легенды и мифы прошивки BIOS

крис касперски ака мыщъх

пожалуй, ни один из компонентов ПК не окружен таким количеством слухов и домыслов, как BIOS. между тем, приписываемое ему мистическое влияние на производительность и стабильность системы сильно преувеличено и гоняться за новыми прошивками, право же, не стоит. эта статья рассказывает когда и как следует обновлять BIOS и какую выгоду из этого можно извлечь…

введение или что есть что

BIOS (***B**asic **I**nput/**O**utput **S**ystem – Базовая Система Ввода/Вывода*) – это довольно сложный аппаратно-программный комплекс по обслуживанию компонентов материнской платы и основных периферийных устройств (как-то: жесткие диски, CD/DVD приводы, модемы и т. д.). Архитектурно BIOS представляет собой микросхему памяти, подключенную к южному мосту чипсета (см. рис 3) и хранящую все микропрограммы и некоторые конфигурационные настройки. Другая часть настроек содержится в микросхеме CMOS, питаемой аккумулятором.

Микропрограммы хранятся в упакованном виде (у Award это последовательность LHA-архивов, разделенных контрольными суммами). В конце идет неупакованный BOOTBLOCK, получающий управление при старте системы и автоматически распаковывающий основной код BIOS в оперативную память. Это усложняет дизассемблирование прошивок, и любителям похакерствовать приходится много работать руками, а еще больше – головой. Впрочем, мы отвлеклись. Вернемся к нашим баранам.

Можно выделить следующие типы микропрограмм (названия условны и могут не соответствовать данным):

- **BOOTBLOCK** – загрузчик BIOS'a, ответственный за первичную инициализацию чипсета и распаковку основной части BIOS'a в память, также проверяющий ее контрольную сумму и запускающий программу аварийного восстановления или переходящий на резервный BIOS (подробнее см. "BIOS которые могут постоять за себя");
- **BIOS.ROM** – основной код BIOS'a, осуществляющий инициализацию и тестирование оборудования (идентификация модели процесса и его настройка, считывание типа/количества DIMM'ов и конфигурирование контроллера памяти, инициализация всех прочих системных устройства – контроллера прерываний, DMA и т.д., он же сканирует память в поиске сигнатур всех остальных BIOS'ов, как то – BIOS'a видео-карты, BIOS'ов SCSI-устройств, и осуществляет их инициализацию). Определяет загрузочный привод и считывает с него загрузочный сектор. Содержит в себе драйвера нижнего уровня, обеспечивающие взаимодействие с основными устройствами ввода/вывода, и программу интерактивной конфигурации более известную в народе под именем BIOS Setup;
- **xxxEXT.ROM** – различные расширения основной части BIOS'a, в частности выводящие таблички с конфигурацией оборудования или показания датчиков мониторинга;
- **CPUCODE.BIN** – обновленный набор микропрограмм для процессора, исправляющий ошибки производителя;
- **ACPI.BIN** – низкоуровневые компоненты ACPI (расширенного управления питанием, отвечающего за усыпление/пробуждение устройств), вызываемые операционной системой;
- **PnP.BIN** – низкоуровневые компоненты PnP-менеджера, распределяющие системные ресурсы между устройствами и предоставляющие операционной системе сведения об аппаратной конфигурации, а так же уведомляющие ее о событиях связанных с удалением/добавлением новых устройств;
- **CALL-BACK** – прочие микропрограммы, вызываемые операционной системой по мере необходимости;

Конфигурационные настройки, в свою очередь, делятся на следующие типы (названия общеприняты):

- **LOGO** – цветастая картинка, скрывающая пугающий черный экран BIOS;

- **ESCD** – ***E**xtended **S**ystem **C**onfiguration **D**ata:* блок данных о PnP устройствах;
- **DMI** – ***D**esktop **M**anagement **I**nterface:* блок данных об аппаратных средствах системы;

При обновлении прошивки, чаще всего перезаписывается лишь **MAIN-BLOCK**, включающий в себя BIOS.ROM, xxxEXT.ROM и CPUCODE.BIN, ACPI.BIN, PnP.BIN и CALL-BACK модули, или даже небольшая его часть (например, только ACPI.BIN как наиболее глючный из всех).

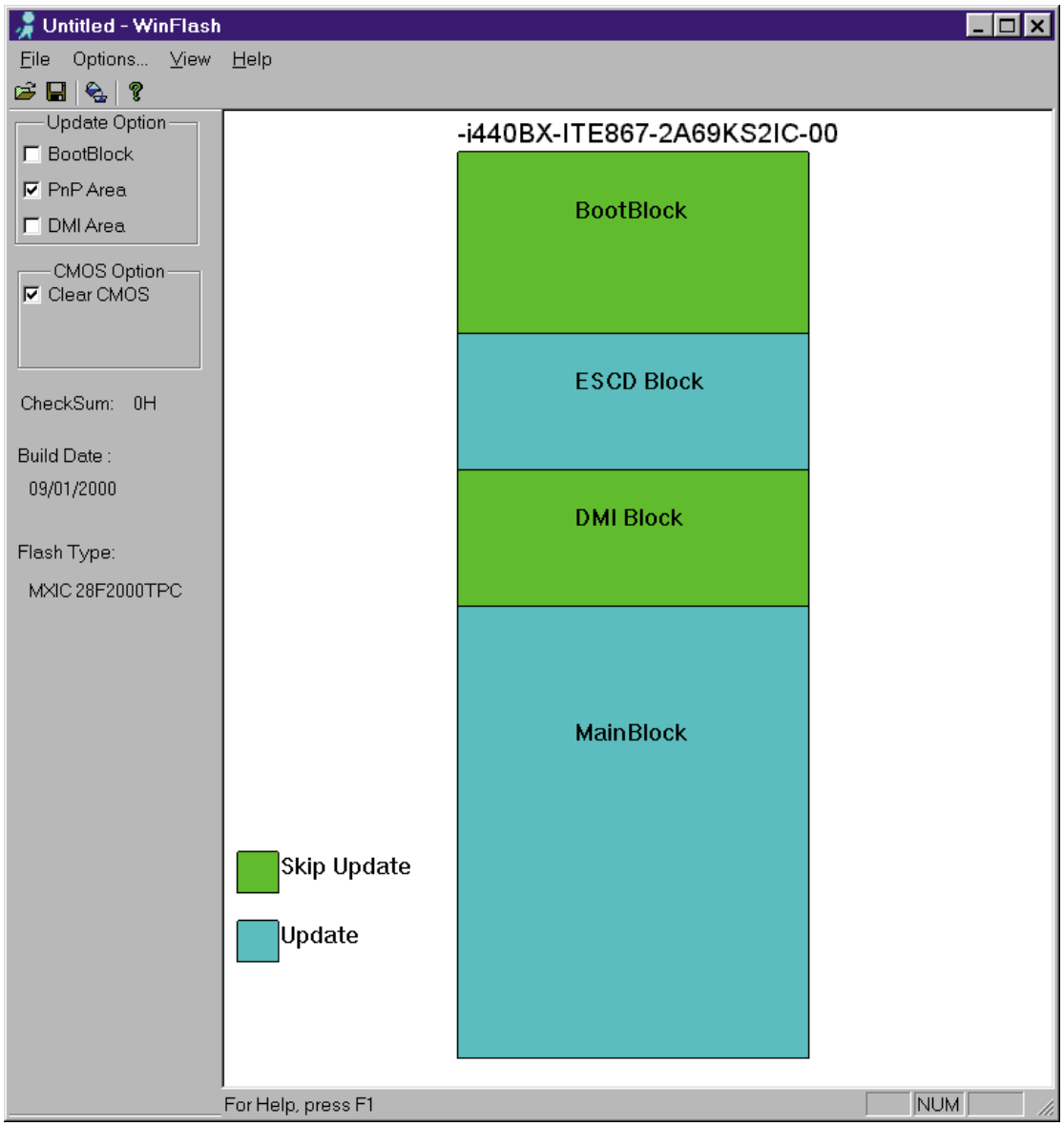

Рисунок 1 внешний вид программы Award Win FLASH, позволяющий перешивать BIOS не выходя из Windows

