Магия ПК

О сложном просто и понятно

#10 (87)

октябрь 2005

Издательство "Техно-Пресс", Санкт-Петербург

- Безопасность с позиции силы
- Твой скорострельный шотган
- Windows XP: ядерная война
- Осторожно, злая@

Мой компьютер — моя крепость

№ 10(87)
октябрь 2005

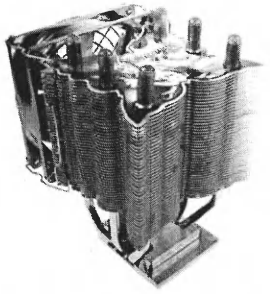
E-mail: mpc@tp.spb.ru
http://www.magicpc.spb.ru

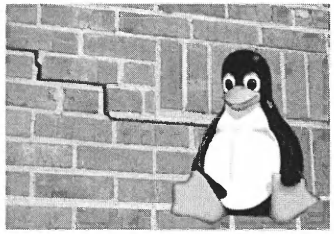
Подписной индекс 29961
по каталогу "Роспечать"

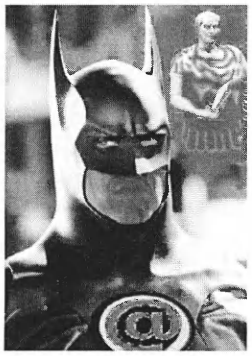
Журнал для любителей компьютеров

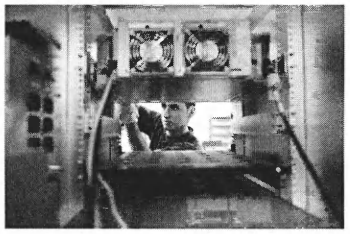
Поддержку сайта осуществляет "ПетерХост"

МАГИЯ ПК









КОМПЬЮТЕРЫ

ПЕРИФЕРИЯ

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

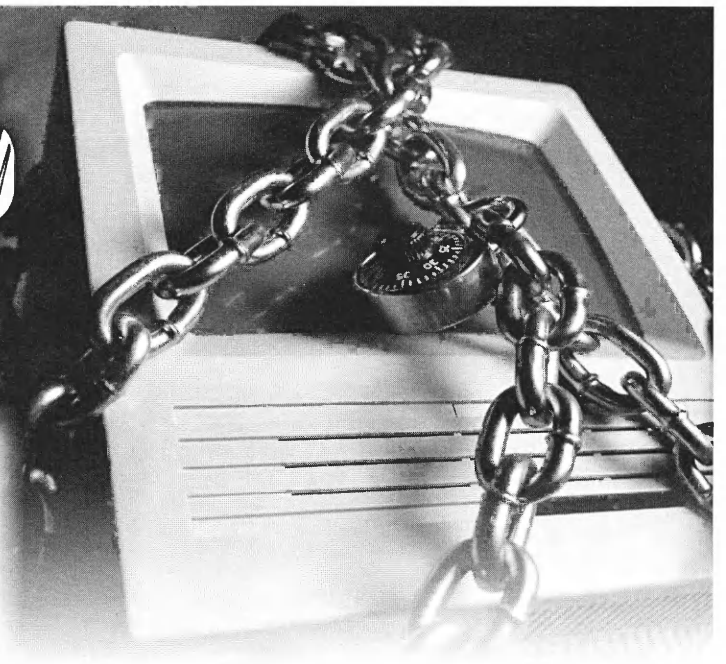
ИНТЕРНЕТ

МУЗЫКАЛЬНЫЙ ПК

КОМПЛИТ

HOMO COMPUTERUS

Безопасность с позиции силы



Анатолий Ковалевский (С.-Петербург)

«Тот, кто ради безопасности готов пожертвовать свободой, не достоин ни безопасности, ни свободы»

Бенджамин Франклин

Эта статья посвящена программно-аппаратным средствам безопасности, которые активно продвигают гиганты компьютерного рынка. Для начала продолжим разговор, начатый в статье «Asta la Vista, Windows!» прошлого номера. Речь пойдет о связанных с ней средствах безопасности.

Windows Vista основывается на трех главных компонентах:

Windows Communication Foundation — так теперь будет называться архитектура веб-сервисов и коммуникаций (ранее Indigo). В состав опытной версии ОС входит Internet Explorer 7beta, который включает браузинг во вкладках, возможность просматривать информацию через Really Simple Syndication (RSS), а перед открытием сайта, замеченного в фишинге, IE 7 будет отображать предупредительное сообщение с рекомендацией «не продолжать работу».

Windows Presentation Foundation — так теперь будет называться подсистема обработки графики и представления данных (ранее Avalon). Вопрос о наличии виджетов (widget), реализованных в Mac OS X Tiger или в программе Aston для Windows, пока остается открытым. Виджеты — это часы, блокнот, словарь и другие программы или функции, которые можно поместить на рабочий стол в полупрозрачном слое. Хотя «прозрачные» окна и меню оставлены.

Windows Future Storage — объектная файловая система, позволяющая легко группировать документы всех видов по разным категориям, таким как имя автора или содержание. По предварительным данным, максимум, что будет реализовано, — это продвинутый локальный поисковик MSN Search и, возможно, WinFS не как часть файловой системы, а как служба ОС.

Куда более значительные изменения предполагаются в сфере безопасности. Microsoft постепенно превращает программу Windows Genuine Advantage по проверке подлинности кода Windows при загрузке обновлений из добровольной в принудительную. Исключение будет сделано лишь для загрузки секьюрити-патчей и обновления для Windows AntiSpyware, которая будет предоставляться бесплатно. Но если бы этим все и ограничилось, то было бы не так печально. Уже обнародованные данные о том, какой вид примет Windows Vista, позволяют понять, почему Microsoft четыре года писала и переписывала Longhorn, но так и не реализовала толком даже WinFS, о которой Билл Гейтс мечтает со времен Windws NT.

А пока представим, что мы сидим за компьютером с Windows Vista и пытаемся проинсталлировать некую программу. Появляются следующие окна:

«А вы уверены в происхождении программы Y/N?»

«Точно уверены Y/N?»

«Предупреждаю, инсталляция будет вестись только в тестовом режиме Y/N?»

«Вы уверены, что вы уверены, что точно хотите открыть этот подозрительный файл Y/N?»

«Последний раз предупреждаю, вы поняли, что это предупреждение последнее Y/N?»

«Программа устанавливаться не будет, еще раз попробуете — запрещу доступ к ПК!»

Конечно, диалог несколько утрирован, но общая суть именно такова. Дело в том, что еще три года назад был учрежден Trusted Computing Platform Alliance, в который входило 5 членов-учредителей — AMD, Hewlett-Packard, IBM, Intel и Microsoft. Через какое-то время к альянсу присоединились еще 10 фирм — Nokia, Phoenix, Sony, Amtel, Infineon, National Semiconductor, Philips, ST Microelectronics, VeriSign и Wave Systems. В длинном перечне разработанных ими технологий — LaGrande (Intel), PadLock Data Encryption (VIA), Core Managed Environment (Phoenix), Palladium (Microsoft), EmBASSY (Wave+AMD) и т. д. Все эти разработки являются закрытыми и направлены на обеспечение безопасности, а главными являются технология обеспечения безопасной среды обработки данных Microsoft's Next Generation Secure Computing Base (она же Palladium) и LaGrande от Intel. Рассмотрим их подробнее.

Palladium

Palladium — технология, названная в честь вооруженного божества греков, которое охраняло безопасность города. По замыслу разработчиков, она должна охранять тайну персональной информации, шифровать данные и электронную переписку, противостоять пиратству (ограничивать доступ к хранящимся в собственном компьютере данным при нарушении лицензионных и других условий), упрощать контроль за своим компьютером, блокировать злонамеренный код (спам, трояны, черви, прочие вирусы), позволять контролировать движение информации даже за пределами ПК пользователя. В результате, если вспомнить греческую мифологию, то скорее приходит на ум другое божество — Мом, бог насмешки (было у него прозвище — «правдивый ложью»), чьи мудрые советы пагубны для того, кто им следовал. И кончил этот бог плохо — с Олимпа его прогнали. Однако 2005 год н. э. — совсем не 2005 год до н. э. А жаль.

Palladium состоит из двух главных частей. Первая — аппаратная, со средствами шифрования и энергонезависимой памятью. Вторая — программная, она надстраивается над аппаратной и содержит два ключевых элемента: Nexus (элемент ядра-системы, управляющий ядром ОС) и Trusted agents (агенты на доверии — программы и сервисы, запускаемые в пространстве, сформированном Nexus). В результате отгораживает часть оперативной памяти с конфиденциальными данными, и для их получения требуется ключ. Ключ хранится в аппаратном виде, поэтому для работы Palladium на системную плату всех компьютеров будет интегрироваться специальная микросхема, а впоследствии, скорее всего, она окажется внутри процессора или чипсета. И без нее работа материнской платы будет просто невозможна. По мнению экспертов, в недалеком будущем это будет одна из самых сложных комплектующих современного ПК — чип будет иметь собственный процессор, защищенную память, блок шифрования, защищенные часы, подсистему ввода-вывода и, главное, — возможность влиять на работу ОС на всех уровнях.

А какие же наиболее уязвимые места сегодняшних компьютеров? Их много — данные на дисках (надо шифровать и ограничивать доступ), устройства ввода (запретить перехват), устройства вывода (запретить доступ к информации из видеопамяти любому приложению), оперативная память (разграничить доступ). Поэтому для полноценной работы Palladium нынешние устройства (процессоры, чипсеты, клавиатуры, мышки и т. д.) совершенно не подходят.

В результате у Windows Vista появится возможность автоматически определять, совместима аппаратная часть с Palladium или нет, а весь софт будет разделен на программы первого сорта, у которых будет доступ к контенту, и программы второго сорта, не имеющие такого доступа. Таким образом будет реализована давняя мечта Microsoft — заставить всех применять только лицензионное ПО.

LaGrande

LaGrande — также программно-аппаратная защита. Вышедшие уже достаточно давно процессоры P4 Prescott имели встроенную поддержку LaGrande, только не активированную.

Необходимо понимать, что Palladium и LaGrande — это по сути одна и та же технология, только с приоритетом программного или аппаратного начала. Эти технологии могут существенно повысить защиту ПК, но в случае злоупотреблений такая модификация аппаратуры и ПО способна причинить еще больше вреда. Дело в том, что проприетарные программы и раньше выполняли подозрительные функции, а теперь подобная практика станет постоянной. Получается, что цель так называемой благонадежной вычислительной техники — защитить данные не от хакеров, а от пользователей. Главная задача технологии — контроль за цифровыми правами над контентом даже в том случае, если он находится на чьем-то ПК. Например, веб-сайт, торгующий музыкой, прежде чем позволить посетителю загружать песни, сможет определить, оборудован ли его ПК средствами защиты авторских прав.

В целом эффект от систем защиты нового поколения будет заметен только когда число ПК с Palladium/LaGrande ПК достигнет 100 миллионов.

ДНК компьютера

Но и это еще не все изменения. Помните, что делает BIOS? Произносит низкоуровневые магические заклинания, пересчитывает имеющиеся железки (многие из которых имеют собственный BIOS) из числа комплектующих на материнской плате и передает управление загрузочному сектору ОС (на дискете, винчестере или CD). И все. Таким образом, так же, как ДНК является основой клетки, BIOS является основой ПК. Правда, со временем, подстраиваясь под новые технологии, по конструкции BIOS из прямолинейного превратился в «миску спагетти». И спагетти решили не распутывать, а поступить с ними «по-македонски».

ДНК? Да. В англоязычной транскрипции это будет звучать как DNA (DeoxyriboNucleic Aacid — дезоксирибонуклеиновая кислота). А в компьютерах это будет озвучено как Device-Networked Architecture (объектно-сетевая архитектура), которая создается в рамках «надежных вычислений» (trustworthy computing). Именно последний вариант продвигает Phoenix, чьи BIOS`ы за четвертьвековую историю установлены уже в более чем миллиарде компьютеров. Архитектура будет называться CME (Core Management Environment, доверенная оболочка, управляющая ядром), а сами продукты — CSS (Core System Software, программное ядро системы) и будут состоять из трех частей:

1) CSP (Cryptographic Service Provider) — криптографический механизм, который не позволит неавторизованному (на уровне BIOS) пользователю извлечь информацию из компьютера (например, украденного ноутбука), запрещая дублирование цифровых сертификатов для ОС (сюда вошли компоненты, связанные с Windows и приложениями .Net через Microsoft CryptoAPI).

2) DRM (Digital Rights Management) — цифровые права, через взаимодействие с Windows обеспечат ограничение на копирование мультимедиа, автоматическую идентификацию при входе в сеть.

3) Размещение «VIP»-программ — тех, что обеспечивают восстановление ОС после сбоя, работу базовой части антивируса, выполнение авторизации пользователя.

Честно говоря, столь запутанное построение наглядно демонстрирует, что огромное количество терминов и их периодическая замена на новые «маркетинговые инициативы» говорят скорее не о сложности проекта, а о желании скрыть за терминологией его суть.

Не отстает и Intel, которая два года назад начала продвигать EFI (Extensible Firmware Interface, расширенный программно-аппаратный интерфейс, зашитый в ПЗУ).

Но какова же цель всех этих телодвижений? Она проста — превратить BIOS в маленькую ОС, которая в состоянии загружать с диска Windows, устанавливать связь по сети, регулировать доступ к критически важным файлам и на основании встроенного интерпретатора может выполнять дополнительные программные модули, встроенные в EFI. BIOS = ОС? Но это уже было. У ZX-Spectrum операционная система была защита в ПЗУ и грузилась, что называется, путем включения в розетку. В старых компьютерах от Apple это называлось Toolbox (включая QuickDraw) и было зашито в ПЗУ, хотя ОС грузилось с диска. Более того, это уже есть — КПК (все эти Palm, Sony и в какой-то степени WMS 2003), где ОС зашита в ПЗУ, а в основной памяти болтаются только патчи, софт и тому подобное. В некоторых серверах Hewlett-Packard и Sun SPARC имеет место аналог BIOS — OpenBoot (но там есть свои нюансы — у этих ОС нет загрузочного сектора и т. д.). Цель всех этих BIOS-подобных ОС в ПЗУ — удаленное управление. Что-то не соответствует сути домашнего компьютера.

Между тем Intel утверждает, что это положит конец необходимости писать отдельные драйверы низкого уровня... По меньшей мере странно. Даже Intel не выпускает один вид материнской платы. А это означает, что в любом случае будут специфические драйверы для работы с железом. Просто драйверы из ядра ОС переносят в BIOS, а для ОС показывают уже как унифицированное стандартное устройство. И этому есть подтверждение — выпускается среда разработки Platform Innovation Framework (ранее Tiano), которая позволяет производителям железа писать программные модули к новой BIOS, аналогичные драйверам Windows.

На троих сообразим?

Таким образом, получается, что все это затеяно для одной цели — постепенно изъять из Windows понятие устройства, прежде всего на уровне драйвера. DRM будет направлена на то, чтобы нельзя было смотреть нелицензионные кино/музыку, обходить DVD-региональную защиту, создавать виртуальные оптические диски и звуковые карты. Хотя в каком-то смысле ничего нового — уже сейчас можно загрузить компьютер с USB-флэшки, если материнская плата выпущена в последние 2-3 года. В результате любая система — EFI от Intel или CSS от Phoenix — дает их обладателю шанс установить проприетарный контроль над ПК через BIOS. Это шаг назад. В первом ПК, изготовленном IBM в 1981-1982 годах, все — от последней гайки до операционной системы (IBM PC-DOS) было изготовлено IBM. За исключением 8068 процессора от Intel. Так бы и дальше продолжалось, если бы Compaq не удалось путем обратного реинжиниринга создать свою версию BIOS, которая при полной совместимости не нарушала ни один из патентов. Только после этого начался взрывной рост числа ПК. Сегодняшняя ситуация отличается лишь тем, что рынок под себя собрался подмять не один монополист, а два — Wintel (Microsoft + Intel), которые могут и на троих (с Phoenix) не «соображать», вполне своими силами обойдутся.

С появлением нового поколения BIOS появится жесткая персонификация данных (за что так ратует Евгений Касперский), к тому же установить ОС с болванки со сборником софта за $2 уже не получится. С другой стороны, рынок ответит выпуском мод-чипов и софтверных взломов, как это было для приставки X-box или PlayStation. Точнее, уже ответил. Уже есть сайты, где можно заказать нужное «лекарство» к программе — patch, crack или keygen. Появился даже trial-кряк: тебе дают crack, а чтобы снять ограничение в его работе, надо заплатить автору. При этом идут разборки даже между крякерами — мол, у этих не покупайте, они продадут, но никакой помощью не обеспечат, если заглючит; а мы в течение 2 месяцев гарантируем поддержку, вплоть до возврата денег. Предположим, программа стоит $200, триальный кряк —$20. Далее, надо думать, выпустят кряк на этот кряк, который будет стоить $2, и так по нисходящей... но это уже другая история.

А пока Intel встраивает поддержку EFI в свои чипсеты и лицензирует ее структуру третьим сторонам, Microsoft отрабатывает совместимость с EFI в Vista. Возможно, что уже в этом году мы увидим первые платы, где EFI будет предлагаться в качестве альтернативы BIOS. Первые EFI-компьютеры появились у Gateway (модель Gateway 610 Media Center), а потом и в некоторых моделях материнских плат. Нечто похожее, но совместимое лишь с самим собой, выпускает IBM в линейке ноутбуков. Кстати, именно Голубой Гигант был одним из заказчиком Core System Software от Phoenix, так что на примере их ноутбуков можно увидеть, что представляет собой эта концепция.

Так что же, новый BIOS, — хорошо или плохо? Теоретически ОС должна быстрее грузиться за счет более грамотно реализованного plug&play. Однако хочется напомнить, что при включении ПК BIOS из микросхемы ПЗУ (ROM) копируется в так называемую «теневую область» оперативной памяти (RAM), потому как доступ к оперативной памяти осуществляется значительно быстрее, чем к ROM. А теперь представим, что BIOS увеличился с 2 Мбайт до 20 или даже до 100. Процесс становится куда более длительным, да как-то и не хочется отдавать под BIOS 100 Мбайт RAM. Неужели мощь процессора стало некуда девать? И вряд ли со всей этой кучей диагностических, антивирусных и прочих модулей ОС будет загружаться быстрее, чем сегодня. Наконец, любой программист знает, что чем больше количество программного кода, тем больше в нем глюков. И чип будет стоить денег, а значит, конечная продукция будет дорожать.

Безопасность или свобода?

До пользователей, к великому сожалению, даже не доходит, что ущемляют их права — права на получение и распространение информации. Защита ПО, восстановление ОС, антивирус — и все это из BIOS... Если говорить кратко и жестко — задача BIOS запустить компьютер и исчезнуть. Все! С остальным вполне справится ОС. А те, кто встраивают в BIOS кучу дополнительного ПО, заботятся прежде всего о недопущении в компьютер конкурентов. Поддержка других ОС (той же Linux) настолько громогласно обещается, что в это уже с трудом верится. По крайней мере, в реальную поддержку. Всем, кто не входит в союз Microsoft-Intel-Phoenix, придется переписывать все драйверы к своему железу. У законодателя мод (Microsoft) останется в рукаве парочка меченых козырей — сертифицированные драйверы будут работать быстрее, приоритет в работе программ будет отдаваться «своим» продуктам. Под ОС уже почти автоматически подразумевается Windows, потому что технологические спецификации EFI разрабатывались именно с учетом и в опоре на Microsoft. Intel (и AMD) могут придумать какую-нибудь хитрость, благодаря которой новые процессоры смогут дружить лишь с новыми ОС.

Уже сейчас, если на ПК с лицензионной Windows записать CD с 74 минутами тишины в майкрософтовском монопольном wma-формате, то выяснится поразительная вещь — прослушать тишину смогу лишь я, она защищена лицензией. Вам кажется это мелочью? А вы попробуйте сделать скриншот экрана, когда фильм проигрывается в Windows Media Player 10. Кроме черного пятна вы ничего не увидите. В Билле Гейтсе многое привлекает, в частности, его редкостная техническая прозорливость. Прямо Жюль Верн какой-то. Но вот все остальное... Война с IBM и Digital Research за ОС, потом с Netscape за браузер, боевые действия за среды разработки с Borland и Sun, засады на OpenGL и DEC Alpha... Хотелось бы относиться с уважением, но не получается. Император Веспасиан, введя налог на пользование туалетами, заметил, что «деньги не пахнут». Но это отнюдь не относится к их хозяевам.

Нас пытаются уверить, что новая BIOS позволит защитить программы внутри от удаления или изменения, по недосмотру или злому умыслу. Хм... Давайте лучше вспомним, как вирус WinCHIH тысячами уничтожал BIOSы, и без всяких Next Generation Secure Base... А это уже будет настоящий Клондайк для вирусописателей: базовая часть вируса хранится в защищенном сегменте BIOSa (с помощью этого самого DRM), а другая часть «снаружи» — внутри ОС. И кто такой WinCHIH-2 сможет убить? Думаете, что вирус в компьютер не попадет? Попадет — вспомните об «универсальных драйверах для подключаемых к материнской плате устройств» — вполне очевидно, что их придется регулярно обновлять, а это означает, что переключатель read-only для флэш-памяти будет перенесен куда-нибудь в ОС и обычным пользователем будет по умолчанию открыт на запись. Со всеми вытекающими.

Вполне могут появиться компьютеры only for Win compatible. Поэтому добиться совместимости можно будет только путем применения мод-чипов. В этом случае компьютер станет обычным утюгом, который можно вернуть/обменять по гарантии. Не важно, какая начинка у вашего компьютера. Пользователь «по определению» — это «чайник», он ничего не должен знать/менять/исправлять, на это есть сервис-центр. В общем, компьютер низводится до уровня бытовой электроники, разве что с расширенным программным управлением. Конечно, посложней холодильника — слишком много личной информации в нем хранится.

А если необходимо управление по сети, то его организовать легче легкого — еще пять лет назад, в сентябре 2000 года, компания Elegent Technologies представила etBIOS. От обычного его отличало наличие встроенного браузера. В 256 Кбайт кода внутри энергонезависимой памяти удалось умесить программу, поддерживающую основные Интернет-протоколы (PPP, TCP/IP, HTTP, SSL) и форматы (html, jpg, gif) и не требующую наличия на ПК винчестера.

Безопасность с Back-door

Так будет ли защищен компьютер благодаря Palladium/LaGrande, Device-Networked Architecture BIOS и иже с ними (например, iAMT — технология, которая позволяет работать с компьютером не только в случае его вирусного заражения, но даже если неисправен сам винчестер)?

Если бы... Американская компания Codex Data Systems выпускает для правительства США один интересный продукт — DIRT (Data Interception by Remote Transmission). Это ПО в полном соответствии с названием (dirt переводится как грязь, отбросы) занимается удаленным перехватом данных, и в руках спецслужб стало мощным средством для слежки за удаленным компьютером, работающим под ОС Windows (и даже управления им). Что-то типа трояна Back Orifice, только работающего по принципу рут-кита и в нулевом цикле, поэтому легко маскируется в системе и обходит защитные программы, в том числе файерволы. За три года использования американскими спецслужбами никто так и не отловил эту шпионскую программу.

А в Израиле из-за нее недавно был серьезный скандал, в результате которого в отставку подали несколько министров, а главы трех крупнейших детективных агентств и бывший министр внутренних дел попали под следствие. А раскрыли программу только потому, что произошла утечка с компьютера одного деятеля, писавшего автобиографию. И только целенаправленный поиск на его компьютере специалистами из отдела информационной безопасности позволил найти трояна.

Может быть, именно поэтому Китай создает свои процессоры — Godson, Gou-Sheng. Пусть они гораздо медленнее интеловских, зато в них гарантированно отсутствуют лишние включения, да и работать эти процессоры будут не под Windows.

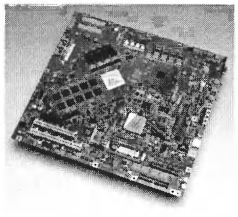
Hard-news

Процессоры Cell пойдут в массы

Представление высокопроизводительного процессора Cell, состоявшееся в этом году, ныне дополнено весомым шагом для переноса его на компьютеры — разработан прототип материнской платы для ПК с этим процессором.

Ожидается, что распространение процессора на ПК начнется в марте-апреле 2006 года, когда монопольные производители (Sony, IBM и Toshiba, разработавшие проект Cell и унифицированную технологию его производства) представят свои новинки, такие как PlayStation-3, но уже в апреле триумвират намерен начать льготное лицензирование разработки для всех изготовителей материнских плат и сборщиков ПК. Таким образом, компьютеры на базе Cell могут появиться в массовом порядке к концу 2006 года. Производство Cell будет освоено одновременно в Японии и США.

На первой материнской плате для Cell (разработка Toshiba) использовано специализированное чипсет-обрамление, оптимизированное для обслуживания процессорных и периферийных запросов (A/V, I/O, Digital Audio & Vidio, 1394 и пр.). Для снижения энергозатрат в состав платы введен чип-оптимизатор, осуществляющий мониторинг активности узлов платы и погружающий неиспользуемые узлы в состояние «глубокого сна». Предполагаемое снижение энергозатрат — 50% от пиковых показателей.



В стартовой версии материнская плата будет обеспечена поддержкой операционных сред Linux и ITRON с соответствующими приложениями. Благодаря реализации ВИРТУАЛЬНОЙ МАШИНЫ на ней будут корректно исполняться пакеты, обладающие кроссплатформенной совместимостью.

Для привлечения разработчиков ПО в состав пакета сопровождения программистов войдет Eclipse — интегрированная среда разработки приложений, ориентированная на создание не только стандартного офисного ПО, но и редакторов Real-Time Audio & Video, включая поддержку записи и трансляции телевизионных и сетевых развлекательных программ.

INTEL идет в народ

По данным исследования Всемирного банка, в настоящее время в 64 тысячах российских средних школ установлено 85 тысяч персональных компьютеров, то есть один ПК в среднем приходится на 50 учащихся (в большинстве стран Европы — семь школьников на компьютер). К Интернету, как следует из публикаций российских газет, подсоединено менее 20% российских школ, причем даже в московских школах компьютеры используются, в основном, лишь на уроках информатики (для сравнения: в Эстонии цифровые ресурсы поддерживают 70% школьных программ, а в Голландии — до 90%). В результате только 55% выпускников российских школ умеют работать на ПК, а из учащихся ПТУ им пользуются не более 16%.

Налицо также заметный разрыв в уровне компьютерной оснащенности школ между столицей и российской «глубинкой». По данным, полученным в ходе реализации программы Intel «Обучение для будущего», в Москве ПК есть в 47% школ, тогда как в других больших городах РФ этот показатель вдвое ниже (22%), не говоря уж о малых городах (17%) и селах (6%).

Поставив себе цель уменьшить масштабы всех этих диспропорций, корпорация Intel объявила о начале программы под названием «Открытый урок Intel». В ходе пилотного проекта, который пройдет в сентябре-октябре этого года в Волгограде, Воронеже, Краснодаре, Нижнем Новгороде, Ростове-на-Дону и Саратове, как минимум 2000 преподавателей и 40000 учащихся 180 российских школ будут ознакомлены с моделями использования современных компьютерных технологий в образовании.

1500 Мбайт в секунду

Специалисты Европейского центра ядерных исследований (CERN), используя кластер высокопроизводительных систем, успешно решили ряд научных задач в ходе работ по созданию большого адронного коллайдера (Large Hadron Collider, LHC). Этот ускоритель частиц, длина окружности которого составляет 27 км, будет введен в строй в 2007 году и станет самым крупным инструментом ядерных исследований в мире.

Специалисты CERN убедились, что кластер на базе процессоров Intel Itanium 2 может экспортировать данные в глобальную сеть других лабораторий центра на протяжении 10 дней с рекордной скоростью, составляющей в среднем 600 Мбайт/с. Итоговая производительность вычислительной системы LHC Computing Grid должна будет обеспечить на протяжении 10 дней передачу данных со скоростью 1500 Мбайт/с в более чем 150 вычислительных центров всего мира. Данные, представляющие собой изображения результатов соударения протонов, летящих навстречу друг другу почти со скоростью света, будут анализироваться тысячами ядерных физиков, которые стремятся обнаружить новые частицы и явления, способные предоставить более точную информацию о происхождении Вселенной.

Гран-при среди роботов-автомобилей

В США начался чемпионат среди роботизированных автомобилей. Выигравший гонку получит приз от Пентагона — 2 млн долларов.

Участники должны преодолеть по пустыне 150 миль и прийти к пункту назначения в местечке Примм, штат Невада.

В прошлом году никто из участвующих машин не выиграл приз в 1 млн долларов. Самое большое расстояние, полторы мили, удалось преодолеть модернизированному Humvee (университет Carnegie Mellon). В нынешней гонке будут участвовать 43 роботизированных автомобиля. Чемпионат начнется в конце сентября — начале октября.

Только 20 машин примут участие в финале, который состоится 8 октября. Машины должны будут пройти маршрут с препятствиями без вмешательства человека. Местоположение и направление они будут определять с помощью системы глобального спутникового позиционирования, различных сенсоров, лазеров, радаров и камер.

Чемпионат является частью глобальной программы Пентагона по оснащению армии на треть роботизированными устройствами, которое должно осуществиться к 2015 году.

Монитор с защитой от посторонних глаз

В Mitsubishi Electric Research Laboratories ведутся работы по созданию монитора, изображение на котором можно увидеть, только если смотреть прямо на него.

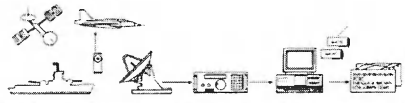
К тому же изображение на экране периодически меняется на прямое и инверсированное с частотой 20 Гц. Нужное изображение доступно для просмотра с помощью специального драйвера и очков с ферроэлектрическим затвором. Эти очки выбирают неинверсированное изображение для просмотра, а посторонним в это время доступно лишь инверсированное изображение в виде мерцающего серого фона. Теоретически можно будет выводить на общую систему отображения информацию, адресованную для просмотра определенным лицам.

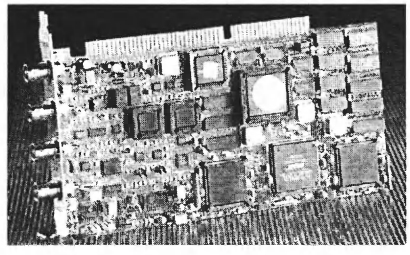
Такой дисплей найдет применение в банках, больницах, аэропортах и других местах, где необходима защита отображаемой на экране информации от посторонних.

«Перехватчик» эфирных коммуникаций

Немецкая компания Wavecom Electronik AG приступила к выпуску процессорных анализаторов, способных в автоматическом режиме осуществлять перехват, предварительный анализ и дешифровку сигналов в каналах эфирного и спутникового вещания (факсы, телетайп, голосовая связь, в частности — роуминг в сетях сотовой связи). При невозможности «раскрыть» сигнал до уровня информационной составляющей она будет «складироваться» на серверах специальной распределенной сети для ручной обработки.

Программно-аппаратная часть «перехватчика» умещается на стандартной печатной плате, которую легко интегрировать в состав персоналки и/или распределенной вычислительной сети, а размер приемной параболической антенны вовсе не будет столь уж велик.





С внедрением системы госслужбы и силовые ведомства смогут осуществлять тотальный контроль за информационными потоками, если только данные не будут шифроваться с использованием тяжелых криптопакетов.

Виртуальный шлем для солдат. И спасателей

В США создан мобильный командный центр M2C2 и специальные модули для морских пехотинцев. M2C2 обеспечивает бойцов радио- и спутниковой связью с поддержкой видеоконференций, а также передачи видео и секретной информации. Новая технология включает в себя широкий канал связи для передачи цифровых данных, использует лазеры, способна транслировать видео, текст, голоса и текстовые приказы. Естественно, все каналы связи надежно шифруются. По словам специалистов, в сравнении с той системой, что использовалась недавно в Ираке, M2C2 далеко впереди.

Если для связи обычными средствами приходится останавливать войска, то новинка позволит отдавать приказы на ходу, что снижает риск для солдат и позволяет экономить время. К тому же командиры смогут получать оперативную информацию прямо с видеокамер, установленных в оборудовании пехотинцев.

В разработке проекта стоимостью 8 млн долларов самым сложным было обеспечить спутниковую связь во время движения: при движении транспортного средства даже небольшая выбоина на дороге может оборвать связь.

M2C2 может использоваться не только военными, но и спасателями, например, при проведении широкомасштабных операций при стихийных бедствиях.

Работы с M2C2 продолжатся, на вторую стадию проекта уже выделено 20 млн долларов. К этому времени устройство приобретет вид шлема VR.

AMD стремится в космос

Официальные лица AMD на Embedded Systems Conference заявили, что программа разработки и выпуска экономичных процессоров в семействе 64 бит AMD-64-Longevity начнется в четвертом квартале 2005 года и будет поддерживаться, как минимум, на протяжении следующих пяти лет.

Заявление было дополнено представлением очередного дуэта мобильных 64-битных процессоров Themis с экстремально низким уровнем энергопотребления. Themis традиционно поддерживает инструкции 32 и 64 бит, что снижает издержки при создании управляющих узлов со встроенным «интеллектом». Практической нишей для процессоров Themis, по мнению руководства компании, станет бортовая авто- и авиатехника (включая космическую и военную).

Чудо-ноутбук

На сайте компании Atom Chip Corp. помещено описание прототипа ноутбука, впечатляющего своими техническими характеристиками: процессор работает на частоте 6,8 ГГц, объем оперативной памяти составляет 1

Тбайт, а постоянной — 2 Тбайт. В подсистемах памяти используется энергонезависимая квантово-оптическая синхронная память, которая характеризуется большой плотностью хранения данных и высокой скоростью работы. В качестве оперативной памяти используется энергонезависимая оптоэлектронная память с произвольным доступом (non-volatile integrated optoelectronic Random Access Memory, NvIOpRAM). Она обеспечивает плотность хранения 3,2 Гбайт на один кубический миллиметр. В основе работы NvIOpRAM лежит магнитный квантово-оптический эффект в пористом кремнии (эффект Гендлина). Скорость записи новой памяти — 6 Гбайт/с, чтения — 8 Гбайт/с.

Процессор AtomChip Quantum II работает на частоте 6,8 ГГц, оснащен 256 Мбайт встроенной памяти и имеет очень низкое энергопотребление. Конфигурация прототипа включает 12,1 WXGA-дисплей (1280x 800, 16:10), 1,3-Мп CMOS-камеру, два интегрированных графических контроллера Intel855GME, DVD-накопитель, Bluetooth, Wi-Fi (802.11aBink+/g), GPRS, 10/100 Base-T LAN, MDC Fax/Modem V.90/V.92. Батарея из 6 li-ion элементов обеспечивает работу в течение 8 часов. Компьютер рассчитан на работу под управлением Microsoft Windows XP Professional или Linux.

Atom Chip обещала продемонстрировать ноутбук в работе на январской выставке CES 2006. В качестве ценового ориентира компания указывает диапазон $8500-15000.

Голографический носитель бьет рекорд плотности записи данных

Компания Inphase разработала новую технологию многоуровневого хранения данных на оптическом носителе, благодаря чему увеличила плотность записи данных до 31 Гбит/см^2, то есть почти в три раза.

Прототип носителя и привода был продемонстрирован компаниям Hitachi, Sony, Sanyo, Toshiba, Samsung, Matsushita, IBM, HP на конференции IBC в Амстердаме. Пока еще «сырой» прототип привода Tapestry от Inphase при емкости носителя 300 Гбайт показал среднюю скоростьчтения/записи данных на уровне 20 Мбайт/с. Носитель в специальном защитном картридже имеет формат 5,25 дюйма.

Предполагается, что уже осенью

Keyboard mobile...

Складывается впечатление, что такая простая и скромная деталь компьютера, как клавиатура, вызывает сегодня не меньший интерес изобретателей, чем perpetuum mobile в средние века.

Новая эргономичная клавиатура от Microsoft

Microsoft готовит к выпуску новое поколение эргономичных клавиатур и мышек. Клавиатура Natural Ergonomic Keyboard-4000 имеет традиционный «излом» поля клавиш, которые не только разделены на два массива (под каждую руку), но и повернуты на определенный угол так, чтобы обеспечить идеальное соответствие ориентации пальцев.

Для облегчения работ с текстами в состав клавиатуры введена клавиша «лупы», добавлена также клавиша ускоренного вызова мультимедийных проигрывателей, калькулятора и IE (последняя — с функцией поиска текста, выделенного в документе).

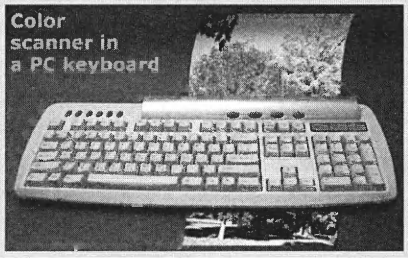
Мыши представлены дуэтом Wireless Laser Mouse 6000 и Wireless Optical Mouse 5000, основное достоинство которых — высокая точность позиционирования курсора (соответствует разрешению 800 dpi).

Клавиатура-сканер

Компания KeyScan решила «скрестить» обычную клавиатуру и сканер (возможности последнего достаточны для качественной оцифровки тестовых документов формата A4 и цветных фотографий).

По мнению разработчиков, их гибрид в ближайшие год-два станет стандартной составной частью домашнего и офисного компьютера.

Встроенный в клавиатуру сканер



имеет аппаратное разрешение 600 dpi, поддерживает лишь режимы сканирования «на отражение». Глубина оцифровки базового набора RGB-цветов — 48 бит.

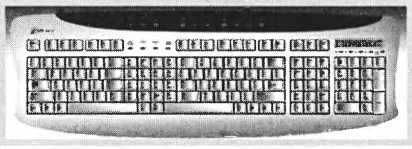
Дополнительным преимуществом композитной клавиатуры является интерфейс USB, через который получает питание сканер, что удешевляет конструкцию.

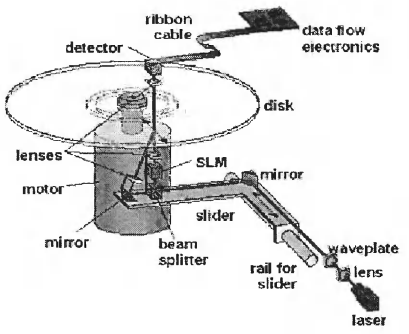
Управлять сканером можно как в автоматическом режиме (он начинает работать, когда пользователь вводит очередной лист в приемный лоток), так и в ручном, для чего в клавиатуру встроены 6 дополнительных кнопок.

Стоимость новинки — порядка $100.

Клавиатура AdapTex: ввод с предсказанием

Речь идет о том, чтобы предугадать, какой следующий символ собирается ввести пользователь. Конструкторы компании KeyPoint Technologies (KPT) решили оснастить стандартную





2006 года появятся носители емкостью 800 и 1600 Гбайт, а к 2008 году — емкостью от 2 до 20 Гбайт при габаритах менее почтовой марки.

Сменный носитель нового диска представляет собой двухкомпозитный полимер, заключенный между двумя карбонатными слоями покрытия. Внутренний объем секретного полимерного диска используется для записи (и перезаписи) трехмерного образа данных (голографической картины), которые хранятся специально отформатированными блоками. Благодаря подключению ТРЕТЬЕГО ИЗМЕРЕНИЯ достигается компрессия данных без потери информации.

«Подушка безопасности» для ноутбука

IBM начинает оснащать свои ноутбуки ThinkPad «подушкой безопасности» APS (Active Protection System). В полной аналогии с автомобильной подушкой безопасности устройство имеет датчик ускорения, при срабатывании которого (в момент падения ноутбука) произойдет экстренная припарковка головок винчестера с сохранением всех данных.

Пароли мешают жить

Компания RSA Security подготовила доклад о паролях, основанный на опросе 1700 корпоративных пользователей США. Вывод таков: пароли неудобны, раздражают и путают пользователей. Девять из десяти опрошенных считают систему парольного доступа неудобной. Системные администраторы заставляют пользователей либо часто менять пароли, либо использовать труднозапоминаемые. Все это толкает их на рискованное поведение (например, хранение важных документов на КПК), которое может подорвать безопасность.

Кроме того, элементарная забывчивость ведет к перегрузке служб поддержки, которые вынуждены удалять старые пароли и принимать новые.

QWERTY-клавиатуру функцией ввода с предсказанием, знакомой многим по мобильным телефонам.

Клавиатура KPT AdapTex разделена на две секции и дополнена вспомогательными блоками клавиш, ускоряющими ввод с предсказанием. По мере работы она приспосабливается к контексту, существенно повышая качество предсказания (и скорость ввода). Чтобы принять оптимальное для пользователя состояние, клавиатура динамически перепрограммирует раскладку в ходе работы. Как утверждает разработчик, распознавание построено на анализе документов и учитывает словарный запас, характерные обороты речи и тематическую направленность, характерные для конкретного пользователя. В результате, если верить KPT, производительность труда повышается на 150%, снижается число ударов по клавишам.

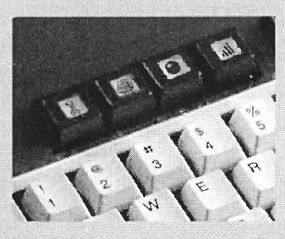
Еще одна ЖК-клавиатура

В прошлом номере мы уже рассказали о подобной клавиатуре (дизайн Optimus студии Лебедева). Ныне компания United Keys (обладающая патентом на клавиатуру с экранами, установленными в клавишах), представила клавиатуру 205PRO, программируемые клавиши которой оборудованы небольшими монохромными ЖК-дисплеями разрешением 20 x 20 точек.

Модель поддерживает интерфейс USB 2.0 и поставляется вместе с приложениями Icon Editor и Image Converter, предназначенными для редактирования изображений на клавишах и конвертирования стандартных иконок в картинки "клавишного" формата.

Изменение изображений в клавишах возможно тремя способами. Во-первых, можно создать свое собственное изображение. Это удобно, например, если пользователь закрепляет за клавишей какую-то макрокоманду.

Во-вторых, разработчики сайтов смогут включать в страницы специальный код, который будет менять изображения на клавишах согласно намерениям дизайнера на то время, пока пользователь находится на сайте. Это облегчит навигацию и ускорит доступ к ресурсам сайта.

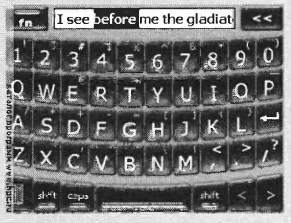


Наконец, наличие бесплатно распространяемого API позволит разработчикам ПО создавать и динамически загружать изображения в ходе работы программ.

