BIOS-моддинг

крис касперски ака мыщъх

модификация BIOS'а таит в себе практически неограниченные возможности: экстремальный разгон системы, разблокирование заблокированных фич, исправление ошибок разработчиков, неуловимые вирусы, "украшательства" под свой вкус — это высший пилотаж хакерства, требующий знания железа и умения держать дизассемблер в руках. это дремучий лес, в котором очень легко заблудится, но я покажу вам кратчайший путь.

введение

Если процессор это сердце компьютера, то BIOS — его душа. Качество прошивки определяет все! К сожалению, качественные прошивки в живой природе встречаются крайне редко. Разработчики допускают грубые ошибки, блокируют многие полезные возможности (вот редиски!) и вообще ведут себя самым непотребным образом. Старые модели материнских плат зачастую вообще не имеют свежих прошивок и с новым оборудованием (например, жесткими дисками большого размера) они уже не работают, а ведь могли бы…

Многие качественные материнские платы умышленно препятствуют разгону, имеют скудный диапазон допустимых знаний или слишком грубый шаг их изменения. Разумеется, очень многое зависит и от электрической части, но без правильной прошивки — никуда! В сети можно найти множество улучшенных прошивок, хакнутых энтузиастами, однако, все они заточены под вполне конкретную модель (как правило, уже устаревшую) и раздобыть прошивку для своей материнской платы невероятно трудно.

А моддинг? Разве не заманчиво заставить компьютер перемигиваться огоньками во время загрузки или выводить красочный логотип на экран?! Наконец, при желании можно написать крутой вирус, заражающий BIOS и препятствующий его удалению оттуда. Это не штука! Ничего сложного в этом нет, особенно если подцепить к вирусу готовые утилиты для редактирования BIOS'а (их объем не составляет и полсотни килобайт), а утилита прошивки, как мы скоро увидим, содержится в самом BIOS'е!

Одним словом, хачить BIOS не только можно, но и нужно. Главным образом мы будем говорить об Award BIOS'ах. В AMI все сильно по другому… Однако, когда-нибудь мы доберемся и до них. Кстати говоря, фирма Award была выкуплена Phoenix'ом и в настоящее время существует только как бренд (в смысле — торговая марка). А это значит, что Phoenix-BIOS'ы устроены точно так же как и Award, поскольку их пишет одна и та же фирма.

что нам понадобиться

Для экспериментов нам потребуется материнская плата с Award-BIOS'ом на борту. Опознать микросхему BIOS'а очень легко — на ней обычно накалена голографическая этикетка, которую необходимо оторвать, чтобы обнажить маркировку. Маркировка представляет длинный ряд цифр наподобие "28F1000PPC-12C4". Идем на http://www.datasheetarchive.com, заполняем строку запроса и получаем pdf-файл с подробным описанием чипа (так называемый datasheet). Теперь необходимо найти идентичный или совместимый чип FLASH-памяти, над которым мы, собственно, и будем экспериментировать. Его можно купить на радио-рынке или вытащить с поломанной матери.

Для "горячей" замены BIOS'а (т. е. выдергивания микросхемы с работающей платы), русские обвязывают микросхему нитками (можно, конечно, подковырнуть и отверткой, но при этом легко что-то закоротить), а вот гады-иностранцы после эпидемии "чиха" придумали специальные приспособления — chip extractor (съемщик чипов) и BIOS saviour (BIOS-спаситель). Приобрести их можно в продвинутых радиомагазинах или заказать по Интернету.

