ОСНОВЫ КОМПЬЮТЕРНОЙ ТЕХНИКИ

Дисциплина: «Архитектура аппаратных средств»

Преподаватель: Солодухин Андрей Геннадьевич

BIOS

BIOS

- Базовая система ввода-вывода (BIOS) является ключевым элементом системной платы, без которого все ее замечательные компоненты представляют собой лишь набор дорогих «железок».
- BIOS, пользуясь средствами, предоставляемыми чипсетом, управляет всеми компонентами и ресурсами системной платы.
- Из этого следует, что используемая версия BIOS в значительной степени привязана к чипсету, и, кроме того, она должна «знать» особенности применяемых компонентов (процессор, память, интегрированные контроллеры).

BIOS

- Код BIOS хранится в микросхеме энергонезависимой постоянной памяти (ROM BIOS) или флэш-памяти (Flash BIOS).
- С точки зрения регулярной работы тип носителя BIOS принципиального значения не имеет.
- Определить, какой носитель BIOS используется на данной системной плате, можно, сняв наклейку с микросхемы (на ней обычно напечатаны выходные данные BIOS) и прочитав обозначение. На самой микросхеме обычно напечатаны выходные данные BIOS.

BIOS

- Обозначения могут быть такими:
- ♦ 28Fxxx — флэш-память 12 В;
- ♦ 29Cxxx — флэш-память 5 В;
- ♦ 29LVxxx — флэш-память 3 В (редкий вариант);
- ♦ 28Cxxx — EEPROM, близкая по свойствам к флэш-памяти;
- ♦ 27Cxxx — память EPROM, записываемая на программаторе и стираемая ультрафиолетом (если есть стеклянное окошко);
- ♦ 29EE011 — флэш-память 5 В фирмы Winbond;
- ♦ 29C010 — флэш-память 5 В фирмы Atmel.

BIOS

BIOS

- Причин взяться за модернизацию BIOS может быть несколько, некоторые из них перечислены ниже:
- ♦ Некорректная работа в некоторых режимах (например, самопроизвольный переход в энергосберегающий режим, выражающийся в остановках винчестера, гашении экрана или внезапном резком снижении производительности вроде бы нормально функционирующего компьютера).
- По мере выявления ошибок производитель выпускает новые версии BIOS (возможно, и с новыми ошибками).

BIOS

- ♦ Несогласованность драйверов BIOS с требованиями новых версий ОС.
- ♦ Получение новых функциональных возможностей.
- ♦ Повышение производительности.
- ♦ Желание иметь самую свежую версию (для любителей экспериментировать на себе).
- ♦ Желание стереть конфигурационную информацию в NVRAM (включая и ESCD), если для этой цели нет переключателя или параметра в CMOS Setup.
- Утилита перепрограммирования флэш-памяти выполняет это действие автоматически или предлагает его выполнить из своего меню.

BIOS

- Обновление флэш-BIOS предполагает программирование микросхем в целевом устройстве без какой-либо дополнительной аппаратуры, с использованием собственного процессора PC.
- Этот процесс «по-научному» называется In-System Write (ISW).
- Для этого необходима возможность загрузки утилиты программирования и собственно обновленного кода.
- Для этого обычно используют дисковые накопители.

BIOS

- При неудачной модификации BIOS возможность загрузки с диска может оказаться утерянной, и если системная плата не предусматривает режима восстановления (boot recovery), придется задействовать внешний программатор.
- Перед обновлением BIOS оцените свои возможности для отступления.
- Если системная плата и применяемый тип микросхемы не поддерживают режим восстановления, в случае неудачи придётся искать программатор флэш-памяти (если микросхема вынимается).

BIOS

- А если микросхема запаяна в плату, а не установлена в специальный разъём, проблема поиска осложнится тем, что понадобится программатор со специальным адаптером на данной системной плате.
- Этот адаптер должен обеспечивать доступность линий адреса, данных, управления и питания флэш-памяти при неработающем процессоре системной платы.
- Такими адаптерами обладают далеко не все программаторы, поддерживающие требуемый тип флэш-памяти, и их подключение предусматривается далеко не всеми системными платами.

BIOS

- Новую версию BIOS лучше всего получать от изготовителя системной платы.
- Фирмы-разработчики BIOS (например, AMI, Award) новые версии для конечных пользователей не поставляют.
- Свои новые продукты с инструментальными средствами они поставляют разработчику системной платы, производящему окончательную подгонку BIOS под конкретную модель платы, особенности которой он знает лучше всех.