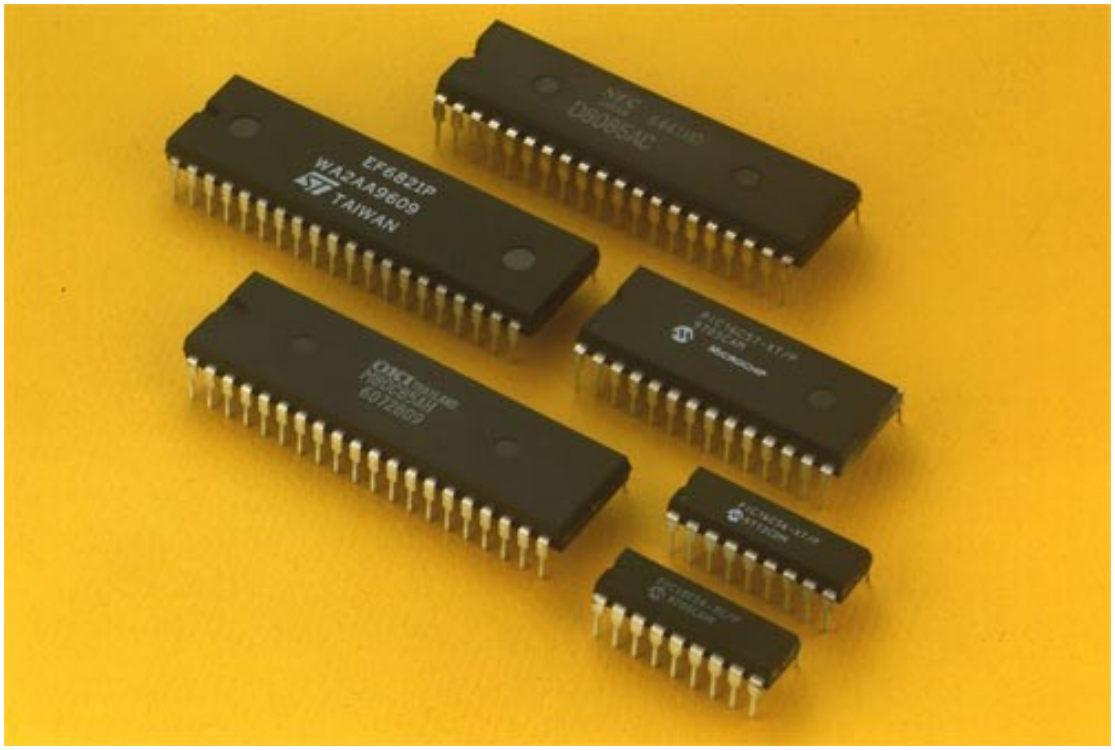

Рисунок 2 BIOS'ы бывают разные…

Нормальные операционные системы (такие, как Windows XP) не используют BIOS в операциях обмена и весь ввод/вывод гонят напрямую через порты и DMA. BIOS лишь конфигурирует устройства, задавая их начальные параметры и режимы работы, но операционная система свободно может переконфигурировать все по-своему (тот факт, что тип обмена с накопителем выставлен в BIOS'е как тормозной PIO не помешает драйверу использовать Ultra-DMA и, соответственно, наоборот). Правда, некоторые устройства настраиваются лишь единожды и динамического конфигурирования не поддерживают. В особенности это касается шинных контроллеров и контроллеров памяти, однако, таких устройств с каждым днем остается все меньше и меньше.

Таким образом, ***непосредственного влияния на производительность системы BIOS не оказывает***. Windows NT 4.x вообще не отображает код BIOS'а на свое адресное пространство, Windows 2000 и XP отображают, но лишь потому, что современные BIOS'ы содержат низкоуровневые компоненты PnP- и ACPI-менеджеров – неиссякаемый источник головной боли для разработчиков драйверов и первородный грех многих глюков и критических ошибок.

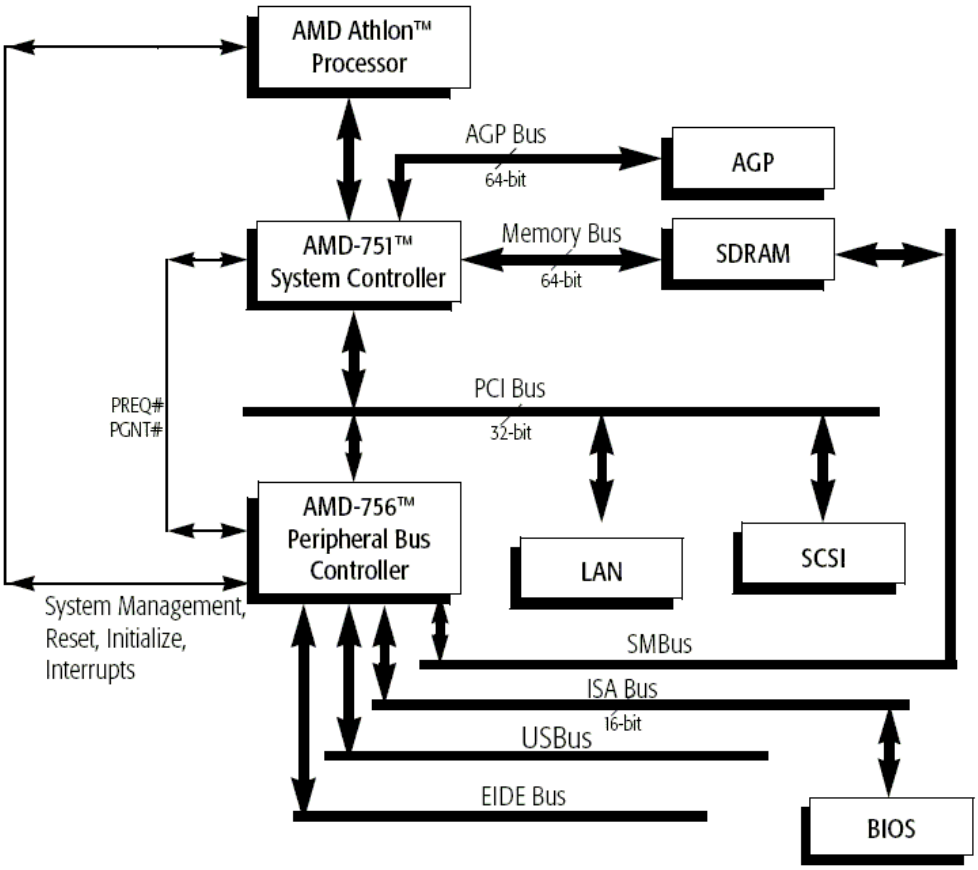

Рисунок 3 конструктивно BIOS соединяется с южным мостом чипсета через ISA-шину или внутреннюю шину специального назначения

