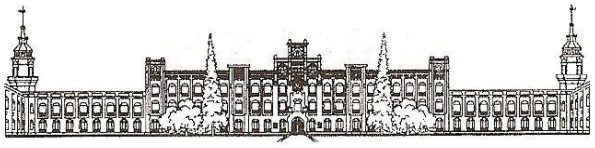

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ імені Ігоря Сікорського»
ФАКУЛЬТЕТ ПРИКЛАДНОЇ МАТЕМАТИКИ

Лабораторна робота №4

з дисципліни «Архітектура комп'ютера. Апаратне забезпечення»

«Діагностика BIOS або UEFI»

Виконав студент IV курсу

групи: КВ-11

ПІБ: Терентьєв Іван Дмитрович

Перевірив: _____

Київ 2024

Завдання для лабораторної роботи

Зробити фотографії пунктів меню BIOS або UEFI Вашого комп'ютера. Надати перелік графічного матеріалу, кожен рисунок підписується в коментарях, до нього наводиться технічні аспекти на які слід звернути увагу.

Навести висновки стосовно:

- загальні властивості системи
- опції завантаження системи
- завантаження fast або compatible
- захист системи
- опції щодо віртуалізації системи
- tpm state
- керування мережевим пристроями
- керування електроживлення
- UEFI

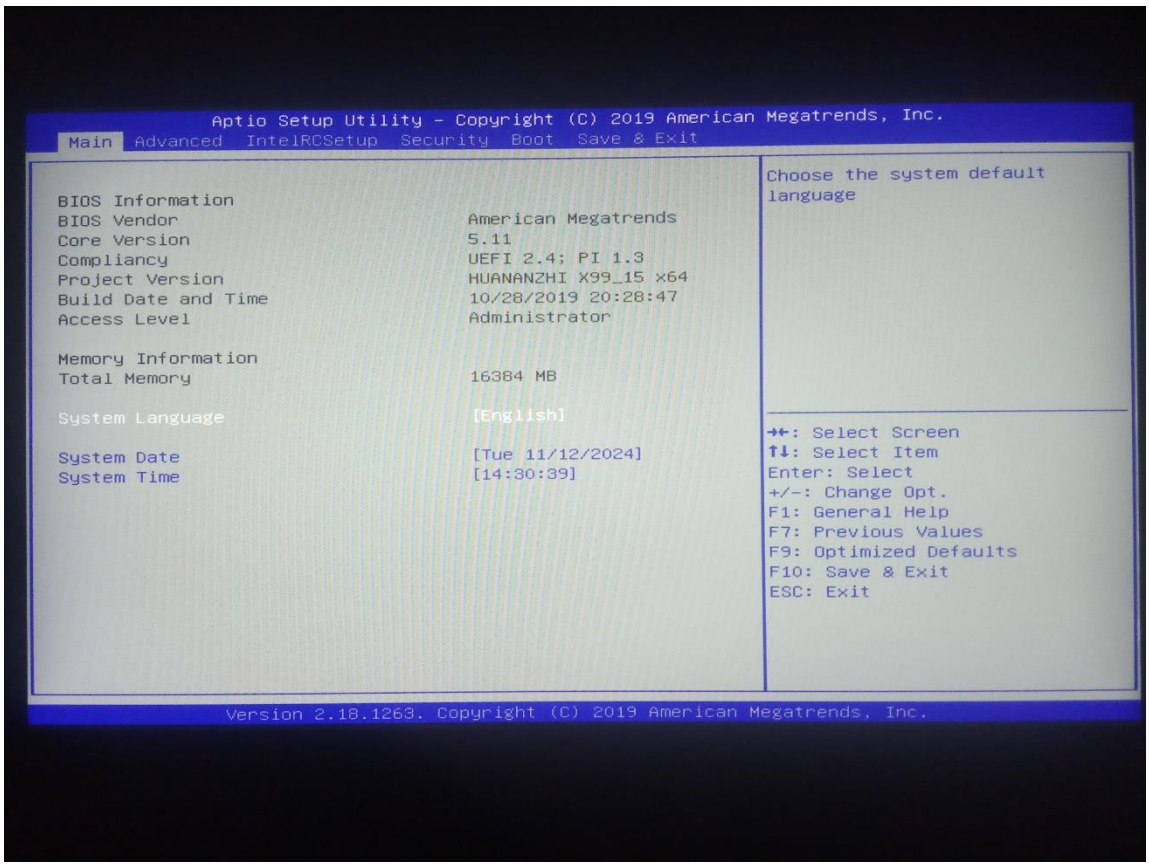

Рис. 1 – Загальні властивості системи (Main)

Відображає основну інформацію про систему, таку як версія BIOS, модель процесора, обсяг встановленої оперативної пам’яті. Це дає змогу швидко оцінити базові параметри системи.