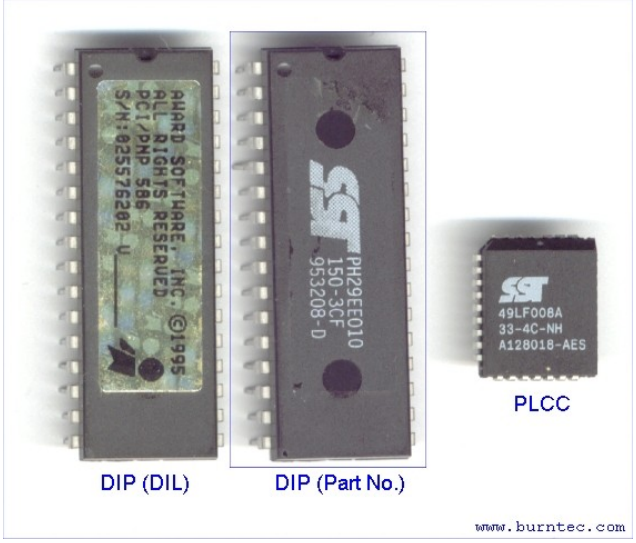

Рисунок 1 различные типы микросхем FLASH-памяти

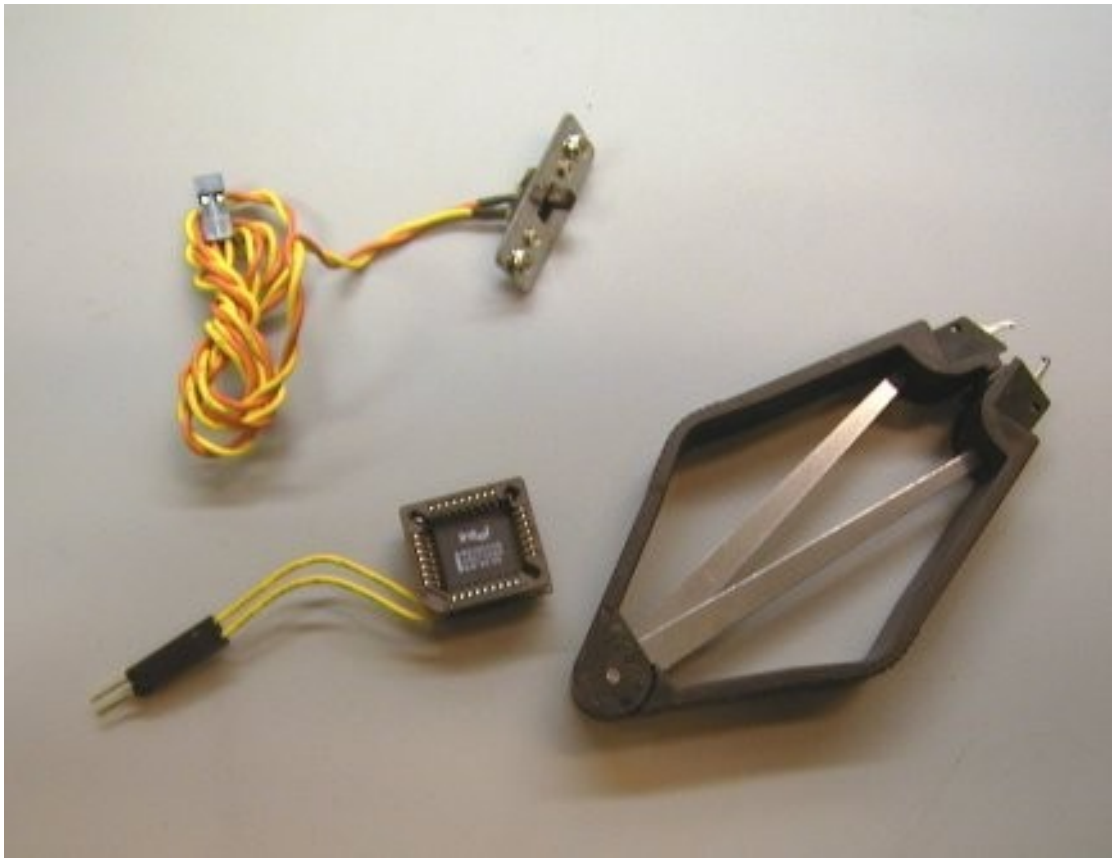

Рисунок 2 BIOS Saviour, облегчающий выемку чипа с работающей матери

Рисунок 3 BIOS extractor в действии!

Еще нам потребуется документация на чипсет материнской платы. Компании Intel и AMD бесплатно выкладывают все даташиты на сайт. Другие производители (VIA, SiS) держат ее под спудом и отдают только за деньги плюс подписку о неразглашении, поэтому приходится изрядно попыхтеть, прежде чем удается что-то нарыть.

Комплект утилит для прошивки BIOS'a можно найти на сайте разработчика BIOS'a или производителя материнской платы. Некоторые производители (например, ASUS) вносят в BIOS множество изменений, в результате чего "родные" Award'овские утилиты перестают с ними работать и приходится использовать инструментарий, поставляемый вместе с материнской платой. Обычно там содержится: awdflsh.exe – "прожигатель", modbin – простой редактор BIOS'a, cbrom – просмотрщик содержимого BIOS'a и "добавитель" новых модулей в прошивку. Все эти утилиты можно найти на сайте www.rom.by. Там же находится замечательный падчер BIOS'a — BP.exe (сокращение от "BIOS Pather"), исправляющий ошибки в известных ему прошивках и разблокирующий многие заблокированные возможности. Нашим основным инструментом будет интерактивный редактор BIOS'a Award BIOS Editor, который можно бесплатно скачать с http://awdbedit.sourceforge.net/.

Ассемблер — MASM, TASM или FASM, дизассемблер — IDA Pro (четвертая версия которой распространяется на бесплатной основе) или NASM, шестнадцатеричный редактор — HIEW или HexWorkshop.

