

# **Server 2008 в томатном соусе – возьми его с собой прежде чем отправиться в межгалактический полет**

крис касперски aka мышъх, a.k.a. nezumi, no-email

**в то время как Linux в стремлении "догнать и перегнать" перенимает \_худшие\_ черты Windows, Microsoft активно заимствует все лучшее из мира никосов, реализуя их в своих серверных системах. во всяком случае, Server 2008 намного больше похож на UNIX, чем последние дистры Линуха. Microsoft действительно проделала большую работу, которая стоит того, чтобы на нее посмотреть**

## **введение**

Проект Server 2008 (ранее известный под кодовым именем Longhorn) стартовал еще до выпуска Server 2003, но первая бета-версия появилась только в июле 2005 года, вторая и третья беты вышли меньше чем через год — в мае 2006 и в апреле 2007 года соответственно. И вот в сентябре 2007 года Microsoft начала раздавать Server 2008 Release Candidate 0, или, сокращенно, RC0, что переводится как "кандидат в релизы нулевой степени готовности". Финальная версия должна выйти где-то в районе первого квартала 2008 года. Если верить прогнозам Microsoft, это случится 27 февраля.

Но даже в настоящий момент популярность Server 2008 такова, что под ним работает по меньшей мере 2.600 Интернет-серверов (для сравнения: под управлением Windows 2000 работает порядка 5 миллионов серверов). Отчасти такая это объясняется тем, что бета-версии Server 2008 распространяется под лицензией "Go Live", не требуя отчислений, но уже достаточно стабильных для использования в некритических областях, к которым, в частности, относятся Web-сайты мелких компаний.

С учетом свойственной серверному рынку консервативности, потребуется не год и не два, чтобы Server 2008 потеснил Server 2003/Windows 2000, однако, достаточно большое количество хакеров ставит его на рабочие станции уже сейчас, поскольку, видят в нем намного меньше зла, чем в ненавистной Висле. Такого же мнения придерживается и мышъх, распотрошавший ядро Longhorn'a под дизассемблером и до того проникнувшегося к нему уважением, что даже загорелся поставить его на соседнюю машину (основная работает под управлением Windows 2000).



**Рисунок 1 Логотип Server 2008**

## **>>> врезка редакции Server 2008**

Microsoft Windows Server 2008 поставляется в пяти редакциях, перечисленных ниже, поддерживающих как 32-битные, так и 64-битные системы. Подробное описание каждой редакции и их отличий можно найти в рекламных проспектах от Microsoft. Это тот редкий случай, когда они не врут.

- Windows Server "Longhorn" Standard Edition;
- Windows Server "Longhorn" Enterprise Edition;
- Windows Server "Longhorn" Datacenter Edition;
- Windows Server "Longhorn" для Itanium-систем;
- Windows Web Server "Longhorn";

## ***fundamentals***

Server 2008 основан на ядре Вислы (которое в свою очередь основано на коде Server 2003) и потому включает в себя все основные фичи Вислы такие, как переписанный с нуля TCP/IP стек (содержащий неизвестное науке количество новых дыр), улучшенная поддержка динамической памяти, файла подкачки, ввода/вывода, рандомизация адресного пространства и контроль целостности кучи для защиты от переполняющихся буферов и т. д. Мысль уже терзала ядро Вислы и много писал о ней в Хакере (см. статьи "вторжение в ядро вислы — спроси меня как!", "IPv6 – демократия или диктатура? tagline1: неизведанное — рядом, но оно запрещен", "аналитическое сравнение XP и Vista – отличия ядер и ядерных компонентов", "глубины и вершины сетевого стека висты", "взлом patch-guard", "археологические раскопки ядра vista/longhorn", "глубоководное погружение в недра vista/longhorn" и др., полные электронные версии которых можно найти на DVD-диске, прилагаемом к журналу).

Что изменилось в Server 2008? Ну, в общем-то, кое-что изменилось. Microsoft продолжает затягивать гайки, усиливая безопасность и оптимизируя систему под работу с мощным железом, что совсем не идет на пользу SOHO-серверам. Более того, Microsoft открыто признает, что код Longhorn'a совсем не оптимизирован под файловый сервер (а в SOHO-сегменте как раз и доминируют файловые сервера!), так что в практическом плане "оптимизация" превращается в "пессимизацию" и конечные пользователи вынуждены вкладывать деньги в железо для получения той же самой производительности, что и на Server 2003/Windows 2000. Ну и чего это ради?!