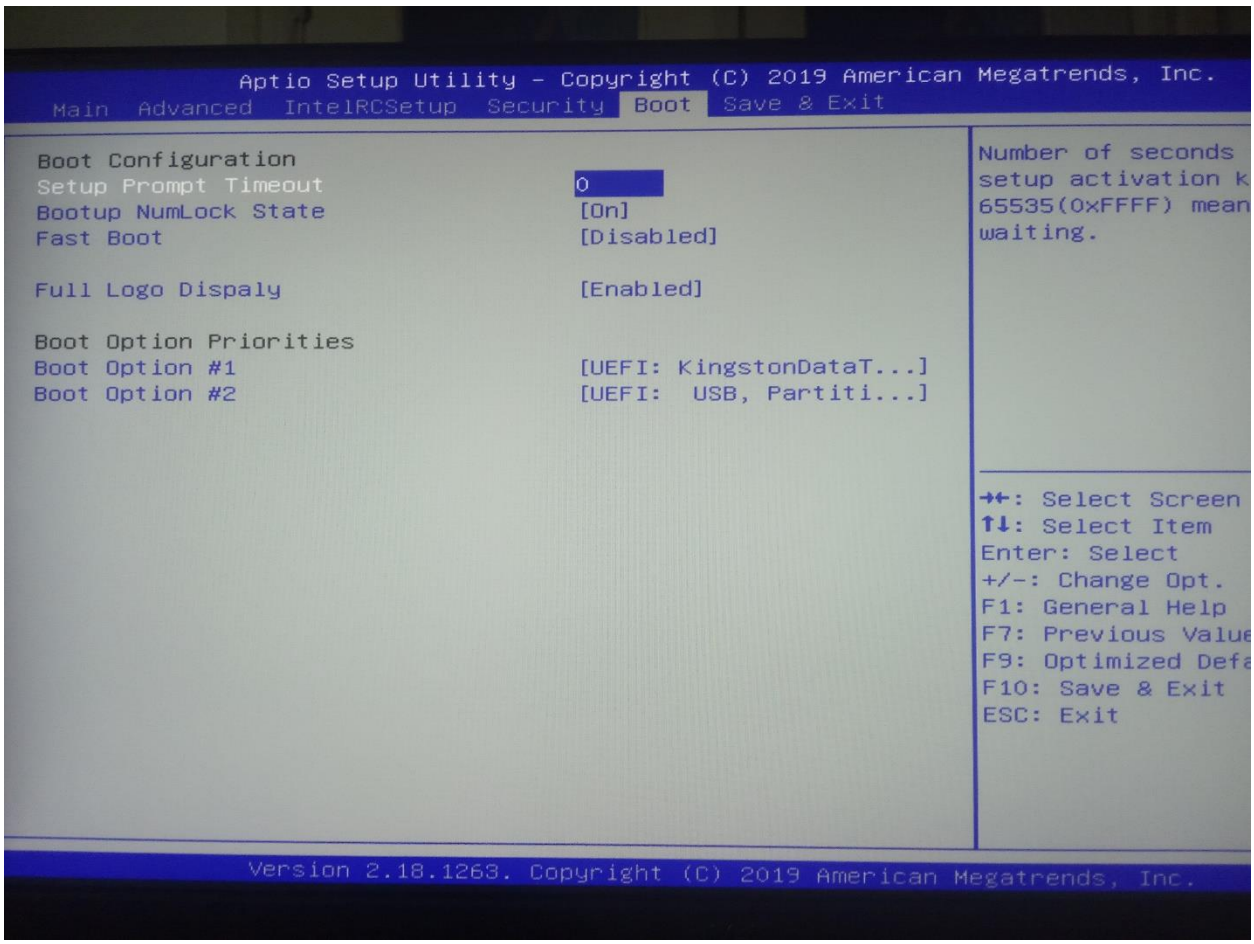

Рис. 2 – Налаштування завантаження (Boot Configuration)

Містить налаштування завантаження системи, включаючи пріоритет завантаження пристроїв та режим Fast Boot, що прискорює завантаження системи.