Пока экранами оснащены только функциональные клавиши. Приобрести United Keys 205PRO можно будет за $299,99, либо по специальной «семейной» цене за $199,99.Начало продаж намечено на первый квартал 2006 года.

Печать на КПК — пальцами

Компания Spb Software House выпустила новую версию программы Spb Full Screen Keyboard, которая существенно облегчает процесс набора объемных текстов. Под виртуальную клавиатуру теперь отведено все экранное пространство КПК. При этом размеры клавиш позволяют печатать, не прибегая к помощи стилуса, то есть привычным образом — пальцами.



В новой версии Spb Full Screen Keyboard заявлена поддержка ОС Windows Mobile 5.0, устройств с различными типами экранов (QVGA, VGA, 240x240), а также ландшафтного и портретного режимов ориентации.

Есть функция автоматического исправления, автозаполнения и интеграции с различными приложениями. На данный момент доступны английская, немецкая и французская версии. Русская, испанская и итальянская будут представлены чуть позже.

КРИПТОГРАФИЯ
ДВЕ СТОРОНЫ МЕДАЛИ

Сергей Бычков (С.-Петербург)

Подобно вековому соревнованию снаряда и брони по сей день продолжается соревнование создателей криптоалгоритмов и тех, кто пытается их взломать. Попробуем взглянуть на проблему с обеих сторон.

Шифрование

Основой для развития в России электронного документооборота по Интернету может стать криптография и AAA (аутентификация, авторизация и администрирование). Но не все здесь безоблачно.

На государственном уровне

Повсеместному внедрению электронного документооборота в России сегодня препятствует существование межведомственных барьеров. Возникшие в этой области проблемы являются следствием принятия ведомственной модели. Системы безопасности и шифрования для получения сертификации обязаны обладать «черным входом». Этому ведомству (я думаю, ясно, какому) законодательством РФ предписан технический контроль за трафиком и пользователями Интернета.

По мнению большинства пользователей Интернета, развитию электронного документооборота в России будет способствовать создание вневедомственных национальных алгоритмов шифрования, модели которых не будут известны ни одному ведомству. Прежде чем подобные программные продукты будут доступны для широкого круга пользователей, Минсвязи должно принять ряд подзаконных актов. Судя по тому как идет процесс подготовки этих документов, соответствующие программы появятся не скоро.

Между тем продолжается поддержка правительственными структурами иностранных программных продуктов шифрования, реализованных на американских алгоритмах шифрования. Модели этих алгоритмов всем известны и не представляют особой сложности для дешифровки. Поучителен в этом отношении опыт китайских чиновников. По указу правительства Китая, начиная с 1 июня 2004 года все оборудование беспроводных локальных сетей, продаваемое в стране, должно удовлетворять разработанному в Китае стандарту шифрования и аутентификации национальной разработки WAPI, Wired Authentication and Privacy Infrastructure (B15629.11-2003).

Американские производители оборудования WLAN не могут получить об этом стандарте никаких сведений — китайское правительство разрешает обмениваться спецификациями технологии только национальным компаниям. Американский специалист по защите информации и шифрованию Брюс Шнейер сообщил, что не знаком с китайским стандартом, но, поскольку американские разработки в области безопасности и шифрования WLAN «все как одна оказались провальными», он готов рекомендовать Западу взять на вооружение китайскую технологию, если та хорошо себя зарекомендует.

Шрифты в мэйлерах

При использования шрифтов в мэйлерах может возникнуть несколько проблем. Текст в мэйлере представлен кодировкой, где каждому знаку присваивается некоторое число — его код. Первая из них заключается в гармонии кодировки у отправителя и получателя. Все современные таблицы кодировок происходят от возникшей еще в 60-е годы 7-разрядной таблицы ASCII (American Standard Code for Information Interchange). При 7-разрядном кодировании каждому символу сопоставляется 7 бит, то есть число в диапазоне от 0 до 127.

Получатель и отправитель должны общаться в одной кодировке, то есть мэйлер должен «понимать» то, что ему посылает отправитель. Для этого отправителю нужно установить систему, которая умеет посылать сообщение о том, в какой кодировке будет получателю прислано сообщение. Мэйлер получателя должен принять и настроиться на правильное отображение сообщения.

Однако в России очень распространен способ, при котором мэйлер автоматически определяет, в какой кодировке приходит сообщение от клиента, и выдает страничку уже перекодированной.

Бурное развитие в последние годы гипертекстовых способов представления информации в мэйлерах обострили существующую уже более десятилетия проблему представления и работу с кириллической информацией в электронном виде. Это связано, в первую очередь, как с отсутствием стандарта на расширенную кодовую таблицу ASCII, включающую кодировку кириллических символов, так и с разнообразием решений, предлагаемых различными коммерческими компаниями. Стандартизирована только половина таблицы ASCII, а именно — первые 128 символов, которые включают в себя буквы латинского алфавита. И с ними никогда не бывает проблем. Вторая же половина таблицы (а всего в ней 256 символов) отдана под национальные символы, и в каждой стране эта часть различна. Например, в России существует около 10 различных кодировок, то есть одному и тому же символу соответствует разный цифровой код, и если мы неправильно определим кодировку текста, то получим абсолютно нечитаемый текст.

Международный стандарт ISO/IEC 8859-1 стал в наши дни заменой для ASCII. В нем первые 32 кода, числа 128-159, соответствуют почти неиспользуемым управляющим символам, общим для всех таблиц кодировки ISO. Хотя 8859-1 может использоваться для текстов почти на всех западноевропейских языках, он не полностью покрывает нужды французского и финского. Этот недостаток, а также отсутствие знака для новой общеевропейской валюты привели в 1999 году к возникновению кодировки 8859-15, в которой использована новая редакция значений кодов 8859-1.

Что же касается кириллицы, то на сегодня существует пять базовых таблиц кодировки русских букв.

Для использования с операционной системой MS DOS была разработана кодовая таблица CP-866 (IBM/Microsoft). Она основана на альтернативной кодировке ГОСТ и создана специально для ОС MS-DOS, в которой используются символы псевдографики. Сегодня эта кодировка так же непопулярна, как и MS-DOS. Для использования в операционной среде Windows используется кодовая таблица CP-1251 (Microsoft). Кодовая страница 1251 для Microsoft Windows стала популярной благодаря огромному влиянию фирмы Mirosoft на рынок компьютерных технологий.

Кроме того, в ней отсутствует ненужная в графических средах поддержка символов псевдографики. Сегодня эта кодовая таблица в России является основной. Кодовая страница 10007 используется на компьютерах Macintosh и по своему набору знаков почти совпадает с CP1251.

В UNIX-среде наиболее распространена кодовая таблица KOI8-R. Это одна из стандартных кодировок русского языка, принятых еще в Советском Союзе на заре развития вычислительной техники. KOI расшифровывается как «код обмена информацией». Цифра 8 обозначает, что этот код 8-разрядный (в отличие от KOI-7, широко применявшегося на советских вычислительных машинах). В настоящее время KOI8-R является одной из основных русскоязычных кодировок в операционных системах Unix. Это вторая по популярности кодировка после CP-1251. Кодировка поддерживает символы псевдографики, занимающие около половины всех кодов. В 1993 году таблица стандартизирована в Интернете.

Международный стандарт ISO определяет для России кодовую таблицу ISO 8859-5. Псевдографика отсутствует. В настоящий момент эта кодировка практически не применяется, хотя и поддерживается во всех мэйлерах.

История развития шифрования

Под шифрованием в мэйлерах имеется в виду преобразование открытого текста в закрытый посредством применения определенных правил (алгоритмов) и некоторых данных (обычно разного рода символов, к примеру, букв и чисел), известных под названием ключа и специфичных для конкретного сообщения. Расшифровать закрытое послание может тот, кто знает алгоритм и ключ для данной криптограммы.

Известно несколько классических систем шифрования: шифры перестановки, библиотечный, одноразовый шифроблокнот и шифры замены, которые часто сочетаются.

Криптография решает задачу изменения ASCII-кодов в мэйлерах и их взаиморасположения относительно друг друга. Кодировка представляет собой таблицу символов, где каждой букве алфавита (а также цифрам и специальным знакам) присвоен свой уникальный номер — код символа.

Задачи криптографии просты: сделать понятное («открытое») сообщение всецело непонятным («закрытым») для непосвященного. Подобный трюк осуществляется при помощи кодирования, а то, что получается в итоге, зовется криптограммой. Криптографический метод защиты, безусловно, самый надежный, так как охраняется сама информация, а не доступ к ней (например, зашифрованный файл нельзя прочесть даже в случае кражи магнитного носителя).

Библиотечный алгоритм

Кодирование осуществляется заменой слова, группы слов, а также целых фраз каким-либо условным словом или знаком, группой символов. Открытые слова здесь называются кодовеличинами, а их закрытые эквиваленты — кодообозначениями.

Набор кодовых символов обычно составляет кодовый алфавит (словарь), причем в таблицах кодирования в алфавитном порядке стоят кодовеличины, а в таблицах раскодирования — кодообозначения.

Для избежания повторов в тексте и усреднения частот встречаемости одному кодовому обозначению нередко соответствуют несколько кодовеличин, а одной кодовеличине (если она слишком часто применяется) — несколько (2-5) кодообозначений.

Если при кодировании слова в таблице не оказывается кодовеличины, то оно кодируется побуквенно, причем каждая буква рассматривается как некая самостоятельная кодовеличина.

Для затруднения дешифровки обычно используют так называемые «пустышки», то есть кодообозначения,

которые разбрасываются по тексту криптограммы, но не имеют никакого значения. Другой мерой предосторожности является последующее шифрование (обычно шифрами перестановки) уже закодированного сообщения.

Полезно важнейшие кодовые соответствия хранить в памяти, вкрапливая их при необходимости в открытый текст, а иной раз использовать простейший акрокод — чтение первых букв слов, строк или каких-то там частей (скажем, глаголов) предложений (к примеру, фраза «надобно еще тренироваться» читается как «нет»). В отличие от истинного кода, защита в акрокоде минимальна.

Для маскировки цифр и дат нередко применяется так называемый примитивный код, в котором буквы ключевого слова четко привязываются к конкретным цифрам.

Алгоритм перестановки

В шифрах перестановки буквы (или другие символы) исходного сообщения не меняются, а лишь переставляются по некоему закону, делая весь текст нечитаемым.

Известно множество программ шифрования, но характерный для всех программ шифр двойной перестановки столбцов и строк. Такие шифры хороши для подстраховки закодированного текста или отдельных криптограмм многоалфавитного шифрования.

Алгоритм замены

В подобных шифрах каждая из букв в открытом тексте заменяется другой буквой или символом, причем порядок букв при этом не меняется.

Замена может быть как однозначной (в шифрах простой замены, где каждой букве соответствует лишь один символ), так и многозначной (в шифрах многоалфавитной замены, где каждой букве соответствуют несколько символов); как однобуквенной (поочередная замена буквы на букву), так и многобуквенной (с шифрованием одновременно двух букв и более).

Шифры простой замены легко дешифруются при длине текста не менее двух-трех алфавитов путем анализа частот встречаемости букв и через знание типичных сдвоенных знаков, сочетаний и окончаний.

Алгоритм Цезаря

Шифры со сдвигом алфавита на некоторое фиксированное число букв («шифр Цезаря») читаются предельно просто, используя, к примеру, метод полосок, на каждой из которых нанесен стандартный алфавит. Полоски прикладывают друг к другу так, чтобы вышло слово из криптограммы, после чего, двигаясь вдоль них, находят осмысленное прочтение, определяя таким образом величину намеренного сдвига.

На практике имеет смысл использовать многоалфавитное шифрование с так называемым «текучим» алфавитом, задействуя какую-либо книгу.

Алгоритм одноразового шифроблокнота

В подобных шифрах каждая из букв в открытом тексте заменяется кодом, причем порядок при этом не меняется. Замена может быть как однозначной (в шифрах простой замены, где каждой букве соответствует лишь один символ), так и многозначной (в шифрах многоалфавитной замены, где каждой букве соответствуют несколько символов); как однобуквенной (поочередная замена буквы на букву), так и многобуквенной (с шифрованием одновременно двух букв и более).

Используя одну из множества таблиц со случайными числовыми последовательностями (число последовательностей больше или равно количеству кодов текста) производят математические операции над каждым кодом текста по заранее определенному правилу. Каждую таблицу со случайными

Биометрия: а ларчик ломом открывался

Сергей Бычков в статье «Биометрия в мэйлерах» (прошлый номер) рассказал об истории биометрии и технических аспектах ее внедрения. Действительно, в подавляющем большинстве рекламных роликов при включении компьютера используется идентификация пользователя по отпечатку пальца, которая в некоторых случаях дополняется еще и индивидуальной смарт-картой. IBM применяет подобную идентификацию пользователя в некоторых линейках своих ноутбуков уже около 5 лет. И все потому, что достоинств у этой технологии множество, и главный из них — простота использования для однозначной идентификации пользователя: отпечаток пальца — это пароль, который всегда при тебе. И взломать его методом перебора фактически невозможно. Да и пользователю ничего не надо запоминать — провел пальцем по окошечку, и все. Главное, чтобы руки были не слишком чистые. Да-да. При тщательно вымытых руках системы сканирования дают очень большой процент ошибок.

Сканеры отпечатков пальцев собираются встроить не только в ноутбуки и настольные компьютеры (как отдельное устройство или как составной элемент мыши, клавиатуры), но и в сотовые телефоны, систему зажигания дорогих автомобилей, оружие. Правда, с автомобилями уже связана одна неприятная история, которая больше напоминает сюжет боевика, снятого на фабриках Голливуда. Был похищен дорогой Mercedes, причем похитители знали, что запускается он только после сканирования отпечатка владельца. Поэтому автомобиль украли вместе с его хозяином. Но потом ворам надоело возиться с запускам двигателя, таская каждый раз автовладельца к сканирующему устройству. Они просто отрубили палец и уехали.

Увы, помимо указанного случая у технологии идентификации по отпечат-

числовыми последовательностями используют при шифровке один раз.

Алгоритм криптографии

Криптографические методы — это методы шифрования, в результате которых содержание информации становится недоступным без ключа криптограммы и обратного преобразования. Рассмотрим классический шифр Вернама. Для шифрования булевой строки длины N используется RSA-ключ — полностью случайная булева строка длины N. При шифровке сообщения (булева строка длины N) его текст побитно складывается с секретным ключом по модулю 2. Получатель, имея точно такой же ключ, сможет восстановить исходное сообщение, побитно сложив полученную строку с ключом.

В настоящее время существуют общепринятые криптографические алгоритмы защиты информации DES, DESX, IDEA, 3DES, AES, WPA, CAST или Blowfish. Алгоритм шифровальной машины Enigma положил начало криптографическим алгоритмам DES (US Federal Data Encryption Standard) и нашел свое продолжение в системе Unix для шифрования файлов. В алгоритме IDEA исходный файл архивируется zip-архиватором, а потом шифруется, этим он отличается от алгоритма DES.

В шифровании ASCII-кодов в криптографических алгоритмах («симметричный» метод закрытия информации) можно условно выделить четыре подхода:

- подстановка — символы шифруемого текста заменяются символами того же или другого алфавита в соответствии с заранее определенным правилом;
- перестановка — символы шифруемого текста переставляются по некоторому правилу в пределах заданного блока передаваемого текста;
- аналитическое преобразование — символы шифруемого текста преобразуются по некоторому аналитическому правилу;
- комбинированное преобразование — исходный текст шифруется двумя или большим числом способов шифрования.

Иногда коммерческие пакеты используют DES, который базируется на Internet Privacy Enhanced Mail (PEM), где один и тот же ключ используется и для шифрования, и для расшифровки. Это значит, что ключ должен первоначально быть передан через секретные каналы так, чтобы обе стороны имели его до того, как шифрованные сообщения поступят по обычным каналам. Существует несколько «режимов операции», которые может использовать DES (некоторые из них лучше, другие хуже). Эксперты не рекомендуют использовать простейший и самый слабый режим для сообщений, режим Electronic Codebook (ECB). Они рекомендуют более сильные и сложные режимы Cipher Feedback (CFB) или Cipher Block Chaining (CBC).

Мультимедийные алгоритмы

Для того чтобы предоставить возможность вести защищенные телефонные разговоры в реальном времени (по телефонным линиям и internet\intranet), используется технология сжатия звука в соответствии с алгоритмом MP3 и стойкие криптографические алгоритмы с открытым ключом (3DES, CAST или Blowfish), так что наличия защищенного канала для предварительного обмена ключами не требуется. Стороны обмениваются ключами с использованием протокола обмена ключами Диффи-Хеллмана, который не дает тому, кто перехватывает разговор, получить какую-либо полезную информацию, и в то же время позволяет сторонам обменяться информацией для формирования общего ключа, который используется для шифрования и расшифровки речевого потока.

ку пальцев есть немалое количество других уязвимых мест. Вот на них и остановимся.

Для начала замечу, что неповторимость отпечатка пальца — это уже не совсем аксиома. Во-первых, отпечатки сравниваются не целиком, а по неким контрольным точкам. Достаточно совпасть установленному количеству точек (в одних экспертных методиках 9, в других 16), и отпечатки считаются идентичными. Из истории криминалистики известно, что когда было увеличено число контрольных точек при анализе отпечатков, выяснилось, что некоторых людей надо выпустить из многолетнего тюремного заключения, так как единственным доказательством преступления были отпечатки, которые в свете новых стандартов оказались вовсе не принадлежащими обвиняемым. Однако требовать 100-процентного совпадения также нереально — даже два отпечатка у одного и того же человека часто не совпадают полностью.

Но и это еще не все. Недавно выяснилось, что в связи с ростом цифровой базы данных отпечатков участились случаи появления практически идентичных образцов. В начале этого года был арестован, а потом с извинениями отпущен адвокат, «пальчики» которого совпали с данными на одного из разыскиваемых террористов. Хотя, надо признать, таких случаев не так много — соотношение где-то около 1:1000000 (точных данных спецслужбы, дабы не компрометировать себя, естественно, не предоставляют).

В свете тотального перехода на паспорта на основе биометрической идентификации это может стать достаточно крупной проблемой. К тому же в этом вопросе так и не достигнуто единство: если во всем мире предполагается в первую очередь использовать отпечатки пальцев, то в США в качестве информации для биометрической идентификации предполагается использовать физиогномистику (идентификация по изображению лица), хотя она дает максимальный процент ошибок. Но тут главная цель — автоматический контроль за перемещением лиц с помощью камер видеонаблюдения.

Наконец, изготовить дубль отпечатка ничего не стоит, при этом нет необходимости в каких-то редких и дорогих материалах — достаточно тех, которые можно купить в любом магазине. В результате можно легко изготовить «пальчик» из геля. Да, уговорить человека сделать отпечаток в заранее подготовленную подушечку вряд ли удастся (разве что напоить его перед этим до беспамятства, а когда идет охота за ценными данными — это не проблема). Но ведь и это не обязательно. Достаточно заполучить один только отпечаток пальца «клиента». Процедура та же,

Защита в Интернет-протоколе

Ассоциация Internet Streaming Media Alliance (ISMA) опубликовала спецификацию защищенной доставки цифрового содержания на устройства различных типов по IP-сетям — Encryption and Authentication Specification 1.0. Спецификация призвана обеспечить совместимость систем кодирования, потоковых серверов и проигрывателей, выполненных по технологиям, основанным на открытых стандартах.

В качестве алгоритма шифрования содержания по умолчанию спецификация предусматривает применение AES со 128-разрядным ключом, но допускает использование любых криптосистем и служб управления цифровыми правами. Основное назначение спецификации — способствовать отказу от применения частных систем защиты потокового контента и внедрению открытых стандартов. В спецификацию включен также механизм дополнительной защиты для систем, полагающихся на инфраструктуру открытого ключа. Технология использует протокол SSL, который является фактическим стандартом защиты Интернет-коммуникаций. Такое решение обеспечит защиту закрытого ключа SSL даже в случае взлома сервера, на котором исполняется криптослужба. Реализуется защита разбиением закрытой части ключа на несколько фрагментов, каждый из которых хранится на отдельном сервере. Полностью закрытый ключ никогда не воссоздается — система по фрагментам генерирует частичные сигнатуры и отдельные расшифрованные участки, объединяя результаты прозрачно для полагающегося на нее приложения. Для дальнейшего повышения защищенности предусмотрена функция периодического обновления фрагментарных ключей.

Аппаратное ускорение

Многие производители процессоров для ноутбуков внедряют на аппаратном уровне команды для ускорения вычислительных операций в криптографии. Процессор C7 начнет новую эру технологий безопасности благодаря внедрению семейства технологий VIA PadLock Hardware Security Suite, предоставляющих аппаратное ускорение ключевых алгоритмов шифрования. В процессоре присутствует аппаратная поддержка генератора случайных чисел, алгоритма кодировки AES (Advanced Encryption System) — PSK (pre-shared key), операции по работе с хэш-функциями SHA-1 и SHA-256, ключа RSA (размер ключа Montgomery Multiplier равен 32 Кбайт). Так же, как и в последних процессорах Intel, наличествует бит NX, защищающий от исполнения потенциально вредоносного кода. C7 работает с шиной VIA V4 (800 МГц), поддерживает наборы инструкций MMX, SSE2 и SSE3, имеет 128 Кбайт L2 кэша.

Дешифровка

Чтобы прочитать зашифрованный текста без представления, каким образом он зашифрован, необходимо знание лингвистической статистики и математической модели алгоритма шифрования. Систему шифра (перестановка, замена...) пытаются определить методикой частотного анализа, выявляя сравнительную частоту присутствия различных букв и сравнивая ее с известным эталоном.

Значительную помощь в расшифровке дают таблицы встречаемости двух букв (биграмм), а также знание встречаемости отдельных букв в началах и в концах различных слов.

Часто используется прием с попыткой просто угадать слово в криптограмме (подпись, термин...), в особенности что в фильме «Семнадцать мгновений весны»: предлагаете человеку взять к руки какую-нибудь гладкую, лучше прозрачную безделушку, предварительно тщательно вытертую, а дальше — дело техники. Приносите домой, сканируете поверхность, в Photoshope наводите контрастность, многократно печатаете изображение на одном и том же месте. А потом за 10 минут изготавливаете «гелевый» пальчик.

Еще одна уязвимость — проблема хранения результатов сканирования. Существует два варианта: когда хранится изображение пальца и когда хранится только некая контрольная сумма, вычисленная по отсканированному изображению. Соответственно, в первом случае высок риск «кражи личности».

Да и шифрование не без изъянов. Никто не застрахован от перехвата данных, как механического, так и программного. Например, известная и очень мощная система шифрования PGP (предложение ее использовать можно увидеть в программе The Bat!, если открыть меню Tools) может быть легко взломана путем подмены одной из библиотек с ее программным кодом. В результате ключи генерируются не случайным образом, а по известной злоумышленникам закономерности.

Поэтому помимо шифрования данных развиваются альтернативные методы защиты, в том числе «экзотические». Начну с защиты на случай экстренной ситуации. Существуют уста-

ти, если известна лексика послания. Затем через вычитание предполагаемого слова (или фразы) из шифротекста можно попробовать найти ключ к шифру многоалфавитной замены.

Дешифрование систем шифроблокнотов возможно при повторном применении какого-либо из участков случайной числовой последовательности. При этом, вычтя из одной шифропоследовательности другую, можно освободиться от ключа, имея в результате разность двух совершенно незакрытых текстов. Предположив в одном из них какое-либо вероятное слово, его пытаются «сложить» с имеющейся «разностью». При правильном угадывании в этом случае становится читабельным и второй текст.

Криптоанализ

Разгадать ключ RSA возможно лишь путем разложения чисел на множители зашифрованного файла или посредством дифференциального криптоанализа. Ключ RSA может быть получен на основе исследования регистров и дифференциального анализа. Метод «разделяй и вскрывай». Самый знаменитый из алгоритмов, реализующий факторизацию, то есть разложение целого числа на простые множители, создан американским математиком Питером Шором. Для числа из n знаков этот

алгоритм требует n3(log n)k (k — константа) шагов. На сегодня это самый быстрый алгоритм, позволяющий взломать RSA — один из самых распространенных криптопротоколов, причем алгоритм реализуется за разумное время на обычном компьютере.

Алгоритм шифрования, который обеспечивается ключами, можно ослабить путем установки некоторого количества входных бит в 0 и таким образом приблизить его к вскрытию. Например, никакой современный классический ПК не способен по-настоящему «вычислить» случайное число из-за переполнения буфера (область памяти внутри процессора для оперативного хранения данных), то есть из-за занесения туда большего объема информации, чем в нем может поместиться.

Математическая схема работы генератора случайных чисел проста. Создается бит в состоянии |0>, затем к нему применяется так называемое преобразование Адамара. После этого при измерении данного бита значения |0> или |1> появятся с одинаковыми вероятностями. Повторив процесс N раз, мы получим случайное целое число в пределах от 0 до 2N - 1. Это число и становится RSA-ключом.

Шеннон доказал, что такой шифр будет абсолютно стойким при условии полной случайности RSA-ключа и однократности его использования. Поскольку это условие как раз и не выполняется из-за переполнения буфера в процессорах Intel и AMD, данную брешь используют для взлома. Отсюда интерес криптологов к квантовым технологиям, где случайность не имитируется детерминированными классическими вычислениями, а связана с физикой работы самого вычислителя.

Разработана также технология поиска повторяющихся фрагментов зашифрованного текста, основанная на алгоритме Тиресия. Этот алгоритм создавался для поиска повторяющихся участков в цепочках ДНК и аминокислот. Применительно к электронным сообщениям алгоритм Тиресия также анализирует последовательности, правда, состоящие из традиционных символов, которыми представлен текст письма. Таким образом можно получить набор буквенно-числовых последовательностей, характерных для RSA-ключа.

новки, внутрь которых помещается винчестер, и в случае опасности вся информация стирается в долю секунды двумя магнитными импульсами. Внутрь винчестеров могут встраиваться емкости с кислотой, которая выливается на диски в момент опасности (при наступлении определенного события).

Есть кое-что и в области контршпионажа. В системной области жесткого диска (которая не затирается даже форматированием) размещается микро-мэйлер, который при подключении к Интернету тут же отправляет хозяевам сообщение с IP-адресом, телефоном и другими данными, которые позволяют однозначно выяснить, где находится похищенное. Появляются носители данных (а также фотоаппараты, сотовые), которые, будучи украденными, смогут послать через GPRS сообщение о своем местонахождении.

Но не будем забывать, что против лома нет приема. В приватной беседе один из сотрудников зарубежных спецслужб сказал: «Пароли, шифрование... На пару часов в допросную комнату — и я буду знать все пароли, какие подследственный только помнит с детства. Не скажет? Ну, если он не хочет превратиться из человека в шевелящийся кусок мяса, то все скажет».

В общем, Мюллер жил, жив и будет жить.

Вот такая получается антибиометрия.

Анатолий Ковалевский

ТВОЙ СКОРОСТРЕЛЬНЫЙ ШОТГАН

Анатолий Ковалевский (С.-Петербург)

Сейчас любой компьютерщик вооружен не хуже ковбоя с Дикого Запада. Редко у кого один винчестер, чаще два или три. Однако любое оружие, будь то огнестрельное или информационное, требует, во-первых, грамотного выбора и, во-вторых, тщательного ухода и правильной эксплуатации. Попробуем разобраться, как выбрать максимально скорострельный «ствол».

Уже достаточно давно бытует мнение, что многогигабайтные винчестеры не нужны, что их кроме как фильмами и музыкой больше просто нечем забить. Скептикам обычно отвечают, что гигабайтов, как и патронов, много не бывает. Человек, которой садится к монитору не только для того чтобы поиграть или посерфить в Сети, от компьютера получает много ценной информации, которую, естественно, хочется всегда иметь под рукой. У меня на диске с данными более 200 тысяч файлов помимо фильмов и музыки. И, самое главное, нужная информация действительно под рукой благодаря реализованной наконец-то возможности мгновенного поиска Google Desktop. Главные плюсы — это мгновенная индексация данных (не надо ждать по 20-30 минут результатов), возможность индексировать PDF-файлы, а также письма из The Bat! и, естественно, возможность четко ограничить поиск только локальным компьютером. Впрочем, о Google Desktop (равно как и о других поисковиках) как-нибудь в другой раз.

Итак, выбор винчестера. Я рассмотрю две наиболее часто встречающиеся ситуации. Вариант 1 — когда надо просто повысить объем винчестера на старой системе (обойдется примерно в $100). Вариант 2 — необходимо максимальное быстродействие. В этом случае покупаем два винчестера, «заточенные» под работу в RAID-массиве, с поддержкой TLER, SATA-II, NCQ (приготовьте $300-350 без учета стоимости материнской платы).

Чтобы было легче ориентироваться, я свел наиболее важные критерии в таблицы и кратко прокомментирую их.

Что такое кэш, скорость, объем, интерфейс, я думаю, пояснять не нужно. RAID — возможность создания из диска массива для ускорения работы (работают одновременно два диска и более) или для резервного копирования данных (в случае физического выхода из строя одного из дисков у вас сохранится его точная копия). Технологии типа TLER (Time Limited Error Recovery) означают, что винчестер специально создается для работы в RAID-массиве (есть автоматическая корректировка ошибок, выше надежность). NCQ (Native Command Queues) — оптимизация работы путем перегруппировки команд в зависимости от того, к каким областям диска они обращаются. Другие параметры — механизмы шумоподавления, парковка головок при падении и прочее — не учитывались, так как оценить их эффективность невозможно, приходится верить производителю на слово.

Надо отметить, что многие параметры из таблицы 1 носят взаимоисключающий характер. Так, с увеличением скорости вращения винчестера резко падает его объем, что связано с невозможностью обеспечить корректное чтение/запись. Поэтому при скоростях больше 7,2 тыс. об./с объем диска не превышает 100 Гбайт (то есть винчестер покупается или большой и медленный, или быстрый и маленький).

Ну, и что мы выберем? Задача, как это часто бывает в жизни, — многокритериальная, то есть требующая учета сразу нескольких параметров. Упомяну хотя бы основные.

Во-первых, выбираем брэнд. Именно поэтому в таблице 2 не указаны фирмы, для которых производство винчестеров является непрофильным, — параметры их дисков заведомо хуже. Поясню: производители должны

Параметр	Максимальный	Вариант 1	Вариант 2
Кэш, Мбайт	16 (из доступных на рынке – 8)	8	8
Скорость, тыс. об./с	15	7,2	10
Объем, Гбайт	400-600 (из доступных на рынке 350)	200	72 x 2
Интерфейс	SCSI или SATA II	IDE	SATA II
RAID	да (с поддержкой TLER и т. д.)	нет	да (без TLER)
NCQ	да (на чипсете и винчестере)	нет	да

Параметры	Seagate	Western Digital	Samsung	Maxtor	Hitachi/IBM
Кэш, Мбайт	16	16	8	2	8
Скорость, тыс. об./с	7,2 (10-15)	7,2 (10)	7,2	7,2	7,2
Объем, Гбайт	400 (96)	350 (76)	200	160	600
Интерфейс	SCSI, SATA-II	SCSI, SATA-II	SATA-II	SATA-I	SATA-I
RAID (+TLER)	да	да	нет	нет	нет
NCQ	да	да	да	да	да

иметь в своей линейке самые быстрые модели, тогда они смогут выпускать и дешевые среднескоростные модели. Должны быть также дорогие модели для серверного и корпоративного рынков — тогда со временем «высокие» технологии оттуда «перетекут» в сегмент общедоступных винчестеров.

Во-вторых, график чтения в тестах должен иметь ровный вид без всяких провалов. Эти провалы через пару лет могут легко вылиться в сбойные участки (чем часто грешат винчестеры Samsung, у которых очень быстрые и очень нестабильные графики чтения).

Далее, желательна большая кэш-память. SCSI и SATA-II (именно версии II, это важно) по производительности сравнялись, однако первая технология стоит раза в 2-3 дороже. NCQ должна поддерживаться и винчестером, и чипсетом, иначе не будет работать. Винчестеры должны иметь минимальный возврат по причине брака (почитайте интервью со сборщиками ПК — K-Systems, МИР, Aquarius и т. д.).

Лично у меня методом исключения выбор пал на Seagate и Western Digital. Окончательно я выбрал первый вариант, хотя по доступности технологий более привлекательной казалась вторая фирма. Сработала мысль, что «при прочих равных» куда легче отслеживать новинки, выкачивать ПО для работы/профилактики с сайта от одного производителя, чем от нескольких. Чтобы ни говорили, а производитель все же лучше знает свое железо, чем авторы разного рода универсальных утилит. Вот на основании этих «интегральных» показателей и был выбран Seagate.

Материнская плата, с которой предстояло работать винчестеру, основывалась еще на первом чипсете nForce, поэтому RAID, TLER, SATA-II или NCQ даже не предполагались. Можно, конечно, купить плату расширения со всеми этими функциями, но работу системы все равно будет ограничивать низкая пропускная способность системной шины. В результате был куплен Seagate 200 Гбайт IDE-винчестер, 7,2 тыс. об./с, 8 Мбайт кэш (на момент покупки в продаже еще не было моделей на 350 Гбайт и с кэшем 18 Мбайт). Модель на 300 Гбайт я проигнорировал в связи с тем, что за дополнительные 100 Гбайт шла уже хорошая наценка, а к тому времени, когда гигабайтов не будет хватать, в продаже наверняка появятся терабайтные диски.

Суета вокруг кластеров

Купил, подключил. Диск опознается Partition Magic как 186 Гбайт. Весело. Форматирую под другие размеры кластера — ситуация не меняется. Получается, что 16 Гбайт остались у производителя в связи с манипуляцией терминами бит/байт (этим страдает не только Seagate). Если пересчитать на стоимость, то $15 я потерял. Ладно. Обращаю внимание на то, что кусок в 7 Мбайт не найден — выделяю в отдельный логический диск. Пытаюсь слить диски — отказ, разная версия кластеров. Точно: маленький диск под кластер 0,512 Кбайт, а большой — под 4 Кбайта. Привожу к одной версии кластера. Снова отказ, на этот раз из-за того, что все 186000 Мбайт «сливаются» на диск 7 Мбайт (он первый). Форматирую, отключаю сжатие, индексацию и наблюдение. Не помогло. Увеличиваю диск 7 Мбайт до 7000 Мбайт — теперь дело пошло, но... опять застопорилось.

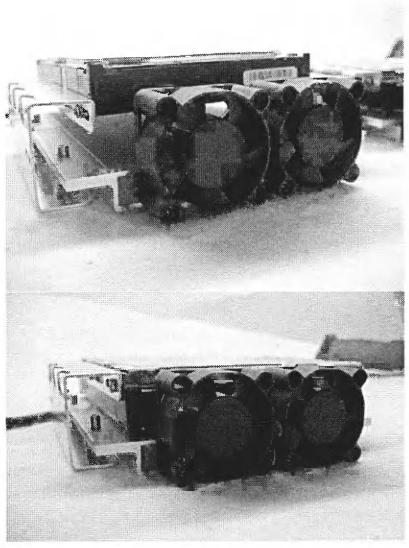
Выяснилось, что один из дисков отформатирован под NTFS 3.0, а другой под NTFS 3.1 (один из дисков форматировался штатной утилитой от Microsoft). Меняю на двух дисках размер кластера под Partition Magic — наконец-то все заработало! Правда, размер диска так и остался 186 Гбайт.

Эти мытарства приведены здесь исключительно для того, чтобы читатель так не делал, — надо запускать фирменную утилиту от производителя (в данном случае это Seagate SeaTools Enterprise Edition), и все утрясется само собой за один раз.

Установка

Теперь осталось грамотно установить винчестер в системный блок.

Исходя из прошлого негативного опыта (винчестер на 40 Гбайт в течение года работал без охлаждения и с отключенной системой S.M.A.R.T.-контроля, из-за чего оброс бэд-блоками), к проблеме охлаждения было решено подойти более основательно: два алюминиевых блока для HDD от Titan'a (TTH-HD82). На них можно поставить



еще один кулер, но пока обойдемся двумя штатными.

И тут выясняется, что закрепить винчестер можно не одним способом, а минимум двумя. Выбираем тот авриант, при котором потоки воздуха от кулеров лучше обдувают плату с микросхемами (днище) — она-то, собственно, и греется. Кстати, современный винчестер не имеет снизу шумоподавляющей крышки, которая, может быть, шум и подавляет, но и теплоотводу мешает заметно. Так что к монтажу надо подойти с головой.

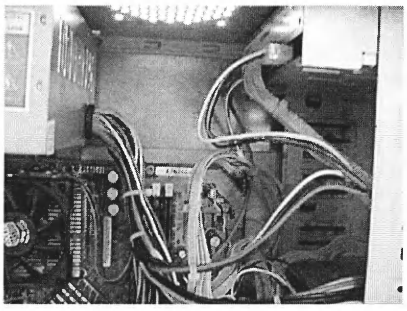
Теперь думаем, где все это лучше разместить. Если поставить в 5" отсеки, то DVD проигрыватель (в дополнение к уже установленному CD-приводу) встанет туда буквально впритык. Да и теплый воздух от четырех железок будет идти через память, процессор и источник питания. Даже если наладить отвод воздуха вверх, это не спасет. Поэтому крепим винчестеры не в 5" отсек горизонтально, как предполагает производитель, а в 3" вертикально (Seagate и Western Digital утверждают, что это никак не влияет на производительность). Крепим винчестеры друг к другу при помощи двух деталей от детского конструктора и ставим в корпус.

Но прежде, чем подключать шлейфы, давайте остановимся на одной немаловажной детали. Деталь эта называется корпус.

Корпус

Выбирая корпус, надо обратить внимание на три важные вещи:

1. Корпус должен быть красив. По-



купка компьютера — это существенная трата семейного бюджета, и домашние должны оценить ее. Переплатите $10, и вы удивитесь, насколько положительнее они отнесутся к покупке.

2. Системник должен быть удобен для монтажа. Совершенно излишне, когда материнская плата выезжает на салазках из корпуса, — ее мы меняем редко, и ради такого случая можно вытащить ее из корпуса руками. А вот крышка должна крепиться одним болтом и легко сниматься с любой стороны — в корпус по разной нужде приходится лазать достаточно часто.

3. И главное — корпус должен быть грамотно спроектирован. Важно это не только для лучшей циркуляции воздуха. В тесном корпусе даже простой вентилятор на винчестер можно установить с трудом. Так что обеспечьте себе заранее более легкий и просторный монтаж. Плюс отверстия под вытяжку в «потолке», а не впритык к стенке.

В результате после установки винчестера, охлаждения к нему и зарауненных шлейфов осталось достаточно места для дальнейшей модернизации компьютера.

Как, вы не знаете, что такое зарауненный шлейф и зачем он нужен? Тогда читайте дальше.

Изготовление зарауненного шлейфа

Удивительная вещь — современный пользователь скорее будет долго и нудно копаться в меню настроек, чем рискнет что-то настроить руками внутри корпуса. Специально для тех, кто сомневается в своих силах, — отдельный и подробный рассказ о том, как своими силами зараундить шлейф.

Прилагательное «зарауненный» происходит от английского round —круглый. Смысл в том, чтобы плоский шлейф превратить в круглый жгут из проводов. Поверьте моему слову и реальным тестам — после такой операции система будет в несколько раз быстрее откликаться на ваши действия — скорее открываются папки, запускаются программы, разворачиваются меню (причина в том, что уничтожаются помехи, которые возникают в плоских шлейфах из-за многочисленных перегибов).

К тому же только так мне удалось перевести работу винчестера из режима DMA 3 в более скоростной DMA 5. Наконец, значительно облегчается вентиляция в корпусе.

В конце концов простой шлейф стоит всего $3, так что смело экспериментируйте.

Serial ATA. Дубль три...

Дисковый стандарт Serial ATA разработан в конце прошлого века, но еще пару лет назад винчестер с этим интерфейсом был в диковинку. Физически интерфейс Serial ATA не имеет ничего общего с параллельным. В параллельном используются пачки импульсов, передаваемые одновременно по множеству пар проводов. В Serial ATA сигнал передается импульсами (0,25 В вместо 5 В), для передачи используется широкая полоса частот (10 — 4500 МГц).

Кабель содержит две двухпроводные линии («дифференциальные пары») и линии питания. Последние передают постоянное напряжение 3,5 и 12 В для различных устройств. Длина кабеля может достигать 1 м (а интерфейсный «шлейф» IDE — не более 45 см). Размеры соединителей также меньше, чем для IDE. Это создает известные удобства для монтажа и позволяет использовать интерфейс для устройств формфактора 2,5" (винчестеры для ноутбуков).

Первые модели винчестеров имели два интерфейса — ATA/100 + Serial ATA или же ATA/133 + Serial ATA. Это были не настоящие Serial ATA: в уже выпускавшиеся модели встраивался контроллер, осуществлявший перекодировку сигналов из параллельной в последовательную, что позволяло сопрягать их и со старыми, и с новыми материнскими платами. Скорость передачи данных они имели не слишком высокую, не более четверти от максимально возможной (150 Мбайт/с).

Следующее поколение винчестеров — «настоящие» Serial ATA, уже без параллельного интерфейса. Скорость увеличилась до 45-55 Мбайт/с.

За последний год на рынке появилось сразу несколько моделей винчестеров (Samsung, Hitachi, Western Digital) с последовательным интерфейсом нового поколения — Serial ATA II. Их емкость составляет от 80 до 400 Гбайт. Все винчестеры имеют привычные характеристики — скорость вращения шпинделя 7200 об./мин, объем буфера 8 Мбайт. Система управления NCQ (Native Command Queues) позволяет жесткому диску обрабатывать несколько запросов, посылаемых процессором, и определять их очередность так, чтобы достигалось максимальное быстродействие системы.

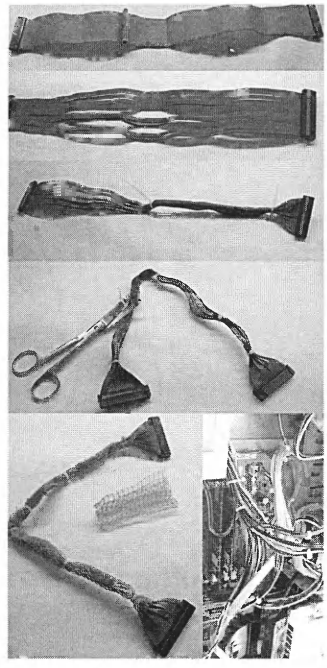
Если верить независимым тестированиям, применение NCQ увеличивает скорость передачи данных на 15-30%, однако реально достижимая скорость увеличилась ненамного. Напомню, что максимальная скорость передачи для стандарта Serial ATA II составляет 30 Мбайт/с. Дело в том, что скорость зависит от задачи. Она максимальна в случае чтения длинного файла, причем записанного на только что дефрагментированный диск, кластер за кластером. Если читаемый файл сильно фрагментирован, его приходится собирать по кусочкам, скорость снижается в 2-2,5 раза.

