Міністерство освіти і науки України

Харківський національний університет радіоелектроніки

Факультет комп’ютерної інженерії та управління
(повна назва)

Кафедра електронних обчислювальних машин
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА

Пояснювальна записка

Рівень вищої освіти другий (магістерський)

Моделі та методи підвищення надійності функціонування BIOS комп’ютерної системи

(тема)

Виконав:

студент II курсу, групи СПм-20-1

Замицький Е.С.
(прізвище, ініціали)

Спеціальність

123 «Комп’ютерна інженерія»
(код і повна назва спеціальності)

Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)

Освітня програма

Системне програмування
(повна назва освітньої програми)

Керівник: доц. Голубничий Д.Ю.
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри ЕОМ _____ Коваленко А.А.
(підпис) (прізвище, ініціали)

2021 р.

Харківський національний університет радіоелектроніки

Факультет комп’ютерної інженерії та управління

Кафедра електронних обчислювальних машин

Рівень вищої освіти другий (магістерський)

Спеціальність 123 «Комп’ютерна інженерія»
(код і повна назва)

Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)

Освітня програма Системне програмування
(повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
“____” _____ 20__ р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

студенту Замицькому Ернесту Сергійовичу
(прізвище, ім’я, по батькові)

1. Тема роботи Моделі та методи підвищення надійності функціонування BIOS комп’ютерної системи

затверджена наказом по університету від “ 05 ” листопада 2021 р. № 1657 Ст

2. Термін подання студентом роботи до екзаменаційної комісії 13 грудня 2021 р.

3. Вхідні дані до роботи 1) IBM PC-сумісний комп’ютер з системою BIOS, UEFI;
2) Операційна система Windows, Linux;

4. Перелік питань, що потрібно опрацювати у роботі
1) Методи управління BIOS комп’ютерної системи
2) Програмні методи пошуку та усунення несправностей
3) Програмна модель та середовище моделювання
4) Рекомендації щодо налаштування параметрів bios

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (слайдів)

Слайд-презентація – 12 слайдів

6. Консультанти розділів роботи (заповнюється за наявності консультантів згідно з наказом, зазначеним у п.1)

Найменування розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		підпис	дата

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Аналіз проблеми та огляд існуючих рішень	09.11.21-11.11.21	
2	Вибір технології розробки та	12.11.21 – 23.11.21	
	інструментальних засобів		
3	Налагодження програмних модулів	24.11.21 – 29.11.21	
4	Оформлення матеріалів кваліфікаційної роботи	30.11.21 – 03.12.21	
5	Подання кваліфікаційної роботи керівникові	03.12.21 – 04.12.21	
	та її попередній захист		
6	Подання кваліфікаційної роботи на	04.12.21 – 05.12.21	
	рецензування		

Дата видачі завдання 8 листопада 2021 р.

Студент _____
(підпис)

Керівник роботи _____ доц. Голубничий Д.Ю.
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка кваліфікаційної роботи: 87 с., 31 рис., 2 табл., 2 дод., 10 джерел.

АРХІТЕКТУРА КОМП’ЮТЕРА, BIOS, UEFI, ОПЕРАЦІЙНА СИСТЕМА, КІБЕРБЕЗПЕКА, POST

Метою кваліфікаційної роботи є покращення процесу налаштування базової системи введення-виведення сучасного персонального комп’ютера для сприяння найшвидшему проведення попереднього тестування при включенні його живлення.

Об’єктом дослідження є процеси налаштування конфігурації апартного забезпечення персонального компютера.

Предметом дослідження є базова система введення-виведення, її архітектура, функції, та стан безпеки.

У ході виконання кваліфікаційної роботи були проаналізовані найважливіші компоненті конфігурацііїї базової системи введення-виведення, та було покращено програмний застосунок задля допомоги користувачеві налаштування системи. Задля полегшення розуміння базової системи введення-виведення було створено 4 розділи, які описують певні компоненти цієї системи. Застосунок відображає системну інформацію щодо операційної системи та самої базової системи введення-виведення та іншу інформацію, яка може бути корисною для користувача. Також, завдяки застосунку можна відобразити детальну інформацію про апаратні помилки комп’ютера та налаштування Secure Boot, Fast Boot, паролю адміністратора.

ABSTRACT

Master’s thesis: 87 pages, 31 figures, 2 tables, 2 appendices, 10 sources.