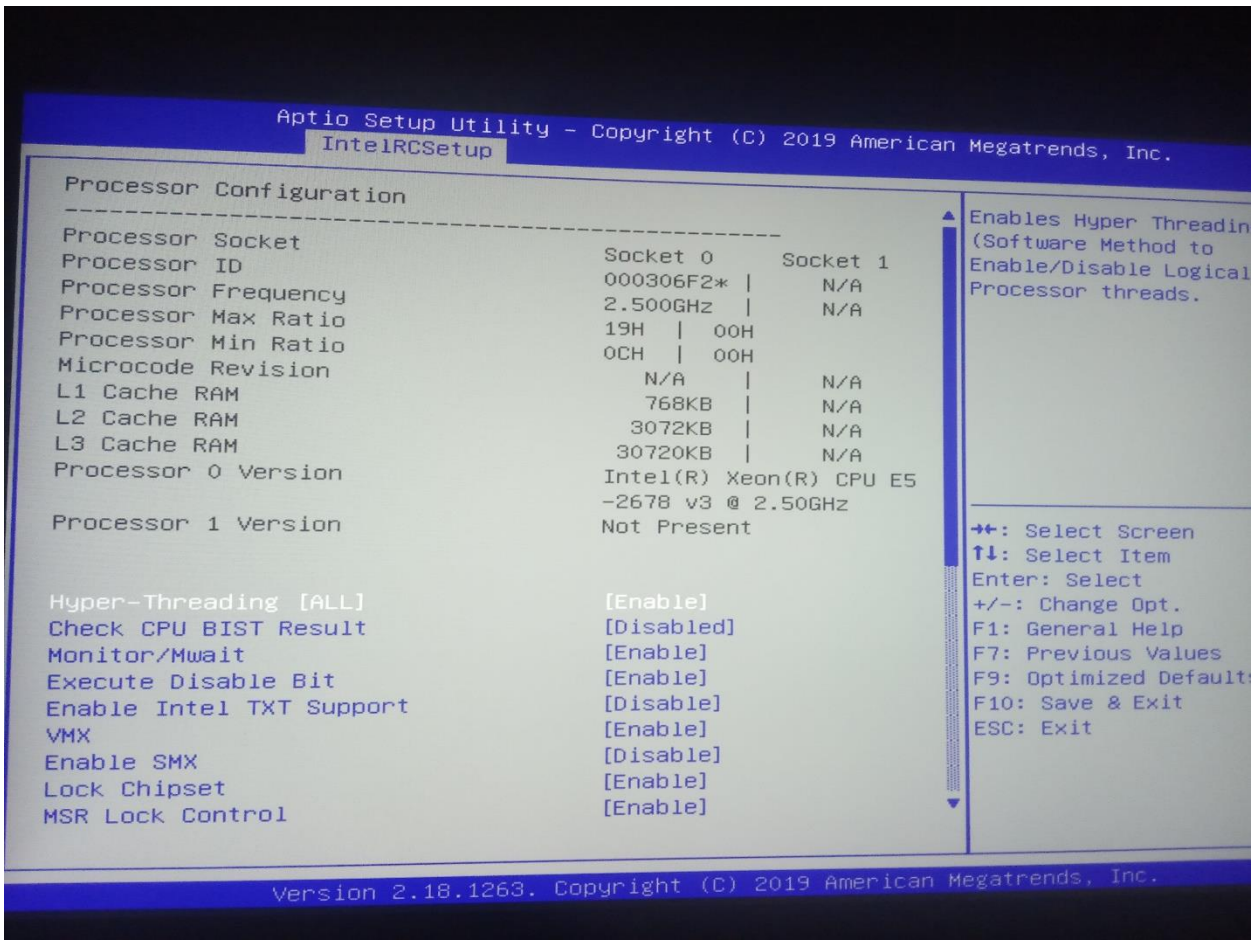

Рис. 3 – Конфігурація процесора (Processor Configuration)

Відображає налаштування процесора, зокрема підтримку Hyper-Threading, віртуалізації (VMX), та інших параметрів, які важливі для продуктивності та сумісності.