При копировании файла скорость ниже, здесь чередуются чтение и за-

Итак, что нам надо — 1 шлейф, 5-6 пластиковых хомутиков, 1 инструмент для резки и 10 минут времени. Все.

Берем для начала 40-жильный шлейф для привода CD/DVD — если вдруг начнете все резать не вдоль, а поперек, то потери составят всего $1,5-2. Набор пластиковых хомутков из 100 шт. на развалах стоит вообще $0,8. В качестве инструмента для резки идеально подходит одноразовый скальпель на пластиковой ручке, который можно купить в большинстве аптек (около $1). Лезвием для бритвы резать неудобно (если только осколком, вколоченным в деревяшку). Можно и ножом — главное, чтобы у него был тонкий и острый как у бритвы конец. Ну, а 10 минут времени — вообще возобновляемый ресурс, потому что они к вам еще 10 раз по 10 раз вернутся за счет более быстрой работы компьютера.

Если необходимо, снимаем со шлейфа промежуточный разъем (по бокам находятся пластиковые ушки, которые слегка отгибаются в сторону, и крепление разнимается на две части), аккуратно вынимаем из провода зубчики контактов.



Далее кладем шлейф на деревянную поверхность и при помощи скальпеля разделяем вдоль жил на две части, потом еще раз и еще, пока весь шлейф не будет состоять из полосок в 3-4 провода.

Не стоит сильно давить на скальпель — за счет бороздки между проводами шлейф отлично разрежется и так. После надреза, кстати, можно вообще больше не резать — достаточно потянуть за два провода. Единственное, где стоит быть аккуратным, — места сгибов кабеля и крепления промежуточного разъема.

После нарезки собираем провода в пучок так, чтобы те полоски, которые идут по краям шлейфа, были либо снаружи, либо внутри.

Стягиваем их при помощи пластиковых хомутиков и отрезаем выступающие хвосты.

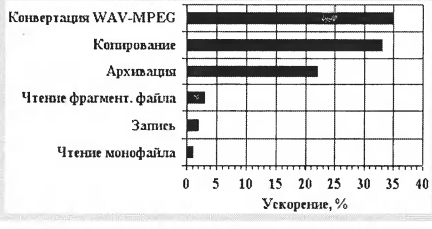
При желании можно найти пластиковую сетку и, обмотав шлейф, закрепить хомутиками сверху. Главное — проследить, чтобы в пластиковой сетке не было никаких металлических элементов в качестве основы для нитей.

Все, зарауненный шлейф готов, не забудьте перевести сэкономленные $10 автору ;)

пись. Еще ниже скорость при архивировании файла, впрочем, здесь она зависит в значительной мере и от быстродействия процессора.

Необходимо заметить, что именно в тех случаях, когда винчестер дает максимальную скорость, при чтении/записи длинного файла, NCQ помогает в минимальной степени: здесь нет множества запросов от процессора, и экономить не на чем. При чтении сильно фрагментированного файла замедление обусловлено тем, что файл приходится собирать по отдельным кластерам, постоянно сверяясь с FAT, так что и здесь NCQ малоэффективно. При копировании файла с одного места на другое NCQ дает заметное ускорение, а максимальное достигается в таких задачах как архивирование и конвертация мультимедийных файлов из одного формата в другой.

Все же для реальных, а не тестовых задач, ускорение будет весьма заметным. Значит ли это, что нужно апгрейдить компьютер?



К сожалению, производители системных плат отстают от производителей винчестеров. Первые винчестеры с двумя интерфейсами можно было без труда установить на старую системную плату. Когда в продаже появились «настоящие» винты Serial ATA, одновременно с ними начали продавать и новые системные платы. Зато сейчас в продаже есть множество винчестеров Serial ATA II, но практически невозможно встретить системную плату, поддерживающую этот стандарт.

Нет, в Москве такие бывают, московские журналы их успешно тестируют, но в Петербурге они в диковинку. В двух магазинах мне сказали, что плату можно заказать, но собрать на ней компьютер они не возьмутся.

Откуда такая осторожность? Дело в том, что стандарты Serial ATA и Serial ATA II имеют частичную совместимость, а грядущий стандарт Serial ATA III будет вовсе несовместим ни с первым, ни со вторым...

На практике «частичная совместимость» означает, что винчестер Serial ATA, подсоединенный к плате стандарта Serial ATA II, будет «винтить» на 150 Мбайт/с. Это не суть важно, поскольку реально достижимая скорость еще не доросла даже до 100 Мбайт/с.

Зато винчестер Serial ATA II в паре с материнской платой Serial ATA работать вообще не будет, а если и будет, то с таким количеством сбоев, что скорость снизится более чем вдвое.

Итак, самые новые винчестеры покупать не следует? Для апгрейда — не надо. Но при сборке нового компьютера есть смысл установить в него и плату, и винчестер Serial ATA II. Причем инженеры должны протестировать готовый ПК, убедиться, что сбоев не будет.

В таком компьютере винчестер и процессор будут обмениваться данными раза в полтора быстрее, что увеличит общее быстродействие системы процентов на двадцать.

Обещают, что в начале 2007 года выйдет стандарт Serial ATA III (максимальная скорость 600 Мбайт/с). Еще через полгода появятся винчестеры, а спустя какое-то время и системные платы. То и другое будет несовместимо с прежними моделями. Итак, до устаревания самого современного компьютера остается полтора-два года...

Николай Богданов-Катьков

ИСПЫТАНИЕ СОЛНЦЕМ

Николай Богданов-Катьков (С.-Петербург)

Качество печати современных принтеров — как струйных, так и термосублимационных — давно удовлетворяет обычным критериям качества: распечатки трудно отличить и от настоящих фотографий, и даже от полиграфической продукции.

Говоря о качестве печати, обычно имеют в виду качество получаемого изображения. Его можно оценить визуально или по тестам. Однако профессионалы к листу бумаги с распечаткой применяют понятие «потребительские качества». Этот термин охватывает все физические, химические и иные свойства данного предмета, имеющие значения для пользователя. Какие именно?

Распечатка струйного принтера, сделанная на специальной бумаге с фотографическим качеством, отличается от фотографии. Чтобы в этом убедиться, достаточно капнуть на лист водой.

Чернила для большинства струйных принтеров водорастворимые, вода испаряется, а краситель остается на бумаге. Но как только на распечатку попадает капля воды, краситель начинает снова растворяться и изображение «плывет».

Это не единственный недостаток струйной печати. Применяемые красители неустойчивы к действию света. Если распечатка лежит в фотоальбоме, она может храниться десятки лет без видимых изменений. Но если ее вставить в рамку и повесить на стену, она начнет блекнуть и через год-другой будет уже совершенно не похожа на фотографию.

Некоторые еще помнят неприятную историю, случившуюся в 2000 году. В начале года фирма Epson (принтеры которой, кстати, печатают с отменным качеством!) выпустила два новых принтера для печати фотографий. Epson Stylus Photo 870 был рассчитан на листы формата A4, а Epson Stylus Photo 1270 — на формат A3. В обоих принтерах использовалась шестицветная печать, и распечатки почти невозможно было отличить от фотографий.

Фирма утверждала, что для этих принтеров были разработаны особые светостойкие чернила, и отпечатки должны сохраняться без видимых изменений до 80 лет. Принтеры охотно покупали, но когда их владельцы вернулись из летних отпусков и начали печатать фотографии, сделанные цифровыми камерами, разразился скандал. Оказалось, что распечатки все же выцветали, и, что хуже всего, выцветали неравномерно! Голубые чернила выцветали быстрее, чем желтые и пурпурные, и фотографии приобретали грязно-коричневые оттенки.

После истории с Epson ни одна фирма больше года не рисковала рекламировать «светостойкий струйный принтер», но затем Canon и Epson выпустили несколько моделей. На этот раз все было сделано как следует. Принтеры фирмы Canon тестировал независимый научный центр. Было заявлено, что распечатки на специальной фотобумаге Canon Photo Paper Pro PR-101 будут сохранять свой натуральный цвет в течение 26-28 лет.

Возникает естественный вопрос: неужели испытания проводились десятки лет? А если нет, можно ли быть уверенным в их корректности?

Выцветание красителей — фотохимический процесс, он поддается расчету и моделированию. Степень выцветания можно определить как уменьшение количества красителя, проще всего это сделать по снижению оптической плотности D. Считают, что изменение цвета отпечатка будет заметно при снижении величины D ниже 70% от исходной. Но чернила выцветают по-разному, и необходимо, чтобы выцветание чернил всех базовых цветов происходило равномерно. По крайней мере, разница не должна превышать 15%.

При испытании моделировались условия, максимально близкие к естественным — освещенность 450 люкс, время освещения 12 часов в сутки. Можно считать, что такому воздействию подвергается фотография, висящая на стене в светлой комнате.

Для испытания выбрали следующие условия (данные Wilhelm Imaging Research Inc.):

- температура 24°C
- влажность 60%
- источник света: белый флуоресцентный свет 30000 люкс.

Образец находился под стеклом.

Поскольку освещенность при испытании примерно в 70 раз выше, чем в естественных условиях, времени на испытание потребовалось меньше — примерно два с половиной месяца.

Если быть точнее, на выцветание красителей влияет не только свет. Красители обесцвечиваются под действием кислорода, окислов азота и серы, постоянно присутствующих в воздухе промышленных городов, а также озона.

Как пример могу привести комнату, где стояли два старых копировальных аппарата, которые при работе выделяли озон. Там выцветали обои, настенные календари, деловые документы. А красные розы в горшке, стоявшие на подоконнике, через три месяца превратились в бледно-розовые...

Но пример не характерен; в большинстве случаев на выцветание влияет почти исключительно характер и интенсивность освещения, а именно это смоделировать очень сложно. В самом деле, лабораторные условия испытания соответствуют реальным условиям хранения лишь очень приблизительно.

Чтобы испытать на практике светостойкость отпечатков, гораздо лучше повесить их на несколько месяцев перед окном. Сошлюсь на личный опыт — настенный календарь, провисевший на стене напротив окна год, практически не потерял цвет; его было нельзя отличить от собрата, пролежавшего тот же год в ящике письменного стола.

Итак, полиграфическая печать выдерживает испытание светом. Почти столь же хорошо сохраняются отпечатки, сделанные традиционным способом в фотолаборатории. Почти — за тем исключением, что они несколько блекнут. Но все красители выцветают равномерно, так что нарушения цветопередачи не происходит. Придется ввести еще одну физическую величину — цветоравномерность. Если она не выходит за пределы 5-7%, глаз не заметит ухудшения качества отпечатка.

Совсем другая картина со струйными и термосублимационными фотопринтерами. Если собрать и подытожить данные, опубликованные в бумажных и сетевых изданиях, то получится примерно такая картина.

1. Отпечатки, сделанные в фотолаборатории (с пленок), практически ничего не теряют. Самое худшее — они могут слегка поблекнуть, но цвета не изменятся.

2. Термосублимационные принтеры не обеспечивают равномерности. Отпечаток, сделанный на принтере Mitsubishi 8000, за полгода потерял около 50% голубого цвета, и фотография приняла красно-желтый оттенок.

3. Так же мало обеспечивают сохранность отпечатков струйные принтеры, печатающие водорастворимыми чернилами. Впрочем, и здесь многое зависит от фирмы-производителя. Так, для принтера Epson R200 наибольшие потери были в желтом цвете, общий цветовой тон принял красно-синие оттенки. Другими словами, фотография человеческого лица стала «синюшной», как будто от легочной недостаточности.

4. У распечаток Canon более всего страдает пурпурный краситель. Человеческое лицо получается желто-зеленым, как при желтухе. Кроме того, выцветает черный краситель, поэтому темные участки фотографий блекнут куда сильнее.

5. Изо всех струйных принтеров лучшие результаты дают те модели Epson, в которых применяются пигментные чернила (например, R800). Разница между освещаемым и «темным» снимками практически незаметна.

Ну, а если печатать только водорастворимыми чернилами? Что будет, если взять желтые и голубые от Canon, а пурпурные и черные от Epson (те и другие выцветают меньше всего)?

Вероятно, ничего хорошего. Дело в том, что принтеры всех фирм хорошо печатают только на тех образцах бумаги, которые проверены и рекомендованы данной фирмой. На любой иной (даже «совместимой» бумаге) результат может оказаться совсем другим.

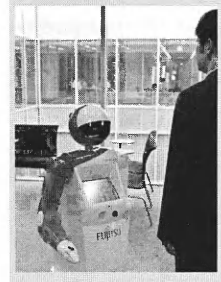
Итак, вывод. С точки зрения светостойкости лучше всего — аналоговое фото, распечатанное в фотолаборатории, оно окажется наиболее долговечным. На втором месте — печать пигментными красителями (наиболее дорогие принтеры Epson). На третьем — сублимационные принтеры, а на четвертом — обычные струйники, печатающие водорастворимыми чернилами.

Но в любом случае не надо надеяться, что распечатки провисят на стене 100 лет и не поблекнут.

На фронтах роботостроения

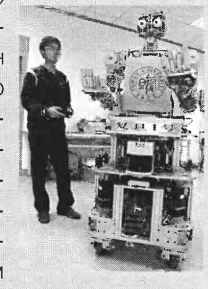
Fujitsu завершила разработку робота «enon» (акронимом фразы «exciting nova on network»), способного выполнять функции портье. Новинка ростом 130 см оснащена ультразвуковым сенсором и шестью камерами, помогающими обходить препятствия.

Робот может сопровождать посетителей, служить проводником и наблюдать за обстановкой в целях обеспечения безопасности. Он оснащен голосовым интерфейсом и цветным экраном на «груди» для взаимодействия с пользователями. Для транспортировки багажа клиентов используется внутренний отсек корпуса. Для «патрулирования» участка робот использует встроенные видеокамеры и маршрут движения, полученный по сети. По команде оператора «enon» может заглянуть в конкретное место и осмотреть его.



Цена новинки на японском рынке — около 50 тыс. долларов.

Специалисты из Фуданского университета в Шанхае изобрели первого сообразительного и общительного робота Fudan-1. Он самостоятельно ходит, видит, слышит и разговаривает. Может как управляться дистанционно, так и общаться со своим «учителем» посредством голоса, жестов и прикосновений.



А в Южной Корее под руководством правительства страны разрабатывается робот для участия в боевых действиях. Совместное детище министерства обороны и коммуникаций обойдется государству в 32,4 млн долларов. Разработку планируется завершить к 2011 году. Робот, передвигающийся на 8 колесах, может быть вооружен и оснащен различными сенсорами. Управляется дистанционно или с помощью собственного искусственного интеллекта.

Hard-news
(периферия)

Минивинчестер для экстремальных условий

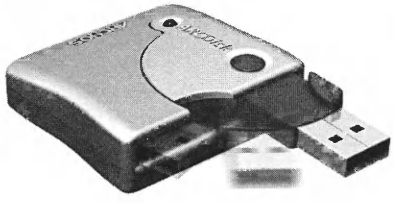
Компания Apricorn выпустила портативное запоминающее устройство Apricorn MicroKey на базе 1-дюймового жесткого диска в прочном корпусе из алюминиевого сплава, который обладает повышенной ударостойкостью: в рабочем режиме выдерживает ускорение 200 g, а в выключенном состоянии — 2000 g.

Накопитель оснащен двумя пакетами ПО: Second Copy 2000 Synchronizing Software для обмена данными между несколькими компьютерами и Cryptainer Encryption Software для защиты информации посредством 128-битного шифрования.

Apricorn MicroKey оборудован вращающимся разъемом с интерфейсом USB 2.0. При размерах 86,3 x 50,8 x 12,7 мм и весе 77,7 г он будет доступен в двух модификациях: емкостью 4 и 6 Гбайт ($159,99 и $199,99 соответственно).

Мини-винчестеры набирают силу и популярность

Сверхкомпакные винчестеры (формфактор не более дюйма) уже активно используются в цифровых диктофонах, MP3-плеерах и средствах сотовой связи, а с недавних пор они приобрели популярность и в качестве карманного носителя данных при наличии интерфейсов USB-1,2 (с убирающимся коннектором), FireWire и/или Wi-Fi. При этом максимальная емкость HDD формфактора 1 и 0,85 дюйма составляет 12-16 Гбайт, однако в производстве пока освоены только приводы на 1, 2, 4 и 5 Гбайт.



Естественно, производители применяют комплекс мер для демпфирования ударов, вводят режимы принудительной парковки головок, что обеспечивает работоспособность и сохранность данных при падении HDD с высоты кармана на рубашке пользователя.

Питание HDD-малютки осуществляется от шины сигнального интерфейса, что обеспечивает им автономность. Пока в малогабаритных HDD нет драйверов, поддерживающих шифрование. По мнению производителей, это ближайшая перспектива, и такие винчестеры появятся в начале 2006 года.

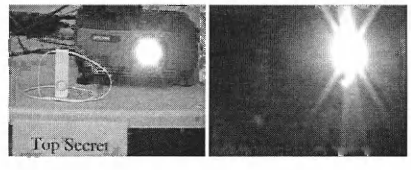
Стартовая цена мини-винчестеров в зависимости от емкости составит от 150 до 350 долларов.

Блокиратор камер слежения

Резкий скачок спроса на технологии промышленного шпионажа и инструментарий папарацци с пересылкой данных или компромата на удаленный сервер стимулирует разработку средств защиты клиента, которыми он сможет воспользоваться не только на дому, но и в командировке, на отдыхе, в библиотеке и т. п.

Разработка конструкторов из штата Джорджия позволит не только просканировать незнакомое помещение на предмет наличия скрытых камер слежения, но и заблокировать их работу при помощи специального теплового или светового источника (за счет перенасыщения ПЗС-матрицы камеры).

Суть технологии предельно проста. Высокочувствительная оптическая система в импульсном или непрерывном режиме сканирует помещение, фиксируя блики от объективов скрытых камер, и включает засветку источником инфракрасного диапазона, вращающимся или неподвижным, с использованием обычной лампы накаливания, импульсного светодиода или даже лазера. В результате подсматривающий получает изображение типа «яркое солнце на ночном небе» (если, конечно, камера не оборудована спецфильтром инфракрасного наблюдения).



Система способна заблокировать камеры на удалении до 10 м. Практическая демонстрация блокиратора состоялась на International Conference on Ubiquitous Computing в Токио.

Сетевой телевизор для цифрового дома

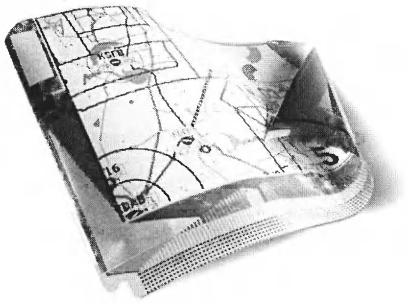
AT3705W-MGW от Acer — не просто ЖК-телевизор, который можно использовать как дисплей. Он еще поддерживает Ethernet 10/100 Мбит/с и беспроводную сеть Wi-Fi (802.11b/g). Мультимедиа-шлюз (Media Gateway) MG-3001P, встроенный в AT3705W-MGW, работает под управлением Linux и обеспечивает воспроизведение файлов в форматах LPCM, WAV, MP3 и Windows Media Audio 7, 8, 9; MPEG 1, 2 и 4, DivX, XviD и Quicktime MPEG4; позволяет просматривать JPEG, TIFF, BMP, GIF и PNG, а также позволяет загружать контент в режиме реального времени, например, с использованием сервиса Live365.

Диагональ 37 дюймов, разрешение 1920x1080, контрастность 800:1, время отклика 12 мс, угол обзора 176 градусов по вертикали и горизонтали, поддерживаемые стандарты — PAL/SECAM.

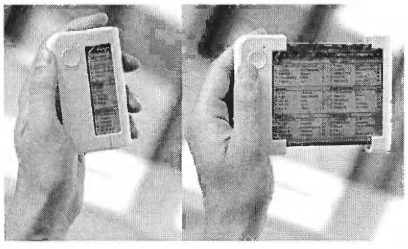
Стоимость AT3705W-MGW в Европе — 2300 евро.

Гибкий экран Readius

На выставке Internaionale Funkausstellung-2005 (IFA) в Берлине Philips в партнерстве с компанией E-Ink продемонстрировала новый гибкий экран Readius, который можно свернуть в трубочку и положить в нагрудный карман. Дисплей использует технологии



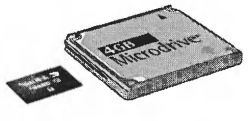
«электронных чернил» (E-Ink), работает в режиме gray-scale. Габариты экрана 100x127 мм, разрешение 320x240 точек.



По словам разработчиков, в состав экрана «для чтения» могут быть встроены высокоскоростные кабельные (USB, FireWire) и радиоканальные интерфейсы (Wi-Fi), что превратит его в компактный информационный таблоид, на который пользователю будет оперативно сбрасываться интересующая его информация (например, оптимальные маршруты движения по городским магистралям, карты местности и снимки GPS-позиционирования). Однако Интернет-аудитория уже нашла ему более перспективное применение (в комплекте с Wi-Fi) — в качестве шпаргалки, которой с легкостью смогут воспользоваться ленивые студенты.

Сверхминиатюрный накопитель емкостью 4 Гбайт

Компания SanDisk разработала флэш-накопитель iNAND (на фото слева, для сравнения справа — MicroDrive). При размерах 12 x 18 x 1,4 мм вес накопителя — всего два грамма. Его предполагается использовать в качестве альтернативы миниатюрным винчестерам в карманных компьютерах, мультимедийных мобильных телефонах, медиаплеерах и т. п.



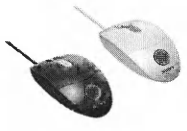
Накопитель построен по технологии многоуровневых ячеек MLC (Multi-Level Cell) и снабжен последовательным интерфейсом. В линейке iNAND представлены модели на 256 и 512 Мбайт, 1, 2 и 4 Гбайт.

Скорость чтения информации составляет 9 Мбайт/с, скорость записи — 5 Мбайт/с. Диапазон рабочих температур — от -25 до 85°C. Максимально допустимая нагрузка в рабочем режиме — до 1000 g.

Массовое производство запланировано на четвертый квартал нынешнего года. Оптовая цена — $95.

Мышь, способная читать электронные карты

Новое семейство мышей с лазерным «прицелом» от Sony отличает высокая точность позиционирования (свыше 800 dpi) и способность быстро считывать и загружать в компьютер данные 6 типов популярных электронных карт: SD, MiniSD, Memory Stick, Duo, PRO, PRO Duo.



Мыши обеспечены интерфейсом USB-2 и набором системных драйверов, обслуживающих популярные форматы персональных хранилищ данных.

По словам разработчиков, узел лазерного считывания координат усовершенствован настолько, что работоспособность мышки гарантируется даже на зеркальном столике.

Для удешевления конструкции Sony отказалась от использования радиоинтерфейса, и новые мыши не потеряли своего стандартного полутораметрового хвоста.

Hitachi увеличивает емкость своих HDD-малюток

Hitachi Global Storage Technologies Inc. подготовила к выпуску новую линейку малогабаритных HDD формфактора 1 дюйм. Их емкость составит 6-8 Гбайт, реальные размеры снижены на 20%, а средний уровень энергопотребления — более чем на 40%.

HDD-малютки ориентированы на использование в портативных MP3-плеерах, диктофонах и средствах сотовой связи. В составе этих HDD использованы новые аппаратные и программные решения. Например, Extra Sensory Protection фиксирует состояние «невесомости» при свободном падении за несколько миллисекунд, предотвращая удары магнитных головок о поверхность вращающегося диска.

По словам разработчиков, Extra Sensory Protection успеет припарковать головки работающего HDD при его падении даже с высоты порядка 10 сантиметров.

В семействе HDD 1,8 дюйма также снижены габариты и увеличена емкость до 30-60 Гбайт.

В следующем году Hitachi намерена представить новые версии малюток и «середнячков», емкость которых увеличится до 10 и 80-100 Гбайт соответственно.

Принтер за миллион долларов

Компания IBM представила общественности очередную разработку — суперпринтер Infoprint 4100, способный печатать текст со скоростью 330 страниц в минуту! Для сравнения: новинка способна распечатать роман Л.Н.Толстого «Война и мир» за одну минуту.

Однако устройство не лишено недостатков — чрезвычайно высокая стоимость: вариант «начального класса» оценивается в 500 тыс. долларов, а «топовая» модель — в 1 млн долларов. Но несмотря на заоблачные цены, принтер уже заинтересовал ряд крупных банков, телефонных операторов и государственных служб, которые печатают несколько сотен миллионов страниц в год, и высокая скорость печати означает для них колоссальную экономию времени и средств.

Джеймс Бонд о таком и не мечтал

Четверо американских изобретателей разработали миниатюрный микрофон, который крепится на зуб как обычная пломба. Новинка выручит, когда невозможно использовать стандартные микрофоны в очень шумных местах (например, на взлетно-посадочной полосе аэропорта). «Зубной» микро-

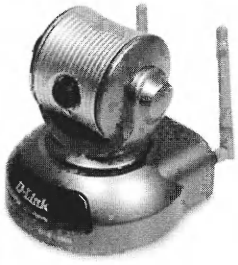
фон хорошо защищен от воздействия внешней среды и прекрасно улавливает речь. Микрофон способен стабильно работать при уровне внешнего шума до 160 дБ (что громче звука взлетающего самолета), а также в случае использования, например, противогаза.

Устройство представляет собой чувствительный элемент, помещенный в полимер. Этот элемент передает низкочастотный сигнал более мощному передатчику, встроенному в корпус наушников. Микрофон (его, конечно, можно снять в любой момент) включается языком при помощи миниатюрного переключателя.

По словам изобретателей, в устройстве может быть также реализована криптографическая защита переговоров.

С камеры наблюдения — в сотовый телефон

Для боссов, которые хотят наблюдать за подчиненными, находясь за пределами своего офиса, компания D-Link выпустила новую беспроводную камеру наблюдения Wireless Internet Camera, оснащенную 3G-функциями. Иными словами, хозяин получит возможность комфортного наблюдения и приема потокового видео прямо на свой сотовый 3G-телефон.



Разместить камеру можно в любом месте, соединив с компьютерной сетью проводами (через Ethernet-порт) или посредством беспроводной сети 802.11g/b. Принимать изображение можно в реальном времени и из любого места, где присутствует телефонная 3G сеть.

После должной авторизации доступ к видеоизображению можно получить и с любого компьютера, подключенного к этой сети. В комплекте с камерой поставляется пакет Windows-приложений, позволяющий работать с 16 такими камерами с одного компьютера.

Веб-камера с углом обзора 200 градусов

Компания Creative выпустила веб-камеру WebCam Live! Motion, оснащенную электроприводом, который автоматически поворачивает объектив. Фирменное ПО Smart Face Tracking отслеживает положение пользователя и поворачивает камеру таким образом, чтобы человек всегда оставался в поле зрения широкоугольного объектива. В итоге углы обзора по горизонтали и вертикали достигают 200° и 105° соответственно.

В камере применена 0,3-мегапиксельная ПЗС-матрица (возможна программная интерполяция до 1,3 млн пикселов). В режиме видеоконференций разрешение составляет 640 x 480 точек при частоте 30 кадров в секунду.

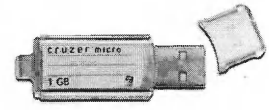
Creative гарантирует совместимость модели WebCam Live! Motion со всеми популярными интернет-пейджерами, в том числе Yahoo Messaging, AOL Instant Messenger, MSN Messenger и Windows Messenger.

Для работы с новинкой потребуется компьютер на базе процессора с тактовой частотой не ниже 700 МГц, 128 Мбайт оперативной памяти, 100 Мбайт свободного пространства на жестком диске и операционная система Microsoft Windows 2000/XP. Соединение с ПК осуществляется посредством порта USB 2.0 (совместим с USB 1.1).

«Умный» USB-привод

На выставке DEMOfall компания SanDisk представила Cruzer Micro — «умный» привод USB, выполненный по технологии U3. Крошечный привод размером с брелок представляет собой мощную платформу, позволяющую пользователям сохранять и управлять своим персональным рабочим пространством, включая файлы, программы, пароли и настройки.

Умные приводы совместимы с любым ПК под управлением Windows XP или 2000. При отключении привода от ПК на нем не остается никакой персональной информации о пользователе. Приводы смогут запускать разнообразные U3-совместимые программы, прозванные «U3 smart», включая антивирусы, программы защиты информации, проигрывания аудио и видеофайлов. Возможности Cruzer Micro достаточны также для больших файлов, цифровых фотографий, графических презентаций.



Cruzer Micro будут поставляться с двумя предустановленными U3-совместимыми программами. Первая, CruzerSync, разработана французской компанией Dmailer и предназначена для синхронизации почтовой программы Outlook, календаря, персональных документов. Она позволяет получать, редактировать и отправлять почту с любого компьютера, даже если на нем не установлена почтовая программа Outlook.

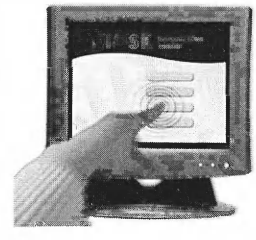
Вторая программа SignupShield Password Manager разработана компанией Protecteer of Bedford и предназначена для хранения паролей в зашифрованном виде, поддерживает браузеры Internet Explorer и Firefox.

Наконец, приводы Cruzer Micro можно использоать в качестве обычной флэш-памяти.

Cruzer Micro емкостью 512 Мбайт и 1 Гбайт поступят в продажу в США в октябре по цене $55 и $100 соответственно.

Сенсорный экран с изменяемым рельефом

На выставке Global Gaming Expo (G2E) в Лас-Вегасе компания Immersion Corporation продемонстрировала новую технологию TouchSense, которая предполагает возможность изменения рельефа поверхности дисплея. На таком экране, например, помимо изображения кнопки может быть воссоздана ее форма, причем в момент нажатия пользователь почувствует ход клавиши. Таким образом,



по замыслу разработчиков, TouchSense позволит воссоздать полную иллюзию того, что человек взаимодействует не с компьютерным изображением, а с реальным объектом.

Такие дисплеи, по замыслу разработчиков, должны найти применение, прежде всего, в игровых автоматах в казино. Не исключено, что в перспективе TouchSense-дисплеи будут востребованы и в других областях, например, в сфере автомобилестроения или военной промышленности.

ЖК-экран с солнечной батареей

Motorola предложила способ экономии расхода электроэнергии экранами, используемыми в мобильных телевизорах, PDA и сотовых телефонах.

Как известно, в обычных ЖК-экранах имеется набор из маленьких красных, зеленых и синих фильтров и белая подсветка. Фильтры поглощают много света, в силу чего подсветка должна быть очень яркой. Motorola предложила использовать монохромный ЖК-экран без фильтров. Благодаря этому в ЖК-экране до 70% рассеивающегося света беспрепятственно проникает сквозь экран и слой органических светодиодов до нижней панели экрана, где располагается солнечный элемент, подзаряжающий аккумулятор.

В обычном режиме такой экран отображает серую картинку, а при необходимости включается цветное изображение, формируемое органическими светодиодами красного, синего и зеленого цветов. Экран обновляется с частотой, в три раза превышающей нормальную частоту.

Цифровая камера с принтером

Австралийская компания Silverbrook Research разработала новый способ получения мгновенных фотографий, наподобие известного Polaroid. Теперь нет необходимости приобретать фотоаппарат Polaroid с упаковкой специальной бумаги для получения мгновенных фотографий. Желающим компания выдаст на прокат цифровой фотоаппарат с разрешением матрицы 1,5 мегапикселов, оснащенный встроенным цветным принтером разрешением 1600 dpi.

Принтер изготовлен из специальной составной кремниевой пластины, совмещенной с тремя резервуарами под цветные чернила. Привод подает бумагу, и на выходе пользователь получает цветную фотографию размером с почтовую открытку. Кроме того, получаемое цифровое изображение поддается редактированию и цифровой обработке.

Возвращенные фотокамеры восстанавливаются путем очистки памяти, перезарядки аккумуляторов и добавления новой бумаги и чернил в принтер.

Фотовьюер Epson P-4000

Компания Epson представила обновленную версию своего устройства P-2000, предназначенного для просмотра фотоизображений. Основные новшества P-4000 — это жесткий диск емкостью 80 Гбайт и батарея большей емкости. Фотоснимки загружаются в него из фотокамеры посредством карт памяти (поддерживаются два формата — CompactFlash II и SD).

Устройство позволяет просматривать даже изображения, сохраненные в форматах RAW или TIFF, а также дает доступ к EXIF-информации. А возможность воспроизводить MPEG-2/4 видео, музыку в форматах MP3 и ACC превращает обычный фотовьюер в полноценный медиаплеер. Розничная цена новинки — около $650.

ТВ-тюнер размером с брелок

Немецкая компания TerraTec Electronic разработала USB ТВ-тюнер, позволяющий смотреть телепередачи на ПК или ноутбуке без внутреннего тюнера. ТВ-тюнер очень напоминает обычный flash-брелок, однако памяти он не содержит, так как предназначен исключительно для приема аналогового и цифрового телевещания.

Новинка может работать даже без телевизионной антенны, хотя качество будет выше, если использовать входящую в комплект антенну или присоединить тюнер к домашней антенне через специальный адаптер. Стоимость новинки $200.

Сотовый телефон для правоверных мусульман

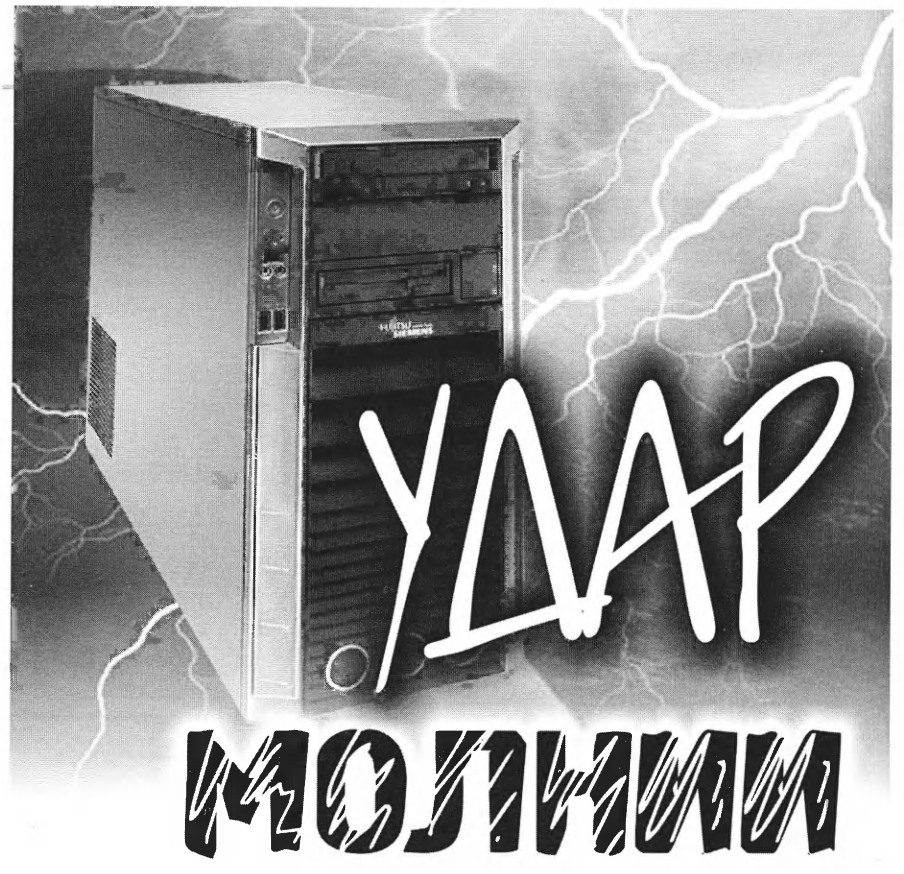
Компания-производитель средств связи и бытовой техники в ОАЭ выпустила первый в своем роде телефон для мусульман. В нем содержится полная версия Корана на арабском и английском языках, электронный компас, указывающий направление на Мекку, а также система звукового оповещения верующих о наступлении времени для совершения молитвы. Телефон продается уже и в Европе ($356).

«Агент 007» в спичечном коробке

Компания Nakomatsu Electronics анонсировала свою новую разработку — цифровую камеру-брелок «Agent 007», которая умеет фотографировать, снимать видеоклипы, работать в режимах веб-камеры и флэш-накопителя.

Несмотря на свои миниатюрные размеры (со спичечный коробок) и вес (около 60 г), «Agent 007» оснащен матрицей с разрешением 2 мегапиксела. Специальная технология LiteSync, впервые использованная в этой камере, позволяет фотографировать без вспышки при искусственном освещении. За счет SD-карты можно увеличить память до 512 Мбайт и снимать видеофильмы продолжительностью около 1 часа.

В России камера будет стоить не дороже $90.



УДАР МОЛНИИ

Николай Богданов-Катьков (С.-Петербург)

В пору питерских летних гроз молния развалила надвое старую липу на Сампсоньевском проспекте, но это еще полбеды: одиннадцать компьютеров в офисе расположенной рядом фирмы отказались работать.

Меня пригласили на роль консультанта и оценщика. Если опустить душераздирающие детали переговоров, сухой остаток окажется следующим.

1. Убиты все 12 сетевых фильтров.

2. Блоки питания погибли у 10 компьютеров из 11.

3 В восьми случаев погибли системные платы (процессоры уцелели).

4. Погибли все четыре модема, а заодно телефакс и единственный на всю фирму многофункциональный центр (МФЦ). Полная стоимость оборудования, вышедшего из строя, составляла около $10000, но косвенные убытки от невозможности заключать сделки, посылать отчеты в налоговую инспекцию и т. п. грозили перевалить за $1000 в день...

По результатам переговоров с десятком ремонтных фирм выяснилось, что «мертвые» блоки питания можно привести в чувство заменой и перепайкой нескольких диодов. На трех системных платах можно вставить новые развязывающие конденсаторы, что много дешевле, чем покупать новые платы. По приблизительным подсчетам ущерб оказался меньше ожидаемого — в сумме около $1600.

И все же, что можно сделать, чтобы это не повторилось?

Первым делом я выяснил, что фирма «кормилась» электричеством не от обычной городской сети, кабели которой пролегают под землей, а от подстанции, расположенной неподалеку. Фирма поставила собственный трансформатор (6 кВ, 220 В). Это оказалось выгоднее (примерно на 20 копеек за киловатт-час), но подводящий кабель висел на столбах и, естественно был подвержен всем условиям погоды — от сильного ветра до удара молнии.

При ударе молнии вблизи токонесущих частей (кабелей, шин), в сети возникает электрический импульс, обычно весьма мощный, способный вывести из строя любой блок питания.

Это и произошло; электрический импульс «убил» 11 компьютеров, хотя все они были подключены к сетевым фильтрам... Почему?

Любой защитный фильтр имеет ограничения по максимальной мощности помех (от 100 до 600 Дж) и по максимальному напряжению (от 2000 до 10000 В). Именно эта помеха и гасится конденсаторами и варисторами, все остальное, что сверх того, проходит через фильтр и бьет по блоку питания.

Защитная мощность сетевых фильтров, как правило, оказывается вполне достаточной, чтобы отсечь обычные помехи, возникающие при нестабильной работе электрических сетей, но в экстремальной ситуации — удар молнии — ее не хватило.

Что можно сделать?

Работники конторы клялись, что все электрооборудование, включая чайник, было заземлено! Если это так, то никакая молния не была бы способна повредить технике. Да, если...

Во всем мире для питания любой сети используется переменный ток. В России его напряжение — 220 В (+10/-15%), то есть от 187 до 242 В, частота 50 +/-1 Гц. Таково требование ГОСТа, но на практике это не всегда бывает так.

Неучтенная ГОСТами составляющая — высокочастотные импульсы. Если из нормальных 220 В вылетит импульс вольт в 2000 и мощностью более 500 Дж, то обычный сетевой фильтр его легко отсечет; на компьютере это никак не скажется. Но удар молнии намного превысит эти параметры, и в данном случае никакие фильтры не спасут.

Чтобы обеспечить нормальное питание, применяют UPS, то есть устройства непрерывного электропитания, хотя от молнии не спасут и они.

Это российский (и европейский) стандарт; в Америке широко используются устройства, рассчитанные на напряжение 110 В, а обычная американская частота — 60 Гц. В Японии стандарт напряжения 100 В, но есть и много стран с напряжением 240 В, а потому БП компьютеров рассчитаны на напряжение от 90 до 265 В.

Еще недавно в Россию поставляли технику, рассчитанную на 110 В, естественно, ее комплектовали трансформаторами.

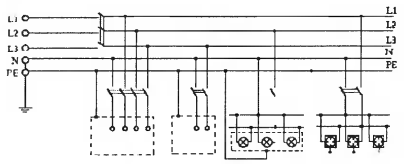
Сейчас вариант заземления, который основан на так называемых «евровилках», часто не работает. Беда в том, что в России традиционно используют двухполюсные вилки и розетки, двухжильные провода. По ним подается «фаза» и «ноль», причем вилка симметричная.

Конечно, удар молнии — это стихия, и здесь никто никаких гарантий дать не может, однако единственный пока способ защиты — заземление.

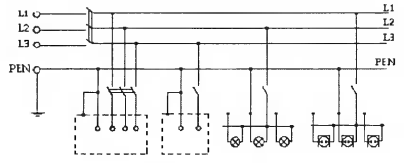
Формально заземляющая жила прокладывается отдельно от собственно электропроводки и замыкается на землю; обычно в подвале здания бурится шпур на глубину в несколько метров, в него погружают стальную болванку, а свободное место засыпают углем для лучшей электропроводности. Это самый безопасный вариант из возможных. Но надо считаться с реалиями. Частному пользователю редко доступен подвал, он может делать лишь то, что в пределах его квартиры.

Прежде всего, необходимо подвести проводку к евророзеткам трехжильным кабелем. Третью, «земляную», жилу следует именно занулить, а не заземлить. Наилучший вариант — «нулевая» клемма домового распределительного щитка.

Довольно распространенный в бытовых условиях вариант — подключение к батарее парового отопления, или же к водопроводной трубе (но не к газовой — вас оштрафует первая же проверка). Водопроводная труба предпочтительнее, так как по нормам варить-менять их можно только при условии сохранения электрического контакта в месте ремонта, а для труб отопления этого не требуется.