BIOS

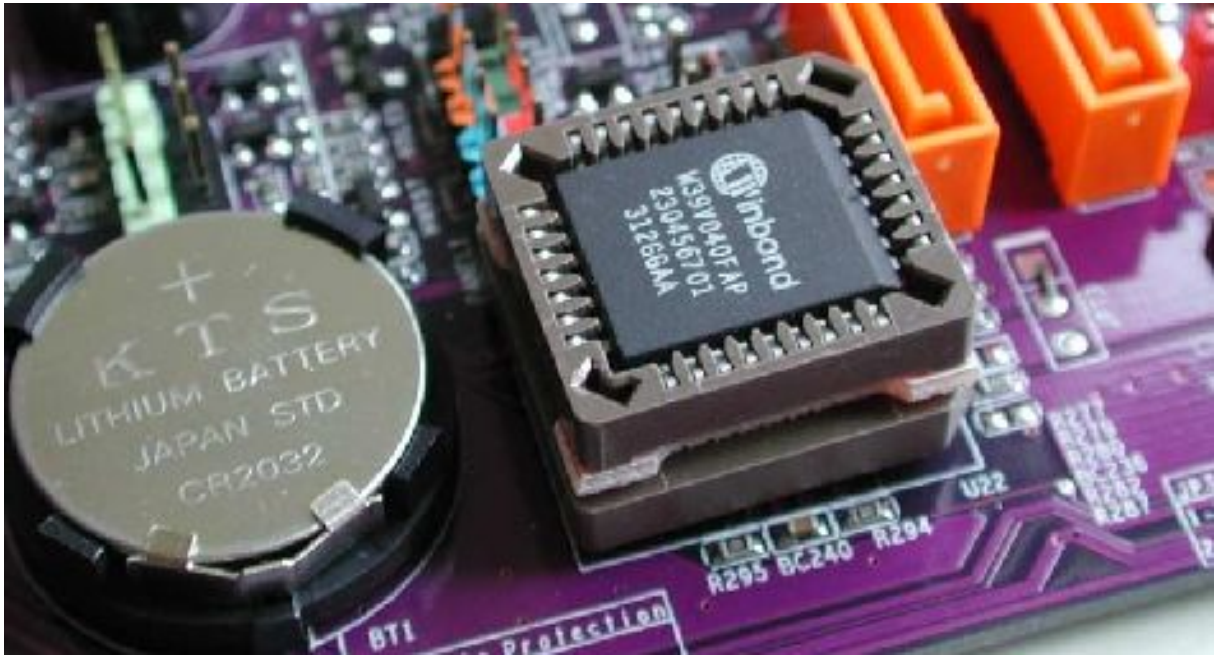
- В первом приближении BIOS различных системных плат с одинаковыми или близкими чипсетами могут оказаться (или показаться) совместимыми — по крайней мере, при включении выводится заставка, проходит тест POST и даже загрузка.
- Однако при более тщательном тестировании может оказаться, например, что невозможно обратиться к дискам (гибким или жестким), не работают порты, доступна не вся память и т. п.
- Хорошо, если при этом удастся загрузить утилиту перепрограммирования BIOS, чтобы вернуться к старой (*предварительно сохраненной!*) версии.