что в обновлении твоем

Правила этики обязывают прилагать к каждой версии прошивки сопроводительное описание, объясняющие чем она отличается от остальных, чтобы пользователь мог осмысленно решать – нужна она ему или нет. Пример одного из таких описаний приведен ниже:

8kt31a19.exe 2001-10-19 248.7 kb N/A

Fixed HCT ACPI test failures under WIN2K. // исправлен отказ HCT ACPI теста под W2K
Fixed system hang when installing a SoundBlaster and Live Ware. // исправлен повис системы при установке SB и LW
Fixed WINXP installation failure with Nvidia Geforce 2MX AGP Card. // исправлен отказ установки XP на GeforceARG2MX
Fixed abnormal FAN signal hanging BIOS // исправлена ненормальная обработка FAN-сигналов
Fixed ACPI errors in event viewer under WINXP // исправлена ACPI-ошибка в Event View'epe XP
Added new BIOS feature to differentiate between Athlon XP or Athlon MP // добавлены новые фичи для различия XP от MP

Разумеется, сопроводительный список может быть и не полным (прошивка исправляет проблемы не перечисленные в списке), или же вовсе отсутствовать (чем, в частности, грешит ASUS). Спрашиваете, какие категории проблем способно решить обновление BIOS'a? Таких моментов всего три:

- поддержка новых устройств (процессоров, модулей оперативной памяти, накопителей);
- разблокирование ранее недоступных режимов работы, тактовых частот и таймингов;
- устранение конфликтов программно-аппаратного обеспечения;

Рассмотрим каждый из этих пунктов поподробнее.

поддержка новых устройств

Устройств, действительно нуждающихся в обновленной версии BIOS, всего два: это **процессор** и **оперативная память**.

Чтобы процессор нормально "завелся" и "раскочегарился", он должен быть соответствующим образом сконфигурирован, что осуществляется как аппаратно (путем подачи на заданные интерфейсные ножки определенных логических сигналов), так и программно (путем записи настроечной информации в служебные регистры). Вместе с процессором конфигурируется и контроллер шины, вживленный в серверный мост чипсета и обеспечивающий взаимодействие процессора с остальным оборудованием. Встретив незнакомый процессор, BIOS может либо вообще отказаться от его запуска, либо не в полной мере реализовать его возможности (например, технологию Hyper-Threading). Если BIOS лояльна к разгону, тактовую частоту ядра и системной шины даже у незнакомых процессоров можно установить вручную, наплевав на то, что BIOS идентифицирует процессор неправильно.

BIOS также отвечает за определение типа установленных модулей памяти и конфигурирования ее контроллера. Помимо емкости, модули памяти характеризуются многими служебными параметрами (например, длиной DRAM-страницы), без учета которых контроллер попросту не запустится или будет работать со сбоями. Поэтому, если вы воткнули в маму заведомо исправный DIMM, а она его "не видит", видит только половину или работает с ним на пониженной тактовой частоте, загляните в юзер гайд (user guide) на предмет выяснения, какой у вас установлен северный мост (Northern Bridge), а затем, обратившись к производителю чипсета, выясните: поддерживает ли контроллер памяти такие DIMM'ы или нет. Если поддерживает – попробуйте обновить прошивку, в противном случае меняйте всю мать целиком или подберите другой модуль памяти.

Корректная поддержка накопителей не столь критична. И хотя древние BIOS не поддерживают жесткие диски большого объема, это никак не сказывается на работе Windows (главное, чтобы файлы первичной загрузки располагались в "видимой" области, затем в игру вступят драйвера и диск заработает на полную как миленький, ну а если не заработает, тогда вам не прошивку обновлять надо, а скачивать свежий Service Pack).

Никогда не следует забывать, что ***BIOS это всего лишь программа и после обновления прошивки новых контроллеров на материнской плате не вырастет и ее аппаратные возможности останутся прежними со всеми свойственными им ограничениями***. Так, если интегрированный контроллер не поддерживает 48-битного LBA, отсекая старшие разряды, то работа с дисками большого объема невозможна. Теоретически свежая версия прошивки может "увидеть" весь винт целиком, но при попытке записи в сектор с отсеченным старшим разрядом, произойдет обращение к младшему сектору диска и… прости - прощай файловая система!

Перечень поддерживаемых устройств жестко ограничен чипсетом с одной стороны, и конструктивными особенностями его воплощения в конкретной материнской плате с другой. Если чипсет не поддерживает таких-то процессоров, модулей памяти или накопителей, то никакая прошивка вам не поможет. Так что читайте доки (на чипсеты) они рулез! А вот руководство на материнскую плату о многих аппаратно реализованных возможностях может и умалчивать, оставляя это как задел на будущее. Кстати, о заделах…

новые режимы работы

Сравнивая характеристики чипсетов с характеристиками матерей, несущих их на своем борту, порой не можешь удержаться от мата – сколь малая часть возможностей поддерживается BIOS'ом. Правда, иногда приходится сталкиваться и с обратной ситуацией, когда BIOS поддерживает недокументированные "запредельные" режимы чипсета.

Причины? Да самые разные. Допустим, производитель материнской платы, будучи не совсем уверенным в безглючности своего детища, заблокировал до конца не протестированные режимы или же во избежании конкуренции со своими же "топовыми" железками, намеренно зарезал производительность дешевых моделей, а затем, по мере наступления научно-технического прогресса, стал открывать некоторые из их возможностей, выкладывая свежие прошивки. Чтобы не утруждать себя постоянными обновлениями BIOS'a советую выбирать материнскую плату впору чипсету. То есть, характеристики чипсета должны совпадать с характеристиками родного BIOS'a. Должна ли BIOS поддерживать разгон или нет – решать вам. Во всяком случае, запас карман не тянет, а качественно новые возможностями на программном уровне поддержать невозможно. Взять хотя бы тот же Hyper-Threading, для включения которого требуется всего лишь обновить BIOS, и он как бы будет работать. "Как бы" потому что у

многоЦПшности своя специфика планирования запросов к памяти, требующая аппаратной оптимизации шинного контролера и контроллера памяти, в противном случае прирост производительности будет просто смехотворным, если еще не упадет ниже плинтуса.

Другое дело, что свежие прошивки частенько содержат различные полезные "вкусности" вроде усовершенствованной системы температурного мониторинга, автоматически снижающей тактовую частоту памяти/процессора при перегреве или уменьшающей скорость вращения вентиляторов (а вместе с ним и шум!), когда они и без того холодны. Но и тут не все гладко. Температурные датчики, установленные в дешевых материнских платах, катастрофически ненадежны и их показания "плавают" в довольно широких пределах, зачастую выходящих за предельно допустимые температурные режимы работы данного процессора. Пользователи начинают волноваться и дергать производителя, а тот в свою очередь переписывает BIOS так, чтобы он выдавал более "политкорректные" показания. Поэтому, если после прошивки, температура процессора понизилась: либо BIOS настроила процессор на более щадящий (но и менее производительный) режим работы, либо пошла на умышленное занижение показаний. Отдельный случай составляют ошибки идентификации процессора и неправильный подбор напряжения питания, исправляемый свежей прошивкой, но это уже из области "маразмы крепчают" и "шлите ширпотреб бочками".