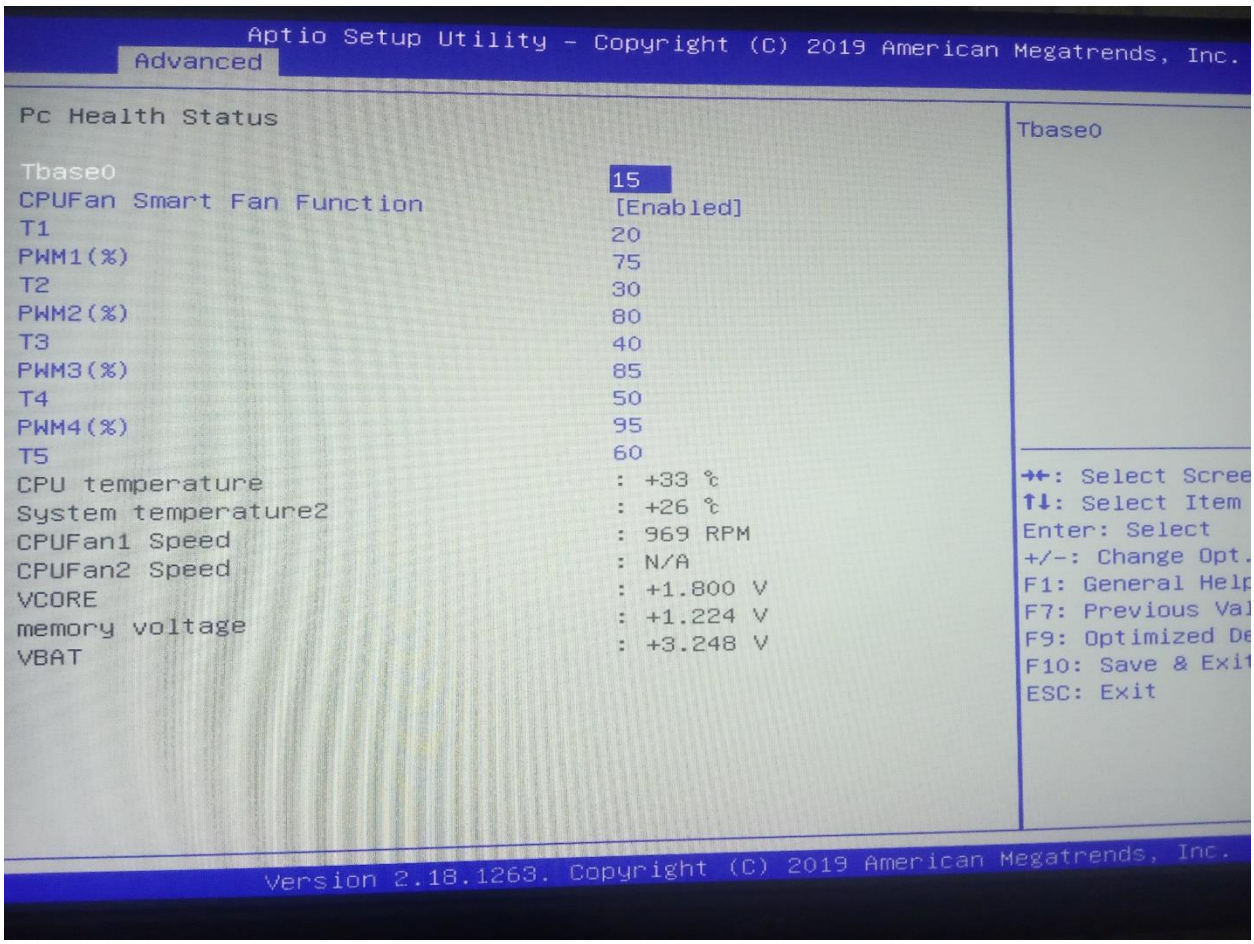

Рис. 4 – Статус системи охолодження (PC Health Status)

Показує поточний стан системи охолодження: температуру процесора, швидкість обертання вентиляторів, напругу на основних компонентах.