OPERATING SYSTEM, COMPUTER, POST, BIOS, UEFI

The major goal of this thesis is to improve the process of setting up the basic I / O system of a modern personal computer to facilitate the fastest preliminary testing when turning on its power.

The object of the study is the process of configuring the hardware configuration of a personal computer.

The subject of the study is the basic I / O system, its architecture, functions, and security status.

In order to solve the problem an application with a user-friendly interface based on a minimalist style was created. Four sections were created to facilitate the understanding of the basic input-output system. These parts describe certain parts of the system. The application shows system information about both operating and basic input-output systems and other information, that may be useful for a user. Moreover, a security check was added, so users now can verify their systems on OS level, and change the settings later on, if needed. Also, due to the application, it’s possible to display detailed information about hardware breakdowns and the main functions of a baseboard so a user will get the full picture of the usage of each of them.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

ПЗ – програмне забезпечення

ПЗП – постійний запам’ятовуючий пристрій

ЦП – центральний процесор

BIOS – Basic Input/Output System

CMOS – Complementary Metal-Oxide-Semiconductor

CSM – Compatibility Support Module

GPT – GUID Partition Table

GUID – Globally Unique Identifier

NVRAM – Non-Volatile Random Access Memory

POST – Power On Self Test

UEFI – Unified Extensible Firmware Interface

ROM – Read-Only Memory

LLVM – Low Level Virtual Machine

MBR – Master Boot Record

HDD – Hard Disk Drive

EEPROM – Electrically Erasable Programmable Read-Only Memory

ВСТУП

На сьогодні питання безпеки не втратило свого пріоритету, саме тому, коли проблеми стосуються найголовніших компонентів різноманітних пристроїв та комп’ютерів, ризик підвищується. З покоління в покоління, з року в рік, технології стають все краще та краще, але спеціалісти, які бажають перевіряти ці системи та технології на міцність теж не стоять на місці, та випробовують різноманітні атаки на системи, які у майбутньому можуть принести будь-які винагороди для грабіжників [1].

Компоненти, які будуть описані в цій роботі є basic input/output system (BIOS) та Unified Extensible Firmware Interface (UEFI). Ці компоненти відповідають за завантаження усіх приладів операційної системи, їх налаштування, та перевірка працездатності усіх компонентів задля успішного завантаження системи. UEFI та BIOS є одними з найважливіших компонентів програмного забезпечення (ПЗ), та безпосередньо працюють з прошивками.

UEFI може працювати в 32-бітному або 64-бітному режимах і її адресний простір більший, ніж у BIOS - а значить, швидше завантаження. Також це означає, що екрани налаштування UEFI можна зробити красивішими, ніж у BIOS, включити туди графіку та підтримку миші. Але це необов’язково. Багато комп’ютерів досі працюють з UEFI з текстовим режимом, які виглядають і працюють так само, як старі екрани BIOS.

UEFI та BIOS відносяться до розряду так званого «низькорівневого» програмного забезпечення, яке стартує ще до того, як комп’ютер почне завантажувати операційну систему. UEFI - це більш сучасне рішення і підтримує велику кількість зручних функцій, корисних на сучасних комп’ютерах. Часто буває так, що виробники називають UEFI на своїх комп’ютерах традиційним словом BIOS, щоб не заплутати користувача. Все ж таки між UEFI і BIOS велика різниця, а сучасні комп’ютери в основному комплектуються саме UEFI.

Доволі-таки рідко звичайна людина стикається з роботою, зміною чи оновленням прошивок на своїх девайсах, але навіть спеціалісти з роками досвіду не завжди можуть помітити будь які зміни в оновлених образах. Найгіршим випадком для звичайного користувача може бути втрата усіх персональних даних та вимагання грошей. Однією з цілей цієї роботи є визначення рівня безпеки компонентів базової системи вводу-виводу та її нинішніх аналогів, та можливість поліпшення безпеки компонентів цих систем.

Розуміння роботи компонентів низького рівня потребує багато часу та витримки, але саме після розуміння цільної архітектури усіх компонентів та їх роботи, можуть виконуватись найрізноманітніші атаки.

Сьогодні дуже важко бути впевненим у достовірності продуктів, бо бувають випадки, коли зловмисникам вдавалося змінювати конфігурації чи образи прошивок прямо на складах чи лабораторіях, або безпосередньо при доставці продукту.