как мы будем действовать

Модификация BIOS'a — очень рискованное занятие (только для сильных духом мужчин!). Малейшая ошибка — и система отказывается загружаться, выдавая унылый черный экран. Большинство современных матерей снабжены защитами от неудачных прошивок, однако, они срабатывают лишь тогда, когда BIOS действительно поврежден. К тому же, как мы покажем в дальнейшем, легко написать свое OEM-расширение ROM, препятствующее перезаписи BIOS"а штатными средствами.

Вот для этих целей нам и требуется второй BIOS! Запускаем материнскую плату, дампим прошивку (или скачиваем обновленную версию с сайта производителя), модифицируем ее по своему вкусу, затем, не выключая компьютера, аккуратно вынимаем оригинальный чип, откладывая его в сторону, вставляем чип, над которым мы будем экспериментировать, и, запустив AWDFLASH.EXE, заливаем хакнутую прошивку в BIOS. Теперь, случись вдруг чего, мы всегда сможем вернуть оригинальный чип на место, исправить ошибку и перешить экспериментальный BIOS вновь.

Насколько такая процедура безопасна? По правде говоря, опасности нас подстерегают на каждом шагу. Микросхема может выскользнуть из рук и упасть на плату, малейшая ошибка в прошивке может вывести оборудование из строя (например, нечаянно "задрать" напряжение или тактовую частоту). До приобретения боевого опыта лучше всего насиловать старые материнские платы, которые все равно идут в утиль (например, Pentium-155).

>>> врезка как прожигают BIOS'ы

AMI BIOS'ы имеют специальный интерфейс, позволяющий работать с микросхемой FLASH-памяти (читать или прожигать), доступный через прерывания INT 15h и INT 16h (подробности — в Interrupt List'e Ральфа Брауна). Award BIOS'ы такой возможности не имеют и программируются через порты ввода/вывода.

Конструктивно FLASH-микросхема подключена к южному мосту чипсета. Со всеми вопросами обращайтесь к нему, а точнее к его документации.

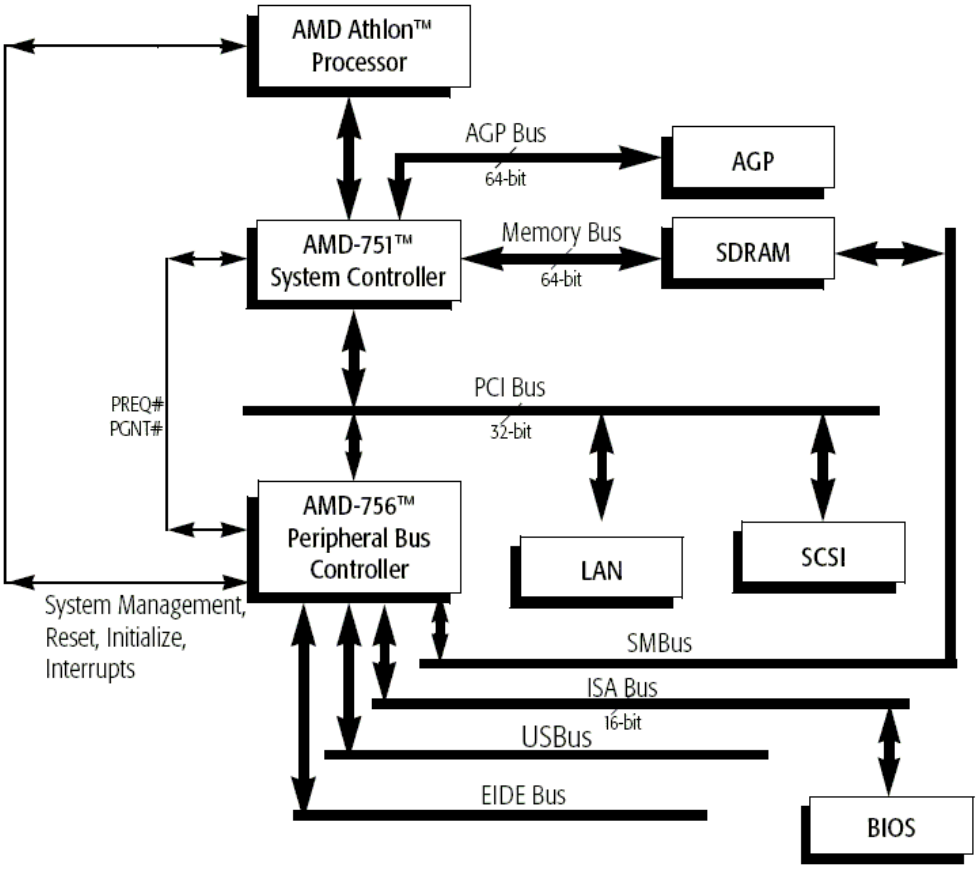

Рисунок 4 микросхема FLASH-памяти, подключенная к южному мосту

>>> врезка DUAL-BIOS своим руками

Всякий, умеющий держать паяльник в руках, может доработать материнскую плату, установив на нее сразу две микросхемы FLASH–памяти. Тогда, между ними можно будет переключаться без рискованных манипуляций с chip-extractor'ом. Пример схемы подключения приведен ниже. Как видно, ничего сложного в DUAL-BIOS'е нет.

