEC Corporation в Украине, проводит маркетинговую программу «Trade-in от NATEC — существенная экономия при замене АТС». Компании малого и среднего бизнеса могут заменить устаревшее оборудования АТС (любых марок и моделей любого года выпуска) на современные мультимедийные телекоммуникационные серверы линейки NEC. Специалисты NATEC проведут оценку существующего оборудования и абонентских устройств — в результате затраты на новое оборудование существенно снизятся. Телекоммуникационные серверы NEC обладают масштабируемостью, расширяемостью и обширными функциональными возможностями (конференция, CallCenter, IVR, биллинг, запись речи, голосовая почта и др.), а также сетевые сервисы для абонентов на основе различных мультисервисных протоколов (в т. ч. IP).

Украинский Интернет становится безопасней

В рамках кампании «Месяц безопасного Интернета» запущен первый в Украине детский сервис электронной почты на сайте «Онляндия» (*www.onlandia.org.ua/mail*). Его цель — научить юных пользователей переписке. Проект поддерживает Интернет Ассоциация Украины (ИнАУ), являющаяся участником Коалиции за безопасность детей в Интернете. Коалиция основана компанией «Майкрософт Украина». По данным «Майкрософт Украина», которая непосредственно обеспечивает работу проекта «Онляндия», безопасная электронная почта осовывается на бесплатном веб-сервисе Windows Live Mail, она не содержит рекламы и захищена от спама и вирусов. Кроме переписки доступен обмен мгновенными сообщениями.



Детский сервис бесплатной и безопасной электронной почты, организованный на сайте проекта «Онляндия», научит детей правилам переписки

БОЛЬШЕ НОВОСТЕЙ НА hi-Tech.UA

ВОЛЯ абонентам

Компания «ВОЛЯ» вместо тарифных планов вводит четыре профиля потребления и предлагает дополнительную услу «Защита от вирусов и СПАМа Dr.Web»

Профили — это пакеты услуг, соответствующие потребностям разных групп потребителей в зависимости от целей и интенсивности пользования Интернетом. В них которые включены не только определенные объемы трафика, но и различные дополнительные сервисы. Минимальный объем трафика (2000 МБ), предоставляемый в профиле «Диалог», будет стоить 50 грн/мес., а максимальный, в профиле «Жизнь» (60 000 МБ), — 150 грн/мес.

Кроме того, началось тестирование дополнительной услуги для абонентов — «**Защита от вирусов и СПАМа Dr.Web**». Это сервис заключается в организации комплексной защиты ПК пользователей на основе функций программного обеспечения Dr.Web для Windows.

До конца марта воспользоваться лицензионной защитой Dr.Web можно бесплатно. При этом абонентам гарантируется бесплатные (без подсчета трафика) обновления вирусных баз, модулей программы, защита почты от СПАМа, а также ограничение доступа детей на ресурсы взрослого содержания (родительский контроль), услуги технической поддержки Dr.Web. С апреля 2009 года услуга будет платной — 10 грн в месяц, что ниже стоимости коробочной лицензии и электронной версии антивирусов.

Работа@Mail.Ru уже для Украины

Лидер российского рынка онлайн-рекрутинга Работа@Mail.Ru (*http://rabota.mail.ru*) вышел на украинский рынок. Посетителям проекта стали доступны несколько десятков тысяч местных вакансий.

После интеграции с ведущим украинским порталом для поиска работы и сотрудников Work.com.ua (*http://work.com.ua*) на Работа@Mail.Ru появилось более 10 тысяч актуальных вакансий из крупнейших городов Украины — от работников низшего звена до топ-менеджмента. Каждый день на проекте появляется свыше 3 тысяч новых предложений.

Стоит отметить, что украинские посетители Mail.Ru теперь будут видеть в информерах на различных сервисах портала — таких, как национальная социальная сеть Мой Мир@Mail.Ru (*http://mir.mail.ru*) — только актуальные для себя вакансии.

Как известно, украинские интернет-пользователи составляют около 10 % аудитории Mail.Ru, а это второе место после россиян.

Онлайн-рекрутинг — это еще одна локализованная услуга российского портала после Афиша@Mail.Ru, которая актуальна для шести городов Украины.

Весь світ на зв’язку. Добре в теорії, чудово на практиці.

Bringing networks to life.
Втілюючи мережі у життя.

До 2015 року ми житимемо у світі, в якому 5 мільярдів людей будуть об'єднані у мережі здебільшого на швидкостях широкосмугового зв'язку. Об'єм передачі даних збільшиться в 100 разів. І ми зможемо отримувати доступ до послуг зв'язку з будь-якого пристрою у будь-якій точці світу. Чи готові ви втілити це в життя з нами?

Nokia Siemens Networks

www.nokiasiemensnetworks.com/unitecommunity

НОВОСТИ КОРОТКО

Google Docs с мобильного

Корпорация Google усовершенствовала свой сервис Google Docs, который позволяет работать с онлайн-документами. Ранее пользователи мобильных телефонов могли только просматривать документы Google Docs, теперь же они могут редактировать электронные таблицы. Можно добавлять новые строки, редактировать информацию в ячейках, фильтровать данные и сортировать столбцы. Обновленным сервисом могут воспользоваться владельцы мобильных телефонов на базе Android и Symbian S60, а также пользователи iPhone и iPod touch.

Зарядка будет единой

Комиссар Евросоюза по промышленности Гюнтер Верхоген (Gunther Verheugen) в интервью немецкой радиостанции Deutsche Welle заявил, что Еврокомиссия намерена заставить производителей разработать единое зарядное устройство для всех мобильных телефонов.

Об этом сообщает информационное агентство ПРАЙМ-ТАСС. По словам Верхогена не исключено, что к производителям будут приняты строгие меры, чтобы принудить их разработать единое зарядное устройство. По мнению комиссара, сложившаяся сейчас ситуация, когда пользователи всякий раз покупают с новым телефоном новое зарядное устройство, неприемлема.

В ответ президент Ассоциации европейской промышленности информационных и коммуникационных технологий Тони Грациано (Tony Graziano) заявил, что единое зарядное устройство для всех телефонов не может быть создано по юридическим и технологическим причинам. В частности, в странах Евросоюза различные требования к аккумуляторам мобильных телефонов.

HP глобально поддержит пользователей

Компания HP объявляет о серии новых и обновленных программ помощи пользователям в онлайн-режиме. Среди них:

- Модернизированный глобальный форум (*www.hp.com/support/consumer-forum*).
- Обновленный веб-сайт HP для клиентов (*www.hp.com/support*), на котором более 20 миллионов посетителей ежемесячно легко находят нужную им информацию.
- Бесплатные онлайн уроки (*www.hp.com/go/freeclasses*), от того как перейти на ОС Windows Vista до безопасной настройки беспроводного офиса.
- Серия видео-роликов онлайн (*www.hp.com/products/howtovideos*).

Мобильный вирус

Защищать от вирусов уже необходимо не только компьютеры, но и мобильные телефоны

«Лаборатория Касперского» информирует пользователей средств сотовой связи о новом мобильном вирусе, способном без ведома абонента управлять его личным телефонным счетом.

Вредоносная программа Trojan-SMS.Python.Flocker.abaf работает в операционной системе Symbian и нацелена на клиентов одного из индонезийских мобильных операторов. Найденное вредоносное ПО относится к классу троянских программ и написано на скриптовом языке Python. Троянец без ведома владельцев телефонных номеров отправляет SMS-сообщения на короткий сервисный номер с командой перевести часть средств абонента на другой счет, принадлежащий злоумышленникам.

Специалисты считают, что с высокой степенью вероятности в обозримом будущем проблема незаконных операций по счетам абонентов сотовой связи в мобильной вирусной индустрии будет приобретать все большую актуальность, постепенно расширяя географию своего присутствия. Пользователи решения Kaspersky Mobile Security защищены от нового троянца, тем не менее, рекомендуется проявлять осторожность при работе с Интернетом при помощи смартфонов и следить за актуальностью антивирусных баз защитных решений.

Yahoo! Mobile обновился

Компания выпустила бета-версию мобильного портала Yahoo! Mobile, сочетающего в себе уже существующие сервисы – oneSearch, oneConnect и onePlace, а также браузер Opera Mini. Портал интегрирован с популярными социальными сетями и службами электронной почты, и включает новости, RSS, адресную книгу, календарь и Yahoo! Messenger. Поддерживаются виджеты от Yahoo! и других брендов.

Портал Yahoo! Mobile обзавелся целым рядом новых сервисов

Yahoo! Mobile будет также доступен в качестве загружаемого приложения для iPhone и смартфонов от Motorola, Nokia, Research In Motion, Samsung Electronics и Sony Ericsson, а также коммуникаторов, работающих по управлением Microsoft Windows Mobile.

SMS-банкинг

Нововведение от ПриватБанка уже успели окрестить «убийцей» платных справочных служб. Заключается оно в том, что банк отвечает на любые вопросы по SMS. Сообщение на одном из 12 языков (украинском, русском, английском, немецком, португальском, итальянском, испанском, латышском, польском, греческом, грузинском, иврите) по стандартным тарифам операторов можно отправить из любой страны мира на номер 3700.

Ответ должен прийтит в течении нескольких минут. В отличие от существующей с 2005 года услуги, предусматривающей только вопросы по околобанковской тематике, в новинке круг вопросов значительно шире. Например, можно узнать, где демонстрируется определенный фильм, или где взять автомобиль на прокат. Информацию ПриватБанк берет из собственной базы данных об услугах юридических лиц. SMS-ответы дополнили линейку мобильных сервисов от ПриватБанка. Сегодня с их помощью можно контролировать остаток денег на счету, оплачивать коммунальные услуги, блокировать карточку, покупать ваучеры мобильной связи и Skype, отправлять денежные переводы.

Миниатюрный флеш-накопитель Atom Blue

Компания Imation, уделяет внимание не только функциональности, но и дизайну своей продукции. Это хорошо видно по новым компактным съемным накопителям.

Малышку Atom Blue отличает высокий уровень защиты данных. Имея размеры большой скрепки (30,5x13x5,6 мм), новый цифровой накопитель способен уместить от 2 до 8 ГБ информации. Водонепроницаемый, ударопрочный алюминиевый корпус надежно защищает Atom Blue от механических повреждений. В девайсе реализованы функции защиты паролем и сегментации данных, что гарантирует сохранность информации пользователя.

В Atom Blue реализовано сразу несколько подходов к защите информации

Благодаря функции Windows ReadyBoost флешку можно использовать не только для хранения данных, но и для ускорения работы системы любого компьютера с ОС Windows Vista. Новый флеш-накопитель от компании Imation совместим с оперативными платформами Windows, Mac и Linux.

Мобильный «Доктор Веб»

Вышла новая версия антивируса Dr.Web 5.0 для Windows Mobile. Программа обеспечивает антивирусную защиту карманных компьютеров и коммуникаторов, работающих под управлением Windows Mobile 2003/5.0/6.0/6.1. При сканировании проверяется как память самого устройства, так и карта памяти, установленная на нем. Программа предлагает два возможных вида сканирования: полное и выборочное. В случае обнаружения вредоносного объекта пользователь может самостоятельно выбрать необходимое действие (игнорировать/удалить/поместить в карантин).

Новая версия Dr.Web для Windows Mobile – это не только новый интерфейс, но и обновленное ядро

Среди изменений и дополнений, вошедших в новую версию Dr.Web для Windows Mobile: обновление ядра, возможность загрузки демонстрационного и лицензионного ключевых файлов с сервера регистрации на устройство с Windows Mobile, изменения в интерфейсе программы.

Кроме того, в Dr.Web 5.0 для Windows Mobile удалена проверка даты начала лицензии. Таким образом, при сбросе текущей даты на устройстве, приложение будет продолжать действовать.

30-дневную демонстрационную версию продукта, можно получить на странице *http://download.drweb.com/demoreq/*. Покупатели продуктов Dr.Web Security Space, Антивирус Dr.Web 5.0 для Windows, Антивирус Dr.Web для Windows + Linux, Dr.Web Бастион для Windows и комплекта Dr.Web «Малый бизнес» по-прежнему смогут получить бесплатное право использования Dr.Web для Windows Mobile при покупке лицензии на 1, 2 или 3 года.

НОВОСТИ ОПЕРАТОРОВ

Beeline...

ввел в коммерческую эксплуатацию собственный международный **коммутационный центр нового поколения** производства компании Huawei Technologies. Это расширяет возможности Beeline по реализации услуг международной связи с использованием IP-телефонии, и организации прямых маршрутов к зарубежным точкам обмена трафиком. Новый коммутатор организовывает более гибкие возможности подключения с международными роуминг-партнерами Beeline. Усиление технических возможностей сети позволит Beeline устанавливать межсетевые интерконнекты с использованием основных современных протоколов IP (таких как SIP и H.323), а также голосовых кодеков, позволяющих существенно экономить пропускную способность оборудования. Новейшее решение SoftX3000, на базе которого построен коммутационный центр, представляет собой унифицированную сетевую структуру управления международными сеансами связи через единую пакетную сеть, с возможностью обработки до 16 млн вызовов в часы наибольшей нагрузки.

Абонентам также предоставлена возможность пользоваться услугами **поисковой системы «Яндекс»** на wap-портале Beeline в разделе «Карты». Уже сейчас с портала можно бесплатно скачивать «Яндекс.Карты» и в режиме онлайн пользоваться картами свыше 20 крупных городов Украины и России. В Украине это Киев, Харьков, Днепропетровск, Донецк, Одесса, Львов и Запорожье. Детализация до дома позволяет находить нужные адреса и даже точно определять свое местонахождение в городе. Доступна информация о заторах на дорогах, постах ГАИ, камерах слежения, дорожных работах и прочих ситуациях в городе. При закачке оплачивается только GPRS-трафик в соответствие с тарифным планом.

С 18 февраля стоимость пользования **услугой «Своя мелодия»**, позволяющей заменить гудки, которые будут слышны вызывающему абоненту, определенной мелодией, составляет 0,25 грн/день, при этом срок использования и количество приобретенных мелодий остается, как и раньше, неограниченными. С 5 марта при звонках на номер 0644, где можно выбрать мелодию, первая минута будет бесплатной, а стоимость последующих — 5 коп. за минуту прослушивания.

БОЛЬШЕ НОВОСТЕЙ НА hi-Tech.UA

НОВОСТИ ОПЕРАТОРОВ

Киевстар...

перевел **услугу «Мобильный Интернет XL»** в разряд постоянно действующих.

Внедрен новый метод **пополнения счета** для всех абонентов — достаточно позвонить в любое время суток на бесплатный номер 999 и, выполняя указания автоответчика, ввести номер абонентского телефонного номера, сумму пополнения и данные платежной банковской карточки систем Visa или MasterCard. Пополнение счета возможно на сумму более 5 грн и кратную 1 грн.

Минимальный **номинал скретч-карточек** пополнения счета теперь составляет 30 грн. С марта 2009 года прекращено изготовление скретч-карточек номиналом 50 грн и 300 грн. Карточки номиналом 25 грн, 50 грн и 300 грн. будут полноценными и рабочими до полного своего распространения.

На портале СтарПорт (*wap.starport.com.ua*) в разделе «Новости» открыт доступ к новостям **«Корреспондент.net»** прямо с мобильного телефона.

Если на счете недостаточно средств, то временно получить дополнительные 5 грн позволит новая услуга **«Экстра деньги»**. Абоненты предоплаченной формы подключения «Киевстар», DJUICE и «Мобилыч», должны при этом пользоваться услугами сети «Киевстар» больше года, тратить на мобильные услуги свыше 15 грн ежемесячно на протяжении последнего года и пополнить абонентский счет минимум один раз. Плата за каждый успешный факт пользования услугой — 50 коп., с учетом НДС и сбора в ПФ. Дополнительные средства предоставляются абоненту, в течение нескольких секунд после заказа, возвращение средств, происходит после очередного пополнения счета.

Бизнес-абоненты теперь могут заменить стандартные гудки, которые раздаются во время ожидания соединения на мелодию или приветствие. Для пользования **услугой «Бизнес Ди-Джингл»** у работников компании-клиента должны быть мобильные телефоны с бизнес-подключением к сети «Киевстар», которое оформлено на предприятие, а у координатора компании подключение к системе «Мой Киевстар» и компьютер с выходом в Интернет. Рядовые работники не могут изменить мелодию. Стоимость подключения услуги на одного сотрудника составляет 3 грн/мес.

БОЛЬШЕ НОВОСТЕЙ НА hi-tech.UA

Мгновенный перевод на мобилках

Компания ABBYY провела на ежегодной выставке Mobile World Congress 2009 предварительный показ нового решения для мобильных устройств ABBYY FotoTranslate. Оно помогает пользователям расширить функциональность смартфонов и воспользоваться всеми преимуществами встроенных камер. Вводить текст не нужно: достаточно просто сфотографировать слово или фразу встроенной камерой и получить перевод на экране мобильного устройства. Все это делает использование ABBYY FotoTranslate в путешествиях и командировках особенно удобным.

Версия ABBYY FotoTranslate, представленная на выставке в Барселоне, позволяет переводить с немецкого, французского, испанского и русского языков на английский и обратно, а также с английского на испанский.

Технология оптического распознавания (OCR) компании ABBYY, лежащая в основе нового продукта, позволяет быстро и точно переводить цифровые фотографии бумажных документов в редактируемые форматы с возможностью осуществлять поиск по тексту. При этом устраняются «шумы», перекосы строк и прочие искажения изображения.

Новая веб-камера от Creative Labs

Камера Creative Live! Cam Video IM Ultra имеет также встроенный микрофон с системой шумопонижения

Компания Creative Labs представила новую веб-камеру высшего класса Creative Live! Cam Video IM Ultra, предлагающую качественную съемку видео и различные развлекательные функции для незабываемого общения через Интернет. Камера оснащена сенсором с разрешением в 1,3 Мпикс. Подключение по интерфейсу USB Hi-Speed (USB 2.0) обеспечивает передачу видеопотока с частотой кадров до 30 в секунду, а микрофон с системой шумоподавления гарантирует высокое качество записи голоса. Для получения яркой качественной картинки используется система автоматической настройки Auto Tuning, а система Smart Face Tracking автоматически направляет и фокусирует камеру на лице пользователя при записи видеоролика или общении по Сети.

Пользователь может в реальном времени модифицировать голос с помощью забавных аудиоэффектов и добавлять разнообразные визуальные эффекты к транслируемому видеопотоку или записываемому видеоролику. Кроме того, в устройстве есть множество дополнительных функций, включая «родительский контроль», средства создания эффектных аватарок, запись и просмотр видео и фотографий, загрузка материала на YouTube, каталогизация и хранение видеороликов и фотографий. Все это обеспечивается поставляемым в комплекте пакетом ПО Creative Live! Central Premium.

Программное обеспечение, поставляемое в комплекте, обеспечивает редактирование избражения и добавление различных эффектов

В комплект поставки веб-камеры также входит программное обеспечение для редактирования домашнего видео muveeNow 2.0.

Мобильные тренды из Барселоны

Телефоны давно стали миникомпьютерами, но в плане красочности интерфейса или медиа функций они никогда не были лидерами. Однако новинки Всемирного Мобильного Конгресса 2009 могут стать действительно мультимедийными спутниками

Презентация сенсорного интерфейса с управлением пальцами, реализованного в iPhone дала долгожданный глоток новизны застоявшимся мобильным интерфейсам. Два года спустя LG представила логичное развитие этого механизма. В двух словах: интерфейс **LG Arena** можно крутить пальцами. Меню устройства выполнено в виде анимированного трехмерного куба, на каждой из граней которого располагается определенный набор приложений. Подобное вы могли видеть на ПК при использовании программ-расширителей рабочего стола (см. hi-Tech PRO 7/2008).

Новый 3D-режим интерфейса позволяет использовать в четыре раза больше ярлыков, чем обычно

В этом году мобильные телефоны также преодолели границу в 12 Мпикс. Первым в мире мобильным аппаратом с таким разрешением стал **Sony Ericsson Idou**.

Остается только заменить телефоном видеокамеру. Это удалось осуществить в **Samsung Omnia HD**, который стал первым в мире телефоном, снимающим HD-видео на свою 8 Мпикс. камеру.

Что же подготовят мобильники в будущем? Скорее всего, это будет массовое использование MEMS-датчиков, помимо акселерометров. Например, телефон сможет измерять атмосферное давление и влажность, а встроенное ПО будет делать более точный прогноз погоды и именно для вашего города. А использование датчиков касания позволит телефону включаться, как только его возьмут в руки. В целом, телефоны будут становиться все более восприимчивыми к действиям пользователя, повышая интуитивность общения с ним.

AMOLED-дисплей телефона может стать хитом года в мобильных экранах

Владелец 12 Мпикс. Idou может со спокойной совестью оставить свою цифромыльницу дома

НОВОСТИ ОПЕРАТОРОВ

life:)...

запустил новую услугу **«life:) Архив»**, которая позволяет абонентам сохранить важную информацию, содержащуюся в телефоне, и быстро ее восстановить, даже если сам аппарат утерян! Мобильный телефон — это не только средство связи, но и место хранения важной и актуальной информации, потеря которой для многих становится серьезной проблемой. С новой услугой «life:) Архив» этого можно избежать, так как абоненты смогут сохранить на сервере оператора свою телефонную книгу, календарь, заметки и задачи с возможностью последующего восстановления и редактирования через удобный веб- или WAP-интерфейс. Все данные защищены при помощи индивидуального имени пользователя и суперпароля. Предоставляется также возможность добавления информации. Стоимость одной синхронизации данных — 1 грн (с НДС и без сбора в ПФ). Объем принятых/переданных данных во время синхронизации оплачивается согласно тарифам доступа в Интернет или WAP.

Для новых и существующих абонентов тарифного плана «Свободный life» действует **акция «Звони вдвое дешевле»**. При пополнении на 35 или 50 грн эти суммы на счете удваивается. Акция действует по 31.12.2009 г. включительно, а подключиться к ней можно до 31.03.2009 г. включительно на территории Украины. Новые абоненты тарифного плана «Свободный life» принимают участие в акции автоматически при подключении, а существующие — после бесплатного подтверждения участия по номеру *141*3#.

Абоненты имеют возможность использовать накопленные бонусы в течение 30 дней только после того, ка полностью израсходуют средства на своем основном счете.

В то же время с 28 февраля на тарифных планах «Свободный life:)», «life:) Легкие деньги», «Простой life:) классический», «Супер life:) 30\50», life Platinum и DCC для тарификации звонков по Украине введена полная тарифная **единица времени — 30 секунд**, начиная с первой секунды. Для тарификации звонков до 30 секунд применяется полная тарифная единица времени — 30 секунд. Кроме того, введена **ежесуточная плата** в размере две гривни за возможность осуществлять исходные звонки в сети life для всех индивидуальных тарифных планов, если с момента последнего пополнения в размере от 25 грн одним платежом минуло 90 календарных дней.

БОЛЬШЕ НОВОСТЕЙ НА hi-Tech.UA

НОВОСТИ ОПЕРАТОРОВ

МТС...

продлил до конца 2009 года акционное предложение **«CDMA+GSM»** в соответствие с которым новые абоненты МТС при подключении к услуге «МТС Коннект» смогут подключиться к услугам мобильной связи со скидкой 66 % на абонплату в тарифном пакете «МТС Первый».

Запущена **услуга «Компас»** на базе технологии определения местонахождения LBS (Location-Based Service), которая поможет абонентам МТС-Украина получать подробную информацию о ближайших объектах с помощью обычного мобильного телефона. При этом можно будет определить местонахождение ближайших объектов (кинотеатры, клубы, рестораны, АЗС, СТО, банки, банкоматы и т. п.) на карте города, получить информацию о них, определить свое местоположение относительно ближайших объектов на WAP-карте. Услуга доступна в 25 городах Украины.

