МОДИФИЦИРУЕМ BIOS

BIOS-моддинг таит в себе практически неограниченные возможности: экстремальный разгон системы, разблокирование скрытых возможностей, исправление ошибок разработчиков, украшения на свой вкус – это высший пилотаж хакерства, требующий знания железа и умения держать дизассемблер в руках. Это дремучий лес, в котором очень легко заблудиться, но я покажу вам кратчайший путь.

КРИС КАСПЕРСКИ

Если процессор – это сердце компьютера, то BIOS – его душа. Качество прошивки определяет все! К сожалению, качественные прошивки в живой природе встречаются достаточно редко. Разработчики допускают грубые ошибки, блокируют многие полезные возможности, в общем, по отношению к потребителю ведут себя нехорошо. Древние модели материнских плат, выпущенные до 2000 года, зачастую вообще не имеют свежих прошивок и с новым оборудованием (например, жесткими дисками большого объема) они уже не работают, а ведь могли бы…

Многие качественные материнские платы умышленно препятствуют разгону, имеют скудный диапазон допустимых значений или слишком грубый шаг их изменения. Разумеется, очень многое зависит и от «железной» части, но без правильной прошивки – никуда! В сети можно найти множество улучшенных прошивок, модернизированных энтузиастами, однако все они ориентированы на вполне конкретную модель материнской платы (как правило, уже устаревшую), и раздобыть прошивку для своего оборудования весьма затруднительно, к тому же нет никаких гарантий, что под видом «улучшенного» BIOS вам не подсунут заживо похороненную или, что еще хуже, умышленно троянизированную версию.

А моддинг? Разве не заманчиво заставить компьютер перемигиваться клавиатурными огоньками во время загрузки или выводить красочный логотип на экран?! Одним словом, модифицировать BIOS не только можно, но и нужно. Главным образом мы будем говорить об Award BIOS. В AMI все сильно по-другому… Однако когда-нибудь мы доберемся и до них. Кстати говоря, фирма Award была выкуплена Phoenix и в настоящее время существует только как бренд. А это значит, что последние версии Phoenix-BIOS устроены точно так же, как и Award, поскольку их разрабатывает одна и та же фирма, правда, на старые прошивки это утверждение не распространяется. Впрочем, существуют готовые редакторы и для них, но не будет заострять внимание на мелочах, а сразу перейдем к делу.

Что нам понадобится

Для экспериментов нам потребуется материнская плата с Award-BIOS на борту. Опознать микросхему BIOS очень легко – на ней обычно наклеена голографическая этикетка, которую необходимо оторвать, чтобы обнажить маркировку. Маркировка представляет последовательность цифр наподобие «28F1000PPC-12C4».

Как ее расшифровать? 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 приобрести в специализированном радиомагазине или вытащить с поломанной материнской платы. Большого дефицита эти чипы не представляют, поскольку в материнских платах используются серийные микросхе-

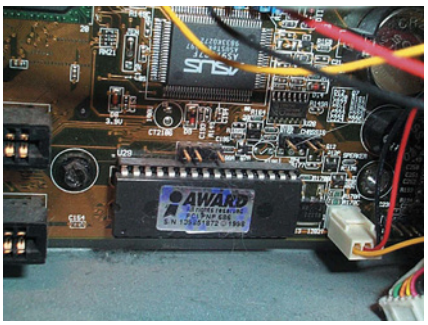

Рисунок 1. Микросхема Award BIOS с традиционной голографической наклейкой, по которой её легко определить

Рисунок 2. Набор BIOS Savior kit для безопасного извлечения микросхемы BIOS с материнской платы и «кроватка» для резервного BIOS с переключателем, устанавливаемым на заднюю панель

