активация висты лапами и хвостом

крис касперски, ака мыщъх, no-email

многие энтузиасты, желающие пересесть на висту, столкнулись с проблемами активации системы, купленной в ближайшем ларьке в полном соответствии с действующим законодательством (sic!). и хотя в сети уже появилась куча "ломиков", большинство из них представляют собой троянские программы, созданные специально для заманивая доверчивых пользователей. между тем, активировать висту не просто, а _очень_ просто, надо только знать как ;)

введение

Лидеры рынка программного обеспечения прекрасно осведомлены о том, что любые защитные механизмы (даже самые невинные и неназойливые) отрицательно сказываются на динамике продаж, поскольку пиратов никакая защита все равно не остановит, а вот у честных пользователей возникают серьезные проблемы, в результате чего они либо уходят к конкурентам, либо обращаются за помощью к хакерам.

Вплоть до появления Windows 2000, компания Microsoft ограничивалась однократной проверкой серийного номера на этапе инсталляции системы, что позволяло пользователям (и пиратам) тиражировать один легально купленный диск в неограниченном количестве экземпляров. Для оценки масштабов пиратства, Microsoft выпустила специальную утилиту, проверяющую подлинность установленной копии Windows, назойливо предлагая пользователям "почекаться" при скачке обновлений. Первое время проверка была необязательна и обновления отдавались и так, но затем Microsoft ужесточила политику, оставив в свободной раздаче лишь критические заплатки, и Service Pack 4 уже отдавался только после проверки подлинности и потому многим пользователям, пользующимися пиратскими версиями, пришлось качать обновления с варезных сайтов.

В XP проверка подлинности стала обязательной и даже легально купленная система требует активации (осуществляемой через интернет или голосовой телефон), в противном случае переходит в режим ограниченной функциональности. К счастью, корпоративная версия (непредназначенная для розничной продажи) работает и без этого "чуда" и проверка подлинности осуществляется лишь при установке обновлений (причем, критические обновления можно по-прежнему скачивать без всяких проверок).

В Висте требуется активировать все версии (в том числе и Enterprise – бывший Corporative Edition), причем при смене железа активацию требуется повторять вновь, причем, Microsoft оставляет за собой право отказать в выдаче нового ключа без объяснения причин. Добавьте сюда еще ложные срабатывания защиты (которые случаются достаточно часто) и ответьте мне на вопрос: вы все еще надеетесь обойтись без хакерских навыков?!

система активации снаружи и изнутри

За проверку подлинности Висты отвечает компонент WGA (Windows Genuine Advantage), ранее реализованный в Microsoft Office, где он назывался Office Genuine Advantage или, сокращенно, OGA.

WGA привязывается к "железу", генерируя специальный серийный номер, отправляемый на сервер проверки подлинности, возвращающий пользователю ключ активации, который необходимо ввести в течении 30 дней с момента установки системы, в противном случае Виста перейдет в так называемый режим ограниченной функциональности (reduced functionality mode или, сокращенно, RFM). В этом режиме нет главного меню, значков рабочего стола, а заставка рабочего стола замещена черным фоном, но хуже всего то, что через час работы система завершает текущий сеанс без всякого предупреждения!

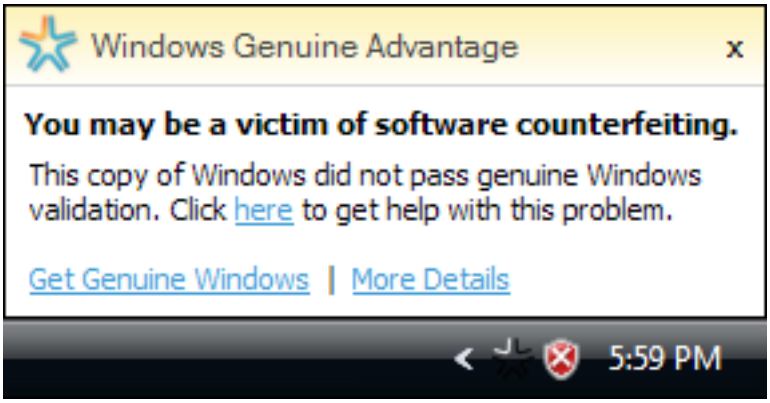

Рисунок 1 предупреждение о необходимости проверки подлинности, выдаваемое компонентом WGA в течении 30-дней, отпущенных для активации