Оказывается, не все так просто и очевидно. Несмотря на все недостатки Longhorn'a интерес к нему продолжает расти. К его достоинствам в первую очередь хочется отнести доработку командной строки, позволяющую выполнять 99% операций с удаленной машины (т. е. без физического доступа к серверу), а также улучшенные механизмы мониторинга, диагностики ошибок и восстановления системы после падений. Наконец, Server 2008 поддерживает технологии аппаратной виртуализации Intel/AMD известные под кодовыми именами "Pacific", "Silvervale"/"Vanderpool" и позволяющими запускать гостевые операционные системы практически без потери производительности.

Скоромные рамки журнальной статьи не позволяют подробно рассказать о всех нововведениях, поэтому мы решили остановиться на самых интересных из них.

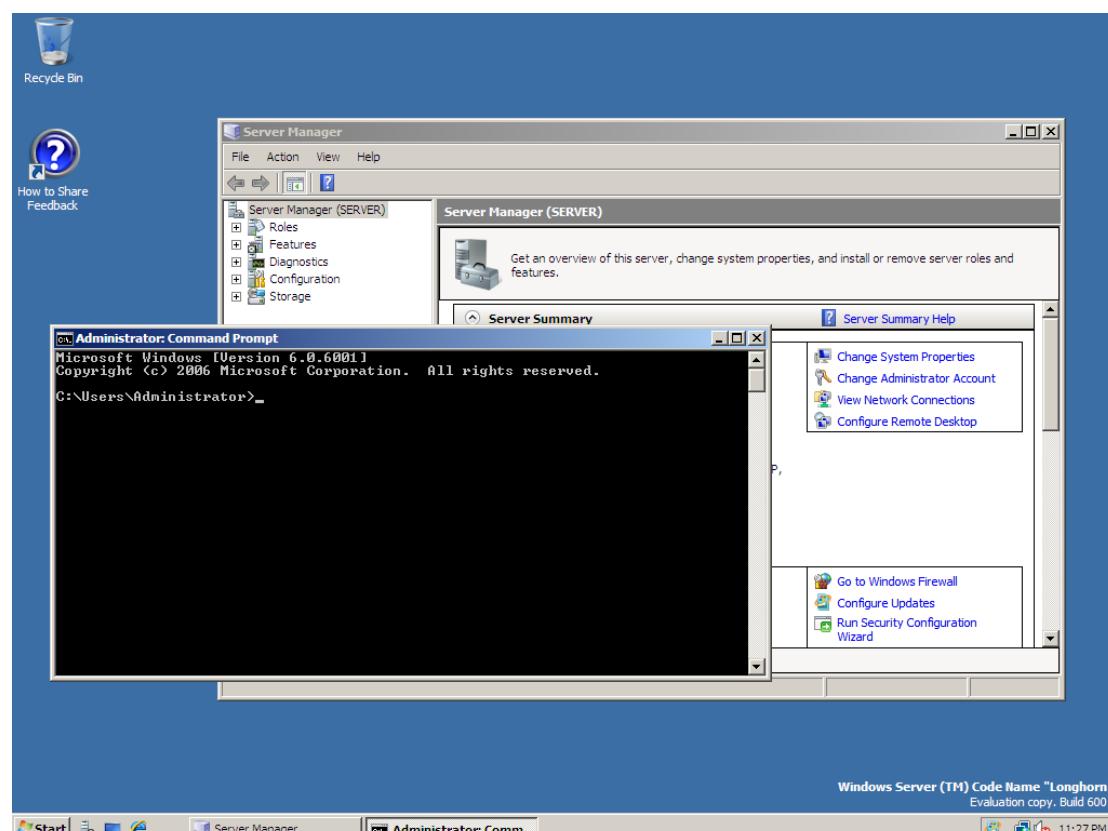


Рисунок 2 так выглядит Server 2008

## **server core**

Linux и xBSD, изначально ориентированные на работу с командной строкой, прочно оккупировали рынок low-end серверов, мощностей которых недостаточно для поддержки графической оболочки, не являющейся частью ядра и устанавливаемой отдельно. По желанию. Или не устанавливаемой. Это уже как захочет администратор. В любом случае, мы получаем полнофункциональный сервер и все необходимые нам программы будут запускаться нормально, даже если мы захотим принять почту, полазить по web'у или отредактировать офисный документ, записанный в формате MS Word. Да-да! Все это можно сделать в текстовом режиме, который на самом деле... графический. Ядро переходит в графический режим еще на самой ранней стадии загрузки, в чем легко убедиться нажав кнопку <info> на мониторе. Спрашиваете — зачем это никсы делают? Ответ — а как еще иначе работать с несколькими кодировками сразу? Да и текстовых режимов (стандартных) немного, и большинство из них выглядят просто ужасно (кто застал MS-DOS — тот помнит). Тем не менее, при желании можно форсировать работу ядра и в текстовом режиме, что ощутимо увеличивает быстродействие на слабых машинах.