Запущен **социальный тариф «Антикризисный»** для контрактных абонентов, на который можно подключиться с 15 февраля по 31 мая 2009 года. Тариф позволяет экономить личный бюджет, так как не имеет абонплаты, платы за соединение, предусматривает бесплатные звонки на два номера «Моя семья» (один из которых может быть другого мобильного оператора Украины), предусматривает единую стоимость звонков на все направления в пределах Украины — 50 коп.

С 1 февраля 2009 г. стартовала **акция «Приведи друга»** для контрактных абонентов МТС, обслуживающихся в тарифных пакетах линейки «МТС Безлимитный». В рамках акции как существующие, так и новые абоненты могут получить скидку 20 % на абонентскую плату в тарифной линейке «МТС Безлимитный».

Введена в действие **услуга «Оптимизатор»** для корпоративных абонентов. Она представляет собой ПО для учета и оптимизации затрат на мобильную связь.

Открыта социальная партнерская **программа для студентов «Мобильный клуб МТС»**, в рамках которой студенты вузов становятся партнерами оператора и получают возможность воспользоваться дополнительным источником дохода в свободное от учебы время.

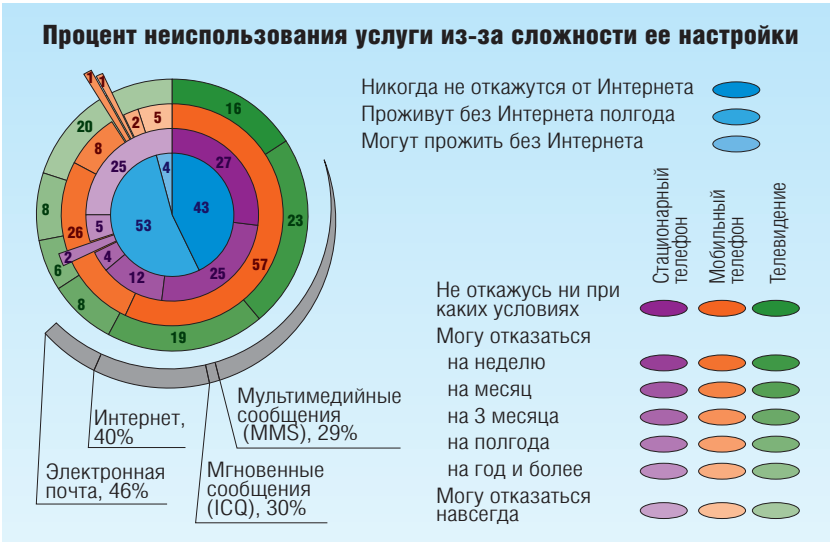
Объявлено о начале конкурсного этапа в рамках всеукраинской долгосрочной программы **«Профессионалы будущего»**, которая уже третий год проводится совместно с Министерством транспорта и связи Украины и Министерством образования и науки Украины.

Мобильникам вредит настройка

Производители выпускают все более умные и функциональные гаджеты, которые поднимают планку возможностей все выше и выше. Но нравится ли это пользователям?

Согласно опросу[1] компании Mformation пользователи готовы отказаться практически от всех функций мобильных девайсов, если его настройка для работы с сервисами окажется слишком сложной. Так 61 % респондентов отметили, что процесс настройки получается не менее трудоемким, чем изменение банковского счета, а 95 % уточнили, что они с большим удовольствием попробовали бы новые мобильные сервисы, если бы для этого не пришлось возиться с настройкой телефона.

Более того, оказалось, что проблемы настройки оказывают значительное влияние не только на доходы операторов мобильных сетей, но и продавцов аппаратов. Так, 45 % опрошенных отказались от замены устаревших моделей на новые только из-за необходимости настройки, а 78 % уточнили, что меняли бы аппараты чаще, если бы на каждом телефоне не приходилось заново выполнять эту процедуру. Часто



Слово «настройка» может легко испугать желающего попробовать новый мобильный сервис

пользователи отказываются даже от основных сервисов, которые бы могли существенно облегчить жизнь только потому, что эти услуги недоступны непосредственно после включения нового аппарата. А 61 % мобильных абонентов попросту отказываются от мобильных приложений, если с ними возникают проблемы.

В среднем, по мнению респондентов, настройка нового мобильного телефона не должна выполняться более 15 минут, хотя сейчас в среднем занимает не менее часа. Больше всего пользователей волнует перенос данных с одного аппарата на другой, поэтому 96 % отметили потребность в сервисе, который бы автоматически копировал телефонную книгу и другой контент со старого телефона на новый.

Исследователи из ROMIR Monitoring пошли еще дальше[2] и узнали, что хотя пользователей многое не устраивает, современные средства коммуникации стали абсолютно незаменимыми. А вот от классических каналов общения и получения информации, как то стационарный телефон, газеты или радио, люди вполне готовы отказаться.

❶ *www.mformation.com/mformation-news/press-coverage/the-herald-keep-i.t.-simple-stupid*
❷ *http://www.romir.ru/news/res_results/278.html*

Видеонаблюдение дома

Проводная IP–камера IP TL–SC3000 от компании TP–Link позволяет незаметно организовать собственную систему видеонаблюдения за всем происходящим внутри дома или офиса

Камера поддерживает технологии передачи видео через Internet, благодаря чему вы можете вести видеонаблюдение за интересующим вас объектом практически из любой точки планеты. Устройство поддерживает два способа компрессии потока видео: MPEG4 и M-JPEG, разрешение видео составляет 738x480, а светосила оптики – 2.0. Угол обзора камеры – 80–55,6°. Кодирование видео проходит со скоростью 30 кадр./с в системе NTSC или 25 кадр./с в системе PAL. Новинка оснащена детектором движения, 10/100 Мбит/с сетевым интерфейсом и утилитой для одновременного управления шестнадцатью камерами, поддерживает DHCP, PPPoE и просмотр видео по HTTP.

Дополнительный аналоговый видеовыход 75Ω позволяет интегрировать устройство в уже существующую аналоговую систему видеонаблюдения и модернизировать ее, сохраняя контроль над всеми наблюдаемыми объектами.

Новая IP-камера TP-Link поддерживает технологию 3GPP и позволяет подключаться к системе видеонаблюдения не только с ПК или ноутбука, но и любого мобильного телефона стандарта 3G.

В розничной продаже новинка появится весной этого года, ориентировочная цена – $100.

Новая IP-камера TP-Link позволяет подключаться к системе видеонаблюдения не только с ПК или ноутбука, но и любого мобильного телефона стандарта 3G

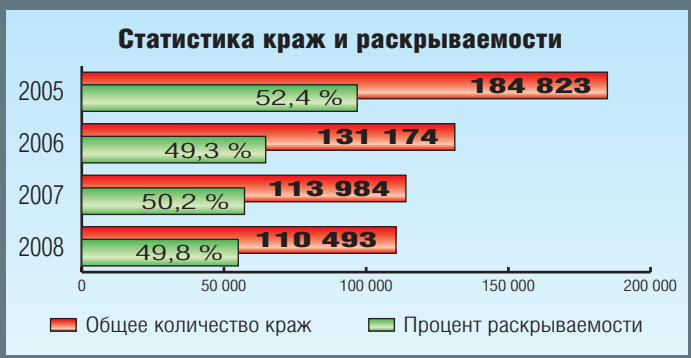
Спасение мобильника — дело рук его владельца

Как предотвратить кражу телефона

Мобильный телефон в настоящее время это роскошь, средство для общения, а еще и возможность кому-то подзаработать, если ваш мобильник станет объектом охоты карманника. Статистика МВД говорит, что из всех краж за прошлый год в Киевской области зарегистрировано почти 5 тыс. заявлений именно о телефонных кражах. А за январь этого года – уже 363, то есть примерно 12 краж ежедневно. Но МВД признает, что реальные цифры примерно раза в 2–3 раза больше, поскольку учитываются только те случаи, по которым были обращения в милицию.

Милиция способна раскрыть лишь половину всех краж, да и закон пока на стороне злоумышленников, поскольку уголовная ответственность наступает только, если украли на сумму более чем 907,5 грн (иначе правонарушитель отделается лишь штрафом в 51 грн). А именно этому ценовому диапазону принадлежит подавляющее большинство используемых украинцами трубок. Поэтому подумать о сохранности столь необходимого средства связи нужно самому.

Для начала можно попробовать простые рекомендации, знакомые каждому: не держите телефон в руках, не кладите сотовый на стол в баре и никогда не давайте незнакомым людям позвонить. Старайтесь также класть телефон в самые труднодоступные карманы вашей одежды. Эти простые меры предотвратят кражу сотового в транспорте или магазине.



МВД рекомендует: не стоит надеяться на успешную поимку вора, о безопасности нужно подумать самому

Но что делать, если телефон все же увели? Постарайтесь тут же позвонить на него: если кража произошла недавно, вор мог не успеть выключить аппарат, и вы сможете его найти по звуку. Кроме того, владельцам аппаратов, например, на базе Windows Mobile доступна программа типа BackStopp (*www.backstopp.com*), которая может стереть всю личную информацию, а также отследить аппарат через встроенный GPS.

Windows Mobile со вкусом Zune

Что нового в Windows Mobile 6.5

Генеральный директор Microsoft Стив Балмер (Steve Ballmer) представляет новую мобильную ОС на Мобильном Конгрессе в Барселоне

Следующую после Windows Mobile 6.1 версию пользователи ждали почти два года и основную ставку делали на «семерку» для мобильников. Однако разработчики не стали выпускать революционную, но сырую Windows Mobile 7, ограничившись обновлением интерфейса, добавлением новых приложений и работой над ошибками. Что же предлагают пользователю разработчики из Microsoft?

В первую очередь, это «сотовый» интерфейс в стиле Zune, который гораздо лучше приспособлен к управлению пальцами, а также новые возможности разблокировки экрана.

Так, движение по верхней части экрана просто разблокирует телефон, а по линиям ниже — открывает заданные программы. Простым скольжением пальца в разных областях экрана можно принять или отклонить входящий звонок.

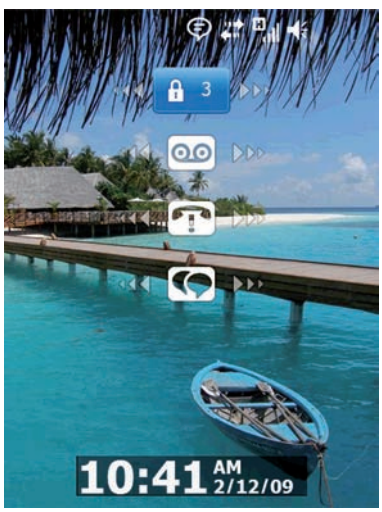
В версии 6.5 также появился новый браузер — Internet Explorer Mobile 6. Созданное на базе десктопного варианта приложение обеспечивает улучшенный веб-серфинг, масштабирование страниц, поддерживает технологии Flash и JavaScript. Всеми функциями отображения можно управлять пальцем, перетаскивая бегунок полосы прокрутки.

Внедрен и ряд передовых технологий. Среди них Microsoft Recite — система голосового поиска, которая предлагает разработчикам и конечным пользователям стандартные инструменты для записи, систематизации и извлечения голосовых заметок.

Microsoft My Phone — комплекс программных компонентов и сервисов для создания, хранения и переноса на другой аппарат резервных копий всех данных коммуникатора. Технология построена на решениях компании MobiComp, которую Microsoft приобрела в июне 2008 г.

Ведущие мировые партнеры уже начали предлагать аппараты с новой системой. Так стильный LG-GM7300 с дружественным интерфейсом, который вначале был выпущен с Windows Mobile 6.1, теперь пополнит семейство аппаратов с новой версией ОС. В новых моделях HTC Touch Diamond 2 and Touch Pro 2, предусмотрена возможность апгрейда до Windows Mobile 6.5. Во второй половине года предполагается появление аппаратов с новой системой и от других производителей. И еще одна новость — с осени все продукты на базе Windows Mobile будут называться Windows-телефоны, как продукты, которые вобрали в себя все лучшее от настольных ПК с операционной системой Windows.

www.microsoft.com/presspass/press/2009/feb09/02-16MWCPR.mspx



Microsoft существенно доработала Windows Mobile, оптимизировав ОС для «пальцевого» интерфейса

Функция «breadcrumb» позволит быстро переместиться на уже посещенные страницы сайта

Алексей Шелухин, shelukhin@hi-tech.ua

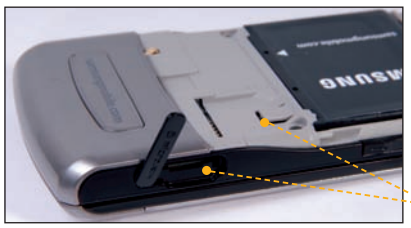
Symbian по-корейски

Смартфон Samsung SGH-L870

Оснастившись программной платформой от Nokia и прочным корпусом из текстурированной нержавеющей стали, смартфон Samsung L870 обещает стать практичным и относительно доступным решением с достаточной функциональностью

С помощью хорошо продуманного и локализированного меню, имеющего несколько тем оформления, можно добраться ко всем приложениям, установленным на смартфон

Под дисплеем расположен блок функциональных клавиш для приема и отбоя звонка, вызова меню и быстрого доступа к календарю (можно переназначить)



Под стальной крышкой аккумуляторного отсека находится слот для SIM-карты с возможностью горячей замены (смартфон выполнит перезагрузку), а карту памяти можно поместить в разъем на правом боку телефона

Правая боковина аппарата оснащена разъемом для наушников и кнопкой спуска камеры, левая – разъемом для карты памяти и клавишами управления громкостью

Данную модель, построенную на мобильной ОС Symbian S60 от Nokia, можно назвать эдаким смартфоном с очевидным телефонным уклоном. Дело в том, что особыми «фичам» L870 не выделяется (например, в аппарате нет Wi-Fi и GPS) и приглянется тем, кто не ставит перед устройством связи особых требований. С другой стороны, будучи построенной на третьем издании платформы S60, эта модель **позволяет воспользоваться рядом полезных приложений, недоступных пользователям обычных мобильных терминалов**. Так, мобильный офис представлен программой QuickOffice для просмотра файлов Microsoft Office (Word, Excel, PowerPoint), PDF и ZIP-архивов, можно также просматривать файлы различных версий Office (97, 2000 и XP). Кроме того, есть словарь-переводчик, приложение CheckIt (простой список покупок или дел), приложение для редактирования фотографий и создания видеороликов из имеющихся фото, а также различные темы оформления, браузер (с возможностью масштабирования веб-страниц, визуальным журналом просмотренных страниц, поиском текста и RSS-каналами), органайзер, календарь и пр. Неплох и предустановленный мультимедийный плеер с различными настройками 8-полосного эквалайзера. Беспроводные коммуникации телефона представлены лишь модулем Bluetooth 2.0 + EDR. Проводное соединение – USB 2.0 с поддержкой режима Mass Storage и синхронизацией с Media Player и PC studio. Аппарат оснащен 3-мегапиксельной камерой с автофокусом и функцией распознавания визиток.

Словом, L870 обладает небольшим, но вполне достаточным набором возможностей. Тем не менее отнести его к топовым имиджевым решениям в модельном ряду можно лишь за счет дизайна и материалов корпуса – похоже, тренд использования металла пришелся Samsung ко двору.

Samsung SGH-L870

Тип устройства/ формфактор: . . . . . смартфон/слайдер
Операционная система: . . . . Symbian S60 v9.3 (3rd Edition Feature Pack 2)
Стандарты: . . . . . GSM 900/1800/1900, GPRS/EDGE, HSDPA/WCDMA
Процессор: . . . . . STMicroelectronics Nomadics STn8815, 334 МГц
Дисплей: . . . . . 2,4", 320x240 (QVGA), 16 млн цветов
Память: . . . . . 100 МБ ПЗУ, поддержка карт памяти microSD
Интерфейсы: USB, Bluetooth 2.0 + EDR
GPS-навигатор/USB-хост: . . . нет/нет
Камера: . . . . 3 Мпикс. (с автофокусом), дополнительная фронтальная
Макс. разрешение фото/ видео: 2048x1536/640x480
Время автономной работы:
в режиме воспроизведения видео: . . . . . до 6 ч
в режиме разговора: . . . . . до 8 ч
Габариты: . . . . . 103,5x50,5x13,5 мм
Вес: . . . . . 120 г
Поставщик: . . . . представ-во Samsung, 8 (800) 502-0000
Цена: $240

Оценка:

- ⊕ прочный металлический корпус
- ⊕ «горячая» замена карты памяти
- ⊖ нет Wi-Fi и GPS

Алексей Шелухин, shelukhin@hi-tech.ua

Всего понемногу

Мобильный телефон LG KS360

Данная модель уже успела снискать славу первого бюджетного мобильного терминала с завидным оснащением (в первую очередь это QWERTY–клавиатура) и рядом интересных фишек. Чем же все–таки придется жертвовать, учитывая невысокую стоимость модели?

■ Изюминка аппарата — встроенная QWERTY-клавиатура. Стоит признать, что реализована эта «фича», доставшаяся в наследство от коммуникаторов (см. hi-Tech PRO 2/2009, с. 32), достаточно удачно — раскладка удобна, хотя и требует адаптации (некоторым буквам места на клавиатуре не нашлось, их вызов возможен с помощью кнопки Fn). Цель же использования полноценной клавиатуры одна — помочь коммуникабельному пользователю вести мобильную переписку более комфортно. Ведь к уже ставшим традиционными возможностям (например, FM-приемник, музыкальный проигрыватель, камера и диктофон) разработчики добавили еще одну — приложение iDea Widgets, которое включает в себя набор средств для онлайн-общения посредством ICQ, Bash.org.ru, Vkontakte.ru, Odnoklassniki.ru, Fishki.net, а также различные новостные ленты и т. п. Помимо набора текста, клавиатура может быть использована и для навигации. Единственная проблема — оранжевая подсветка ее кнопок, как оказалось, достаточно тусклая.

Вторая по значимости «фича» KS360 — сенсорный экран с тактильной отдачей. Правда, сенсорный он, условно выражаясь, не полностью... Дело в том, что **дисплей устройства реагирует на прикосновения лишь в режиме набора номера** (для его активации предусмотрена специальная кнопочка, расположенная немного ниже кнопки вызова). Во всех же остальных случаях экран становится абсолютно нечувствительным к прикосновениям. Впрочем, несмотря на такую «подставу», слайдер не нужно открывать, если требуется всего лишь набрать номер.

Телефонная составляющая LG KS360 реализована удачно. Динамик для передачи голоса достаточно громкий, собеседника хорошо слышно даже на шумной улице. Из прочих особенностей — возможность горячей замены карты памяти microSD (без необходимости выключать телефон и извлекать батарею).

LG KS360

Тип устройства/формфактор: . . . . . мобильный телефон/слайдер
Стандарты: . . . . . GSM 900/1800/1900, GPRS/EDGE
Дисплей: . . . . . 2,4", 320x240, 262 144 цветов
Память: . . . . . 15 МБ, поддержка карт памяти microSD
Интерфейсы: . . . . . USB, Bluetooth 2.0
QWERTY-/цифровая клавиатура: . . . . . да/нет
Камера/макс. разрешение: 2 Мпикс./1600x1200 (фото), 320x240 (видео)
Батарея: . . . . . Li-Ion, 800 мАч
Габариты: . . . . . 101,5x51x16,8 мм
Вес: . . . . . 112 г
Поставщик: . . . . . представ-во LG, 8 (800) 303-0000
Цена: $200

Оценка:

- ⊕ QWERTY-клавиатура и набор приложений для онлайн-общения
- ⊕ доступная цена
- ⊖ неполноценный сенсорный дисплей
- ⊖ тусклая подсветка клавиш клавиатуры

Сенсорным экран LG KS360 становится лишь в режиме набора номера

Управлять практически всеми функциями телефона можно и в закрытом состоянии аппарата

Кнопки QWERTY-клавиатуры расположены довольно удобно, впрочем, огорчает их подсветка

2-мегапиксельная камера не оснащена автофокусом и вспышкой, зато есть сферическое зеркальце для автопортретов

Правая боковина оснащена разъемами для наушников и карты памяти, левая — кнопками управления громкости и спуска камеры

Алексей Шелухин, shelukhin@hi-tech.ua

Не такой как все?

Нетбук Toshiba NB100-10Y

Довольно качественная сборка, интересное покрытие корпуса, относительно мощная платформа и набор интересных нестандартных «фич» — таков словесный портрет нового 8,9-дюймового нетбука Toshiba

Виртуальная панель ConfigFree Launcher служит для быстрого доступа к беспроводным интерфейсам, инструментам настройки и окружению Bluetooth

Клавиатура Toshiba NB100 не отличается особой эргономичностью, что, впрочем, свойственно большинству нетбуков

Одно из новшеств нетбука от Toshiba – разные по длине клавиши тачпада

Toshiba NB100-10Y

Процессор: . . Intel Atom N270 (1,6 ГГц)
ОЗУ установлено/максимально: . . . DDR2, 1024/1024 МБ
Жесткий диск тип: . . . . . 120 ГБ
Графический адаптер: . Intel GMA 950
Встроенный CD/DVD-привод: . . . нет
Дисплей: . . . . . 8,9" (1024x600, WSVGA)
Клавиатура: . . . . . 80 клавиш, тачпад (55 мм)
USB/FireWire: 3/0
VGA/DVI/S-Video: 1/0/0
Wi-Fi/Bluetooth/Ethernet: . . . да/да/да
Кардридер: . . . . . MMC/SD/MS/MS Pro
Веб-камера: . . . . . да (1,3 Мпикс.)
Батарея, емкость: . . . Li-Ion, 4400 мАч
ОС: . . Microsoft Windows XP Home Edition
Время автономной работы:
Интернет + офисные приложения: . . . . . 3:07 ч
просмотр видео: . . . . . 2:44 ч
Габариты: . . . . . 225x190,5x33 мм
Вес: . . . . . 1,05 кг
Поставщик: . . . . . представ-во Toshiba
Цена: $650

Оценка:

- ⊕ прочный корпус
- ⊕ простой доступ к слоту ОЗУ
- ⊖ клавиатура прогибается по краям
- ⊖ габаритный блок питания

■ Производитель этого нетбука, безусловно, не открыл Америку, анонсировав данную модель как второй мобильный ПК для владельцев достаточно мощного ноутбука или первый компьютер для тех, кому не требуется высокая производительность. На практике мы имеем вполне стандартный нетбук (см. hi-Tech PRO 10/2008, с. 42), который действительно подойдет и первым, и вторым, что и неудивительно. Но все же есть в Toshiba NB100 нечто особенное...

В первую очередь, речь идет о наличии портов USB (всего их, как и ожидалось, три), которые могут заряжать подключенную к нетбуку технику (USB 2.0 с технологией Sleep-and-Charge). К фишкам стоит отнести и **Bluetooth 2.1 с профилем с EDR, который может быть использован для подключения беспроводных наушников**. Также отметим весьма приятное фирменное приложение для быстрого доступа к беспроводным интерфейсам, инструментам настройки и окружению Bluetooth (по умолчанию виртуальная панель ConfigFree Launcher находится в нижней правой части экрана).

Toshiba NB100 построен на базе хорошо знакомого нам процессора Intel Atom N270, имеет 1 ГБ предустановленной оперативной памяти (в попавшей к нам на тест комплектации) и работает под управлением Microsoft Windows XP Home Edition (SP3). Нетбук оснащен 8,9-дюймовым TFT-экраном с глянцевым покрытием Toshiba TruBrite и светодиодной подсветкой, который поддерживает разрешение 1024x600 (WSVGA) и имеет широкий угол обзора по горизонтали (чего не скажешь о вертикальном угле обзора). Дополняют оснащение основные сетевые интерфейсы — помимо Bluetooth, это Wi-Fi (802.11 b/g), а также Ethernet (10/100), есть и кардридер. Также отметим традиционно маленький тачпад с двумя «мышиными» кнопками, визуально объединенный в один блок с линейкой системных индикаторов.