Тому, метою кваліфікаційної роботи є покращення процесу налаштування базової системи введення-виведення сучасного персонального комп’ютера для сприяння найшвидшему проведення попереднього тестування при включенні його живлення.

Об’єктом дослідження є процеси налаштування конфігурації апартного забезпечення персонального компютера.

Предметом дослідження є базова система введення-виведення, її архітектура, функції, та стан безпеки.

1 МЕТОДИ УПРАВЛІННЯ BIOS КОМП’ЮТЕРНОЇ СИСТЕМИ

На теперішній час більшість комп’ютерів використовують UEFI, але все ще залишилася частина користувачів з так званим Legacy BIOS. У цьому розділі буде проведений аналіз роботи обох систем, їх порівняння та майбутнє.

1.1 Призначення та використання BIOS

BIOS (Basic Input/Output System) – Базова система вводу/ввиводу, яка виконує низькорівневе обслуговування усіх компонентів комп’ютера, визначення, та установка взаємозв’язку між цими компонентами та режимів іх роботи. Встановлення параметрів BIOS є однією з найсерйозніших проблем, які виникають при зміні конфігурації комп’ютера, наприкад некоректна робота система, чи її зависання[2]. Для початку потрібно виділити причини втручання користувачів до даної системи, наприклад:

- самостійне усунення збоїв та неполадок ПК;
- самостійний «розгін» ПК;
- самостійна зміна конфігурації ПК;
- придбання нового ПК.

BIOS материнської плати (основний BIOS), відповідає за ініціалізацію, тестування та запуск усіх компонентів, а також пошук та подготовку до роботи інші BIOS, які розташовані на накопичувачах, платах розширення, і т.д. Щодо фізичного розташування BIOS, можна сказати що це набір мікросхем постійної пам’яті на рисунку 1.1.

Основні функції BIOS:

- завантаження операційної системи;
- пошук та діагностика обладнання;
- надання інтерфейсу для налаштування обладнання.