Ключ активации генерируется на основании следующих данных и автоматически аннулируется при их изменении (включая даже такую невинную операцию как обновление прошивки BIOS), требуя повторной активации:

- product key и product ID;
- контрольная сумма BIOS;
- вендор/версия/дата BIOS;
- MAC-адрес сетевой карты;
- версия операционной системы;
- серийный номер жесткого диска;
- языковые профили операционной системы;

Естественно, подобный подход неприемлем для крупных компаний и корпораций, поскольку он ставит их в прямую зависимость от Microsoft и потому последней пришлось пойти на уступки, включив поддержку многопользовательских ключей активации (они же — Multiple Activation Keys или, сокращенно, MAK), впервые реализованных в пакетах MSDN Universal и Microsoft Action Pack.

Рисунок 2 состояния лицензирования Висты и Longhorn Server

Каждый MAK-ключ может активировать определенное количество компьютеров заданное число раз (основанное на типе соглашения между потребителем и компанией

Microsoft). При исчерпании активаций, потребитель может бесплатно возобновить MAK-ключ, позвонив в местный центр обработки активаций (естественно, доказав при этом, что он не хакер, не пират и вообще не лось).

MAK-ключи можно использовать для активации любой многопользовательской версии Висты (не стоит путать MAK-ключи с ключами установки, MAK-ключи — это ключи активации!).

При выполнении MAK-активации клиентский компьютер генерирует идентификатор установки (ID) и передает его серверу активации Microsoft по сети Интернет или "вручную" через голосовой телефон. При успешном завершении операции сервер возвращает MAK-ключ и идентификатор подтверждения (CID).

MAK-ключи хранится в незашифрованных XML-файлах, копируемых на компьютер в процессе автоматической установки в папку %systemroot%\panther, но в конце установки подлинное значение параметра ProductKey удаляется и заменяется строкой SENSITIVE*DATA*DELETED (конфиденциальные данные удалены), чтобы пользователи не могли влиять на этот ключ и не могли получить его после того, как он был установлен на компьютер, поэтому, чтобы получить MAK-ключ, необходимо иметь оригинальный инсталляционный диск, которым можно пользоваться не только на работе, но и дома. В принципе, имея знакомых в IT-сфере, выпросить валидный ключ — не проблема. После чего его останется установить по методике описанной во врезке "активация Висты с помощью MAK-ключа".

Служба управления ключами Key Management Service (или, сокращенно, KMS) позволяет выполнять самостоятельную активацию компьютеров в локальной сети _без_ обращения к серверам компании Microsoft. KMS-службу можно задействовать на любом компьютере под управлением Висты или Server Longhorn, установив KMS-ключ и затем активировав этот компьютер через сервер компании Microsoft. В отличии от MAK-ключей, KMS-ключи устанавливается только на компьютер, управляющий KMS-службой, но никогда — на активируемые им компьютеры!

Версии Висты, предназначенные для розничной продажи, не могут быть активированы через KMS-службу, что, впрочем, не является камнем преткновения, поскольку найти корпоративную версию можно в любом киоске, осле или варезном сервере. Предоставление прав на корпоративную версию Висты предполагает наличие корпоративной лицензии на предыдущую операционную систему. По умолчанию носители с 32-разрядными корпоративными версиями Висты предназначены только для обновления и не являются загрузочными, поэтому, сначала необходимо установить предыдущую версию Windows, а затем поверх нее водрузить Висту (кстати говоря, загрузочные носители также можно получить по запросу через портал корпоративных лицензий). Носители с 64-разрядными версиями не имеют подобных ограничений, однако, пользоваться ими в силу отвратительной обратной совместимости категорически не рекомендуется.