Музыка нас связала

Инна Иванова, ivanova@hi-tech.ua

В тестировании:

- Nokia 6600 FOLD
- Sony Ericsson W902
- Motorola MOTOZINE ZN5
- Samsung i8510 INNOV8
- Samsung L700
- Sony Ericsson T700

Музыкальные телефоны занимают второе место по продаваемости, уступая пальму первенства лишь бюджетным моделям. Данный тест объединил в себе несколько медийных гигантов

Градиентный музыкант

Nokia 6600 FOLD

Модель Nokia 6600 FOLD позиционируется, прежде всего, как имиджевая. Однако при тестировании она показала достаточно хорошие музыкальные способности. Именно поэтому мы включили ее в наш тест.

Новинка привлекает, безусловно, дизайном. Ее верхняя крышка имеет градиентную окраску: с верхнего края цвет более насыщен, тогда как к низу он практически сходит на нет. Механизм автодоводки в этой «раскладушке» реализован слабо. Зато с правого торца имеется клавиша раскрытия створок. Внутри телефона встроены магниты для притягивания половинок друг к другу. В аппарате имеется два экрана. Внешний реализован по типу уже знакомого нам Motorola U9. То есть он скрыт и совсем не заметен в «спящем» состоянии. Цифры и буквы проступают будто бы из глубины телефона. Правда, на улице они совсем не различимы.

Медиаплеер стандартен для платформы Symbian S40, на которой и реализован сотовый. Только в данной модели он обзавелся несколькими новыми скинами, которые отлично подходят к ее внешнему виду. Присутствует пятиполосный эквалайзер с предустановленными настройками под разные музыкальные направления. Треки можно передавать как проводным путем, так и посредством Bluetooth-протокола.

Общее впечатление портят слабый аккумулятор и маркая глянцевая поверхность. Однако это компенсируется возможностью нетрадиционного управления. Так, например, чтобы вызвать часы, можно просто постучать по корпусу закрытого аппарата.

Рсцветка Nokia 6600 Fold градиентная: сверху цвет яркий и насыщенный, а к низу сходит на нет

Поверхность модели глянцевая – выглядит красиво, но постоянно надо протирать

Nokia 6600 FOLD

Стандарт . . . . . GSM 850/900/1800/1900, 3G
Дисплей . . . . . OLED, 240x320 пикс., 16 млн цветов
Память . . . . . 485 МБ + microSD
Камера . . . . . 1,9 Мпикс.
Интерфейсы . Bluetooth 2.0, A2DP, USB
Возможности . . . FM-радиоприемник, MP3-проигрыватель, поддержка MP3, midi, amr, aac, wma
Вес . . . . . 109 г
Размеры . . . . . 88x44x17 мм
Аккумулятор . . . . . Li-Ion

Время работы

в режиме разговора . . . . . 5:26 ч
в режиме ожидания . . . . . 154:12 ч
Цена (около) **$280**

Оценка

- ⊕ привлекательный внешний вид
- ⊕ нетрадиционное управление
- ⊖ слабый аккумулятор
- ⊖ маркая поверхность

8 «гектар» в придачу

Sony Ericsson W902

Большой выбор цветов корпуса расположит к себе представителей молодежной аудитории

Модель позиционируется как флагман среди плеерофонов производителя. Основные ее потенциальные поребители – молодежь в возрасте 20–35 лет. На это указывает, в первую очередь, характерный дизайн. С первого взгляда он неброский, но все равно чем-то цепляет. Например ребристой поверхностью, что одновременно и функционально, и эстетично. Или необычным блоком навигационных клавиш – вроде бы небольшим, но удобным. В общем посмотреть есть на что.

Качество сборки неплохое. Огорчает только задняя крышка. Она болтается в пазах. Экран прикрыт минеральным стеклом но имеются зазоры. Хотя в целом это мелочи. Дисплей очень качественный. Информация на нем отлично читается как внутри помещения, так и снаружи.

Аккумулятор в условиях умеренного использования продержался двое суток. Но батарея, как это и должно быть в плеерофонах, оптимизирована под воспроизведение музыки. В этом режиме заряда хватило аж на 24 часа.

Плеер в Sony Ericsson W902 установлен третьей версии. В нем улучшена навигация и добавлено несколько опций. Например, имеется поддержка DRM 2.0, а также поддержка MTP, что позволяет напрямую передавать песни из Windows Media Player. В остальном все привычно. Стандартные функции SensMe, Shake Control и TrackID, качественный звук и удобство в использовании оставляют за шведами лидерство в сфере музыкальных решений.

Относительно фотоспособностей модель слегка подкачала. Несмотря на 5-мегапиксельный CMOS-модуль, снимки не идут ни в какое сравнение с аналогичными предложениями от других производителей. Преимуществом данной камеры можно назвать лишь возможность переключения различных функций прямо с клавиатуры.

Своей памяти в телефоне всего 32 МБ. Но это с лихвой компенсируется комплектационной картой памяти на 8 (!) ГБ. Всего же поддерживаются модули объемом до 16 ГБ. Предусмотрена горячая замена.

Ребристая поверхность не позволит Sony Ericsson W902 выскользнуть из рук владельца

Sony Ericsson W902

Стандарт . . . . . GSM 900/1800/1900
Дисплей . . . . . TFT, 240x320 пикс., 262 тыс. цветов
Память . . . . . 1021 МБ + microSD
Камера . . . . . 1,9 Мпикс.
Интерфейсы . Bluetooth 2.0, A2DP, USB
Возможности . . . FM-радиоприемник, MP3-проигрыватель, поддержка MP3, midi, amr, aac, wma
Вес . . . . . 83 г
Размеры . . . . . 101x49x16 мм
Аккумулятор . . . . . Li-Ion
Время работы
в режиме разговора . . . . . 4:36 ч
в режиме ожидания . . . . . 261:15 ч
Цена (около) **$175**

Оценка

- ⊕ отличное качество звучания и проигрыватель
- ⊕ хорошая комплектация
- ⊖ слабая камера
- ⊖ среднее качество сборки

Полку камерофонов прибыло

Motorola MOTOZINE ZN5

■ Телефон показывает одновременно как хорошие фотографические, так и музыкальные способности. Но обо все по порядку. Материал корпуса приятен на ощупь. Практически вся поверхность металлическая. Лишь края выполнены из резины, что только добавляет прочности терминалу. Сборка отличная: все части плотно прилегают, нет ни люфтов, ни зазоров.

Дисплей довольно качественный, однако все же несколько выцветает на улице. Но за счет большой диагонали (2,4 дюйма) картинка все равно остается читабельной. Цифровая клавиатура создана на основе полимерной пленки. Клавиши абсолютно плоские и ни визуально, ни физически никак не разделены. У кнопок имеется небольшой ход. К использованию такой клавиатуры придется некоторое время привыкать, но в целом достаточно удобно.

Выпуская эту модель, разработчики учли все самые сильные стороны уже существующих камерофонов и аккумулировали их в своем новом детище. В результате имеем 5-мегапиксельный модуль с ксеноновой вспышкой и 4х зумом. Объектив расположен очень удачно: его при всем желании сложно закрыть рукой. **Основной упор в Motorola ZN5 сделан на скорость работы: и камера запускается в считанные секунды, и обработка фотографий происходит чуть ли не мгновенно.** Кроме того, данная модель является первым на нашей памяти камерофоном с возможностью съемки в режиме RAW. Правда, на практике этот формат мало чем напоминает классический RAW. Суть его состоит в том, что в результате просто получаются два снимка в форматах JPEG и TIFF, при чем последний — черно-белый. В темное время суток фотографии заметно шумят.

Плеер прост и удобен в использовании. Имеется эквалайзер. Звучание по субъективным ощущениям одно из лучших на рынке, сравнимо даже с MP3-плеерами. Гарнитура работает как антенна. Имеется 3,5 мм разъем для стандартных наушников. С ними звук становится еще качественнее. При прослушивании треков телефон проработал 14 часов без подзарядки. Это достаточно неплохой показатель. При обычном использовании аккумулятор может продержаться около 3 суток.

Передача голоса на высоком уровне. То же можно сказать и про громкость звонка, и про вибровызов. Пропустить трели Motorola ZN5 невозможно.

При всей своей шикарности, дизайн Motorola ZN 5 напомнил нам середину 90-х

Motorola MOTOZINE ZN5

Стандарт	GSM 900/1800/1900
Дисплей	TFT, 320x240 пикс., 262 тыс. цветов
Память	1980 МБ + MSmicro
Камера	3,1 Мпикс.
Интерфейсы	Bluetooth 2.0, A2DP, USB
Возможности	FM-радиоприемник, MP3-проигрыватель, поддержка MP3, midi, amr, aac, wma
Вес	103 г
Размеры	100x48x16 мм
Аккумулятор	Li-Ion
Время работы	
в режиме разговора	5:29 ч
в режиме ожидания	400:14 ч
Цена (около)	$265

Оценка

- ⊕ отличная камера
- ⊕ качественная сборка
- ⊖ спорная клавиатура
- ⊖ дизайн «на любителя»

Камера в модели одна из самых быстрых в своем классе — собственно, на это и уповал производитель, выпуская на рынок телефон

И швец, и жнец...

Samsung i8510 INNOV8

Объем встроенной памяти (16 ГБ) позволит разгуляться и фотографу, и меломану

■ Samsung i8510 INNOV8 является флагманом от корейского производителя. Несмотря на то что упор в модели сделан на фотографические способности, меломаны ее тоже оценят по достоинству. Здесь также присутствует 3,5 мм «джек», для подключения наушников, но это не основной аргумент в пользу музыкальности телефона. **16 ГБ встроенной памяти избавят вас от необходимости постоянно удалять старые, но еще любимые треки.** Радуют и настройки эквалайзера. Предустановленных их имеется 18 штук, включая три с 3D-звучанием. Если же и этого не хватает, существует возможность запоминания собственноручно настроенного эквалайзера. Через наушники слушать музыку — одно удовольствие. Зато внешние динамики грешат шумами и характерным «песком». FM-приемник достойно проявляет себя. Он может запомнить до 50 радиостанций, а также записывать мелодии с эфира. Автопоиск происходит быстро и вполне корректно.

Камера в модели тоже очень сильная. Огромное количество настроек сравнимо даже не с «мыльницей», а с полупрофессиональным фотоаппаратом. Помимо стандартного выбора можно варьировать светочувствительность (ISO 50–1600), замер экспозиции, баланс белого. Самые важные настройки доступны в одно касание. Дисплей огромный — 2,8 дюйма. Правда, из-за небольшого разрешения заметны пиксели, но через сутки-двое использования это перестает бросаться в глаза. На солнце дисплей слепнет.

Нововведение в клавиатуре представлено двумя клавишами: M1 и M2. Первая вызывает музыкальное меню, вторая — RealPlayer. Аппарат работает на платформе Symbian 60. Этим обусловлены и программные особенности устройства.

На огромном дисплее в 2,8 дюйма удобно смотреть фото или клипы, но если приглядеться, видно зерно

8-мегапиксельный модуль камеры делает из Samsung i8510 INNOV8 практически вотоаппарат-мыльницу

Samsung i8510 INNOV8

Стандарт	GSM 850/900/1800/1900, 3G
Дисплей	TFT, 240x320 пикс., 16 млн цветов
Память	7720 МБ + microSD
Камера	8 Мпикс.
Интерфейсы	Bluetooth 2.0, A2DP, USB
Возможности	FM-радиоприемник, MP3-проигрыватель, поддержка MP3, midi, amr, aac, wma
Вес	139 г
Размеры	107x55x20 мм
Аккумулятор	Li-Ion
Время работы	
в режиме разговора	6:43 ч
в режиме ожидания	408:46 ч
Цена (около)	$660

Оценка

- ⊕ отличная камера
- ⊕ большой объем памяти
- ⊖ высокая цена
- ⊖ «зернистость» экрана

Стильно и экономно

Samsung L700

Samsung L700

Стандарт . . . . . GSM 850/900/1800/1900, 3G
Дисплей . . . . . TFT, 176x220 пикс., 262 тыс. цветов
Память . . . . . 30 МБ + microSD
Камера . . . . . 1,9 Мпикс.
Интерфейсы . Bluetooth 2.0, A2DP, USB
Возможности . . . FM-радиоприемник, MP3-проигрыватель, поддержка MP3, midi, amr, aac, wma
Вес . . . . . 109 г
Размеры . . . . . 109x47x14 мм
Аккумулятор . . . . . Li-Ion

Время работы
в режиме разговора . . . . . 6:00 ч
в режиме ожидания . . . . . 381:17 ч
Цена (около) $140

Оценка

- ⊕ соотношение цена/качество
- ⊕ стильный внешний вид
- ⊖ слабая камера
- ⊖ зернистый экран

Samsung L700 демонстрирует неплохое сочетание цены и качества

Кнопки на клавиатуре большие и удобные – случайные нажатия практически исключаются

Samsung L700 при своей невысокой цене оставляет впечатление дорогого и добротного телефона. Особенно, если у вас в руках находится классический серебристый вариант. Благодаря металлическим вставкам, телефон создает приятную тяжесть в руке. Клавиатура пластиковая, но покрыта краской «под металл». Кнопки большие и удобные.

Экран достаточно большой – 2,1 дюйма, но при просмотре фотографий заметно зерно.

Хорошо себя проявил аккумулятор. При 20 минутах разговоров в день, нескольких SMS и паре-тройке фотографий телефон проработал 5 дней. Действительно, очень хороший показатель.

Проигрыватель в Samsung L700 установлен базовый. Из существенных недостатков отметим отсутствие эквалайзера. В остальном всех функций вполне хватало. Воспроизводятся самые популярные форматы, есть самые необходимые стили воспроизведения, поддерживается фоновый режим. В шумных местах громкости немного не хватает, но есть подозрения, что эта проблема исчезнет при подключении через переходник хороших наушников. FM-радио на достаточно высоком уровне. В настройках есть возможность установить сигнал как будильник, а так же как напоминание, чтобы не пропустить какой-либо эфир.

Камера весьма посредственна. 2 Мпикс. модуль способен на нормальные снимки только в «тепличных» условиях. В остальных же случаях он существенно сдает позиции. Вспышки часто не хватает на освещение объектов съемки.

Как вывод, отметим то, что аппарат своих денег стоит. Если у вас есть плеер и фотоаппарат и для полного счастья не хватает только телефона, можете остановить свой выбор на Samsung L700.

Металлический стиляга

Sony Ericsson T700

Корпус модели пластиково-металлический. Сочетание черного и серого светов делает дизайн привлекательным и строгим одновременно

Телефон представляет собой классическую модель среднего класса с дорогим дизайном и компактным корпусом. Корпус, как и в большинстве моделей данного теста, частично выполнен из металла. Лишь некоторые части пластиковые, например, обрамление экрана. Последний, кстати сказать, удобен как для обычного использования (SMS, звонки, управление файлами), так и для серфинга в Интернете. Предустановленный браузер, Netfront, является классическим для данной платформы. Однако в базовой поставке имеется еще и Opera mini. Он традиционно проявил себя несколько лучше в работе.

Аудиоспособности аппарата реализованы на одинаково высоком уровне с его фотовозможностями. **Звук чистый, однако гнезда для подключения обычных наушников нет.** Но в данном случае это не такая уж и проблема, ибо шведско-японский тандем славится своей фирменной гарнитурой. FM-радио тоже присутствует и справляется со своей задачей отлично: быстро ловит волну и устойчиво держит сигнал.

Недостатком модели стала клавиатура. Клавиши шаткие, и кажется, что они, того и гляди, выпадут. Правда, за две недели этого так и не произошло, но страх не покидал нас все это время. Вторым недостатком является слабый сигнал. В условиях, где другие телефоны показывали одно-два деления, Sony Ericsson T700 наотрез отказывался находить сеть. Если вы живете в обастях с хорошим покрытием, можете подумать о покупке этой модели. Жителям пригородных районов с ней придется тяжело.

Sony Ericsson T700

Стандарт	GSM 850/900/1800/1900, 3G
Дисплей	TFT, 240x320 пикс., 262 тыс. цветов
Память	530 МБ + MS-micro
Камера	3,1 Мпикс.
Интерфейсы	Bluetooth 2.0, A2DP, USB
Возможности	FM-радиоприемник, MP3-проигрыватель, поддержка MP3, midi, amr, aac, wma
Вес	78 г
Размеры	104x47x11 мм
Аккумулятор	Li-Ion
Время работы	
в режиме разговора	6:00 ч
в режиме ожидания	333:11 ч
Цена (около)	$220

Оценка

- ⊕ приятный дизайн
- ⊕ качественная гарнитура в комплекте
- ⊖ плохая клавиатура
- ⊖ слабая антенна

Клавиши на клавиатуре довольно шаткие на вид, но прочные на практике

Телефон ориентирован, прежде всего, на молодежь, ценящую современные тенденции в мобильной моде

Мир связи ДИЗАЙН

Мир связи ВЫБОР РЕДАКЦИИ

Мир связи ЭКОНОМ

РЕЗУЛЬТАТЫ ТЕСТИРОВАНИЯ

ТЕХНИЧЕСКИЕ ДАННЫЕ

Производитель Модель	Nokia 6600 FOLD	Sony Ericsson W902	Motorola MOTOZINE ZN5	Samsung i8510 INNOV8	Samsung L700	Sony Ericsson T700
ОСНАЩЕНИЕ						
UMTS (WCDMA)	●	●	—	●	●	●
GSM 850/900/1800/1900	●/●/●/●	●/●/●/●	●/●/●/●	●/●/●/●	●/●/●/●	●/●/●/●
Выход из сети без выключения устройства	●	●	●	●	●	●
Комплект поставки: тип аккумулятора/гарнитура hands-free	Li-Ion/●	Li-Pol/●	Li-Ion/●	Li-Ion/●	Li-Ion/●	Li-Pol/●
Главный дисплей: тип/разрешение, пикселей	OLED/240x320	TFT/240x320	TFT/240x320	TFT/240x320	TFT/176x220	TFT/240x320
Размер дисплея (ширина x высота), мм	31,5x45,0	33,5x45,0	36,0x48,5	42,0x56,0	33,5x41,5	31,0x41,0
Дисплеи: цветность главного/наличие дополнительного	16 700000/●	262 144/—	262 144/—	16 700000/—	262 144/—	262 144/—
Телефонная книга: группы/запрет звонков определенных абонентов/рингтон на каждого абонента	●/●/●	—/●/●	●/—/●	●/●/●	●/●/●	—/●/●
Громкая связь/голосовой набор/быстрый набор	●/—/●	●/●/●	●/●/●	●/—/●	●/—/●	●/●/—
Ситуационные профили: встроенные/пользовательские/кол-во	●/●/>6	●/●/>6	●/●/5	●/●/>6	●/●/6	●/●/>6
КОММУНИКАЦИИ						
Встроенный модем/GPRS-класс/EDGE	●/32/●	●/10/●	●/12/●	●/12/●	●/10/●	●/12/●
WLAN/HSDPA	—/—	—/●	●/—	●/●	—/—	—/●
GPS/A-GPS/PTT	—/—/—	—/—/—	—/—/—	●/●/—	—/—/—	—/—/—
e-mail/Bluetooth	●/●	●/●	●/●	●/●	●/●	●/●
Bluetooth: профили/обмен объектами (контактами тел. книги, заметками, файлами)/работа с гарнитурой hands-free	● ●/●/●	● ●/●/●	● ●/●/●	● ●/●/●	● ●/●/●	● ●/●/●
Инфракрасный порт/дата-кабель в комплекте	—/●	—/●	—/●	—/●	—/●	—/●
Синхронизация с Outlook/удаленно SyncML	●/●	●/●	●/●	●/●	●/●	●/●
Слот для флеш-карт (формат)	● (microSD)	● (MS-micro)	● (microSD)	● (microSD)	● (microSD)	● (Memory Stick Micro)
Подключение внешней антенны	—	—	—	—	—	—
Наличие оригинального автокомплекта	●	●	—	—	●	—
СООБЩЕНИЯ						
SMS/MMS (макс. КБ)/e-mail-клиент	●/● (300)/●	●/● (300)/●	●/● (300)/●	●/● (300)/●	●/● (300)/●	●/● (300)/●
Кол-во памяти для SMS/выбираемая пользователем папка для сообщений	1000/●	1000/—	1000/●	2000/●	500/●	1000/●
Предиктивный ввод текста (T9 и т. п.)/текстовые блоки/шаблоны	●/●/●	●/—/●	●/—/●	●/●/●	●/—/●	●/—/●
Групповая рассылка SMS	●	●	●	●	●	●
КОНТАКТНАЯ КНИГА И ОРГАНАЙЗЕР						
Макс. кол-во контактов/кол-во полей на один контакт/фотоопределитель	1000/>10/●	1000/>10/●	1000/>10/●	2000/>10/●	1000/>10/●	1000/>10/●
Календарь/заметки с напоминаниями	●/●	●/●	●/●	●/●	●/●	●/●
Часы/калькулятор/конвертер валют	●/●/●	●/●/—	●/●/●	●/●/●	●/●/●	●/●/●
Будильник/секундомер/таймер	●/●/●	●/●/●	—/—/—	●/—/—	●/●/●	●/●/●
Диктофон: продолжительность одной записи/макс. кол-во записей	●/>60 сек./>7	●/>60 сек./>7	●/>60 сек./>7	●/>60 сек./>7	●/>60 сек./>7	●/>60 сек./>7
МУЛЬТИМЕДИА						
Память в Мбайтах (встроенная)	485,5	7630,0	1400,0	7720,0	30,5	530
Встроенная камера/тип/разрешение	●/CMOS/1,9	●/CMOS/5	●/CMOS/4,9	●/CMOS/8	●/CMOS/1,9	●/CMOS/3,1
Запись видео (макс. продолжительность)	● (>5 мин.)	● (>5 мин.)	● (>5 мин.)	● (>5 мин.)	● (>5 мин.)	● (>5 мин.)
Видоискатель для автопортрета/автоспуск	●/●	●/●	—/●	●/●	●/●	●/●
Серийная съемка/панорамная съемка/вспышка (лампа подсветки)	●/—/●	●/●/—	●/—/●	●/●/●	●/—/●	●/●/●
Цифровой зум/оптический зум/автофокус	8x/—/—	>9x/—/●	4x/—/●	9x/—/●	3x/—/—	8x/—/—
Кол-во разрешений съемки/уровней качества	6/3	4/2	4/1	>6/3	5/4	4/2
Увеличение изображения в режиме просмотра	●	●	●	●	●	●
Браузеры: версия WAP/HTML	2.0/●	2.0/●	2.0/●	2.0/●	2.0/●	2.0/●
Поддержка Java/кол-во встроенных игр	●/3	●/3	●/2	●/2	●/>4	●/3
Видео: телефония/потоковое/загрузка	●/●/●	●/●/●	—/●/●	●/●/●	●/●/●	●/●/●
FM-приемник/MP3-плеер/аудиовход для записи	●/●/—	●/●/—	●/●/—	●/●/—	●/●/—	●/●/—
Поддерживаемые форматы: H.263/MPEG-4/MIDI/AMR/MP3/AAC/M4A/WMA	●/●/●/●/●/●/●/●	●/●/●/●/●/●/●/●	●/●/●/●/●/●/●/●	●/●/●/●/●/●/●/●	●/●/●/●/●/●/●/●	●/●/●/●/●/●/●/●