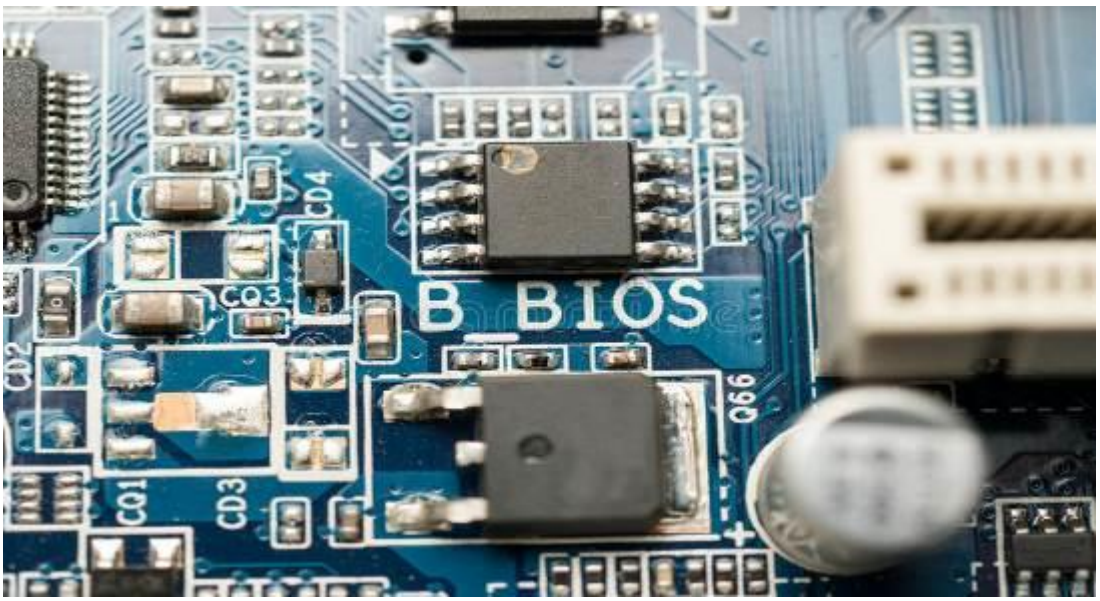

Рисунок 1.1 – Мікросхема, на якій розміщується BIOS

1.2 Принцип роботи BIOS

Стосовно логічної структури, то можна виділити два головні рівня. Перший рівень, Boot Block, являє собою набір підпрограм, необхідних для ініціалізації, де іде перевірка робота тактових генераторів, рівні робочих напруг, температура, та інше. У результаті цього визначається можливість роботи ініціалізуючого пристрою, після чого активується черговий рівень ПЗ. Другий рівень, Main Block, надає сервісні послуги з діагностіки та інколи уникненню різноманітних несправностей. На цьому етапі відбувається фінальна ініціалізація пристрою та виведення результатів самодіагностики Power-On Self-Test (POST). Бувають випадки, коли в результаті дій користувача або збою BIOS перестає працювати [3]. В цей час управління передається спеціальній процедурі, яка називається Crisis Recovery та являє собою функцію відновлення.

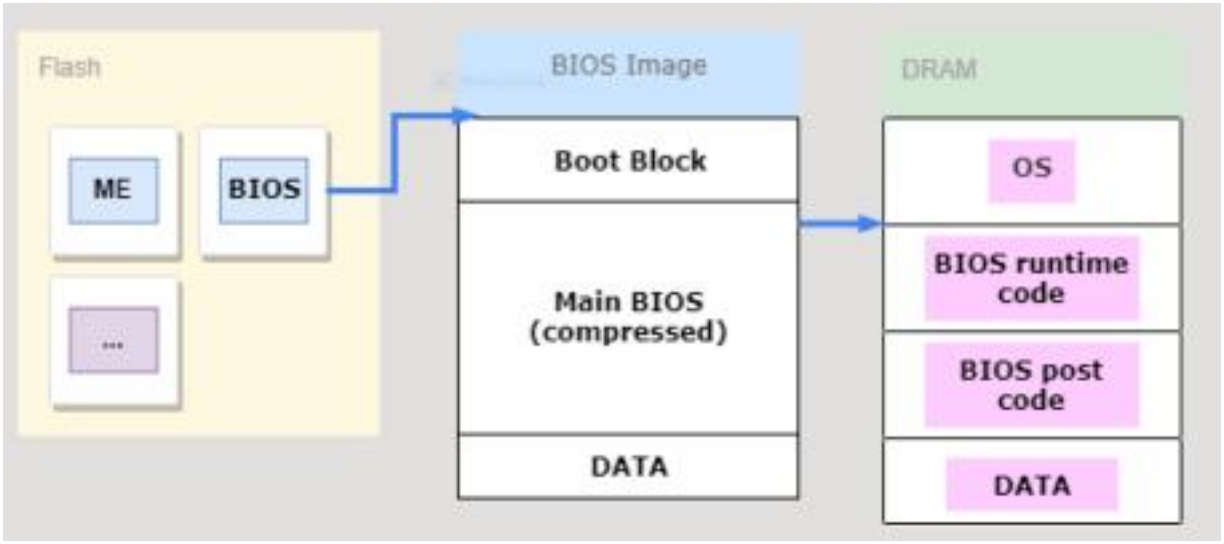

Рисунок 1.2 – Процес розпакування BIOS

Додатково можна відмітити що усі BIOS розділи являються архівом, записаним у форматі LHA. На прикладі Award BIOS можна побачити зміст архіву:

- awardepa.bin – лого;
- acpitbl.bin – підпрограми ACPI;
- awardext.rom - підпрограми BIOS, які відповідають за правильне виведення таблиці про конфігурацію комп’ютера;
- original.tmp – основні програми BIOS;
- vga.rom – відео підпрограми BIOS;
- cpucode.bin – мікрокод.

На етапі запуску комп’ютеру, в першу чергу, електроніка блока живлення проходе етап POST, а після цього вже подає живлення на внутрішні компоненти комп’ютера. Цей процес займає приблизно 0,1-0,5 секунди. На центральний процесор після цих операцій поступає сигнал RESET. Блок живлення, який не пройшов POST, запускатися не буде, саме тому і не буде комп’ютер, у разі успіху, ЦП отримує Power Good сигнал. Зараз ЦП готов до роботи, але йому доступна лише одна програма, стартовий блок, який записаний у схемі ПЗУ. На цьому вже етапі знов відбувається

перевірка стану ЦП та його робочих характеристик, таких як температура, напруження, частота, та інші. Далі, перевірка змісту мікросхеми ПЗУ, яка являється сховищем для стартового блоку та інших підпрограм, які потрібні задля наступних етапів. Як тільки система завершила усі перевірки програм, починається їх запуск. Перед початком будь-якої операції POST генерує спеціальний код, розміром в один байт, та записує його у порт 80h. Якщо виникає помилка, процес діагностіки зупиняється, а цей POST-код, визначає операцію при якій виникла помилка. З минусів POST системи можна виділити той факт, що таблиці з кодами для виробників різних BIOS різні, але потрібну користувачу таблицю можна знайти в інтернеті чи у посібнику.