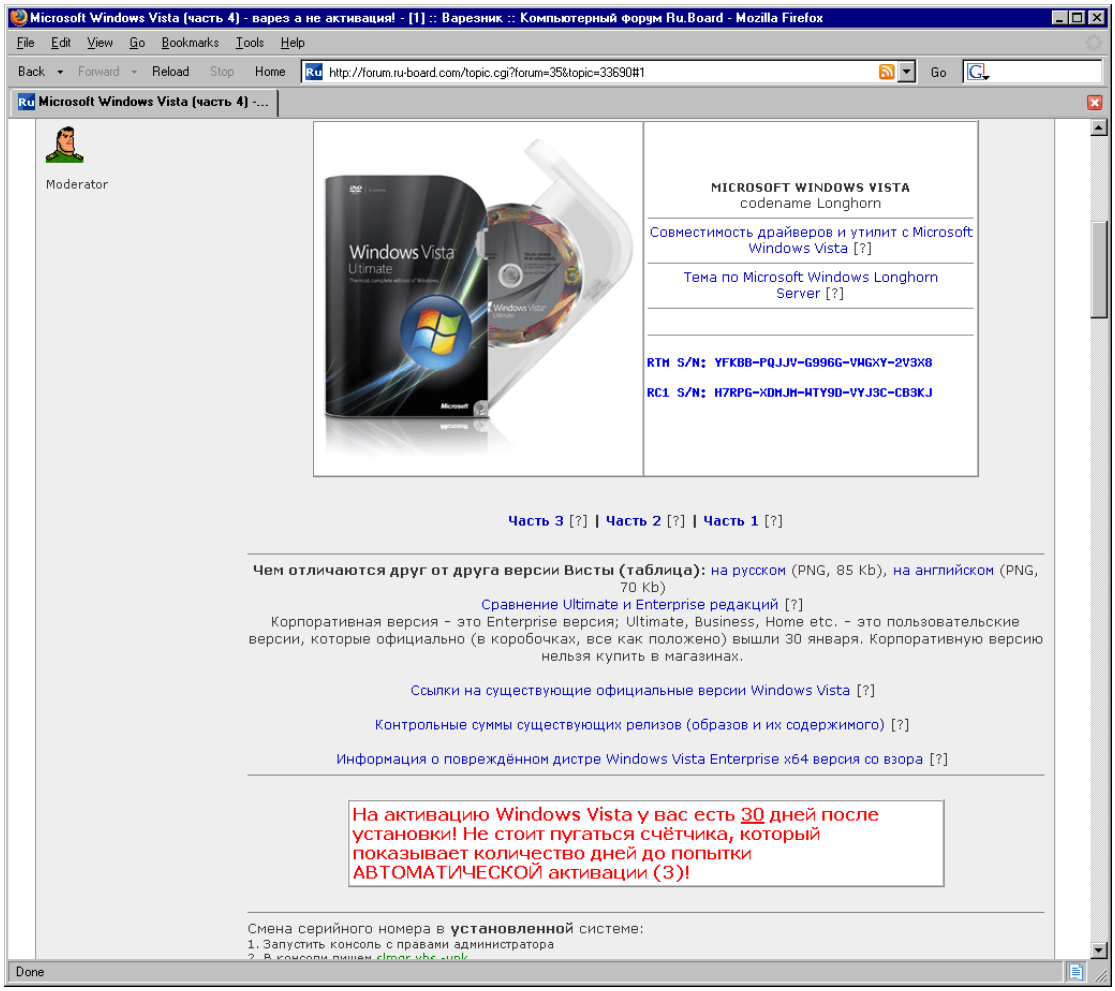

Рисунок 3 ссылки на корпоративную версию Висты на форуме www.ru-board.com

По умолчанию ключи, выдаваемые службой KMS, ограничиваются 6 компьютерами, каждому из которых предоставляется до 9 повторных активаций, однако, при необходимости Microsoft может предоставить специальные KMS-ключи, рассчитанные на заданное количество активаций, впрочем, если покурить хорошей травы, то можно обойтись и без помощи Microsoft. Достаточно, например, установить систему на виртуальную машину, получить KMS-ключ и снять образ, используя его столько раз, сколько компьютеров необходимо активировать.