BIOS

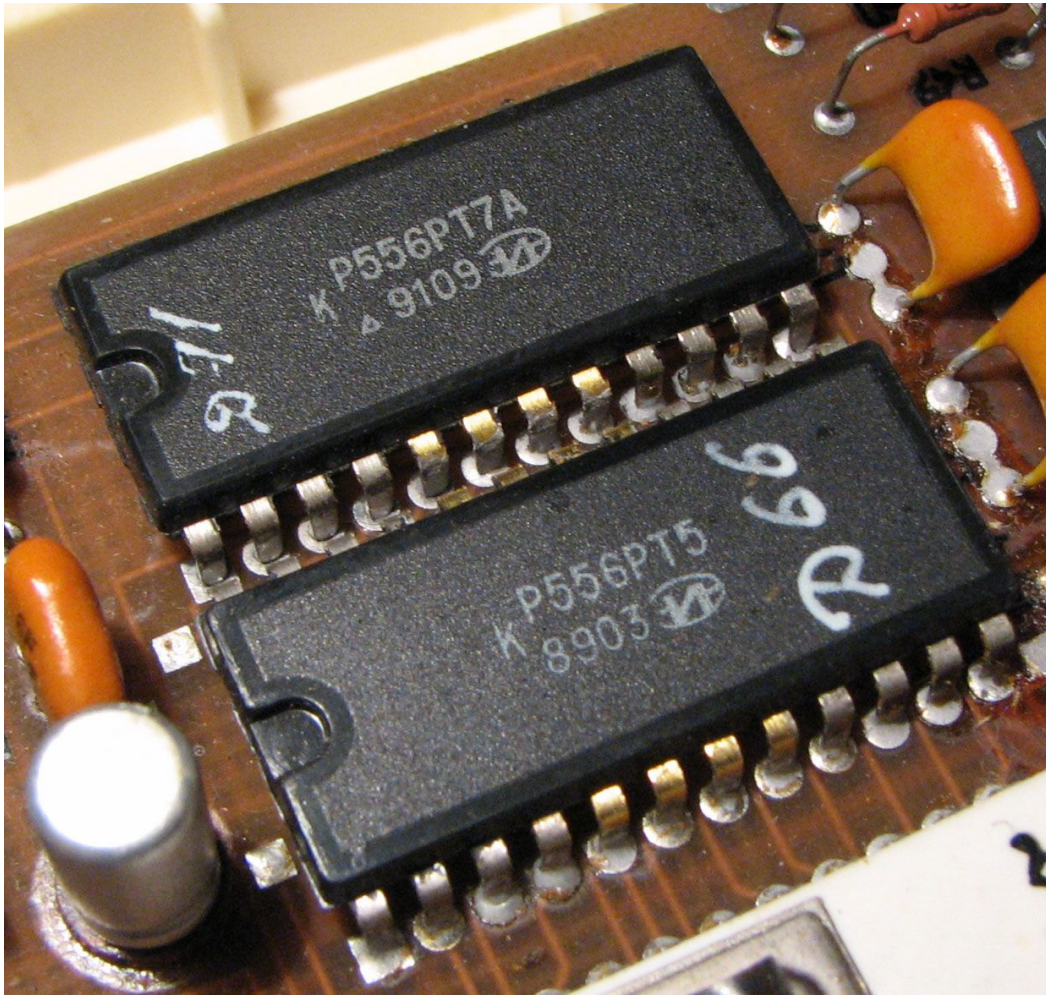
- Утилиты перезаписи флэш-памяти привязаны к поддерживаемым типам микросхем энергонезависимой памяти, системным платам (чипсетам) и производителям (иногда и версиям) BIOS.
- Обычно не удается штатным способом (в компьютере) переписать BIOS со сменой производителя (Award, AMI, Phoenix).
- Как вариант возможна замена (хотя бы временная) микросхемы BIOS на снятую с аналогичной системной платы, но если микросхема припаяна, а не установлена в специальный разъём, процедура замены сильно осложняется.

BIOS


40P


K T S
LITHIUM BATTERY
JAPAN STD
CR2032
Winbond
W39V040FAP
2304567 01
3126BAA
U22
R294
R295 BC240
BT1

BIOS



BIOS

- Смело заниматься перепрограммированием BIOS можно если:

  - вы имеете доступ к программатору,
  - микросхема BIOS установлена в специальный разъём.

BIOS

BIOS

- Если новая версия BIOS не позволяет загрузить компьютер, то ряд системных плат позволяют включить режим восстановления.
- Для этого на плате должен быть специальный переключатель или джампер.
- В режиме восстановления работает только дисковод, в который необходимо установить специальную диск с файлом-образом ROM BIOS.
- Этот диск необходимо подготовить заранее.

BIOS

- При этом «сообщения» пользователю могут сводиться к подмигиванию индикатора дисковода и гудкам динамика.
- Язык этих сообщений должен приводиться в описании системной платы.
- Иногда режим восстановления включается автоматически, если блок начальной загрузки получает управление в начале теста POST.
- Он всегда может оценить корректность содержимого основного блока ПЗУ и при необходимости включить режим восстановления.