● – да, — – нет

РЕЗУЛЬТАТЫ ТЕСТИРОВАНИЯ

ИЗМЕРЕННЫЕ ЗНАЧЕНИЯ

Производитель / Модель	Nokia 6600 FOLD		Sony Ericsson W902		Motorola MOTOZINE ZN5		Samsung i8510 INNOV8		Samsung L700		Sony Ericsson T700	
Стандарт	GSM-900	GSM-1800	GSM-900	GSM-1800	GSM-900	GSM-1800	GSM-900	GSM-1800	GSM-900	GSM-1800	GSM-900	GSM-1800
КАЧЕСТВО ПЕРЕДАЧИ И ПРИЕМА												
Эффективная мощность излучения, дБм	20,9	19,1	22,1	20,6	22,6	23,9	22,2	24,1	22,2	19,4	20,6	19,3
Относительная чувствительность, дБ	-16	-18	-15	-16	-13	-16	-13	-13	-20	-15	-17	-20
Коэффициент SAR	0,61		1,48		0,86		0,414		0,718		1,55	
АКУСТИЧЕСКИЕ ИЗМЕРЕНИЯ												
Направление передачи/приема												
Громкость, дБ	9,6/13,1		6,0/10,8		9,6/6,0		7,9/17,1		10,7/11,9		14,9/13,2	
Искажения, дБ	-27,0/-22,9		-24,5/-20,7		-28,1/-29,8		-27,2/-15,5		-30,5/-21,3		-27,1/-24,6	
Шум в режиме молчания, дБ	-68,0/-45,0		-69,8/-43,9		-70,3/-53,3		-68,2/-21,1		-69,5/-31,1		-67,0/-35,8	
Частотная характеристика (число очков из 5)	3/3		3/3		4/4		3/2		3/1		4/2	
Эхо-шумы и мешающие шумы												
Подавление эха, мужской голос, дБ	40,1		46,2		47,5		43,5		46,9		43,7	
Подавление эха, женский голос, дБ	42,2		48,3		49,8		44,7		49,2		45,5	
Перекрестный разговор, дБ	15,3		16,1		16,3		17,3		17,8		16,7	
РАЗМЕРЫ, ВЕС И ПРОДОЛЖИТЕЛЬНОСТЬ РАБОТЫ												
Масса, г	109		100		114		139		109		78	
Длина х ширина х толщина, мм	88x44x17		110x51x14		117x51x16		107x55x20		109x47x14		104x47x11	
Продолжительность разговора, ч:мин.	5:26	6:12	6:48	6:02	6:56	7:00	6:43	8:12	6:00	6:18	6:00	5:49
Продолжительность работы												
в режиме ожидания, ч	154:12	153:40	376:40	408:53	501:29	610:10	408:46	419:16	381:17	378:32	333:11	360:47
при включенном дисплее, ч:мин.	25:53	25:53	10:59	10:59	6:26	6:26	5:38	5:38	8:45	8:45	9:18	9:18

Мир связи ДИЗАЙН

Мир связи ВЫБОР РЕДАКЦИИ

Мир связи ЭКОНОМ

РЕЗУЛЬТАТЫ ТЕСТИРОВАНИЯ

БАЛЛЫ И ОЦЕНКИ

Производитель / Модель		Nokia 6600 FOLD	Sony Ericsson W902	Motorola MOTOZINE ZN5	Samsung i8510 INNOV8	Samsung L700	Sony Ericsson T700
Оиентировочная цена, $		280	400	320	660	140	220
ПРОДОЛЖИТЕЛЬНОСТЬ РАБОТЫ	**100**	**хорошо (77)**	**оч. хорошо (85)**	**оч. хорошо (91)**	**хорошо (84)**	**хорошо (84)**	**хорошо (83)**
Время работы							
в режиме разговора	60	48	49	60	54	50	50
в режиме ожидания	20	9	19	20	20	19	18
с включенным дисплеем	20	20	17	11	10	15	15
ОСНАЩЕНИЕ	**150**	**оч. хорошо (128)**	**оч. хорошо (130)**	**хорошо (123)**	**оч.хорошо (134)**	**хорошо (122)**	**хорошо (126)**
Операционная система и аппаратное обеспечение	30	30	30	27	31	29	29
Передача данных	40	25	23	23	28	22	22
Возможность использования в автомобиле	20	20	19	20	20	20	20
Дополнительные функции	20	20	20	17	18	19	19
Функции SMS, MMS, e-mail	40	33	38	36	37	32	36
ЭРГОНОМИКА	**150**	**оч. хорошо (129)**	**хорошо (124)**	**удовлетв. (111)**	**хорошо (121)**	**оч. хорошо (128)**	**хорошо (123)**
Руководство пользования	30	27	27	24	25	27	27
Дисплей	30	27	26	19	25	24	24
Вес	40	36	33	31	37	37	31
Размеры	15	12	12	13	13	11	11
Удобство управления	10	9	9	7	3	9	10
Удобство меню	10	7	5	6	6	7	7
Клавиатура	10	9	8	9	10	10	10
Качество исполнения	5	2	4	2	2	3	3
СВЯЗЬ	**50**	**недостаточно (29)**	**удовлетв. (35)**	**оч. хорошо (47)**	**хорошо (42)**	**недостаточно (29)**	**недостаточно (26)**
АКУСТИЧЕСКИЙ ТЕСТ	**50**	**хорошо (40)**	**хорошо (38)**	**хорошо (40)**	**удовлетв. (36)**	**хорошо (39)**	**хорошо (41)**
Измерение звука при приеме	20	16	14	14	16	17	17
Измерение звука при передаче	20	15	14	16	10	12	14
Измерение эха и помех	10	9	10	10	10	10	10
Общее число баллов	макс. 500	403	412	412	417	402	399
Оценка		**хорошо**	**хорошо**	**хорошо**	**хорошо**	**хорошо**	**хорошо**

Алексей Васильченко, vasilchenko@hi-tech.ua

Предохраняйся!

Как защитить ПК от автозагружаемых вирусов?

Несмотря на то что самым массовым и опасным источником распространения вирусов является Интернет, помнить о компьютерной безопасности нужно и тем, у кого машина не подключена к Сети

Эра гибких дисков, иначе говоря дискет, ушла в прошлое, прихватив с собой культуру массовой антивирусной безопасности. Согласитесь, сегодня далеко не все проверяют съемные накопители на наличие вредоносного кода. И оправдание таким действиям у многих простое. Очень часто можно услышать, что, копируя, к примеру, фильм в формате AVI, заразить машину невозможно.

Отчасти это так... С одной стороны, цифровой фильм — это не исполняемый EXE-объект, к которому вирусы цепляются проще всего, с другой — это и не офисный документ, а значит, макровирусов можно не бояться... Но если присмотреться к проблеме повнимательнее, выясняется, что не все так просто.

Константин Здыбель,
ведущий специалист по информационной безопасности компании «БАКОТЕК»

Лучшее лечение — ампутация

Насколько безопасно использовать флеш-накопители без установленного антивируса? Велик ли риск потерять данные на флешке или на ПК при случайном заражении?
Отсутствие антивирусного ПО на любом ПК крайне опасно. В моей практике было несколько случаев, когда люди теряли данные из-за того, что использовали ПК без установленного антивируса. Характерно, что во всех случаях объяснение было одно: «У меня нет доступа в Интернет, поэтому я думал, что антивирус мне не нужен». Как результат — уничтожение некоторой информации различной важности и невозможность полноценного использования зараженной операционной системы. Источником вирусов во всех вышеописанных случаях были флеш-накопители.

Какие вирусы опаснее — те, что можно подцепить в Интернете, или те, которые распространяются на флешках?
Говорить о том, какие вирусы опаснее, все равно, что спорить, какая боль сильнее: головная или зубная. Вне зависимости от источника ущерб может быть одинаковым. Единственный мнимый «плюс» при заражении ПК без доступа в Интернет — это гарантия того, что данные в худшем случае будут уничтожены, тогда как при наличии доступа во Всемирную паутину информация может попасть в чужие руки, что значительно хуже ее уничтожения.

Какие системы защиты ПК вы рекомендуете использовать, чтобы обезопасить себя от заражения через флеш-накопитель (многие пользуются только файловым сканером антивируса)? Могли бы вы объяснить принцип работы рекомендуемых систем защиты?
В первую очередь нужно отключить в ОС автозапуск для всех приводов и флеш-накопителей. Большинство (если не все) вредоносных программ попадают на ПК с внешних устройств именно благодаря этому сомнительному функционалу, призванному облегчать работу. Получается такая себе «медвежья услуга». Мне, например, совершенно не трудно для доступа к файлам открыть *Проводник*, а не использовать автоматический сценарий. Вторым этапом защиты должен стать резидентный антивирус, который следует обновлять ходя бы раз в пару дней. Это нужно делать, даже если доступа в Интернет нет. Почти все антивирусы могут обновляться в режиме офлайн, когда антивирусные базы скачиваются там, где есть выход в Сеть, а потом вручную переносятся на нужный ПК.

Какие эффективные методы лечения зараженной «флешки» вы бы могли порекомендовать?
Лучшее лечение в данном случае — ампутация, то есть удаление. Если вы обнаружили в корневом разделе на флешке скрытые файлы — это практически наверняка какая-то зараза. Особенно если среди них есть файл *autorun.ini*. Я в таких случаях сразу их удаляю. Если у вас возникли сомнения, действительно ли файл опасен для вас, — проверьте его на сервисе *virustotal.com*. Ну и, конечно же, перед использованием каких-либо флешек их надо проверить антивирусом.

Дело в том, что со времени повсеместного распространения дискет вирусы успели мутировать. Сегодня огромное количество вредоносных программ распространяется через съемные накопители. И это не только повсеместно используемые флешки и переносные жесткие диски, подключаемые через USB-интерфейс. Сегодня опасность несут и цифровые фотоаппараты, и видеокамеры, и портативные проигрыватели, и сотовые телефоны...

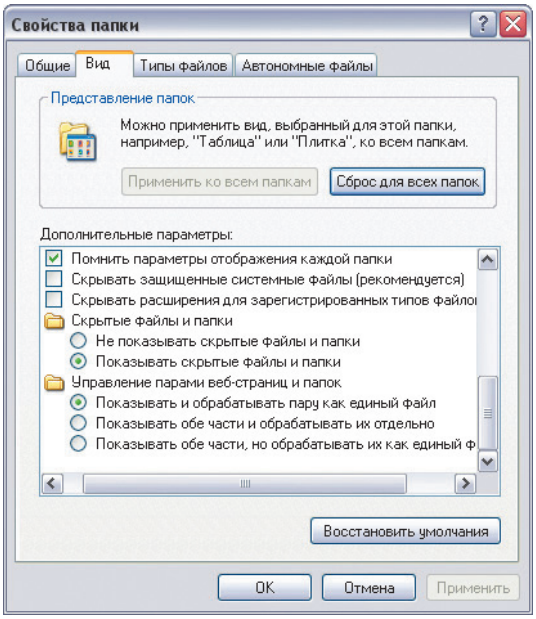
Системная уязвимость

Создатели самой популярной в мире операционной системы предусмотрели возможность автоматической загрузки сторонней программы при подключении нового девайса. Так, практически на любом носителе можно создать файл *autorun.** (вместо звездочки могут стоять различные разрешения — INF, EXE, VBS, TXT, BAT), который автоматически откроется Проводником Windows при загрузке накопителя. Далее автозагружаемый файл обычно запускает вредоносный объект, который может быть сознательно скрыт от глаз пользователя, и машина заражена...

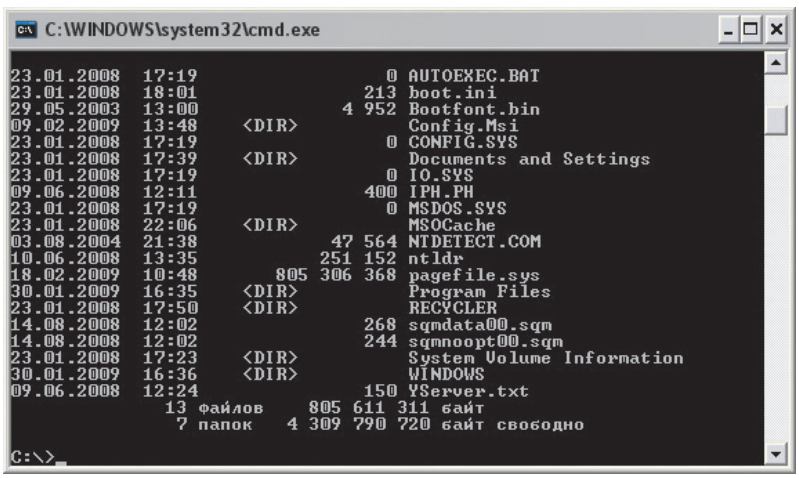
Как это ни удивительно, но во многих случаях пользователь даже не подозревает о том, что его компьютер заражен вирусом. Хорошо, конечно, что многие вредоносные программы себя практически никак не проявляют (например, не вносят изменения в документы и не удаляют важные данные), но от этого их деятельность не несет меньшей опасности. Гораздо хуже, когда с помощью вирусов конфиденциальная информация пользователя может попасть в чужие руки.

Чтобы защититься от вирусной активности, не лишним будет помнить прописную истину о необходимости использования современных средств безопасности — регулярно обновляемого брандмауэра и антивируса. Но если учесть, что большинство пользователей начинают бороться с вирусами уже после заражения ПК, а также то, что антивирусы не всегда находят свежие модификации вредоносных программ, мы опишем способ уничтожения просочившегося автозагружаемого вируса. Причем без переустановки операционной системы!

Скрытая болезнь

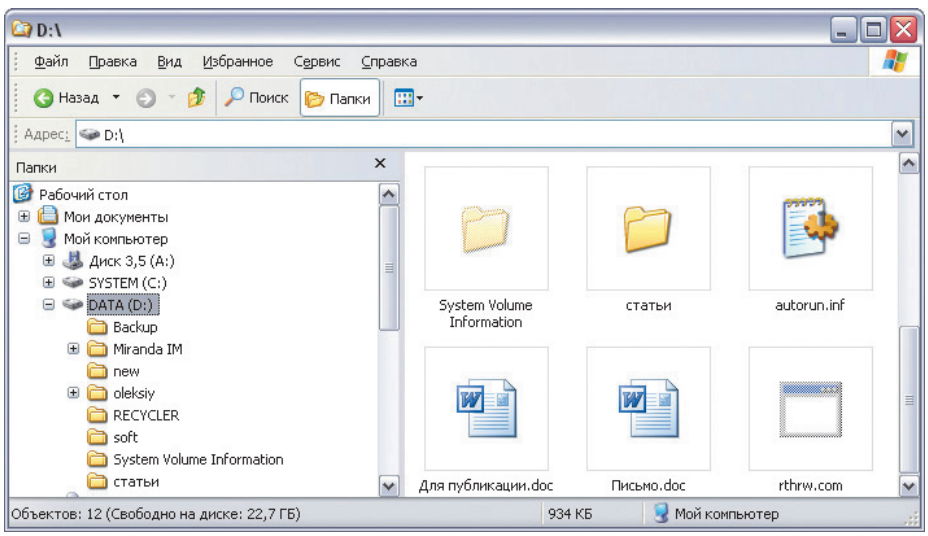


1 Практически все вирусы, которые хранятся на дисках в виде файлов, прячутся от глаз пользователей с помощью скрытого атрибута в свойствах вредоносного объекта. Поэтому для того чтобы видеть все данные, которые вы переносите на флеш-диске, не забудьте в свойствах *Проводника* задать отображение скрытых данных. Для этого в *Панели управления* откройте окно *Свойство папки* и на закладке *Вид* поставьте переключатель на *Отображение скрытых файлов* и снимите галочку *Скрывать защищенные системные файлы (рекомендуется)*.



2 Часто случается, что, даже включив функцию отображения скрытых файлов, вы не увидите их в *Проводнике*. Одно это событие уже говорит о вероятности заражения ПК вирусом. В таких случаях для отображения скрытых объектов имеет смысл воспользоваться альтернативным файловым менеджером (например, Total Commander) либо отобразить листинг корневых директорий через командную строку. Для этого в меню *Пуск* отметьте команду *Выполнить...*, наберите *cmd*. Затем в командной строке введите команду *cd* (переход в главный каталог), а после – *dir G: /a* (параметр *a* означает просмотр файлов корневого каталога диска *G:* со всевозможными атрибутами).

3 Если в результате этих действий вы увидите в корневом каталоге флеш-диска (или других дисков) файл *auto run.inf*, а с ним какой-нибудь командный файл (например, *rthrw.com*), ваш ПК наверняка заражен. В большинстве случаев простое удаление этих объектов либо невозможно, либо не приводит ни к каким результатам (файлы прямо на глазах появляются вновь). Это значит, что вирус поместил в оперативную память процесс, который постоянно следит за присутствием вредоносных файлов на локальных и флеш-дисках.



Эшелонированная оборона ПК

Сергей Шабашкевич,
начальник службы технической поддержки ЦТП «Доктор Веб»

Насколько безопасно использовать флеш-накопители без установленного антивируса? Велик ли риск потерять данные на флешке или на ПК при случайном заражении?

Если заглянуть немного в историю, то, в свое время удобным средством переноса информации были гибкие накопители (дискеты), соответственно, существовало большое количество вирусов, которые имели встроенные функции распространения через данные устройства хранения информации. Развитие и проникновение Интернета в различные сферы жизни человека обусловило распространение различных видов вредоносного кода с использованием данного канала передачи информации. В последнее время флеш-накопители стали очень распространены среди пользователей компьютеров по всему миру, прежде всего из-за своего удобства в использовании. Вирусописатели не могли пройти мимо этого — недавняя эпидемия опасного сетевого червя *Win32.HLLW.Shadow.based* (известный также под именем *Conficker.worm*, *Downadup* и *Kido*) ясно дала понять даже не очень опытным пользователям — использование флеш-накопителя является также и удобным средством для распространения вирусов. То есть налицо новый виток развития вредоносного кода. Сегодня использование антивирусных программ — это не роскошь, а суровая необходимость! Я бы не стал разделять случаи заражения на случайные или неслучайные: с точки зрения жертвы оно случайно, с точки зрения киберпреступников — вполне закономерно.

По поводу потери данных на флешке могу заметить, что риск в этом случае гораздо ниже, чем при заражении самой системы, потому что большинство червей рассматривают флешку лишь как средство доставки вредоносного кода на новые компьютеры-жертвы, а не как цель вирусной атаки. Однако и здесь есть свои исключения.

Какие вирусы опаснее — те, что можно подцепить в Интернете, или те, которые распространяются на флешках?

Все зависит от того, насколько ценна для пользователя информация на зараженной системе. Файловые вирусы, распространяющиеся с помощью флеш-накопителей, могут модифицировать файлы в системе, что, естественно, сильно повышает вероятность потери ценных данных. С другой стороны, вредоносный код, попадающий на компьютер через интернет-канал, обычно имеет вектор атаки не модификацию данных на файловом уровне, а кражу конфиденциальной информации (пароли, PIN-коды и т. д.) или превращение компьютера в зомби-солдата, управляемого извне и используемого, например, для организации DDOS-атак на неугодные сайты или массовой рассылки спам-писем.

Какие системы защиты ПК вы рекомендуете использовать, чтобы обезопасить себя от заражения через флеш-накопитель? Могли бы вы объяснить принцип работы рекомендуемых систем защиты?

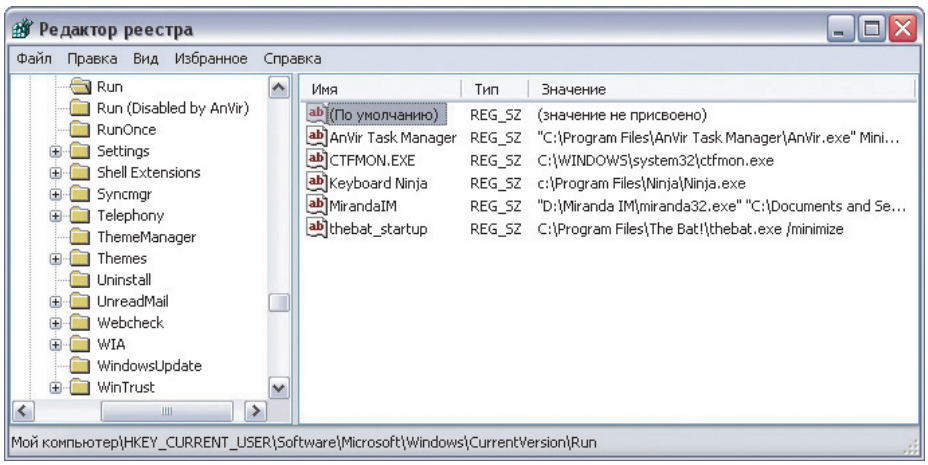
Я не открою чего-то нового, но не боюсь повториться в сотый раз — нужна так называемая эшелонированная оборона. То есть, образно говоря, если мы говорим об антивирусе, то он должен автоматически обновляться, должен работать резидентный сторож. Если мы говорим о сетевом уровне, то в системе необходимо использование межсетевого экрана (firewall), пусть даже самого простого. Если мы говорим об операционной системе, то необходимо регулярно устанавливать «заплатки», выпускаемые разработчиками программного обеспечения, благо, что эту функцию в большинстве случаев можно автоматизировать. Необходимо работать за компьютером, а тем более в Интернете, с правами пользователя, а не локального администратора. Также полезной практикой является архивирование резервных копий важной информации, хранящейся на компьютере. К сожалению, большое количество пользователей не придерживаются этих несложных правил, что в итоге рано или поздно приводит к печальным последствиям.

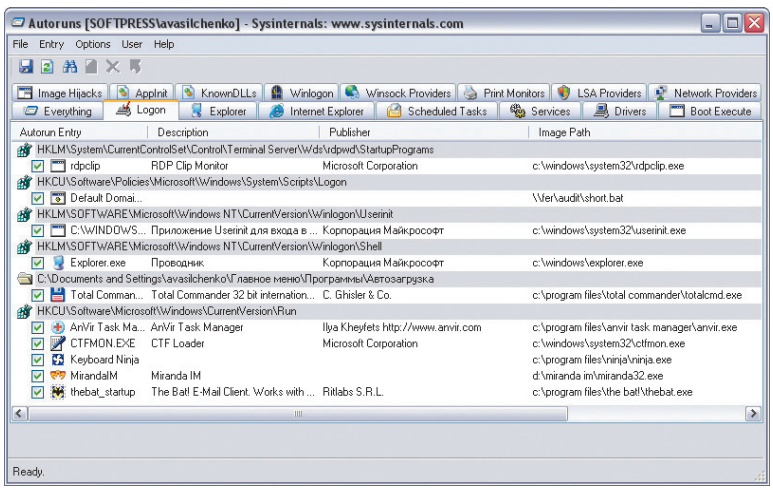
Какие эффективные методы лечения зараженной флешки вы бы могли порекомендовать?

Во-первых, на компьютере должен быть установлен антивирус, базы которого содержатся в актуальном состоянии. Во-вторых, необходимо отключить в операционной системе функции автозапуска и автопроигрывания сменных носителей информации, которые, например, в ОС Windows включены по умолчанию. В-третьих, периодически проверять содержимое флешек с помощью антивирусного дискового сканера или бесплатных лечащих утилит, например таких, как Dr.Web CureIT!. В-четвертых, следует активировать режим записи на флеш-накопитель только тогда, когда это действительно нужно. Отсюда совет — покупать флеш-накопители, поддерживающие режим «только чтение».