Windows — совсем другой зверь. Оконная подсистема интегрирована в ядро и является неотъемлемой частью подсистемы win32-API, которую "отодрать" от ядра очень трудно. Собственно говоря, понятие "ядра" совершенно неприемлемо к Windows, поскольку этих ядер у него... ну, скажем так, намного больше одного и все они переплетены в тугой клубок, работающий по принципу — не трогай, а то развалится. Какой вред от интеграции графической оболочки в ядро? Ну, в общем-то, никакого. Да и ресурсов жрет намного меньше, чем Gnome/KDE (популярные оболочки для UNIX). Недостаток Windows в том, что многие действия можно выполнить только через графическую оболочку, что требует физического доступа к серверу или установки дополнительных программных пакетов для удаленного администрирования, но в ряде случаев не помогают даже они. Печально, да?

В Server 2008 появился режим "server core", позволяющий устанавливать систему без графической оболочки и без библиотеки .NET Framework, управляя сервером через командную строку или удаленно через консоль управления (Microsoft Management Console). При чтении рекламных обзоров создается впечатление, что Microsoft наконец-то отодрала оконную подсистему от ядра, подарив нам "чистый" текстовой режим, которого все от нее так должно ждали.

Увы, это всего лишь реклама. В "server core" действительно отсутствует Windows Explorer, но графическая подсистема никуда не делась и API-функции USER32/GDI32 продолжают работать как ни в чем не бывало, пожирая системные ресурсы. Аналогичного эффекта можно добиться и на Server 2003, выбрав в опциях загрузки режим "command prompt only with networking support". Разница между Server 2008 и Server 2003 в том, что "server core" не ставит Explorer и .NET на винчестер, экономя пару сотен мегабайт дискового пространства. Какое большое достижение!!! Как будто нельзя снести Explorer и вручную, превратив Server 2003 в Server 2003 Core. На самом деле, руками можно сделать гораздо больше, в том числе и отодрать графическую оболочку, поскольку сетевые сервисы начинают работать еще до ее загрузки. Однако, это не превратит Server 2003/Server 2008 в UNIX, поскольку ряд действий осуществляется только в графическом режиме (например, управление оборудованием).

Тем не менее, "server core" — это большой шаг вперед и теперь нам уже не придется сразу же после установки сервера браться за метлу и выметать все ненужное. Впрочем, ненужного в server core по-прежнему много. Это и лишние службы и неиспользуемые системные компоненты и т. д. и т. п.