Система TN-S — так устроена электросеть в большинстве стран, в Москве и Питере она применяется в основном в новых домах



Система TN-C-S используется путем преобразования системы TN-C разделением рабочего нуля PEN на PE и N на участке до первого коммутационного щита. Достаточно на квартирном щитке до входного автомата или выключателя подключить провод к нулевой шине, и он станет защитным проводом PE

В принципе, все трубы обеспечивают почти идеальный контакт с землей (слабое место — резьбовые соединения). Тем не менее, это формально запрещено, да и небезопасно. Если ниже вашей квартиры поставили пластиковую трубу, никакого заземления не получится, а у соседей появится почти половина от 220 В на оставшихся металлических трубах. Не смертельно, поскольку ток идет от конденсаторного делителя в БП, но щекотно будет.

Корпоративным пользователям лучше установить общую заземляющую шину с выходом на нулевую клемму и со всеми требованиями, предусмотренными ГОСТами. Еще лучше — заказать соответствующий проект компетентным фирмам. Проектирование систем электробезопасности требует соответствующей лицензии, что и понятно, всякое дело нужно поручать специалистам.

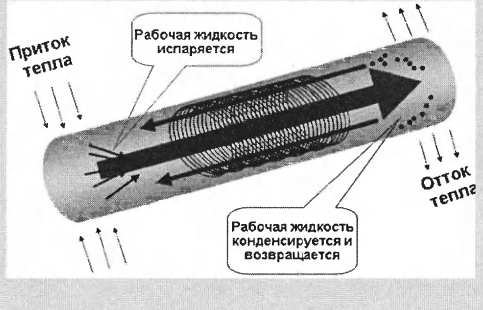
Каждый решает сам, но оставлять компьютеры безо всякой защиты — накладно.

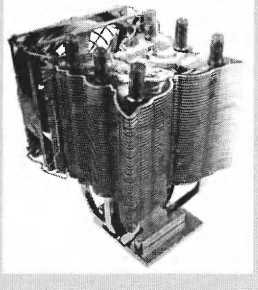
Тепловые трубки

Современный процессор выделяет 110-120 Вт, да и остальные компоненты системного блока греют себя и своих соседей. Звуковая карта нагревает конденсаторы на системной плате, винчестер — расположенный рядом «флоповод», а микросхемы оперативной памяти греют весь системный блок. В результате на платах пересыхают конденсаторы, винчестер перегревается, на нем чаще появляются bad-блоки, а блок питания работает в нештатном режиме — 50-60 градусов.

Приходится искать радикальные средства для охлаждения системного блока.

До недавнего времени модной темой были водяные системы охлаждения. Значительное их достоинство — они не разгоняют тепло по корпусу, а выводят его вовне. За это приходится платить и деньгами (немалыми!), и неудобствами: внешний модуль радиатора весит 5-6 кг и его нужно куда-то поставить.





Альтернативный и, похоже, более перспективный вариант — радиаторы с тепловыми трубками.

Теплопроводящая трубка представляет собой полую медную трубку, которая в вакуумной среде заполняется жидкостью и запаивается с обеих сторон. Рабочая жидкость переносит тепло от одного края трубки к другому с более высокой скоростью, чем если бы тепло распространялось через медь (примерно в 10 раз). Чаще всего в качестве рабочей жидкости применяют спирт, ацетон или аммиак. Данный хладоагент (им может быть даже обычная вода) циркулирует между нагреваемой и охлаждающей поверхностями. На нагретой он испаряется, отбирая тепло, на холодной — конденсируется, отдает тепло и стекает обратно.

Фирма AVC (Asia Vital Components) уже полностью перешла на такие радиаторы. Подобные же системы на теплотрубках уже делают ASUS, Titan и другие фирмы.

Николай Богданов-Катьков

БЕЗОПАСНОСТЬ Linux vs. Windows

Михаил Емельченков (г. Красногорск)

Безопасность — постоянная забота системных администраторов. Попробуем сравнить с этой точки зрения две наиболее популярные операционные системы — Linux и Windows.

Существует множество версий операционных систем Windows — Windows 95/98, Windows NT/2000, Windows XP, Windows 2003 Server. Дистрибутивы Linux отличаются версиями ядра (2.2, 2.4, 2.6) и версиями поставляемых с ними пакетов программного обеспечения.

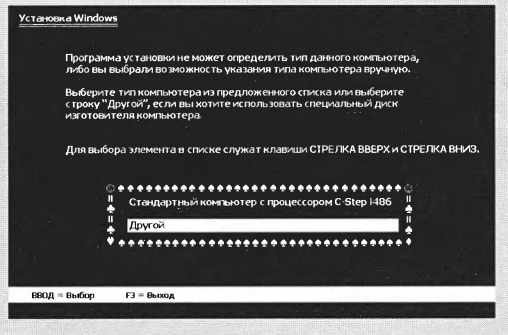
Надо понимать, что существует фундаментальное различие между архитектурой Linux и Windows. Windows разработана таким образом, что в ее ядре сосредоточена большая функциональность, позволяющая глубже интегрировать приложения в ядро. Linux отличается от Windows тем, что в ней присутствует разделение между ядром и прикладным ПО. Это имеет большое значение, потому что безопасность ОС зависит от ее архитектуры.

Растущая популярность Linux заставила Microsoft вкладывать гораздо больше ресурсов в безопасность Windows. Несомненным прогрессом в этой области можно считать выпуск Service Pack 2 для Windows XP. Этот пакет усиливает безопасность Windows посредством отключения некоторых сервисов по умолчанию, а также добавляет несколько новых security-инструментов, таких как улучшенный брандмауэр Windows. В большинстве случаев отключение сервисов делает систему в целом безопаснее, но не стоит это делать в ущерб гибкости или функциональности.

Microsoft сконцентрировалась на усилении безопасности через повыше-

Windows XP: ядерная война

Вскоре после появления на рынке финальной редакции Microsoft Windows XP на многочисленных тематических форумах в Интернете стала появляться любопытная информация. Суть публикаций сводилась к следующему: если на начальном этапе установки системы, в процессе тестирования устройств, когда на экране отображается надпись «Программа установки проверяет конфигурацию оборудования» (Setup is inspecting your computer's hardware configuration), нажать клавишу F5, то программа установки покажет удивительное диалоговое окно.



Одни пользователи утверждали, что, выбирая в данном меню пункт «Стандартный компьютер с процессором C-Step i486», можно добиться значительного прироста производительности Windows XP. В качестве объяснения этого явления авторы выдвигали следующую теорию: дескать, коварные разработчики из Microsoft вступили в тайный сговор с производителями процессоров и прочего компьютерного «железа». Как результат, программисты намеренно тормозят работу Windows, чтобы стимулировать людей к покупке новых компьютеров, а выбор режима установки для процессоров серии C-Step i486 позволит вернуть все на свои места. Следуя этой логике, Windows, якобы, будет считать, что она работает на очень медленной машине — отсюда и резкое возрастание быстродействия.

Другие пользователи предлагали своим оппонентам не молоть чепухи и заняться вместо этого чем-нибудь полезным, например, сбегать в магазин за пивом, а еще лучше — за дополнительной «линейкой» оперативной памяти, либо дефрагментировать, наконец, жесткий диск, что приведет к росту производительности гораздо быстрее, нежели попытка «обмануть» Windows.

В специализированных конференциях разгорались горячие дискуссии, порой перераставшие в самую настоящую войну между сторонниками противоречивых версий. Не удовлетворяясь голословными аргументами, противники провели множество практических исследований с использованием различных специализированных программ, позволяющих определить быстродействие компьютера и операционной системы. Кто-то действи-

ние удобства работы. Вспомним, что появление нескольких эксплоитов в 2003 году вылилось в эпидемию e-mail-вложений, рапространяемых как исполняемый файл (например, MyDoom). Service Pack 2 вводит специальный сервис для обработки вложений Outlook/Exchange, Windows Messenger и Internet Explorer вместо того, чтобы исправлять неработающую инфраструктуру и безопасность коммуникаций. В Linux подобного никогда не происходило.

Service Pack 2 внес много нововведений для пользователя Windows, но все равно обеспечение безопасности лежит на плечах системных администраторов и пользователей Windows, а не обеспечивается исходным кодом системы.

Фундаментальное различие между Linux и Windows состоит и в моделях лицензирования. Linux лицензируется под GNU General Public License, которая дает возможность пользователю копировать, изменять и распространять исходный код. Windows же, напротив, — закрытая ОС, безопасность которой обеспечивается недоступностью исходного кода. Правда, в 2001 году Microsoft открыла часть кода Windows для своих партнеров. Некоторые нашли это полезным для отладки приложений и, таким образом, обеспечения большей безопасности.

Скрытая угроза безопасности Windows — мнимая простота администрирования. Как известно, в Windows все действия по настройке и эксплуатации ОС выполняются с помощью графического интерфейса, а в Linux — с помощью командой строки (шелла). Графический интерфейс подкупает своей простотой, позволяя администрировать систему даже новичку, не обладающему глубокими знаниями в вопросах обеспечения безопасности. Этим он подвергает риску не только администрируемую систему, но и финансы компании, нанявшей такого системного администратора.

Еще одно фундаментальное различие Windows и Linux — в их принципе построения. Windows — монолитная, а не модульная система, в отличие от Linux. По сути это означает, что слишком много компонентов интегрировано в ядро Windows. Например, интеграция в ядро Internet Explorer скрывает в себе потенциальные дыры в безопасности всей системы. Или, скажем, интеграция подсистемы рендеринга изображений в ядро при ее крахе приведет к краху ядра в целом, а не отдельной подсистемы. Монолитная структура нестабильна по своей природе. Каждая подсистема такого ядра имеет множество зависимостей, и при ее модификации приходится следить за всеми зависимостями, что, естественно, довольно трудно.

Сетевая безопасность и протоколы

И Linux, и Windows включают IPSec как отрытый стандарт криптографической защиты IP-протокола. IPSec проверяет, не было ли каких модификаций передаваемой по сети информации, и шифрует ее. OpenSSH, OpenSSL и OpenLDAP реализованы на Linux, их закрытые реализации SSH, SLL и LDAP — на Windows.

Безопасность приложений

Linux превосходит Windows в вопросе безопасности приложений, особенно отмечал прирост производительности, но при этом упоминал, что Windows стала работать «как-то не так», тогда как другие не замечали решительно никакой разницы. В конечном итоге данный вопрос так и оставался открытым.

Тем не менее, никакого секрета в данном случае попросту нет. Упомянутое выше диалоговое окно, доставшееся вполне современной операционной системе «в наследство» еще от Windows NT, всего-навсего позволяет выбрать тип ядра, с котором Windows будет работать впоследствии. Эксперименты с установкой различных версий ядра и подсистемы уровня аппаратных абстракций (HAL, Hardware Abstraction Layer) проводились пользователями и на более ранних версиях NT-совместимых платформ. Другой вопрос, сможет ли замена стандартного ядра Windows XP повлиять на производительность операционной системы в целом? Давайте разбираться.

Для начала следует определиться с терминологией. Ядро операционной системы — это набор элементарных функций (примитивов) и процессов, на которых, как на фундаменте, строится все остальное «здание» ОС. С практической точки зрения ядро реализует такие задачи, как запуск приложений, распределение ресурсов оперативной памяти и процессорного времени между различными программами, управление прерываниями и системными функциями, обеспечение взаимодействия с устройствами при помощи драйверов, и т. д.

Уровень аппаратных абстракций (HAL, Hardware Abstraction Layer) — это один из компонентов операционной системы, обеспечивающий поддержку таких модулей, как драйверы устройств низкого уровня, диспетчер ввода-вывода, отладчики ядра и т. д. При этом подсистема HAL позволяет ядру Windows абстрагироваться от конкретных аппаратных интерфейсов, что обеспечивает высокую степень независимости компонентов системы от особенностей различных аппаратных платформ. Вполне естественно, что выбор ядра и подсистемы HAL во многом определяется конфигурацией компьютера, на котором будет работать операционная система. Например, для однопроцессорных и двухпроцессорных компьютеров используются различные версии ядра и HAL, изделия некоторых компаний-производителей, таких как, в частности, Compaq, также иногда требуют установки специально разработанного для них ядра, хотя в большинстве случаев операционная система прекрасно функционирует на подобных машинах и в стандартной конфигурации.

В обычных условиях программа установки Windows XP автоматически выбирает наиболее подходящие для данной аппаратной платформы ядро и модуль HAL. Если в процессе тестирования оборудования на начальном этапе установки Windows XP нажать клавишу F5, процедура определения конфигурации компьютера будет отменена, и вы сможете выбрать ядро вручную.

Вариант «Стандартный компьютер с процессором C-Step i486» подразумевает установку ядра для устаревших однопроцессорных персональных

бенно в связи с постоянными дырами в безопасности Microsoft ISS и Exchange/Outlook. Apache и Postfix — кросс-платформенные приложения, они имеют лучшую защищенность по сравнению с продуктами Microsoft. Безопасность Linux также обеспечивает брандмауэр, встроенный в ядро, и Snort — де факто стандарт систем защиты от вторжения.

Настораживает тенденция Microsoft смешивать данные и код в приложениях. Например, ActiveX приносит непроверенные данные из внешних систем и запускает непроверенный код.

Одна из основных проблем Windows — переполнение буфера. Пользователи Linux оценят возможность использовать защиту от выполнения, появившуюся в ядре Linux 2.6. Она обеспечивает защиту от эксплоитов, которые перезаписывают структуры данных или вставляют код в эти структуры.

Еще одно подспорье в безопасности — использование User-Mode Linux (UML), специального патча для ядра, который позволяет запускать несколько независимых ядер Linux одновременно. Таким образом можно тестировать приложения, не опасаясь за безопасность рабочей системы.

Безопасность пользователей

Windows XP — первая ОС семейства MS Windows, относительно полноценно поддерживающая многопользовательскую работу за ПК. Файлы пользователей отделены друг от друга, и каждый пользователь имеет свои приватные файлы, недоступные для других, а также ограниченные системные привилегии. Функция «Fast User Switching» позволяет работать одновременно нескольким пользователям за одним ПК, но имеет одно существенное ограничение: в таком режиме компьютер не может входить в домен Windows. В Linux многопользовательская поддержка работает с самой первой версии системы.

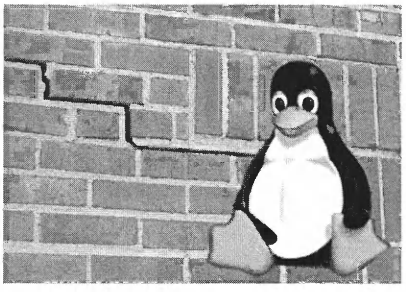
Открытые стандарты

Закрытые стандарты, которые так любит Microsoft, несут в себе потенциальные дыры в безопасности. Об этом свидетельствуют многочисленные вирусы в документах Word и Excel, чего нет в документах Open Office, построенных на открытой модели.

Большое заблуждение — думать, что открытые стандарты и открытый исходный код опаснее закрытого, так как предоставляет возможность злоумышленникам исследовать его. На практике веб-сервер с открытым исходным кодом Apache гораздо популярнее и безопаснее веб-сервера Microsoft IIS. Исследование кода разными людьми позволяет не только найти уязвимости, но и оперативно устранить их.

Вирусы и трояны

И еще одно заблуждение: Windows, якобы, больше подвержена вирусам, троянам, атакам хакеров и т. д. Факты говорят об обратном: если сравнить количество заплаток Windows и Linux, то под Linux их выходит больше. Причиной этого заблуждения стала повсеместная распространенность Windows и, как следствие, больший интерес к ней злоумышленников.



компьютеров, не поддерживающих технологию ACPI.

Спецификация ACPI (Advanced Configuration and Power Interface, расширенный интерфейс конфигурации и управления питанием) — это технологический стандарт, совместно разработанный компаниями Microsoft, Intel, Compaq, Toshiba и Phoenix. Данный стандарт позволяет операционной системе управлять питанием персональных компьютеров, серверов и рабочих станций. Кроме того, именно стандартом ACPI в архитектуре современных компьютеров определяются основные параметры работы периферийных устройств, в частности, назначение ресурсов и прерываний шинам AGP и PCI, управление режимами энергосбережения и т. д. На практике использование данной технологии, во-первых, исключает необходимость установки дополнительных драйверов и программ для обеспечения нормальной работы системы управления питанием, а, во-вторых, позволяет нескольким устройствам использовать одни и те же ресурсы, если эти устройства технологически могут взаимодействовать, не вызывая аппаратных конфликтов.

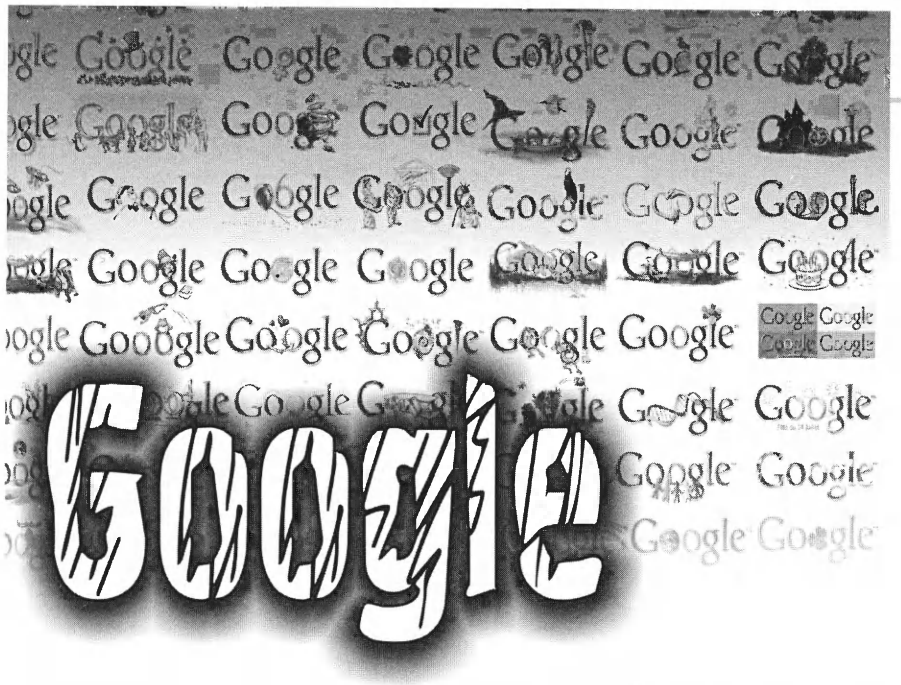
Поддержка технологии ACPI обеспечивается материнской платой компьютера, и следует отметить, что практически все современные материнские платы полностью совместимы с ACPI. Вместе с тем, если ваш компьютер собран на базе процессора Intel Pentium II/Celeron или более ранних моделей процессоров, возможно, что об ACPI вам придется лишь мечтать: даже если материнская плата и совместима с этим стандартом, ACPI может не поддерживаться со стороны BIOS.

В данном случае есть определенный резон для использования нестандартного ядра Windows XP: отказ от поддержки ACPI операционной системой позволит более рационально распределить аппаратные ресурсы между различными устройствами и оптимизировать таким образом их работу.

Тем не менее, за все нужно платить: одновременно с этим вы, скорее всего, лишитесь возможности использовать так называемый «Ждущий режим» (Hibernate) и переводить компьютер в спящий режим (Sleep mode). Возможно, утратится функция программного управления бесперебойными источниками напряжения (UPS). Кроме того, будет заблокирован механизм автоматического выключения питания: после выгрузки операционной системы на экране появится сакраментальная надпись «Теперь питание компьютера можно выключить», как в старом добром Windows 95.

Если же ваш компьютер вполне современный и поддерживает технологию ACPI, в использовании ядра для аппаратной платформы C-Step i486 нет решительно никакого смысла.

Валентин Холмогоров (С.-Петербург)



НА ВСЕ РУКИ

Анатолий Ковалевский (С-Петербург)

Намечается война между создателями известнейшего поисковика и хозяевами самой распространенной ОС. Чем может угрожать Google, оборот средств которой в 10,5 раз меньше? Очевидно, только одним — правильным видением будущего. Именно тем, благодаря чему Microsoft и стала тем монстром-монополистом, с которым приходится считаться всем, хотят они этого или нет.

Напомню, что одной из трех опорных колонн Windows Vista будет Windows Communication Foundation (ранее Indigo) — архитектура, обеспечивающая прозрачное взаимодействие с веб-сервисами и интернет-коммуникациями вообще. Microsoft обещает, что, мол, в Vista будет такой поиск, что никакие Google Desktop и даром не будут нужны, но пока это только обещания.

Google выпустила и продолжает выпускать новые сервисы. При этом многие из них были выпущены раньше, чем у Microsoft, или остаются более функциональными. Бесплатный двухгигабайтный ящик Gmail наступает на мозоль фактически платному Hotmail от Microsoft, к тому же куда меньшего объема; локальные поисковики Google Desktop Search и Google Picasa вышли раньше и работают лучше MSN Desktop и Microsoft Max; Google Talk, Google Toolbar и Google Blogger напрямую пересекаются с MSN Messenger, MSN Toolbar и MSN Spaces, хотя используются на практике куда реже, чем их рендмоновские аналоги. Интерактивная карта земли Google Earth вообще напрямую пересекается с Microsoft Virtual Earth. Мало того, очевидно, что успех Google как поисковика (а искать можно внутри текстов, фильмов, картинок, музыки, блогов, новостных лент) похоронил идею поисковика от Microsoft. К тому же Google смогла запустить службы, которых у Microsoft пока вообще нет — Google Print, Google News, Google Translate, Google SMS, Google Mobile и т. д. (на настоящий момент 29 штук), вот-вот выйдет Google Money и Google WebAccelerator.

Наконец, давно ходят слухи о GoogleOS. Конечно, создать свою ОС сверхсложно даже для мощных корпораций — в этом убедились и IBM с P/S2, и Sun с Solaris, и Be с BeOS, и создатели Lindows (которую после судебных тяжб с Microsoft уже трижды переименовывали). У всех этих ОС остались крошечные доли рынка, к тому же им приходится прикладывать множество усилий к тому, чтобы в их продуктах в обязательном порядке имелись встроенные средства для взаимодействия с ОС семейства Windows. Вряд ли в Google решили повторять чужие ошибки, ведь в руководство компанией входят люди, участвовавшие не в одном споре с Microsoft (в те времена они работали в Sun, Novell, Netscape).

Google вкладывает огромное количество денег не только в сегодняшние проекты, но и «на перспективу». На ее сайте, в разделе «Требуются сотрудники», очень часто появляются довольно странные вакансии для компании, которая занимается поиском, — специалисты по компиляторам, архитекторы ОС... Мало того, Google умудрилась переманить более 100 сотрудников Microsoft, в том числе из высшего менеджмента. Для Microsoft это не только оскорбительно в моральном плане, но и достаточно неприятно в плане утечки информации. И, очевидно, в пику своему сопернику, Google опубликовала принципы добросовестного программного обеспечения (www.google.com/corporate/software_principles.html), в соответствии с которыми программа должна устанавливаться только по желанию пользователя; четко предупреждать, что собирается показывать рекламу или собирать информацию; должна присутствовать возможность деинсталлировать ее в любой момент; программа не должна быть связана с другим программным обеспечением. А на деле получается, что большая часть программ от Microsoft их нарушает — попробуйте-ка, например, удалить Internet Explorer или Outlook!

Так что же будет?

По всей видимости, фактически готовится платформонезависимая операционно-подобная система, которая для пользователя будет выглядеть одинаково что из окна Windows, что из окна Unix. К тому же надо будет тратить минимум сил на соответствие windows-стандартам — достаточно соответствовать международным. Ведь огромному количеству пользователей вполне хватает браузера, почтового клиента, текстового редактора с простейшими возможностями форматирования и плеера для музыки и видео. Поэтому возможно, что Google попытается создать не ОС, а надстройку над ней, которая будет состоять из двух частей:

1. Браузер (G-browser на основе открытого кода Mozilla), обогащенный платформонезависимыми веб-приложениями, — Gmail, Desktop Search, Google Print и т. д.

2. веб-сервер, запущенный на машине пользователя и позволяющий ему работать локально со всеми перечисленными сервисами.

Новые версии популярных программ

Андрей Соловьев (г. Конаково)

Мы продолжаем обзор новых версий популярных программ, которые вышли в сентябре 2005 года.

Интернет

COCO 2.3 beta 4

Данная программа позволяет значительно расширить возможности браузера Opera по сохранению веб-страниц.

Основные возможности:

- Сохранение в различные форматы (chm, rar, zip, 7z, IEFormat), для каждого необходима дополнительная программа-упаковщик.
- Автоматическая подстановка в имя файла заголовка страницы.
- Сохранение в заранее указанную папку без использования диалога («быстрый режим»).
- Быстрый переход к «любимым» папкам.
- Создание специального информационного файла в папке сохранения с комментарием к странице.
- Добавление в код страницы сопроводительной информации (комментарий, адрес, дата и др.).
- Гибкая система макростроек.

Статус: Shareware

Сайт: http://fubus.narod.ru/coco.html

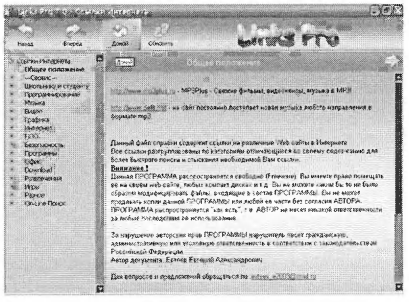
Размер: 180 Кбайт

Язык: русский, французский, английский, украинский, немецкий

Скачать: http://fubus.narod.ru/Download/COCOSetup2.3b4.exe

Links Pro 8.0

Это программа — хранилище ссылок на веб-сайты сети Интернет. Все ссылки удобно структурированы, что позволяет быстро находить необходимую информацию, не обращаясь к поисковым машинам Интернета.



Статус: Shareware

Сайт: http://www.linkspro.narod.ru/

Размер: 853 Кбайт

Язык: русский

Скачать: http://www.linkspro.narod.ru/Linkspro.exe

Cyr2Unicode 1.0

При создании WAP-страниц сталкиваешься с тем, что телефоны не понимают кириллицу в стандартных кодировках (например, Win-1251, cp866). Приходится переводить текст в UTF-8 или Unc-HTML. Первый компактнее (2 байта на символ), второй универсальнее (его понимают абсолютно все телефоны с поддержкой хотя бы WAP 1.2). Программ для перекодировки существует не так много, да и постоянно приходится их вызывать, вставлять текст, копировать результат и т. д. Эта программа работает абсолютно прозрачно! Вам надо лишь скопировать в буфер обмена нужный текст и тут же вставить его обратно, при этом вставится уже сконвертированный вариант! Любой русский текст будет сразу превращаться в буфере в Unicode. Программа поддерживает и обратное преобразование.

Статус: Freeware

Сайт: http://prog-soft.narod.ru/

Размер: 16 Кбайт

Язык: русский, английский

Скачать: http://prog-soft.narod.ru/cyr2unc.zip

Club Admin 5.2

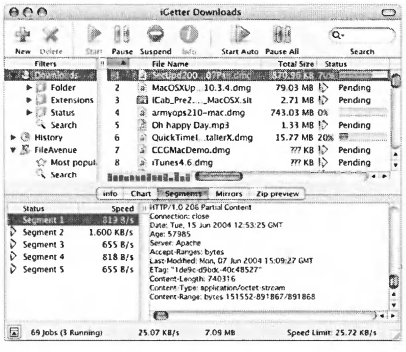
Специально для клубов с Battle Net: блокировка Интернета и подсчет любого трафика. Посчет записи на CD и печати на принтере. Два вида тарифов: динамический (со скидкой в зависимости от времени) и фиксирован-

ный, когда клиент платит за всю ночь или день со скидкой. Работа в режиме сервиса как на клиетах, так и на сервере. Неограниченное количество тарифов. Удаленный контроль за работой клуба через Интернет. Без клиентской части программа может вести точный учет трафика для домашних/офисных сетей.

Статус: Shareware
Сайт: http://clubadmin.jalita.com/
Размер: 3200 Кбайт
Язык: русский
Скачать: http://clubadmin.jalita.com/soft/setup.exe

iGetter 2.0

Многофункциональный менеджер закачек файлов. Поддерживает протоколы HTTP, FTP, HTTPS, SSL. Интегрируется во все распространенные браузеры.



Статус: Shareware
Сайт: http://www.igetter.net/iGetter.html
Размер: 1670 Кбайт
Язык: английский
Скачать: http://www.igetter.net/cgi-bin/downloads/iGetter2.4_En.dmg

NetCom

Программа предназначена для контроля трафика в Интернете или локальной сети, роутинга, протоколирования, контроля скорости, выставления приоритетов (QoS) для различных видов трафика. Есть средства автоматизации (скрипты) и удаленного администрирования.

Статус: Shareware
Сайт: http://www.routix.net/netcom/
Размер: 1800 Кбайт
Язык: английский
Скачать: http://www.routix.net/netcom/files/NetComSetup.exe

HotMailPlus 1.0

Программа предназначена для чтения и отправки электронных сообщений через веб-интерфейс почтового сервера http://www.hotmail.com. Все действия по чтению и отправке электронной почты максимально автоматизированы. Теперь вам не нужно заходить на сайт, чтобы проверить почту. Достаточно нажать кнопку «Проверить почту», и присланные сообщения будут загружены и сохранены. С помощью специального сценария, который был разработан, учитывая структуру сайта http://www.hotmail.com, программа сама делает все нужные действия для просмотра и отправки сообщений: открывает сайт http://www.hotmail.com, авторизуется под вашим именем, заходит на страницу «Входящие», определяет новые сообщения и поочередно открывает каждое, затем отделяет текст сообщения от текста страницы и сохраняет его на вашем компьютере. Все вложения также сохраняются.

Статус: Shareware
Сайт: http://www.hotmailplus.net/
Размер: 603 Кбайт
Язык: русский, английский
Скачать: http://www.hotmailplus.net/hotmailplus.rar

Duplicate Email Remover 2.8.0

Плагин Duplicate Email Remover (DER) предназначен для поиска и обработки (удаления, перемещения, копирования, пометки) дублирующихся почтовых сообщений и записок в папках Microsoft Outlook и в общих папках на сервере Microsoft Exchange. С помощью DER вы сможете найти копии почтовых сообщений и записок, находящиеся как в одной, так и в разных папках. Найденный дубликат сообщения или записки может быть помечен, удален, скопирован или перемещен в нужную папку. Механизм приоритетов позволит вам указать, что из двух одинаковых сообщений или записок, лежащих в

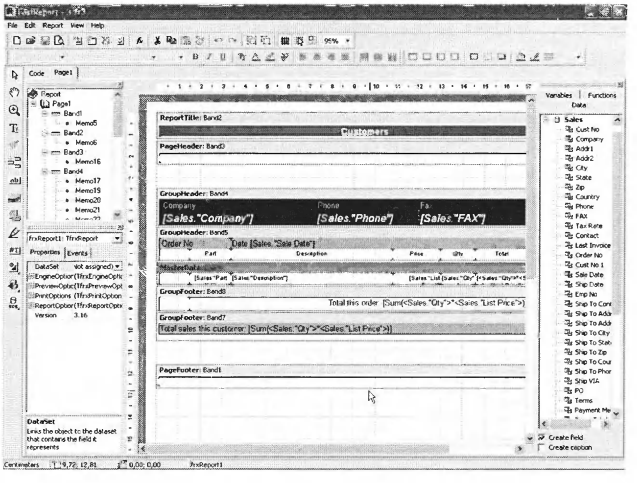
папках, например, «Важные письма» и «Временная папка», надо считать дубликатом. Лишнее можно удалить (пометить, переместить). DER позволит вам с легкостью найти ненужную информацию в папках Microsoft Outlook / Microsoft Exchange Server и избавиться от нее.

Статус: Shareware
Сайт: http://www.mapilab.com/ru/outlook/duplicate_remover/
Размер: 2002 Кбайт
Язык: русский, английский
Скачать: http://www.mapilab.com/files/duplicate_remover.zip

Для программистов

FastReport 3

По аналогии с FastReport for Delphi для Delphi-программистов выпущен FastReport Studio, поддерживающий разработку в MS VisualStudio, FoxPro, и PowerBuilder и т. п. Пакет можно применять как самостоятельное приложение в повседневной работе для формирования практически любых отчетов. Можно создавать как простые отчеты (красиво оформленные данные из таблиц), так и отчеты с многоуровневыми группами, отчеты с отношениями master-detail, перекрестные отчеты, отчеты с вложенными подотчетами, диаграммы и др. Помимо распечатки на



принтере, FastReport Studio поддерживает экспорт отчетов в форматы PDF, RTF, простой текст, HTML, CSV, таблицы Excel, передаваемые с помощью OLE или XML, а также форматы изображений BMP, JPEG и TIFF. К услугам разработчиков мощный API, позволяющий программно управлять созданием отчетов с использованием технологии COM+. В комплект поставки включены подробные примеры использования FastReport Studio из различных сред разработки. Особое внимание уделено разработчикам под .Net. Много возможностей для C# — использование внутреннего подключения к базе данных из приложения, а не из отчета, функция «сумма прописью» и т.п. При этом генератор отчетов очень мал — инсталляционный архив (с примерами) занимает менее 4 Мбайт. (сравните, например, с Crystal Reports, занимающим более 200 Мбайт).

Статус: Shareware

Сайт: http://www.fast-report.com/

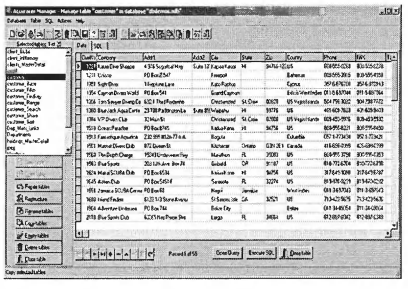
Размер: 4000 Кбайт

Язык: русский, английский

Скачать: http://www.fast-report.com/pbc_download/fr_studio_demo.exe

Accuracer Database System 4.03

Это компактная высокопроизводительная однофайловая встраиваемая файл-серверная/клиент-серверная Windows/Linux кросс-платформенная система базы данных для замены BDE с поддержкой SQL'92 (DML & DDL), транзакций, широким диапазоном настраиваемого сжатия данных с возможностью переключения алгоритмов, большим выбором криптостойких алгоритмов и режимов шифрования. Поддержка транзакций (уровень изоляции — READ COMMITTED); высокая скорость работы (особенно для больших таблиц); быстрая индексная система; in-memory режим для сверхскоростной работы с таблицами в оперативной памяти, используя богатый набор средств SQL; минимальное использование ресурсов оперативной памяти; компактный формат хранения данных на диске. Все таблицы, индексы и метаданные — в единственном файле базы данных. Компактный код добавляется прямо в файл приложения, никаких внешних DLL или других библиотек и модулей. База данных может быть интегрирована внутрь исполняемого файла вашего приложения. Совместимость с TTable, TQuery, TDatabase, TSession, TBatchMove; встроенные средства архивации/восстановления; Reverse engeneering (экспорт таблиц в SQL скрипты); поддержка IProvider (ClientDataset) и групповых операций (BatchMove component); ODBC-драйвер.



Статус: Shareware

Сайт: http://www.aidaim.com/client_server_single-file_bde_replacement_delphi_database_embedded_database.htm

Размер: 3723 Кбайт

Язык: русский, английский

Скачать: http://www.aidaim.com/download/accuracer/accuracer403d7.zip

Операционная система

Super Optimization XP 3.5

Это мощная программа для тонкой настройки и оптимизации производительности операционной системы Windows XP. Утилиты позволяют настроить скрытые установки операционной системы, имеется расширенная настройка меню «Пуск», настройка панели управления, доступ к скрытым настройкам производительности системы, оптимизация соединения с Интернетом, настройка программ и многие другие утилиты.

Статус: Shareware

Сайт: http://comerz.narod.ru/

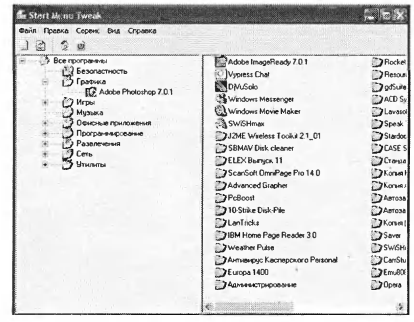
Размер: 535 Кбайт

Язык: русский, английский

Скачать: http://comerz.narod.ru/SOptimizationXP.exe

Start Menu Tweak 2.5b

«Начните работу с нажатия этой кнопки» — знакомая подсказка? Она появляется, там, где «живет» меню «Пуск». Почему «живет»? Потому что



растет. Растет, увеличиваясь в размерах, обрастая тремя панелями, битыми ярлыками и редко используемыми программами. Вам надоело искать нужную программу в зеленом меню «Пуск»? Оно слишком большое и долго открывается? Рассортируйте с помощью Start Menu Tweak ярлыки и папки своих программ в главном меню по категориям, это позволит вам применять схемы. Смена схем меню «Программы» «на лету» позволит вам эффективней использовать меню «Пуск».

Основные возможности:

- сортировка ярлыков и папок из подменю «Программы» меню «Пуск»
- поддержка неограниченного количества схем
- смена схем «на лету»
- смена иконок для папок
- автоматическое построение меню по базе данных
- наличие автозапуска вместе с Windows
- удаление битых ярлыков из текущей схемы

Статус: Shareware

Сайт: http://mipsoft.jino-net.ru/index.php?option=content&task=category&sectionid=2&id=7&Itemid=27

Размер: 951 Кбайт

Язык: русский, английский

Скачать: http://mipsoft.jino-net.ru/startmenutweak2.5b.zip

FileForFiles 2.0

Предположим, что вы просматриваете некий файл, используя Word, Excel, Internet Explorer, Paint, AutoCad или другое приложение, и нашли в нем важную информацию. Выделите ее при помощи мышки. Всего один щелчок, и программа FileForFiles сохранит выделенный фрагмент в общем файле, в персональном для каждого фрагмента или в буфере обмена

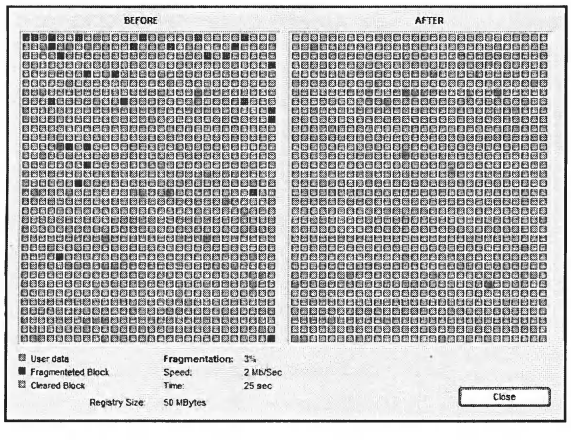
(Clipboard). Ссылка на соответствующий файл будет помещена в специальное меню программы. Открыв его позднее, вы как на ладони увидите эти файлы. FileFofFiles послужит также для создания каталогов, справочников, картотек о файлах, простых баз данных на основе информации из файлов. Есть поиск в содержании файлов по логическому выражению, состоящему из фраз.

Статус: Shareware
Сайт: http://ab.vlink.ru/
Размер: 1482 Кбайт
Язык: русский
Скачать: http://ab.vlink.ru/FFF/FileForFiles.rar

Registry Defragmentation 7.6.9.6

Это утилита для дефрагментации системного реестра Windows 95-XP. Со временем реестр увеличивается, в нем накапливаются неиспользуемые данные, при этом структура реестра становится далека от оптимальной. Дефрагментация системного реестра позволяет увеличить скорость загрузки Windows и уменьшить время отклика программ. Кроме того, программа позволяет создавать резервные копии системного реестра. Работает она практически в автоматическом режиме, позволяя для оптимизации реестра и создания резервных копий использовать планировщик заданий.

Статус: Shareware
Сайт: http://www.elcor.net/rdefrag.php
Размер: 1300 Кбайт
Язык: русский, английский
Скачать: http://www.elcor.net/download/rdefrag-7.6.9.6.exe



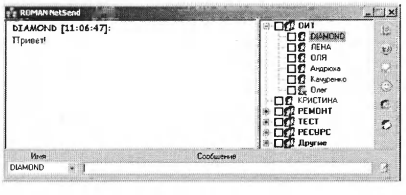
R-Wipe & Clean 5.1

Данная программа поможет удалить бесполезные файлы, освободит дисковое пространство, используя быстрые и безопасные алгоритмы по удалению данных, очистит информацию об онлайн- или оффлайн-активности, удалит временные интернет-файлы, историю, куки, формы автозаполнения и пароли, список открытых документов, MRU Explorer'a, временные файлы и т. д. Конкретные задачи можно выбрать в желаемой комбинации из списка в течение одной процедуры. Поддерживаются браузеры Internet Explorer, AOL, MSN, Opera, NETSCAPE и Mozilla, файловые системы FAT и NTFS.

Статус: Shareware
Сайт: http://www.r-wipe.com/
Размер: 1700 Кбайт
Язык: русский, английский
Скачать: http://www.r-wipe.com/downloads/rwc_en_5x.exe

ROMAN NetSend 4.3.2

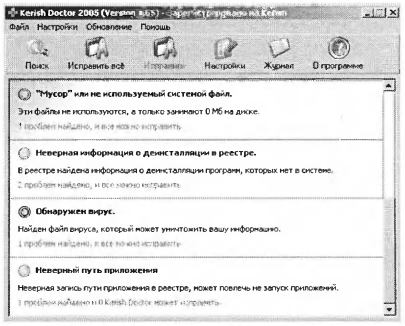
Это многофункциональная утилита, позволяющая по нажатию клавиши Esc закрывать, минимизировать или прятать активные окна. При этом спрятанное окно не видно ни в панели задач, ни в списках по нажатию клавиш Alt-Tab и Ctrl-Alt-Del. Другой вариант, для более аккуратной работы, — устанавливать курсор мыши в правый верхний угол активного окна, где находится кнопка «Закрыть».



Статус: Freeware
Сайт: http://www.roman-efko.narod.ru/
Размер: 700 Кбайт
Язык: русский, английский
Скачать: http://www.roman-efko.narod.ru/download/MyNetSend/RNS_Setup.exe

Kerish Doctor 1.80

Данная универсальная система диагностики



систем Windows постарается заменить вам специалиста. Она поможет в устранении сбоев и множества проблем, удалении вирусов и adware-модулей, а также исправлении некорректных удалений программ, в очистке системы от «мусора». Основные функции:

1. Ищет на всех дисках ярлыки, которые указывают на несуществующие пути. Некорректный ярлык исправляется или удаляется.
2. Ищет на всех дисках файлы с расширениями *.tmp, *.temp, считая их мусором. Все они удаляются по желанию пользователя.
3. Проверяет секцию деинсталляции и ищет ссылки на приложения, которые не существуют и были удалены некорректным способом.
4. Проверяет реестр на наличие ключей, которые используют Adware или Spyware приложения.
5. Проверяет записи в секции автозагрузки реестра. Если существуют записи на приложения, которых нет, то они удаляются по желанию пользователя.
6. Производит эвристический поиск вирусов (по известным путям, которые они создают). Найденные вирусы удаляются по желанию пользователя.
7. Проверяет секцию реестра Microsoft Shared на наличие записей библиотек, которых не существует.
8. Проверяет незначимые секции реестра (типа Shared Tools) на наличие ссылок на несуществующие библиотеки и приложения.
9. Проверяет наличие некорректных шрифтов в системе.
10. Проверяет наличие восстановленных программой ScanDisk потерянных сегментов в директоиях FOUND.***.