1.3 Методи управління функціями BIOS

Задля зміни різноманітних параметрів, режимів роботи внутрішніх компонентів та периферійного обладнання мікросхема BIOS обладнана спеціальною програмою, яка називається CMOS Setup Utility. Саме цю програму можна назвати основою BIOS, бо завдяки їй, користувач має змогу конфігурувати комп’ютер [4].

Рисунок 1.3 – AwardBIOS CMOS Setup Utility

Вхід в програму встановлення параметрів можливий тільки після увімкнення чи перезапуску комп’ютера, ініціалізації усіх приладів та проходження тестів. Існує декілька комбінацій клавіш задля відкриття цієї програми, але усі вони залежать від виробника.

При вході в CMOS Setup Utility, на рисунку 1.3, можна побачити сірий або синій екран. Загалом, усі виробники BIOS мають певну структуру розділів, але інколи деякі параметри можуть відрізнятись, що залежить лише від самих виробників.

Розглянемо основні розділи на прикладі найпопулярнішої BIOS – Award BIOS 4.5:

- BIOS Features Setup / Boot – параметри цього розділу дозволяють встановити режим роботи системи, наприклад на рисунку 1.4, порядок запуску системи, робота кеш-пам’яті, процес початкового тестування, та інше;

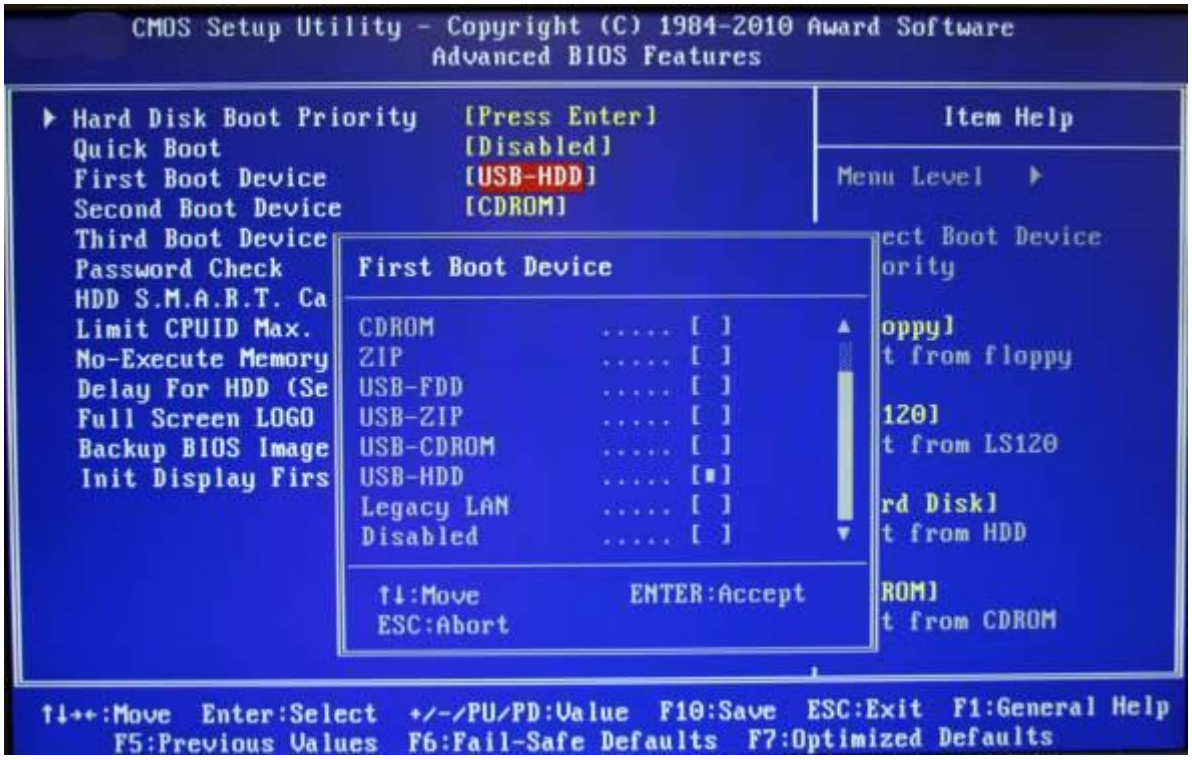

Рисунок 1.4 – Award BIOS CMOS Setup Utility

- Chipset Features Setup / Advanced Chipset Setup / Advanced BIOS Features – параметри даного розділу дозволяють налаштовувати роботу чіпсету материнської плати. Змінюючи ці параметри можна суттєво вплинути на продуктивність комп’ютера. Більшість значень цього розділу встановлюють швидкість роботи компонентів конфігурації відносно частоти роботи материнської плати;

- Frequency / Voltage Control – встановлення тактової частоти та коефіцієнту множення ЦП;

- Hard Disk Utility / HDD Low Format – цей розділ містить програми для роботи з жорсткими дисками, та використовується коли інші засоби відновлення роботоздібності не дають ефекту. Після того як з’явилися жорсткі диски об’ємом більше за 10Гбайт, цей розділ перестали включати до складу BIOS ;

- HDD Auto Detection – цей пункт потрібен для автоматичного визначення фізичних характеристик жорстких дисків IDE стандарту;

- Integrated Peripherals – цей розділ містить параметри, які визначають режими роботи вбудованих контролерів. Параметри цього розділу можуть знаходитись десь інше, так як не усюди цей розділ присутній;