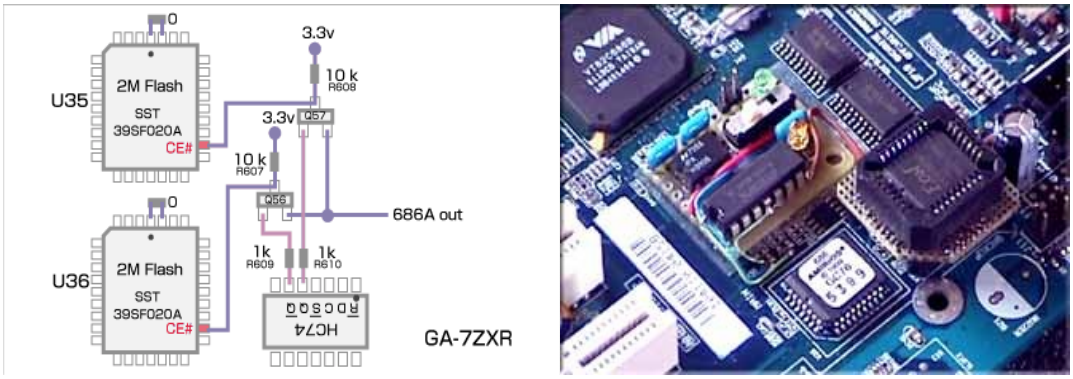

Рисунок 5 принципиальная схема DUAL-BIOS'a и ее материальное воплощение

начинаем хулиганить

Запускаем Award BIOS editor (кстати говоря, он запускается только из-под GUI, а под FAR'ом просто "слетает"), в меню File выбираем файл с прошивкой, которую мы будем модифицировать (предварительно ее необходимо скачать с сайта производителя или запустить AWDFLASH.EXE с ключом /sy, чтобы сдампить текущую прошивку в файл). В левой колонке выбираем пункт "System BIOS" и смотрим, что хорошего тут можно изменить. А изменить тут можно достаточно многое! Например, имя BIOS'a, высвечивающееся при загрузке (в моем случае это: Award Modular BIOS v6.00PGN), дату выхода и название чипсета (03/29/2001-i815-W83627F-6A69RI3DC-00) и другие идентификационные строки подобного типа. А давайте напишем "hacked by Visual Sex Ltd, hacker's Turbo-BIOS", чтобы потом поприкалываться над подвыпившими приятелями.