Осознавая слабость KMS-ключей, Microsoft ужесточила правила KMS-активации. Прежде всего, KMS-сервер начинает раздавать CID'ы только после того, как получает по меньшей мере 25 запросов на активацию от _разных_ машин. Microsoft прямо так и пишет: "*использование службы KMS предназначено для управляемых сред, в которых к сети организации постоянно подключено более 25 компьютеров… Клиентские компьютеры используют информацию, полученную на сервере службы KMS, для самостоятельной активации. К серверу службы KMS должно быть подключено не менее 25 физических клиентских компьютеров под управлением системы Windows Vista, прежде чем какой-либо из этих компьютеров сможет пройти активацию. Это число называется значением n или счетчиком n. Компьютеры, работающие в средах виртуальных машин (VM), также могут активироваться с помощью службы KMS, но они не включаются в число активированных систем*". Как обеспечить подключение 25 узлов в рамках домашней локальной сети?! Ну это даже не вопрос! Ставим виртуальную машину на 24х компьютерах, на каждый из них водружаем Висту, забрасываем образ KMS-сервера и отправляем запрос на активацию, после чего перетаскиваем образ KMS-сервера на свою основную систему и отправляем 25й запрос. Все! Сервер считает, что к нему подключено 25 узлов и активирует нас словно родную маму.

В отличии от MAK-активации (которую достаточно выполнить всего один раз), KMS-активацию необходимо повторять каждые 180 дней, по прошествии которых она аннулируется и система переходит в 30-дневный период, а когда он закончится — в режим ограниченной функциональности до момента подключения к KMS-серверу или MAK-активации, что по

замыслу Microsoft'a предотвращает использование компьютеров в течение неопределенного срока без наличия соответствующей лицензии после их изъятия из организации.

По умолчанию неактивированные клиенты пытаются подключиться к KMS-серверу каждые два часа (это значение является настраиваемым), а после прохождения активации — каждые семь дней (это значение так же является настраиваемым) и в случае успешного завершения операции обновляют 180-дневный счетчик дней, оставшихся до истечения срока активации. Если активизацию по каким-то причинам выполнить не удалось, система продолжит "долбить" сервер, предпринимая настойчивые попытки повторной активации, отключить которые можно путем изменения значения параметра реестра HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SL\Activation\Manual на 1.

Причиной провала активации зачастую становится недемократично настроенный брандмауэр. Для KMS-активации Виста использует анонимный RPC-протокол поверх TCP, стучащийся в порт 1688 (впрочем, номер порта не является жестко заданным и при желании может быть изменен). Клиентский компьютер устанавливает TCP-соединение с KMS-сервером и передает один пакет запроса. KMS-сервер отвечает и закрывает сеанс. Как при запросе активации, так и при запросе обновления используется один и тот же тип передачи запроса и получения ответа, суммарная длина которого составляет 450 байт. Запросы и ответы регистрируются клиентом в журнале событий приложений (события компонента Microsoft Windows Security Licensing SLC 12288 и 12289, соответственно). KMS-сервер регистрирует клиентских компьютеров запросы в событиях компонента Microsoft-Windows-Security-Licensing-SLC 12290.

установка и активация Висты

Таким образом, для миграции на Висту нам необходимо иметь загрузочный DVD-образ Windows Vista Business/Enterprise Edition, который можно добыть в осле или скачать с www.ru-board.com. В Enterprise-версии ключ продукта (Product Key, он же серийный номер) уже зашит внутри pid.txt и потому вводить его при установке не требуется.

Активировать Висту можно на любом "подпольном" KMS-сервере, адреса которых публикуются на хакерских форумах (см. так же одноименную врезку). Для этого необходимо запустить консоль с правами администратора, воспользовавшись службой RunAs (или, завершив текущий сеанс, войти в систему под администратором), после чего набрать следующие команды:

```
$cscript \windows\system32\slmgr.vbs -skms IP_адрес_KMS_сервера:порт
$cscript \windows\system32\slmgr.vbs -ato
```

Листинг 1 активация через хакерский KMS-сервер

Для проверки успешности активации можно воспользоваться ключом -dli, переданным все тому же скрипту slmgr.vbs:

```
$cscript \windows\system32\slmgr.vbs -dlv
Версия службы лицензирования программного обеспечения: 6.0.5384.4
ActivationID:          14478aca-ea15-4958-ac34-359281101c99
ApplicationID:         55c92734-d682-4d71-983e-d6ec3f16059f
Расширенный PID:       11111-00140-009-000002-03-1033-5384.0000-1942006
Установочный ID:       000963843315259493598506854253663081409973656140419231
```