конфликты

Столкнувшись с конфликтом оборудования или голубыми экранами смерти, не торопитесь сваливать вину на BIOS. В подавляющем большинстве случаев она ни в чем не виновата. Основной источник ошибок – программное обеспечение сторонних производителей, наплевательски относящихся к рекомендациям Microsoft и потому не вполне Windows-совместимых. Затем (по статистике) идут дефекты оборудования (особенно разогнанного), кривая настройка операционной системы и/или BIOS Setup. Попробовать перешить BIOS, конечно, можно, но скорее всего это ничего не даст.

Как выглядят конфликты BIOS? Windows либо вовсе не находит конфликтующего устройства, либо неверно его идентифицирует (например, обзывает звуковую карту джойстиком), либо одно или несколько устройств никак не удается развести по разным IRQ/DMA/IO, а если даже и удается, то они соглашаются работать только по очередности. Это характерный баг PnP-менеджера.

Если же все устройства определяются нормально, но при выходе из "сна" неожиданно исчезают или начинают работать некорректно, то тут либо дефект BIOS, либо само устройство не соответствует спецификации APCI, либо ошибка его драйвера. На всякий случай попробуйте установить свежий Service Pack на ось, скачайте последнюю версию драйвера устройства, проиграйтесь настройками Power Manager'a в BIOS'e и только затем обновляйте прошивку. Ну или как вариант, запретите компьютеру "спать".

Ошибки, допущенные при проектировании BIOS'a, могут стать источником следующих голубых экранов смерти (см. листинг 1). Аналогичные экраны вызываются неполадками железа, сбоями памяти, дефективными секторами, чрезмерным разгоном, некорректно работающими драйверами… Список можно продолжать бесконечно. Записывайте BIOS в виновники только тогда, когда эти BSOD'ы стабильно появляются даже на свежеустановленной системе с заведомо исправным железом (как тестировать железо? да в квейка в дос погоняйте – если не свалится, значит есть шанс, что работает).

Иногда проблему удается решить запретом кэширования BIOS'a (Shadow BIOS или BIOS cacheable в BIOS Setup должен быть в Disable). А теперь обещанный перечень ошибок:

```
Bug Check 0x1E: KMODE_EXCEPTION_NOT_HANDLED
Bug Check 0x0A: IRQL_NOT_LESS_OR_EQUAL
Bug Check 0x2E: DATA_BUS_ERROR
Bug Check 0x7B: INACCESSIBLE_BOOT_DEVICE
Bug Check 0x7F: UNEXPECTED_KERNEL_MODE_TRAP
Bug Check 0x50: PAGE_FAULT_IN_NONPAGED_AREA
Bug Check 0x77: KERNEL_STACK_INPAGE_ERROR
Bug Check 0x7A: KERNEL_DATA_INPAGE_ERROR
Exception Code 0xC0000221: STATUS_IMAGE_CHECKSUM_MISMATCH
```

Листинг 1 перечень голубых экранов смерти и критических ошибок приложений, виновником которых может быть кривой BIOS

Может случиться и так, что Windows вообще откажется устанавливаться на несовместимый BIOS, зависая, перезагружаясь или аварийно завершая процедуру инсталляции. Однако, учитывая, что все, уважающие себя, производители материнских плат, тестируют прошивку на совместимость с популярными операционными системами, маловероятно, чтобы главным виновником была именно BIOS. Скорее уж кривая настройка последнего или конфликт оборудования (как привило, видео-карты).

>>>> врезка когда следует обновлять BIOS

Если ваша система работает стабильно и все устройства опознаются нормально, в обновлении BIOS'a нет никакой необходимости. Если же у вас проблемы, в первую очередь сгоняйте за пивом, а затем не спеша пошартесь по support и knowledge base производителей материнской платы, чипсета, конфликтующего оборудования и программного обеспечения (не забывая в том числе и о фирме Microsoft). Быть может эта проблема уже решена и виновна вовсе не BIOS! Проверьтесь на вирусы, убедитесь в наличии хорошего контакта в нужных местах, сбросьте BIOS Setup в конфигурации по умолчанию. Если неправильно идентифицируется оборудование, не поленитесь заглянуть в справочное руководство – а должно ли оно вообще идентифицироваться? Например, моя материнская плата распознает Athlon 1400/133 как Athlon 1050/100, т. к. даже и не пытается автоматически определять частоту шины, о чем честно признается в тех. паспорте, ручная же установка проходит вполне нормально.

Кратко перечислим проблемы, которые при благоприятном стечении обстоятельств могут быть устранены обновлением прошивки:

- неправильно идентифицируется процессора (частота, тип, напряжение питания);
- неправильно идентифицируется объем/тип оперативной памяти;
- неожиданно низкая производительность процессора/памяти;
- неправильно идентифицируются жесткие диски и CD/DVD накопители;
- сбои в процессе установки операционной системы;
- сбои в работе операционной системы;
- материнская плата не запускается;

>>>> врезка хачим BIOS

Современные чипсеты имеют воистину гигантское количество настроек, даже краткий перечень которых растягивается на сотни страниц убористого текста, но BIOS Setup дает доступ лишь к некоторым из них, а остальные настраивает сам, справедливо полагая, что полной власти над машиной пользователю лучше не давать. Для тонкого настройки чипсета на максимальную производительность, обычно прибегают к модификации кода BIOS или в просторечии к его "хаку". Хакнутые прошивки можно найти на некоторых форумах или выменять на пиво у знакомого кодокопателя. Используя их вы сильно рискуете – хорошо если спалите чипсет, память или процессор, хуже если задымятся сами сигнальные дорожки – *такую* материнскую плату не примет ни один продавец. Тем не менее, риск ради риска – благородное дело, а потому хакерские прошивки рулят и процветают.

Хотите самостоятельно хакнуть свой BIOS? Предупреждаем, это занятие не для ленивых. Потребуется очень много читать по-английски и долго-долго сидеть за отладчиком/дизассемблером, прежде чем хоть что-то прояснится. Для начала вам понадобиться: IDA PRO или любой другой дизассемблер по вкусу, подробная техническая документация на чипсет (не путать с рекламными проспектами!), набор утилит для распаковки/упаковки/подсчета контрольной суммы BIOS'a (обычно можно взять на сайте производителя BIOS'a, ну или на худой конец, распотрошив прошивающую программу, написать все самостоятельно).

Наконец, необходим сам образ BIOS'a который вы собрались хачить. Если два пути его получения: снятие образа уже прошитого BIOS'a и скачивание с сервера производителя свежей прошивки. Оба пути порочны. BOOTBLOCK зачастую распаковывает не весь BIOS, а лишь "нужную" его часть, после чего перемешивает страницы памяти так, что доступ к исходному ROM'у становится невозможен. Кроме того, неясно в каком формате должен быть образ BIOS'a, чтобы его "проглотила" прошивающая программа. Обновляемые прошивки в этом плане выглядят намного более привлекательными, но как уже говорилось, далеко не всякая прошивка включает в себя весь BIOS целиком, поэтому, скачивайте все прошивки какие только есть. Не

обращайте внимание на их размер – он еще ни о чем не говорит (не прошиваемые байты обычно имеют значение FF, некоторые версии прошивок на 99% из этих FF'ов и состоят).