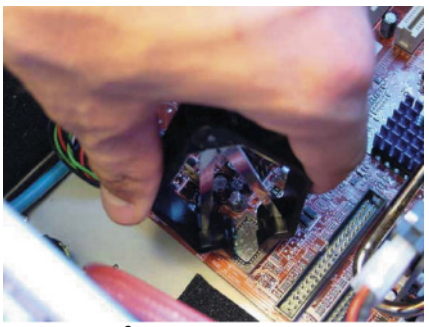

Рисунок 3. Положение рук при съемке микросхемы

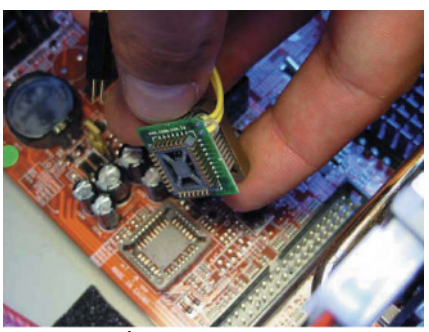

Рисунок 4. Установка «кроватки» с двойным BIOS — снизу оригинальная микросхема, сверху — экспериментальная

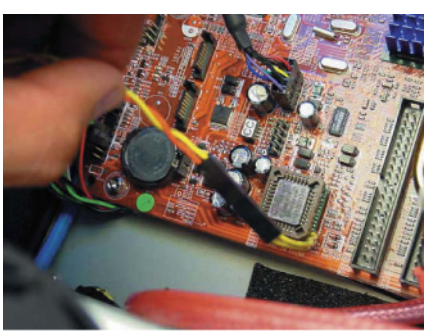

Рисунок 5. Двойной BIOS в собранном состоянии

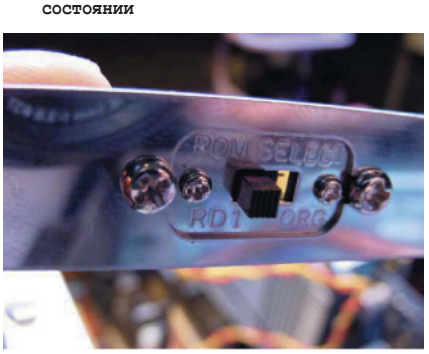

Рисунок 6. Переключатель, отвечающий за выбор между оригинальным (ORG) и экспериментальным (RD1) BIOS

мы, выпускаемые независимыми поставщиками.

Для «горячей» замены BIOS (т.е. выдергивания микросхемы с работающей платы) русские умельцы аккуратно обвязывают микросхему нитками, а затем осторожно тянут вверх (можно, конечно, просто подковырнуть отверткой, но при этом легко что-то закоротить), а вот иностранцы после эпидемии «чиха» придумали специальные приспособления – chip extractor (съемщик чипов) и BIOS savior (BIOS-спаситель). По сути дела, это одно и то же приспособление, только торговые марки разные. Приобрести их можно в радиомагазинах или заказать по Интернету (см. **рис. 1-6**).

Еще нам потребуется документация на чипсет материнской платы. Компании Intel и AMD бесплатно выкладывают все, что нужно на сайт. Другие производители (VIA, SiS) держат документацию под спудом и отдают только за деньги плюс подписку о неразглашении. В частности, на дисках, рассылаемых компанией AMD, встречается много интересной документации со штампом «confidential», пролистывая которую, ощущаешь волнующее чувство причастности к тайне.

Комплект утилит для прошивки BIOS можно найти на сайте разработчика конкретного BIOS или производителя материнской платы. Некоторые производители (например, ASUS) вносят в BIOS большое количество изменений, в результате чего «родные» утилиты от Award перестают с ними работать и приходится использовать инструментарий, поставляемый вместе с материнской платой. Обычно там содержится:

- awdflsh.exe – «прожигатель»;
- modbin – простой редактор BIOS;
- cbrom – просматривает содержимое BIOS и добавляет новые модули в прошивку.

Все эти утилиты можно найти на сайте www.rom.by. Там же находится замечательный «патчер» BIOS – BP.exe (сокращение от «BIOS Patcher»), исправляющий ошибки в известных ему прошивках и разблокирующий многие заблокированные возможности. Нашим основным инструментом будет интерактивный редактор BIOS Award BIOS Editor, который можно бесплатно скачать с http://awdbedit.sourceforge.net.

Как мы будем действовать

Модификация BIOS – очень рискованное занятие. Малейшая ошибка – и система отказывается загружаться, выдавая унылый черный экран. Большинство современных материнских плат снабжено защитой от неудачных прошивок, однако обычно она срабатывает лишь тогда, когда BIOS действительно поврежден (например, не соответствует контрольная сумма).