Листинг 2 проверка успешности KMS-активации

Узнать сколько дней осталось до повторной KMS-активации поможет ключ -dli, выдающий подробную информацию по регистрации (для вывода более детальной информации о лицензировании используйте ключ -dlv all):

```
$cscript \windows\system32\slmgr.vbs -dli
Имя: Windows(TM) Vista, Enterprise edition
Описание: Windows Operating System - Vista, ENVIRONMENT channel
Частичный ключ продукта: RHXCM
Состояние лицензирования: Лицензированное
Истечение срока действия корпоративной активации: 43162 минут (29 дней)
Окончание ознакомительного периода: 29.08.2007 16:59:59
Client Machine ID (CMID): 45d450a8-2bef-4f04-9271-6104516a1b60
Автоматическое обнаружение с помощью DNS: Имя сервера KMS не доступно с помощью DNS
Расширенный PID сервера KMS: 11111-00140-008-805425-03-1033-5384.0000-1752006
Интервал активации: 120 минут
```

```
Интервал обновления активации: 10080 минут
```

Листинг 3 получение сводной информации по KMS-активации

Если slmgr.vbs возвращает код ошибки (записанный в шестнадцатеричной нотации), определить соответствующее ему текстовое сообщение можно с помощью утилиты slui.exe, запущенной из командой строки следующим образом: slui.exe 0x2a 0x<код ошибки>, например:

```
$slui.exe 0x2a 0x8007267C
Для локальной системы не настроено ни одного DNS-сервера.
```

Листинг 4 пример использования утилиты slui, для получения описания ошибки по ее hex-коду

Ключи активации, сгенерированные подпольным KMS-сервером хорошо подходят для локальной регистрации системы, но "палятся" при установке обновлений, которые Виста загружает автоматически и чтобы не нарваться на неприятности службу "Windows Anytime Upgrade" следует отключить, скачивая критические обновления безопасности вручную (они не требуют проверки подлинности).

Открываем редактор реестра, заходив в HKLM\Software\Microsoft\Windows \CurrentVersion\Policies, создаем там раздел \Explorer\WAU (в результате чего, полная ветвь будет выглядеть так HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\WAU), переходим к \WAU и создает там ключ "Disabled" типа DWORD, установленный в значение "1". Все! Теперь служба автоматических обновлений отдыхает!!!

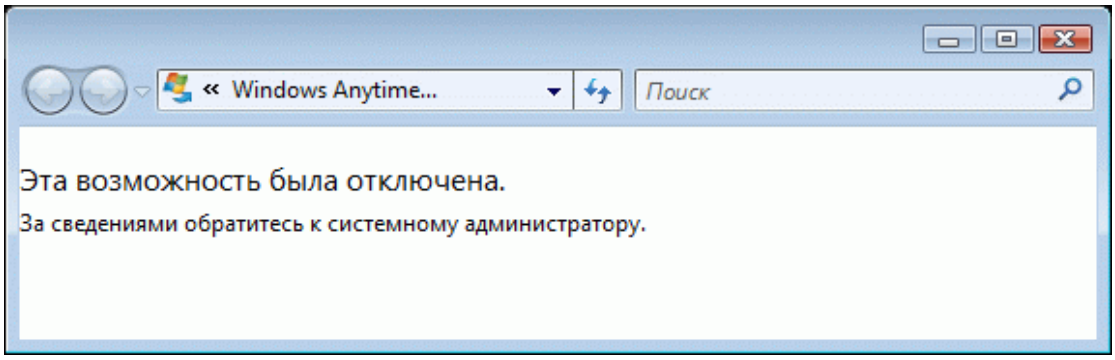

Рисунок 4 служба автоматического обновления системы Windows Anytime Upgrade успешно отключена!

Как вариант, можно активировать систему с помощью образа уже активированного KMS-сервера, который можно найти либо на самом DVD-диске известного происхождения, либо скачать с www.ru-borad.com или осла. Достоинство этого решения в том, что образ, устанавливаемый на виртуальную машину (которой обычно является VM Ware) не требует наличия выхода в Интернет и вообще не зависит ни от чьей воли (подпольные KMS-сервера могут закрыться в любой момент, ищи их потом…), а недостаток — необходимость устанавливать VM Ware, представляющую собой коммерческий продукт весом в полгектара. И хотя существует бесплатный "проигрыватель" образов VM Ware Player, с ним приходится изрядно потрахаться, прежде чем KMS-сервер увидит виртуальный сетевой адаптер, связывающий его с основной операционной системой.