Перед загрузкой прошивки в дизассемблер ее желательно распаковать, использовав соответствующую утилиту, найденную на сайте разработчика BIOS'a. Правда некоторые из них, распаковывают не все микропрограммы и лучше всего распаковывать BIOS руками, дизассемблируя BOOTBLOCK в HIEW'e или ИДЕ. Тоже самое приходится делать, если программа распаковки для вашей версии BIOS'a недоступна.

BOOTBLOCK всегда идет в конце образа, но точка входа в него неизвестна. Мы знаем, что после включения питания (или аппаратного RESET'a) процессор передает управление по адресу FFFFFFF0h, но каким именно способом наш образ отображается на память – заранее неизвестно. Будем исходить из того, что конец образа совпадает с адресом FFFFFFFFh (как чаще всего и бывает), тогда точка входа будет расположена в 10h байте от его конца.

Обычно здесь торчит что-то вроде JMP FAR'a, соответствующего опкоду EAh, "окантованного" осмысленными текстовыми строками (например, датой выпуска BIOS):

```
seg000:7FE0 41 30 30 30 39 30 30 30+aA0009000      db 'A0009000',0
seg000:7FE9 00                                     db      0;
seg000:7FEA 00                                     db      0;
seg000:7FEB 00                                     db      0;
seg000:7FEC 00                                     db      0;
seg000:7FED 00                                     db      0;
seg000:7FEE 00                                     db      0;
seg000:7FEF 00                                     db      0;
seg000:7FF0 ; ──────────────────────────────────────────────────────────────────
seg000:7FF0 EA AA FF 00 F0                         jmp     far ptr 0F000h:0FFAAh
seg000:7FF0 ; ──────────────────────────────────────────────────────────────────
seg000:7FF5 30 35 2F 31 38 2F 30 34+a051804        db '05/18/04',0
seg000:7FFE FC 7D                                  dw offset unk_17DFC
```

Листинг 2 окрестности точки входа в ASUS AMI BIOS

```
seg000:3FE8 36 41 36 4C 4D 50 41 45 a6a6lmpae      db '6A6LMPAE'
seg000:3FF0  ; ─────────────────────────────────────────────────────────────────
seg000:3FF0 EA 5B E0 00 F0   jmp     far ptr 0F000h:0E05Bh
seg000:3FF0   ; ────────────────────────────────────────────────────────────────
seg000:3FF5 2A 4D 52 42 2A   aMrb    db '*MRB*'
```

Листинг 3 окрестности точки входа в EPOX AWARD BIOS

Теперь мы должны преобразовать целевой адрес перехода в действительный адрес. Смотрите, если адрес seg000:7FF0 физически представляет собой F000:FFF0h, то, очевидно, что физический F000:FFAA соответствует нашему seg000:7FAA. Аналогично и в следующем случае: если seg000:3FFF0 – это F000:FFF0, то F000:E05Bh естественным образом транслируется в seg000:3E05Bh. Чтобы не заморачиваться с этими вычислениями, можно просто попросить ИДУ изменить базовый адрес сегмента так, чтобы seg000:70000 соответствовало segXXX:0000.

Если вы встретите переход или вызов процедуры, указывающий на длинную цепочку FF'ов, это значит, что данный участок кода в вашей версии образа отсутствует и не пере прошивается.

Если вы встретите бессмысленный мусор, то либо данный участок кода упакован, либо вы не правильно определили его разрядность. Основной код BIOS 16-разряден, но в нем может присутствовать большое количество 32-разрядных фрагментов, вызываемых операционной системой. Возможно также, что вы начали дизассемблирование с середины инструкции. А как определить позицию дизассемблирования в сплошном байтовом потоке? Хороший результат дает поиск байт E8h, соответствующего началу команды CALL NEAR и EAh, соответствующего JMP FAR, ну и других подобных им. Также, отыщите все текстовые строки и восстановите перекрестные ссылки на них (для этого необходимо поискать смещение строки прямым поиском в памяти, только не забывайте, что младший байт смещения должен располагаться по старшему адресу, т.е. если строка расположена по seg000:ABCD, нужно искать CD AB, подробности в "Образе мышления ИДА" и "Фундаментальных основах хакерства" Криса Касперски, то есть меня).

Правильно дизассемблированный код выглядит приблизительно так:

```
seg000:2D1C    cli
seg000:2D1D    mov     si, offset aMemoryTesting ; "Memory Testing : "
```

```
seg000:2D20     call    sub_1CC44
seg000:2D23     push    0E000h
seg000:2D26     push    offset loc_12D34
seg000:2D29     push    0EC31h
seg000:2D2C     push    offset locret_13470
```

Листинг 4 дизассемблированный фрагмент BIOS'a, строку "Memory Testing" можно заменить например на "MATRIX loading"

По ходу дизассемблирования вы встретите множество обращений к портам ввода/вывода. Чтобы понять их физический смысл обратитесь к техническому описанию чипсета. AMD и INTEL бесплатно распространяют всю сопутствующую документацию. У остальных с этим похуже. На худой конец загляните в знаменитый Interrupt List Ральфа Брауна.

Хачить код лучше всего в HIEW'e, т .к. повторное ассемблирование дизассемблерного листинга ни к чему хорошему не приведет. Хакнутый файл пропустите через "упаковщик" (или упакуйте его вручную, заново рассчитав контрольную сумму), и попробуйте "скормить" прошивальщику BIOS'a. Если все сделано правильно – открывайте пиво и радуйтесь, в противном случае переходите к пункту "BIOS которые могут постоять за себя".

>>>> врезка внутри прошивателя

Скажем сразу, написать универсальный прошивальщик для всех моделей BIOS'ов не под силу никакому одиночке, т. к. методы управления напряжением программирования, способы разрешения записи во FLASH, особенности затенения RAM, алгоритмы запрещения кэширования BIOS у всех чипсетов и BIOS'ов сильно неодинаковые.

Но если уж вам невтерпеж, вы можете использовать следующие источники информации: дизассемблировать фирменную программу-прошиватель и разобраться с ее алгоритмом, при случае свиснув его ключевую часть, а то и весь код целиком. Это самый корректный с технической точки зрения путь, однако, во-первых, программы прошивки может и не быть, а во-вторых, дизассемблирование требует чудовищного количества времени, не говоря уже о соответствующих навыках и уровне подготовки.

Как вариант, загляните в Interrupt List или побродите по Интернету. Если вам повезет, вы найдете всю необходимую информацию. Вот, например, на AMI BIOS'ах за обслуживание прошивки отвечает прерывание INT 16, которое Браун подробно описывает.

Самый правильный, но вместе с нем, наименее романтичный путь – обратиться к описанию чипсета, а точнее его южного моста. Пусть для определенности это будет AMD 756. Открываем руководство на разделе "Flash Memory Support" и читаем: "Support for programmable flash memory is provided by enabling write cycles to the BIOS ROM regions. Bit 0 of the ISA Bus Control register (Function 0 offset 40h) is provided to enable write cycle generation.". /* *Поддержка программируемой flash-памяти осуществляется разрешением циклов записи в BIOS ROM-регион. Бит 0 контроллера ISA шины (функция 0 смещение 40h) обеспечивает генерацию циклов записи*" */. Коротко и ясно. И ничего не надо дизассемблировать. Правда, если вы захотите испортить чей-то BIOS, то скорее всего у вас ничего не получится, т. к. другие чипсеты в этом отношении ведут себя иначе.