Статус: Freeware
Сайт: http://www.kerish.org/

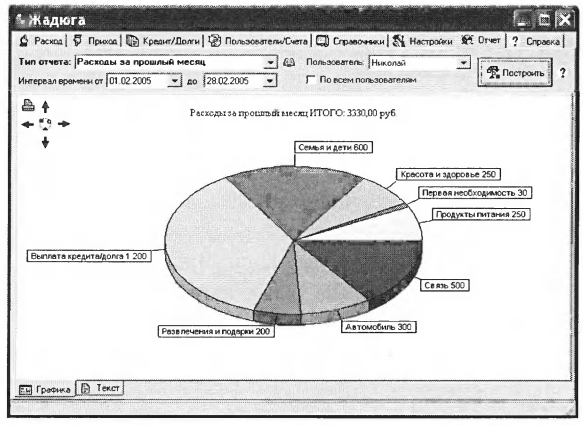
Размер: 1200 Кбайт
Язык: русский, английский
Скачать: http://www.kerish.org/Products/Doctor/Setup.exe

LanSurfer 2.5

LanSurfer предназначен для:

- быстрого многопоточного сканирования компьютеров, расшаренных папок и серверов в локальной сети и составления списка сети, содержащего исчерпывающую информацию о компьютерах и ресурсах сети.
- открытия ресурсов сети указанными пользователем приложениями.
- вывода ресурсов сети, сходных по содержанию, вместе (например, видео- или аудиопапки)
- быстрого многопоточного поиска файлов/папок в локальной сети (доступен расширенный поиск)
- управления локальными расшаренными папками (на своем компьютере)
- мониторинга и управления подключениями к локальным расшаренным папкам

Полностью настраиваемый интерфейс с многоязычной поддержкой (включая русский). Широко используются профили (для хранения настроек). Например, можно создать профили сети, сканирования, поиска один раз, а потом одним щелчком переключаться между ними. LanSurfer полностью бесплатный для соотечественников.



Статус: Freeware
Сайт: http://www.anetto.com.ru/als.php
Размер: 1000 Кбайт
Язык: русский, английский
Скачать: http://www.anetto.com.ru/download/als.zip

Просто полезные программы

Жадюга 1.6

Программа для учета личных финансов «Жадюга» автоматизирует учет ваших доходов и расходов. Имеет простой и понятный интерфейс, не требует знаний в области бухгалтерского учета. Основные возможности:

- Учет доходов и расходов
- Возможность добавления расхода или дохода через СМС
- Поддержка кредитов, долгов
- Поэтапная выплата кредита и долга
- Учет должников

Soft-news

Windows Vista. Назревает скандал

Казалось, ничто не предвещает беды. Председатель Microsoft Билл Гейтс продемонстрировал Windows Vista и Office 12 на конференции профессиональных разработчиков Microsoft в Лос-Анджелосе.

Было объявлено, что Windows Vista выйдет сразу в семи вариантах: Starter Edition (начальный), Home Basic Edition (домашний базовый), Home Premium Edition (домашний расширенный), Professional Edition (профессиональный), Small Business Edition (для малого бизнеса), Enterprise Edition (корпоративный) и, наконец, Ultimate Edition (самый полный). Пакеты Windows Vista будут разделены на две главные категории — для дома (первые 3) и бизнеса (последние 4) — Home и Business, что соответствует домашнему и профессиональному (Home и Pro) вариантам Windows XP.

Затем неожиданно последовала «мягкая» отставка Джима Алчина, руководившего группой разработчиков систем Windows (ему дали доработать до окончания проекта Vista).

Чуть позже стало известно, что руководство Microsoft вынуждено пересмотреть планы и саму парадигму разработки новой операционной среды Vista — она не только получила неудовлетворительную оценку большинства тестеров, но и была практически забракована частью руководства корпорации как весьма далекая от обкатанного ядра новой «ударной» ОС.

По словам Джима Алчина, Vista создана по принципу «лоскутного одеяла» (группы разработчиков решают собственные задачи в рамках единой операционной среды) и не может быть оптимизирована для увеличения производительности, как и реализована в легко перестраиваемом варианте для латания «дыр» в системе безопасности, не в состоянии обеспечить интегрирование дополнительных сервисов, которые могут появиться позже.

По мнению Алчина, ОС Vista необходимо создавать с чистого листа и единой командой, которая должна представить универсальное наращиваемое ядро, что позволит не только поэтапно подключать новые возможности, но и отсекать и/или временно блокировать те ее составные части, в которых выявлены ошибки.

Алчин уверен, что необычайная громоздкость нынешнего процессорного ядра Vista крайне затруднит процесс внедрения новых программных технологий, а это позволит главным конкурентам Microsoft — Google, Apple Computer, Linux, Mozilla (и сонму независимых разработчиков прикладного ПО) — не только вырваться вперед, но и приступить к ПЕРЕДЕЛУ программного рынка.

Microsoft взялась за коррекцию изображений

Конкурентные баталии Adobe и Corel, видимо, не дают покоя Microsoft. Подразделением Microsoft China Recearch Lab на конференции разработчиков Юго-Восточной Азии Professional Developer Conference представлен специальный фильтр (plug-in) для графической системы обработки изображений, особенность которого — возможность тонкого ретуширования и удаления части цифрового изображения.

- Поддержка неограниченного числа пользователей и их счетов
- Поддержка валютных счетов
- Система справочников расходов и доходов
- Ежемесячные напоминания
- Напоминания о просроченных выплатах по кредиту/долгу
- Бесплатное использование программы при доходах менее 6000 р. в месяц

Статус: Shareware
Сайт: http://www.amosoft.net/
Размер: 4100 Кбайт
Язык: русский, английский
Скачать: http://www.amosoft.net/rus/file/setupjm.exe

HyperSaver 1.03

У вас много любимых скринсейверов? Эта утилита поможет вам автоматически менять их при каждом запуске или по времени. На домашней странице можно получить zip-версию без инсталляции (265 Кбайт)

Статус: Freeware
Сайт: http://www.terraspace.ru/~max/progs/
Размер: 95 Кбайт
Язык: русский
Скачать: http://www.terraspace.ru/gmax/progs/hypersaver_setup.exe

Oparin Clock 1.9

В основу работы скринсейвера положена совершенно новая идея отображения времени на циферблате часов. Она запатентована автором в Роспатенте как «Устройство индикации времени на циферблате часов» (N 43088). В программе реализованы следующие настройки: Время: текущее / со времени старта > Размер кругов: одинаковый/разный > Картинка в центре часов: предустановленная/пользовательская/слайд-шоу > Язык меню: русский/английский

Статус: Shareware
Сайт: http://www.newart.ru/
Размер: 150 Кбайт
Язык: русский
Скачать: http://www.newart.ru/oparin/clock/OparinClock_trial.zip

Календарь на обоях 2.0

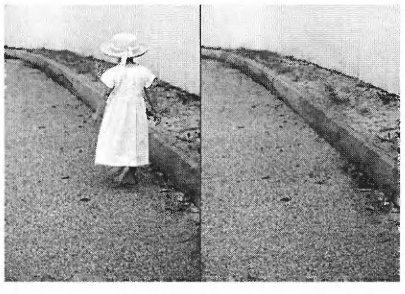
Эта программа рисует календарь прямо на картинке рабочего стола. Сама картинка на диске при этом не изменяется. Устанавливается автоматически.

Статус: Freeware
Сайт: http://hksetup.narod.ru/
Размер: 230 Кбайт
Язык: русский, английский
Скачать: http://hksetup.narod.ru/files/desktop_20050904.exe

ZoneTick 2.6.6

Программа для изменения внешнего вида часов в системной панели, отображения времени в нескольких часовых поясах.

Статус: Freeware
Сайт: http://www.zonetick.com/
Размер: 266 Кбайт
Язык: английский
Скачать: http://www.softodrom.ru:8086/3233/setup.exe



Фильтр реализован на базе закрытого патентного решения под названием Visual Simulation of Weathering by Gamma-ton Tracing, хотя некоторые «секреты» фильтрации фрагментов фотографий — вычленение дифференциальной составляющей реального и симуляционного изображений — достаточно очевидны.

Вероятно, новый фильтр ретуширования изображений будет встроен в состав графических пакетов операционной среды Windows Vista.

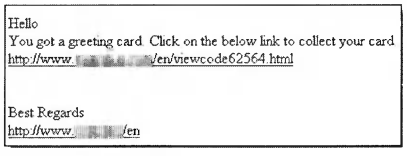
Microsoft пересматривает нормы криптобезопасности

Официальные представители Microsoft признали, что уровень криптостойкости таких бесплатных алгоритмов шифрования, как DES-56, MD4, MD5, SHA0, SHA1, недостаточен для надежной защиты данных, произведенных офисными приложениями Microsoft. Главная причина тому - наличие развернутой теоретической базы и программных средств для успешного взлома документов, что может серьезно поколебать рыночные позиции программной продукции Microsoft.

В связи с этим корпорация «изымает» указанные алгоритмы шифрования из своего набора программных средств и настоятельно рекомендует «дружественным» разработчикам ПО не использовать их в своих новых разработках.

Поздравительная открытка с сюрпризом

SophosLabs предупреждает о новой уловке вирусописателей. Электронная поздравительная открытка, которую спамеры рассылают по по всему миру, пытается установить на пользовательский компьютер троянскую программу.


Hello
You got a greeting card. Click on the below link to collect your card.
http://www. /en/viewcode62564.html

Best Regards
http://www. /en

Если пойти по ссылке в письме, вы получите на ПК трояна Troj/Dloader-UT, с помощью которого хакеры смогут шпионить за вашей работой на ПК и воровать пароли.

Microsoft заинтересовалась смарт-картами

Microsoft приобрела компанию Alacris, разработчика программ для работы со смарт-картами. Судя по всему, корпорация рассчитывает облегчить себе процесс встраивания в Windows систем управления смарт-картами в рамках стратегии аутентификации и авторизации.

В Windows уже есть платформа для использования смарт-карт и других технологий аутентификации (подтверждения подлинности пользователя). Она состоит из Active Directory и Microsoft Certificate Services. Технологии Alacris ускорят внедрение системы обработки новых смарт-карт и настройки существующих, обеспечат управление веб-ориентированным процессом на основе принятых политик.

БИБЛИЯ ПОЧТОВОЙ БЕЗОПАСНОСТИ

Антон Орлов (Москва)

Как ни прискорбно сознавать, но в настоящее время среди населения Земли встречается немало тех, для кого нанесение вреда ближнему является видом развлечения, а то и средством обогащения. Поэтому система электронной почты, как и весь Интернет, стала источником разного рода опасностей. При всем разнообразии суть их сводится к одному: попадание в почтовый ящик того, чего там быть не должно.

В почтовый ящик помимо нужных и важных писем могут попадать:

- Письма с рекламой, на получение которых вы не давали согласия.
- Письма-обманки (так называемый фишинг)
- Письма с компьютерными вирусами
- Письма от недоброжелателей, цель которых — захламить ваш почтовый ящик.

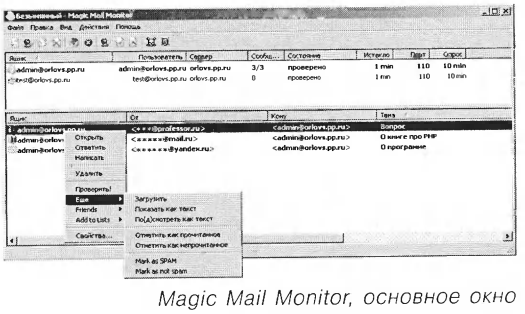
Наконец, возможен прямой «взлом» вашего почтового ящика, то есть получение доступа к нему помимо вашего желания.

Книга первая. Общие правила гигиены

Один из главных методов защиты почти от всех «почтовых угроз» — контроль пришедших писем без их загрузки на компьютер, прямо в почтовом ящике. Так можно удалить ненужные и опасные письма. Это первейшее правило гигиены, все равно что мытье рук перед едой.

Первый способ такого удаления — через веб-интерфейс почтового сервиса, на котором расположен ящик. Для этого необходимо зайти на главную страницу почтового сервиса, ввести в специальные поля логин и пароль, а затем, ориентируясь на содержание тем и на адреса отправителей, удалить ненужные и потенциально опасные письма. Можно сначала просмотреть тексты писем и потом решить, нужно ли данное письмо загружать.

Однако веб-интерфейсами снабжены не все почтовые сервисы, да и работать с ними не всегда удобно. Поэтому созданы специальные программы для просмотра писем в почтовом ящике (без их загрузки на компьютер) и удаления «мусора». Например, такое делает программа Magic Mail Monitor (она служит еще и оповещателем о приходе писем в ящик), доступная с адреса http://www.geeba.org/magic. В последних версиях программы есть русский интерфейс.



Magic Mail Monitor, основное окно

Magic Mail Monitor способна одновременно проверять сразу несколько почтовых ящиков. Программу можно настроить так, что при появлении новых писем в разных ящиках будут проигрываться разные звуки. Кроме того, вы можете приказать ей при приходе новых сообщений автоматически развертывать свое основное окно. Команда «Просмотреть» позволяет загрузить письмо на компьютер, отобразить его в текстовом файле и ознакомиться с его содержанием.

Удобной особенностью программы является то, что с ее помощью можно загрузить с почтового сервера для просмотра лишь часть сообщения, а не все целиком, сэкономив тем самым время и трафик. Для этого следует воспользоваться командой «Еще» > «По(д)смотреть как текст» из контекстного меню сообщения. В диалоговом окне «Файл» > «Настройки» можно указать, насколько большой должна быть загружаемая часть.

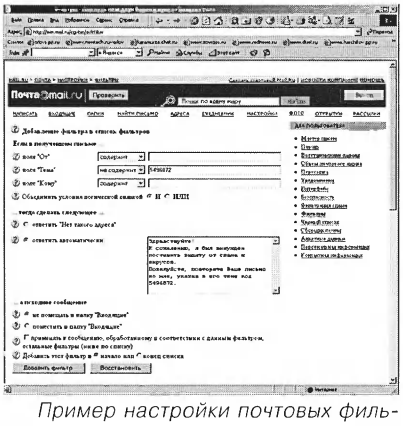
Есть еще один универсальный способ защиты, правда, с одним «но». Он дает почти стопроцентную гарантию от вирусов и спама и довольно значительную — от умышленных пакостей, однако несколько неудобен вашим респондентам. Суть его сводится к настройке фильтров на почтовом сервере.

1. Придумайте некую кодовую последовательность, которую относительно легко запомнить, но кото-

рая никогда не может случайно встретиться в теме письма. Например, какая-нибудь группа цифр или бессмысленное слово.

2. Создайте фильтр, согласно которому на все сообщения без такой последовательности в теме письма будет отправляться автоматический ответ с текстом вроде «Извините, я был вынужден поставить систему защиты от спама и вирусов. Пожалуйста, отправьте Ваше письмо мне снова, но обязательно укажите в его теме ... (ваша кодовая последовательность)». Если допускают настройки фильтров, прикажите сервису включать в конец этого текста исходное письмо отправителя.

3. Создайте фильтр, согласно которому все сообщения без такого кода в теме письма будут автоматически удаляться.



Пример настройки почтовых фильтров для отсева спама и вирусов

В результате тот, кто отправит вам письмо, вышлет его повторно, указав в теме код. Спамерская программа или вирус, рассылающий сам себя по адресной книге, понять, что вы написали, не смогут, и на этом их общение с вашим ящиком закончится.

Для обороны от спама и вирусов схема вполне эффективна. С другой стороны, отправлять письмо еще раз, модифицировав тему, многим респондентам может показаться излишне хлопотно. А некоторые могут вообще отказаться с вами общаться, посчитав ситуацию для себя оскорбительной.

Наконец, возможна «патовая» ситуация, если такая система установлена на двух ящиках, и владелец одного из них отправит письмо другому. В ответ будет послан запрос о подтверждении... который будет расценен как «несанкционированное» письмо и вернется отправителю с просьбой подтвердить отправку. А там схема зеркально повторится, ведь в «перекидываемом» между ящиками запросе нет секретного кода! В итоге — почтовый пинг-понг, последствия которого для почтовых серверов могут быть сравнимы с хакерской атакой. Так что стоит ли использовать данный способ — решать вам.

Вот небольшая памятка с кратким перечислением мер безопасности при работе с электронной почтой:

1. Выбирая почтовый сервис для ящика, обращайте внимание на наличие на нем средств защиты от вирусов и спама, фильтров и возможности SSL-доступа. Чем больше средств защиты, тем лучше. Поищите в Интернете и печати отзывы о безопасности разных сервисов и на основе полученных данных принимайте решение.

2. Регистрируя ящик, придумывайте сложные пароли и контрольные вопросы.

3. При выборе почтового клиента ориентируйтесь в том числе и на его безопасность: невосприимчивость к вирусам, троянам, наличие средств борьбы со спамом.

4. Перед загрузкой писем из ящика просматривайте их список через веб-интерфейс почтового сервиса или специальной программой вроде Magic Mail Monitor.

5. Проверяйте антивирусными программами все вложения в присылаемых вам письмах.

6. Регулярно устанавливайте «заплатки» на ПО или его новые версии, если в старых обнаружены уязвимости. Регулярно обновляйте антивирусные программы.

7. Установите файервол и правильно его настройте. При выборе файервола обращайте внимание на наличие модулей «защиты почты» или других подобных.

8. Зарегистрируйте несколько почтовых ящиков, используя один для переписки с друзьями и коллегами, а другие — со всеми остальными. При атаке «почтовыми бомбами», вирусами или спамом на один из «других» зарегистрируйте новый.

9. При работе с почтовым ящиком с чужого компьютера не используйте почтовые программы — довольствуйтесь веб-интерфейсом.

10. Работая с почтовым ящиком с чужого компьютера через веб-интерфейс, отказывайтесь от всех предложений сохранить пароль, а после работы очистите «Историю», кэш и «Автозаполнение» браузера, после чего закройте все его окна.

Книга вторая. Вирусы

Вирусом называют программу, без ведома и желания пользователей размножающуюся путем включения своего кода в исполняемые файлы и в файлы, способные хранить программный код. Электронная почта в настоящее время стала одним из основных каналов распространения вирусов. Письмо, зараженное вирусом, содержит в себе его исполняемый файл с собственно вирусным кодом.

При запуске такой файл:

- сканирует адресную книгу в почтовом клиенте пользователя или уже пришедшие письма (если почтовый клиент это позволяет);
- рассылает свои копии по всем адресам, найденным в адресной книге или в этих письмах.

Если кроме такой рассылки вирус больше ничего не делает, то его называют «червем», но чаще вирусная программа копируется также в папку с файлами операционной системы и помещает в системный реестр команду своего автоматического запуска при старте ОС. Запущенная программа может регулярно повторять свои рассылки, а также выполнять те или иные разрушительные действия, например, стирать нужные файлы, похищать пароли, секретные сведения, личную информацию.

Чтобы компьютер был заражен вирусом, вирусная программа должна быть на нем запущена. Это может произойти двумя способами:

- из-за глупости самого пользователя, запустившего вложенный в письмо исполняемый файл;
- из-за уязвимости в почтовом клиенте, допускающей автоматический запуск вложенных программ.

Методы защиты от вирусов, скоро, наверное, будут писать большим фломастером на большом листе ватмана

и вывешивать в каждом офисе. Но все же считаю нужным их перечислить — хотя бы для того, чтобы было откуда списывать их на лист ватмана...

Некоторые сервисы бесплатных почтовых ящиков (например, http://www.mail.ru, http://www.360.ru) предоставляют своим пользователям такую услугу, как проверка всей приходящей почты на наличие вирусов. Поэтому обязательный ежедневный ритуал — посещение веб-интерфейса почтового ящика и просмотр писем с вложениями на предмет зараженности перед загрузкой почты на свой компьютер.

Особое внимание уделяйте вложениям с расширениями .exe, .com, .pif, .scr и невразумительным текстом самого письма. Такие письма лучше сразу удалить. Порядочные респонденты никогда не будут пересылать по почте программы в формате .exe или .com, во всяком случае, без предварительного согласования с вами.

Конечно, вследствие несовершенства системы отсева вирусов на почтовом сервисе или ваших ошибок при просмотре информации о пришедших письмах некоторые зараженные письма могут все же проникать сквозь этот первый уровень защиты.

Следующий уровень — это использование антивирусных программ.

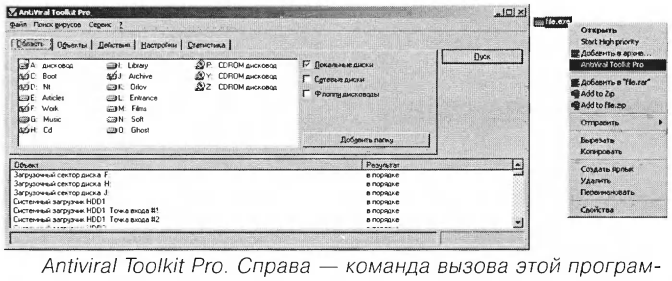
К настоящему времени наиболее популярными являются такие, как Antiviral Toolkit Pro от Лаборатории Евгения Касперского (http://www.avp.ru или http://www.kaspersky.ru), Doctor Web от Лаборатории Игоря Данилова (http://www.drweb.ru), Norton Antivirus от компании Symantec (http://www.symantec.com). По эффективности они вполне сравнимы: на периодически проводящихся конкурсах пальмой первенства они по очереди меняются между собой. Цены на легальные версии антивирусных программ колеблются в пределах $40-70 для российских разработок и порядка $100 долларов для западных.

Принцип работы антивирусных программ основан на том, что каждый вирус имеет код, характерный только для него, и, кроме того, может располагаться лишь во вполне определенных местах зараженного файла (тех, с которых операционная система считывает исполняемый код). Поэтому антивирус может просмотреть файл, определить, есть ли в нем код того или иного вируса, и затем выдать пользователю информацию об этом или даже сразу удалить вирусный код — «вылечить» файл. Соответственно, в каждом антивирусе есть встроенные библиотеки вирусов (базы данных), которые периодически обновляются.

Некоторые антивирусы используют эвристический алгоритм — с помощью специальных средств моделируют действия программы, как если бы она была запущена, и смотрят, не похожи ли эти действия на действия вируса. Такой метод позволяет обнаруживать и те вирусы, описания которых нет в базе данных антивируса, однако тут возможны и ложные срабатывания.

При работе с электронной почтой все вложения в приходящие письма — документы Word, архивы и, в особенности, любые исполняемые файлы — следует перед открытием или запуском обязательно проверять антивирусом!

Кроме того, практически все современные антивирусы имеют и так называемый монитор — модуль, который постоянно проверяет на наличие вирусов все файлы, открываемые пользователем или какими-либо программами. В ходе приема почты весьма желательно держать включенным такой монитор: если с почтой придет вирус, то в зависимости от вида программы и ее настроек монитор автоматически удалит его или запретит прием вирусного письма.



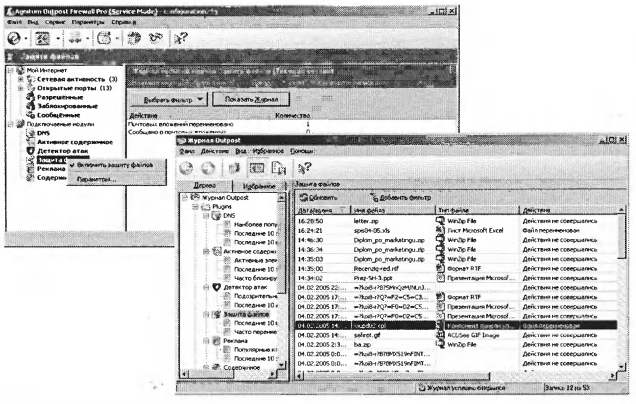
Antiviral Toolkit Pro. Справа — команда вызова этой программы в контекстном меню файла

Для предотвращения поражения вирусом из-за уязвимости в ПО (их еще именуют «дырами») соблюдайте такие правила:

- Своевременно устанавливайте «заплатки» к почтовым программам или инсталлируйте их новые версии. Разработчики почтовых клиентов обычно дорожат своей репутацией и в случае обнаружения «дыр» выпускают обновления, доступные на их сайтах.
- При выборе и настройке ПО для работы с электронной почтой уделяйте внимание антивирусной стойкости.
- Регулярно посещайте специализированные сайты, посвященные безопасности (например, в Рунете это http://www.securitylab.ru), чтобы оперативно устанавливать обновления или до появления обновлений временно переходить на другой почтовый клиент.

Даже если вам все-таки удастся подхватить вирус, то выполнению им своей вредоносной функции может помешать установленный файервол. Если не вдаваться в подробности, то файервол контролирует, какие программы работают с Интернетом с данного компьютера, и если к такой работе пытается приступить неизвестное приложение, невесть откуда взявшееся на компьютере, то файервол строго запрещает такую работу и поднимает тревогу.

Сам по себе файервол не является антивирусной защитой. Он может лишь предотвратить некоторые последствия заражения — например, помешает вирусам отправить конфиденциальные данные с вашего компьютера или хакеру управлять им через Интернет. Некоторые файерволы выполняют еще и дополнительные функции по защите компьютера от сетевых опасностей. Так, файервол Outpost Firewall фирмы Agnitum (бесплатная версия доступна с сайта http://www.outpostfirewall.com) имеет блок защиты электронной почты от вирусов во вложении. Этот блок автоматически переименовывает файлы с определенными расширениями во вложениях к письмам: например, файл virus.com будет автоматически переименован в virus.com.safe, что предотвратит его автоматический запуск даже в случае наличия у почтового клиента соответствующей уязвимости.



Файервол Outpost Firewall, модуль защиты электронной почты

Для большей эффективности все способы защиты лучше сочетать. Многоступенчатая система защиты может выглядеть, например, так:

- Вся почта поступает на почтовый сервис с веб-интерфейсом и антивирусной проверкой.
- Перед перекачиванием в почтовый клиент каждое сообщение с вложением просматривается на предмет зараженности или похожести на вирус.
- Почтовый клиент либо не имеет «дыр», либо на все известные «дыры» установлены заплатки.
- Во время приема почты работает антивирусный монитор и система защиты файервола.

Если использовать такую защиту, то риск заражения вирусом можно свести к ничтожно малой величине.

Книга третья. Спам

В мире Интернета словом «спам» называется реклама, которую вам навязывают помимо вашего желания. Этим способом в основном рекламируются товары, цена которых завышена, а качество чем-то особым от других товаров не отличается. Те, кто прибегает к услугам спамеров, тупо следуют неглубокой идейке «всем вдалбливай, авось кто-то и поверит».

По сути спам в Интернете представляет собой рассылку рекламных писем по электронной почте множеству адресатов. Отправить одно и то же письмо сразу по нескольким тысячам адресов очень просто — для этого достаточно небольшого сценария на PHP или Perl на сервисе бесплатного хостинга или даже обычного почтового сервера, на котором не приняты меры безопасности против спама. Собрать же коллекцию e-mail-адресов тоже труда не составляет — достаточно сделать специальную программу по типу «поисковой машины» (подробнее см. ниже). Так что затраты на рассылку нескольких тысяч писем весьма невелики.

Результат такой рекламы, бесспорно, низкий, но срабатывает закон больших чисел. Если из каждой тысячи адресатов найдется один, соблазнившийся предложением спамера, то рассылка по миллиону адресов принесет тысячу покупателей. То, что остальные девятьсот девяносто девять тысяч получателей потратят свое время и деньги, чтобы загрузить рекламное письмо на свой компьютер и затем удалить его, спамера не волнует — для него важна лишь собственная выгода.

В настоящее время в почте многих пользователей спам занимает уже от 75 до 90% всех приходящих сообщений. К сожалению, потоки спама продолжают нарастать.

Однако со спамом можно бороться. И нужно.

Первое и самое основное правило борьбы со спамом — не покупать ничего у спамеров! Никогда и ни при каких условиях. Тем более, что посредством спама часто рассылаются предложения мошенников (об этом чуть ниже).

Однако простое игнорирование спама, может, и помешает спамеру достичь желаемой выгоды, но вам-то жизнь не особо облегчит. Поэтому желательно предотвратить захламление почтового ящика.

Нередко в письмах спамеров дается информация, как отказаться от их услуг — «отписаться от рассылки». Обычно для этого предлагается отправить специальное письмо на определенный адрес или зайти на тот или иной сайт по указанной в письме ссылке. Иногда это действительно помогает, и спамер удаляет адрес отписавшегося из своей базы данных, но чаще всего такое действие лишь укажет спамеру, что его спам хотя бы читают, что только усилит рекламный натиск на вас.

Основное правило защиты от спама — как можно реже указывать свой реальный e-mail-адрес на ресурсах Интернета!

Спамеры получают адреса e-mail для своих занятий с помощью специальных программ, которые путешествуют по ресурсам Сети и копируют имеющиеся на веб-страницах адреса электронной почты. Алгоритм такого выделения несложен — ведь в адресе обязательно присутствует символ «@» и не может быть пробелов, скобок, запятых. А значит, для получения списка адресов достаточно приказать программе найти на ней все символы «@» и взять то, что находится слева и справа от каждого из них до первого символа, недопустимого в адресе, — это и будет искомым адресом. После этого программа ищет на странице гиперссылки и загружает другие веб-страницы, повторяя с ними ту же процедуру. Найденные адреса записываются в список, который после удаления повторов выдается спамеру. Особенной любовью спамеров пользуются всевозможные гостевые книги и открытые форумы, указание e-mail на которых зачастую является необходимым условием для получения возможности добавлять сообщения.

Отсюда следует, что для того, чтобы ваш адрес не попал спамерским программам, нужно вообще не указывать его на общедоступных веб-страницах Интернета. Но электронная почта на то и существует, чтобы с вами могли связаться. Значит, сокрытие в тайне e-mail — явно не выход.

Не расстраивайтесь, есть некоторые простые приемы, которые позволяют «обманывать» спамерские программы. Вот некоторые из них.

- Вместо символа «@» указать любой другой символ, похожий на него, например, «#» или «0» - например, address#someserver.ru. Если посетители гостевой книги или форума не совсем глупые люди, то они поймут, что должно стоять вместо этого «похожего» символа. К сожалению, вызвать почтовую программу путем щелчка

мышью на e-mail им не удастся: придется копировать адрес в буфер обмена и заменять в нем символы.

- Вместо символа @ указать какой-либо текст, например, «собака» — address-собака-someserver.ru. Недостатки те же: на замену символов ваш респондент тратит время.
- Вставить в адрес какие-либо символы, а рядом указать, что их надо удалить: add***res***s@som###eserv ###er.ru (удалите * и #). Так как символ @ сохраняется, спамерская программа считает этот адрес, но в каком виде — догадаться нетрудно. Заодно спамер будет вынужден потратить время на удаление этого адреса из своей базы данных.

Если вы указываете e-mail на страницах своего сайта, то к упомянутым методам можно добавить еще несколько. Укажите e-mail в неизмененном виде, но внутрь него спрячьте комплексы тегов «!—» (они ничего не отображают на экране). Например, ваш e-mail будет выглядеть как «mya»!—»ddre»!—»ss@ne»!—»tman.r»!—»u». Можно использовать теги «span» с пустым содержанием: mya»span»»/span»ddre»span class=red»»/span»ss@ne»span class=blue»»/span»tman.r»span»»/span»u. Можно сочетать оба варианта. На веб-странице такие адреса отображаются без изменений, а вот спамерская программа, анализирующая исходный текст страницы, будет поставлена в тупик. Недостаток способа в том, что посетителям придется вручную копировать e-mail в свою почтовую программу, да и многие программы спамеров уже научились «выкусывать» лишние теги из адресов.

В различных сетевых публикациях встречаются сценарии на Javascript, призванные отображать на веб-странице e-mail полностью, а в коде веб-страницы указывать его в измененном виде. Использование таких сценариев позволит, надежно защитив e-mail от спамеров, оставить посетителям возможность помещать его в поле адреса почтовой программы простым щелчком мыши. Есть и программы, которые могут генерировать подобные сценарии для любого адреса электронной почты — например, Blackman E-mail Encoder (http://www.blackman2003.da.ru).

Вторым элементом обороны от спама является грамотный выбор почтового сервиса для размещения своего ящика. Многие почтовые сервисы используют специальные программные комплексы «спамообороны», автоматически отсеивающие рекламные письма. Анализ писем ведется по содержанию заголовков, обратных адресов, содержанию текстов. На основании этих данных программа принимает решение, является письмо спамом или нет. Наиболее эффективные из таких систем могут отсеивать до 90% рекламных писем, и те, что все же прорвутся через «защитные кордоны», не так долго удалить вручную.

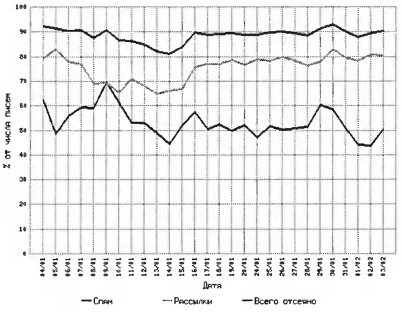


График отсеивания спама на одном из сервисов бесплатных почтовых ящиков

Вместе с тем на почтовых сервисах с такими программными комплексами есть риск отсеивания и не рекламных писем. Письмо от вашего друга вполне может быть уничтожено без всяких известий вам или отправителю лишь за то, что в его теме находилось какое-либо слово. Бесспорно, разработчики принимают меры против ошибок «централизованной спамообороны», однако стопроцентную гарантию дать никто не может.

Поэтому при выборе сервиса для размещения своего почтового ящика обращайте внимание на то, какая система защиты от спама на этом сервисе установлена. Почитайте отзывы о ней на Интернет-форумах, в компьютерных журналах, подумайте, что вам важнее: сохранить ящик чистым или не допускать пропадания писем. Если важно первое (например, вам пишет лишь ограниченный круг лиц, и вы знаете, что письма от них спокойно проходят через любую «спамооборону»), то ищите сервис с мощной системой отсева рекламы (в Рунете такими, например, являются сервисы http://www.mail.ru, http://mail.yandex.ru). Если важнее второе (вам приходят письма из разных мест и их пропажа недопустима) — обратите внимание на сервисы вообще без систем обороны от спама или с малоактивными системами (например, http://www.netman.ru, http://www.mailgate.ru).

Третья ступень обороны почтового ящика от спама — это почтовые фильтры, то есть настраиваемые вами алгоритмы автоматической обработки писем в зависимости от каких-то параметров (например, удаления всех сообщений с теми или иными обратными адресами).

Ранее, до разработки систем «спамообороны», именно настройка почтовых фильтров была основным средством защиты от спама. Теперь на наиболее крупных сервисах «оборонная» значимость фильтров ушла на задний план, однако на тех, что не снабжены автоматической системой фильтрации спама, такую систему приходится создавать вручную.

Возможность создания и настройки фильтров есть практически у всех почтовых клиентов и на всех приличных почтовых сервисах. Например, в почтовом клиенте Microsoft Outlook Express настройка фильтров выполняется в меню «Сервис» > «Правила для сообщений» > «Почта». Однако при возможности выбора лучше использовать систему фильтров на почтовом сервисе — хотя бы потому, что тогда при работе с почтой через другой почтовый клиент или с другого компьютера фильтры останутся столь же эффективными. Кроме того, применение фильтров вызывает существенное замедление работы большинства почтовых клиентов и в некоторых режимах не дает эффекта (к примеру, при фильтрации по словам в тексте письма сообщения загружаются на компьютер в любом случае). Если же фильтры будут отрабатывать на почтовом сервере, то скорость получения почты клиентом не замедлится.

Если вы все же решите защищать свой ящик самостоятельно, то смиритесь с тем, что добавлять новые алгоритмы обработки придется каждый месяц, если не каждую неделю.

Если вы беспокоитесь, что созданные вами фильтры уничтожат не только

ненужную, но и важную почту, то вместо удаления отфильтрованных писем прикажите фильтрам помещать их в отдельную папку на почтовом сервере.

В какой-то степени снизить остроту проблемы спама вы также можете, если зарегистрируете на разных почтовых сервисах несколько ящиков и будете использовать один или два только для переписки с друзьями и коллегами, а остальные адреса будете указывать в общедоступных местах.

В результате первый, «доверенный» e-mail будет свободен от спама (если, конечно, ваши друзья не отправят его спамерам), и загрузка писем с него потребует лишь минимального контроля. Остальные же ящики можно проверять реже, со всеми описанными выше предосторожностями. Тем респондентам, что свяжутся с вами через эти «общедоступные» адреса, вы впоследствии дадите «доверенный» e-mail для более быстрой переписки. «Общедоступные» адреса можно время от времени менять.

Однако проверка множества ящиков и чистка их от рекламной продукции все же дело довольно трудоемкое и отнимающее время.

На многих почтовых сервисах есть возможность пересылки поступающих в ящик сообщений на какой-либо другой e-mail или, наоборот, средство автоматического забора почты из другого почтового ящика.

Эти возможности облегчат вам жизнь, если вы решите создать несколько ящиков для работы. Так, поставив перенаправление с «общедоступных» ящиков на «доверенный», можно будет ограничиваться проверкой и забором почты только с последнего. А если один из «общедоступных» ящиков начнет забиваться спамом, просто отключите пересылку с него на «доверенный» адрес и вернитесь к описанному выше варианту независимых ящиков. Такая схема, к сожалению, пропустит «первый удар» спамеров, но работать по ней немного удобнее.

Немало интересной информации о борьбе со спамом и спамерами можно найти на сайте http://www.antispam.ru, специально предназначенном для сбора таких сведений.

Книга четвертая. Ловись, рыбка...

Довольно распространенный (во всяком случае, на Западе) вид спама —э то фишинг, рассылка жуликами обманных писем с целью похитить ваши конфиденциальные данные — реквизиты кредитных карт и пароли доступа к банковским счетам. Фишинговые письма внешне выглядят как от легитимных веб-сайтов, с которыми вы регулярно работаете в онлайне, — к примеру, от банка, организации по обслуживанию кредитных карт или интернет-провайдера, то есть от любого сайта, где для удостоверения личности требуется ввод данных.

В таком письме у вас могут запросить ваши конфиденциальные данные в связи с «обновлением систем защиты» или по другой причине, либо предложат пойти по ссылке на сайт (поддельный), который выглядит в точности так, как и оригинальный, но построен исключительно для похищения вашей конфиденциальной информации. По данным противофишинговой рабочей группы (Anti-Phishing Working Group, http://www.antiphishing.org/), до 5% получателей тих писем поддаются на уловку и передают фишерам свои конфиденциальные данные.

Некоторые фишинговые письма содержат программы, способные собирать информацию о ваших действиях в Интернете (шпионские программы) или открывать «черный ход», позволяющий хакерам проникать в ваш компьютер (троянские программы).

Вот набор простых правил поведения, необходимых для того, чтобы не стать жертвой фишинговых атак.

- Никогда не отвечайте на письма, запрашивающие вашу конфиденциальную информацию. Банки или компании, занимающиеся электронной коммерцией, в своих письмах, как правило, персонифицируют обращения к клиентам, а фишеры — нет. Зато они часто используют ложные, но звучащие сенсационно сообщения типа «Срочная информация — реквизиты вашего счета могут похитить», чтобы побудить получателя письма к немедленной реакции.

Уважаемые компании никогда не запрашивают у клиентов пароли или данные счетов через электронную почту. Даже если вы предполагаете, что письмо легитимное, все равно для подстраховки лучше сначала обратитесь в компанию по телефону.

- Посетите веб-сайт банка путем ввода его URL-адреса через адресную строку браузера. Фишеры часто используют ссылки в письмах, чтобы завлечь свои жертвы на поддельные веб-сайты, имеющие похожие адреса (к примеру, mybankonline.com вместо истинного mybank.com). Если пойти по указанной ссылке, то адрес сайта в адресной строке может выглядеть как настоящий, однако, существует несколько приемов его фальсификации, чтобы вывести вас на поддельный сайт. Если подозреваете, что письмо является фальшивым, не используйте указанные в нем ссылки. Да и вообще, чтобы не попасться на удочку фишера, нельзя следовать ссылкам, указанным в письмах, — всегда вводите адреса через браузер.
- Регулярно проверяйте операции по своим онлайн-счетам. Если обнаружите какую-то подозрительную транзакцию, свяжитесь с банком или поставщиком кредитной карты.
- Проверьте веб-адрес в адресной строке браузера. Если веб-сайт, который вы посетили, расположен на защищенном сервере, то адрес должен начинаться с “https://” (“s” от security), а не с обычного “http://”.
- Никогда и никому не открывайте свои PIN-коды или пароли, не записывайте их и не используйте один и тот же пароль для всех своих онлайн-счетов.

И воообще, пользуйтесь здравым смыслом, когда читаете электронные письма. Если что-то в письме вам кажется неправдоподобным или до такой степени хорошим, что не верится, то, скорее всего, так оно и есть.

Книга пятая. Зло ближнему

От чего защититься действительно трудно, так это от личного врага, желающего делать вам всяческие пакости. А способов совершать их в Интернете много...

Одно время в Сети был распространен метод сведения счетов посредством «мусорной атаки». На двух сер-

висах бесплатной почты создавалось по почтовому ящику, и каждый из них настраивался так, что все приходящие письма отправлялись на ящик на другом сервисе и на адрес ящика жертвы. После этого на один из ящиков отсылалось письмо с ругательствами. Это письмо начинало циркулировать между ящиками, и при каждом проходе через каждый ящик на адрес жертвы отправлялась копия этого письма. В результате ящик жертвы вскоре заполнялся копиями ругательного письма, и его владелец был вынужден тратить время и деньги на его очистку.

Конечно, владельцы почтовых сервисов приняли меры против «Мусорных атак», однако способов делать пакости другим осталось еще немало. Например, «почтовая бомба» — отправка по e-mail кому-либо с модемным доступом в Сеть ненужных файлов огромного размера (несколько мегабайт). В результате получатель «бомбы» вынужден тратить немало времени и денег на загрузку сообщений.