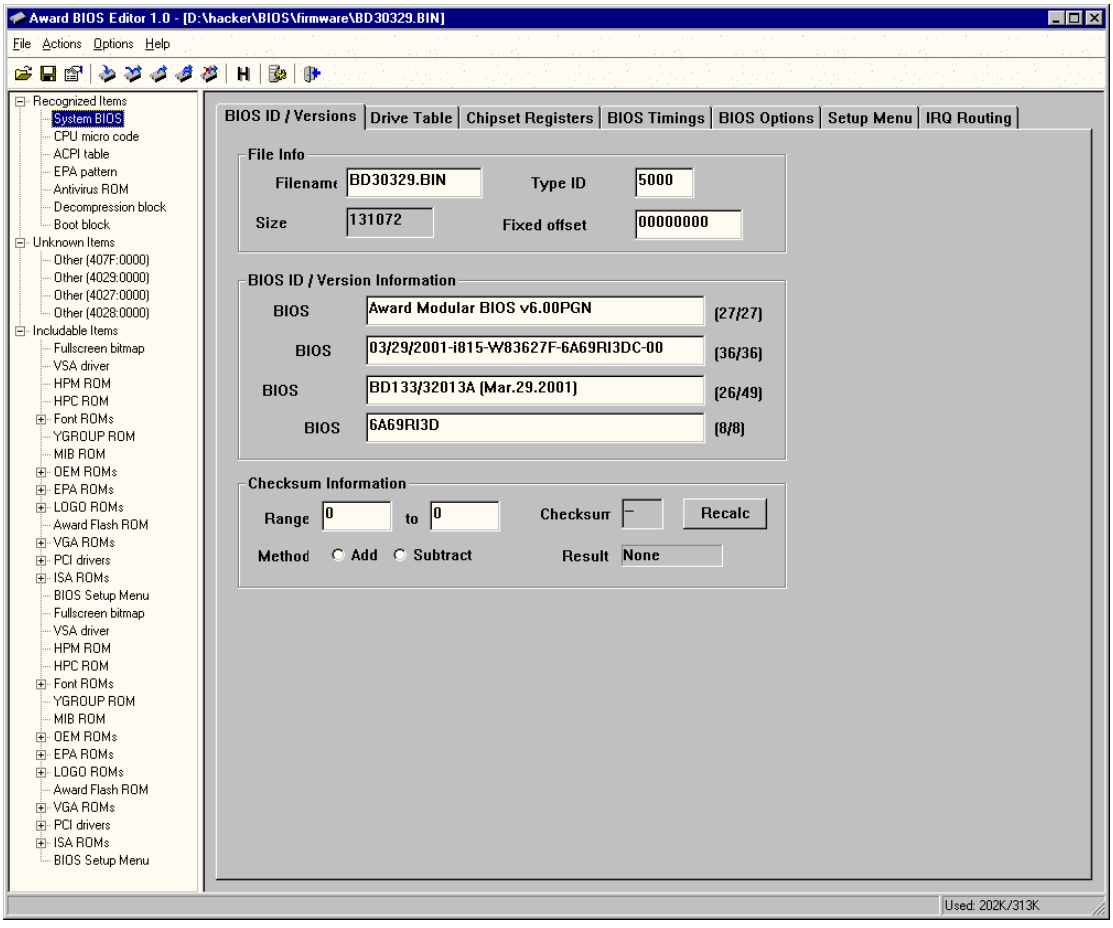

Рисунок 6 Award BIOS editor готовый к хачинью текстовых строк, высвечивающихся при загрузке системы

Точно так же можно заменить все надписи в BIOS Setup (они находятся во вкладке BIOS Options), при желании указав значения по умолчанию (ну те самые, что загружаются по команде "load default BIOS configuration"). Наибольший интерес представляют пункты, помеченные как "Disabled". Это опции, заблокированные производителем! Простым переводом радио кнопки в состояние "Active" мы разблокируем их! Разумеется, никакой гарантии, что они заработают у нас нет! Чаще всего блокируются недоделанные или нестабильно работающие режимы и возможности. Реже — производитель просто не хочет, чтобы материнские платы начального уровня конкурировали с дорогими моделями, вот и тормозит их.