Простое исцеление

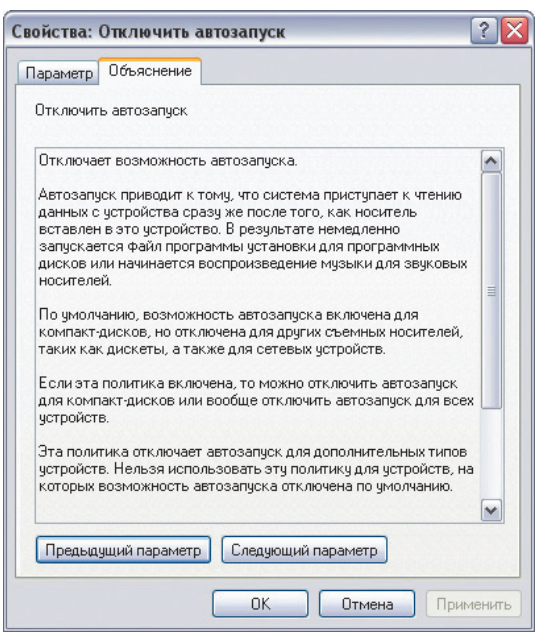
1 Если вы определили, что ваша машина заражена вирусом, прежде всего, проверьте список активных процессов. Для этого одновременно нажмите клавиши [Ctrl]+[Alt]+[Del]. Профессионал в два счета определит, какой из запущенных процессов опасен, а какой нет. Если какой-то из выполняемых файлов у вас вызывает подозрения, нужно проверить, не запускается ли он автоматически при старте Windows. Для этого в меню *Пуск|Выполнить* наберите команду *regedit* и проверьте ветви реестра *HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run* и *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run*.





2 Для поиска всех файлов автозапуска и полноценного наблюдения за системными процессами лучше использовать стандартные утилиты Microsoft. Это приложение Autoruns (*http://technet.microsoft.com/ru-ru/sysinternals/bb963902.aspx*), отображающее все автозапускаемые программы, библиотеки и драйверы, Process Explorer (*http://technet.microsoft.com/en-us/sysinternals/bb896653.aspx*), показывающее детальную информацию об активных процессах, и Process Monitor (*http://technet.microsoft.com/en-us/sysinternals/bb896645.aspx*), следящее за действиями всех процессов (обращения к реестру, файловой системе и т. д.). Теперь нужно определить, где скрывается вредоносный элемент.

3 Если вам удалось обнаружить вредоносные элементы автозагрузки и системные процессы, нужно удалить файлы, которые их запускают (появление этих файлов обычно является следствием деятельности вирусов и они обычно маскируются под системные объекты). Отключите автозапуск дисков. Для этого выполните команду *Пуск|Выполнить*, наберите *gpedit.msc*. Теперь в группе *Политика «локальный компьютер»* отметьте строку *Конфигурация компьютера|Административные шаблоны|Система|Отключить автозапуск* и установите переключатель в положение *Включено*. Далее удалите через программу Autoruns ветку реестра, которая загружает вирус, перезагрузите компьютер и удалите сам вирус (например, он может называться так *C:\Windows\system32\amv0.exe* или *C:\Windows\system32\amvo0.dll*), а также и файлы *autorun.inf* и *rthrw.com* на всех локальных дисках. Удаляя вирус, нужно внимательно проверять свойства подозрительного объекта, чтобы случайно не стереть важные системные данные.



Беспроводная домашняя сеть

Антон Черкасов, author@hi-tech.ua

Широкополосный доступ к Интернету уже не редкость, как и наличие дома сразу нескольких компьютеров. Вполне естественно желание объединить их в локальную сеть и иметь возможность не только обмениваться информацией между ними, но и выходить с каждого из них в Сеть. Давайте рассмотрим подробно, как это можно практически реализовать

Схема локальной сети с доступом к Интернету

Чтобы охватить наиболее часто встречающиеся варианты, предлагаем рассмотреть следующую задачу. Необходимо построить локальную сеть из нескольких стационарных ПК, ноутбука, КПК или коммуникатора. Доступ в Интернет должен быть с любого из этих устройств. Кроме того, необходимо иметь возможность пересылки данных внутри квартиры или дома. Интернет получаем от ADSL- или кабельного модема.

Очень часто к решению подобной задачи приступают уже после того, как локальная сеть была создана. Например, несколько десктопов уже были связаны между собой витой парой и даже имели общий выход во Всемирную паутину. Но вот появилась необходимость подключить ноутбук или КПК, или коммуникатор. Использовать провода уже становится либо не рациональным, либо вообще невозможным. К тому же при перестановке или переезде кабельная локальная сеть становится обузой — очень уж трудоемко каждый раз прокладывать провода. Беспроводные решения в этом случае оказываются наиболее эффективными. Именно поэтому мы и сделаем основной упор на них, хотя и витую пару для некоторых устройств пока оставим.

Для решения задачи нам дополнительно потребуется следующее оборудование:

Маршрутизатор должен иметь достаточное количество разъемов для подключения витой парой и иметь Wi-Fi-интерфейс для организации беспроводной сети. Желательно также наличие одного или двух встроенных портов USB, чтобы можно было в будущем подключить сетевой принтер и, возможно, сетевой накопитель NAS. Не следует забывать и о безопасности, поэтому маршрутизатор должен, как минимум, поддерживать шифрование по алгоритму WEP, а желательно WPA, как более надежное. Правда, при выборе этого алгоритма следует учитывать, что его должны поддерживать абсолютно все устройства, которые планируется включить в локальную сеть.

Адаптеры. Настольные компьютеры должны иметь сетевые карты либо под витую пару, либо беспроводные. Возможно также использование внешних Wi-Fi- адаптеров, подключаемых к USB-порту. Последние удобно использовать и с теми ноутбуками, у которых нет встроенных. Выпускаются также соответствующие PCMCIA-карты. Какие из этих устройств выбрать, решать вам. Что касается современных коммуникаторов, то они уже обычно имеют встроенный Wi-Fi.

И еще. Желательно, чтобы все беспроводные устройства были от одного производителя — проблем с совместимостью будет меньше.

Режимы Wi-Fi

Следует понимать, что если бы наша сеть состояла из нескольких компьютеров, то можно было бы вполне ограничиться Wi-Fi-адаптерами, которые бы работали напрямую друг с другом в режиме *Ad-Hoc*.

Однако для повышения производительности сети и для обеспечения ее масштабируемости необходимо использовать режим *Infrastructure*, который к тому же обеспечит централизованную защиту сети и расширит радиус ее дейс-

Основы Wi-Fi

Wi-Fi — технология беспроводного обмена данными, относящееся к группе стандартов организации беспроводных сетей IEEE 802.11. Аттестацией продукции занимается Wi-Fi Alliance.

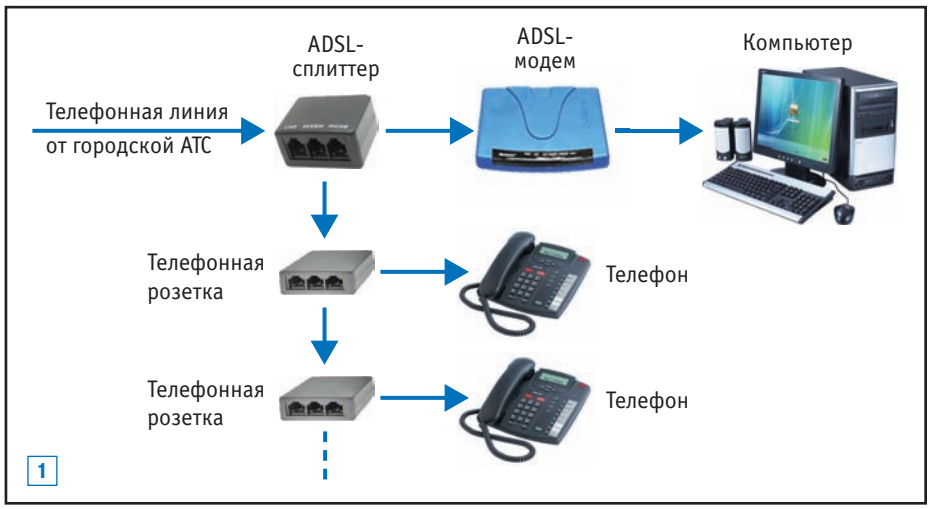
Наиболее распространены протоколы 802.11b и 802.11g, использующие частоту 2,4 ГГц.

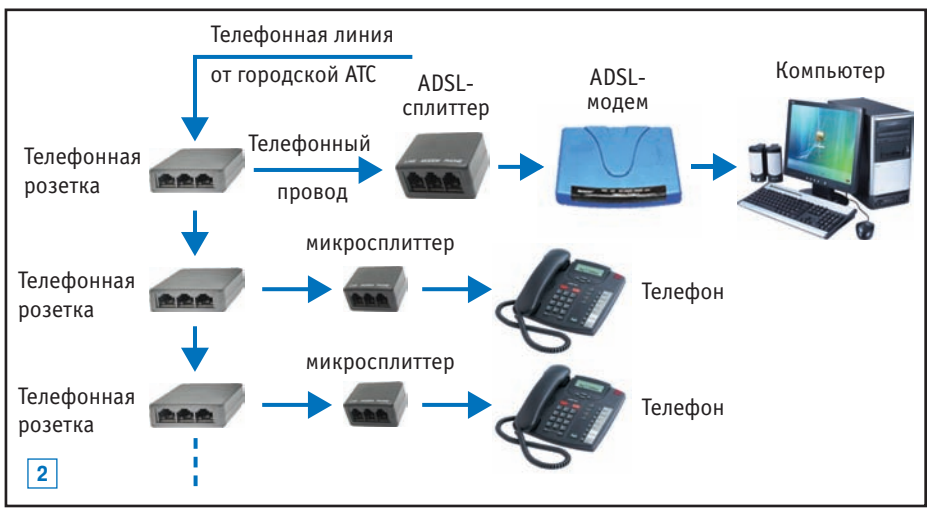
Протокол 802.11a, под частоту 5 ГГц, не совместим со стандартами 802.11b/g, и не получил у нас широкого распространения.

Стандарт 802.11n draft поддерживает обе эти частоты и обеспечивает значительно более высокую скорость передачи благодаря использование технологии MIMO (Multiple Input, Multiple Output — «много входов, много выходов») обеспечивающей одновременную передачу и прием данных.

Сравнение Wi-Fi-протоколов

Протокол	Используемая частота, ГГц	Максимальная теоретическая скорость, Мбит/с	Типичная скорость на практике, МБ/с	Дальность связи в помещении, м	Дальность связи на открытой местности, м
802.11b	2,4	11	0,4	38	140
802.11a	5	54	2,3	35	120
802.11g	2,4	54	1,9	38	140
802.11n	2,4 и 5	600	7,4	70	250





твия. Для этого нужна точка доступа или, еще лучше, беспроводной маршрутизатор. Он не только объединяет в себе функции сразу трех самостоятельных устройств (точки доступа, коммутатора и маршрутизатора), но и компактнее, удобнее и проще в настройке. Более того, в таком «комбайне» зачастую реализованы аппаратно и межсетевой экран, и DHCP-сервер и NAT, которые остается только включить и правильно настроить.

Что касается стандартов беспроводной связи b/g/n (подробнее во врезке «Основы Wi-Fi»), то при выборе всех перечисленных устройств следует учитывать, что сеть будет работать по протоколу самого медленного. В тех случаях, когда нужно отсечь медленные b-устройства, стоит сразу настроить точку доступа на *g only*.

Разворачиваем сеть:

В дальнейшем предполагается, что на- стольные компьютеры и ноутбук, подключаемые к сети, работают под управлением Windows XP.

Шаг 1. Расстановка и подключение устройств

Подключение модемов подробно описано в документации и в принципе проблем вызвать не должно. Обратим только внимание на некоторые моменты, показанные на схемах.

1 ADSL-модем следует подключать не напрямую к телефонной линии, а через сплиттер, который должен быть первым устройством, подключенным к АТС. Ко второму его выходу должны подключаться телефоны. Задача сплиттера отделить частоты голосового сигнала (0,3–3,4 КГц) от частот, используемых модемом (26 кГц — 1,4 МГц).

2 Когда телефонная разводка не позволяет подключить первым сплиттер, телефонные аппараты нужно подключать через отдельные микросплиттеры или фильтры.

Беспроводной маршрутизатор/коммутатор желательно размещать на равноудаленном расстоянии ото всех мест, где может понадобиться связь, но при этом учитывать, что на прохождение сигнала очень сильно влияют толстые стены, особенно бетонные. Значительные помехи могут создавать микроволновые печи, DECT-телефоны, Bluetooth-устройства, работающие на той же частоте 2,4 ГГц. Все это приводит к уменьшению скорости пе-

редачи данных или делает связь вообще невозможной.

Шаг 2а. Настройка автономного модема

В настоящее время одним из самых популярных украинских DSL-провайдеров является «Укртелеком» с услугой «ОГО». В числе рекомендованных им для использования модемов чаще всего применяется Iskratel Callisto 821+R3. Поэтому на его примере и рассмотрим процесс настройки.

ADSL–модем в режиме моста

Для настройки, модем нужно подклю-

ADSL-модем. К гнезду DSL подключается телефонный кабель от сплиттера, к гнезду PWR – питание, а к Ethernet – витая пара, другой конец которой соединяют с ПК, маршрутизатором или коммутатором

чить кабелем витой пары к компьютеру, но предварительно на последнем нужно зайти в свойства TCP/IP сетевого адаптера, к которому будет подключаться модем (*Панель управления/Сеть*) и настроить IP-адрес: 192.168.1.3, маска – 255.255.255.0, шлюз – 192.168.1.1 (соответствующий внутреннему адресу модема по умолчанию) и адреса первичного и вторичного DNS-серверов – 192.168.1.1 и 195.5.46.12, соответственно (здесь и далее для «Укртелеком»). Сохранив настройки, перезагружаем компьютер и включаем модем.

Набираем в командной строке или в адресной строке любого браузера: *http://192.168.1.1* и на открывшейся вебстранице указываем логин и пароль (по умолчанию оба *admin* или *qe1dg7bm* / *qa6yo9km*). В результате откроется панель управления устройством. Здесь можно выбрать пункт *Quick Setup* и пошагово провести все настройки, каждый раз щелкая по кнопке *Next*. Более детальные настройки можно выполнить через меню *Advanced*. Рассмотрим его подробнее.

Переходим в реаздел *LAN / DHCP Server* и проверяем, что флажок там выключен. Здесь же можно подредактировать при необходимости IP-адрес модема.

3 Переходим в раздел *WAN/Connections*. Создавая новую конфигурацию (*Add*), вводим значения параметров VPI=1, VCI=32, выбираем режим *Bridging*, метод инкапсуляции *LLC/SNAP* и также применяем все эти настройки. Если теперь остается щелкнуть на кнопке *Finish* и модем перезагрузится. Это займет секунд 40, после чего он будет готов к работе в режиме моста.

Если бы к Интернету подключался только один компьютер, следовало бы только включить на нем брандмауэр. В нашем же случае для совместного использования Сети несколькими компьютерами потребуется подключить модем ко внешнему маршрутизатору, и уже с него «раздавать» Интернет.

О модемах

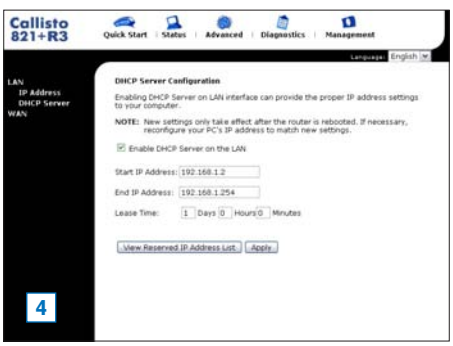
В рассматриваемом нами случае широкополосный доступ к Интернет будет обеспечиваться модемами.

ADSL-модемы подключаются через сплиттер к телефонной линии. Один или несколько их LAN-портов служат для подключения к компьютера, коммутатора или маршрутизатора. Эти модемы, как правило, способны работать в одном из двух режимов: мост(bridge) или маршрутизатор (router). И в зависимости от выбранного режима дальнейшие действия по организации локальной сети могут отличаться.

В режиме моста (обычно стоит по умолчанию) модем работает аналогично обычному dial-up модему (правда без дозвона), используя для соединения с провайдером логин и пароль (PPPoE). Достоинства данного режима — простота для неподготовленого пользователя, а недостаток — необходимость каждый раз для соединения с Интернет запускать соответствующее сетевое подключение. Для организации совместного доступа в Сеть с нескольких ПК потребуется дополнительный маршрутизатор. Необходимо также предусмотреть специальные меры по безопасности, так как без них локальная сеть будет видна извне.

В режиме маршрутизатора модем работает как самостоятельное устройство, он сам соединяется с провайдером и сам раздает Интернет в локальную сеть. Достоинства — пользователь фактически имеет постоянное и при этом безопасное подключение к Интернету. В этом режиме можно без дополнительных затрат подключить существующую локальную сеть к Интернету, используя уже установленный в ней коммутатор. Недостаток — для работы некоторых программ может потребоваться настройка маршрутизации, а безопасность будет все-таки ниже, чем при использовании внешнего маршрутизатора.

Кабельный модем, имеет всего один режим работы — мост(bridge) и обычно никакой дополнительной настройки не требует. Отметим только, что к нему необходимо просто подсоединить коаксиальный антенный кабель, идущий от сплиттера, а к Ethernet-порту сразу можно подключить сетевую карту компьютера (если он один) или маршрутизатор (если в локальной сети несколько ПК). После включения питания постоянное соединение с Интернетом будет установлено автоматически.



ADSL-модем в режиме маршрутизатора

4 В том случае, когда необходимо организовать подключение уже существующей локальной сети к широкополосному Интернету имеет смысл перевести модем в режим роутера. Для этого его также следует подключить к компьютеру, зайти в веб-интерфейс и перейти в реаздел *LAN/ DHCP Server*, как это было описано выше. Там следует включить флажок, проверить предлагаемый диапазон допустимых IP-адресов и щелкнуть на *Apply*.

5 Теперь переходим в окно создания новой конфигурации *WAN/Connections*. В нем необходимо ввести параметры VPI=1, VCI=32, выбрать режим *PPPoE*, разрешить использование NAT, а также заполнить поля *PPP Username* и *PPP Password* (логин и пароль, полученные от провайдера).

После этого остается только щелкнуть на кнопке *Finish*, и модем перезагрузится.

Есть возможность включить аппаратный брандмауэр, настроить маршрутизацию и т. д. Подробно мы здесь на настройке этого режима останавливаться не будем, так как более надежным все-таки является использование внешнего маршрутизатора.

Шаг 2б. Настройка модема-маршрутизатора

В качестве примера возьмем беспроводной маршрутизатор ASUS DSL-N13. Это устройство включает ADSL-модем, маршрутизатор, коммутатор с четырьмя LAN-портами и точку доступа, выполненную в соответствии со стандартом 802.11n (draft) и обеспечивающую беспроводную передачу данных на скорости более чем 100 Мбит/с. При этом сохранена совместимость с устройствами 802.11b/g, благодаря чему нет острой необходимости перестраивать существующую домашнюю сеть.

Маршрутизатор ASUS DSL-N13 – это комбинированное устройство, включающее и ADSL-модем (с режимом моста), и маршрутизатор, и точку доступа

6 Подключившись к компьютеру, заходим на домашнюю веб-страничку устройства, используя IP-адрес 192.168.1.1 и маску сети 255.255.255.0.

7 По умолчанию откроется окно быстрой настройки. Модем попытается автоматически определить тип ADSL-соединения. Если это не удастся, придется перейти к ручной настройке, выбрав *Advanced Setup/WAN*. Там можно создать новое соединение (*Add*), удалить (*Remove*) или отредактировать (*Edit*) существующее. В нашем случае соединение должно быть PPPoE и для него нужно будет указать имя пользователя и пароль, полученные от провайдера Интернет, а также параметры VPI и VCI.

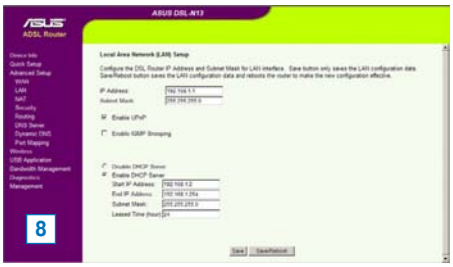
8 Поскольку устройство комбинированное, его необходимо настроить на работу с локальной сетью. Для этого заходим в раздел *LAN*, где проверяем значения IP-адреса и маски нашего маршрутизатора, а также включаем его встроенный DHCP-сервер. Для последнего указываем для допустимый диапазон адресов, которые будут автоматически назначаться сетевым устройствам (*Start IP Adress* и *End IP Address*). Маску, в нашем случае, одноранговой сети оставляем без изменения (255.255.255.0).

9 В дальнейшем следует настройка беспроводной сети (пункт *Wireless*), в ходе которой требуется включить флажок *Anable Wireless*, задать имя сети (SSID), а затем, на страничке Security, указать уровень безопасности с соответствующим протоколом шифрования (*Network Autentication*) и соответствующим ему значением ключа.

Настройки каждой странички следует сохранять (*Apply*), а самом конце не забыть перезагрузить устройство, щелкнув мышью на кнопке *Save/Reboot*. Перезагрузка займет порядка минуты, после чего на экране появится домашняя страничка с обновленными настройками.

В рассмотренном устройстве есть различные дополнительные возможности, например, настройка разделения общей пропускной способности между такими задачами, как игры, Интернет, FTP-сервер и VoIP (пункт *Bandwidth Management*), диагностика устройства (*Diagnostics*) и другие.

Значительно упростить базовую настройку устройства может программа EZSetup, поставляемая в комплекте на диске, но перед использованием ее нужно инсталлировать на ПК. Затем пошагово с картинками вам будет подробно рассказано, что следует сделать.



Обратите внимание!

При использовании не комбинированного, а автономных устройств, DHCP-сервер можно включить и на одном из них, например, на точке доступа. Однако, если локальная сеть получает Интернет от маршрутизатора следует поднимать этот сервер именно на нем.

Основы безопасности

WEP (Wired Equivalent Privacy) — устаревший алгоритм для обеспечения безопасности беспроводной IEEE 802.11 сети, которые используя радиосвязь, в большей степени подвержены прослушиванию, чем проводные. WEP позволяет администратору беспроводной сети определять для каждого пользователя набор ключей, основанный на «строке ключей». Пользователь, не имеющий требуемого ключа, не может получить доступ в сеть. Используется алгоритм шифрования RC4 с 40-битным или 104-битным ключом. Все станции (как клиентские, так и точки доступа) получают свой ключ, который применяется для шифрования данных, прежде чем последние будут переданы на передатчик. Если станция получает пакет, не зашифрованный соответствующим ключом, он исключается из трафика. В то же время было обнаружено, что WEP-связь имеет лазейки в обеспечении секретности и ее можно взломать за несколько минут. Поэтому в 2003 г. Wi-Fi Альянс предложил использовать WPA. Несмотря на свои недостатки, WEP и сегодня широко используется, поскольку далеко не все устройства способны поддерживать WPA.

WPA (Wi-Fi Protected Access) — обновленную программа сертификации устройств беспроводной связи с усиленной безопасностью данных и ужесточенным контролем доступа к беспроводным сетям. По сути это сумма не-скольких технологий: EAP, TKIP, MIC и 802.1X.

EAP (Extensible Authentication Protocol) — основа для механизма аутентификации пользователей, непременным условием которой является предъявление пользователем свидетельства (мандата), подтверждающего его право на доступ в сеть. Для этого права пользователь проходит проверку по специальной базе зарегистрированных пользователей, расположенной на специальном сервере (чаще всего RADIUS). Без аутентификации работа в сети для пользователя будет запрещена. WPA также имеет упрощенный режим, подходящий для домашнего применения — WPA-PSK (Pre-Shared Key), в котором аутентификация производится с использованием пароля, а не по сертификату.

TKIP (Temporal Key Integrity Protocol) — отвечает за увеличение размера ключа с 40 до 128 бит, а также за замену одного статического ключа WEP-ключами, которые автоматически генерируются и рассылаются сервером аутентификации. Благодаря специальной иерархии ключей и методологии управления ими исключается их излишняя предсказуемость.

MIC (Message Integrity Check) — механизм проверки целостности сообщений для предотвращения перехвата пакетов данных, построен на основе мощной математической функции, которая применяется на стороне отправителя и получателя, после чего сравнивается результат. Если проверка показывает на несовпадение результатов вычислений, данные считаются ложными и пакет отбрасывается.