Защититься от «почтовых бомб» и «мусорных атак» трудно, но можно. Некоторые механизмы защиты уже встроены в сервисы бесплатных почтовых ящиков: например, при отправке на ящик на почтовом сервисе http://www.netman.ru или http://www.mail.ru сотни одинаковых писем (это можно сделать, например, многократно указывая адрес получателя в поле «Копия:») до адресата дойдет только одно, остальные будут отсеяны. Многие сервисы не принимают письма с приложениями больше определенного размера (обычно 3-5 Мбайт): такое письмо будет отослано назад отправителю с указанием причины отказа в доставке.

«Почтовую бомбу» также можно удалить посредством доступа к ящику через веб-интерфейс или с помощью программ вроде Magic Mail Monitor или The Bee.

Для защиты от пакостей по e-mail можно использовать и почтовые фильтры, например, настроив их так, что письма с вложениями размером больше дозволенного будут автоматически перекладываться в некую папку в ящике или вообще сразу удаляться (согласно правилам сетевого этикета пересылку больших файлов необходимо заранее согласовывать с получателем).

Если вредитель отправляет вам «мусорные письма» с одного адреса, можно заблокировать его в настройках фильтров. Однако такое бывает редко — подделать содержимое поля обратного адреса труда не составляет.

Естественный прием защиты от таких пакостей — завести несколько почтовых ящиков, как описано выше.

Книга шестая. Взлом почтового ящика

Стоит сказать и о том, как уберечь от проблем сам почтовый ящик — размещенный не на вашем компьютере, а на сервере в Интернете. Проблема тут одна — «взлом» этого ящика, то есть захват контроля над ним со стороны злоумышленника. Следствие взлома понятно — своей почты вы больше не увидите, а ваши адресаты могут получить письма с очень нежелательным содержанием, будучи уверенными, что их отправителем являетесь именно вы.

Взлом почтового ящика возможен в двух вариантах:

- получение доступа к почтовому сервису путем прямой атаки;
- получение каким-либо способом авторизационных данных пользователя без работы с почтовым сервисом.

Вероятность взлома по первому варианту зависит от администратора почтового сервиса — от того, насколько квалифицированно он настроил программное обеспечение, насколько внимательно следит за новостями «компьютерной безопасности» и насколько правильно была спроектирована сама почтовая система. Пользователю остается разве что выбирать между сервисами.

Сохранение в тайне пароля — это уже забота пользователя. И думать об этом нужно сразу же, как только вы зарегистрировали ящик. Вернее, даже еще раньше.

Можно проделать простой тест на безопасность работы с почтовым сервисом, и те сервисы, которые его не пройдут, лучше пусть останутся без вашего ящика. Зарегистрируйте на сервисе аккаунт с произвольным именем и паролем, затем зайдите на него и пройдитесь по страницам веб-интерфейса (по папкам «Входящие», «Удаленные», по странице создания сообщения). У каждой из страниц смотрите исходный код (например, в Microsoft Internet Explorer это можно сделать командой «Вид» > «Источник HTML»). И если в коде хоть одной страницы веб-интерфейса вы найдете свой пароль, указанный в открытом виде, то уходите с этого сервиса и больше на него не возвращайтесь. Хранение пароля в коде веб-страниц интерфейса — просто подарок для хакеров. Большинство современных почтовых сервисов такого недостатка не имеют, но проверить все же стоит.

Первое правило защиты от взлома — не придумывайте простых паролей. Имена жены, детей, кота хоть и легко запоминаются, но тут не подойдут: подобрать их легче легкого. Лучше используйте приемы создания сложных в подборе, но легких в запоминании паролей:

- Можно взять какую-нибудь стихотворную фразу (например, «На красных лапках гусь тяжелый») и из каждого слова включить в пароль первые две буквы, поставив при этом английскую раскладку клавиатуры (например, из упомянутой фразы получится пароль «yfrhkfuenz»). Вам придется помнить лишь саму фразу.
- Можно взять какой-нибудь известный вам, но достаточно сложный профессиональный термин (скажем, «теодицея», «аллантоис») и вставить в его середину цифровой код (скажем, год какого-то события), опять же поставив английскую раскладку клавиатуры (например, из упомянутых слов могут получиться пароли «ntj1917lbwtz», «fkkf1812ynjbc»).
- Можно использовать набор стоящих рядом клавиш, чередуя прописные и строчные буквы — скажем, «Uuu76t5RFd». Вы быстро запомните даже не сам пароль, а те движения кисти, которыми он вводится.

На большинстве почтовых сервисов имеется система напоминания пароля в случае, если вы его забудете. Обычно она представляет собой «контрольный вопрос», то есть пару строк текста (первая строка может быть заранее фиксированной, например, «Номер паспорта»). При восстановлении пароля первая строка будет продемонстрирована вам на экране, и

вы в ответ должны будете вспомнить и ввести вторую строку. Если вы сделаете это правильно — вам либо выдадут новый пароль, либо сообщат старый.

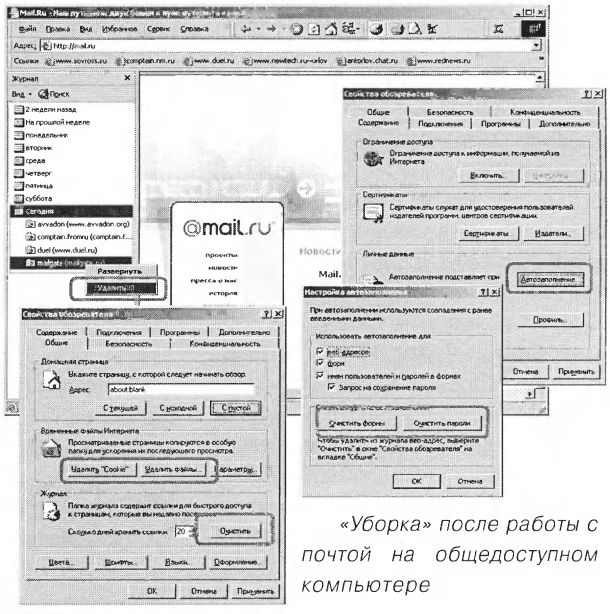
Система, конечно, полезная, но помните, что получение контроля над почтовым ящиком путем подбора ответа на контрольный вопрос — один из самых частых способов «взлома». Никогда не используйте в качестве ответа на контрольный вопрос фразы, очевидным образом вытекающие из вопроса! Не стоит, выбрав в качестве вопроса «Ваш возраст» или «Девичья фамилия матери», правдиво отвечать на них — для подбора первого необходимо менее полусотни попыток, а ответ на второй можно незаметно выведать в дружеской беседе. Лучше сделайте ответ совершенно не соответствующим вопросу — скажем, ответьте «я Кощей Бессмертный» или «я знаю, вы не узнаете». Только не забудьте, что ответили...

Правила сохранения пароля в тайне при работе с почтовым ящиком незамысловаты, но их все же стоит перечислить.

- Предотвращайте доступ к вашему компьютеру тех, кто может похитить пароль. В большинстве почтовых клиентов пароли на доступ к почтовым ящикам хранятся либо в открытом, либо в плохо защищенном виде. Так, пароли, сохраненные в Microsoft Outlook Express, легко вывести на экран с помощью утилиты Fidolook.
- Если вы подключаетесь к Интернету не путем прямого соединения с провайдером, а через корпоративную или «домовую» сеть, то недобросовестные администраторы или даже другие пользователи этой сети могут похитить ваш пароль на доступ к почтовому ящику путем «перехвата трафика», то есть скопировав себе на компьютер все данные, передаваемые вами в Интернет, и вытащив из них пароли (они ведь передаются из вашего браузера на почтовый сервер, не так ли?). Для такого перехвата есть специальные программы. Чтобы защититься от них, можно использовать специальный протокол SSL, поддерживаемый некоторыми почтовыми сервисами (например, http://www.hotbox.ru).

Если вы работаете с общедоступных компьютеров:

- никогда не сохраняйте пароли в установленных на них почтовых программах, а еще лучше — пользуйтесь веб-интерфейсами почтовых сервисов;
- избегайте сохранения паролей в cookies (отметка «Сохранить пароль» на странице входа), иначе те, кто воспользуется компьютером после вас, смогут поработать и с вашим ящиком;



«Уборка» после работы с почтой на общедоступном компьютере

- при вводе логина и пароля на вход в почтовый ящик в веб-интерфейсе почтового сервиса отказывайтесь от предложения браузера сохранить пароль — иначе сохранится он отнюдь не только для вас;
- работая с веб-интерфейсами почтовых сервисов, лучше всего использовать функцию «Чужой компьютер» (если, конечно, она есть), при ее включении пароли сохраняются не в cookies, а в специальной переменной, уничтожающейся при закрытии всех окон браузера;
- не забывайте нажимать на кнопку «Выход» из веб-интерфейса к почтовому ящику при завершении работы с ним, при этом почтовый сервис «забывает» о вашем браузере, и для повторного входа потребует ввести логин и пароль;
- по завершении работы не поленитесь очистить «Историю» и кэш браузера, а также «Автозаполнение» форм: если страницы почтовой службы закэшируются, то те, кто сядет работать на вашем компьютере после вас, смогут, пользуясь «Историей» и кэшем, по меньшей мере почитать ваши входящие и исходящие письма. Автозаполнение вполне может подсказать им как минимум логин для входа в вашу почту, если не пароль. Кроме того, завершив работу на общедоступном компьютере, закройте абсолютно все открытые окна браузера.

Если вы отправляетесь в путешествие и планируете пользоваться услугами Интернет-салонов, то перед отъездом зарегистрируйте себе еще один ящик на каком-либо почтовом сервисе и поставьте на его адрес перенаправление с вашего основного ящика (не «сборщик почты»!).

Это нужно на случай, если злоумышленник поставит на компьютер салона программу-клавиатурный шпион (например, HookDump) и тем самым узнает пароль на вход в ваш ящик. Если ящик, взломанный таким способом, будет у вас единственным, то проблема окажется весьма серьезной. А если взломанный ящик был лишь «отпускным», то по возвращении достаточно будет убрать перенаправление из основного ящика, чтобы ликвидировать последствия «взлома». Разве что пришедшая почта может быть потеряна.

Книга седьмая. Око за око

Выполняя перечисленные выше рекомендации, вы выступаете в роли защищающегося, а спамер, вирусописатель или пакостник — в роли атакующего.

Однако, как известно, лучшая защита — это нападение, в нашем случае — ответный удар. Нет, не ответным спамом или «почтовыми бомбами». Во-первых, вам могут ответить тем же, во-вторых, как-то не очень достойно все это...

Лучше попытаться выследить злоумышленника — выявить, через како-

го провайдера он работал, с какого IP-адреса. Ну, а потом можно связаться со службой сервиса провайдера и потребовать от нее прекратить деятельность вредителя. С учетом наличия практически у всех провайдеров автоматических определителей номера это будет довольно просто.

«Вычислить» вредителя можно таким способом.

1. Для начала внимательно изучите заголовок нежелательного письма. В Microsoft Outlook Express это можно сделать, выделив письмо в папке и выбрав из меню правой кнопки мыши пункт «Свойства > Подробности». Аналогичные средства есть и в других почтовых клиентах, а также в веб-интерфейсах почтовых сервисов (иногда нужная команда называется «Источник»).

В заголовке письма записывается весь его путь через цепь почтовых серверов. Запись ведется снизу вверх, то есть каждый новый почтовый сервер помещает информацию о себе в самое его начало.

2. Найдите в заголовке письма самый нижний абзац из начинающихся словами «Received: from». Самая верхняя строчка — это обычно «Return-Path» или «From», обратный адрес письма. При нажатии кнопок «Ответить», «Ответить отправителю» в почтовых клиентах именно на этот адрес отправляется ответ.

Но: в письме злоумышленника здесь может быть что угодно. Поэтому не стоит принимать его во внимание. В конце концов, рассылка спама может быть провокацией, направленной на дискредитацию честного производителя, а при отправке вирусов или пакостей тем более под ответный удар подставят кого-то невинного. Поместить в письмо липовый обратный адрес легче легкого — в Microsoft Outlook Express он указывается в настройках учетных записей, а в The Bat! вообще вписывается в текст письма отправителем.

Чтобы выследить сетевого бандита, вам нужен самый нижний абзац заголовка письма, в котором есть слово «Received». Это — запись самого первого почтового сервера, на который автор письма отправил его со своего компьютера. Именно ее и надо изучить.

Сказку сразу — максимум, что можно узнать из заголовка письма, это IP-адрес отправителя и время отправки письма. По этому IP-адресу можно вычислить координаты первичной сети (провайдера, локальной сети в офисе, университете, Интернет-кафе и т. д.), ее местонахождение, а также контактную информацию владельцев и администраторов.

3. Если в этом абзаце есть текстовый адрес, можно проанализировать его и определить, через какого провайдера подключался отправитель, посетить сайт провайдера и связаться с его службой поддержки.

Как вы помните, в поле «Received:» включается адрес компьютера, с которого письмо было отправлено (если отправляющий письмо почтовый сервер этот адрес определил). Этот адрес может содержать только IP-адрес, а может — и текстовое имя компьютера, обычно представляющее собой доменное имя четвертого-пятого уровней. В последнем случае это имя будет принадлежать зоне провайдера — обычно веб-сервер провайдера размещается на входящем в эту зону имени второго уровня: например, если адрес компьютера-отправителя — dialup4546.dial.provider.ru, то логично ожидать, что на адресе http://www.provider.ru окажется и сайт провайдера.

Все, осталось только посетить сайт провайдера, узнать на его страницах e-mail службы противодействия незаконным действиям (обычно ее адрес имеет вид abuse@provider.ru) и переслать письмо на него как вложение. Именно как вложение — с помощью соответствующей функции почтовой программы. Иначе в пересылаемое письмо не войдет его заголовок, что обесценит пересылку.

Сотрудники службы изучат заголовок письма, посмотрят в лог-файлах сервера, с какого номера телефона и каким пользователем оно было отослано, а затем примут меры (могут запретить доступ к своим модемным пулам с этого телефона).

4. Если текстового адреса компьютера отправителя в заголовке письма нет, то отыскать в той же строке IP-адрес злоумышленника. Если и там IP-адреса нет, то посмотреть расположенный выше абзац, начинающийся словами «Received: from» и взять адрес оттуда. Запомнить или записать найденный IP-адрес.

5. Узнать из базы данных Whois, к какой сети принадлежит компьютер злоумышленника и связаться с ее службой поддержки.

Если текстовый адрес компьютера указывается в заголовке письма не всегда, то IP-адрес присутствует там куда чаще. Подделать его непросто — обычный спамер или вредитель нечасто располагает средствами для этого. Поэтому по IP-адресу компьютера отправителя можно определить сеть, в которую этот компьютер входил в момент отправки письма.

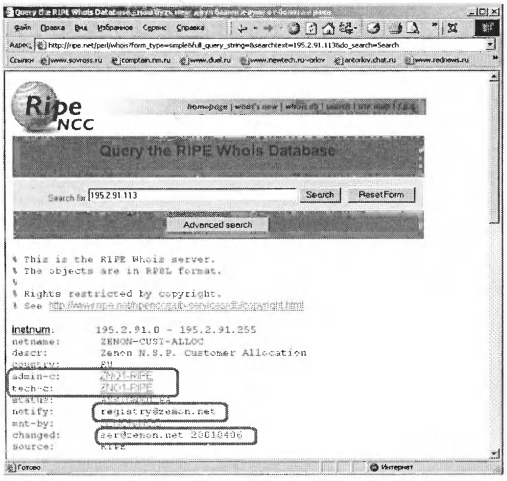
Если в заголовке письма нет указаний на сеть, в которую входит компьютер бандита, то следует посетить сайт RIPE http://www.ripe.net и вос-

```
Return-Path: <spamer@spam.ru>
Received: (qmail 18756 invoked from network); 30 Feb 2001 02:39:12 -0300
Received: from ns.provider.ru ([178.39.34.56] helo=provider.ru)
  by mx9.port.ru with esmtp (Exim 3.14 #4)
  id 14M14M-0002v14M0; Sun, 30 Feb 2001 02:39:12 +0300
X-Recipient: alexey@mail.ru
Received: from LocalHost (pp2545.dialup.provider.ru [178.39.0.1])
  by provider.ru (Postfix) with SMTP
  id 9ACDD8751; Sun, 30 Feb 2001 02:39:12 +0300 (MSK)
  (envelope-from superspamer@spam.ru)
Message-ID: <4854542485fggfwew45454ewe454we@LocalHost>
From: "Reklama" <spamer@spam.ru>
To: <alexey@mail.ru>, <anton@mail.ru>, <igor@mail.ru>,
    <andrey@mail.ru>, <petr@mail.ru>, <maxim@mail.ru>,
    <alexey@chat.ru>, <anton@chat.ru>, <igor@chat.ru>,
    <andrey@chat.ru>, <petr@chat.ru>, <maxim@chat.ru>
Subject: Реклама
Date: 30 Feb 2001 02:39:12 +0300
MIME-Version: 1.0
Content-Type: multipart/mixed;
  boundary="----=_NextPart_000_0111_2145887B.ADC458FD"
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 5.5
```

Заголовок письма спамера (все параметры полностью вымышлены)

```
Received: from LocalHost (pp2545.dialup.provider.ru [178.39.0.1])
  by provider.ru (Postfix) with SMTP
  id 9ACDD8751; Sun, 30 Feb 2001 02:39:12 +0300 (MSK)
  (envelope-from superspamer@spam.ru)
From: "Reklama" <spamer@spam.ru>
Subject: Реклама
Date: 30 Feb 2001 02:39:12 +0300
MIME-Version: 1.0
X-Mailer: Microsoft Outlook Express 5.5
```

Часть заголовка письма. Виден текстовый адрес компьютера-отправителя



Отчет сервиса Whois RIPE. Обведены координаты администрации сети, к которой принадлежит узел с данным IP-адресом, и ссылки на страницы с более подробной информацией о ней

пользоваться базой данных Whois по IP-адресам. В полученной из базы данных информации будет несколько ссылок на координаты администратора сети, ее владельца, в общем — тех, кто за эту сеть отвечает. Эти данные всегда верны — ведь именно по ним RIPE связывается с администрацией сети по техническим вопросам. Так что посмотрите отчет поближе — наверняка и e-mail найдете, и телефон.

Дальнейшие действия те же — отправка письма администратору сети с вложенным письмом злоумышленника. Пусть наводит порядок.

Разумеется, можно не затруднять себя расшифровкой текстового адреса, а сразу обратиться к базе данных http://www.ripe.net. Найти IP-адрес в заголовке будет непросто, если сеть, откуда письмо было отправлено, сложноструктурированная. Анализ заголовка может ничего не дать, если письмо отправлено через специальный сервер отправки анонимных писем или с помощью особой программы. Но в любом случае можно определить IP-адрес первого неподконтрольного негодяю сервера и, если ситуация достаточно серьезная, отправить его администрации просьбу помочь выследить вредителя.

* * *

Не бойтесь «сетевых опасностей». Они не опаснее реальной жизни. Но все же готовьтесь к войне, и будете жить в мире.

Net-news

Позиционирование с помощью Wi-Fi

Специальная группа Intel завершает разработку проекта дистанционного определения местоположения клиента с ноутбуком, подключенным к сети с использованием Wi-Fi. Точность позиционирования заявлена на уровне нескольких метров.

Принцип системы — анализ разницы времени прихода на узловые станции стартовых пакетов связного протокола и различия амплитуды несущей сигнала на разных станциях, благодаря чему воможна персонификация и территориальная локация клиента, которому пересылается (или от кого получается) та или иная информация.

По словам разработчиков, система исключает перехват данных легального клиента, то есть злоумышленник, припарковавший свой автомобиль вблизи офиса конкурента или даже взобравшийся на чердак дома, не сможет получить от ближайшей Wireless Access Station данные, ему не предназначенные, а сам факт попытки перехвата будет зафиксирован в логах провайдера, которые доступны как пользователю, так и силовым ведомствам государства.

В качестве аргумента для продвижения новой системы позиционирования приводятся случаи оказания клиенту помощи при нападении гангстеров, похитителей и хулиганов. Кроме того, технология существенно упростит поиск украденных ноутбуков. Ноутбук с указанной системой сам подаст сигнал о краже службам локального провайдера и спецподразделениям ближайшего полицейского участка.

Наконец, она позволит выявлять и отключать от сети распространителей спама и вирусов. Правда, как известно, благими намерениями вымощена дорога в ад. Не получить бы в итоге виртуальное вселенское гестапо...

Проект мирового Интернет-правительства провалился

Проект создания мирового правительства в сети Интернет, усиленно проталкиваемый США, Великобританией и их союзниками из Прибалтики, неожиданно натолкнулся на айсберг национальных интересов, которыми не намерен жертвовать ряд независимых стран. Они не согласились с идеей передачи своих суверенных прав в руки мифического «мирового сообщества». В итоге в Женеве за три недели согласовано не более 10% документов.

Предполагалось, что функции Интернет-правительства будет исполнять выборный неправительственный комитет. Он должен решать вопросы наднационального арбитража в деле обмена информацией, регулирования информационных прав граждан и стран, стандартизации технологий и программных средств, интеллектуальной собственности и миллион иных вопросов, включая виртуальный терроризм.

Дабы спасти положение, оргкомитет (представленный почти полностью прибалтами) предложил провести новые переговоры в октябре, но это предложение не прошло. Скорее всего, сессия в Женеве будет признана НЕСОСТОЯВШЕЙСЯ, а запланированное на октябрь окончательное подписание документов — перенесено на неопределенный срок.

Троян отключает антивирусы

Эксперты SophosLabs предупредили о появлении троянской программы, распространяемой через спам-письма, которая пытается отключить антивирусное и другое защитное ПО. В рассылаемых спам-письмах нет текста в поле «Тема:», но есть текст «new price» в теле письма и вложенный файл, который может иметь разные имена, но со словом *price*. Внутри архива файл price.exe, который и является троянской программой Troj/BagleDI-U отключающей защитное ПО.

Дмитрий Костяхин,
Генеральный директор PeterHost.Ru

По данным исследования, проведенного недавно в рамках программы ЮНЕСКО «Информация для всех» (IFAP), размер ущерба от деятельности спамеров для российских интернет-пользователей составляет не менее 30 миллионов долларов в год, или 2,5 миллиона долларов в месяц.

Цена вопроса

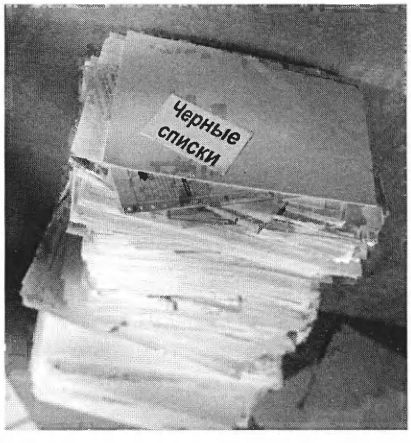
Если для обычного пользователя, который получает несколько писем в день и просматривает их в свободное время, отсортировать свою почту вручную не составляет труда, то для компаний, которые ведут по e-mail деловую переписку, общаются с клиентами и получают заказы, потери от спама могут быть очень значительными. Они складываются, во-первых, из затрат на входящий трафик. Элементарный подсчет: например, компания подсоединена через выделенную линию и платит $30 за гигабайт. В день приходит в среднем 100 Мбайт почты, то есть 3 Гбайт в месяц, но из них в среднем 2,7 Гбайт являются спамом. Таким образом, из общей ежемесячной платы за трафик ($90), $81 будет потрачен впустую. К этому нужно добавить значительные потери рабочего времени, которое тратит сотрудник на сортировку писем. Например, на мой рабочий ящик в день приходит около двух тысяч писем. У человека, активно работающего с электронной почтой, на удаление спама может уходить до получаса в сутки. А если этот человек к тому же занимает руководящую должность, то даже полчаса стоят совсем недешево. К тому же при большом объеме входящей почты очень легко ошибиться и случайно удалить нужное письмо. В таких случаях выгоднее отказаться от ручной сортировки писем и приобрести специальную программу, так называемый «антиспам».

Профессия: спамер

Программы «антиспам» появились как защитная реакция на действия недобросовестных рекламодателей, засоряющих почтовые ящики пользователей. Чтобы понять принцип работы «антиспама», нужно посмотреть на проблему с другой стороны — определить, каким образом действует профессиональный спамер.

На заре своей «карьеры» спамеры поступали примитивно: массовая рассылка писем шла с одного сервера, который, например, можно было запросто взять в аренду. Соответственно, первым и на тот момент весьма эффективным способом борьбы со спамом было занесение IP-адреса компьютера, с которого происходила рассылка спама, в так называемые «черные списки» (blacklists). «Черные списки» составлялись и обновлялись энтузиастами (у истоков этого движения стоял Пол Викси и организаторы проекта ORBS), системному администратору при настройке почтового сервера достаточно было указать тот «черный список», которым он хочет пользоваться, которому он доверяет. И все — с этого момента вся почта, приходящая на mail-сервер, фильтровалась по указанному «черному списку». В случае, если письма приходили с нежелательных адресов, они автоматически удалялись.

Но в последнее время эффективность этой технологии снизилась. Отчасти это связано с тем, что «черные списки» превратились в своеобразный политический инструмент в руках владельцев, и туда заносятся IP-адреса не только спамеров, но и, например, неугодных провайдеров. В результате все пользователи этого провайдера не могут отправить почту на серве-



ры, использующие этот «черный список». Потери в итоге несут обе стороны: ведь недошедшее письмо может оказаться очень важным. При этом в «черный список» легко попасть, но чрезвычайно сложно из него выбраться. В отдельных случаях за исключение из blacklist могут даже вымогать деньги. У нашей компании был такой неприятный прецедент с Sorbs.

Но главная причина того, что «черные списки» сегодня теряют актуальность, заключается в смене тактики работы самих спамеров, которые теперь действуют гораздо изощреннее.

В арсенале современного спамера обязательно присутствует «шпионское программное обеспечение» — программы-вирусы (трояны), предназначенные для проникновения на компьютеры пользователей и контроля за ними. «Заразиться» таким вирусом пользователь может или получив письмо с ним по электронной почте, или скачав троян с какого-нибудь сайта, где он находится в виде exe-файла и предложен, например, в качестве интересной игрушки. Установленный в системе вирус позволяет спамеру не только следить за всеми действиями пользователя (просматривать, на какие сайты он заходит, какие пароли и логины вводит), но и полностью их контролировать.

Зараженные компьютеры называются «зомби», и таких «зомби» по всему миру сейчас очень много. Одной из причин является то, что за границей системы антивирусов используются гораздо реже, так как стоят достаточно дорого. Тысячи «зомби» формируют botnet — сеть из зараженных компьютеров, которые подключаются к указанному вирусом серверу и ждут команды. Как только спамер получил заказ, он оповещает всех своих «зомби» о том, что нужно начинать рассылку, предоставляет им нужный текст и список IP-адресов. После этого зараженные компьютеры, если они в данный момент подключены к Интернету, без ведома пользователя начинают отправлять тысячи писем. Сегодня botnet и список электронных адресов можно купить или взять в аренду.

Проблема заключается в том, что спам идет сразу с 10 тысяч IP-адресов, и люди, которые владеют этими IP-адресами, в принципе, не виноваты. Поэтому внесение их в «черные списки» не поможет решить проблему. Профессиональные провайдеры сегодня используют специальное программное обеспечение и рекомендуют своим пользователям использовать другие способы борьбы со спамом.

На каждый спам свой фильтр

На смену составлению «черных списков» пришел способ контентного анализа, то есть анализа содержимого письма. На его основе как раз и работают фильтры «антиспам». При поступлении письма на сервер оно всесторонне изучается: анализируется, откуда пришло, есть ли обратный адрес, как подписано, есть ли в тексте заглавные и латинские буквы, выделены ли они жирным шрифтом и т. д. Тщательно изучается содержание письма и делается частотный анализ использованных слов. Известно, что в спаме часто присутствует реклама самой спам-рассылки, виагры, порнографии, казино; в зависимости от сезона может появляться новая актуальная тема (например, курорты — летом, специальные предложения — к праздникам).

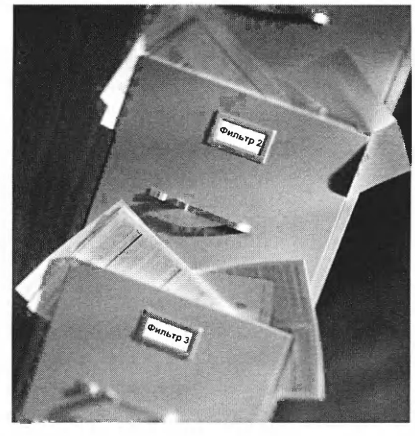
Этот набор самых типичных для рекламных писем слов хранится в памяти «антиспама» и постоянно обновляется производителями программ. Фильтр оценивает письмо по ряду параметров и на основе математического метода за каждый из них выставляет определенный балл. Потом эти баллы суммируются и получается общая оценка «спамоватости» каждого письма. В зависимости от настроек, которые системный администратор сделает на сервере, есть определенный порог — количество баллов, после которого письмо признается спамом. При этом фильтр можно регулировать, то есть для каждого параметра повышать или снижать значимость.

Метод контентного анализа может быть совмещен с использованием «черных списков»: если письмо пришло с IP-адреса, внесенного в «черный список», оно не отсеивается сразу, вместо этого ему добавляется определенный балл. Решение об удалении письма может быть принято автоматически на основании превышения количества баллов.

Но если работа подразумевает ведение важной переписки, то можно установить режим, когда все письма проходят к пользователю, но при этом размечаются по принципу спам — не спам. В таком случае почтовая программа может их сортировать, отправляя спам в отдельную папку. Например, вероятность ошибки установленного у меня фильтра — около 0,5%, то есть из 200 писем, помеченных как спам, одно оказывается нужным.

На основе технологии контент-анализа можно отфильтровать до 80-90% спама. Однако движение спамеров тоже не стоит на месте. В последнее время их действия направлены на засорение «частотных» фильтров —программ, которые сортируют письма по признаку частоты употребления «нежелательных» слов в рассылке. Реклама разбавляется совершенно отвлеченным текстом, например, цитатой из Пушкина. Причем каждое письмо идет со своим вставным текстом, поэтому зачастую очень сложно определить, какими словами пополнять частотный фильтр. К тому же, если содержание письма очень «критично» и фильтр наверняка не пропустит его, спамеры могут видоизменять все «чувствительные» слова: например, заменять «о» на ноль, делать грамматические ошибки, писать через пробел, вставлять вместо слова картинку и т. д.

В связи с этим как вариант контентного способа может рассматриваться установка частотного фильтра, но уже непосредственно на компьютере пользователя. «Обучение» такого фильтра ведет сам пользователь. Указы-



вая, какие письма являются спамом, а какие — нет, он постепенно формирует свою индивидуальную базу.

Еще один способ защиты — доставка писем с подтверждением. В этом случае почтовая программа выкачивает всю почту с сервера, и далее фильтр определяет, есть ли отправитель письма в списке доверенных лиц получателя. Если нет, то программа отправляет письмо обратно с просьбой перейти по ссылке или написать еще одно письмо, чтобы быть внесенным в доверенные лица. Расчет делается на то, что указанное действие программа, рассылающая спам, совершить не в состоянии. Однако способ обладает рядом существенных недостатков: во-первых, доставка почты сильно задерживается, а во-вторых, письма, которые отсылаются роботами, но не являются спамом (например, вам выслали логин и пароль), скорее всего, не дойдут.

На практике

Пользователям почтовой программы The Bat! можно порекомендовать специальный плагин — частотный фильтр с обучением BayesIt! Для серверов неплохими вариантами будут технология «Спамтест» лаборатории Касперского (www.spamtest.ru) или «Спамоборона» от Яndex (www.so.yandex.ru).

Бесплатные почтовые службы также используют встроенные фильтры, но, как и многие вещи, рассчитанные на массовую аудиторию, они не гарантируют надежной зашиты. Провайдеры, предлагающие услугу платной электронной почты, вместе с ней должны предоставлять и программы «антиспама».

Например, в компании PeterHost.Ru вся корреспонденция сначала проверяется антивирусом Clam AntiVirus. Мы даже составляем рейтинг самых популярных вирусов, отловленных за день; его можно посмотреть на нашем сайте www.peterhost.ru в разделе «статистика». Затем фильтруем почту по собственным «черным спискам». Поскольку мы являемся одним из крупных почтовых провайдеров, такие списки составляем сами. Проверяются также различные технические параметры: например, наш почтовый сервер сразу отсеивает письма, отправленные с несуществующих e-mail-адресов. Таким образом, серьезная первичная обработка осуществляется еще до того, как письмо дойдет до фильтра. На этом этапе отсеивается примерно 48% писем. Оставшиеся пропускаются через фильтр, и около 75% из них помечается как спам.

Профилактика

Конечно, всем известно, что лучший способ борьбы со спамом — не иметь почтового ящика. Но уж если вы решили его себе завести, лучше с самого начала стараться свой e-mail нигде не «светить». Для этого можно порекомендовать:

1. Не оставлять свой настоящий (деловой) адрес на досках объявлений, в гостевых книгах, форумах, не вывешивать на свой сайт. У спамеров существуют программы, которые работают по принципу поисковых систем: они собирают e-mail-адреса пользователей на форумах, чатах, досках объявлений. Если все-таки есть необходимость указать свой настоящий адрес, то лучше как-то его видоизменить. Например, значок @ заменить словом [собака] или картинкой. Тогда адрес будет иметь вид: имя[собака]mail[точка]ru.

2. Для «публичных» целей лучше специально завести второй e-mail.

3. Если уж спам пришел, никогда на него не отвечайте. Иногда спамеры делают пробные рассылки. Например, берут популярный домен, такой как mail.ru, подставляют перед ним разные имена (masha@mail.ru, anton@mail.ru и т.п.) и пишут сообщение вида «Привет, ты еще здесь?» или «Если вы не хотите, чтобы вам приходило это письмо, напишите нам». В случае ответа спамер делает вывод, что адрес «живой», и заносит его в свою адресную базу.

4. Помните, что если у человека, с которым вы общаетесь, стоит почтовая программа Outlook, то вы тоже можете оказаться в адресной базе данных спамера, так как очень многие вирусы при проникновении на компьютер крадут адресную книгу из Outlook и высылают ее спамеру.

5. Базу данных e-mail-адресов организаций легко составить по различным каталогам и справочникам.

Net-news

Провайдеры отказываются оплачивать перехват информации спецслужбами

Большая группа интернет-провайдеров в Нидерландах (Xs4all, KPN Telecom, Casema, @Home, Wanadoo, T-Mobile, Telfort, Vodafone и Orange) планирует подать иск против правительства с целью получить компенсацию за монтаж специального оборудования для перехватывания информации спецслужбами страны. К примеру, Xs4all пришлось потратить на это 500 тыс. евро.

Соответствующие положения содержались в законе о телекоммуникациях, подписанном еще в 1998 году. Правительство Нидерландов считает, что это нормально, когда операторы связи несут некоторые расходы на поддержку правоохранительной деятельности общества, однако операторы не согласны с такой постановкой вопроса, ссылаясь на то, что в других европейских странах (Италия, Финляндия, Франция и Великобритания) интернет-провайдерам уже давно компенсируют все затраты на монтаж специального оборудования и перехват данных.

Еще одна надвигающаяся угроза — предложение со стороны Евросоюза принять обязательство по сохранению данных телефонных звонков и логов доступа к глобальной сети на протяжении от одного до трех лет.

Троян — защитник морали

В Интернете появился троян Yusufali-A, который прерывает навигацию по порносайтам, высвечивая на экране цитаты из Корана.

Троян анализирует содержимое строки заголовка сайта в текущем окне.

Обнаружив такие слова, как «teen», «xx», «sex» или «penis», он закрывает окно, а вместо страницы сайта высвечивает на экране цитату из Корана.

Если неприемлемый сайт остается открытым, троян Yusufali-A продолжает высвечивать цитаты и через некоторое время выдает на экране кнопку с названием «For Exit Click Here». Как только мышка ПК начнет двигаться, на экране появится окно с текстом «OH! NO i'm in the Cage» и кнопками LogOff, ShutDown и Restart, а указатель мышки оказывается заблокированным в границах окна. Нажатие любой из кнопок ведет к завершению сеанса работы с компьютером.

В отличие от других злонамеренных программ, которые пытаются похитить деньги или конфиденциальные данные, эта выступает как защитник морали — блокирует наблюдение веб-сайтов, которые трактует как неприемлемые.

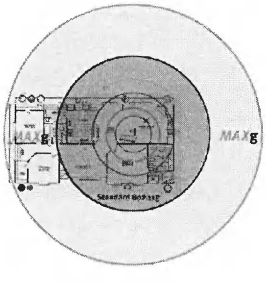
MAXg извлекает из стандарта g максимум

U.S. Robotics представила в Санкт-Петербурге MAXg — свое семейство продуктов для разворачивания беспроводной локальной сети на основе действующего стандарта IEEE 802.11g (Wi-Fi). MAXg предназначен для охвата целого дома или небольшой организации.

Основные особенности:

- 50-процентное увеличение радиуса действия по сравнению со стандартом 802.11g (при условии совместимости и в зависимости от архитектурной среды);
- Пропускная способность 125 Мбит/с (фактическая скорость передачи данных может меняться в зависимости от внешних условий и расстояния между устройствами и узлами доступа);
- Полная совместимость со всеми продуктами 802.11g и 802.11b

К тому же U.S. Robotics предельно упростила установку MAXg и повысила уровень безопасности. Сеть устанавливается за пять минут и полностью защищается за десять.



Это не первая линейка U.S. Robotics в области Wi-Fi. В 2002 году компания впервые вышла на этот рынок, предложив решение USR Turbo. Тогда оно стало первым, предложившим скорость передачи данных 125 Мбит/с.

Россия вошла в TOP 20 по «выделенкам»

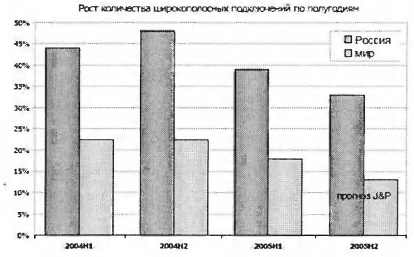
По результатам исследования, проведенного компанией J'son&Partners, российский рынок широкополосного доступа по динамике роста опережает все крупнейшие рынки мира. Ожидается, что к началу 2007 года в регионах в сумме будет уже больше «выделенок», чем в Москве.

В первом полугодии количество выделенных подключений в России составило 1,24 млн, а по итогам года ожидается рост на 85%. Таким образом, Россия занимает сейчас 19-е место в мире по количеству широкополосных подключений и 9-е место — по темпам роста.

Конечно, 1240 тыс. широкополосных подключений в России выглядят не очень внушительно по сравнению с 38 миллионами в США или 31 миллионом в Китае, однако Россия с первой попытки вошла в Топ 20 рейтинга Point-Topic по количеству широкополосных подключений, расположившись на 19-м месте между Швецией и Польшей.

Правда, в Москве и области распространенность широкополосного доступа (4,4 широкополосных подключений на 100 жителей) вполне сопоставима с уровнем Венгрии, Польши, Чили, зато показатели остальной России крайне низки — 0,4 подключения на 100 жителей, примерно как на Ямайке и в Таиланде.

Российский рынок широкополосного доступа растет в первую очередь за счет «квартирного» сегмента: количество домашних подключений за полугодие выросло более чем в 1,5 раза и достигло 870 тыс., при этом 85% новых широкополосных подключений приходится на индивидуальных пользователей, и только 15% — на корпоративный сегмент рынка.



Очевидный лидер роста среди технологий — DSL-подключения: за 6 месяцев их количество выросло на 62%, а если учитывать только домашние подключения, то рост DSL-рынка составил почти 80%.

Впрочем, наиболее популярным способом подключения у домашних пользователей остается Ethernet от «домовых» сетей. В сумме у них в 2,7 раза больше абонентов, чем у DSL-операторов.

Быстрее, чем Wi-Fi

Airgo Networks разработала два новых чипа беспроводной связи, которые позволяют создавать более скоростные и удобные домашние сети. По заявлению компании, новые чипы смогут обеспечить скорость передачи данных 240 Мбит/с, ускорят беспроводные сети вчетверо по сравнению с существующими сетями Wi-Fi (обычная скорость 54 Мбит/с). Даже с учетом факторов, снижающих реальную скорость передачи данных, новые чипы все равно будут быстрее, чем обычная проводная Ethernet-сеть (100 Мбит/с).

«Мы достигли поворотной точки, — говорит глава компании г-н Ралей, — Беспроводные сети становятся быстрее проводных».

В основе технологии лежит использование интерференции волн для одновременной передачи по радиоканалу большего объема данных. Она получила название MIMO OFDM (многоканальный ввод, многоканальный вывод и мультиплексирование с ортогональным делением частот).

По словам Ралея, технология Airgo совместима с существующим стандартом Wi-Fi (802.11a/b/g), однако чипы Airgo дают большую, чем Wi-Fi, площадь покрытия: с их помощью можно охватить дом целиком, тогда как большинство сетей Wi-Fi способны охватить лишь пару комнат.

Google hacking
ГОРЕ ОТ УМА

Анатолий Ковалевский (С.-Петербург)

Владеющий информацией владеет миром. Истина избитая, но от того не переставшая быть правдой. Поисковая машина Google обработала большинство интернет-сайтов и сохранила результаты на своих серверах. Причем, если текст на сайте уже удален, то в кэше он еще, возможно, сохранился. Нужно только знать, что и как спрашивать. В результате появилось новое направление информационной атаки — google hacking, взлом при помощи поисковика www.google.com.

Поскольку поисковик Google хранит пентабайты информации, полученной от различных серверов Интернета, к настоящему времени из инструмента поиска данных он превратился в мощное оружие вторжения.

Дело в том, что некоторые из серверов при формировании (сознательном или случайном) неправильного запроса отвечают служебной информацией, содержащей IP-адрес, детали логина или какие-либо параметры конфигурации внутренней сети. Например, известно такое развлечение: находят адрес сетевого принтера, подсоединяются к нему и шутки ради печатают какую-нибудь глупость типа «Глюк — это когда компьютер играет с нами, а не мы с ним», «Компьютер — это полнейший идиот с феноменальной памятью» или «Если долго портить машину, она сломается». Причем печать идет, пока бумага не кончится. Или другой пример — введем в строку поиска «not for distribution» confidential, и через 0,17 секунды получим 12300 страниц, отвечающих этому запросу. А еще год назад ссылок было в 7 раз меньше...