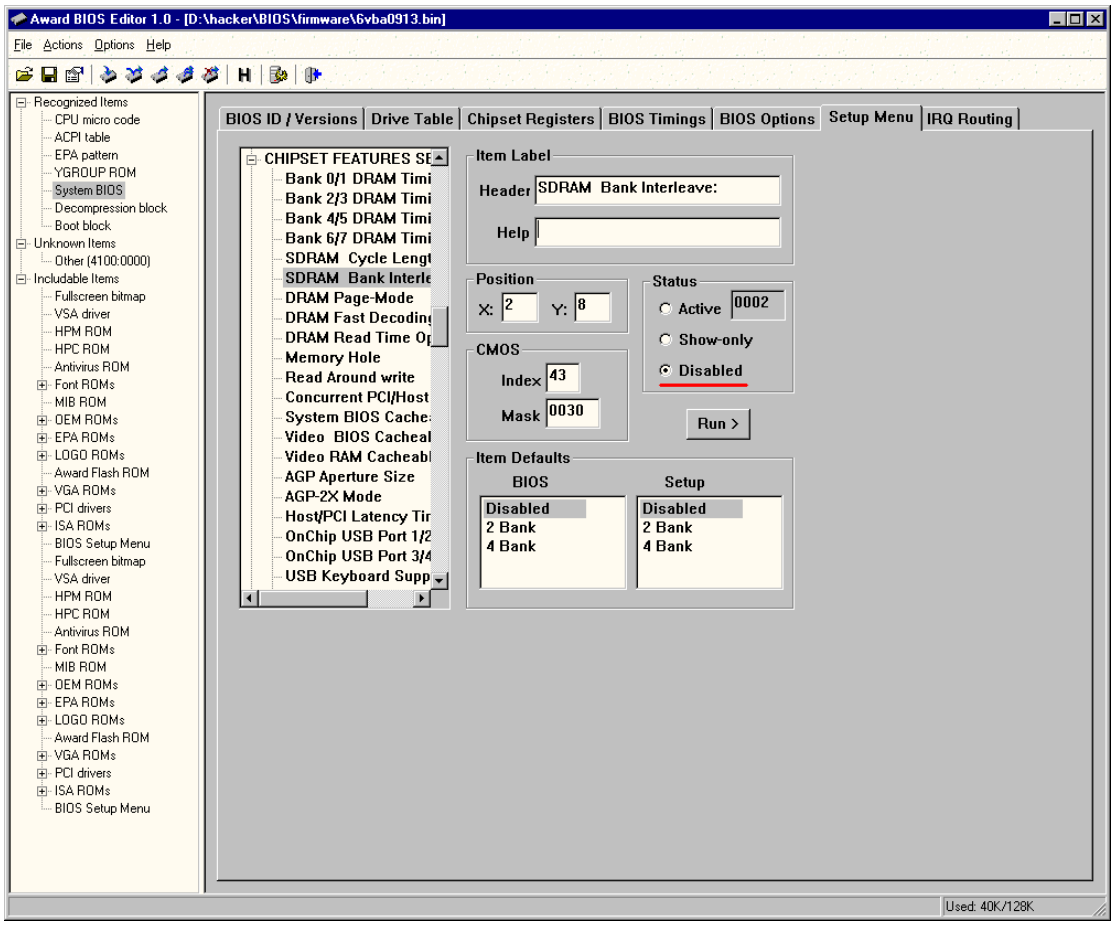

Рисунок 7 разблокирование заблокированных возможностей в BIOS Setup

А хотите изменить логотип, высвечивающийся в северо-восточном углу экрана? Это совсем несложно сделать. Старые BIOS'ы хранили картинку в logo-формате (конвертор для которого прилагается к статье), который страдал кучей ограничений. Сейчас же секция "LOGO" обычно пуста, а картинка хранится в секции "EPA pattern" в стандартном BMP-формате. Ограничений на размер и глубину цветности нет никаких, однако, не все BIOS'ы поддерживают слишком большие и цветастые картинки. Я поступал так: извлекал оригинальный логотип в файл ("Export as Windows BMP"), загружал его в Paint, где и правил его в свое удовольствие без изменения количества цветов и размеров. Результат моей работы приведен ниже. Мыщъх – это я. И я атакую! При желании можно зашить в BIOS полноэкранное лого, высвечивающиеся при загрузке (этим занимается одноименная утилита от Award, входящая в штатный комплект поставки многих ASUS'ых матерей).

Рисунок 8 хакнутый логотип

Запустив утилиту BP.EXE с ключиком /c, мы сможем вручную задать имя процессора, высвечивающиеся при загрузке и его тактовую частоту. Реальная тактовая частота процессора отображаться уже не будет. Почему бы не написать "AMD Pentium-5 600 GHz" и не показать это друзьям?

Да много чего можно придумать! В умелых руках BP.EXE и Award BIOS editor творят чудеса! Как бы там ни было, после всех издевательств прошивка должна быть залита в BIOS. О том как это сделать, можно прочитать в документации на материнскую плату, мы же не будем толочь воду в ступе, оставим мелкие шалости и перейдем к более серьезным вещам.

настройка PCI-регистров

Конфигурирование чипсета осуществляется через специальные регистры, доступные через шину PCI. При загрузке системы BIOS настраивает процессор, контроллер системной шины, контроллер оперативной памяти и всю прочую периферию в соответствии с настойками, выбранными в BIOS Setup. Однако, практически ни один BIOS не дает доступа ко всем настройкам или умышленно ограничивает диапазон доступных значений. Как быть, что делать?

Запускаем Award BIOS editor, заходим в System BIOS, находим вкладку "Chipset Registers" и открываем документацию на чипсет. Где-то там будет раздел "PCI Configuration Registers" или что-то в этом роде. Для каждого из регистров будет указано устройство (device), к которому он "подключен"), номер функция (function) и номер самого регистра, называемый смещением (offset). Все регистры 8-битные, однако, несколько последовательных регистров могут объединяться в слова или даже двойные слова.

Сравнение конфигурационных возможностей чипсета с BIOS Setup показывает, что часть настроек в ней отсутствуют. Даже в заблокированных возможностях (о которых мы уже говорили выше) их нет! В частности, мой любимый AMD 761 поддерживает намного больший диапазон таймингов, чем BIOS. В частности, чтобы установить tPR в 1 такт (BIOS по умолчанию ставит 3 такта и не дает это умолчание изменять), необходимо модифицировать 8 и 7 биты регистра Dev 0:F0:0x54, присвоив им значение 2 (или "10" в двоичной нотации). Остальные биты не трогать! А как это сделать? Необходимо наложить маску (mask), которая в данном случае будет выглядеть так: "XXXX XXX1 1XXX XXXX". Как видно, 8 и 7 бит установлены в единицу, остальные помечены знаком "X", указывающим BIOS'у что данный бит необходимо оставить без изменений.