Шаг 3. Настройка сети

В этом разделе необходимо обеспечить связь между компьютерами по локальной сети. Для этого потребуется настроить сетевой интерфейс. Коротко остановимся на этом, предполагая, что настольный компьютер будет подключаться витой парой, а ноутбук по Wi-Fi. Если же оборудовать десктоп беспроводной сетевой картой или адаптером, то настройки будут такими же, как на ноутбуке. Предполагается также, что драйверы сетевых карт и адаптеров в операционных системах всех компьютеров уже установлены.

Настольный ПК

Открываем *Пуск/Сетевое окружение/Отобразить сетевые подключения*. Если ни одного соединения еще нет, выбираем задачу *Создание нового подключения* и следуем указаниям Мастера. Если подключение по локальной сети уже есть, достаточно просто проверить и при необходимости изменить его свойства. Поскольку на маршрутизаторе был включен DHCP-сервер, выбираем в свойствах протокола TCP/IP автоматическое получение адресов IP и DNS-сервера. Это избавит нас от многих забот по их выбору. В качестве шлюза для выхода в Интернет будет использоваться маршрутизатор.

Ноутбук

В свойствах беспроводного соединения выбираем вкладку *Беспроводные сети*. Там добавляем новую сеть (кнопка *Добавить*) и заполняем поля в открывшемся окне значениями, которые мы использовали на «Шаге 2б» при настройке беспроводного маршрутизатора.

Подробнее о режимах шифрования и аутентификации рассказывается во врезке «Основы безопасности». Выбирать следует те, которые поддерживаются абсолютно всеми устройствами, входящими в сеть. При настройке Wi-Fi лучше сначала отключить шифрование и только после того, как все заработает, настроить и его.

Шаг 4. Дополнительные меры безопасности

Поскольку беспроводная сеть может стать доступной не только членам вашей семьи, но и соседям, нужно обязательно позаботиться о ее безопасности. Для этого нужно:

- изменить установленные по умолчанию логин/пароль на доступ к интерфейсу управления маршрутизатором или точкой доступа.
- Отключить режим трансляции имени беспроводной сети (SSID). Это усложнит процесс подключения: придется вручную прописывать имя сети, к которой необходимо подключиться, зато исключает случайное ее обнаружение сторонними пользователями
- Установить режим шифрования всех передаваемых данных 64/128-битным ключом и использовать сложные ключи с разнообразным набором символов.

Можно также установить привязку к MAC-адресам беспроводных устройств работающих в сети, чтобы разрешить вход в систему только ранее прописанным в системе пользователям и установить время доступа к сети, в течение которого возможно подключение к ней. Однако в настоящее время эти приемы нельзя назвать очень надежными.

Что еще подключить?

Многих может заинтересовать, как дополнить нашу сеть принтером, чтобы он был доступен с любого компьютера. Очень интересные возможности открывает также подключение к локальной сети сетевого накопителя NAS. Но обо всем этом и многом другом мы расскажем в следующих номерах.

Редакция благодарит компанию «КорТел» и представительство ASUS в Украине за предоставленное оборудование

Евгений Барилюк barilyuk@hi-tech.ua

Как стать **невидимкой** в Сети

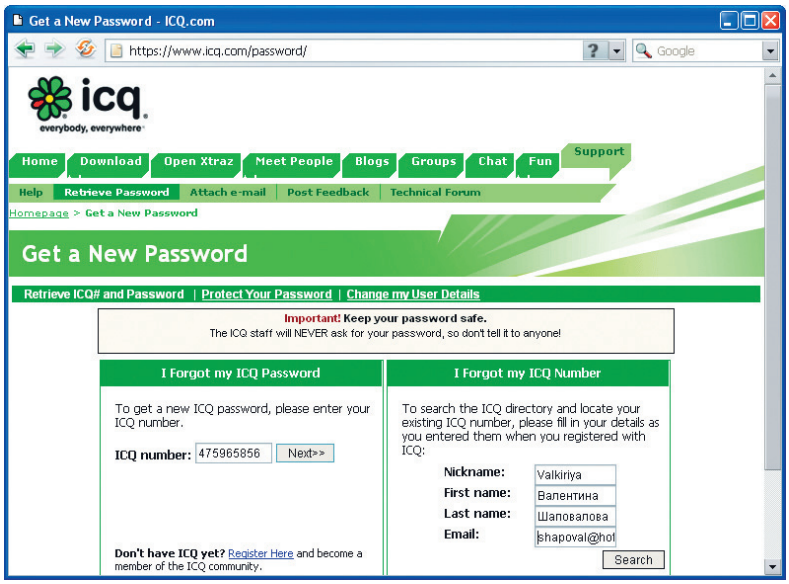
Путешествуя по Интернету вы, сами того не желая, оставляете массу информации потенциальным злоумышленникам. Но скрыться от их взглядов и тем самым обезопасить себя и свой ПК все-таки можно и нужно. Вот пять наиболее распространенных атак и рекомендаций, как не потерять ваше виртуальное, а иногда и реальное имущество в Глобальной паутине

Задумываетесь ли вы, сколько информации о вас и вашем ПК передается в Сеть после одного щелчка мышкой? Оказывается, хотите вы того или нет, вы отправляете много информации о себе: IP-адрес, версию и название операционной системы, конфигурацию браузера (включая название и номер версии) и даже разрешение экрана. По идее, эта информация предназначается лишь для «электронных мозгов» сервера, чтобы он знал, какую веб-страницу вам отправить. Например, некоторые веб-сайты для разных браузеров могут иметь разные варианты веб-страниц. Однако на практике веб-мастеры чаще всего создают лишь одну версию страницы под один браузер (зачастую это Internet Explorer), но хотя для вывода веб-страницы ваши данные уже не нужны, они все равно высылаются серверу.

На первый взгляд, ничего страшного в том, что кто-то узнает ваш IP-адрес, особенно когда при этом вы еще думаете, что ничего такого на вашем ПК нет, и злоумышленников вам бояться не нужно. Но недоброжелатель, зная высылаемые серверу параметры, может вычислить ваш адрес электронной почты, географическое местоположение, и, что самое важное, паспортные данные. Кроме того, он может просто ограничиться атакой на ПК для пополнения своей бот-сети, рассылающей спам. Поэтому имеет смысл скрыть часть отправляемой информации, а также принять меры для повышения уровня безопасности вашей личной информации от кражи.

1 Угнать тетю Асю

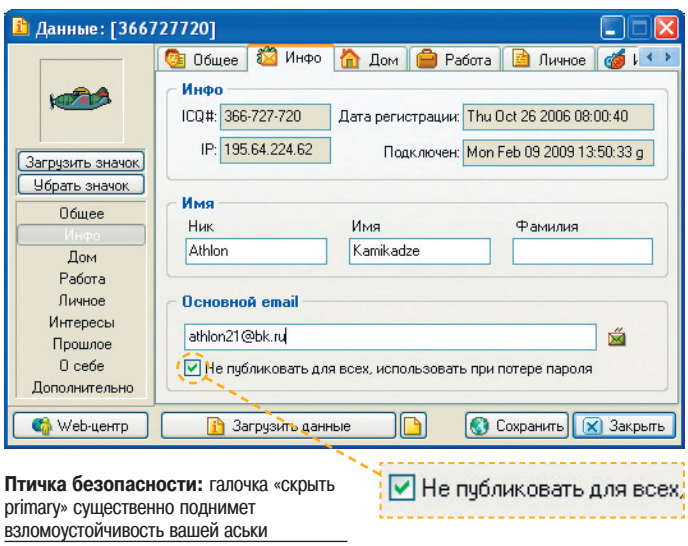
Большинство отечественных пользователей сети воспринимают сервис обмена мгновенными сообщениями ICQ как нечто должное и даже не представляют, что идентификационный номер аськи может стать объектом виртуальной охоты с целью последующей перепродажи. Еще меньше пользователей помнят, что идет активная охота практически на все номера сервиса. Продается все: от девяток (девятизначных номеров) для спама до пятерок. Только на памяти автора числится два угона, владельцы которых поленились использовать пароль посложнее, чем «123456» (на взлом ICQ с таким паролем уходит не больше десяти секунд). Так как же защитить свой UIN (user identification number — идентификационный номер пользователя) от угона (будь то свежекупленный или кровно зарегистрированный номер)? **Для этого вам нужно соблюдать несколько простых правил, которые снизят риск угона до минимума**.



Превратности безопасности: восстановить пароль аськи можете не только вы, но и злоумышленник

Первое: не используйте простой пароль: он не должен содержать часто произносимые слова, имена, даты рождения, числа, названия мест, городов и популярных музыкальных групп. Например, такой пароль как «boombox» современный двухъядерный компьютер подберет за 13 минут. Никогда не используйте один пароль на форумах и других программах: очень часто бывало, что хакеры взламывали форум, а потом по его базе подбирали пароли на номера ICQ пользователей, и иногда пароли совпадали.

Конечно, запомнить пароль вида «m@Z!138#» просто нереально, но зато все тот же двухъядерный ПК потратит на его взлом аж 23 года — но, скорее всего, хакеры оставят эту затею раньше ☺. А чтобы лучше запоминалось, следует использовать осмысленные слова, добавляя к ним пару спецсимволов и чередуя регистр. Например, фраза «kRiShKa@17» если и не является абсолютным паролем, то, по крайней мере, доставит существенные хлопоты взломщикам. И, наконец, самое главное: пароли рекомендуется менять один раз в месяц или даже чаще.



Птичка безопасности: галочка «скрыть primary» существенно поднимет взломоустойчивость вашей аськи

Второе: по возможности не пользуйтесь своим номером в интернет-клубах, кафе, компьютерных клубах и пр. Для этих целей заведите себе простой девятизначный номерок, который не жалко и потерять.

Третье: служба ICQ позволяет в случае утраты пароля восстановить его (*icq.com/password*), отправив ответ на секретный вопрос и на указанный e-mail (он называется primary — первичный). Даже если вы укажете несколько e-mail-адресов, пароль будет высылаться только на primary. Однако используемая система несовершенна. Например, в качестве primary e-mail часто указывают ящик на бесплатном хостинге, о котором потом забывают. Со временем хостинг-провайдер удалит ящик как неиспользуемый. В итоге взломщик может повторно зарегистрировать этот ящик и затребовать новый пароль. Как видите, с таким заданием справится и ребенок. Поэтому рекомендуется скрывать адрес primary e-mail (эта настройка есть во всех современных IM-клиентах), а также не использовать его для регистрации на форумах.

Полезные ссылки

- *http://ru.wikibooks.org/wiki/Защита_конфиденциальных_данных_и_анонимность_в_интернете* — детальная информация об анонимности и безопасности в Сети
- *http://ru.wikipedia.org/wiki/SOCKS* — подробная информация о socks, особенностях их работы и использования
- *http://proxyfree.ru* — здесь всегда есть свежие прокси-серверы
- *http://ip-whois.net* — узнать чей-нибудь IP-адрес и географическое расположение можно с помощью этого сервиса
- *http://russianproxy.ru/socks5_proxy_list_fastest* — список доступных socks-серверов

2 Зомби из ПК

В последнее время не только в электронной почте и ICQ, но и социальных сетях стали появляться различные программы, «сенсационные новости», фотографии знаменитостей и прочая интересная информация. Но не доверяйте и никогда не запускайте подобные ссылки (даже если антивирус проверил и сказал, что в письме вирусов нет). Дело в том, что вместе с присланным ПО вы в нагрузку получите и троянского коня, а ссылка на сайт с сенсациями превратит компьютер в зомби (звено бот-сети). Тогда вы наверняка лишитесь и номера ICQ, и почтового ящика, а ПК будет использоваться для рассылки спама. Плюс ваши друзья начнут получать от вас письма с вредоносным ПО или ссылки на сенсационные новости. **Поэтому ни в коем случае не открывайте неизвестные приложения, даже если письмо пришло от человека, которого вы давно знаете.** Все просто — его компьютер взломали и от его имени рассылают трояны по всему контакт-листу.

Кроме того, полностью доверять антивирусам и файрволу вообще не следует — самым слабым звеном в системе компьютерной безопасности, как всегда, остается человек, а самое главное оружие против компьютерных злоумышленников — ваш здравый рассудок. Дело в том, что в Сети есть огромное количество программ, которые просто перемешивают код зловредного ПО, и эвристические анализаторы и проактивная защита зачастую «не узнают» давно известного троянского коня.

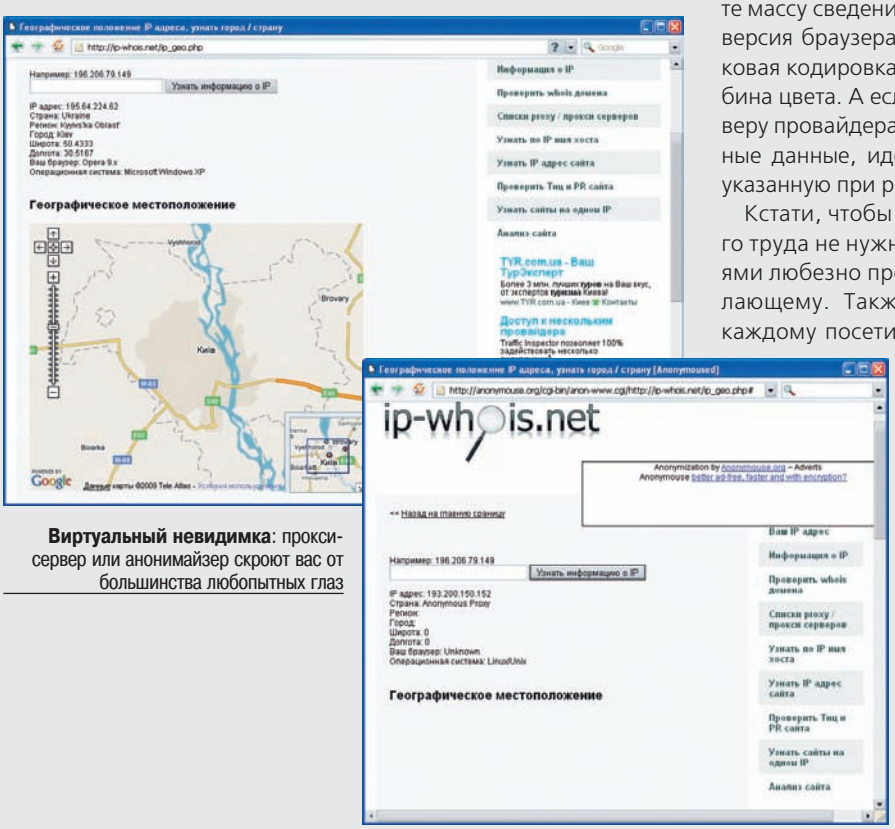
Но поскольку большинство спамеров не используют самые передовые наработки вирусописателей, то регулярное обновление антивирусов и установленный файрвол снизят риск зомбирования вашей машины как минимум вполовину. Кстати, эксперты по безопасности утверждают, что лишь использование учетной записи без прав администратора повышает безопасность Windows на 60 %.

Популярные Socks-клиенты

SocksCap — *www.vpnservice.info/sockscap.html*
FoxyProxy — *http://foxyproxy.mozdev.org*
FreeCap — *www.freecap.ru*
Proxifier — *www.proxifier.com*
Anonymous Guest Professional — *www.spszone.com/anguest*

3 Алло, это кто?

Говоря о сетевой безопасности, стоит для начала развеять самый устойчивый миф, касающийся анонимности в Интернете. Нет, не о том, что еще многие люди думают, будто в Сети о человеке ничего нельзя узнать. Очень часто можно услышать: «Мне не нужна анонимность, ведь я не занимаюсь ничем предосудительным. Пусть хакеры об этом беспокоятся...». А теперь подумайте, понравится ли вам, если прохожие будут знать ваш адрес, следить за вами и стараться проникнуть к вам домой? Поэтому обеспечению анонимности в Интернете следует уделять должное внимание.



Виртуальный невидимка: прокси-сервер или анонимайзер скроют вас от большинства любопытных глаз

Нажимая мышкой на ссылку, вы, хотите того или нет, передаете массу сведений о своем ПК, как то IP-адрес, используемая ОС, версия браузера, URL предыдущей посещенной страницы, языковая кодировка, часовой пояс и даже разрешение экрана и глубина цвета. А если заинтересованное лицо получит доступ к серверу провайдера, то по IP-адресу сможет получить ваши паспортные данные, идентификационный код и другую информацию, указанную при регистрации у провайдера.

Кстати, чтобы получить о вас подробную информацию, много труда не нужно: ICQ и другие программы обмена сообщениями любезно предоставляют IP-адрес собеседника любому желающему. Также некоторые форумы показывают IP-адреса каждому посетителю, а после написания комментария вы можете с удивлением обнаружить, что рядом с никнеймом выводится и ваш IP-адрес

Для начала можно попробовать «спрятаться» с помощью прокси-сервера, который является посредником между компьютером пользователя и серверами Сети. Но это лишь на первый взгляд использование прокси-сервера — гарантия анонимности. Оказывается, подавляющее большинство прокси-серверов в своих запросах передают в специальном поле IP-адрес конечного пользователя. Правда, есть и анонимные службы, вот только найти их не так уж и просто, так как они обычно закрываются в течении недели после публикации. Взять себе свежий прокси можно по адресу http://*ip-whois.net/proxy.php*.

Ручная дезинфекция

Довольно часто бывает, что даже новейшие версии антивирусов рапортуют о безвирусной системе, которая тем временем выдает глюк за глюком. Как отловить заразу? Достаточно простым, но эффективным тестом на внедрение вирусов был и остается поиск по вновь созданным файлам. Почти все троянские и шпионские компоненты не утруждают себя модификацией даты создания файла, а потому обнаруживаются в момент. Все, что нужно после посещения подозрительных уголков Сети, — как можно быстрее нажать на «*Пуск — Найти — Файлы и папки*». Ищем файлы, созданные за последний день на диске C: (для надежности можно охватить и другие диски). Там будет много всего, но нас в первую очередь интересуют исполняемые файлы (EXE), динамические библиотеки (DLL) и прочие программные компоненты, расположенные в *Program Files* и каталоге *Windows*.

Далее необходимо избавиться от инфицированных файлов, предварительно отослав их в антивирусную лабораторию на анализ, и восстановить «чистые» компоненты с диска установки Windows.

Для восстановления компонентов Windows вставьте компакт-диск с дистрибутивом, а в меню *Пуск-Выполнить* наберите команду *sfc /scannow*. Запустится утилита *Защита файлов Windows*, которая проведет сканирование и предложить заменить отсутствующие или поврежденные файлы на оригинальные.

Другой вариант сохранения анонимности в Интернете — использование анонимайзеров (anonymizer). Анонимайзеры — это, по сути, просто анонимные прокси-серверы, имеющие собственный веб-интерфейс. И работать с ними очень просто. Заходим на сайт, вводим в специальное поле адрес нужного нам сервера — и все, запрашиваемая страничка загружается. Правда, при использовании анонимайзеров придется смириться с парой недостатков. Во-первых, скорость загрузки страниц может значительно уменьшиться. А во-вторых, на сегодняшний день уже практически невозможно найти бесплатный анонимайзер. Конечно, когда эти службы только появились, никому и в голову не могла прийти мысль о сборе денег за свои услуги. Максимум, что владельцы могли себе позволить, — это «повесить» несколько рекламных баннеров. Теперь же пользователям приходится платить за роскошь остаться неузнанным.

Логичным будет объединение нескольких прокси-серверов по всему миру в последовательную цепочку, что существенно затруднит поиск отправителя. Эта задумка реализована в проекте Tor (*www.torproject.org*). Tor работает со многими существующими приложениями, включая веб-браузеры, системы мгновенного обмена сообщениями и другим ПО, использующим протокол TCP.

Существует еще один способ обеспечения анонимности в Интернете, который является на сегодняшний день самым надежным. Речь идет о socks-протоколах. Принцип действия этой технологии в общем-то похож на работу прокси-сервера. Правда, есть несколько серьезных различий. Так, «общение» клиентского компьютера и socks-сервера происходит не по общепринятым, а по специальным протоколам (socks4, socks5 и т. д.). В результате передача IP-адреса пользователя невозможна в принципе. Кроме того, socks-сервер сам преобразовывает информацию от пользователя в запросы для общепринятых протоколов. А это значит, что ни один сервер «не догадается», что отправляет данные не конечному пользователю, а посреднику. Да и работать с технологией socks очень удобно — достаточно скачать любой Socks-клиент (см. вставку «Популярные Socks-клиенты»). Установив клиент, настройте его — и можно больше ни о чем не беспокоиться.

Безопасность без прав

Практически все пользователи используют дома лишь одну учетную запись, имеющую права администратора, и продолжают ругать Windows за «дырявость», не догадываясь, что для существенного повышения безопасности Windows вовсе не требуется иметь продвинутые знания по администрированию ПК, а достаточно лишь использовать учетную запись с ограниченными правами.

Как подсчитали в компании BeyondTrust, если бы пользователи работали в Windows без административных полномочий, то для них 92 % из обнаруженных в системе за год критических уязвимостей оказались бы не столь опасны или вообще не имели бы значения.

В компании изучили бюллетени по безопасности Windows, выпущенные корпорацией Microsoft за 2008 год. Как выяснилось, в подавляющем большинстве из них в разделе о мерах по снижению и устранению риска атаки говорилось, что пользователи, работающие без привилегий администратора, менее уязвимы. Это касается 92 % критических уязвимостей и 69 % от всех 154 ошибок, выявленных и исправленных за прошлый год.

Когда же исследователи перешли к изучению браузера Internet Explorer и офисного пакета Microsoft Office, выяснилось, что и здесь доли уязвимостей, от которых можно защититься отказом от привилегий администратора, составляют соответственно 89 и 94 %.

Кстати, недавно опубликованный способ обхода системы UAC в Windows 7 (*www.thevista.ru/page.php?id=10752*) тоже касается только пользователей с правами администратора.

И напоследок: если вам никак нельзя обойтись без учетной записи с правами администратора, используйте как можно более сложный пароль.

4 Виртуальный дядя-миллионер

В наш прогрессивный XXI век даже мошенники переходят на электронную форму работы. Сейчас они активно рассылают спам-письма, в которых пишут, что вы являетесь дальним родственником миллионера из Великобритании, предлагая оплатить офисные расходы по получению денег богатого родственника. И если в это вряд ли кто поверит, то в выигрыш в лотерее поверят многие. Поэтому такие письма стоит просто удалять не читая, особенно если вы не принимали участия ни в каких розыгрышах.

Лучше внимательно читайте бланки уведомлений банков, копии счетов и прочую конфиденциальную информацию, приходящую к вам по электронной почте. Документы могут быть подделками, с помощью которых злоумышленник пытается узнать ваши персональные данные. Если есть сомнения, обратитесь в свой банк за подтверждением.

Возьмите за правило: никому в Сети нельзя доверять свои персональные данные – номера счетов, веб-кошельков, пароли доступа и пр. А участвуя в онлайн-аукционах или покупая товары в Интернете, никогда не соглашайтесь на предоплату товара, так как потом будет проблематично вернуть свои деньги.

И помните, мошенники эксплуатируют самые простые человеческие чувства – жадность, гордость, любовь к «клубничке», лень. Если вы видите какое-то «странное» сообщение, которое давит как раз на них, – это тоже повод задуматься, не пытаются ли вами манипулировать. Если вам предлагают удивительно выгодные условия сделки, скорее всего, вас хотят обмануть.

Вообще, социальная инженерия – один из самых продуктивных (и иногда единственный) способ взлома, так как жертва сама выдает все, что нужно. Суть метода проста: вор заговаривает зубы, вытягивая требуемую информацию. Допустим, что вы получили письмо, в котором администрация ICQ, приносит свои извинения, сообщает о каких-то технических неполадках и просит вас повторно выслать им пароль. Не верьте, на 100 % это обман. Или помните, как регистрируясь на бесплатном mail-сервере, вы заполняли поле «секретного вопроса»? К примеру, это мог быть вопрос: «Как зовут мою собаку?». Вор запросто может в милом разговоре по аське аккуратно вытянуть из вас имя вашего питомца.

