

Лекція 2. Додаткові відомості про апаратне забезпечення



3.1 Завантаження комп'ютера

Video Demonstration – BIOS – UEFI Menus

Video Demonstration: BIOS - UEFI Menus

In this video demonstration, you will learn about the menus found in a typical UEFI BIOS:

- Main Screen
- Settings
- OC
- M-Flash
- OC Profile
- Hardware Monitor
- Board Explorer



POST, BIOS, CMOS і UEFI

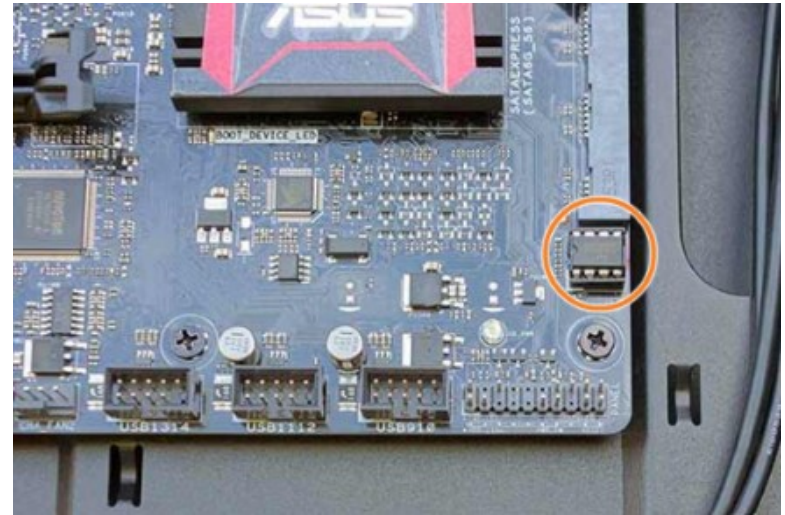
POST

- BIOS = basic input/output system (базова система введення-виведення)
- На початку завантаження комп'ютера BIOS виконує перевірку основних апаратних компонентів.
 - Ця перевірка називається POST (power-on self-test).
- Якщо котрийсь компонент працює неправильно, виводиться повідомлення або видається звуковий сигнал.
- Виробники BIOS використовують різні коди та сигнали на позначення різних апаратних проблем.
 - За потреби звертайтеся до документації конкретної материнської плати.

POST, BIOS, CMOS і UEFI

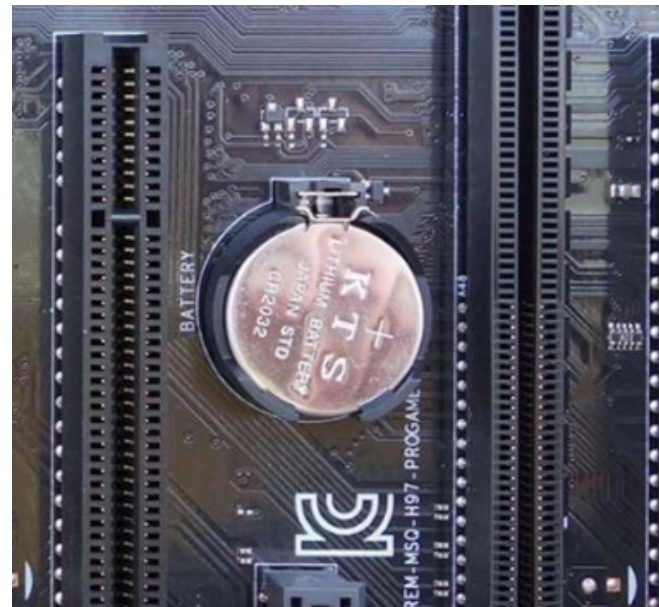
BIOS і CMOS

- Всі материнські плати мають BIOS (BIOS/UEFI).
- BIOS міститься на чипі ROM на материнській платі.
- BIOS є невеликою програмою.
- За що відповідає BIOS:
 - POST;
 - які диски доступні, які з них завантажувальні;
 - які налаштування пам'яті потрібно застосувати;
 - як налаштовано слоти розширення PCIe і PCI;
 - як налаштовано порти SATA та USB;
 - опції керування живленням материнської плати.