Bit Definitions (Continued) **DRAM Timing (Dev0:F0:0x54)**

Bit	Name	Function
11–9	t_{RC}	**t_{RC}** This bit field indicates the t_{RC} timing value (bank cycle time: minimum time from activate to activate of same bank). 111 = 10 cycles 110 = 9 cycles 101 = 8 cycles (recommended "safe" configuration) 100 = 7 cycles 011 = 6 cycles 010 = 5 cycles 001 = 4 cycles 000 = 3 cycles
8–7	t_{RP}	**t_{RP}** This bit field indicates the t_{RP} timing value (precharge time: time from precharge to activate on the same bank). 00 = 3 cycles (recommended "safe" configuration) 01 = 2 cycles 10 = 1 cycles 11 = 4 cycles
6–4	t_{RAS}	**t_{RAS}** This bit field indicates the t_{RAS} timing value (minimum bank active time: time from activate to precharge of same bank). 111 = 9 cycles 110 = 8 cycles 101 = 7 cycles (recommended "safe" configuration) 100 = 6 cycles 011 = 5 cycles 010 = 4 cycles 001 = 3 cycles 000 = 2 cycles
3–2	t_{CL}	**CAS Latency of SDRAM** 11 = Reserved 10 = 2.5 cycles 01 = 2 cycles (recommended "safe" configuration) 00 = 3 cycles

Рисунок 9 страничка из документации на чипсет, описывающая конфигурационные регистры

Запись "Dev0:F0:0x54" обозначает: Device 0:Function 0:Register 0x54. На самом деле, этих регистров целых два. Регистр 0x54 хранит младшую, а 0x55 — старшую половину слова. Следовательно, в 0x54 необходимо занести 80h ("10.00.00.00"), а в 0x55 – 01h. Соответственно, в первом случае маска будет равна 80h ("1X.XX.XX.XX"), а во втором 01h.

Возвращаемся к Award BIOS Editor'y, находим среди регистров регистр с номером 0x54, и кликнув правой клавишей мыши, выбираем пункт "modify". В появившимся окне первые три поля (Register, PCI, PCI) оставляем без изменений (это номер регистра, устройства и функции), а вот с двумя последующими полями "Resister" и "Value" придется разобраться особо. Мы не можем просто взять и записать значение 0x80, поскольку в этом регистре уже хранятся какие-то параметры, модифицирующие остальные поля. Мы должны устанавливать лишь "наши" биты (в данном случае это бит 7), а над остальными выполнить операцию логическое "OR" по маске. Аналогичным образом настраивается и регистр 55h.