Вот для этих целей нам и требуется второй BIOS! Запускаем материнскую плату, считываем содержимое прошивки соответствующей утилитой (или скачиваем обновленную версию с сайта производителя), модифицируем ее по своему вкусу, затем, не выключая компьютера, аккуратно вынимаем оригинальный чип, откладывая его в сторону, и вставляем чип, над которым мы будем экспериментировать. Остается запустить AWDFLASH.EXE и зашить модифицированную прошивку в BIOS. Теперь, случись вдруг что, мы всегда сможем вернуть оригинальный чип на место, исправить ошибку в экспериментальной прошивке и повторить всю процедуру вновь. Другими словами, мы будем экспериментировать только над «нашим» чипом, оставляя родной BIOS в неприкосновенности.

Насколько такая процедура безопасна? По правде говоря, опасности нас подстерегают на каждом шагу. Микросхема может выскользнуть из рук и

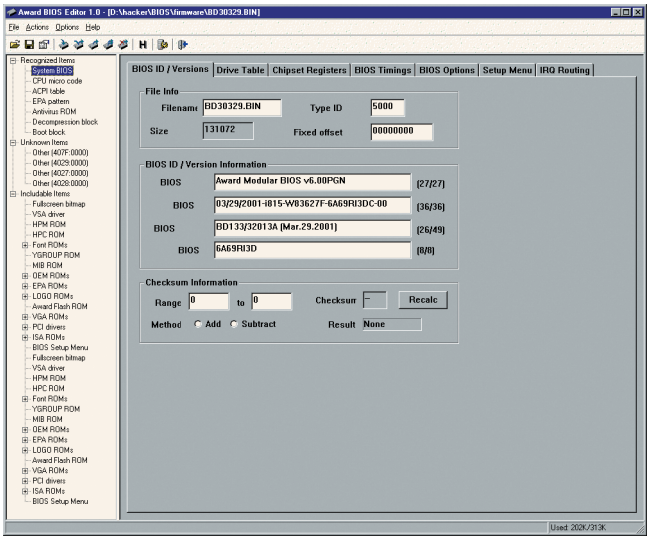

Рисунок 7. Award BIOS editor, готовый к модификации текстовых строк, отображающихся при загрузке системы

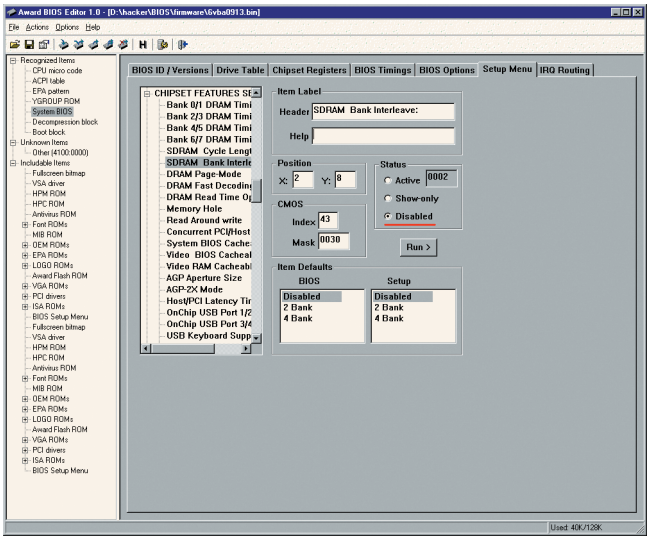

Рисунок 8. Разблокирование заблокированных возможностей в «BIOS Setup» в Award BIOS editor

упасть на плату, малейшая ошибка в прошивке может вывести оборудование из строя (например, переключить стабилизатор на повышенное напряжение, выбрать слишком большую тактовую частоту и т. д.). До приобретения боевого опыта лучше всего экспериментировать над старыми материнскими платами, которые все равно идут в утиль (например, Pentium-155).