BIOS

- Если же после неудачного перепрограммирования режим восстановления не спасает или отсутствует, а доступного программатора нет, то есть хотя и рискованный, но возможный вариант «горячей замены» ROM BIOS.
- Для этого из аналогичной работоспособной системной платы извлекают микросхему BIOS, устанавливают ее вместо испорченной, включают и загружают компьютер как для режима перезаписи BIOS.

BIOS

- При этом в Setup должно быть разрешено применение теневой памяти для области системного модуля BIOS.
- Далее, не выключая питания (опасно, но в безвыходном положении можно рискнуть), заменяют микросхему на неверно записанную и выполняют процедуру перезаписи.
- Компьютер продолжает работать, поскольку код BIOS исполняется из теневой области ОЗУ.
- Для перезаписи может быть использован файл-образ, полученный как копия «спасительной» микросхемы, сделанная той же программирующей утилитой.

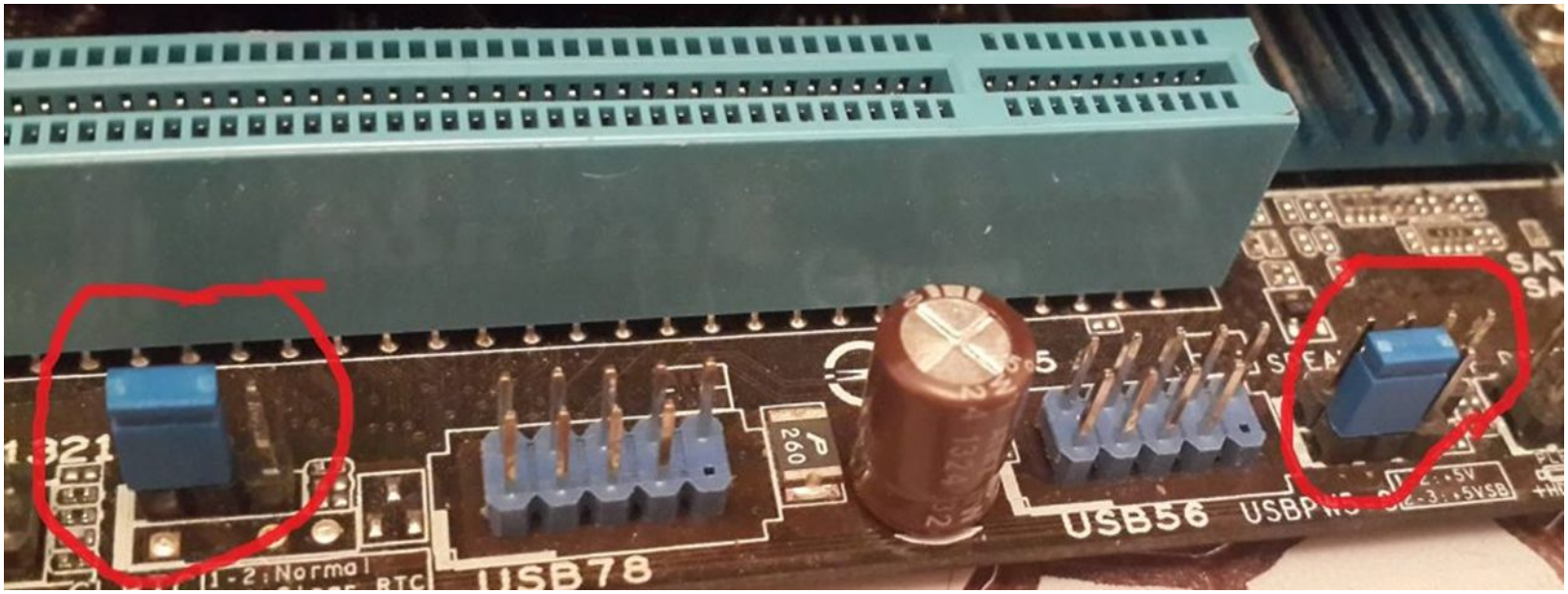
BIOS

- Если говорить о недостатках флэш-BIOS, имеется в виду не только опасность потери работоспособности системной платы из-за неосмотрительных действий пользователя, модернизирующего BIOS, но и дополнительное «поле деятельности» для вирусов.
- Парольная (программная) защита перезаписи может быть взломана, а надежная аппаратная защита (необходимостью подачи высокого напряжения для стирания и программирования, а также сигнала защиты записи) имеется далеко не у всех микросхем энергонезависимой памяти и системных плат.