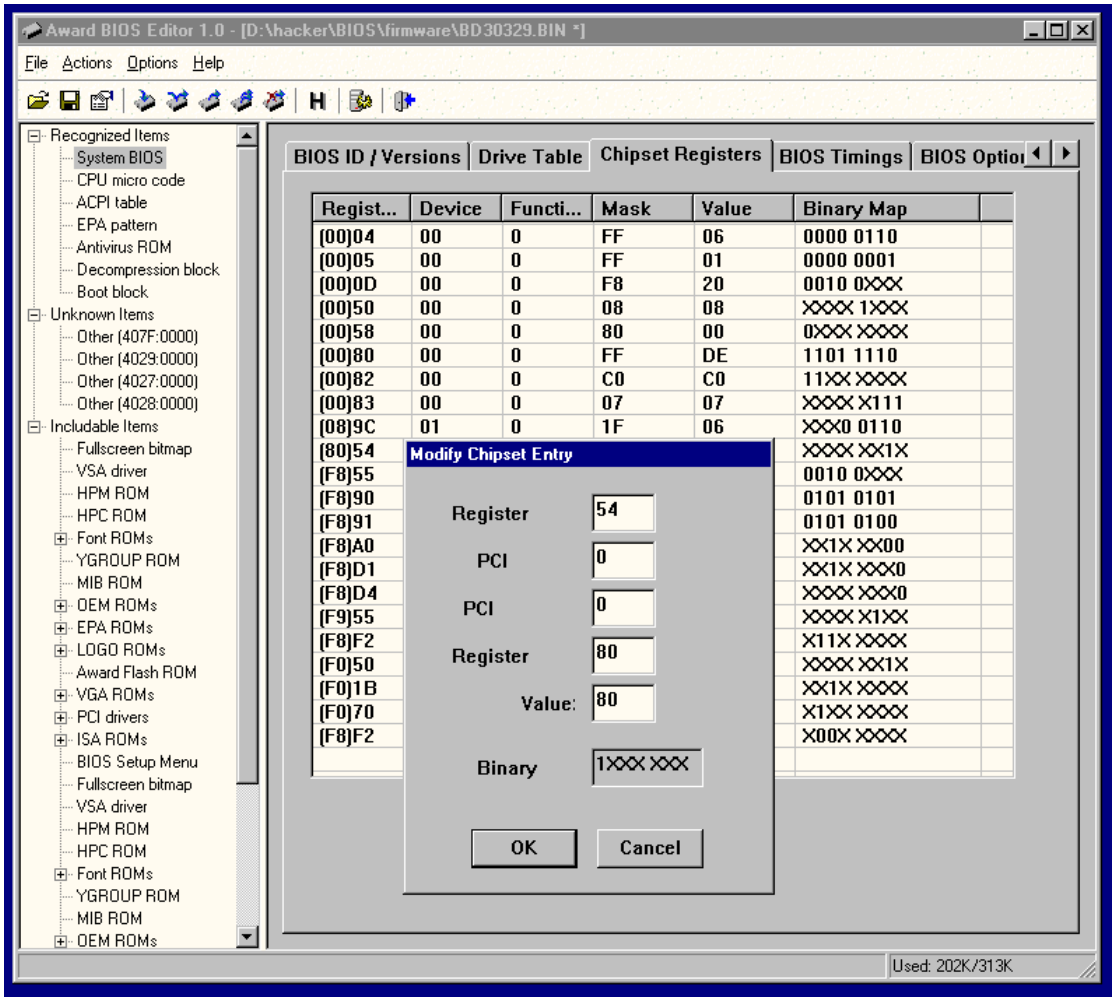

Рисунок 10 разгон системы при помощи редактирования конфигурационных регистров

Залив обновленную прошивку в BIOS и установив качественные модули памяти, мы с удовлетворением замечаем, что быстродействие системы ощутимо возросло. Таким же точно образом можно редактировать и остальные регистры, отсутствующие в BIOS Setup, однако наши возможности будут довольно ограничены.

>>> выноска

Некоторые утилиты, например, WPCREDIT.EXE, позволяют редактировать содержимое некоторых регистров чипсета "налету" прямо из-под Windows, что особенно полезно для экспериментов по экстремальному разгону систем, однако, их возможности весьма ограничены, поскольку многие регистры должны настраиваться лишь на стадии инициализации чипсета и всякая попытка их изменения на работающей системе носит непредсказуемых характер или не носит вообще никакого (чипсет нас попросту игнорирует).

>>> врезка интересные ссылки

- **BIOSmods**
  - портал, посвященный BIOS'у и его доработке (на английском языке): http://www.biosmods.com/;
- **ROM**
  - статьи по прошивке и доработке прошивок, уникальный инструментарий (на русском языке): http://www.rom.by;
- **Часто задаваемые вопросы о BIOS**
  - довольно устаревшее, но все-таки полезное FAQ по BIOS'ам (на русском языке): http://www.ixbt.com/mainboard/faq/biosfaq.shtml;
- **The Official Website of Pinczakko**

- сайт улетного индонезийского хакера, исследовавшего кучу BIOS'ов вдоль и поперек и вытворяющий с ними такое, что другим даже не снилось (на английском и индонезийском языках): http://www.geocities.com/mamanzip/;

- **Modification of GigaByte GA-586HX BIOS rev 2.9 for support of HDD above 32 GiB**
  - интересная статья о модификации BIOS, название которой говорит само за себя (на английском языке): http://www.ryston.cz/petr/bios/ga586hx_mod.html;
- **Award BIOS Reverse Engineering**
  - статья известнейшего хакера BIOS'a Mappatutu Salihun Darmawan по внедрению своего кода в BIOS (на английском языке):http://www.codebreakers-journal.com/include/getdoc.php?id=83&article=38&mode=pdf;
- **Award BIOS Code Injection**
  - новые идеи по внедрению своего кода в BIOS (на английском языке): http://www.codebreakers-journal.com/include/getdoc.php?id=127&article=58&mode=pdf;
- **AWARD BIOS Source**
  - исходные тексты пары устаревших прошивок со скупыми комментариями. помогают понять общие принципы функционирования BIOS'a и разобраться в некоторых тонких местах, неочевидных при дизассемблировании: (на языке ассемблера): http://miscellaneous.newmail.ru/;
- **Редактируем BIOS (Award Modular v.4.51)**
  - описание формата BIOS'a для его ручной распаковки (на русском языке): http://www.winsov.ru/bios002.php;
- **AMD 762 Chipset Tweaking (MP/MPX) Guide**
  - статья по редактированию регистров чипсета (на русском языке): http://www.tweakfactor.com/articles/tweaks/amd762/1.html;
- **Using Oda's WPCREDIT On VIA Motherboards**
  - разгон системы путем редактирования регистров чипеста (на английском языке): http://www.overclockers.com/tips105/index.asp;
- **H.Oda's Home Page**
  - утилита для модификации регистров чипеста на лету: http://www.h-oda.com/;
- **Award BIOS Editor**
  - редактор Award BIOS'ов, распространяемый с исходными текстами на бесплатной основе: http://awdbedit.sourceforge.net/;
- **AWDhack v1.3**
  - утилита для автоматизированного внедрения своего кода в BIOS http://webzoom.freewebs.com/tmod/Awdhack.zip;