Первые эксперименты

Запускаем Award BIOS editor (кстати говоря, он запускается только из-под GUI, а под FAR 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 сохранить текущую прошивку в файл). В левой колонке выбираем пункт «System BIOS» и смотрим, что хорошего тут можно изменить. А изменить тут можно очень многое! Например, имя BIOS, 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 «assembled at military-industrial USA factory», чтобы потом подшучивать над приятелями (см. **рис. 7**).

Точно так же можно заменить все надписи в «BIOS Setup» (они находятся во вкладке «BIOS Options») и отредактировать значения по умолчанию (те самые, что загружаются по команде «load default BIOS configuration») под свой вкус. Наибольший интерес представляют пункты, помеченные как «Disabled». Это и есть опции, заблокированные производителем! Простым переводом радиокнопки в состояние «Active» мы разблокируем их! Разумеется, никакой гарантии, что система после этого заработает, 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. Нестабильно работающая материнская плата способна разрушить содержимое жесткого диска еще в процессе загрузки Windows, поэтому экспериментировать на своем рабочем винчестере недопустимо! Используйте запасной жесткий диск, на котором нет ничего ценного. Запустите несколько тестирующих программ и дайте им поработать несколько суток. Если за это время не произойдет ни перезагрузок, ни зависаний, можно переходить на основной жесткий диск, на всякий случай, предварительно зарезервировав его содержимое (см. **рис. 8**).

А хотите изменить логотип, высвечивающийся в северо-восточном углу экрана? Это совсем несложно сделать. Старые BIOS хранили картинку в секции «LOGO» в нестандартном формате, условно называемом logo-форматом. С ним была связана куча ограничений, и требовался специальный конвертор, иногда прилагаемый к ма-

Как прожигают BIOS

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

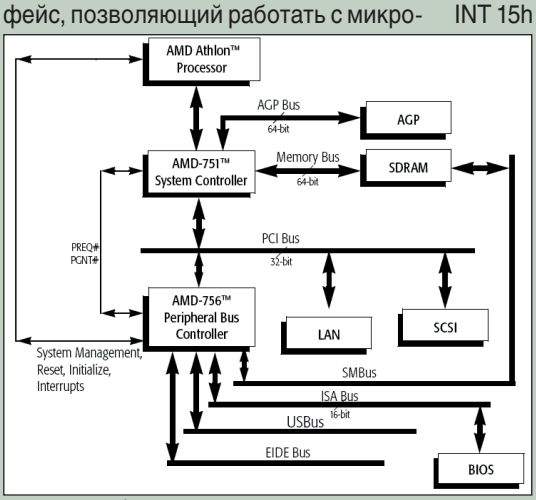

Рисунок 9. Микросхема FLASH-памяти, подключенная к южному мосту

Конструктивно FLASH-микросхема подключена к южному мосту чипсета, поэтому описание интерфейса взаимодействия с BIOS, следует искать именно в документации на южный мост. Как вариант, можно воспользоваться готовым программатором, с которым поставляется все необходимое программное обеспечение.

теринской плате, но чаще его приходилось писать самостоятельно.

Сейчас же секция «LOGO» в большинстве случаев пуста, а картинка хранится в секции «EPA pattern» в стандартном BMP-формате. Ограничений на размер и глубину цветности нет никаких, однако не все BIOS поддерживают слишком большие и цветастые картинки. Что произойдет, если подсунуть BIOS картинку, которую он не в состоянии обрабатывать? Ничего страшного! Система либо откажется выводить ее на экран или выведет с искажениями. Чтобы не попасть впросак, рекомендуется отталкиваться от уже существующей картинки: извлекаем оригинальный логотип в файл (в Award BIOS Editor за это отвечает команда «Export as Windows BMP»), загружаем его в Paint и правим в свое удовольствие без изменения глубины цветности и размеров. Один из примеров такой работы приведен ниже.

При желании можно зашить в BIOS полноэкранный логотип, высвечиваемый при загрузке. Этим занимается одноименная утилита от Award, входящая в штатный комплект поставки многих материнских плат ASUS. Однако в некоторых BIOS задержка вывода полноэкранного логотипа столь мала, что ряд CRT-мониторов просто не успевают прогреться за это время! Но ведь не переходить же ради этого на LCD-монитор? Разумеется, нет! Достаточно найти величину задержки в настройках BIOS и увеличить ее! А для этого нам вновь пригодится Award BIOS editor (см. **рис. 11**).