Орфография, пунктуация, синтаксис

Сначала поговорим о том, на каком языке будем разговаривать с Google. Знание языка запросов поможет нам не только во взломе, но и для более корректного составления обычных запросов. Знак «+» заставляет Google включать в поиск слова, которые он не считает важными. В английском языке это вопросительные слова, предлоги и артикли (are, of, where и т. д.). Знак «—» делает то же самое, но с точностью до наоборот. Искать не только указанное слово, но и его синонимы поможет знак «~». «По умолчанию» Google ищет на каждой странице все вхождения слов из строки запроса без учета их взаимного расположения. Чтобы заставить искать точную фразу, ее нужно взять в кавычки. Чтобы найти хотя бы одно из указанных слов, надо применить логический оператор OR (или). Знак «*» позволяет обозначить любое слово или любую букву в слове (последнее особенно актуально, когда правильное написание точно не известно).

Однако это не все, есть еще операторы, которые и позволяют сделать из Google нечто большее, чем поисковая машина. Итак, оператор link: показывает все сайты, ссылающиеся на указанную страницу. Оператор cache: показывает содержание сайта в кэше Google, то есть таким, каким оно было, когда робот Google в последний раз посещал эту страницу. Оператор intitle: ищет указанное слово только в заголовке страницы, а allintitle: ищет несколько указанных слов. Оператор site: ограничивает поиск только по указанному сайту (указываем доменное имя или IP-адрес). Оператор filetype: позволяет искать только в файлах определенного типа — Google работает как минимум со следующими форматами:

Adobe Portable Document Format	pdf
Lotus 1-2-3	wk1, wk2, wk3, wk4, wk5, wki, wks, wku
MacWrite	mw
Microsoft PowerPoint	ppt
Microsoft Works	wks, wps, wdb
Rich Text Format	rtf
Text	ans, txt
Adobe PostScript	ps
Lotus WordPro	lwp
Microsoft Excel	xls
Microsoft Word	doc
Microsoft Write	wri
Shockwave Flash	swf

Остальные операторы можно посмотреть на www.google.com/help/operators.html. Так вы сможете задать язык результатов, дату, настроить точку вхождения, включить безопасный поиск и т. д. Единственное, что надо помнить, — не должно быть пробелов ни между поисковым знаком и словом, ни между названием оператора и словом.

Лопатки чешутся от прорезающихся крыльев?

И что же мы можем в результате? Можно составить карту сайта (оператор site:). В результате у вас на руках будут все ссылки, даже те, которые создаются динамическими скрипами. И что самое забавное — владельцы исследуемого сервера даже не узнают, что вы исследовали их сайт, поскольку запросы направляются к кэшированным страничкам Google.

Некоторые ОС (не будем тыкать пальцем) при установке сразу запускают веб-сервер, о чем многие пользователи даже не подозревают. Поэтому можно поискать тестовую станицу, которая устанавливается при инсталляции сервера, — если она есть, значит, высока вероятность, что компьютер не подвергался настройке и, значит, уязвим для атаки:

intitle:Test.Page.for.Apache it.worked!

allintitle:Welcome to Windows 2000 Internet Services

Можно запросить версию ОС веб-сервера, а также версии софта, который там крутится. Поясню: знание версий ПО сервера — это первый шаг для атаки на сайт, поскольку можно легко сопоставить версию ПО и дырки в системе безопасности, которые характерны именно для нее. После этого достаточно сконфигурировать рабочий эксплойт (крошечная программка, созданная с единственной целью, — используя определенную уязвимость проникнуть на компьютер и передать управление хакеру) — и сервер у вас в руках. Да, подобное проникновение возможно только в том случае, если владелец сервера не устанавливает path-заплатки на открытые уязвимости, а хакер не боится попасть в тюрьму за незаконные действия.

Можно использовать Google как cgi-сканер на поиск уязвимых скриптов, которых набрался уже целый список:

/cgi-bin/cgiemail/uargg.txt
/random_banner/index.cgi
/random_banner/index.cgi
/random_banner/index.cgi
/cgi-bin/mailview.cgi
/cgi-bin/maillist.cgi
/cgi-bin/userreg.cgi
/iissamples/ISSamples/SQLQHit.asp
/iissamples/ISSamples/SQLQHit.asp
/SiteServer/admin/findvserver.asp
и многие другие.

Вот еще примеры google hacking:

#mysql dump filetype:sql — дампы баз данных mySQL.

Host Vulnerability Summary Report — узнаете, какие еще уязвимости бывают.

filetype:conf inurl:firewall-intitle:cvs — конфигурационные файлы файерволов.

intitle:index.of finances.xls — в чужой кошелек заглянуть не желаете?

intitle:Index of dbconvert.exe chats — логи icq чата, там могут лежать пароли.

intitle:index.of ws_ftp.ini — конфигурационные файлы ftp.

inurl:ipsec.secrets holds shared secrets — секретные ключи. От чего? А от всего.

intitle:Index of pwd.db — пароли.

intitle:index.of master.passwd — пароли.

inurl:passlist.txt — пароли.

intitle:index.of administrators.pwd — пароли.

filetype:htpasswd htpasswd — пароли

filetype:xls username password email — пароли

filetype:properties inurl:db intext:password — пароли

filetype:cfm cfapplication name password — пароли

index of /password — пароли

index of / +passwd — пароли

index of / password.txt — пароли

И это далеко не полный список.

А что интересного можно найти, если взламывать вы ничего не собираетесь? Да море. Заходим на сайт крупной автомобильной, чипсетостроительной или любой другой технической компании и начинаем искать файлы не для публикации в форматах doc, ppt или pdf. Уверяю, вы будете поражены открытиями. Если ничего не обнаружится, откройте файл robots.txt (он лежит в корне сервера) и посмотрите, какие директории закрыты.

Другой вариант — зная структуру сайта, можно получить доступ к хранилищу картинок или флэш-мультиков, которые на веб-ресурсе закрыты скриптами.

Желающего идти судьба ведет, не желающего — тащит

Как защититься от взлома:

1. Даже временно не выкладывайте важные данные на веб-сервер. Можете забыть об этом, или кто-то успеет скопировать их даже за короткий срок. Если так уж неймется использовать сервер для передачи информации — держите на нем конфиденциальные данные только в зашифрованном виде.

2. Регулярно проверяйте свой сайт, основываясь на описанных выше методах. За новыми вариантами веб-взлома заходите на сайт Johnny Long www.johnny.ihackstuff.com.

3. Хотя бы раз прочитайте правила настройки роботов-индексаторов. Там указано, как сделать, чтобы поисковик не индексировал сайт или его часть, а уже проиндексированное удалил (www.google.com/remove.html). Хотя для большинства описанных действий вам понадобится подтвердить факт владения сайтом и, возможно, поместить на сайте файл-сертификат. Можно положить в корень сайта файл robots.txt, в котором после слова Disallow будут указанны разделы, запрещенные для индексации.

4. Помните, что Google — только один из поисковиков, поэтому лучшим способом защиты будут действия, описанные в п. 1. Да и своевременно устанавливать заплатки на инсталлированное на сервер ПО никто кроме вас не будет.

Curiosity killed the cat — говорят англичане, а русский эквивалент этой поговорки — Любопытной Варваре нос оторвали. Учтите, что существуют сайты, которые призваны следить за теми любопытными людьми, что ищут дырявые версии программ и неправильно сконфигурированные серверы. Этакие ООО. Нет, не Общества с Ограниченной Ответственностью, а Отделы Охотников за Охотниками. Например, www.gray-world.net/etc/passwd/.

Эта статья — не руководство к действию. Она написана "чтобы помнили". Будьте бдительны. Наступайте на грабли только для того, чтобы поднять их с земли.

СЕТЬ: ДЛЯ ХАКЕРОВ И БОРЦОВ С НИМИ

Игорь Ананченко (С.-Петербург)

В Интернете представлено много разных сайтов, на которых в том или ином аспекте рассматриваются вопросы компьютерной безопасности, взлома и противодействия таким попыткам. При желании и умении в Сети можно найти практически все — от записок школьников о том, как быстро и просто крякнуть ту или иную игру, до веб-сайтов и порталов, представляющих серьезные коммерческие разработки в области систем безопасности, антивирусные программы, системы шифрования данных. Информации много, и качество ее тоже разное. В этом небольшом обзоре я расскажу о ресурсах Интернета, знакомство с которыми будет полезно тем, кто не является специалистом в области компьютерной безопасности, но хочет существенно повысить свой уровень знаний.

Настоящему хакеру диплом или сертификат, подтверждающий профессиональные знания, ни к чему. Поскольку его область деятельности скользкая и противозаконная, секреты «профессии» оберегаются особенно тщательно. Да и вообще, нет такой профессии, как, например, специалист по взлому банковских систем, хотя профессионалы есть. Просто их мало, и найти их бывает не просто даже товарищам из компетентных органов.

Обласканный начальством хакер на постоянном довольствии — уже и не хакер вовсе, а дипломированный специалист по компьютерной безопасности. Хотя, на мой взгляд, быть хорошим специалистом в области безопасности намного трудней, чем хакером, потому что для проникновения в защищенную систему нужно найти всего одно слабое место в системе безопасности, тогда как для предотвращения взлома необходимо предусмотреть и закрыть все потенциальные уязвимости, которыми может воспользоваться нарушитель. Надежная защита — вещь комплексная, достигаемая соблюдением административных, юридических и технических норм.

Для серьезного обучения

Для того чтобы стать профессионалом по защите информации с высшим образованием, необходимо изучить множество профилирующих и смежных дисциплин, а само обучение займет несколько лет. Тем, кого не пугает такая перспектива, рекомендую взглянуть на примерный учебный план специальности 075300 «Организация и технология защиты информации» (очная форма обучения) на http://db.informika.ru/spe/plan_zip/075300P.html. Обучающимся по специальности читаются, в том числе, такие курсы, как «Комплексная система защиты информации на предприятии», «Защита информационных процессов в компьютерных системах», «Криптографическая защита информации», «Программно-аппаратная защита информации».

Не только эта, но и другие специальности, связанные с защитой, есть во многих технических вузах. Например, «Информационную безопасность телекоммуникационных систем» можно изучить в Российском Государственном Гидрометеорологическом Университете (http://dovus.rshu.ru/priem_kom/priem.asp).

Не останавливаясь подробно на программах учебных курсов, отмечу, что типовые образцы программ также можно без особого труда найти в Интернете (например, программа дисциплины «Программно-аппаратные средства обеспечения информационной безопасности» — http://www.aiv.spb.ru/ufiles/programma.doc).

Курсы, очные и заочные

Высшее образование хорошо, особенно второе или третье, но возможность получить его есть не всегда, да и не всегда надо. Не каждый пользователь персонального компьютера захочет стать профессионалом по компьютерной безопасности, но получить знания о том, как настроить файервол, установить антивирусную программу или межсетевой экран хотят многие. В Интернете представлено множество организаций, специализирующихся на чтении очных и заочных курсов по разным аспектам компьютерной безопасности. Некоторые организации, например, центр компьютерного обучения «Специалист» при МГТУ им. Н.Э.Баумана (http://www.specialist.ru), обеспечивают оба варианта обучения. В заочном режиме можно пройти семь курсов из раздела «Информационная безопасность», например, курс «М2823 Настройка и администрирование безопасности в сетях Microsoft Windows Server 2003» (http://www.specialist.ru/

programs/course.asp?idc=572), читаемый в соответствии с официальной учебной программой авторизованного курса Microsoft.

Курсы по информационной безопасности можно прослушать и на факультете переподготовки специалистов Санкт-Петербургского государственного политехнического университета (http://www.avalon.ru/it_courses/scp/), и в ряде других организаций.

Конечно, хорошее образование стоит денег, но отдать сто долларов и более за заочный курс готов не каждый. С этих позиций весьма привлекательна возможность обучения в Интернет-Университете Информационных Технологий (http://www.intuit.ru/), где возможно как дистанционное бесплатное, так и очное платное обучение. В разделе «Безопасность информационных технологий» любой желающий может изучить четыре курса: «Протоколы безопасного сетевого взаимодействия», «Криптографические основы безопасности», «Стандарты информационной безопасности» и «Основы информационной безопасности». К каждому курсу доступен конспект лекций, которые можно читать в режиме on-line или же распечатать. После каждой лекции предлагается небольшой тест для самопроверки знаний.

Завершив курс обучения, можно сдать экзамен и получить сертификат. Можно попробовать сразу сдать экзамен экстерном. Успешно сдавшие экзамен получают сертификат — ссылку на электронную версию сертификата можно разместить на собственном сайте или включить в резюме, отправляемое работодателю по электронной почте. Если необходима бумажная версия сертификата, придется заплатить 100 рублей. Можно получить русскоязычный или англоязычный вариант сертификата (или оба сразу, но за двойную плату).

Пройти тестирование в онлайн-режиме по курсу «Основы безопасности сетей» и получить сертификат можно в организации RetraTech (http://www.certifications.ru). Экзамен включает в себя такие темы, как основы криптографии, безопасность передачи данных по сетям, защита от внешних сетевых атак и защита информации на предприятии. В тесте 40 вопросов. Количество правильных ответов, необходимое для сдачи, — 28.

Пройти тест с тем же названием, но от другого разработчика, можно на сайте «Академия Велеса» (http://www.velesa.ru/). Кроме теста «Основы безопасности сетей» доступен тест «Организация безопасности сетей в Windows 2000». Тестирование бесплатное, а стоимость бумажной версии сертификата — 300 рублей.

Информация к размышлению...

Сертификаты и дипломы, подтверждающие знания в области защиты информации, весьма полезны при общении с работодателями, да и на чайников производят благоприятное впечатление. Однако сертификаты сертификатами, но иногда и честному человеку бывает нужно быстро и с минимальными усилиями преодолеть ту или иную защиту. Например, возвратившись из отпуска, вы узнали, что в ваше отсутствие успели не только поменять все пароли с уровнем доступа «администратор», но и благополучно потерять лист с новыми паролями. В общем, начинается увлекательная игра под названием «Взломай собственную систему с первой попытки». Конечно, можно полностью переустановить систему, но процесс это длительный и не слишком приятный. Так что информация о том, где можно найти софт для различного рода взломов, лишней не будет, к тому же собственную систему надо периодически проверять на взламываемость и затыкать дыры по мере их обнаружения.

Итак, небольшой, но, на мой взгляд, полезный список сайтов с различными инструментами для хакеров и борцов с ними.

1. http://www.passwords.ru/ — информационный сервер о технологиях парольной защиты. «Наши программы помогут вам восстановить потерянный пароль в течение нескольких секунд!». Например, «Proactive Password Auditor (PPA) — утилита для тестирования качества парольной защиты в операционных системах Windows NT, 2000, XP и Windows 2003 Server. Она позволяет системным администраторам находить аккаунты пользователей, имеющие пароли, не стойкие к перебору. Системный администратор также может найти пароль любого пользователя, используя прямой перебор и атаку по словарю.

Для получения хешей паролей могут использоваться следующие способы:

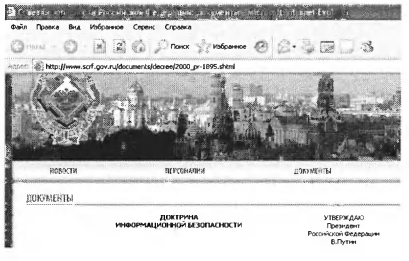
- использование готовых дамп-файлов, полученных утилитами pwdump, pwdump2 и pwdump;
- чтение реестра локального компьютера;
- чтение памяти локального компьютера;
- чтение памяти удаленных машин (поддерживаются компьютеры с Active Directory).

Восстанавливаются пароли на аккаунты LAN Manager и NTLM. Код программы оптимизирован по скорости перебора паролей.

2. http://www.astalavista.com/ ASTALAVISTA SECURITY GROUP. Information and Internet Security Portal. Полезная тематическая информация, в числе прочего есть ссылки на сайты с различными продуктами для взлома, новости, руководства. Но, к сожалению, сайт на английском.

3. http://www.xakepy.ru/ Portal of Russian Hackers — форум, подборка ссылок на программы для взлома и другие тематические сайты той же направленности.

Список сайтов можно продолжить и далее, но, думаю, и этого достаточно. На прощанье приведу адрес еще одного сайта, который тоже посвящен вопросам безопасности, хотя и несколько другой — http://www.scrf.gov.ru/ (САЙТ СОВЕТА БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ). На сайте представлена информация, имеющая прямое отношение и к компьютерным технологиям: «Доктрина информационной безопасности Российской Федерации» (http://www.scrf.gov.ru/documents/decree/2000_pr-1895.shtml).



МУЗЫКА, КОМПЬЮТЕР, Интернет

Передо мной сидят четверо молодых музыкантов группы «Lovecraft», возможно, будущих звезд. Я включаю диктофон, и...

— Для начала расскажите немного о себе. Кто есть кто в группе?

Ольга Пауль: Я — тиран и деспот этой группы! А если серьезно, то инициатор всего: пишу музыку, тексты, частично делаю аранжировки, а на сцене пою и соединяюсь в единое целое со скрипкой в порыве творческой страсти.

Ace of Magic: Дмитрий. Соло-гитарист.

Фауст: Егор. Играю на ударных.

Евгений Петрович: Евгений Петрович. И. о. бас-гитариста.

Ольга Пауль: Есть еще наша клавишница, Mulvina. Но ее похитили инопланетяне (обещали вернуть к ближайшему концерту), так что в интервью она участвовать не смогла.

Ace of Magic: В принципе, Оля и есть главный затейник этого бедлама, который вопреки всем законам природы продолжает существовать до сих пор.

Ольга Пауль: Группе немногим больше 3-х лет. За это время состав неоднократно менялся. Кстати, раньше мы и назывались по-другому — »Velvete».

— Откуда пришло название группы и что оно означает?

Ольга Пауль: Название, во-первых, созвучно с фамилией писателя, чьи книги мне нравятся, — Говарда Лавкрафта. Во-вторых, если разделить «Lovecraft» на два слова, то получится «Love Craft», то есть «Искусство любви». Когда мы думали о смене названия группы, мне на глаза попалась книжка Лавкрафта, и все было сразу решено...

Фауст: Кстати, название наше вовсе не связано с популярными играми «Warcraft» и «Starcraft»! А то меня уже достали такими вопросами.

— В процессе создания или обработки музыки вы используете компьютер?

Ольга Пауль: Компьютер мы обязательно используем во время записи и редактирования нот. При создании музыки пока что не приходилось. Правда, теперь у Мульвины новые клавиши, так что ей придется изрядно поработать с компом, так как там туча неотредактированных звуков. Вот так со временем и понимаешь, что без компьютера музыканту — никак...

Ace of Magic: Я все же считаю, что при создании музыки живое воображение лучше. Вот для обработки — куда же без этого. В любой, даже самой дешевой студии стоит комп, и с его помощью, собственно, все и делается.

Евгений Петрович: Для использования компьютера при создании музыки нужно найти специалиста в этом деле, а их не так уж много. Это программистов у нас в стране пруд пруди...

— Сегодня многие музыканты считают, что синтезатор и другие компьютерно-музыкальные «примочки» — это инструменты, лишенные души, и что в настоящей музыке им не место. Что вы об этом думаете?

Ace of Magic: Я думаю, это такие же инструменты, как и все остальные, и каждый вкладывает в них свою душу как может.

Фауст: Душа инструмента напрямую зависит от музыканта, на нем играющего.

Евгений Петрович: Я тоже думаю, что если человек вступает во взаимодействие, например, с синтезатором, вкладывая душу, энергетику и все оставшиеся силы, то и результат, безусловно, будет излучать оттенки «живой» музыки.

— Каково ваше мнение о музыке синтезированной, полностью созданной компьютером?

Ольга Пауль: Она на любителя. Не могу сказать, что мне она вся по душе, хотя некоторые вещи я слушаю — в основном расслабляющую и танцевальную музыку.

Ace of Magic: Компьютер — всего лишь инструмент. Любую музыку можно делать хорошо, а можно и плохо. Каждый делает как умеет и на том, на чем умеет.

Фауст: Если честно, то я не испытываю к электронной музыке особой симпатии. Какая-то она игрушечная...

Евгений Петрович: Живую и электронную музыку можно сравнить с общением между людьми: с глазу на глаз и, допустим, по телефону. Во втором случае нет главного — присутствия человека. Так что мне по душе больше музыка, созданная человеком.

— По вашему мнению, электронная музыка изживет традиционную?

Ace of Magic: Я считаю, что нет. Электронная музыка занимает отдельную нишу и имеет такое же право на существование, как и другие стили. Как говорится, «это две большие разницы, и сравнивать их нельзя».

Фауст: Нет, я думаю, электроника никогда не заменит живых людей! Ведь профессионально сыграть на инструменте — это вам не пару кнопок на компьютере ткнуть.

Евгений Петрович: Пока будет жив человек, будет жива и традиционная музыка. Это естественная потребность. Так что, скорее всего, в итоге получится нечто среднее. Крайности, я думаю, исключены.

— Какая мелодия стоит на вашем сотовом и почему?

Ольга Пауль: На старом мобильнике у меня стоит «Paranoid» Black Sabbath, «Light My Fire» The Doors, «Funeral Of Hearts» и «Sacrament» HIM. На новом какие-то неизвестные мне темы, одна — явно восточная...

Ace of Magic: У меня сейчас там саундтрэк к фильму «Полицейский из Беверли Хиллс». Просто он мне нравится.

Фауст: У меня стоит стандартная «Нокиевская» мелодия, «Croak». Дело в том, что у меня давно не работает вибровызов, а в университете, например, просто необходимо, чтобы телефон работал тихо и никому не мешал. Вот я и нашел выход из ситуации.

Евгений Петрович: Robert Miles — «Childrens». Одна из электронных вещей, которая мне нравится. А выбор пал на нее, ибо лишь ею выбор мой и ограничен. Остальные мелодии на сотовом — заводские...

— Как творческие личности, что вы вообще думаете о «мобильной музыке»? В частности, с использованием формата MP3?

Ольга Пауль: Иногда музыки ну та-а-ак не хватает, что в каком хочешь виде подавай. А вообще, MP3 — удобная штука!

Ace of Magic: Я о ней не думаю, я ей пользуюсь. А что делать? CD-плееры очень громоздки и неудобны, а стоят практически столько же, сколько и MP3-плееры. К тому же CD-плееры имеют свойство ломаться по истечении срока гарантии.

Фауст: Вообще мне как-то не особо нравится ставить чьи-то песни себе на мобильник, особенно, если они не полифонические — звучит как-то убого и некрасиво. По-моему, «мобильная музыка» должна существовать только для обогащения самих музыкантов, а с эстетической точки зрения это полное фуфло.

Евгений Петрович: Я отношусь к людям, которым телефон нужен только для звонков и SMS, а как он звонит — для меня не столь важно. Главное — чтобы было слышно. Внедрение MP3-плеера в телефоне лишним ни для кого не будет, а вот MP3 в качестве звонка — это на любителя.

— Что вы думаете по поводу затянувшегося на годы скандала вокруг этого формата? Вот если бы вы обнаружили в Интернете пиратскую копию вашей песни в формате MP3, что бы вы сделали?

Ольга Пауль: Наверное, мы бы «авторов» этого дела убили! Хотя, честно говоря, у нас на сайте размещена музыка как раз в формате MP3.

Ace of Magic: По-моему, скандал вокруг MP3 выеденного яйца не стоит. Музыкантов он вообще не касается — им достается лишь небольшой процент с их авторских прав. А вот звукозаписывающие компании пусть сами разбираются, кто к чему. Ну, а если бы в Интернете появились MP3-шки с нашей музыкой, я бы только порадовался.

Фауст: Скандал этот, конечно, обоснован с точки зрения финансовой, и тут я полностью на стороне правообладателей. Но если бы наши песни появились в этом формате в Интернете, то я бы обрадовался! Ведь если нас начнут «пиратить», значит, мы набираем популярность. В общем, пока группа набирает популярность, появление ее музыки в этом формате я приветствую, но потом, когда появляется прямая зависимость благосостояния музыканта от продаж его дисков, тут уже не до жалости к малоимущим...

Евгений Петрович: Я за этот формат обеими руками. В нашей стране рынок буквально наводнен пиратской продукцией, и основной доход музыкантов — живые выступления, так что появление в Интернете нашей песни в MP3 — хороший способ стать еще более известными.

— А сами пользуетесь MP3 на своих домашних компьютерах? Если да, то каково их происхождение?

Ольга Пауль: Еще как пользуемся! Качество, естественно, не то что у дисков, но зато количество! Прямо обратный принцип диалектики Гегеля получился... А пользуемся пиратскими записями, ибо они дешевле.

Ace of Magic: Все мои MP3-шки я либо купил, либо скачал, либо сграбил с CD сам, когда надо было перевести в формат MP3 песни какого-то редкого коллектива.

Фауст: Естественно, я, как большинство жителей нашей необъятной Родины, слушаю музыку в MP3, в основном покупаю диски со всеми альбомами той или иной группы. Но те песни и мелодии, которые мне запоминаются или нравятся, я стараюсь при-

обрести в хорошем качестве, то есть на компакт-дисках.

Евгений Петрович: 90% моей музыкальной коллекции хранится в MP3. Источники — самые разнообразные. Большинство, конечно же, с пиратских MP3-дисков, кое-что из Интернета, да и друзья выручали не раз...

— Кроме прослушивания музыки, как вы еще используете свои компьютеры? Какова их конфигурация?

Ольга Пауль: Люблю облагораживать фотографии в редакторах. Это, черт возьми, увлекательно!

Ace of Magic: Я ползаю по Интернету, общаюсь со своими зарубежными друзьями, редактирую наши фотки, делаю афиши и флаеры на наши концерты. Для этого мне вполне хватает P2 433 Mhz с Radeon 7000.

Фауст: Мне нравится 3D-графика, поэтому использую 3D Studio Max, Light Wave и разные другие редакторы. После покупки цифрового фотоаппарата сижу в графических программах, таких как PhotoShop, PaintShop, Corel Draw и так далее. А конфигурация простенькая — четвертый «пень» с 1500 мегагерцами на борту, 256 ОЗУ и 64 видео, второй GeForce.

Евгений Петрович: В последнее время преимущественно пользуюсь Интернетом, ICQ. Еще компьютер использую как гитарный процессор, DVD-плеер, MP3-плеер. По молодости записывал музыку, играл в игры. Конфигурация — Celeron 2 Ghz, 128 RAM, видео — Geforce 2 MX 400 64 Mb.

— А Интернетом вы пользуетесь? Для каких целей?

Ольга Пауль: Теперь уже едва ли могу без Интернета. Ни для кого не секрет, что это безумно удобно! Прежде всего — искать интересующую тебя информацию.

Фауст: Пользуюсь в основном для электронной почты, но и в чатах люблю посидеть. Иногда что-то качаю из Сети, хотя сейчас найти что-то нужное в Интернете становится все сложнее — он превращается в большую информационную помойку.

Евгений Петрович: А мне Интернет в основном нужен для общения или поиска нужной информации, а также как почтовый ящик.

— В Интернете есть ваш сайт http://www.lovecraft.hut1.ru/. Расскажите, как он создавался. В частности, почему он первоначально создан на английском языке и будет ли реализован на русском?

Ольга Пауль: О... Сайт — это нервотрепка была еще та. Делали его Ace of Magic и Фауст. Сначала версия Фауста повлекла с моей стороны негодования по поводу дизайна. Изменили шрифт, цвета, лого по ходу дела даже придумали — иероглиф напоминает. А что касается языка... по той же причине, по которой Моцарт писал оперы на итальянском, будучи австрийцем, — особенность стиля. У нас ведь и тексты песен англоязычные...

Фауст: О том, как создавался сайт, можно написать книгу! С русской версией пока полнейшие непонятки — у нас в группе на эту тему мнения разошлись. А изначально он на английском потому, что красивый шрифт, который мы используем на сайте, не поддерживает русскую раскладку. Писать же обычным Times New Roman — неэстетично. Придется, видимо, новый дизайн придумывать...

— Насколько важным вы считаете свое присутствие в Интернете? Что оно вам дает?

Ольга Пауль: Общение. Мы знакомимся с людьми, люди — с нами... Сейчас ведь очень много народу сидит перед мониторами, гипнотизируют экран, а он их.

Ace of Magic: Присутствие в Сети — это важная часть такой штуки, которая называется модным словом «промоушн». С помощью Интернета мы хотим познакомить как можно больше людей с нашей музыкой.

Фауст: Помню, один человек сказал мне такую фразу: «Нахрена вам сайт? Сайты делают те, кому больше нечего добиваться, когда есть признание, много дисков и денег. Вот тогда от скуки можно и сайт сделать!» Я с этим категорически не согласен. Когда есть сайт —о группе гораздо быстрее узнают. Это такая же реклама, как по телевизору и радио.

Евгений Петрович: Конечно, в Интернете можно найти творческих единомышленников, обмениваться опытом, найти музыкантов... Хотя все это фигня. Самое главное — с помощью форума можно душевно пообщаться с поклонницами!

— Как вы думаете, что нужно знать музыканту о компьютере и Интернете и нужно ли?

Ольга Пауль: Компьютер нужен и музыканту, и немузыканту. Ведь сейчас век коммуникаций! Но не стоит, конечно, полностью отдаляться от живого общения.

Фауст: Музыкантам, конечно, нужно уметь общаться с компьютером. Например, поработать над обложкой в каком-нибудь редакторе, набрать мелодию, послушать, как она звучит... А Интернет — это уже по желанию. Хотя очень многие музыкальные проекты собираются именно через Интернет...

— А был ли в вашей музыкальной жизни интересный случай, связанный с компьютером?

Ольга Пауль (мрачно): Дааа... Был один случай. Тогда мы записывались у нашего бывшего басиста дома (он звукорежиссер). Старались, старались, он ночи бессонные просиживал... А потом у него винчестер сгорел. Мы так и не услышали, что же у нас получилось...

Ace of Magic: А еще один раз ЭтотБлинДос упал как раз перед тем, как нужно было нести афиши в типографию... Пришлось за 2 часа в авральном темпе все создавать заново.

Евгений Петрович: Что-то особое не припомню. Разве что немало винчестеров полегло от моей звукозаписи...

— Что бы вы хотели сказать на прощанье читателям «Магии ПК»?

Евгений Петрович: Думаю, что я выскажу общее пожелание группы. Уважаемые читатели, огромное спасибо тем, кто дочитал это интервью до конца! Желаю вам всем быстрого Интернета, бесперебойного питания, поменьше вирусов, стабильности ПО, удачи и незабываемых впечатлений!

С группой общался

Артем Платонов

Дмитрий Тарабанов (г. Николаев)

Алекс свесил ноги с развороченной кровати, посмотрел вслед натягивающей платье Анне, и как был — босиком — прошлепал к компьютеру. Щелчок по экранной иконке «Летучей мыши», — и с шумом хлопающих крыльев в комнате появился Бэтмен. Тот самый. В черном плаще из латекса и украшенной островерхими эхолотами маске. Разумеется, это был не человек, а все та же популярная почтовая программа. Бэтмен улыбнулся:

— Вы Алекс Андр?

— Я, — кивнул Алекс. На более остроумный ответ с утра не хватало задора.

— Он, — кивнула Анна. Остренький подбородок, улыбка неисправимой проказницы и такие же шкодливые глаза.

— Получите почту... Но прежде прочтите мне число с таблички. Новая степень защиты, знаете ли, во избежание перехвата посылок хакерами. Алекс присмотрелся к табличке, которую держал в руке Бэтмен. Она представляла собой мешанину из острых углов, трещин, следов губной помады и автомобильных шин, отпечатков ног и пальцев, пятен, «тучек» цветного аэрозоля и прочей декоративной мишуры, из которой адресату следовало вычленить четыре арабские цифры.

— 4557, — подсказала Анна, — я уже вижу.

— Погоди ты. — Алекс выискал пока только вторую цифру. О существовании двух последних он еще даже не догадывался. — Я сам:

— Не тормози! 4557!

Слово «тормози» его уязвило.

— 4557! — словно отмахнулся он, уже на семерке поняв, что ошибся и зря доверился подведенным карандашом глазам Анны.

LAPSUS IN FABULA — ошибка в басне (лат.) Вариация на тему известного выражения «Lupus in Fabula» (букв. «как волк в басне», эквивалент: «легок на помине»).

Кибербрат

В небольшом павильоне с DVD-дисками было душно и тесно. Олег еле пробился к прилавку и стал требовать новинок.

— У нас два новых сборника — на одном все части «Кошмаров на улице Вязов», а на другом — вся «Матрица». Лучше берите второй, качество лучше, — посоветовал сердобольный продавец.

— Действительно, возьму лучше «Матрицу», — решил Олег.

На выходе его задержал парень немного странной наружности:

— Давай выйдем из этой духоты, у меня к тебе дело.

— Хорошо, но если хочешь денег, то все равно ничего не получишь. Я быстро бегаю, а в экстренных ситуациях больно пинаю ногами, — предупредил Олег.

На улице незнакомец представился:

— Николай, можно просто Нео. Я киберчеловек и готов сделать из тебя тоже не просто человека, а с приставкой «кибер». Согласен?

— А, все понятно! Ты, наверное, из какой-то новой секты, где поклоняются героям «Матрицы». Дорогой, если ты видишь в моих руках этот DVD-бокс, то это еще не значит, что я молюсь на Тринити.

— Не веришь?

— Ничуть!

— Хочешь, сейчас я убью вон того верзилу, даже не прикоснувшись рукой к его телу?

— Ну, если иметь в руках пистолет или базуку...

— Зачем? В киберпространстве все проще. Я просто отключу его от...

— Матрицы? Нет, ты точно больной! — засмеялся Олег. — Ты хотя бы сделай его хрюкающим кабанчиком.

Николай подошел к долговязому и спокойно сказал:

— Парень, надеюсь, ты живешь в другом микрорайоне. А то все твои знакомые до конца жизни будут вспоминать тот солнечный денек, когда здоровенная детина встала на четвереньки и захрюкала.

— Чего? Ты, пацан, по ходу понятия попутал...

Но тут верзила вдруг ойкнул, хрюкнул и встал на четвереньки.

— Среди бела дня, зараза, наклюкался! — возмущались прохожие.

— Как ты это сделал? Это сговор? Он тоже из твоей компашки? — запричитал Олег.

— Фома неверующий! Хорошо, надеюсь, хоть это заставит тебя поверить мне, — Николай очертил окружность вокруг себя и Олега, и они оба очутились в каком-то лесу.

— Неверно, — отреагировала программа. — Попробуйте еще раз!

И показала новый код.

Скрипя зубами и не реагируя на отпускаемые Анной замечания, Алекс со всей тщательностью отыскал злополучные цифры. На этот раз Бэтмен беспрекословно выдал программисту несколько файлов.

— Анечка, программистки из тебя не выйдет, — резюмировал Алекс. — Кесарю — кесарево, а Анне — анютины глазки...

— Почему это?

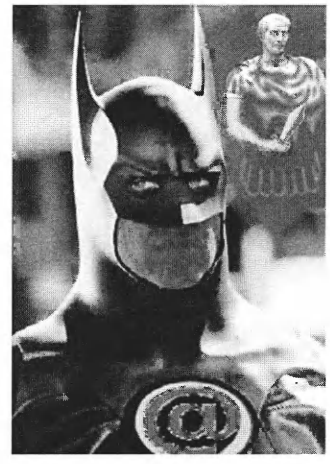
— Потому что в мире, где все могут программировать, осторожностью владеют жалкие единицы. А это — главное...

— Что нам, нулям, рядом с вами, палочками! — фыркнула она и удалилась, жеманно покачивая бедрами.

— Хорошее начало позитивного утра, — сказал Алекс, едва за ней захлопнулась входная дверь.

Алекс откинулся на спинку кресла и раскрыл посылку.

В приложении оказалось десять видеофотографий — восьмисекундных роликов, которые уже повсеместно вытеснили статичные фотографии. Все — от их общего с Анной друга Макса, тоже программиста. С фотографий он похвалялся своими новыми сборками. Вот он с точной копией Дэвида Бэкхема — оба зачесали на голове хохолки и набивают на ногах мячи. На втором снимке — Макс в обнимку с румяной блондинкой Сильвией Саинт. Непонятно, зачем ему вздумалось собирать порнозвезду, когда ее копий наделали по всему миру. Вот он в компании лондонцев-музыкантов из нью-вэйв группы «Man Sun», поверчивает между пальцами барабанную палочку, другой рукой поднимая вверх кружку пенящегося пива. Дальше Макс с Пенелопой Круз. Макс со Стивеном Кингом. С Рихардом Вагнером за клавесином, с Сергеем Лукьяненко...



Алекс вдруг остолбенел. Нет, не улыбающееся лицо классика фантастики напугало его до дрожи в коленках: Осторожно, одним щелчком мыши, Андр закрыл последнюю, страшную фотку. В желудке похолодело, словно он выпил стаканчик фреона из компрессора старенького холодильника. На фотке был Кесарь.

Кесарь! В кроваво-алой римской тоге, золотом панцире на груди, с выставленной вперед ногой и занесенным для последнего удара мечом. Орудием, настигшим не один миллион программистов, посмевших ошибиться.

Что за злая шутка? — подумал Алекс. — Что за намеки?..

Короткий текст письма «Как твой сборный жираф?» тоже ничего путного не сообщил.

Алекс задумался.

Может, Макс намекал на возможную ошибку в коде жирафа, которого программист скомпилировал для лондонского зоопарка? Это была последняя сборка Алекса...

Нет, еще чего! Даже думать об этом противно! Его жираф безупречен. Ошибки в коде нет.

Все в порядке. Алекс спокойно подошел к клетке сборщика, на ходу чистя и кусая банан. Волк, всю ночь мирно спавший, при виде разработчика поднялся на лапы. Точнее, на лапки, так как был он пятнадцати сантиметров от головы до хвоста, и из-за миниатюрных

— Видишь ли, на самом деле мы живем в единой киберсистеме. Конечно, братья Вачовски немного перегнули палку, но кое-что правдивое в их картине есть. Каждое живое существо на этой планете представляет собой набор файлов, объединенных в одну папку. Внутри — куча подкаталогов: внешний вид, интеллектуальные, физические способности, заболевания, история жизни и прочее. Кстати, есть даже файл, где указана дата прогнозируемой смерти. Генетика, ничего не попишешь.

— И сколько тому Хрюше предначертано?

— У них по мужской линии никто до пенсии не доживал, так что ему еще лет двадцать с хвостиком остается. Правда, проведет он их в дурдоме.

— Скажи, а ты действительно смог бы убить его, не моргнув глазом?

— Это вам кажется, что тяжело, а на деле — просто клавиша Delete. Знаешь такую?

— Еще бы! С самого, можно сказать, детства. Однажды удалил какой-то файл в корневом каталоге. Он мне показался ненужным и даже вредным — игра не запустилась. А он еще, зараза, не хотел удаляться, под защитой был. Ну, я превратил системный файл в обычный, а потом и того... клавиша Delete, как ты говоришь. Ох, и влетело тогда от отца...

— Я возлагаю на тебя большие надежды, — вставил Нео, но Олег не дал ему договорить:

— Слушай, а как там у вас кибермолодежь развлекается? Как и простые смертные — пьют горячительные напитки, пристают к девушкам, а наутро страдают от похмельного синдрома?

— Нет. Но кое-какие развлечения все-таки есть — периодически устраиваются состязания. Выглядит это как пейнтбол.

— Ты любишь командные шутеры?

— Нет, я больше по стратегиям. Так вот, киберпарни перемещаются в какой-нибудь глухой лес, создают там постройки, делятся на две команды, оговаривают оружие и... радуются жизни. Если, конечно, тебе доставляет радость осознание того, что тебя могут в любой момент убить.

— Убить? Вы же практически боги, и не бессмертны?

— Это сейчас тебе кажется, что мы все можем, а на деле все зависит от кибернавыка. Вот я, например, могу убить человека, просто удалив его корневой каталог. Но обычно кибер-убийца, решив убрать с дороги смертного, делает это весьма тщательно: прописывает в нужном файле строчку об инфаркте, а потом ждет результата. Пойдем, за два дня ты должен намного поднять свой навык, иначе тебе не быть нашим братом.

— А зачем?

— Ты хочешь остаться, чтобы лакать водку, развлекаться с девушками и сорить деньгами? Если волнуешься за родителей, то мы создадим

размеров обладал повадками мелкого грызуна. Обыкновенный человек подумал бы, что это баг, но так выглядели все программы до официальной компиляции. Вскинув продолговатую мордочку и обнажив острые иглы-зубы, волчонок протяжно завыл. Хорошая акустика выдала пустоту в желудке.

— На, возьми. — Программист просунул через прутья решетки огрызок банана. Волк тут же цапнул тропический фрукт и принялся жевать. Алекс на секунду залюбовался животиной, не пытаясь, однако, почесать программку между ушей. Зачем рисковать, когда программа поедает настоящий банан?

Пройдет не меньше месяца, прежде чем Алекс протестирует грызуна, научит его слышать голос предков и исключит «недопустимые операции». Потом...

Позвонили в дверь.

— Кто там? — негодующе спросил Алекс, направляясь в прихожую.

— Бэтмен, принес посылку!

Алекс дернул дверь за ручку и уставился на гостя. Никакой это был не Бэтмен. Ни латекса, ни эхолот-маски. В кроваво-алой римской тоге, с выставленной вперед ногой и мечом в руке в дверях стоял...

— Алекс Андр! Ваша программа «Лондонский жираф» совершила недопустимую операцию, и ее разработчик будет убит.

Кесарь. Еще до того, как карающая программа дочитала не подлежащий обжалованию приговор, босые ноги занесли побелевшего от страха Алекса в дальнюю комнату. Трехногим табуретом он разбил окно и выпрыгнул на улицу.

Люди под стеной дома завизжали под градом осколков стекла. А Алекс, взвыв от острой боли в ступнях, резво побежал, оставляя на тротуаре кровавые разделительные полосы.

По толпе снова прокатился рев — это Кесарь выпрыгнул на улицу. Алекс споткнулся и, пролетев честные три метра (зачет по физкультуре), распластался на шершавом асфальте. Попытался подняться, снова упал. И долго ждал, пока Кесарь подойдет и тяжелым острым мечом отсечет ему голову.

Но Кесарь не приходил. И голову не отсекал. Алекс искоса, судорожно извернувшись, поглядел назад. Фигура Кесаря замерла в мутной луже. Бред! Кесарь не может зависнуть. Это неоспоримый факт!

Выходит, в луже стоял не Кесарь. В луже стояла чья-то злая шутка. Только чья?

Алекс вынул мобильник и позвонил Максу домой. К его удивлению, трубку сняла Анна.

— Привет! — сказала она, едва сдерживая смех. — Как тебе наш безобидный..?

— Анна! Срочно скажи Максу, что ему угрожает опасность! Его Кесарь выполнил недопустимую операцию и сейчас за ним придет настоящий Кесарь! Анна захохотала, а когда смогла остановиться, сказала только:

— Алекс! Вчерашняя хохма уже не хохма. Я позову Макса... — раздался звонок. — Погоди, кто-то пришел... Он сейчас дверь откроет и подойдет.