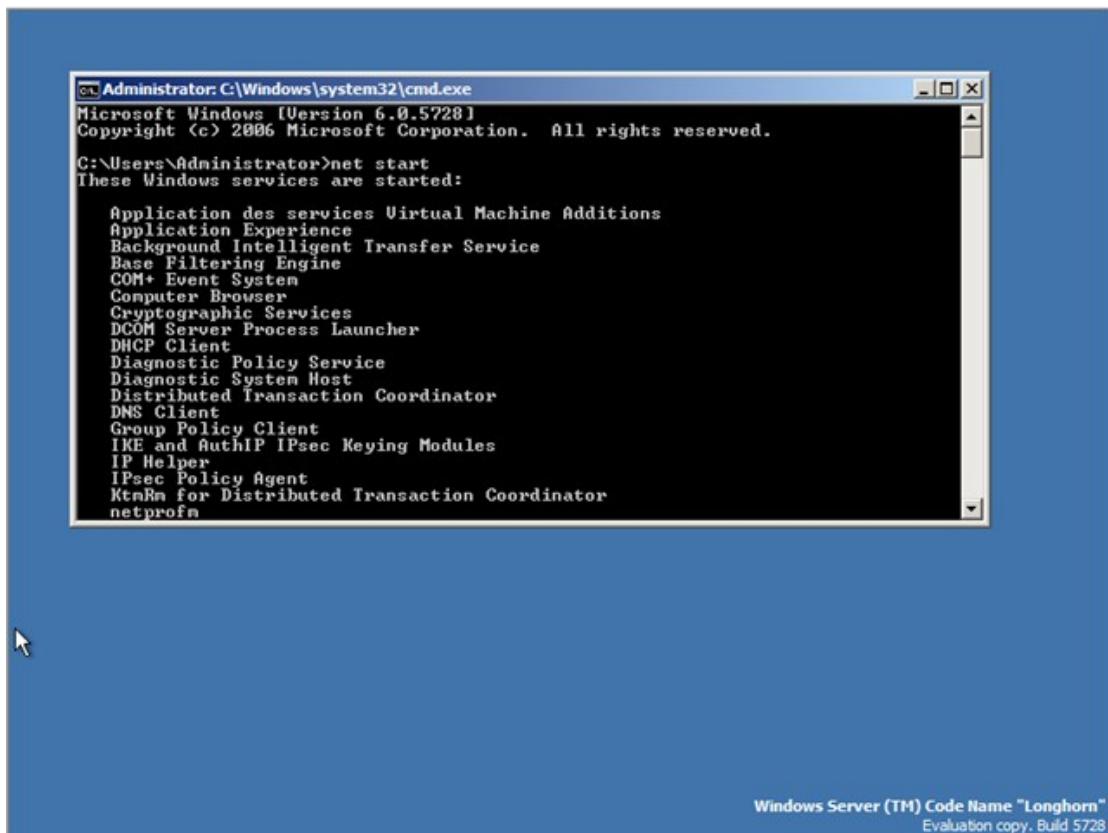


Рисунок 3 так выглядит Server 2008 Core

### >>> врезка как можно использовать Server 2008 Core

- Active Directory Domain Services;
- Active Directory Lightweight Directory Services (AD LDS)
- Dynamic Host Configuration Protocol (DHCP) Сервер;
- DNS-Сервер;
- Файловый Сервер;
- Сервер печати;
- Streaming Media Services;
- Web Server (IIS)

### >>> врезка какие компоненты включает Server 2008 Core

- Microsoft Failover Cluster;
- Network Load Balancing;
- пародию на POSIX подсистему для UNIX-приложений;
- Microsoft Windows Backup;
- Multipath I/O;
- Removable Storage Management;
- Windows Bitlocker Drive Encryption;
- Simple Network Management Protocol (SNMP);
- Windows Internet Naming Service (WINS);
- Telnet-клиент;
- службу Quality of Service (QoS)

### **виртуальные миры виртуальных осей**

Огромная популярность виртуальных машин типа VM Ware наконец-то сподвигла разработчиков процессоров на поддержку аппаратной виртуализации, позволяющей эмулировать выполнение машинных команд практически без потери производительности.

У AMD эта технология называется "Pacific" (Athlon 64/Turion 64/ Opteron), у Intel – "Silvervale" (Itanium)"/"Vanderpool" (Pentium 4) и она реализована практически на всех процессорах, выпущенных после середины 2006 года.

В состав Server 2008 входит встроенный виртуализатор, устанавливаемый опционально и сконструированный на базе эмулятора "Microsoft Virtual PC" (который можно приобрести отдельно за дополнительную плату и установить, например, на W2K), что позволяет запускать несколько операционных систем одновременно! Причем, поддерживаются не только оси от Microsoft, но так же UNIX-клоны: Linux, xBSD и т. д. Естественно, на виртуальных машинах можно запускать и саму Windows, что очень полезно для "вскрытия" червей, обкатки подозрительных программ, полученных из сомнительных источников, или для различных экспериментов в системой, которая в худшем случае может "грехнуть" только виртуальный диск, на котором кроме нее нет ничего ценного.

Провайдеры могут использовать эмулятор для предоставления виртуального хостинга, позволяя клиентам устанавливать свои собственные операционные системы, что доселе было невиданной роскошью и стоило немеряных денег. Аналогичным образом обстоят дела и развертыванием отказоустойчивых систем. Теперь, вместо приобретения резервного сервера, достаточно запустить несколько виртуальных машин. Если упадет одна система, обработку запросов возьмет на себя другая. Естественно, эмулятор страхует только от программных сбоев и потому в критических инфраструктурах без аппаратного дублирования железа по-прежнему не обойтись, однако, критические инфраструктуры занимают сравнительно небольшую часть рынка, да и аппаратные отказы случаются не так уж часто.