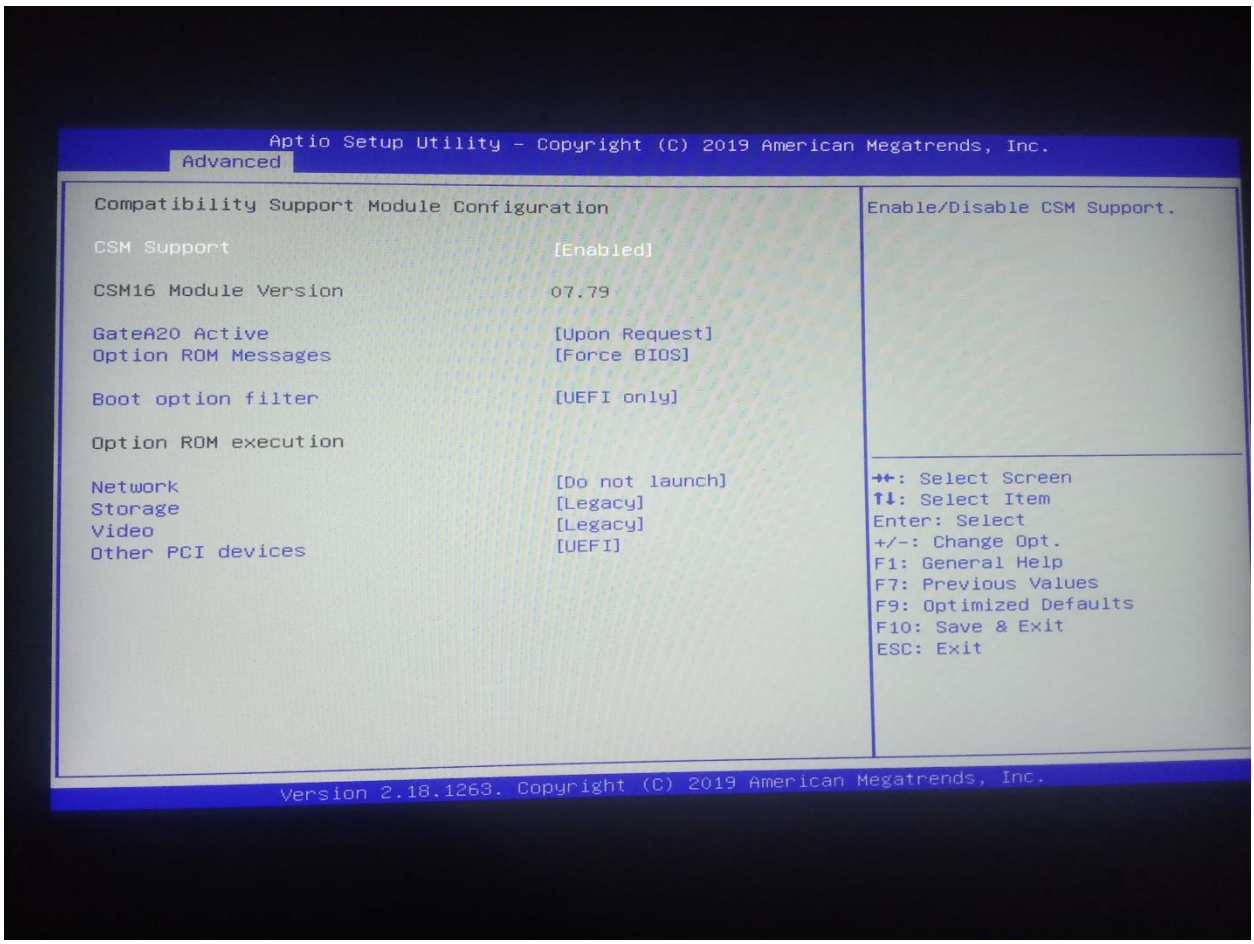

Рис. 5 – Підтримка сумісності (Compatibility Support Module, CSM)

Відображає налаштування CSM для підтримки завантаження в режимі сумісності, що дозволяє використовувати старі ОС та пристрої.

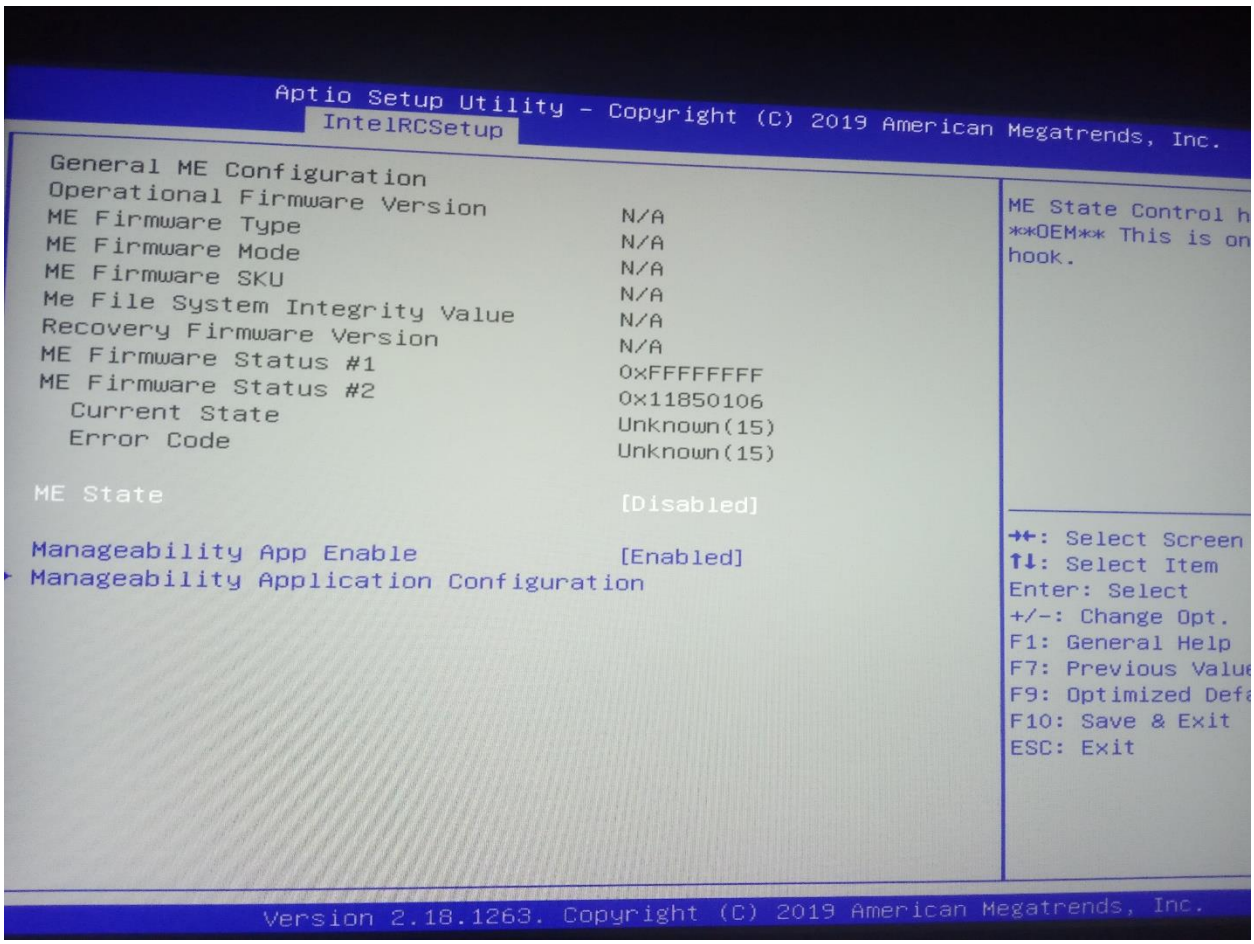

Рис. 6 – Intel Management Engine (ME) Configuration

Відображає налаштування Intel ME. На цій платформі Intel ME не функціональний, тому деякі параметри недоступні.