Просмотреть количество оставшихся лицензий, а так же узнать параметры сервера можно следующим образом:

```
$cscript \windows\system32\slmgr.vbs -dli
Служба управления лицензиями активна
Текущее количество: 7
Порт: 1688
Опубликование DNS-записей: разрешено
Приоритет KMS: нормальный
```

Листинг 5 просмотр параметров KMS-сервера

заключение

Помимо описанных выше, существует множество других способов активации, основанных на модификации исполняемых файлов или редактировании прошивки BIOS'a с целью включения в него валидного OEM-идентификатора, обнаружив который Виста вообще не требует никакой активации. Однако, все эти способы ненадежны и небезопасны, а потому прибегать к ним можно разве что из желания поэкспериментировать. Никаких других оснований у нас нет. Какой смысл отказываться от MAK/KMS-активации, особенно в нашей стране, где достать корпоративную редакции Висты ничуть не сложнее, чем версию для розничной продажи?!

>>> врезка активные хакерские KMS-серверы

Ниже приводятся адреса некоторых "подпольных" KMS-серверов, пригодных для активации корпоративных версий Висты, приобретенных в соседнем киоске в полном соответствии с действующим законодательством.

Номера портов периодически меняются, поэтому, прежде чем активироваться следует посетить главную страницу и ознакомиться с оперативной ситуацией. В частности, для захода на сервер "kms.vbs.net.cn:7249" необходимо оттяпать номер порта (7249) и субдомен "kms", набрав в адресной строке браузера: "vbs.net.cn", где среди китайских иероглифов отыскать необходимую информацию (см. рис. 5).

- kms.vbs.net.cn:7249
- pkms.xicp.cn
- 210.51.189.66:1025
- 210.51.189.66:1888
- 121.46.195.58:1688