BIOS і CMOS (Продовження)

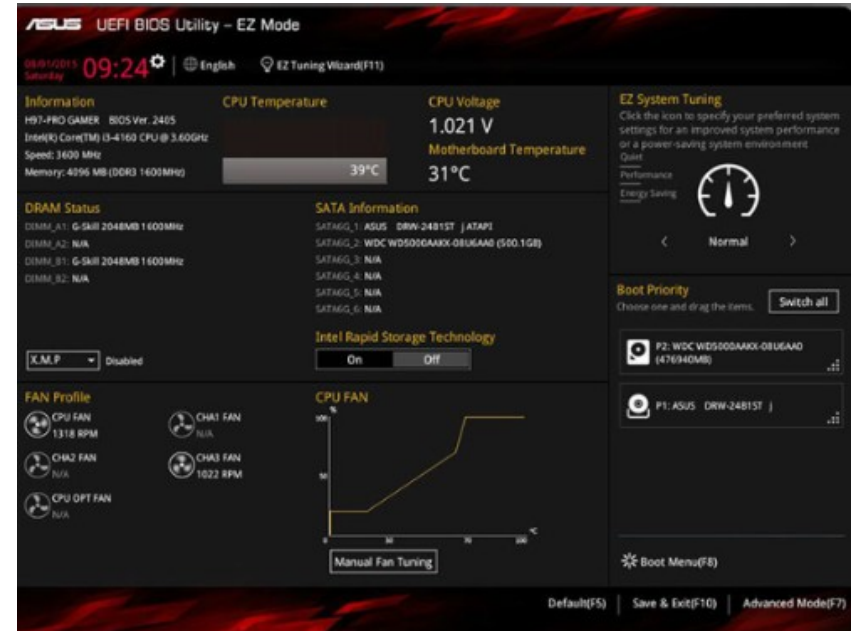
- Налаштування BIOS зберігаються на чипі пам'яті CMOS (Complementary Metal Oxide Semiconductor).
- Під час завантаження комп'ютера BIOS зчитує конфігурацію з CMOS і використовує її.
- CMOS живиться спеціальною батарейкою.
- Якщо батарейка розряджається, налаштування скидаються до стандартних.
- **Порада:** якщо на комп'ютері весь час збиваються налаштування дати та часу або інші BIOS-залежні налаштування (наприклад, налаштування апаратної віртуалізації) — варто поміняти батарейку CMOS.



POST, BIOS, CMOS і UEFI

UEFI

- На більшості сучасних комп'ютерів BIOS замінено на UEFI (Unified Extensible Firmware Interface).
- UEFI забезпечує більше опцій, зокрема безпекових.
- UEFI часто має графічний інтерфейс.
- UEFI підтримує 32-бітні та 64-бітні системи, більші завантажувальні розділи, технологію Secure Boot тощо.
 - Технологія Secure Boot забезпечує, щоб комп'ютер завантажив визначену ОС, як підтримує Secure Boot.
 - Це зроблено для запобігання руткітам.



Video Demonstration – Configure BIOS – UEFI Settings

Video Demonstration: Configure BIOS - UEFI Settings

In this video demonstration, you will learn about configuring typical UEFI BIOS settings:

- Boot Options
- Security Settings
- Interface Configurations
- Firmware Backup and Update Tool