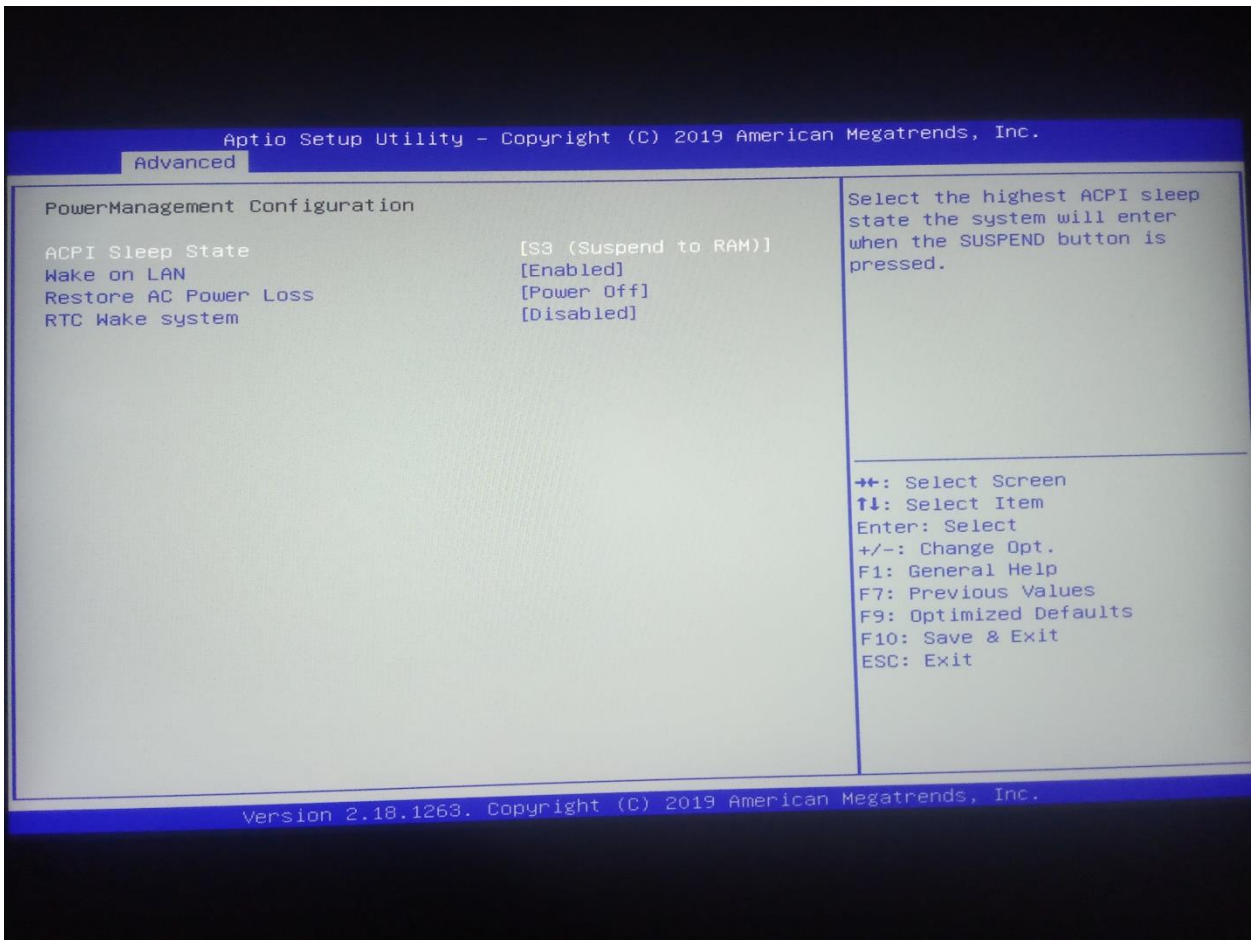

Рис. 7 – Управління електроживленням (Power Management Configuration)

Відображає налаштування управління живленням, включаючи ACPI Sleep State, Wake-on-LAN, параметри відновлення після втрати живлення.