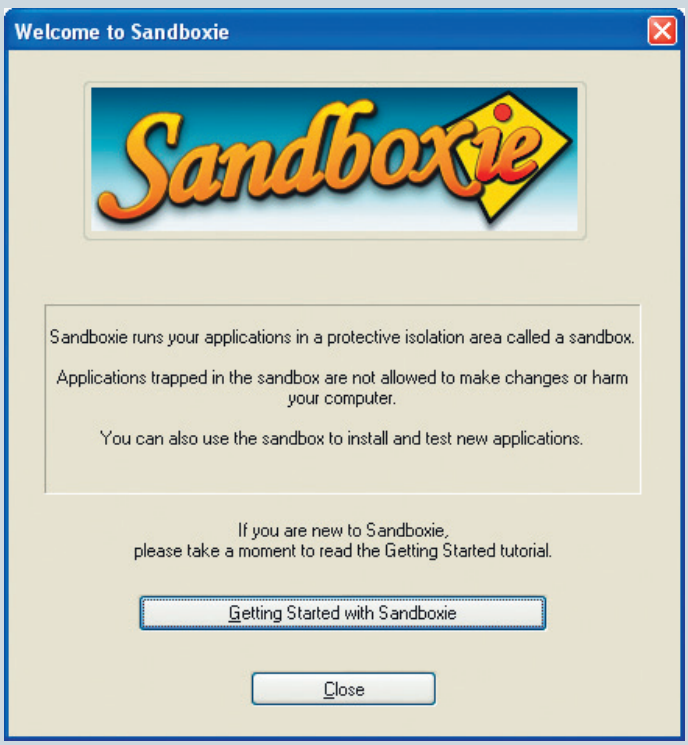
Безопасная песочница

Тем пользователям, которые не смогли воспользоваться технологией VirtualSurf (см. вставку на следующей странице) для защиты компьютера во время серфинга, хорошо подойдет программа Sandboxie (*www.sandboxie.com*). При этом установка и настройка, в отличие от VirtualSurf, займет всего несколько минут.

Утилита предназначена для контроля за работой других программ, которые через нее запущены. При этом результаты работы этих программ не влияют на работу системы в целом, а сохраняются в отдельной папке. Таким образом, это ПО собой своеобразный фильтр, в котором задерживаются все изменения, производимые программами. Основная функция Sandboxie — защита и сохранение вашего компьютера в рабочем состоянии, поэтому о защите конфиденциальных данных нужно будет позаботиться отдельно.

Ценность данной утилиты заключается в том, что можно вообще не выполнять ее настройку. Скачали, установили, пользуетесь. Sandboxie создает в меню быстрого запуска и в меню «Пуск» ярлык «Sandboxed Web Browser», который запускает ваш браузер по умолчанию через программу. Это уже будет защищать вашу систему от вирусов, троянских коней и их последствий.

Правда, при настройке по умолчанию защита ваших конфиденциальных данных минимальна. Поэтому сразу же рекомендуется заблокировать для доступа папки и файлы с конфиденциальными данными. Для этого нужно их добавить в список «Blocked Access», который доступен в настройках SandBoxie.



Sandboxie позволяет запускать каждую программу так, что любые изменения в системе сохраняются в ограниченной среде («песочнице») и их можно отменить

5 Дырявое окошко

Браузер поистине может считаться окном в Сеть, через которое не только мы выходим в Интернет, но и могут войти к нам. Сделать это можно, например, атакой на сам браузер с засылкой троянской программы или сбором данных о пользователе (с какой страницы пришел, под каким IP). Кроме того, не забывайте, что все браузеры сохраняют компрометирующие данные о посещенных страницах на жестком диске.

Internet Explorer — до сих пор самый популярный сетевой обозреватель всех времен и народов. Но это же и сделало его самым небезопасным. Практически каждую неделю в нем обнаруживается свежая порция новых «дыр». Но «дыры» — это еще не все. Хуже всего, что IE страдает хроническим недержанием конфиденциальной информации. В первую очередь это относится к кешу и истории. По умолчанию кеш размещается в каталоге *Documents and Settings\user-name\Local Settings\Temporary Internet Files* и, по идее, в любой момент может быть удален по команде. Но не все так просто! Из-за ошибок в системе индексации часть файлов порой просто не удаляется (в чем легко убедиться, заглянув в указанный каталог после его очистки). Туда же попадают и вложения электронной почты при открытии вложений в Outlook Express, причем штатными средствами IE они не удаляются. Самое интересное, что индексный файл index.dat, находящийся в том же подкаталоге, вообще не очищается и продолжает хранить адреса посещенных сайтов.

Решение проблемы состоит в ручном удалении всего содержимого папки Temporary Internet Files, но при этом необходимо выйти из системы и войти под именем другого пользователя, поскольку в противном случае доступ к части файлов будет заблокирован. Кроме того, можно пойти радикальным путем и заменить себе браузер. Например, Internet Explorer 8 и Firefox 3.1 имеют функцию приватного серфинга, удаляя всю информацию о посещенных страницах при выходе.

Универсальная защита

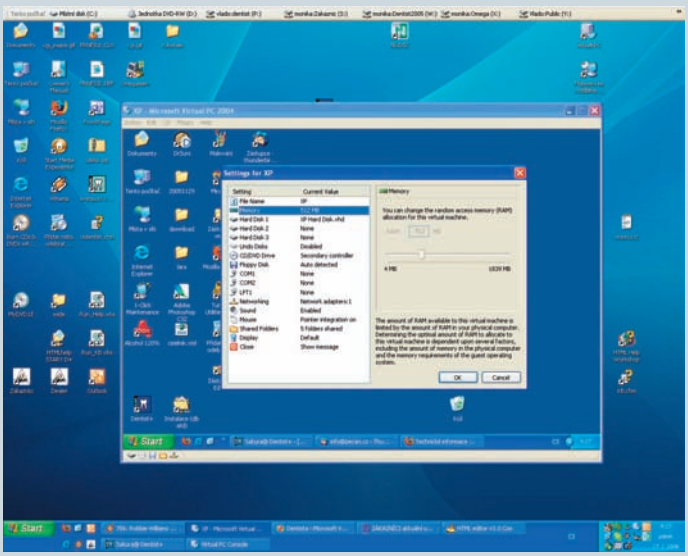
Говорят, что ничего абсолютного в мире нет, однако абсолютную защиту во время серфинга в Сети получить можно. Это обеспечивает технология VirtualSurf. При этом, хотя время настройки равно времени установки Windows + дополнительного ПО, данный метод гарантирует 100 % сохранность данных вашего компьютера и защиту конфиденциальных данных от кражи.

Для этого вам нужно создать виртуальную машину, на которой будут открываться сайты. Виртуальная машина (ВМ) — это программа, которая создает на вашем компьютере еще один компьютер, который запускается в окне программы. Фактически специальное ПО эмулирует аппаратную начинку виртуального ПК, поэтому его настройка ничем не отличается от настройки реального компьютера. Фишка в том, что виртуальный ПК и физический могут не иметь никакой связи. Поэтому при наличии на сайте вредоносного кода последствия его выполнения будут отражаться только на виртуальной машине, не принося вашему компьютеру никакого вреда. А настроив виртуальную машину соответствующим образом, можно избавиться и от этих последствий — при выключении ВМ все изменения будут стираться и возвращаться к первоначальным настройкам, когда никаких вирусов на ВМ еще не было. В безопасности будет и личная информация, которая хранится на компьютере-хозяине и недоступна из ВМ.

Создать и настроить на своем компьютере виртуальную машину совсем несложно. Достаточно скачать бесплатную утилиту VirtualPC от Microsoft (*www.microsoft.com/windows/downloads/virtualpc/default.mspx*). В итоге вы получите инструмент, который позволит вам не бояться кражи личной информации и зловредного ПО.

Настройка ВМ заключается в следующем:

1. Установите эмулятор компьютера (виртуальную машину) VirtualPC.
2. Установите ОС на виртуальную машину и все нужные вам программы (браузеры, антивирус, файрвол и т. д.).



Потратив пару часов на настройку виртуальной машины, вы сэкономите гораздо больше времени на переустановке ОС и программ на своем реальном ПК

3. Разрешите в настройках ВМ доступ к сетевой карте вашего ПК для виртуальной операционной системы.
4. Включите опцию создания дисков отмены (для возврата к изначальным настройкам при повреждении операционной системы зловредным ПО).
5. Настройте сетевое подключение (введите логин, пароль, адрес прокси-сервера и т. д.) и начинайте безопасный серфинг в Сети.

Карты, деньги, два ствола

Инна Иванова, ivanova@hi-tech.ua

Выражение «полный кошелек денег» уже утрачивает свою актуальность. Все больше и больше людей переходят на новое средство оплаты – платежные карты. Издательство «СофтПресс» тоже идет в ногу со временем. Скоро на нашем сайте читатели смогут не только оформить, но и сразу оплатить подписку на любое издание через систему Portmone. В этой связи мы решили рассмотреть тему электронных расчетов подробнее

Фразы при краже кошелька в разное время:

XVIII век: «Сударь, вы украли мой кошелек. Дуэль! Иного выхода нет!»

XX век: «***, как же теперь до получки дожить?!»

XXI век: «Алло, банк? Заблокируйте, пожалуйста, карточки!»

Платежные карты, безусловно, стали частью нашей жизни. Сейчас они есть у всех — от студентов до пенсионеров. И если раньше они служили, в основном, для снятия наличных в банкоматах, то теперь стали равноправным средством оплаты в магазинах, банках, финучереждениях. И это не удивительно. Ведь карты не только защищают ваши деньги от кражи (мошенничество не в счет), но и помогают контролировать счета, регулировать расходы и просто делают жизнь несколько проще.

На лицевой стороне любой платежной карты всегда имеется минимум два логотипа. Один из них принадлежит банку-эмитенту, второй — платежной системе, по которой работает карта. В мире существует четыре международные платежные системы: VISA, MasterCard, Dinners Club, American Express. Первые две являются банковскими, вторые, — соответственно, небанковскими. Разница состоит в том, что за границей карты может эмитировать любая организация, на Украине — лишь та, что обладает лицензией на данную операцию. Иными словами, платежные карты в нашей стране может выпускать только банк. Именно по этой причине Dinners Club и American Express у нас практически не встречаются.

Клуб любителей пообедать

Исторически первой платежной системой была Dinners Club. В 1949 г. ее организовали для сотрудников небезызвестного Empire State Building. Как и сейчас, ни один банк к ней не имел никакого отношения. Плата за обслуживание этих карт тогда не взималась, а кредитная история держателей не исследовалось. Да это и не было нужно, ведь такие кредитки использовались для оплаты обедов в близлежащих ресторанах. Отсюда, собственно, и название. Лишь через несколько лет карты Dinners Club начали принимать магазины, парикмахерские, химчистки и другие торговые площадки. И только через пару десятилетий Dinners Club переплыли океан и попали в Европу. Но к тому времени их обслуживание стало платным (около $3 в год), и если американский потребитель уже привык к новой услуге и готов был за нее платить, то европейцу это все еще было чуждо.Поэтому отдавать $3 непонятно за что он не желал. Dinners Club так и не стала популярной в Старом Свете.

Life takes Visa

На экономных чувствах европейцев в 1958 г. сыграл Bank of America. Он выпустил карту BankAmericard, аналогичную по функциям Dinners Club, но бесплатную. Позже для поддержки данных карт даже была учреждена отдельная компания «BankAmericard Service Corporation». Она занималась не только обслуживанием своих карточек, но и продажей лицензий на их выпуск другим предприятиям. А в 1976 г. впервые появился бренд VISA (Visa International Service Association). Bank of America сразу взял глобальную цель: распространить свои карты не только по Манхеттену, но и по всей Северной Америке вместе с Европой. По прошествии длительного времени цель была достигнута.

Visa Electron, VISA VIRTUAL CARD, Visa Classic, Visa Gold, Visa Platinum. Все они имеют четкую градацию. Visa Electron является наименее престижной, Visa Platinum,соответственно, — наиболее. Зачасую клиент не имеет права выбирать тип карты. Банк-эмитент сам решает, какую карту выдать клиенту в зависимости от его кредитной истории, платежеспособности, продолжительности сотрудничества и т. п.

Visa Electron имеет ряд существенных ограничений. Как правило, она не эмбоссированная. На нее распространяются лимиты по количеству проведенных за день операций. Также она является наименее защищенной и может быть только дебетной. Несмотря на свое название, для интернет-расчетов она не предназначена, но это условие может меняться в зависимости от банка-эмитента. Из преимуществ — дешевизна в обслуживании.

VISA VIRTUAL CARD по функциональности схожа с Visa Electron. Однако физически она не существует. Фактически на руки клиенту выдается только номер карты, ее PIN-код и срок действия. Такая карта не предусматривает возможности пополнения счета, поэтому делают ее для совершения единоразо-

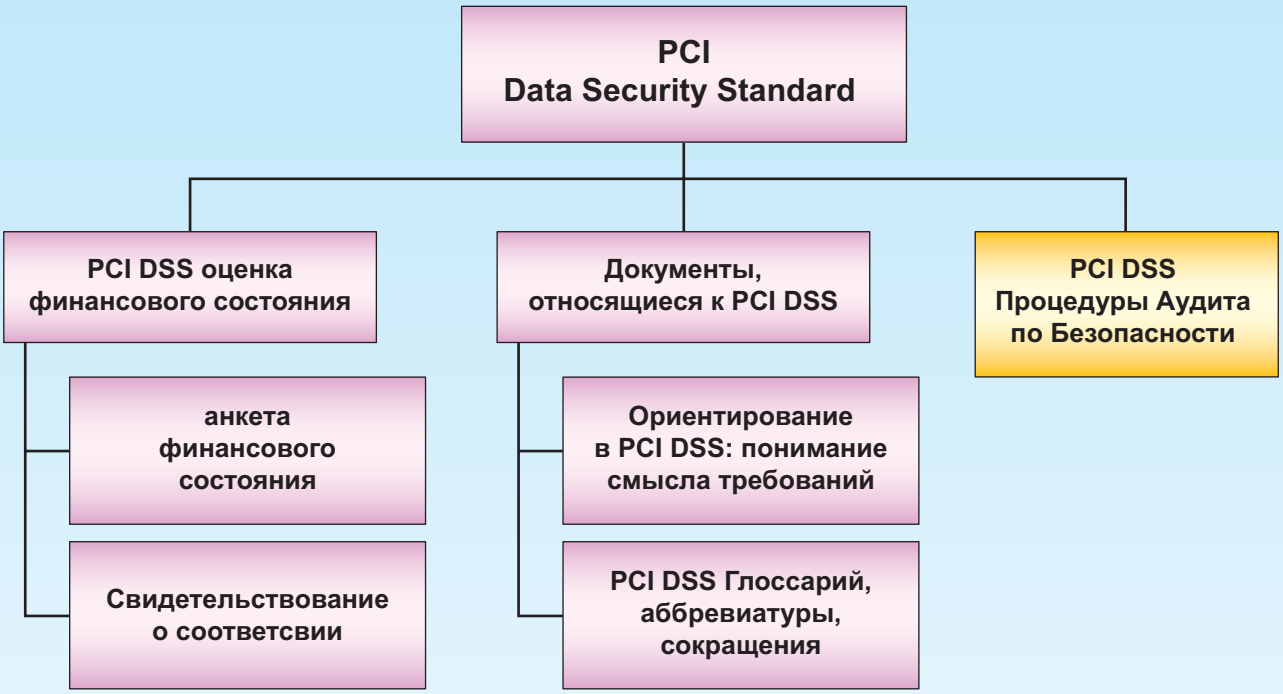
Коротко о VISA

- Основана в 1958 году
- Более 140 млн клиентов
- Листинг на бирже — NYSE: V
- Штаб-квартира в Сан-Франциско, США
- Президент — Кристофер Родригес

Коротко о MasterCard

- Основана в 1966 году
- Более 110 млн клиентов
- Листинг на бирже — NYSE: MA
- Штаб-квартира в Нью-Йорке, США
- Президент MasterCard Europe — Хавьер Перес

Структура стандарта PCI DSS



вой покупки в интернет-магазине с целью обезопасить свои средства.

Visa Classic бывает как дебетной, так и кредитной. Для ее получения необходим постоянный источник дохода, поэтому эта карта говорит о платежеспособности держателя. Обычно она эмбоссированная, но возможны варианты. В обслуживании Visa Classic несколько дороже, но это компенсируется усиленной безопасностью.

Visa Gold, естественно, имеет всю базовую функциональность. Кроме того, с ней намного проще совершать крупные покупки. Выдается она только старым клиентом со значительным остатком на счету. Таким образом Visa Gold свидетельствует о статусе ее обладателя. По данной карте возможно получение скидок в определенных гостиницах, ресторанах, автосалонах.

Visa Platinum является не столько инструментом платежа, сколько статусной вещью, как, например, Bentley или Vertu. По сути, никаких новых возможностей по сравнению с Visa Gold она не предоставляет, помимо более обходительного обращения с ее держателем не только в банке, но и в магазинах, отелях, ресторанах.

Карта от Мастера

В середине 60-х у VISA появился первый и основной конкурент – MasterCard. Компания была основана банковским консорциумом и называлась тогда Interbank Card Association и широко практиковала «захватническую» модель бизнеса. Так, она уже выкупила 100 % акций Cirrus. В результате ей принадлежат такие бренды, как MasterCard, а так же Cirrus и Maestro. Помимо последних двух типов карт компания выпускает еще MasterCard Electronic, MasterCard Unembossed,

Интересно о картах:

- Ребро всегда белого цвета
- Размеры — 54x86x1,26 мм
- При попытке изменить подпись проявляется надпись «VOID», что делает карту недействительной
- В Северной Америке на некоторых картах VISA изображены герои игры The Sims
- 80 % пластиковых карт в Украине — так называемые «зарплатные»

Mastercard Mass (Standard), Mastercard Gold, Mastercard Platinum и MasterCard Virtual.

Maestro и MasterCard Electronic, по сути, являются аналогами. Они наделены базовой функциональностью и дешевы в обслуживании. По этим картам редко проходят интернет-платежи. Однако Maestro принимают в значительно меньшем количестве стран, чем MasterCard Electronic, поэтому отправляясь за границу, поинтересуйтесь этим вопросом.

Mastercard Mass (Standard) уровнем выше, чем Electronic. Для ее получения необходимо предо- ставить больший пакет документов и заверить банк в своей финансовой стабильности. При желании она может работать как в дебетном, так и в кредитном режимах. Подходит такая карта и для расчетов в Интернете.

MasterCard Unembossed практически такая же по функциональности, как и Standard. Единственное отличие в том, что она неперсонифицирована, то есть на ее стороне не обозначено имя держателя. Этот факт может создать проблемы при совершении крупных покупок.

MasterCard Virtual не выпускается физически. Предназначена она исключительно для e-платежей и не предусматривает снятие наличных в банкоматах или расчеты в обычных магазинах.

Mastercard Gold, Mastercard Platinum подчеркивает статус держателя. По функциям они аналогичны Visa Gold и Visa Platinum, соответственно.

Виды платежных карт

На самом деле не так важно, к какой платежной системе относится ваша карта. Намного важнее, какого она типа. Классифицируются карточки по разным принципам. Во-первых, по функциональности различают кредитные и дебетные. Исходя из названий, первые предполагают оформление кредитной линии для клиента и позволяют использовать деньги в пределах определенного кредитного коридора. Вторые же четко ограничивают использование средств в рамках остатка на счету. Дебетные карты легче оформить и они дешевле в обслуживании, зато по сравнению с кредитными, дают меньше возможностей.

Во-вторых, по географической пинадлежности. Существуют двусторонние и многосторонние карты. Двусторонние функционируют в пределах определенной сети торговых точек, контролируемых эмитентом. Многосторонние такого ограничения лишены, однако могут действовать в пределах какого-либо географического региона либо же быть мировыми.

В-третьих, различают карты по способам регистрации. По этому фактору они бывают основанными на бумажной или электронной технологиях. «Бумажные» карты, например, предполагают следующий механизм расчета. При совершении операции держатель ставит свою подпись на счете. Этот документ является подтверждением для банка о согласии клиента провести данную транзакцию. Электронная система напрямую связывается с банком через POS-терминал, а подтверждением транзакции является ввод PIN-кода.

В-четвертых, по технологическим особенностям карты делят на магнитные и оснащенные чипами. И на чип, и на магнитную полосу записывается информация, позволяющая идентифицировать держателя. Однако карты с чипами считаются более защищенными от взлома. Еще одно их важное преимущество в том, что они могут работать без

Сергей Шабашкевич,
начальник службы технической поддержки ЦТП «Доктор Веб»

Защита должна быть комплексной

1. Какие вирусы наиболее опасны при выполнении платежей в Сети? На что необходимо обратить внимание, чтобы не стать жертвой? Как проявляют себя такие вирусы?

Этот тип вредоносного кода называется троянскими конями с функцией кражи паролей. Обычно легитимные веб-ресурсы платежных систем имеют обязательное защищенное соединение (https) для обмена данными между платежной системой и клиентом. Если такого соединения нет, это сигнал остановиться, проверить корректность введенного имени сайта, возможно, проверить компьютер на наличие вирусов. Проявляют себя подобные вирусы генерацией паразитного интернет-трафика.

2. Какие меры безопасности необходимо предпринять при расчетах в Сети? Опасно ли при этом пользоваться коммуникатором, корпоративным ПК?

Нет, пока не опасно, так как количество вирусов под такие устройства на сегодняшний день ничтожно мало. Однако существуют два вида популярных сетевых атак, о которых стоит упомянуть — фишинг (Phishing) и спуфинг (Spoofing).

Фишинг — технология интернет-мошенничества, заключающаяся в краже личных конфиденциальных данных, таких как пароли доступа, данные банковских и идентификационных карт и т. д. При помощи спамерских рассылок или почтовых червей потенциальным жертвам рассылаются подложные письма, якобы от имени легальных организаций, в которых их просят зайти на подделанный преступниками «сайт» такого учреждения и подтвердить пароли, PIN-коды и другую личную информацию, используемую впоследствии злоумышленниками для кражи денег со счета жертвы и в других преступлениях.

Спуфинг — вид сетевой атаки, заключающейся в получении обманным путем доступа в сеть посредством имитации соединения. Используется для обхода систем управления доступом на основе IP-адресов, а также для набирающей сейчас обороты маскировки ложных сайтов под их легальных двойников или просто под законные бизнесы.

При получении подобных писем пользователю лучше связаться с организацией, от которой якобы пришло письмо, и уточнить информацию, о которой идет речь в письме. Ни в коем случае не нужно переходить по ссылкам, содержащимся в такого рода письмах, потому что они ведут на поддельные сайты-двойники легитимных веб-ресурсов. Также рекомендуется использовать альтернативные веб-браузеры, например, Mozilla Firefox или Opera. Ну, и не забываем об эшелонированной обороне.

Константин Здыбель,
ведущий специалист по информационной безопасности компании «БАКОТЕК»

Береженого Бог бережет

1. Какие вирусы наиболее опасны при выполнении платежей в Сети? На что необходимо обратить внимание, чтобы не стать жертвой? Как проявляют себя такие вирусы?

Не стоит ограничиваться при обсуждении только лишь вирусами. Ведь видов вредоносного ПО намного больше: шпионское ПО, трояны, черви, кейлоггеры и т. д. Опасность могут представлять любые из них. Если вы используете какие-либо системы электронных платежей, то одного лишь антивируса для вас будет недостаточно. Обязательно нужно обзавестись антишпионом и полноценным брандмауэром, который будет контролировать открытые порты и приложения, осуществляющие доступ в Интернет. При возникновении несанкционированного соединения с внешним миром этот программный продукт уведомит вас об этом и сможет заблокировать такое соединение.