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 10. Страничка из документации на чипсет, описывающая конфигурационные регистры

А вот еще один трюк. Запустив уже упомянутую утилиту BP.EXE с ключом /c, мы сможем вручную задать имя процессора, высвечивающееся при загрузке, и его тактовую частоту. Реальная тактовая частота отображаться уже не будет. Почему бы не написать «AMD Pentium-V 666 GHz beta» и не похвастаться перед друзьями?

Да много чего можно придумать! В умелых руках BP.EXE и Award BIOS editor творят настоящие 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 (см. **рис. 12**).

Редактирование BIOS

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

Настройка PCI-регистров

Конфигурирование чипсета осуществляется специальными регистрами, доступными через шину PCI. При загрузке системы BIOS настраивает процессор, контроллер системной шины, контроллер оперативной памяти и всю прочую периферию в соответствии с настройками, выбранными в «BIOS Setup». Однако практически ни один BIOS не дает доступа ко всем настройкам чипсета 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 должен быть раздел «PCI Configuration Registers» или что-то в этом роде. Для каждого из регистров будет указано устройство (device), к которому он «подключен», номер функции (function) и номер самого регистра, также 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 указано в BIOS Setup. Взять хотя бы величину tPR (time to precharge), определяющую время закрытия DRAM-страницы, в процессе которого происходят возврат данных в банк памяти и его перезарядка. По умолчанию BIOS ставит 3 такта и не дает его изме-

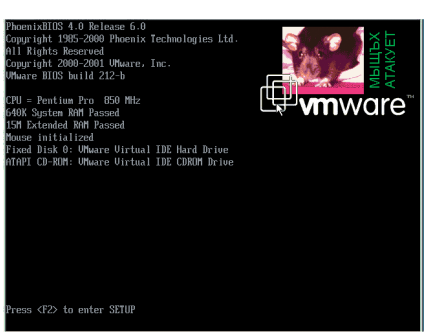

Рисунок 11. Изменение стандартного логотипа, выводимого при загрузке на экран

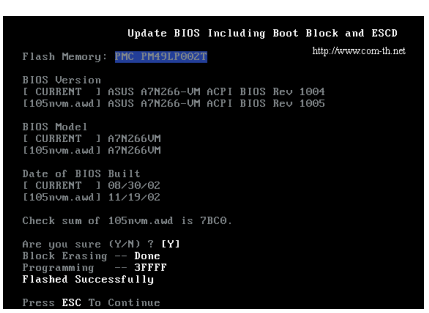

Рисунок 12. Прожигание BIOS специализированной утилитой от ASUS

нять. Чтобы сократить tPR до 1 такта, необходимо модифицировать 8 и 7 биты регистра Dev 0:F0:0x54, присвоив им значение 2 («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 биты установлены в единицу, остальные помечены знаком «X», указывающим BIOS, что данный бит необходимо оставить без изменений (см. **рис. 10**).

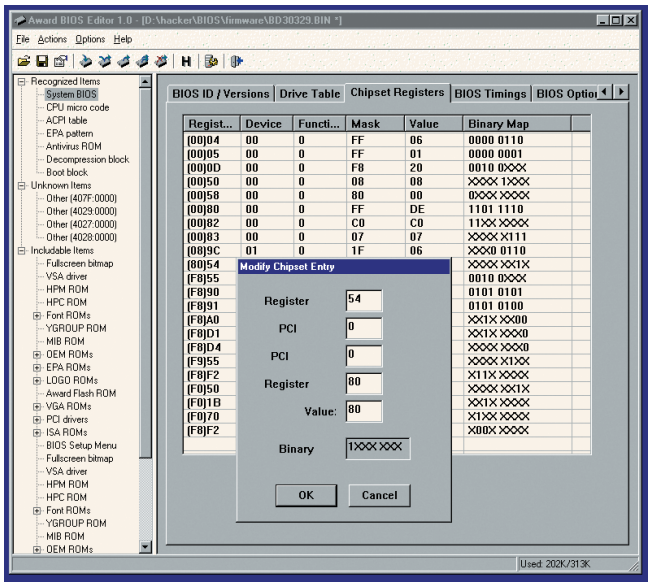

Рисунок 13. Разгон системы при помощи редактирования конфигурационных регистров

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, находим регистр с номером 0x54 и, кликнув правой клавишей мыши, выбираем пункт «modify». В появившемся 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 (см. **рис. 13**).