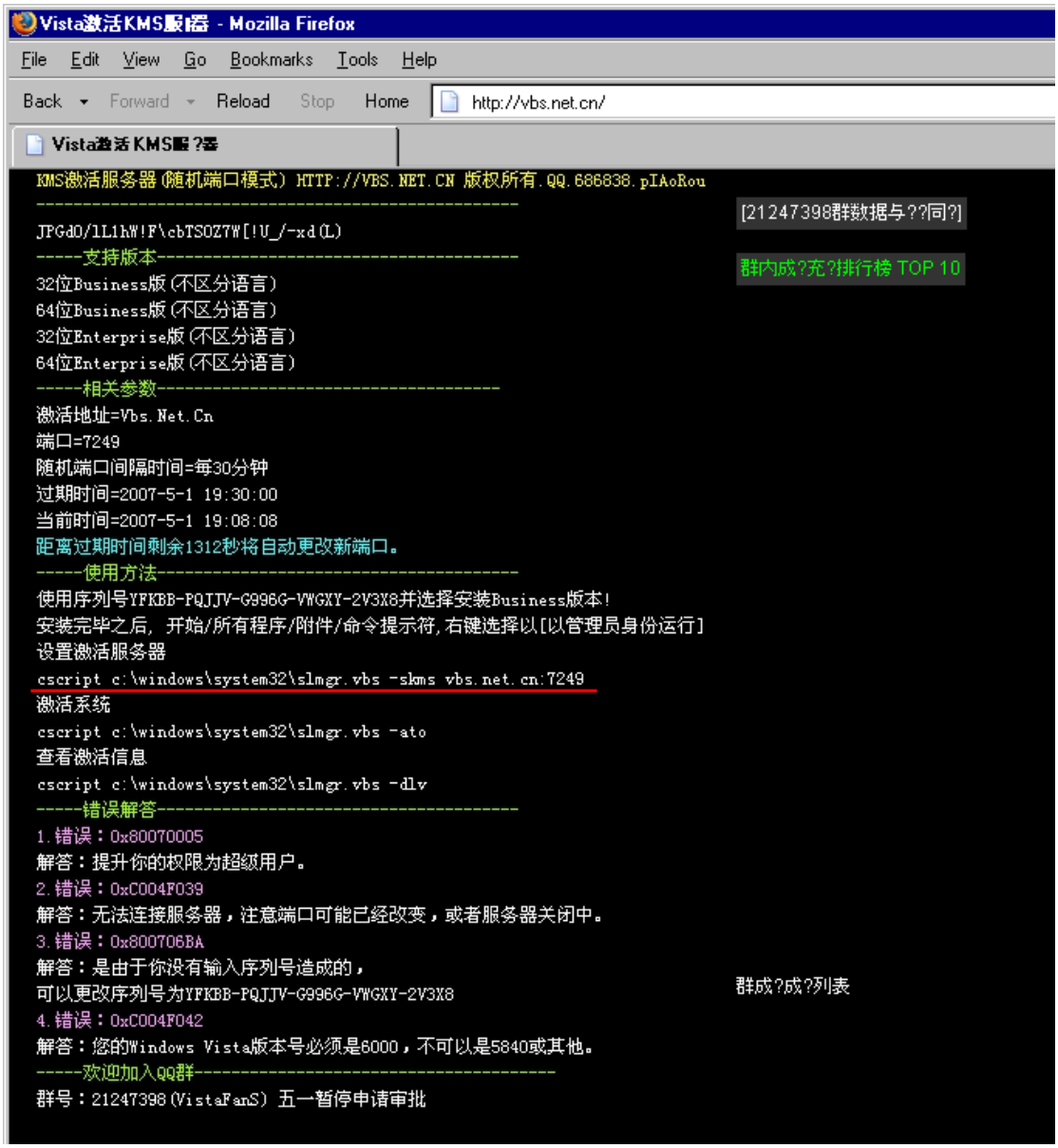

Рисунок 5 главная страница подпольного китайского KMS-сервера vbs.net.cn, где среди иероглифов отчетливо выделяется текущий назначенный порт, равный в данном случае 7249

>>> врезка активация висты с помощью MAK-ключа

Существует два способа MAK-активации: самостоятельная и опосредованная. Самостоятельная MAK-активация выполняется пользователем и требует прямого соединения с Интернет. Опосредованная MAK-активация позволяет выполнять централизованный запрос активации для нескольких компьютеров с помощью одного подключения к серверам компании Microsoft, однако, в настоящее время она все еще находится в стадии разработки, проходящем под кодовым названием "средство VAMT" (что расшифровывается как Volume Activation Management Tool — средство управления многопользовательской активацией), поэтому, ниже будет рассмотрена только самостоятельная активация.