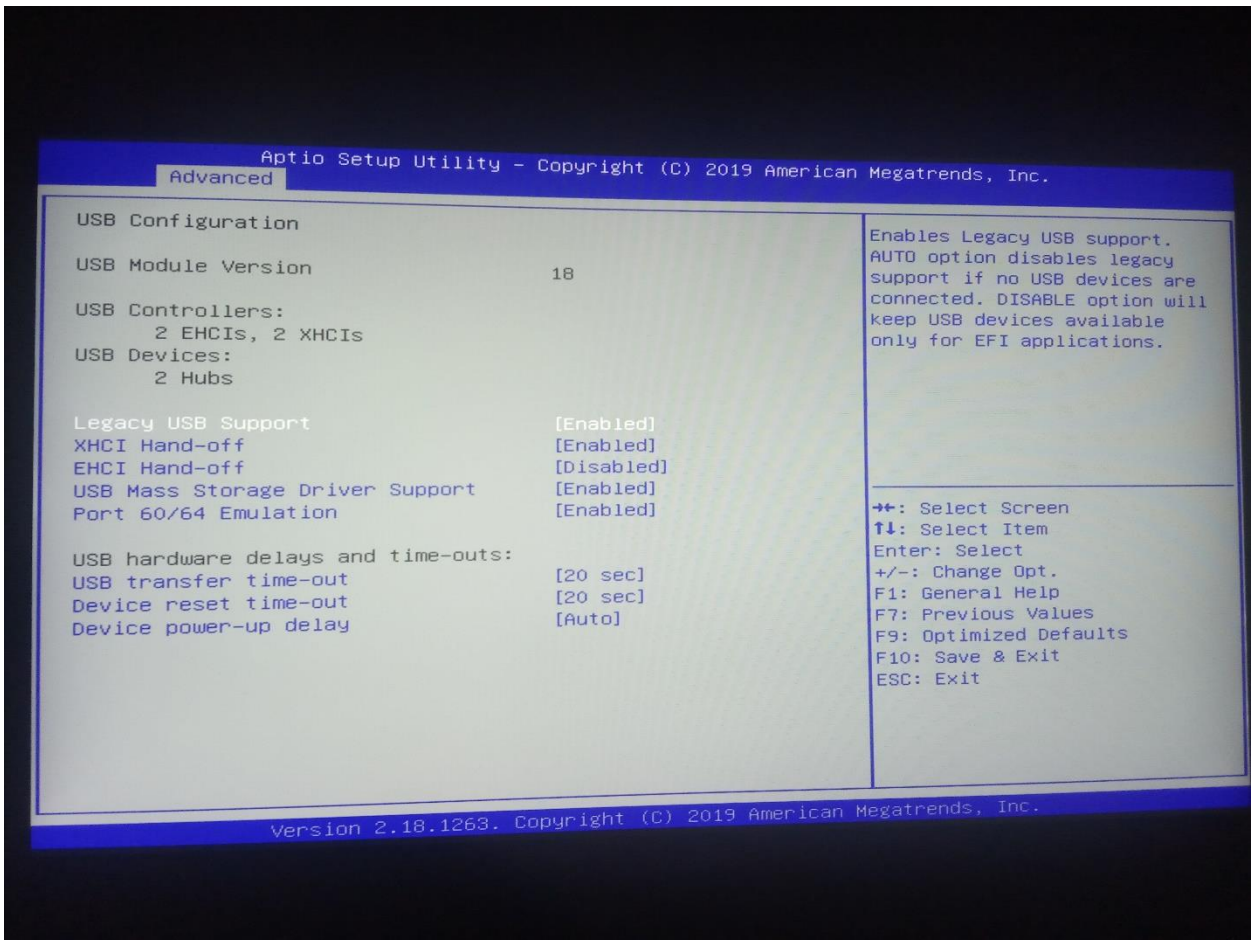

Рис. 8 – Конфігурація USB (USB Configuration)

Налаштування USB-контролерів, підтримка старих USB-пристроїв (Legacy USB Support), емуляція портів та налаштування таймінгів.