2. Какие меры безопасности необходимо предпринять при расчетах в Сети? Опасно ли при этом пользоваться коммуникатором, корпоративным ПК?

Как я уже сказал, необходимый минимум в данном случае — антивирус, антишпион и брандмауэр. Для портативных устройств таких решений, к сожалению, очень мало. Поэтому я не рискую производить электронные платежи со своего смартфона. Корпоративный ПК тоже не лучшая возможность для этого, так как вы в любом случае не единственный, кто имеет полный доступ к информации на нем. Как минимум, доменный администратор может получить полное управление над всем, что происходит на любом компьютере в домене. Я не утверждаю, что администраторам нельзя доверять, но береженого бог бережет.

связи с банком, ведь чип содержит в себе еще и динамичную информацию о состоянии счета.

В-пятых, в зависимости от статуса клиента выделяют индивидуальные или корпоративные карты. Их использование существенно ничем не отличается друг от друга. Единственное что, корпоративная карта выдается на руки лицу, уполномоченному использовать финансовые ресурсы организации. А ответственность перед банком за использование этих ресурсов несет организация, но не ее фактический держатель.

Кроме того, карты бывают эмбоссированными и неэмбоссированными. Эмбосирование — выдавливание данных о клиенте и сроках действия карточки на лицевой стороне карточки. Это дает возможность проводить платежи не только с помощью POS-терминалов, но и посредством импринтера — устройства, копирующего номер и другие данные карты. Такой метод не очень распространен в нашей стране.

А гарантии?

В условиях кризиса и без того слабое в нашей стране доверие к электронным расчетам еще больше па-

Алло, банк?...

Те, кто пользуются банковскими картами, рано или поздно сталкиваются с определенными проблемами. Самые распространенные из них мы описали ниже. Журнал «hi-Tech.МИР СВЯЗИ» также дает советы, как действовать в подобных ситуациях.

Карта утеряна

Что ж, случается со всеми и при правильных действиях данная ситуация ничего серьезного за собой не влечет. Как только вы обнаружили пропажу карты важно тут же сообщить об этом в банк-эмитент и заблокировать кредитку. Горячие линии банков должны работать круглосуточно, поэтому не обязательно для совершения данной операции ждать утра или понедельника. Важный момент: если с вашего счета была списана определенная сумма после того, как вы сообщили о пропаже карты, то по правилам эти деньги банк вам должен вернуть.

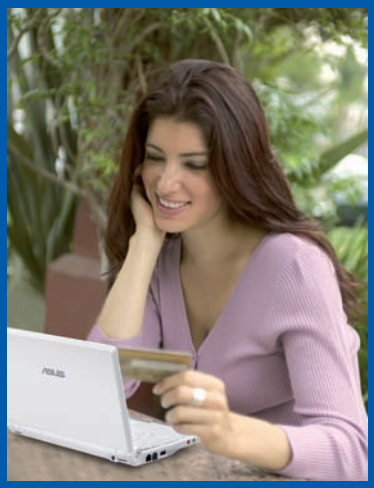
Деньги с карты списаны без ведома держателя

Как показывает практика, это сложный случай и держателю довольно редко удается что-либо доказать. Деньги могут исчезнуть по разным причинам: мошенничество, сбой оборудования, человеческий фактор. Как бы там ни было, первым делом нужно написать заявление в банк-эмитент. И чем скорее, тем лучше, потому что срок подачи заявления может быть ограничен. С этого момента банк-эмитент и банк-эквайер начинают искать виновного. Если банки сами не могут разобраться в ситуации, направляется прямое обращение к платежной системе, к которой принадлежит карта. В некоторых случаях может иметь место даже международный арбитраж. В общем процесс этот долгий и утомительный и еще не факт, что выигрышный.

Банкомат изъял карту

Случается это либо при троекратном неправильном введении PIN-кода, либо, если карту долго не забирали из окошка, ну и, естественно, сбой в работе аппаратуры никто не отменял. В таком случае нужно немедленно позвонить по телефону, указанному на банкомате, даже если последний не принадлежит банку-эмитенту. Обычно изъятые карты возвращают в течении недели. При ее получении нужно иметь при себе документ, удостоверяющий личность. Если на счету внушительная сумма денег, не лишним будет заблокировать карточку.

Случись такая ситуация за границей. проблема несколько усложняется. Вы можете обратиться непосредственно в банк, банкомат которого «съел» кредитку, либо же связаться с «родным» банком, и тот уже сам будет разбираться с иностранным партнером. Третий вариант — связаться с сервисным центром платежной системы. У Visa она называется Global Customer Assistance Service (GCAS), у MasterCard — MasterCard Global Service (MCGS).



На всякий случай, следует всегда помнить, что в крупных банках существует услуга экстренной выдачи наличных. Процедура не дешевая, но в кризисной ситуации может пригодиться.

Банкомат не принимает карту

Эта проблема чаще технического характера. За исключением довольно редких случаев, когда банкомат просто не работает с той платежной системой, к которой принадлежит карта. Чаще же бывает просто повреждена или размагничена магнитная полоса. При низких температурах сам банкомат также может выйти из строя.

Банкомат не выдал денег или выдал меньше

Ситуация, как и многие ей подобные, сложно доказуемая. При данных обстоятельствах вам нужно сохранить чек, который выдал банкомат, записать номинал выданных банкнот и их номера. Желательно привлечь еще двух свидетелей. Затем отправляйтесь в ближайшее отделение банка и пишите там заявлении в двух экземплярах. На вашей копии сотрудник банка обязательно должен сделать пометку о получении обращения. Разбирательство может длиться до трех месяцев, а по его итогам банк обязан в письменной форме сообщить вам о своем решении.

Банкомат втянул деньги обратно

Такое случается, если деньги не были забраны в течение минуты. Сумма списана, а кошелек от этого не пополнился. Этот случай напоминает предыдущий, с той лишь разницей, что здесь доказать свою правоту легче. Порядок действий аналогичен. Но банк прежде всего проверит остаток в банкомате. Именно по этой причине процедура возврата вам денег существенно укорачивается.

Ну и последняя ремарка. Во многих странах банкоматы работают с шестизначными PIN-кодами. Естественно, у украинской карты такового быть не может. Но это не означает, что вы не можете снимать наличные за пределами своей страны. Нужно просто дополнить имеющийся у вас пароль двумя нулями.

дает. В такой ситуации особенно важным для банков и других коммерческих структур становится вопрос безопасности. И важным инструментом в этом плане является стандарт PCI DSS (Payment Card Industry Data Security Standard). Это международный стандарт безопасности в области платежной индустрии, поддерживаемый такими структурами, как Visa International, MasterCard Worldwide, American Express, и др. Он определяет процедуры проведения платежных операций как на стороне процессора, так и на стороне торговца-ретэйлера. Стандарт регламентирует получение, передачу, хранение и обработку информации о кредитных картах. Его целью является достижение максимального уровня безопастности при всех операциях связанных с кредитными картами. PCI DSS поддерживается и развивается независимой международной огранизацией – PCI Security Standards Council. Все торговцы в свою очередь обязаны придерживаться стандарта PCI в своих операциях с кредитными картами.

Решение о создании единого стандарта было принято компаниями Visa и MasterCard в связи с увеличением числа компаний, сообщивших о потерях и кражах конфиденциальной информации со счетов их клиентов.

PCI DSS – это единый стандарт безопасности данных картообладателя. Он поддерживается всеми карточными системами, основан на специфических программах защиты данных (Visa CISP, MasterCard SDP и т. д.), устанавливает единый стандарт защиты хранения, передачи, и обработки карточных данных. Основным преимуществом стандарта PCI DSS и отличием его от ранее существовавших документов является четкая структуризация и прозрачность, что существенно облегчает внедрение описанных в нем требований.

Nota Bene о безопасности

Недавние исследования американских ученых подтвердили беззащитность информационных данных. Так, количество утечек информации в американских компаниях увеличилось на 47%, что указывает на проблемную ситуацию в обеспечении информационной безопасности. Как сообщила организация Identity Theft Resource Center (ITRC), в большинстве случаев похищенная информация была незащищена паролем или не зашифрована.

С захлестнувшей страну волной краж персональных данных, правительство Китая решило бороться по-новому. В связи с этим был предложен новый законопроект, согласно которому виновные в незаконном доступе к информации будут лишены свободы сроком на 7 лет.

Я всегда буду рядом

Инна Иванова, ivanova@hi-tech.ua

Нетбуки воистину претендуют на роль спутника жизни. Легкие и компактные, они помещаются даже в дамскую сумочку. Однако, их функциональность пока еще оставляет желать лучшего. Но путем небольших финансовых вложений, ее можно несколько повысить

Нетбуки, конечно, нельзя назвать полноценными заменителями традиционных лэптопов, но в удобстве использования им не откажешь. Правда, в угоду малому весу и скромным габаритам приходится жертвовать рядом существенных характеристик. Минимизировать, а то и вовсе избавиться от этого недостатка можно с помощью дополнительных устройств, подключаемых к нему.

Для проекта мы выбрали нетбук MSI Wind U100 по нескольким причинам. Во-первых, покопавшись на специализированных форумах, мы обнаружили, что именно эта модель удостоилась наибольшего количества хвалебных отзывов, да и в наших тестах (см. hi-Tech PRO №10/2008) он показал неплохие результаты. Во-вторых, Wind U100 предлагает отличное сочетание цена/качество. Кроме того, в нем большой объем жесткого диска – минимум 120 ГБ, что не может не радовать.

Разумеется, не обошлось и без минусов. Например, с первых дней использования устройства остро ощущается нехватка оптического привода. Весь цинизм ситуации проявляется еще и в том, что ПО к устройству поставляется именно на дисках :). Производитель решил эту проблему выпуском внешнего привода MSI WIND DRIVE.

Второго, чего нам не хватило в Wind U100, это звука. Естественно, в нетбуке имеется встроенная акустика, но честно говоря, проку от нее, как от заячей шубы в летний день. Поэтому рекомендуем сразу же обзавестись миниатюрными колонками. К примеру, подойдут SVEN PS-30. Их мощности, конечно, не хватит

Нетбук

MSI Wind U100

Легкий и компактный нетбук за приемлемые деньги. Технические характеристики: объем оперативной памяти – 1024 МБ, жесткий диск – мин.120 ГБ, процессор – Intel Atom N270, масса – 1,1 кг, размеры – 260x180x19–31,5 мм.

Цена: 4100 грн

Привод

MSI WIND DRIVE

Корпус устройства выполнен из анодированного алюминия. Оно может прожигать не только CD–, но и DVD–диски, в том числе и двухслойные. Для первых скорость записи составляет до 24x, для вторых – до 8x. Дополнительного питания не требуется – привод получает энергию от ноутбука.

Цена: 470 грн

Колонки

SVEN PS-30

Для питания акустика не нуждается в дополнительной розетке, а черпает энергию через USB-порт. Колонки, мощностью 2 Вт каждая, стены, конечно, не сотрясают, но звучат весьма прилично.

Цена: 80 грн

ТВ–тюнер

MSI VOX USB2.0 TV BOX

Тюнер, как и подобает мобильному устройству, достаточно маленьких габаритов — 100x60x9,5 мм. Разрешение видео — 720x480 пикс. В комплекте поставляется пульт дистанционного управления. Подключается к лэптопу через USB 2.0.

Цена: скоро в продаже

Батарея

MSI Wind U100 4400mAh 11.1V

Решает проблему со слабой комплектационной батареей U100. Она работает в два раза дольше, чем штатный аккумулятор. Емкость — 4400 мАч, напряжение — 1,1 В, количество элементов — 6.

Цена: 1300 грн

Мышь

A4–Tech 2X Mini Optical Mouse MOP–59D

Миниатюрная оптическая мышка — 23x15,9x7,1 мм — очень удобна в дороге и не занимает много места. Разрешение — 800 dpi, подключается как через USB, так и через PS/2-вход (переходник в комплекте). Прорезиненные прокладки по бокам корпуса делают работу с устройством комфортной.

Цена: 130 грн

Модем

ZTE MF622

Комплект «Київстар. Мобільний Інтернет» можно купить в любой специализированной точке. Работает такой модем и в 2G- и в 3G-сетях, поддерживая технологии GPRS и EDGE, а также UMTS. Скорость соединения — до 7,2 Мбит/с на вход и до 3,1 Мбит/с — на выход.

Цена: 749 грн

В ПРОЕКТЕ ИСПОЛЬЗОВАНЫ:

Нетбук MSI Wind U100	4100 грн
Привод MSI WIND DRIVE	470 грн
Колонки SVEN PS-30	80 грн
ТВ-тюнер MSI VOX USB2.0 TV BOX	скоро в продаже
Мышь A4-Tech 2X Mini Optical Mouse MOP-59D	130 грн
Батарея MSI Wind U100 4400mAh 11.1V	1300 грн
Модем ZTE MF622	749 грн
Итого:	**6898+ грн**

для домашней вечеринки, но с комфортом посмотреть фильм вполне возможно.

Не помешает также и ТВ-тюнер. Нетбук, безусловно, рабочий инструмент, но делу — время, а потехе — час. Развлекаться тоже иногда не помешает. Особенно это актуально в дороге или поездках, скажем, в горы, ведь в местных гостиницах не всегда есть телевизоры, а с другими способами вечернего времяпрепровождения там и вовсе сложно.

В комплекте с MSI Wind U100, к сожалению, нет мыши. Тачпадом пользоваться, конечно, можно, но удобными такие операции не назовешь. Мы предлагаем миниатюрное решение от A4-Tech — MOP-59D. Разнообразие цветов позволит подобрать манипулятор в тон к основному устройству. Напомним, что MSI Wind U100 также выпускается в нескольких цветовых решениях.

Слабым местом нашего нетбука является батарея. Даже при достаточно экономном использовании она может продержаться едва ли два часа. Нивелировать этот недостаток можно, купив более емкий элемент питания. В Украине в продаже мы нашли аккумулятор на 4400 мАч, это при том, что «штатник» ровно вдвое меньше.

И наконец, чтобы добавить мобильности нашему проекту, мы решили подключить к нему Интернет. Естественно, о проводном варианте речь даже не шла. Wi-Fi, несомненно, всем хорош, но под концепцию «всегда и везде» не подходит. Из доступных альтернатив мы остановились на предложении от «Киевстара». Основным преимуществом данного комплекта является то, что для его использования не нужно подписывать контрактов. Получить такую Сеть не сложнее, чем новый мобильный номер. Нужно просто купить «Київстар. Мобільний Інтернет». Однако, стоит оговориться, что в данный набор входит SIM-карта, позволяющая подключаться только к 2G-Интернету. Чтобы перейти на Сеть третьего поколения, придется отдельно покупать специальную карту.

СОВЕТЫ УМЕЛЫХ

в этом выпуске:

- Как сделать поиск в Google более точным
- Как сделать автоответчик из ПК
- Как настроить Интернет под Virtual Machine

Как сделать поиск Google более точным

Мало кто знает, но поисковик Google имеет довольно много дополнительных параметров, повышающих точность поиска. Google позволяет вам искать определенные типы файлов. При этом определенными являются файлы *.xls, *.doc, *.pdf, *.ps, *.ppt и *.rtf. Для поиска файлов этих типов введите в строку поиска следующее: Filetype:xls для Excel-файлов или filetype:doc для Word-файлов.

Другой полезный параметр поиска – inurl: опция, которая позволяет искать некоторые слова в URL. Это дает пользователю возможность искать определенные каталоги/папки, особенно в комбинации с index of-опциями. Пример: inurl:film, в результате которой вы получите ссылки, имеющие слово "film" в URL.

Опция index of, о которой не особенно думали создатели Google, оказывается, очень удобна. Если вы используете index of-строку, то найдете списки каталогов определенных папок на серверах. Пример: «index of» film или «index.of.film».

Опция Site позволяет вам получать результаты, которые только принадлежат некоторому домену или определенному сайту. Например, можно искать .com сайты или .box.sk сайты или .nl сайты. Пример строки для поиска: Site:mil или site:gov.

Intitle – другая хорошая опция. Она позволяет вам искать HTML-файлы, имеющие некоторое слово или слова в заголовке. Формат intitle:wordhere.

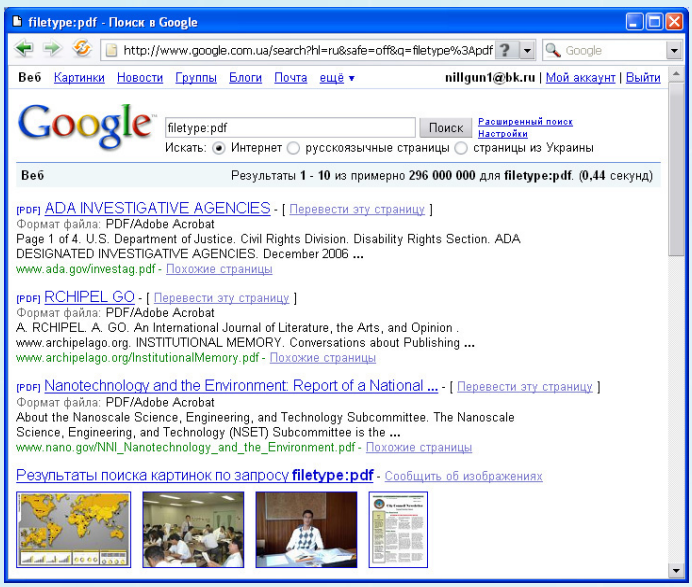
Для получения еще более точных результатов параметры поиска можно компоновать. К примеру, можно пробовать эту строку для поиска: inurl:nasa.gov filetype:xls «restricted» or this one: site:mil filetype:xls «password»

Валентин КАРПЕНКО

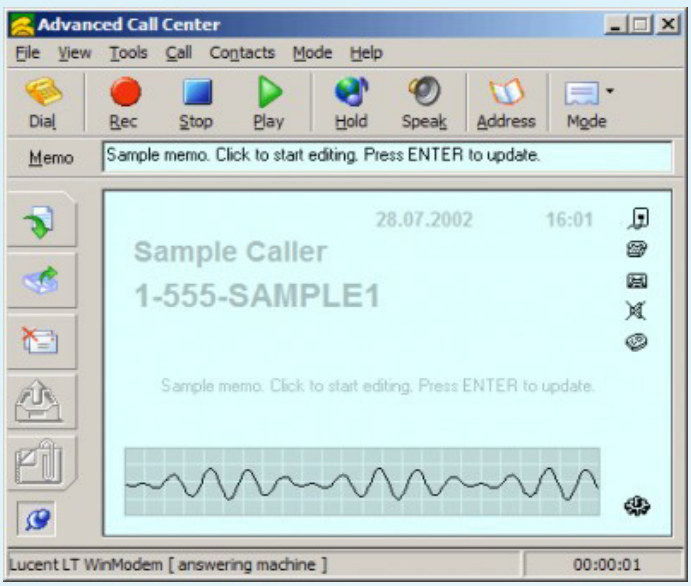
Как сделать автоответчик из ПК

Когда вы уезжаете в отпуск или командировку, бывает, что на домашнем автоответчике скапливается масса неотвеченных сообщений. В таком случае можно научить компьютер выполнять роль оператора на телефоне. Для этого его нужно превратить в автоответчик. Все, что от него потребуется, – поднять трубку, проговорить заранее записанное приветствие и записывать последующее сообщение в файл (wav или mp3), по окончании повесить трубку. Далее записанный файл можно отправить по e-mail или записать на файловый сервер, сделав его доступным для удаленного прослушивания. Либо просто переадресовать сам звонок на заранее установленный номер.

В таком случае может подойти программа Advanced Call Center (*www.voicecallcentral.com/rus/advancedcallcenter.htm*). Фактически Advanced Call Center – электронный секретарь, обладающий функцией автоответчика с автоматическим определением номера. Программа позволяет использовать имеющиеся аппа-



Для более точного поиска введите требуемые параметры запроса в строку поисковика



Advanced Call Center превратит ваш ПК в персонального электронного секретаря

ратные средства для определения номера телефона вызывающего абонента, либо осуществлять программное определение номера, используя возможности, предоставляемые модемами с поддержкой голосовых функций (voice modems). Кроме того, в программу встроена записная книжка, режимы громкой связи и одностороннего прослушивания линии через колонки, подключенные к звуковой плате. Вам лишь остается запустить программу — и автоответчик из ПК готов!

Роман КОШЕВОЙ

Как настроить Интернет под Virtual Machine

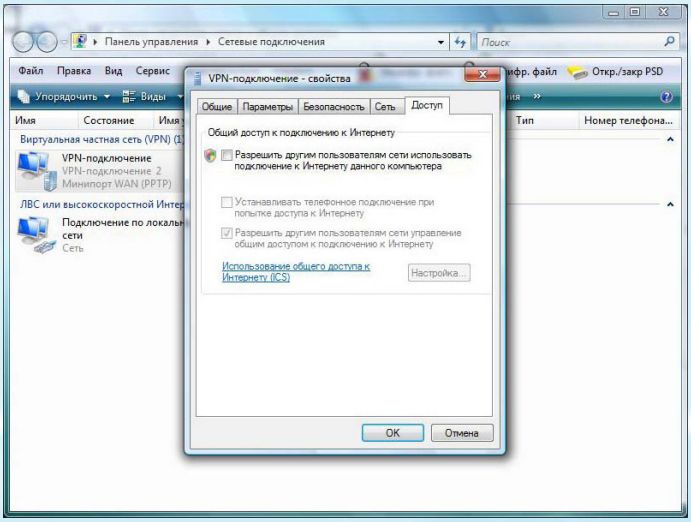
■ Очень часто для экспериментов над операционной системой ПК (установки сомнительных программ, модификации реестра и т. д.), а также безопасного серфинга в Интернете пользователи ставят Virtual Machine (VMware, виртуальная машина). Благодаря тому, что гостевая ОС на виртуальной машине не имеет никакой связи, кроме выделенных вами каналов, с реальным ПК, ваша основная ОС останется неповрежденной даже в случае вирусной атаки. Однако в VMware просто настроить локальную сеть, а вот с настройкой Интернета у многих возникают проблемы. Решить ее можно двумя способами: прямое соединение и VPN.

При прямом соединении процесс настройки самый простой: на хост-машине (реальном ПК) настраивается доступ в Интернет, а гостевая машина (виртуальный ПК) будет подключаться как будто по локальной сети. Единственный минус при этом — обе ОС имеют доступ в Сеть одновременно, причем гостевая машина зависит от хозяина.

Гораздо удобней, когда у вас VPN-подключение, тогда и реальное, и виртуальное подключения будут независимыми.

Сделать это можно так:

1. зайдите в VMware в настройки сетевых соединений (*settings-hardware-ethernet*) и отметьте галочками пункты *connected* и *connected at power on*.



Подключение виртуальной ОС через VPN позволит сделать ее независимой от интернет-соединения реального ПК

2. В Network Connection выставьте флаг в положение *Custom: VMnet0 (default bridget)*.

3. Далее на реальной машине в сетевых подключениях для локальной сети откройте свойства, выберите *VMware Bridge Protocol* и вновь нажмите Свойства.

4. Настройте VPN также, как и на реальном ПК.

Примечание: если у вас лишь один IP-адрес, то Интернет на гостевой машине будет работать лишь после выключения VPN на хост ПК. Однако если взять у провайдера дополнительный IP-адрес, виртуальная машина будет полностью независима от ПК-хозяина.

Евгений ДМИТРУК

"Магнолія - ТВ" представляє:
телеканал надзвичайних новин

Бачити щоб жити

Тільки для людей з міцними нервами! -Подробиці на сайті
www.magnolia-tv.com

Якщо Ви ще не бачите телеканал "ЧП.INFO",
зверніться до кабельного оператора Вашого міста