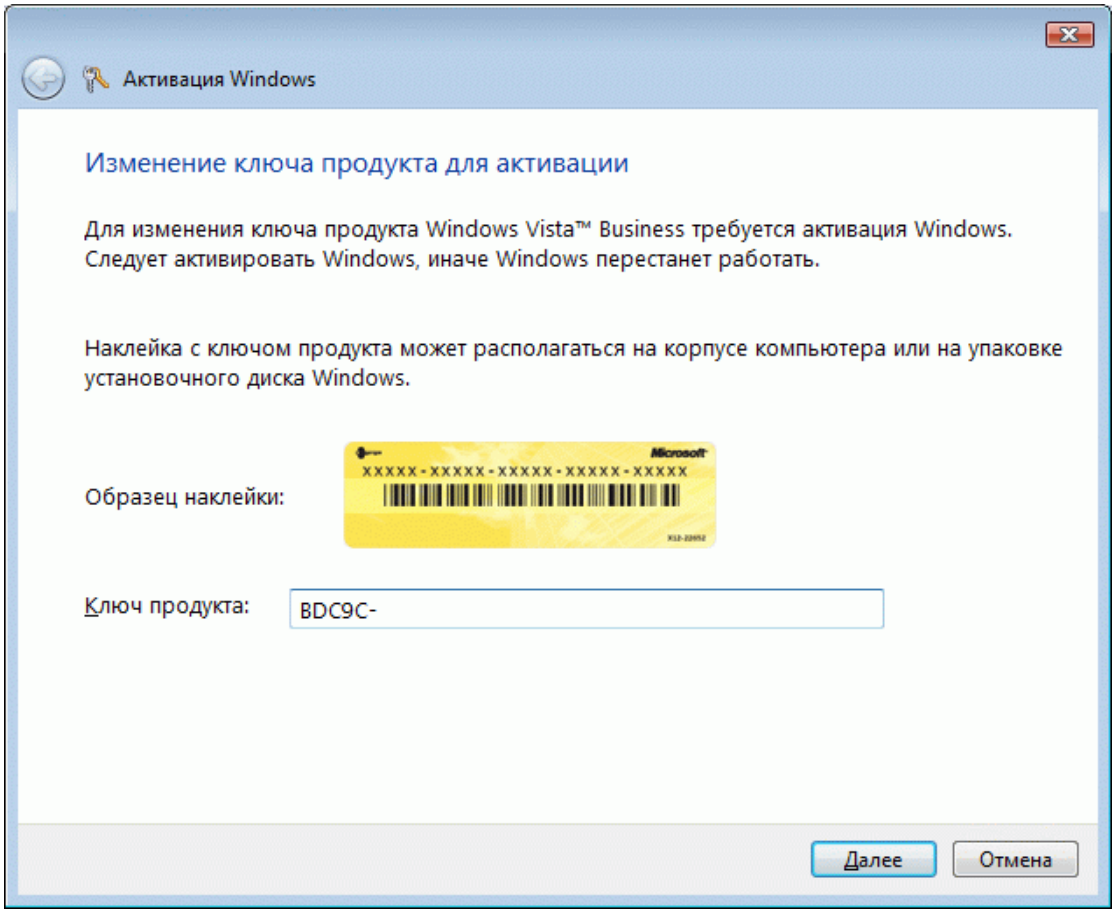

Рисунок 6 ввод MAK-ключа для активации Висты через графический интерфейс

Проще всего активировать компьютер через графический интерфейс. Для этого необходимо:

- установить нужный носитель с корпоративной лицензией (во время установки ключ продукта не требуется);
- войдя в систему с правами администратора, открыть Пуск → Панель Управления → Компьютер → Свойства;
- в разделе "активация" нажать кнопку "изменить ключ продукта";
- подтвердив запрос на изменение (кнопка "продолжить"), ввести MAK-ключ;
- в следующий запланированный интервал времени компьютер попытается выполнить активацию через Интернет, сообщая об успешности (или не успешности) операции;

Поклонники командной строки могут активировать Висту через скрипт slmgr.vbs, передав ему ключ -ipk вместе с MAK-ключом:

```
$cscript \windows\system32\slmgr.vbs -ipk <MAK-ключ >
```

Листинг 6 немедленная MAK-активация в командной строке

>>> врезка полезные ссылки

- **Microsoft Windows Vista — варез а не активация**!
  - ссылки на корпоративную редакцию Висты, образы активированных KMS-серверов, пошаговые руководства по активации (на русском языке): http://forum.ru-board.com/topic.cgi?forum=35&topic=33690#1;
- **Windows Genuine Advantage**:
  - обзорная статья на wikipedia, посвященная WGA (на английском языке): http://en.wikipedia.org/wiki/Windows_Genuine_Advantage;
- **Пошаговое руководство к службе Windows Vista Volume Activation 2.0**:

- официальный документ от Microsoft по системе активации (на русском языке): http://www.microsoft.com/rus/technet/windowsvista/plan/volact1.mspx;

- **The Windows Genuine Advantage (WGA) and Office Genuine Advantage (OGA) FAQ**:
  - официальный FAQ по WGA и OGA от Microsoft (на английском языке): http://www.microsoft.com/genuine/downloads/FAQ.aspx?displaylang=en;
- **SLA 2.0 Supported BIOSes for Instant Windows Vista OEM Activation**:
  - статья, рассказывающая об OEM-активации Висты, осуществляемой путем редактирования прошивки BIOS (на английском языке): http://www.mydigitallife.info/2007/02/21/sla-20-supported-bioses-for-instant-windows-vista-oem-activation/;
- **LogMeIn Hamachi**:
  - популярная программа для безопасного обмена файлами через VPN, используемая многими хакерами для распространения Висты: http://www.hamachi.cc/;