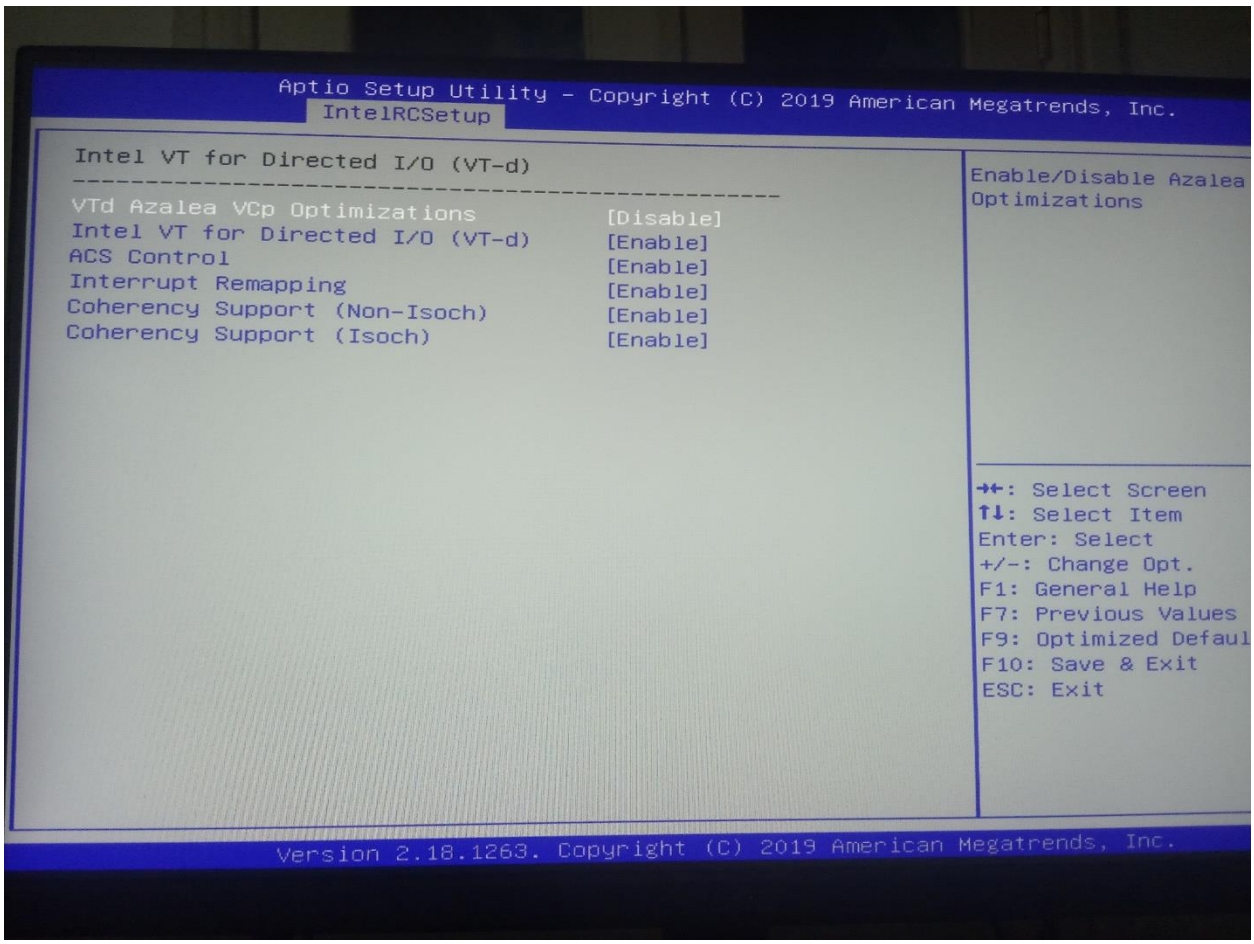

Рис. 9 – Налаштування віртуалізації (Intel VT for Directed I/O)

Включає параметри Intel VT-d для апаратної віртуалізації вводу/виводу, що є важливим для роботи віртуальних машин.

Висновки

- **Загальні властивості системи**

Встановлений процесор Intel Xeon E5-2678v3, обсяг оперативної пам’яті – 16 ГБ. Версія BIOS – AMI 5.11, що надає базові функціональні можливості для стабільної роботи системи. Інформація в BIOS дозволяє швидко оцінити сумісність системи з іншими компонентами.

- **Опції завантаження системи**

Налаштування завантаження надають можливість встановити пріоритети для різних завантажувальних пристроїв, таких як USB, жорсткий диск або SSD, а також включити або вимкнути режим Fast Boot для прискорення завантаження. Це забезпечує зручне управління порядком завантаження та налаштування середовища під специфічні потреби користувача.

- **Завантаження Fast або Compatible**

Підтримка режиму сумісності (Compatibility Support Module, CSM) дозволяє використовувати старі операційні системи та пристрої, які потребують сумісності з традиційним Legacy BIOS. При потребі доступний і режим Fast Boot, який прискорює завантаження, пропускаючи деякі перевірки апаратної сумісності.

- **Захист системи**

Налаштування безпеки включають основні параметри, такі як встановлення паролів для доступу до BIOS, що забезпечує додатковий рівень захисту від несанкціонованого доступу. Однак, функціонал TPM на цій платформі відсутній, що обмежує використання певних засобів безпеки, таких як шифрування дисків BitLocker.

- **Опції щодо віртуалізації системи**

Підтримка технологій Intel VT-x та VT-d дозволяє системі використовувати апаратну віртуалізацію. Це робить можливим запуск віртуальних машин, що корисно для тестування програмного забезпечення та емуляції різних операційних середовищ.

- **TPM State**

На цій платформі модуль TPM відсутній, що знижує рівень безпеки системи. Це може обмежити можливості використання певних функцій безпеки, які залежать від TPM, таких як надійне шифрування даних та інші функції захисту.

- **Керування мережевими пристроями**

BIOS підтримує функцію Wake-on-LAN, що дозволяє вмикати комп'ютер через локальну мережу. Ця функція може бути корисною для віддаленого керування та моніторингу системи. Також доступна підтримка PXE для мережевого завантаження, що забезпечує додаткові можливості для адміністрування системи.

- **Керування електроживленням**

Налаштування управління живленням включають підтримку ACPI для управління режимами енергозбереження та функцію відновлення живлення після його втрати. Це забезпечує гнучкість налаштувань споживання енергії та дозволяє системі автоматично відновлюватися у випадку перебоїв з електроживленням.

- **UEFI**

BIOS підтримує UEFI, що дозволяє використовувати сучасні завантажувальні засоби та сумісність з новітніми ОС. Завдяки UEFI система забезпечує швидше завантаження та підтримку GPT-розділів, що розширює можливості для управління пам'яттю і завантаження.