>>>> врезка не дайте себе обмануть в другом месте или покупайте только у нас

Часто хак BIOS преследует одну-единственную, но очень коварную цель, а именно – искажение выдаваемой при загрузке информации в стиле Pentium-7, 666.66 GHZ, 1024 Gbytes RAM с целью выдать свою старую клячу за борзого рысака породистых кровей и загнать его подороже.

Поэтому, не доверяйте показаниям BIOS при покупке компьютера с рук! Запустите квейка и посмотрите тянет ли он на заявленные мегагерцы или нет!

техника прошивки

Перешиваемые BIOS'ы первого поколения часто дохли во время обновления (причиной тому могло быть банальное зависание компьютера, отключение питание или некорректная версия BIOS), после чего материнскую плату приходилось либо выбрасывать, либо в срочном порядке искать человека-с-программатором. Но первое – дорого, второе – хлопотно. Вот производители материнских плат и пошли на уступки, оснастив BIOS более или менее

продвинутыми средствами защиты и самовосстановления, о которых рассказывает врезка "BIOS которые могут постоять за себя", так что современные BIOS'ы можно перешивать не боясь. Тем не менее, настоятельно рекомендуется запастись UPS'ом (ну или на худой конец оповестить всех домашних, чтобы не вздумали химичить с электричеством), войти в BIOS Setup и выбрать конфигурацию по умолчанию – как наиболее стабильную и безглючную. Также убедитесь, что у вас отсутствуют аппаратные проблемы – компьютер работает в DOS и не виснет, т. к. если он виснет, то: а) прошивка тут не причем, б) если компьютер зависнет во время прошивки, то вам обоим сильно поплохеет.

Когда все подготовительные операции позади, стащите с официального сайта производителя своей мамаши свежую версию BIOS'a. Причем, если она была выложена не позднее, чем вчера, повремените с обновлением, дав ей выдержаться несколько дней – в противном случае вы рискуете нарваться на грубые ошибки разработчиков, которые со всеми ними периодически случаются. Неофициальных источников и "хакнутых" прошивок в особенности лучше избегать, впрочем, риск не так уж и велик, тем более что запорченный BIOS практически всегда можно восстановить.

Обновление BIOS может быть запрещено как переключателем на материнской плате, так и одноименным пунктом в BIOS Setup. Обратитесь к руководству пользователя и уберите все препятствия со своего пути.

Конкретная техника обновления BIOS'a варьируется от одной программы прошивке к другой и мне остается лишь посоветовать внимательно изучить прилагаемую к ней документацию, не пренебрегая даже мелочами. Практически все прошивающие программы – это консольные приложения, запускаемые из MS-DOS. Даже не пытайтесь запускать их из Windows (если только приложение само об этом не попросит, как например, Win Flash изначально спроектированная для прошивки в среде Windows).

Обычно вместе с программой поставляется и ее инсталлятор, автоматически формирующий установочную дискету (обязательно проверьте, что дискета записалась без сбоев, для этого нажмите кнопку выброса, чтобы Windows заново перечитала ее содержимое, а не брала данные из кэша). Убедитесь, что на дискете достаточно места для записи текущей прошивки (ее должна сохранить прошивающая программа), обычно для это требуется 200 – 500 Кб. Не стоит сохранять текущую прошивку на совершенно чистую дискету – помимо нее там должна находится программа аварийного восстановления, автоматически запускающаяся при загрузке с дискеты.

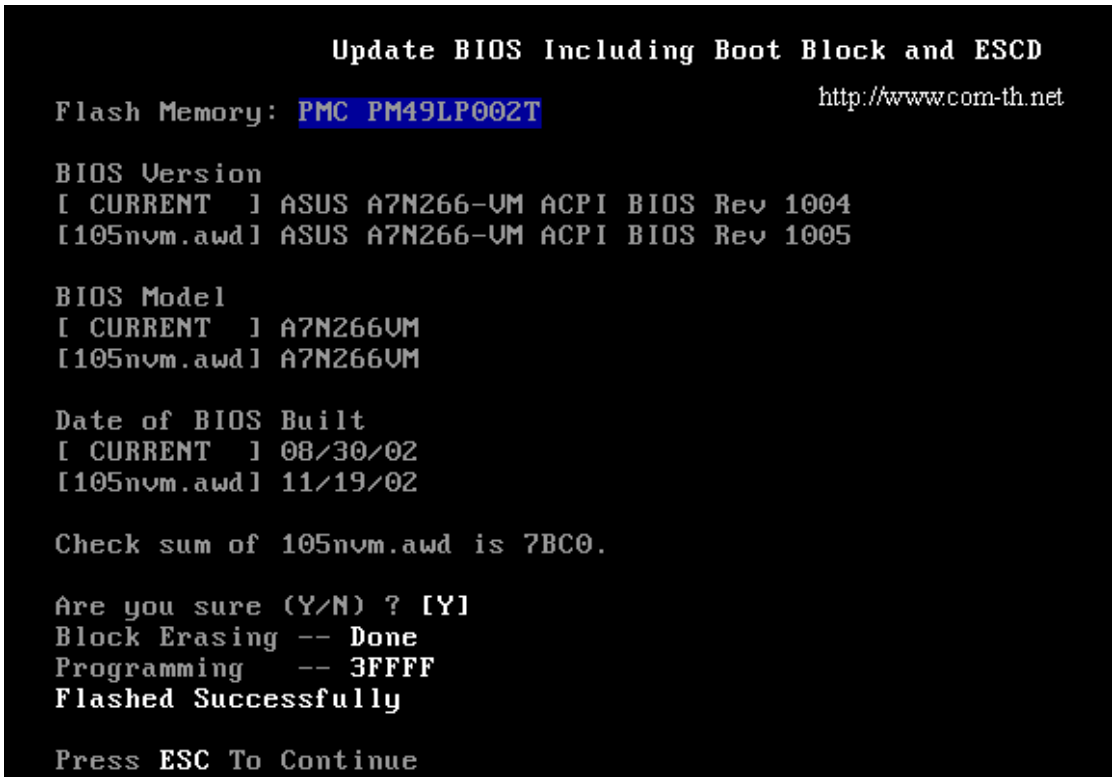

Рисунок 4 интерфейс типичной прошивающей программы

По окончании прошивки сбросьте CMOS (если это не сделала сама прошивающая программа), т. к. новая версия может использовать другой формат хранения конфигурационных данных, несовместимый с предыдущим и вызывающий различные конфликты. После перезагрузки и успешного прохождения POST'a войдите в BIOS Setup и найдите в нем пункт типа "Reset configuration", осуществляющий сброс всех установок, сделанных предыдущей версией BIOS'a. Наконец, после загрузки Windows (если она вообще загрузится), запустите "менеджер устройств" и дайте ему поработать – устройства, не определяющиеся (или конфликтующие) ранее теперь должны определиться. В крайнем случае, переустановите Windows (если обновление прошивки преследовало цель активации Hyper-Threading'a, то переустанавливать систему по любому придется, т. к. однопроцессорное ядро не способно поддерживать несколько процессоров в принципе, а смена ядра на лету – операция не для слабонервных).