BIOS

- Решившись на обновление BIOS, необходимо придерживаться следующих рекомендаций:
- ♦ Убедитесь в том, что системная плата поддерживает программирование флэш-памяти (ISW).
- ♦ Убедитесь, что установленная микросхема BIOS не относится к EPROM. У этих микросхем имеется окошко, которое можно прощупать через наклейку или увидеть, сняв ее. Однако отсутствие окошка — еще не явный признак флэш-памяти: имеются микросхемы EPROM 27xxx без окошка.
- ♦ Установите джамперы в режим программирования флэш-памяти.

BIOS



джамперы

BIOS

- ♦ Компьютер желательно подключить к источнику бесперебойного питания — сбой питания во время программирования при отсутствии режима восстановления (переключателя Boot Recovery) может привести к потере возможности программирования в режиме ISW.
- ♦ В CMOS Setup необходимо отключить применение теневой памяти (Shadow ROM) к области BIOS и запретить функции энергосбережения (Power Management — Disable).

BIOS

- ♦ ОС для запуска утилиты программирования должна загружаться в реальном режиме и без драйверов верхней памяти.
- Этого можно достичь загрузкой с системного диска, не содержащего ссылок на драйверы.
- В MS-DOS6.x можно шунтировать стартовые файлы нажатием клавиши F5 в начале загрузки.
- При использовании Windows в меню, появляющемся при нажатии клавиши F8 в начале загрузки, выбирают команду Safe mode command prompt only.

BIOS

- ♦ Загрузив утилиту программирования, прежде всего сделайте файл резервной копии текущей версии BIOS — она ещё может пригодиться.
- ♦ Утилита обычно определяет тип установленной флэш-памяти.
- Если определить тип ей не удается («unknown»), программирование выполнять нельзя — требуется подыскать подходящую утилиту.

BIOS

- ♦ Если во время программирования появляются сообщения об ошибках — не выключайте питание, не нажимайте кнопку Reset или клавиши перезагрузки.
- Попытка перезагрузки в этом случае может привести к «зависанию» компьютера навсегда или до восстановления.
- Не выходя из утилиты, попытайтесь восстановить прежнюю версию BIOS с ранее сделанной копии.
- ♦ После успешного завершения обновления перезагрузите компьютер и поработайте с новой версией BIOS.
- Старую версию желательно сохранить — возможные проблемы новой версии могут проявиться позже.

BIOS

- ♦ Если модификация была безуспешной и привела к невозможности загрузки компьютера, воспользуйтесь переключателем (джампером) Boot recovery и восстановите прежнюю версию BIOS, после чего верните переключатель в исходное состояние.
- ♦ Пользоваться возможностью перепрограммирования блока начальной загрузки без веских на то причин не стоит — версия его кода на нормальную работу PC обычно не влияет.
- Перепрограммировать блок начальной загрузки можно только при нормальной работе основного блока BIOS.

BIOS

- В противном случае сбой программирования блока начальной загрузки загонит пользователя в тупик.
- ♦ Некоторые утилиты позволяют очищать блоки параметров — память ESCD.
- Эта очистка приведет к потере информации об установленных устройствах PnP, что потребует их повторного конфигурирования.
- В некоторых случаях такая чистка даже полезна, поскольку система PnP пока еще далека от совершенства.

BIOS

- Иногда перепрограммировать флэш-BIOS приходится и для того, чтобы проинициализировать или сбросить некоторые параметры в энергонезависимых ячейках памяти чипсета, которые для обычных утилит (CMOS Setup) недоступны, но могут быть неудачно настроены, например при установке ОС Windows.

BIOS

- Помимо обновления версии перепрограммирование BIOS используют и для других целей.
- Можно, например, изменить или вставить логотип, появляющийся во время теста POST, на произвольную растровую картинку определенного формата.
- Возможно также изменение параметров, принимаемых в CMOS Setup по умолчанию (BIOS Defaults, Power-On Defaults).
- Для этого существуют специальные утилиты, ориентированные на определенные версии BIOS.