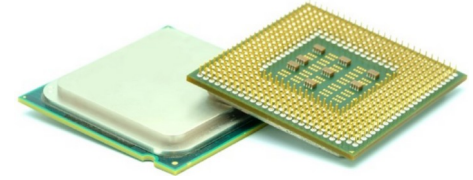
Оновлення прошивки

- Виробники материнських плат можуть публікувати нові версії BIOS, які мають покращення стабільності, сумісності та продуктивності.
- Початково BIOS зберігалася на ROM-чипі. Тому для оновлення BIOS потрібна була фізична заміна ROM-чипа.
- Сучасний BIOS (BIOS/UEFI) використовує пам'ять EEPROM (Electrically Erasable Programmable Read Only Memory), вміст якої можна змінити, навіть не відкриваючи корпус комп'ютера.
 - Така операція називається перепрошивкою BIOS ("flashing the BIOS").
- Завантажити нову версію BIOS зазвичай можна на вебсайті виробника материнської плати.

3.2 Додаткові питання функціонування комп'ютера

Архітектури та операції ЦП

Архітектури ЦП



- Програма є послідовністю інструкцій, які зберігаються у пам'яті, і які виконуються на ЦП відповідно до спеціального набору інструкцій.
- Є два типи наборів інструкцій, які можуть використовуватися у ЦП:
 - **RISC (Reduced Instruction Set Computer)** — архітектура, яка використовує порівняно малий набір інструкцій. RISC-процесори орієнтовані на дуже швидке виконання інструкцій. Приклади: PowerPC, ARM
 - **CISC (Complex Instruction Set Computer)** — архітектура, яка використовує широкий набір інструкцій. На відміну від RISC, CISC-процесори здійснюють меншу кількість кроків за операцію. Такими є процесори Intel x86.
- Поки виконується один крок програмного коду, інші інструкції та дані зберігаються у спеціальній пам'яті швидкого доступу, яка називається **кеш (cache)**.
- (Доступ до кешу ЦП є *швидким відносно звичайного доступу* до цих коду та даних в оперативній пам'яті, де ці код та дані зберігаються, якщо зараз виконується код інших процесів (потоків) — прим. О. Г.)

Архітектури ЦП

- Процесори Intel використовуються технологію **Hyper-Threading** для підвищення продуктивності своїх ЦП.
 - У разі застосування Hyper-Threading кілька фрагментів коду (**потоків**) можуть виконуватися на ЦП паралельно.
 - (Hyper-Threading не рівносильне багатоядерності ЦП. Натомість ідеться про можливість одночасно зберігати в регістрах ЦП даних, пов'язаних з виконанням двох різних потоків. Тоді, поки один з потоків не може виконуватися, зможе виконуватися другий потік, і навпаки — О. Г.)
 - Процесори AMD використовують технологію **HyperTransport** для підвищення продуктивності ЦП.
 - HyperTransport забезпечує високошвидкісне з'єднання між ЦП та чипом північного мосту.
 - Потужність ЦП вимірюється швидкістю та кількістю даних, які він може опрацювати.
 - **Частота процесора** (speed of CPU, CPU frequency) вимірюється у циклах за секунду, наприклад, мільйон циклів за секунду становить 1 МГц (MHz), а мільярд циклів за секунду — 1 ГГц (GHz).
-  Обсяг даних, які процес може обробити за раз, залежить від **розмірів передньої шини** (FSB, front side bus), яку також називають шиною ЦП або шиною даних ЦП.

Покращення показників роботи ЦП

- **Розгін (overclocking)** — це техніка збільшення швидкості роботи ЦП, порівняно з оригінальною специфікацією цього ЦП.
 - Розгін НЕ є рекомендованим шляхом покращення продуктивності комп'ютера і може завдати шкоди ЦП.
- **Тротлінг (CPU throttling)** є протилежною технікою.
- The opposite of overclocking is CPU throttling.
 - Тротлінг ЦП передбачає зниження частоти процесора для економії енергії та зменшення нагрівання.
- **Віртуалізація ЦП** (CPU virtualization; *також hardware-assisted virtualization* — О. Г.) є апаратною опцією, підтримуваною процесорами AMD та Intel, яка дозволяє одному процесору поводитися як декілька (*віртуальних* — О. Г.) процесорів.