BIOS которые могут постоять за себя

Если после обновления BIOS'a материнская плата не подает никаких признаков жизни, то не спешите хвататься за валидол, а поищите на ней перемычку типа "BIOS recovery" (обычно она присутствует на Intel'ых материях).

Вообще же говоря, существует множество технологий защиты BIOS от некорректного обновления. Рассмотрим три наиболее популярные из них: **Die Hard Lite**, **Die Hard I/II** и **Dual BIOS**.

Die Hard Lite BIOS конструктивно представляет собой крошечный регион памяти внутри BIOS'a (Boot Kernel), логически или физически защищенный от записи и содержащий минимально работающий загрузчик, поддерживающий ISA-видео карту (или не поддерживающий ни хрена, если ISA-слотов на матери нет, поддержка PCI слишком громоздка для Boot Kernel'a) и считывающий старую прошивку с дискеты (если вы ее предварительно сохранили перед прошивкой и если дискета еще не успела посыпаться). Короче говоря, это очень примитивная технология, но все же она лучше чем ничего!

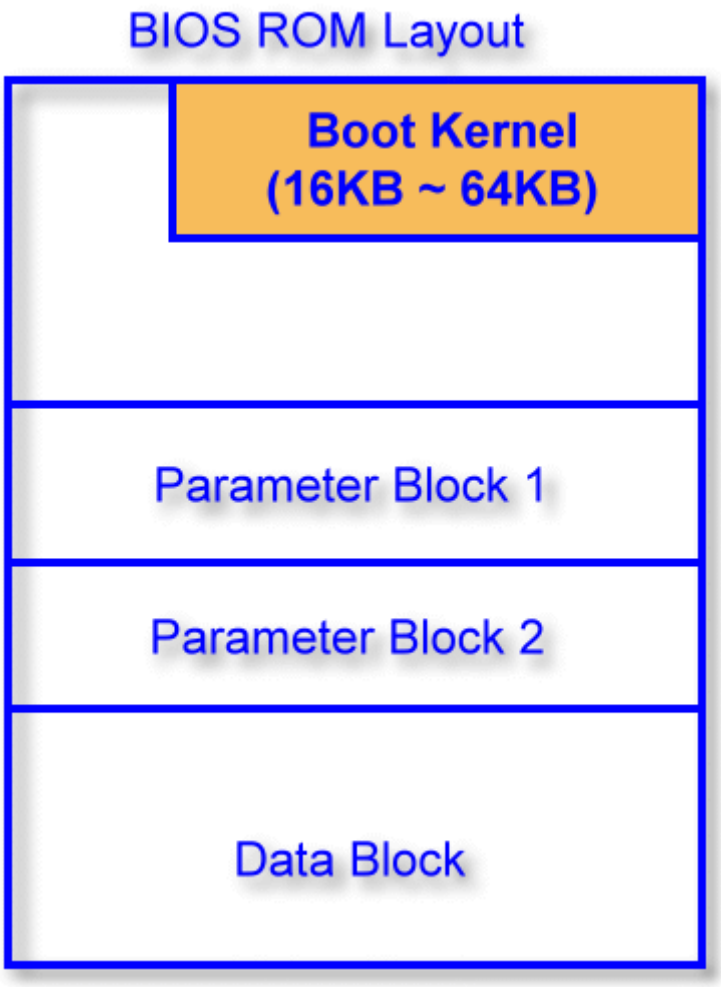

Рисунок 5 Die Hard Lite оставляет нетронутым boot kernel, поддерживающий аварийное восстановление прошивки с дискеты

DieHard BIOS состоит из двух микросхем памяти, каждая из которых несет полноценный код BIOS. Одна микросхема (Normal Flash ROM) поддерживает перезапись, а другая (Rescue ROM) – нет. При возникновении проблем всегда можно переключиться на резервную микросхему, переставив переключатель на материнской плате, и повторить попытку прошивки с учетом предыдущих ошибок. Главный минус этой технологии в том, что откат всегда осуществляется на наиболее древнюю версию BIOS'a, в то время как пользователь предпочел бы предыдущую.

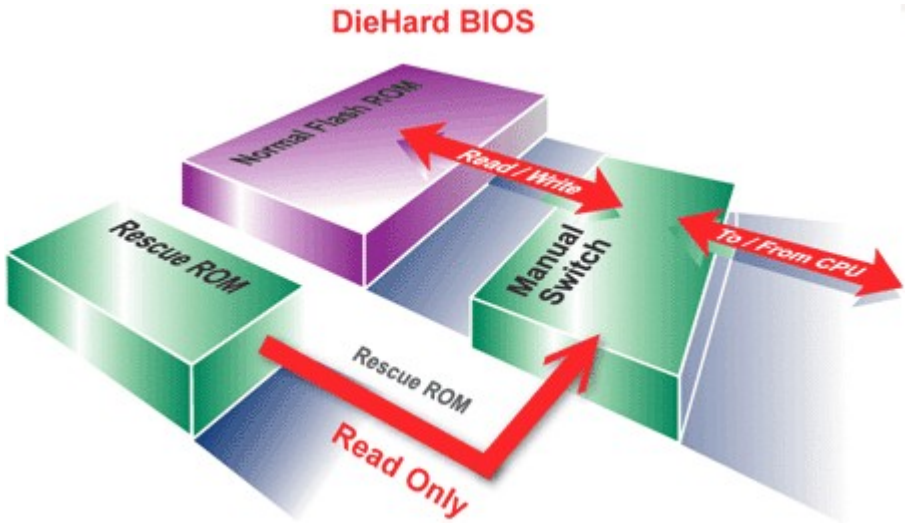

Рисунок 6 Die Hard состоит из двух микросхем памяти, одна перешиваемая, а другая нет

DieHard BIOS II является усовершенствованной версией технологии Die Hard. Теперь обе микросхемы памяти полностью уравнены в правах и каждая из них поддерживает возможность обновления. Если обновление основной BIOS прошло успешно, пользователь может обновить и резервную, тогда самая свежая прошивка всегда будет с ним, что бы не случилось с основной микросхемой BIOS'a.

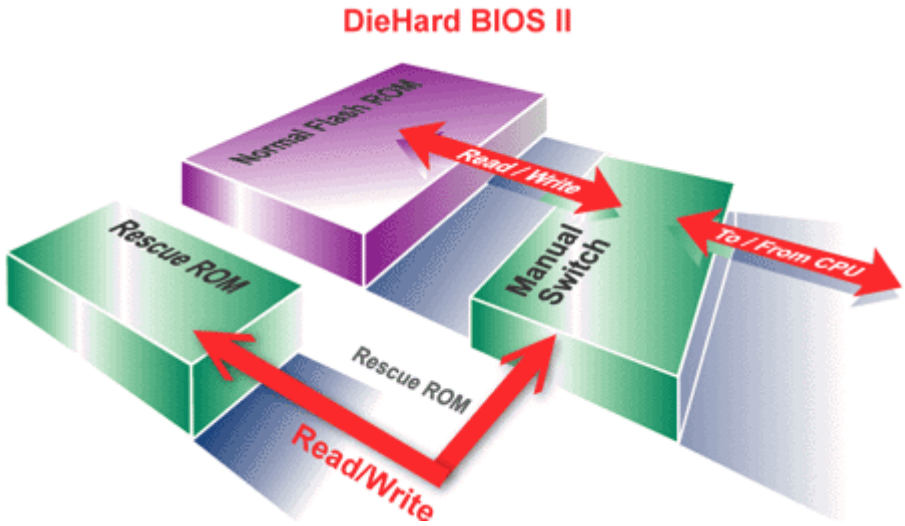

Рисунок 7 Die Hard II состоит из двух равноправных микросхем, каждую из которых можно перешивать

Dual-BIOS представляет собой разновидность Die Hard II, но несколько отличается конструктивными решениями. Здесь так же используются две равноправные микросхемы памяти, но переключение может осуществляться как программно, так и аппаратно, в том числе и автоматически, не требуя вскрытия корпуса (который может быть опечатан) для доступа к перемычкам. Кстати говоря, реализовать эту технологию можно и самостоятельно, используя нижеприведенную схему.