Память CMOS — питание и обнуление

Память CMOS — питание и обнуление

- CMOS – специальная микросхема динамической памяти, в которой записан BIOS Setup (название технологии, по которой производится микросхема: Complementary Metal-Oxide-Semiconductor - комплементарный металлооксидный полупроводник или КМОП).
- Память CMOS, совмещенная с часами-таймером, является энергонезависимой памятью конфигурации компьютера. Помимо ячеек стандартного назначения в CMOS имеются ячейки, которые используются по усмотрению разработчика BIOS для хранения текущих параметров чипсета, задаваемых встроенной утилитой CMOS Setup.

Память CMOS — питание и обнуление

- Для питания этой памяти на системной плате устанавливается литиевая батарейка (аккумуляторы применяются редко).
- Она имеет нормальный срок жизни несколько лет.
- О необходимости ее замены говорит сообщение «CMOS Battery State Low» или «CMOS Checksum Error» во время теста POST, обычно появляющееся после длительного (несколько дней) перерыва в работе машины.
- Первым признаком необходимости ее замены может быть и остановка внутренних часов-календаря при выключении машины (они превращаются в счетчик «моточасов»).

Память CMOS — питание и обнуление

- Иногда параметры Setup из-за разряда батареи теряются и без диагностических сообщений.
- Память CMOS является важным узлом компьютера, и правильность ее питания может существенно влиять на работоспособность компьютера в целом.

Память CMOS — питание и обнуление

- Случай из практики: «села» батарейка, терялись время и параметры, но поменять батарейку не торопились еще и из-за «капризности» системной платы.
- После включения компьютера плата долгое время «не заводилась» — POST нажатием кнопки Resety давалось запустить лишь после длительного прогрева.
- Проверка и даже замена блока питания результатов не дала.

Память CMOS — питание и обнуление

- Однако после ОТКЛЮЧЕНИЯ батарейки плата стала работать нормально.
- При этом плата естественно, теряла содержимое CMOS при выключении, но запускалась без проблем.
- Установка свежей батарейки полностью восстановила работоспособность платы.

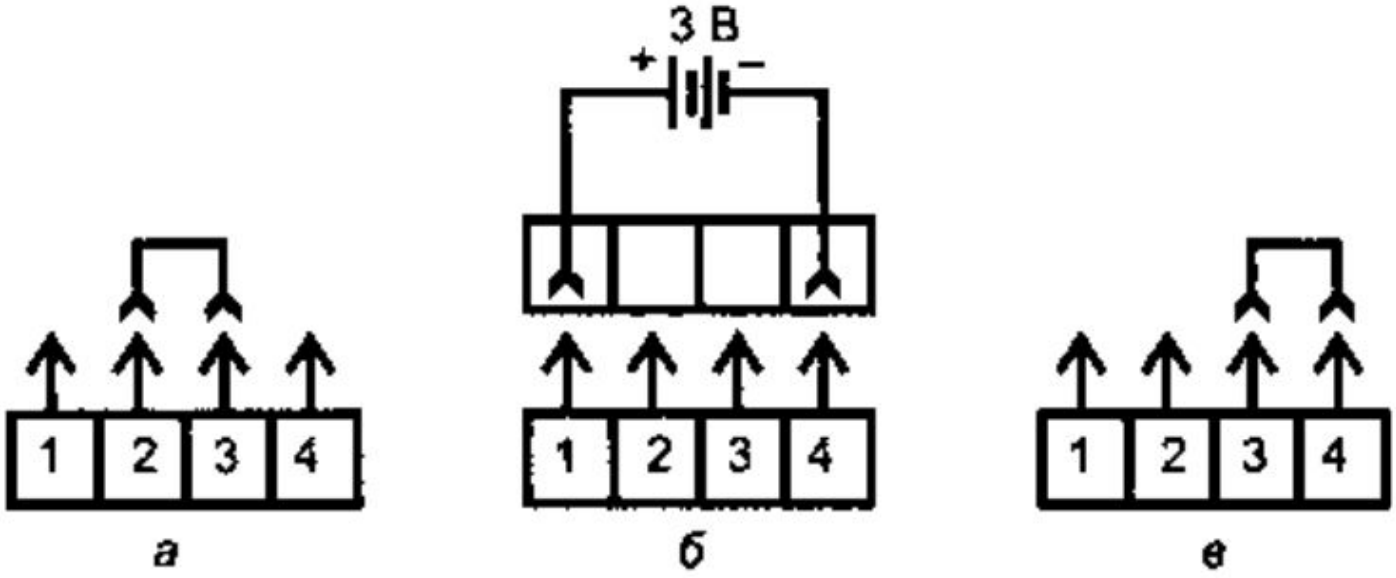
Память CMOS — питание и обнуление

- На старых платах батарейка представляла собой обычно синий бочонок, припаянный к плате.
- Со временем пришла пора их массового выхода из строя на системных платах машин.
- При этом теряется информация CMOS, но что гораздо хуже — электролит может растечься и вызвать появление паразитных контактов и разъедание элементов системной платы.
- Протекшую батарейку надо обязательно извлечь, а плату отчистить щеточкой и промыть.