Главный минус виртуализатора — необходимость в апгрейде старого железа. Учитывая, что средний срок "амортизации" оборудования колеблется от 3х до 5ти лет, можно сделать вывод, что количество серверов, оснащенных процессорами, выпущенных после середины 2006 года, на данный момент крайне невелико. Реально материнские платы и сервера с поддержкой аппаратной виртуализации появились на отечественном рынке в начале 2007 года и цена на них все еще достаточно велика для их массового внедрения. Народ предпочитает брать слегка устаревшее железо по бросовой цене.

Кстати, о ценах. Microsoft до сих пор не определилась с политикой лицензирования своих систем, запущенных на виртуальных машинах и в настоящий момент необходимо платить за каждую инсталляцию, включая виртуальную. Очевидно, что аппаратная эмуляция позволяет использовать базовую операционную систему как "фундамент" для всех остальных. Но платить за фундамент как за полнофункциональную ось, не используя и 10% ее возможностей — смешно, если не сказать что обидно и грустно. Намного выгоднее возложить эту задачу на FreeBSD или Linux, под которые есть куча бесплатных эмуляторов, поддерживающих аппаратную виртуализацию (например, XEN), и которые позволяют запускать Server 2008 как гостевую операционную систему, в результате чего мы платим всего лишь за одну инсталляцию, а не за две.

### >>> врезка пределы виртуализации

виртуальное устройство	maximum maximore
SCSI контроллеров на каждую виртуальную машину	4
устройств на один SCSI-контроллер	7
макс. размер SCSI-диска (виртуального)	2 ТБ
макс. совокупный размер всех дисков одной виртуальной машины	56 ТБ
макс. кол-во ЦП на каждую виртуальную машину	1
макс. объем виртуальной памяти одной виртуальной машины	3.6 GB
макс. кол-во виртуальных NIC'ов одной виртуальной машины	4
макс. IDE-устройств на каждую виртуальную машину	4
гибких дисков на каждую виртуальную машину	1
параллельных портов на каждую виртуальную машину	1
последовательных портов на каждую виртуальную машину	2
макс. кол-во виртуальных сетей	128

Таблица 1 максимальное количество и объем виртуальных устройств, поддерживаемых эмулятором

аппаратное устройство базового компьютера	maximum maximore
---	------------------

макс. объем физической памяти, доступной для виртуализации	256 GB
макс. кол-во физических NIC'ов	9999
макс. кол-во хостов на кластер	8

**Таблица 2 максимальное количество и объем физических устройств, поддерживаемых эмулятором**

## **Plug-n-Pray**

**/\* РЕДАКТОРУ: это не опечатка! включи-и-молись!!! \*/**

Вот раньше, года этак в 60е, все было классно — sex, drugs & rock'n'roll. А сейчас? Suxx, bugs & plug'n'play... Точнее plug-n-pray. В смысле включи-и-молись. И ведь есть о чем помолиться! Не дай бог еще зависнет все на хрен... Ну ладно, если мы что-то к USB подключаем, а если наращиваем паять или вставляем еще один процессор? А что — при поддержке материнской платой технологии hot-plug еще и не такое возможно. Правда, это должна быть очень крутая плата, обслуживающая критически важный ресурс, не допускающий даже плановой (эх, слово-то какое!) перезагрузки. И стоять на ней скорее всего будет QNX или другая "правильная" операционная система, поставляемая вместе с машиной.

Windows (вплоть до Вислы) определяла количество процессоров и объем оперативной памяти на ранних стадиях загрузки своего ядра и не допускала никакой возможности изменения конфигурации в дальнейшем. Более того, переход с одноЦПшной на многоЦПшную машину требовал не только перезагрузки, но еще и переустановки системы. Теперь же, и процессор, и память включены в общее дерево Plug-n-Pray устройств, а это, значит, что они могут подключаться/отключаться на лету без перезагрузки. Теоретически. Практически же реализовано только распознавание новых устройств, но ядро Server 2008 ни морально, ни физически не готово к исчезновению одного или нескольких процессоров или планок оперативной памяти. То есть замений память/процессор на лету мы все равно не сможем. А наращивать их количество... чисто слот на матери не бесконечно, да и к тому же для достижения максимальной производительности следует устанавливать память/процессор с идентичными характеристиками, а если они отличаются от уже установленных, останов системы все равно неизбежен, хоть бейся зубами об лед, хоть убейся об газель.