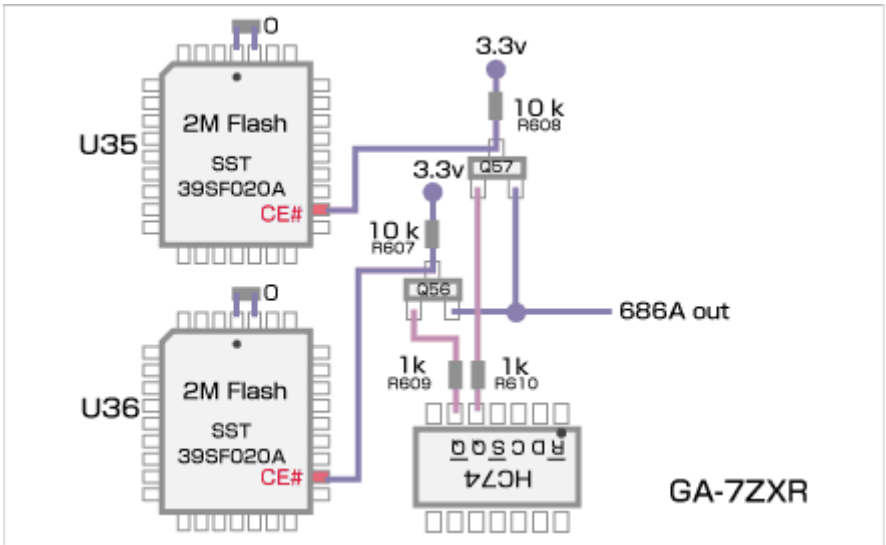

Рисунок 8 Dual-BIOS это разновидность Die Hard II

Рисунок 9 так выглядит "рукотворный" Dual BIOS

BIOS которые не могут постоять за себя

Можно ли реанимировать сдохший BIOS, если мама не подает признаков жизни, а поддержка аварийного восстановления в ней конструктивно не предусмотрена? Существуют по меньшей мере два пути. Лучше и безопаснее всего воспользоваться **программатором**, который можно приобрести практически на любом радиорынке (только убедитесь, что ваш тип FLASH-памяти им поддерживается). К программатору должна прилагаться инструкция, которой необходимо следовать. Если же инструкции нет, а вы не чувствуете себя достаточно подготовленным, обратитесь за консультацией к продавцу. Если он не шланг и не валенок, то поможет.

Если же программатора нет, но есть точно такая же мама, то вытащите из нее BIOS, обвяжите нитками и неплотно воткните ее в свой компьютер, загрузившись с системной дискеты с прошивальщиком. Теперь, не выключая питания, аккуратно вытащите BIOS из панельки, и вставьте свою, стараясь не вызывать коротких замыканий, высекающих искры. Если все пройдет успешно и ничто не сдохнет, вы сможете повторить прошивку BIOS'а заново. Искренне надеюсь, что в этом раз вам повезет.

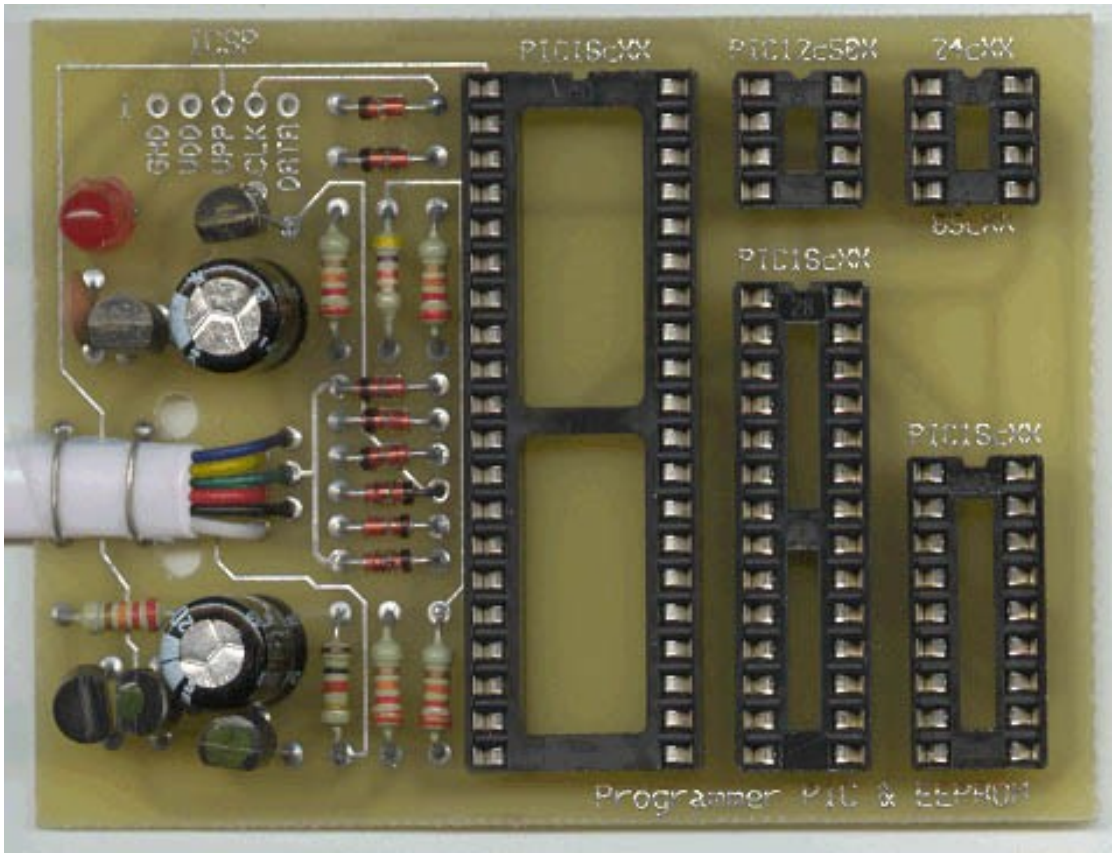

Рисунок 10 внешний вид самодельного программатора

заключение

Несмотря на титанические усилия производителей, обновление BIOS все еще остается достаточно нетривиальной задачей, доступной только квалифицированным пользователям и сопряженной со множеством неочевидных особенностей. Тем не менее, есть надежда, что в скором будущем эта операция будет осуществляться столь же просто, сколько и установка/удаление обычных программ. Впрочем, не будем строит из себя пророков, заглядывающих вперед, ибо будущее непредсказуемо…