Память CMOS — питание и обнуление

- На современных системных платах чаще применяется батарейка-таблетка в специальном держателе, которую легко заменить.
- Разъем подключения внешней батарейки используется и для обнуления CMOS (на старых платах).
- Такая необходимость может возникнуть, например, при утере входного пароля, заданного в CMOS Setup (или при необходимости его замены).
- Теоретически, для этого достаточно при выключенном компьютере на несколько минут переставить перемычку в положение, показанное на рисунке *в*.

Память CMOS — питание и обнуление



Подключение внешней батарейки и обнуление CMOS: а — работа от внутренней батарейки, б — работа от от внешней батарейки, *в* — обнуление CMOS

Память CMOS — питание и обнуление

- Иногда для сброса пароля предназначен отдельный джампер или переключатель (применяется, если пароль хранится не в CMOS, а в NVRAM).
- В этом случае, переключив джампер, необходимо включить компьютер — только тогда пароль будет сброшен, после чего вернуть джампер в исходное состояние.
- Однако бывают случаи, когда штатными способами пароль не сбросить.
- Тогда есть еще один способ — закоротить выводы микросхемы CMOS при отключенном питании и отключенной батарейке.

Память CMOS — питание и обнуление

- Для этого кусочек фольги прикладывается сверху к микросхеме и аккуратно приглаживается к выводам по периметру корпуса.
- Чтобы не утруждать себя идентификацией микросхемы CMOS, эту операцию можно проделать со всеми «подозрительными» многовыводными микросхемами — их не так уж много.
- Обнуление CMOS (сброс всех параметров к значениям, заданным по умолчанию) может быть выполнено чисто программно, записью определенного кода в одну из ячеек CMOS.

Память CMOS — питание и обнуление

- Периодическое разрушение информации CMOS при включении питания может быть вызвано вовсе не батарейкой, а недостаточной задержкой сигнала PowerGood относительно момента установления питающего напряжения или, наоборот, излишней задержкой этого сигнала после выключения источника.
- Определить причину довольно просто.
- Если перед включением питания удержать нажатой кнопку Reset и отпустить ее только через несколько секунд, в большинстве случаев это имитирует увеличение задержки сигнала PowerGood.

Память CMOS — питание и обнуление

- Если при таком способе включения данные CMOS сохраняются, дело в малой задержке при включении.
- Если данные CMOS все равно теряются, нужно проверить версию задержки при отключении.
- Для этого кнопку Reset следует нажимать перед выключением питания и удерживать еще несколько секунд — этим имитируется ускорение снятия сигнала PowerGood.
- Если при таком способе выключения данные CMOS сохраняются, дело в большой задержке при выключении.
- В обоих случаях требуется замена или ремонт (подстройка) блока питания.

Список литературы:

1. Аппаратные средства IBMPC. Гук М.Ю. Энциклопедия. 3-е изд. — СПб.: Питер, 2006.
2. Архитектура аппаратных средств. Конспект лекций. Барсукова Т. И.
3. Архитектура аппаратных средств. Конспект лекций. Забавина А. А.

Список ссылок:

https://i.ebayimg.com/00/s/OTAwWDE2MDA=/z/ATkAAOSwAWlajflo/$_57.JPG?set_id=8800005007
https://ds04.infourok.ru/uploads/ex/07aa/00132e01-b4054430/img52.jpg
https://www.vikrambedi.com/wp-content/uploads/2018/01/BIOS.jpg
http://zxbyte.ru/pic/byte03_09.jpg
http://zxbyte.ru/pic/byte03_13.jpg
https://www.robotistan.com/tl866a-universal-usb-programmer-with-icsp-feature-1363-55-B.jpg

Благодарю за внимание!

Преподаватель: Солодухин Андрей Геннадьевич
Электронная почта: asoloduhin@kait20.ru