— Нет, не открывайте, это Кесарь! — закричал Алекс.

— Я же сказала, не смешно!

В следующую минуту из трубки послышались знакомый фригидный голос, крики, грохот стульев... И тишина.

Алекс прислонил трубку к груди, словно вещь близкого безвременно ушедшего человека... И вдруг засомневался.

А выполнил ли Кесарь недопустимую операцию? Может, операция была допустима, и Кесаря запрограммировали остановиться в луже?! Что, если это не баг, а мастерски спланированный прикол? Значит, шутка продолжается?

твоего клона, а ты пойдешь с нами. Разумеется, клон будет твоей точной копией, с той лишь разницей, что в его памяти будет отсутствовать этот разговор.

— А если мне не понравится, я смогу вернуться в семью?

— Конечно, только это вряд ли случится.

— И все-таки, зачем я вам нужен?

— Какой ты, однако, любопытный! Я ведь тебе уже рассказывал, что иногда мы играем в войнушки. До первого трупа. Дело в том, что система ведет строгий учет: киберлюдей должно быть ровно столько, сколько есть, не больше и не меньше. Сегодня погиб мой напарник. А как только погибает киберчеловек, система, чтобы восстановить равновесие, тут же дарует уникальные способности простому смертному, обладающему максимальным кибернавыком. Так вот, этим смертным оказался ты.

— А что, нельзя просто отредактировать этот параметр?

— Это значение только для чтения, его нельзя исправить.

— Да, а как же мой клон?

— Он уже там, где надо. А теперь нам надо вернуться к магазину. Нехорошо, когда по твоей вине нормальный человек тронулся умом. Сделаю, как в Word, «Отменить», когда ненароком удалил не тот абзац текста.

— Да пошел он, — неожиданно сказал Олег.

— Что ты сказал?

— Да так. Ведь я тоже скоро стану всесильным, молодым богом, так стоит ли нам обращать внимание на простых смертных? К тому же ты сам сказал, что ему не очень много жить осталось.

— Кажется, я в тебе ошибся. Ты не прошел тест «Эйч».

— Какой еще тест?

— «Эйч» — это гуманность. Чтобы стать полубогом, нужно быть человеком. Если честно, ты уже третий за сегодняшний день, кого я пытаюсь сделать своим братом по киберпространству. И третий, кто, узнав о нашей огромной силе, тут же шалеет и проявляет свою гнилую сущность. Прощай, — сказал Нео и исчез.

В ту же секунду он оказался возле магазина, где в луже лежал долговязый. Его обступили зеваки.

— Разойдитесь, это мой брат! Да, сегодня он не в духе, его бросила любимая девушка, но вот сейчас он хрюкнет напоследок и встанет.

Верзила покорно встал на ноги и обвел толпу угрожающим взглядом. Зеваки мигом исчезли.

— Скажи, ты смотрел «Матрицу»? — начал Николай.

— Ну.

— Я киберчеловек и готов сделать из тебя тоже не просто человека, а с приставкой «кибер».

— Чаво? Это я пидер? Ты на кого хлебало раззявил...

Виктор Лысов (г. Волгодонск)

Homo-news

Сделать хотел грозу, а получил козу...

Эксперты SophosLabs предупредили о появлении серии троянских программ, рассылаемых в виде спам-писем по миллионам адресов во всем мире (главным образом, в США и Англии, а также в Германии, Италии, Австралии, Канаде, странах Юго-Восточной Азии и Южной Африки). На долю этих троянов пришлось 25% сообщений о злонамеренных кодах, полученных Sophos за последние 24 часа. Однако из-за ошибки в коде они не причинили вреда ПК получателей.

Спам-письма не имеют темы и, как правило, содержат текст «new price», а также вложенный файл, который может иметь разные имена, такие как 09_price.zip, price_new.zip и price2.zip.

Все вложенные ZIP-файлы содержат файлы с расширением .CPL. Будучи запущенными, эти CPL-файлы сбрасывают на жесткий диск компьютера другой файл и запускают его на выполнение.

Эксперты SophosLabs внимательно изучили варианты этих троянов (известные под именами Troj/Dropper-BB, Troj/Dropper-BC, Troj/Dropper-BD и Troj/Dropper-BE) и обнаружили, что из-за элементарной программистской ошибки они не могут причинить вреда пользователям, хотя и создавались со злобными целями.

Балмер поклялся уничтожить Google

Уже второй ведущий специалист переходит из Microsoft Google, что привело Стива Балмера в состояние исступления. В порыве бешенства он (якобы) заявил, что сотрет Google в пыль, если та не прекратит порочную практику переманивания ключевых разработчиков корпорации и примет на работу двух бывших сотрудников Microsoft.

По словам Марка Луковского, Балмер потребовал от него назвать имя компании, куда он уходит и, услышав ненавистное слово «Google», в ярости швырнул стул в доску анонсов в своем кабинете и произнес как заклинание: «I am going to f***ing kill Google!».

Пресс-секретарь Стива Балмера моментально опубликовал опровержение, мол, Луковский сильно преувеличил реакцию руководителя Microsoft, хотя и признал, что Балмер был действительно взбешен.

Руководство Google заявило о том, что Microsoft нарушает законодательство штата Калифорния, вынуждая своих сотрудников «держаться подальше от плохих парней из Google...».

Адвокатская команда Microsoft нанесла контрудар по Google, опубликовав деловую переписку своего бывшего менеджера в Китае (Кай Фу Ли), из которой следует, что последнему предложено возглавить новый проект (в составе нового подразделения Google в Китае) — разработку поисковых технологий в Интернете на основе речевого распознавания.

Особую пикантность ситуации придали данные из той же переписки о размере компенсации, которую Google согласна выплатить Кай Фу Лии за оперативный переход, — 10 млн долларов. Кроме того, Кай Фу Ли перетащил ряд программистов из из китайского отделения Microsoft в отделение Google.

Один из «отцов» Интернета стал сотрудником Google

Уинтон Серф, считающийся одним из «отцов» современного интернета, перешел на работу в компанию Google.

Серф родился в 1943 году, а в семидесятые годы прошлого века стал одним из соавторов протоколов TCP/IP. В течение последних одиннадцати лет Серф работал в компании MCI, где занимался развитием проектов, тесно связанных с Интернетом. Несколько лет назад Серф стал президентом

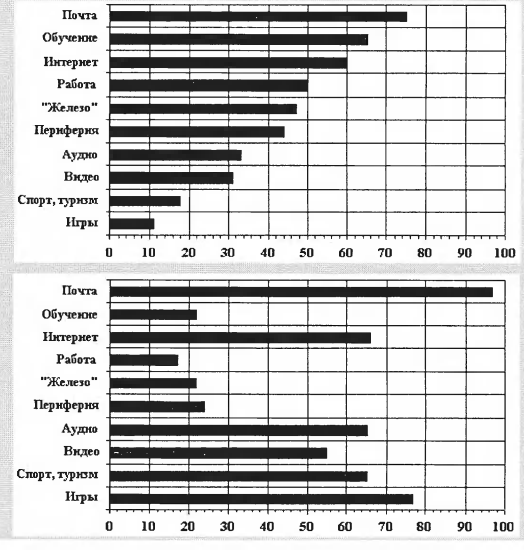
О чем пишут и что читают

Недавно в одной из массовых газет были опубликованы результаты соцопроса среди компьютеризованных петербуржцев. Тема — «зачем вам нужен компьютер». Оказывается, около 75% предпочитают компьютер как средство связи (e-mail), на втором месте — обучение, на третьем —сбор информации (через Интернет). Игры оказались на пятом, чаты — на восьмом.

Мы внимательно изучили последние номера ведущих российских компьютерных журналов. Оказалось, что в среднем они расставляют приоритеты (по числу опубликованных статей) совсем иначе. Да, почтовые программы, антиспамерские фильтры дают очень много публикаций. Об Интернете их меньше, и совсем забыли журналисты такую важную тему, как обучение... Зато много про аудио и видео, спорт и игры, хотя читатели эти темы не очень жалуют (диаграммы представляют картины «о чем читают» и «о чем пишут»).

Между тем, еще в 2000 году продукция наших журналистов удовлетворяла спрос читателей куда лучше. Темы «Железо», «Интернет» и «Обучение» занимали первые три места как среди читательских опросов, так и по объему публикаций...

Николай Богданов-Катьков



ICANN (Internet Corporation for Assigned Names and Numbers) — Международной организации по контролю над распределением доменных имен. Кроме того, Серф является членом исследовательской группы Interplanetary Network, проекта NASA.

В Google Серф займется построением сетевой инфраструктуры и разработкой стандартов для интернет-приложений нового поколения. Вместе с тем он продолжит занимать пост главы ICANN.

Как отнесется Шварценеггер к сценам насилия?

Сенат штата Калифорния на прошлой неделе одобрил законопроект, который предусматривает маркирование коробок с компьютерными играми, содержащими сцены насилия и проявления жестокости, специальным стикером, и запрещает продажу подобных игр несовершеннолетним. Законопроект ожидает окончательного решения губернатора Арнольда Шварценеггера.

Ассоциация продавцов компьютерных игр обратилась к губернатору с просьбой наложить вето на законопроект, мотивируя это тем, что в случае его принятия те же условия должны быть распространены на индустрию музыки и кино.

В прошлом году попытки введения подобного закона (запрещающего продажу лицам, не достигшим 17-летнего возраста, игр, демонстрирующих проявление насилия по отношению к представителям правопорядка; продавцы, нарушившие закон, штрафовались бы на 500 долларов) были квалифицированы как нарушение свободы и провалились главным образом ввиду довольно расплывчатых формулировок критериев, по которым та или иная игра должна быть квалифицирована как «жестокая». К тому же судья отметил, что пока нет фактов, подтверждающих, что виртуальная жестокость может спровоцировать реальное насилие.

Реорганизация в Microsoft

Начался очередной раунд реорганизации Microsoft, совпавший с «мягкой» отставкой Джима Алчина, руководившего группой разработчиков Windows. Корпорация отныне будет представлена тремя стратегическими направлениями разработок, и глава каждого из новых подразделений компании будет подчиняться непосредственно Стиву Балмеру (имя Билла Гейтса в перечне реорганизационных мер не упоминается).

Business Division возглавит Джефф Райкес (Office product Line + Business Solution Package + MSN).

Platform Product и Services Division временно возглавят Кевин Джонсон и Джим Алчин, обязанности будут сведены к нулю (отставка) в момент начала рыночного распространения ОС Vista.

Entertainment and Devices Division возглавит Робби Батч.

По словам Стива Балмера, реорганизация компании преследует цель упрощения схемы принятия решений и установления новой иерархии ответственности за практическое исполнение принятых решений.

Четверо из пяти богатейших американцев работают в ИТ

В списке 400 самых богатых американцев, составленном журналом Forbes, лишь каждый пятый не относится к сфере ИТ.

Список возглавляет сэр Уильям Гейтс, председатель Microsoft, с состоянием 51 млрд долларов (Стив Балмер, исполнительный директор Microsoft, на 11-м месте с 14 миллиардами). Второе место принадлежит медиа-магнату Уоррену Баффетту, исполнительному директору Berkshire Hathaway — 41 миллиард. Он не имеет отношения к ИТ. На третьем — Пол Аллен, сооснователь Microsoft (22,5 млрд). Майкл Делл, глава одноименной компании-производителя компьютеров в США, обладает 18 миллиардами и стоит под номером 4. Ларри Эллисон, глава Oracle — на пятом. Его состояние оценивается в 17 миллиардов.

Вирт на берегах Невы

Не умаляя заслуг Microsoft, отметим, что у людей, серьезно занимающихся программированием, другие кумиры: Бэкус, Кнут, Дейкстра, Страуструп... Среди людей, ставших культовыми фигурами в программировании, и швейцарский математик Никлаус Вирт, создатель языка программирования Pascal.

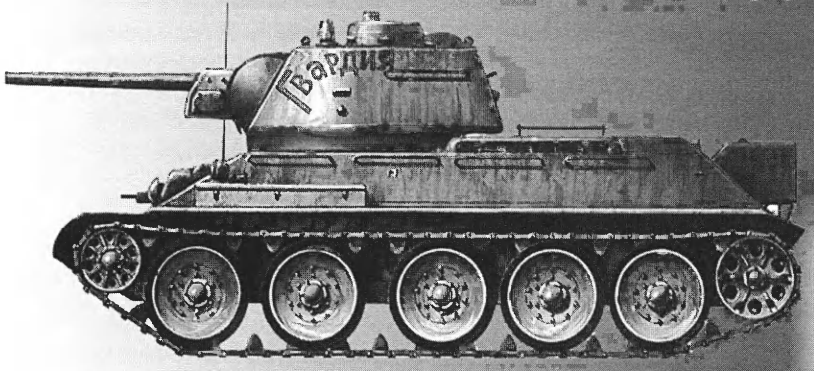
13 сентября профессор Вирт был гостем 239-го лицея Санкт-Петербурга, а затем в ИТМО ему вручили мантию почетного профессора этого университета. Кстати, первый язык программирования, созданный Виртом, назывался «Эйлер», в честь великого математика, тоже из Швейцарии, долгие годы жившего в Петербурге и похороненного в Александро-Невской лавре.

Ученый (хотя и 1934 года рождения) вполне бодр. Он давно уже вернулся из США в родной Цюрих, где возглавлял институт программирования, а в возрасте 65 лет вышел на пенсию и наукой занимается в частном порядке. Круг его интересов в последние годы — вопросы создания процессоров, ориентированных на определенный язык программирования, например, «Оберон-машины» (Оберон — один из языков, созданных ученым в 80-е годы XX века).

То, что Никлаус Вирт был приглашен именно ИТМО, вполне логично: сборная вуза по программированию, многократный победитель всемирных олимпиад, решает задачи пользуясь языком Pascal, а не C. Кроме того, университет наладил прочные контакты с петербургским филиалом фирмы Borland, а эта фирма считает Вирта своим идейным прародителем: она начинала написанием турбо-среды для Pascal, затем разработала Delphi, и руководитель филиала полагает, что будущее именно за этим языком. Именно Borland и организовала визит ученого на берега Невы.

Александр Хайт

ПРОТИВОСТОЯНИЕ & СО



ИСКУССТВО ПОБЕЖДАТЬ

Разговор о бронетехнике в играх данной серии в самом разгаре. Но, прежде чем перейти к описанию танков, давайте закончим с бронетранспортерами.

Итак, главное для БТР — это быстро сократить как можно больше расстояния между собой и врагом и дать команду на выгрузку. Бронетранспортеры можно также использовать как конвои для грузовиков — танки на это дело разбазаривать жалко (почему — объясню позже), а больше ничего подходящего и нет. От слабого налета отобьетесь, а от сильного не помогут и танки. Можно послать БТРы на разведку. Правда, у них не очень большой радиус обзора, зато приличная скорость, и они могут отбиться от небольшой группы противника в одиночку или уйти. Если эти машины необходимо задействовать в общевойсковом бою, то старайтесь их ввести в бой под прикрытием чего-нибудь более массивного. Например, пока танки по полю грохочут, как им и положено по песне, пронеситесь на машинках пару раз вдоль линии фронта. Огонь пулеметов будет как раз кстати, в БТРы вряд ли кто-нибудь попадет из-за их скорости.

Легкие танки

Легкие танки вследствие своей большой скорости и не слишком сильного вооружения во вторую мировую использовали для разведки, а также для непосредственной огневой поддержки пехоты на поле боя. Не будем думать, что мы умнее наших дедов, и поступим точно так же. Для разведки, вообще говоря, танки использовать жалко. А ну как на мину нарвешься — и прощай, родимый экипаж? Трупы возле танка украшают его, только если принадлежат врагу. А самому терять бронеединицу жалко. Так что использовать легкий танк для разведки можно только в том случае, если больше некого послать. Или по другим, столь же весомым причинам. К тому же приближение танка загодя выдаст лязг гусениц, так что... В общем, договорились: танк в разведке — крайний случай.

Гораздо лучше у танка получается выполнять свое прямое предназначение: властвовать на поле боя. Пушка и/или пулемет позволяют без особого труда разбираться с вражеской пехотой и даже с небольшими укреплениями. К примеру, раздербенить дом, в котором сидят снайперы и не дают вашей пехоте головы поднять, или уничтожить пулемет за мешками с песком, который не позволяет продвинуться дальше, — вот именно для этого они и предназначены. Для противостояния средним и, тем более, тяжелым танкам они не подходят — броня слабовата. А помочь пехоте и учинить разборки с бронетранспортерами, легкими танками и пехотой врага — это запросто.

Но не забывайте, что кроме оружия в танке еще имеется совсем неплохой двигатель, позволяющий развивать довольно большую скорость. Используйте это преимущество на всю катушку — постоянно двигайтесь. Лучше параллельно врагу, чтобы не попасть под гранаты пехоты. От такого мельтешения на экране у вашего оппонента за клавиатурой зарябит в глазах, закружится голова и, возможно, случится глубокий обморок.

Благодаря высокой скорости на легкие танки ложится еще одна нелегкая задача — уничтожение артиллерийских батарей противника. Пока на поле боя гремят взрывы и солдаты идут в последний бой, рекомендуется в обход, по краю совершить резкий маневр, подобраться к пушкам вплотную и начать носиться вокруг них кругами. Даже противотанковая артиллерия в этом случае бессильна, потому что вращать пушку быстро невозможно. Ну не может она вращаться вокруг своей оси как вентилятор — все же несколько тонн веса. А вот танковая башня может вращаться на 360 градусов довольно быстро.

Так что, достигнув позиции артиллерии, первым делом заходите к ней в тыл. А там уже дело техники. Если вы настигли гаубицы или минометы, то тут дело еще проще — просто войдите в «мертвую» для них зону, и всего делов. На месте орудийных расчетов я бы сдался. Загодя. Если бы в игре это можно было...

Танками можно также проделывать проходы в заборах, проволочных и иных заграждениях, которые пехота вынуждена огибать. Зачем усложнять себе жизнь — поломали и готово. А с бабушкой, на чьей картошке мы намереваемся воевать, как-нибудь разберемся.

Помните, в начале я говорил, что танки в разведке выдает лязг гусениц? Так вот, то же самое можно применить с пользой для себя, если, конечно, подойти к делу с умом. Ведь противник не видит нас, но слышит. Берем пяток легких танков, обводим их рамочкой и начинаем шуметь вдоль линии фронта, на флангах и вообще везде, куда дотянемся мышкой. Воспаленное воображение вашего противника сразу рисует стройные танковые колонны «Тигров» или «ИСов», которые подбираются со всех сторон... В общем, понервничает изрядно. К тому же он может перекинуть часть сил на отражение мнимого танкового удара, ослабив тем самым свои войска. А вы тем временем можете ударить своими основными силами.

Этот же трюк, с лязгом гусениц, можно применить и для имитации удара — уже не легкими, а средними или даже несколькими тяжелыми танками с грохотом вывалиться из тумана прямо на врага. Тот подумает, что это всего лишь авангард... Что делать дальше, я думаю, говорить не стоит. У вас самих есть голова, чтобы думать.

Если у танка кончились снаряды, а саперов нет и не предвидится, то танк можно использовать в качестве мишени для вражеского огня (в конце концов, у них боекомплект не резиновый) или же для острастки. Был случай, когда я с двумя стреляющими танками и с десятком не стреляющих выиграл бой с полностью вооруженным и снабженным противником, почти равным мне по численности. Главное — это указывать цели вручную, причем использовать концентрацию огня. Это когда оба танка палят по одной мишени — так она быстрее выйдет из строя.

В общем, для легких танков итог таков: поддержка пехоты на поле боя, быстрые рейды с точечными ударами по позициям артиллерии, в крайнем случае — противотанковая борьба, разведка и отвлечение противника.

Средние танки

В среднем танке наиболее выражены все те качества, для коих, собственно, и создавался танк. Это самостоятельное нанесение ударов противнику на всю глубину его боевых порядков. Неплохая скорость и достаточное для самостоятельных рейдов вооружение делают его незаменимым участником штурма. Много об этом классе танков, к сожалению, рассказать нельзя. Применять их лучше всего в качестве штурмовых средств, нанося внезапный удар в неожиданном для противника месте. Достаточная скорость позволит закрепить успех, если он наметился, или уйти от серьезного преследования. Применять их лучше в сочетании с пехотой или бронетранспортерами, чтобы эффект был максимальным. В общем, средние танки — это своеобразные фрегаты на поле боя. Чем больше вы их задействуете одновременно, тем лучше.

Артем Платонов

Исповедь жертвы хирурга

Он опять ковыряется в моих внутренностях. Засунул руки в самое нутро и что-то трогает...

Эй! Что ж ты делаешь?! Вот гад — в мозги полез! Ну никакой жизни не дает!

Ай! Чтоб ему! Похоже, оперативную память наращивает. Дело-то хорошее, но почему без анестезии?! Чего же ему все неймется? Как будто на шиле каком сидит. Нет, чтобы напрячь извилины и хоть как-то обезболить! Фигушки, все лучшее — им. А для нашего брата только одна анестезия — молоток.

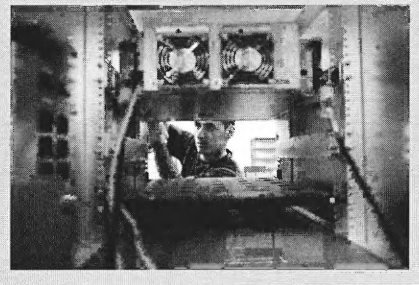
Ох! Хорошо пошло...

Но почему постоянно нужно что-то во мне менять? Вот и в этот раз... Я ведь и так быстро думаю! Вечно всякие мелочи не устраивают! Себе бы чип какой-нибудь в башку вставил — очень бы пригодилось! Так нет же, отыгрывается на тех, кто ответить не может. А мы же почти как дети. Нас хвалить надо и вкусными программками кормить.

И как только ему не надоело мои внутренности теребить? Чуть только что-то успело устареть — сразу безжалостно извлекает и вставляет новое. О донорах боюсь и подумать. Бедненькие. Их настиг наш общий конец — свалка!

А еще хозяину нравится на меня голого смотреть. Бывает, снимет кожух и любуется... Извращенец!

Хотел как-то током тряхнуть, но подумал: «Что ж без него делать буду?» Он — хороший...



Помогаю ему считать. В игры вместе играем. Правда, когда что-то печатает — удавил бы! Шнуром от клавиатуры... Просто садюга какой-то! А скорость, скорость-то какая.

Уф, вроде бы закончил над моим организмом измываться. Мать! Мать не тронь!

Пронесло... Да, действительно чуть было не... Впрочем, неважно. Просто этот косорукий самое святое случайно задел.

Кожух обратно натянул, теперь винты вкручивает. М-м-м... Больно-то как! Нежнее надо! Еще нежнее...

Нормально! Даже как-то комфортнее себя чувствовать стал.

О! Перезагрузка! Замечательно! Может, поиграем сейчас во что-то новенькое. Лично я больше всего стратегии люблю. А этот растяпа последнее время пострелять часок-другой норовит. И чтоб крови побольше. Вот, вот где его подлинная натура открывается.

Может, хотя бы лицо мое протрет. А то в последнее время забывает. Уже все пылью заросло.

Нахал! Опять!!!

Стыдно признаться, но он... Он трогает руками мою... мою мышку. И щекочет, колесико крутит... Просто растлитель какой-то!

Жаль. Похоже, не поиграем в этот раз. Опять работу на дом взял.

Эй! Эй!!! Ты куда мне дискету пихаешь?! А-ах...

Артем Мурадьян (Москва)

Земля 2150: Война миров

Сюжетная линия

Год 2140 от Рождества Христова. Месторасположение: Земля. Действующие лица: Евразийская Династия (судя по всему, куча китайцев, использующих европейские достижения), Цивилизованные Соединенные Штаты (к 2150 году наконец-то цивилизовались) и Лунная Корпорация. Завязка: кто-то спьяну надавил Главную Красную Кнопку, последовал ответный удар, затем ответ на ответный удар... Короче говоря, через 10 лет войны все дружно решили взять таймаут. Выяснилось, что от страшных по силе ударов, обрушенных на одну шестую Земли, орбита ее сдвинулась, и планета стремительно сближается с Солнцем. Причем так стремительно, что у вас в распоряжении осталось всего полгода. Или 183 дня, если быть точным.

Выход очевиден: надо рвать когти. На любую планету, выбирать времени нет. Марс, например, вполне подойдет. Правда, науке и в ту пору было неизвестно, есть ли жизнь на Марсе, — все были заняты стрельбой, перезарядкой оружия и еще раз стрельбой.

Но спасаться все-таки надо. Причем не только правительствам, но и народам. Как выяснилось, за 10 лет войны на эту самую войну ушло больше половины всех ресурсов нашей некогда голубой планеты, а посему построить Ноев Ковчег, который всех увезет, невозможно. Влезает ровно половина оставшегося населения. Угадайте, какое решение приняли воюющие стороны? Правильно. Сократить выбор оставшихся, руководствуясь принципом «Кто первый ударит оппонента шахматной доской по голове, тот и улетит». Короче, противоборствующие стороны начали новый, еще более ожесточенный виток войны. Отличие от остальных в том, что проигравшие выбывали из игры. Навсегда.

Итак, в наличии три совершено независимые друг от друга по технологическому развитию расы. Это означает, что у каждой воюющей стороны свои юниты, своя тактика боя (хотя это в большой степени зависит от вас) и способы их применения. На военной технике остановимся поподробней.

Как не запутаться в паутине

Постулат 1: В Интернете можно найти все.

Постулат 2: Не все так оптимистично в российском Интернете.

Следствие 1: Но что-то найти все-таки можно.

Следствие 2: В конце концов, есть англоязычный Интернет.

Наверное, у каждого, кто в первый раз выходил в мировую Сеть, дух захватывало от обилия самой разнообразной информации. Потом эффект новизны проходит, и это средство поиска уже не кажется нам таким чудесным. Да, там можно найти нужную информацию, но для этого приходится часами перебирать разные страницы, и в какой-то момент осознаешь, что в поисках не всегда важной информации тратится самый наш важный ресурс — время.

Попробую предложить основные методы ЭФФЕКТИВНОГО поиска информации. Их можно условно разделить на:

- Поиск любого из слов. Это когда ищется хотя бы одно из заданных в поисковой строке слов. Наример, если вы не уверены в правильном написании ключевого слова, просто задаете все варианты.
- Все слова. Ищутся все слова в любом порядке.
- Точная фраза. Поиск точной фразы оптимален в тех случаях, когда нужно найти полный текст произведения или уточнить имя автора цитаты, фамилию которого вы забыли.
- И, наконец, самый эффективный способ — логический поиск, о котором и пойдет речь.

Для начала отмечу, что во всех поисковых системах существует набор символов, которые позволяют задавать особые условия поиска.

Большая часть поисковых систем поддерживает такие обозначения.

Фраза или словосочетание берется в кавычки («»), если необходимо найти документ с точно такой же последовательностью слов, например, «Как открыть свой бизнес».

Когда нужно найти любое из слов, используется оператор OR, например, Эксперт OR «Южная столица».

Если в тексте должны встречаться все указанные слова, поставьте между ними AND: «Южная столица» AND «газета деловых людей». Некоторые поисковые системы, например Rambler, используют этот оператор по умолчанию и автоматически ищут все введенные слова.

Если необходимо, чтобы слово в

Начнем, пожалуй, с Евразийской Династии. На вооружении армий этого альянса имеется целая куча бронетехники, от бронетранспортеров до разнообразных танков.

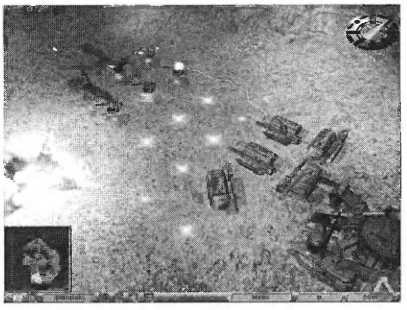
Штатовцы, как и можно было ожидать, за 10 лет наклепали себе целую кучу разных шагающих роботов (привет Mech Commander). Из оружия на роботах преобладают всевозможные энергетические штучки — лазеры и плазмометы. Вся эта шагающая братия является основой войск цивилизовавшихся Штатов.

Лунная Корпорация пошла по другому пути (как известно, если гора не идет к Магомету, то Магомет идет на фиг). Немного посидев на Луне и осознав, что помогать им в разработке оружия никто не собирается, ученые Корпорации научились обращать в оружие антигравитацию, управлять погодой, изобрели звуковое оружие и множество тому подобных прибамбасов. Самая главная особенность Корпорации в том, что управляют ею... женщины. Они же за нее и воюют, и трудятся в цехах. Короче говоря, Корпорация представляет собой показательный пример, до чего может докатиться мир к 2150-му году.

Теперь самое время поведать о том, чем же эта игра отличается от десятков своих собратьев по жанру.

Особенность первая. Начинаете игру вы на базе, однако на карте нет врагов. Что, опешили? Это еще не все. Вы можете производить войска, покуда хватит ресурсов. «А куда же мне их девать?» — спросите вы. Отвечаю. Видите большой вертолет, висящий неподалеку от базы? Правильно, загружаем войска в вертушку, сколько влезет, и вперед на веслах. Куда лететь, спрашиваете? А вы что, пилот? Ах, генерал... Тогда поясню. Лететь можно в любую выбранную вами миссию. Там вам в зубы выдадут задание, которое вы должны будете выполнить. Коль скоро ресурсы на основной базе скоро подойдут к концу, за новые придется драться. Драться нужно будет тем, что произведете на базах. Это означает, что вы можете наклепать войск в миссии, переправить их на главную базу, а оттуда забрать кого надо на следующее задание. По моему мнению — оригинальный, удобный и правильный подход.

Более того, юниты можно создавать самим из предлагаемых шасси и башен! Так сказать, набор «Сделай сам». Число вариаций, конечно, конечно (гм, во загнул), но зато количество вариантов использования созданных вами боевых единиц стремится к бесконечности. Кроме того, если некуда поставить орудийные башни, их можно прилепить на здания (в первую и



вторую мировую так и делали — с подбитого танка снимали башню и ставили в ДОТ). Короче говоря, дерево технологий точно не даст вам скучать.

Одна из главных особенностей игры — это то, что она ведется на время. Кто не успел построить кораблик за 183 дня, тот опоздал и на Марс не поедет. В действие вступает, таким образом, еще и глобальный фактор времени.

Отдельно стоит рассказать о графике и звуке. Графика — выше всяких похвал. Вселенная игры полностью трехмерна и выглядит потрясающе. На высоте выполнены и световые эффекты, такие, как горящие фары у техники ночью, реверсивные следы от ракет и красочно горящие обломки. Тут разработчикам ставим жирный плюс. Звук интерактивен и приятен.

Какой же будем подводить итог, товарищи геймеры? Пожалуй, игрушку стоит взять. Время зря не потеряете.

Артем Платонов

тексте присутствовало обязательно, поставьте перед ним знак (+). Например: +южная +столица. В этом случае поисковик покажет вам все документы, в которых присутствуют оба эти слова, хотя и не обязательно в нужной последовательности.

По аналогии, если поставить перед словом знак минус (—), то будут искаться все документы, в которых отмеченные слова отсутствуют. Например: Билл Клинтон — Моника. В этом случае результат поиска биографии экспрезидента Америки не будет изобиловать пикантными подробностями его любовных отношений. В системе Rambler плюсы и минусы для выделения слов не используются, придется ограничиться другими операторами.

Если вам необходимо искать заданные слова только в заголовках, воспользуйтесь оператором $title(искомое слово). Например, $title(«Южная столица»). Не все поисковые системы поддерживают такой оператор, но в ряде случаев это способно значительно облегчить вам работу.

Если вы хотите найти слово в любой грамматической форме, поставьте в поисковике Rambler перед нужным словом знак # (образец: #столица), а в англоязычном Altavista после искомого слова звездочку (образец: star*). В этом случае выдадут все встречающиеся грамматические формы: star, stars, столица, столицы, столице и т. д.

Очень удобен в Altavista специальный префикс url: он позволяет отбирать только те документы, в адресах которых встречается искомое слово. Пример: url:star

Незаменим для владельцев собственных сайтов префикс link:, дающий перечень всех страниц, на которых есть ссылка на заданную. Например, если у вас есть сайт под названием www.openbusiness.ru, то, введя в поисковике link:www.openbusiness.ru, вы получите полный перечень всех, кто на вас ссылается. По крайней мере, так обстоят дела на Altavista.

Удобным представляется для поиска и оператор NEAR, который по умолчанию ищет все в той же Altavista (и в ряде других систем) все введенные слова, которые в тексте между собой разделяет не более девяти других слов. Пример: government NEAR sensation.

И еще несколько советов, которые помогут вам сэкономить время при поиске в Интернете. Прежде всего существует так называемый «закон Зипфа», который опирается на утверждение, что слова с большим количеством букв встречаются в тексте реже коротких слов. Отсюда полезный для нас вывод — по возможности использовать в качестве ключевых самые длинные из возможных слов, описывающих иско-

Не пугайтесь, речь пойдет о перезаправке картриджей принтеров своими руками. Как заправлять картриджи любых лазерных принтеров и ксероксов без механических повреждений фотобарабана? Ответ на этот вопрос интересует многих, если не всех, обладателей копировальной техники. Ну что же, поделюсь опытом.

Каждый раз, когда заканчивается тонер, перед вами во всей красе встает проблема перезаправки. Путей здесь три: можно воспользоваться услугами фирм, можно аккуратно разобрать и заправить самому, а можно модифицировать картридж, и последующие заправки будут выполняться за 5-7 минут на месте, без пачканья рук.

Итак, для быстрой и качественной заправки тонером картриджей лазерных принтеров и ксероксов картридж необходимо сначала доработать. На это у нас уйдет около 10 минут.

Картриджи многих лазерных принтеров являются одноразовыми по условию эксплуатации, тем не менее они выдерживают от 4 до 20 заправок практически без потери качества печати. В принципе, их можно перезаправлять и дальше, но это уже ведет к снижению качества печати за счет износа фотобарабана. Поэтому, если хотите перезаправлять картридж более 20 раз, то вам необходимо будет заменить также и фотобарабан.

Стандартный способ предполагает разбор (располовинивание) картриджей для изъятия отработанного тонера и засыпки нового. Здесь нас подстерегают засветка фотобарабана прямыми солнечными лучами, а также неудобство вытягивания шплинтов — они изначально утоплены в картридже (HP LJ 1100,HP LJ 5L). Поэтому вооружимся ножом с крепким лезвием или ножницами, скотчем, пылесосом, пластиковой бутылкой с носиком или же бумажной воронкой. Понадобится также гоночный шлем или маска сварщика. И, естественно, нужен сам тонер. Гм, а вы поверили, что гоночный шлем нужен? Шучу, не нужен. Снимайте.

Итак, на плоской стороне картриджа со стороны полости с тонером вращательными движениями прорезается отверстие ножом или ножницами диаметром больше того, которое уже есть. Необходимо следить, чтобы между краями отверстия и окончанием плоской стороны полости оставалось достаточно места для последующего глушения отверстия скотчем. Будьте осторожны и при прорезке отверстия следите за глубиной проникновения режущего инструмента, чтобы не повредить противоположную стенку.

Обрезки пластика, попавшие внутрь, высасываются пылесосом путем переворота картриджа отверстием вниз и поднесением втягивающего конца шланга к отверстию. При последующих заправках необходимости в очистке полости с тонером уже нет.

Затем на плоской стороне картриджа со стороны полости с отработкой ножом или ножницами прорезается отверстие диаметром с толщину большого пальца. Здесь также необходимо следить, чтобы между краями отверстия и окончанием плоской стороны полости с отработкой оставалось достаточно места для последующего глушения отверстия скотчем. Поскольку полость отработки разделена внутренними ребрами, желательно прорезать отверстие в каждой из разделенных полостей. Впрочем, ребра не перекрывают полость отработки полностью, так что если при отсосе отработки постукивать по полости отработки, то можно обойтись и парой отверстий. Для лучшей очистки можно потрясти картридж. После удачного удаления опилок отрежьте кусок скотча и аккуратно прилепите к отверстию. Для хорошего прилегания достаточно 1-2 см скотча от краев отверстия.

Затем тонер засыпается в бутылку с носиком, а при отсутствии таковой сворачивается воронка из бумаги. Носик воронки должен заходить внутрь отверстия не менее чем на 0,5-0,7 мм, иначе можно просыпать тонер. Чем

мую информацию. Незаменимы в этом смысле разнообразные профессиональные термины. Чем больше вы введете специфичных для искомого объекта ключевых слов, тем больше вероятность, что подходящий документ появится уже в начальных ссылках.

Полученные ссылки всегда открывайте в новом окне (для этого щелкните правой кнопкой мыши и выберите соответствующий пункт). Не тратьте время на прокрутку текста: нажмите комбинацию Ctrl+F и введите искомое слово. Браузер автоматически перенесет вас к тому месту в документе, где оно встречается.

И последнее. Если поиск не дал желаемых результатов, не отчаивайтесь, воспользуйтесь другой поисковой системой. Часто одни и те же запросы в разных поисковых системах дают абсолютно разные результаты.

Татьяна Никитина (Ростов-на-Дону)

шире отверстие, тем скорее будет происходить заправка. Тонер засыпается небольшими порциями, для ускорения процесса можно легко постукивать по стенкам воронки. После засыпки очередной партии тонера он разравнивается боковыми движениями картриджа с легким потряхиванием. Не стоит забивать картридж «под завязку», необходимо оставить примерно 1-2 см от края отверстия до поверхности тонера. По окончании заправки отверстие обтирается от просыпавшегося тонера и глушится скотчем.

Для последующей заправки вам нужно всего лишь отклеить скотч, вытянуть отработку пылесосом, заглушить отверстие отработки, отклеить скотч на заправочном отверстии, засыпать тонер, заглушить отверстие. На все про все уходит около 10 минут.

Достоинствами данного метода является быстрота заправки, исключение засветки фотобарабана и механических повреждений, связанных с разборно-сборочными операциями, что, безусловно, удлиняет их срок службы и увеличивает количество перезаправок.

Подобное модифицирование картриджей возможно и для любых других моделей лазерных принтеров и ксероксов.

При желании отверстия можно обработать надфилем и оборудовать пластиковыми пробками, но, поскольку картриджи являются расходными материалами, я отдаю предпочтение скотчу. Под картридж можно подкладывать бумажку с датой и количеством перезаправок, чтобы не сбиться.

Подобным образом мною были модифицированы картриджи от HP LJ 1100, HP LJ 4, HP LJ 4L, HP LJ 5L и ксерокса Canon (2 типа).

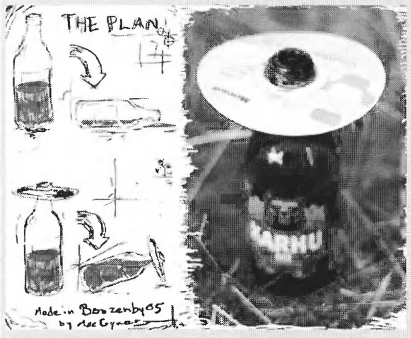
Остается добавить, что перезаправлять можно практически любые картриджи, лишь бы было место для отверстий. Главное —заправлять надо тонером именно того класса, к которому относится сам принтер, иначе возможны неполадки. Например, при заправке картриджей от HP1100 тонером от HP6L у многих принтеров выходит из строя печка, что не случается при использовании «родного» тонера 5P-6P.

Константин Иванищев
(г. Новокузнецк)

Отдыхалки

Непроливашка

Какого только применения не придумывали оптическим дискам — и новогодние елки ими украшали, и как подставки для чашек использовали, и в качестве «отпугивателя» радаров автоинспекции на лобовое стекло автомобиля вешали. Однако теперь, кажется, компакт дискам наконец-то нашли достойное применение. Надев на горлышко пивной бутылки CD- или DVD-диск, можно получить бутылку-непроливашку. Клавиатуру уже не зальете.



Прогресс, однако

Если заранее заказать фотографию рабочего места, распечатанного плоттером на клеенке, то даже ваш начальник не сразу сможет сообразить, что системный администратор спит, а не несет ночную трудовую вахту. Прогресс, одним словом.

Жизнь после смерти

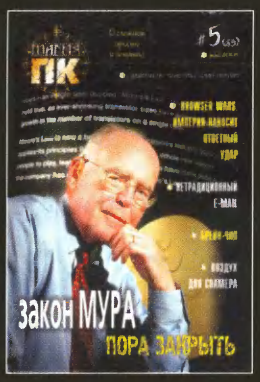
Тем, у кого умер домашний питомец, предлагается «...наиболее инновационный способ превратить лучшего друга человека в преданного слугу даже после его смерти. Достаточно обраться в таксидермический магазин Bob Schuck's Cheese для набивки чучела (www.octanecreative.com/Parodyville/doggybags/index.html)». Боб Шук предлагает вам отправить вашего скончавшегося питомца в контейнере с сухим льдом и через 8 недель получить обратно в виде сумки с ручкой. Однако стоит это удовольствие столько (от $1000 до $4000), что впору подумать над тем, что за такие деньги лучше устроить нормальную жизнь своему питомцу при жизни.

До недавнего времени сервис был ориентирован на жителей США, но теперь и в России стало не протолкнуться от столь же «заманчивых» предложений (http://stoplinks.ru/linkdump.php?mode=show_link&link_id=1046)

Анатолий Ковалевский

Издание зарегистрировано Северо-Западным региональным управлением комитета РФ по печати (С.-Петербург). Регистрационное свидетельство П-2745 от 28.10.97.
Учредитель: ООО "Техно-ПРЕСС". Адрес редакции: 190020, СПб, наб.Обводного канала, 193, тел.(812)33-11-811, 970-29-55. Гл.редактор А. Альбов. Дизайн М. Смирнов.
Подписано в печать 30.09.2005. Тираж 4500 экз. Цена свободная. Отпечатано в типографии "Турусел".

Информационное партнерство — компания «Nikolaev eConsulting», официальный представитель ИА «Интегрум» в СЗФО.



"Магия ПК" – в Сети!

полная версия журнала публикуется для открытого доступа на сайте **www.magicpc.spb.ru.**

МАГИЯ ПК

Оформить подписку на журнал "Магия ПК" с любого номера
вы можете в редакции по адресу: С.-Петербург, Наб. Обводного канала, 193
Оформить подписку на II полугодие 2005 г.
можно в любом почтовом отделении по каталогам "Прессинформ" и "Роспечать".
Подписной индекс журнала **29961.**
Сайт журнала "Магия ПК" находится по адресу:
http:// www.magicpc.spb.ru