- Load BIOS Defaults / Load Fail Safe / Restore BIOS Defaults – вибір цього пункту загружає найбезопасніші значення усіх параметрів BIOS. Параметри «за замовчуванням» записуються у спеціальну область BIOS, що не перезаписується на заводі, де виставляють найбільш безпечні параметри певної материнської плати;

- Load EEPROM Defaults – цей пункт виконує загрузку змісту CMOS з дискети;

- Load Setup Defaults/Load Performance Defaults/Load Optimized Defaults/Original/Auto Configuration with Power-On Default – виконує встановлення оптімальніших значень параметрів. Встановленні параметри переводят BIOS в стабільний режим роботи, що допоможе запустити комп’ютер після якийсь проблемі, але робота не буде найоптімальнішою;

- Load Turbo Defaults – загрузка найоптимізованіших значень для усіх параметрів BIOS. Дані параметри дозволяють максимально використовувати можливості даного апаратного забезпечення;

- MB Intelligent Tweaker (M.I.T) – цей пункт дозволяє встановити тактову частоту ЦП та відношення тактової частоти оперативної пам’яті до базової частоти ЦП;

- PC Health Status – даний розділ відображає поточні значення температури, напруги та частоти обертання вентиляторів;

- PnP/PCI Configuration – дозволяє налаштовувати тонкощі розподілення ресурсів комп’ютера між платами розширення. У цій секції представлені параметри, за допомогою яких можна налаштувати розподіл обробників переривань на кожен із PCI-слотів, прив’язати переривання до відео- або USB-адаптера тощо;

- Power Management Setup / Power – визначають режими управління електроживленням та режими енергозбереження. Дозволяють також визначити умови переходу з режиму «сну», та вихід з нього;

- Save and Exit Setup / Write To CMOS And Exit – збереження усіх змінених параметрів;

- Save EEPROM Defaults – збереження налаштувань на дискеті;

- Select Language – вибір мови інтерфейсу;

- Set Supervisor Password – дозволяє встановити пароль адміністратора;

- Set User Password - дозволяє встановити пароль користувача;

- Standard CMOS Setup / Main – встановлює стандартні налаштування комп’ютера. Параметри цього розділу дозволяють задавати базову системну інформацію для деяких апаратних засобів, а також встановлювати системну дату та час. Також, тут можна побачати розмір встановленної пам’яті;

- Top Performance – при встановленні цього пункту в Enabled, надає можливість досягнути максимальної продуктивності комп’ютера;

- Exit Without Saving – вихід з програми без збереження встановлених налаштувань.