Залив обновленную прошивку в BIOS и установив качественные модули памяти, мы с удовлетворением замечаем, что быстродействие системы ощутимо возросло, особенно на операциях хаотичного доступа к памяти, когда закрытие DRAM-страниц происходит чуть ли не на каждом шагу.

Аналогичным образом можно редактировать и остальные регистры, отсутствующие в BIOS Setup, однако наши возможности будут довольно ограничены.

Заключение

Кроме Award BIOS editor существуют и другие программы для редактирования BIOS или расширения его возможностей. Они перечислены во врезке.

В рамках одной-единственной статьи просто невозможно охватить все подробности этого увлекательного процесса целиком, поэтому не воспринимайте ее как законченный путеводитель. Скорее это пригласительный билет в удивительный мир, скрытый в недрах небольшой микросхемы. И пускай кто-то скажет, что редактирование BIOS носит скорее познавательный, чем практический характер (устанавливать «разблокированный» BIOS в ответственный сервер я бы не рискнул)! Но должны же у администратора быть хоть какие-то развлечения, тем более что экспериментировать со списанными материнскими платами никто не запрещает!

DUAL-BIOS своими руками

Каждый радиолюбитель, умеющий держать паяльник в руках, может доработать материнскую плату, установив на нее сразу две микросхемы FLASH–памяти. Тогда между ними можно будет переключаться без труднодоступного и притом весьма дорогостоящего chip-extractor. Как видно из **рис. 14,** ничего сложного в DUAL-BIOS нет.

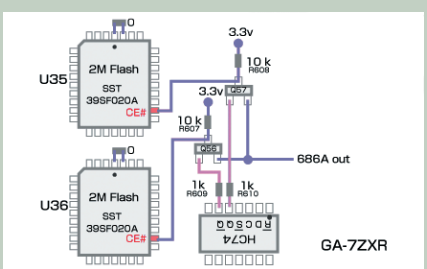

Рисунок 14. Принципиальная схема DUAL-BIOS

Интересные ссылки:

1. http://www.biosmods.com (на англ.)
2. Статьи по прошивке и их доработке (на русс.): http://www.rom.by.
3. FAQ по BIOS (на рус.): http://www.ixbt.com/mainboard/faq/biosfaq.shtml.
4. Сайт хакера, исследовавшего кучу BIOS вдоль и поперек (на англ.): http://www.geocities.com/mamanzip.
5. Статья о модификации BIOS (на англ.): http://www.ryston.cz/petr/bios/ga586hx_mod.html.
6. Статья известнейшего хакера по внедрению своего кода в BIOS (на англ.):http://www.codebreakers-journal.com/include/getdoc.php?id=83&article=38&mode=pdf.
7. Новые идеи по внедрению своего кода в BIOS (на англ.): http://www.codebreakers-journal.com/include/getdoc.php?id=127&article=58&mode=pdf.
8. Исходные тексты пары устаревших прошивок (на ассемблере): http://miscellaneous.newmail.ru.
9. Описание формата BIOS для его ручной распаковки (на рус.): http://www.winsov.ru/bios002.php.
10. Статья по редактированию регистров чипсета (на рус.): http://www.tweakfactor.com/articles/tweaks/amd762/1.html.
11. Разгон системы путем редактирования регистров чипсета: http://www.overclockers.com/tips105/index.asp.
12. Утилита для модификации регистров чипсета: http://www.h-oda.com.
13. Редактор Award BIOS: http://awdbedit.sourceforge.net.
14. Утилита для автоматизированного внедрения своего кода в BIOS: http://webzoom.freewebs.com/tmod/Awdhack.zip.