К тому же, как уже говорилось, в критических инфраструктурах Windows практически не применяется, и с учетом астрономической стоимости железа, поддерживающего горячую замену процессоров и оперативной памяти, намного дешевле купить резервный сервер, чтобы спокойно останавливать основную систему для планового апгрейда. Опять-таки, Server 2008 выполняет распределение ресурсов (сколько памяти отдать под системный кэш, столько-то под все остальное) на ранних этапах загрузки и не меняет его в дальнейшем, даже если мы увеличим количество RAM. Но это еще что! Подумаешь... неэффективное использование памяти! Намного хуже то, что наращивание оперативной памяти приводит к невозможности сохранения полного дампа ядра, которое требует, чтобы файл подкачки был равен объему RAM или превышал последний, а максимальный размер файла подкачки устанавливается при загрузке системы и по умолчанию равен 1,5 \* RAM. Изменение размеров файла подкачки требует обязательной перезагрузки. То есть, если мы увеличим объем памяти более чем на 50%, создание полного дампа ядра станет невозможным! А без полного дампа ядра разобраться почему вспыхнул голубой экран смерти намного труднее, чем с ним. Так что эта технология еще сыра и Microsoft'у тут есть еще над чем поработать.

## **Intel под угрозой вытеснения с рынка!**

Server 2008 – это последний сервер в линейке Windows NT, поддерживающий x86. Дальше пойдут только 64-битные версии (см. блог разработчиков Вислы: [windowsvistablog.com/blogs/windowsvista/archive/2007/05/18/on-64-bit-and-windows-client.aspx](http://windowsvistablog.com/blogs/windowsvista/archive/2007/05/18/on-64-bit-and-windows-client.aspx)).

Microsoft объясняет это своим стремлением сосредоточить все имеющиеся в ее распоряжении ресурсы для работы над одним ядром, чтобы не распылять усилия по ветру. Типа, самая преуспевающая компания мира настолько обнищала, что не может позволить себе такую "роскошь" как поддержку еще одно ядра. А вот xBSD и Linux-системы портированы под сотни различных архитектур. Странно не правда ли? Особенно, если вспомнить, что x86 – даже не одна из самых популярных, а самая популярная платформа на сегодняшний день и дело тут совсем не в том, что у Microsoft денег/сотрудников не хватает или что для реализации

очередной серверной версии позарез требуется как минимум 64-бита (что же это за монстр будет такой?!). Все гораздо проще.

64-битные версии построены с учетом последних веяний DRM, включая такие инквизиторские штуки как обязательную подпись всех драйверов, невозможность модификации ядра и т. д. То есть все то, что позволяет Microsoft'у вытеснять неугодных игроков с рынка, одновременно с этим заигрывая с Голливудом и другими держателями авторских прав на медиаконтент, позиционируя Windows как систему, защищенную от цифрового грабежа. Естественно, при желании можно сграбить и контент и ядро отмодифицировать так, что система ляжет и больше не встанет, но это уже хакерство...

Интересно, что будет делать Intel — ведь рынок SOHO-серверов не просто широк, он огромен как Атлантический Океан, а позиции Itanium'a на нем выглядят довольно слабой и вообще неубедительной. Поэтому, администраторам придется либо переходить на xBSD/Linux, либо AMD x86-64 + очередную поделку от Microsoft. Желающих перейти на UNIX-системы навряд ли окажется слишком много (куда девать накопленный опыт администрирования? за какие шиши перестраивать сложившуюся инфраструктуру?), а раз так, то AMD становится практически единственной альтернативой.

Выпускать "народную" версию Itanium'a Intel не сможет хотя бы потому, что он не совместим с x86, а зачем народу процессор под которым не запускаются никакие программы? Скопировать x86-64 и добавить его в Pentium? Но это значит превратиться из лидера в догоняющего... В общем, над Intel нависла не слишком-то увлекательная перспектива потери значительной части рынка. Но Intel без боя не сдается и будет просто замечательно, если она начнет проталкивать Linux в массы, вкладывая деньги в его рекламу, поддержку, etc.

Но, как говорится, поживем — увидим.