1.4 Специфікація UEFI

UEFI (Unified Extensible Firmware Interface) - це чиста специфікація інтерфейсу, яка не визначає, як будується мікропрограмне забезпечення платформи, цим займається PI (UEFI Platform Initialization). Стосовно UEFI, то він займається завантаженням та передачею керування наступним рівням керування, наприклад, завантажувачу операційної системи, як зображено на рисунку 1.5. UEFI пропонує багато цікавих можливостей і може мати обмежений час виконання для певного набору програм, замість завантаження повної операційної системи, як Microsoft Windows, Apple OS, Linux[5].

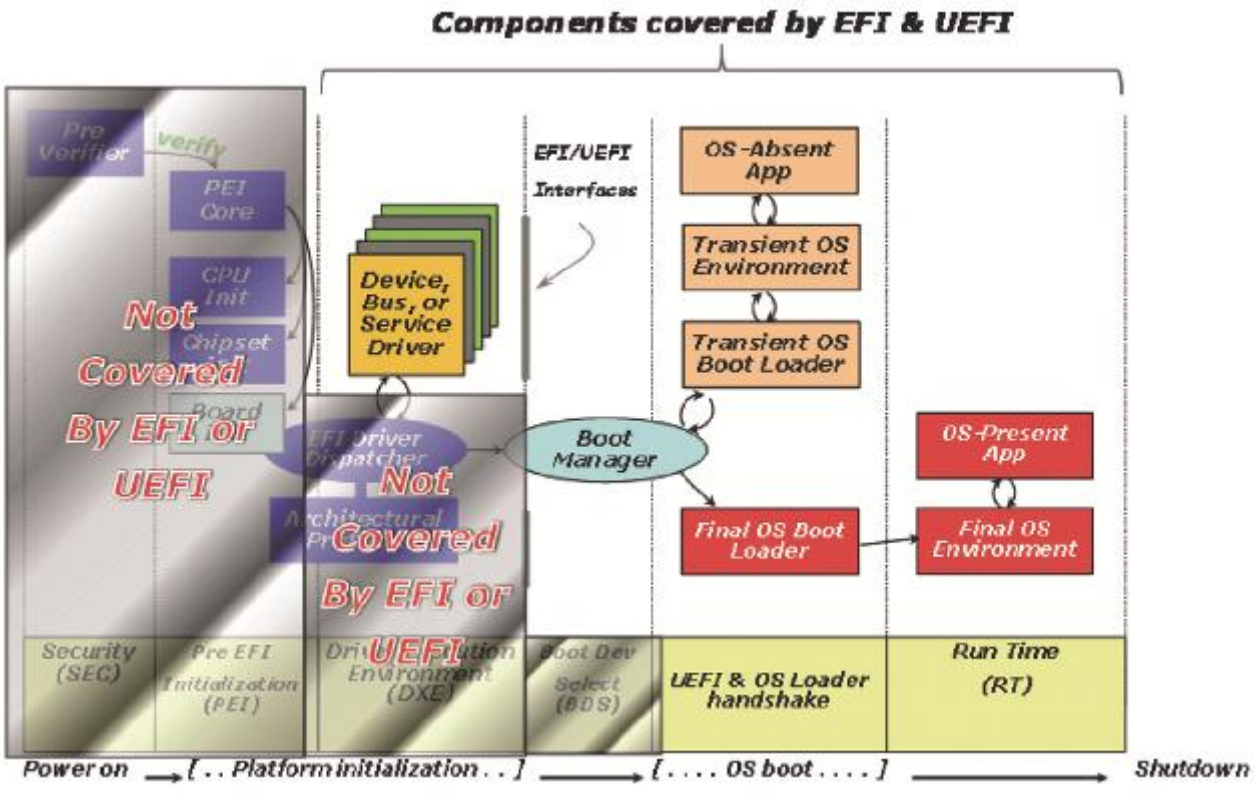

Рисунок 1.5 – Components covered by UEFI

PI, з іншого боку, повинен бути значною мірою непрозорим для пристроїв завантаження до ОС, операційних систем та їх завантажувачів, оскільки він охоплює багато програмних аспектів побудови платформи, які

не мають відношення до цих споживачів. Натомість PI описує етапи керування від скидання платформи до фази успішної роботи, включаючи середовище, сумісне з UEFI, як показано на рисунку 1.6.

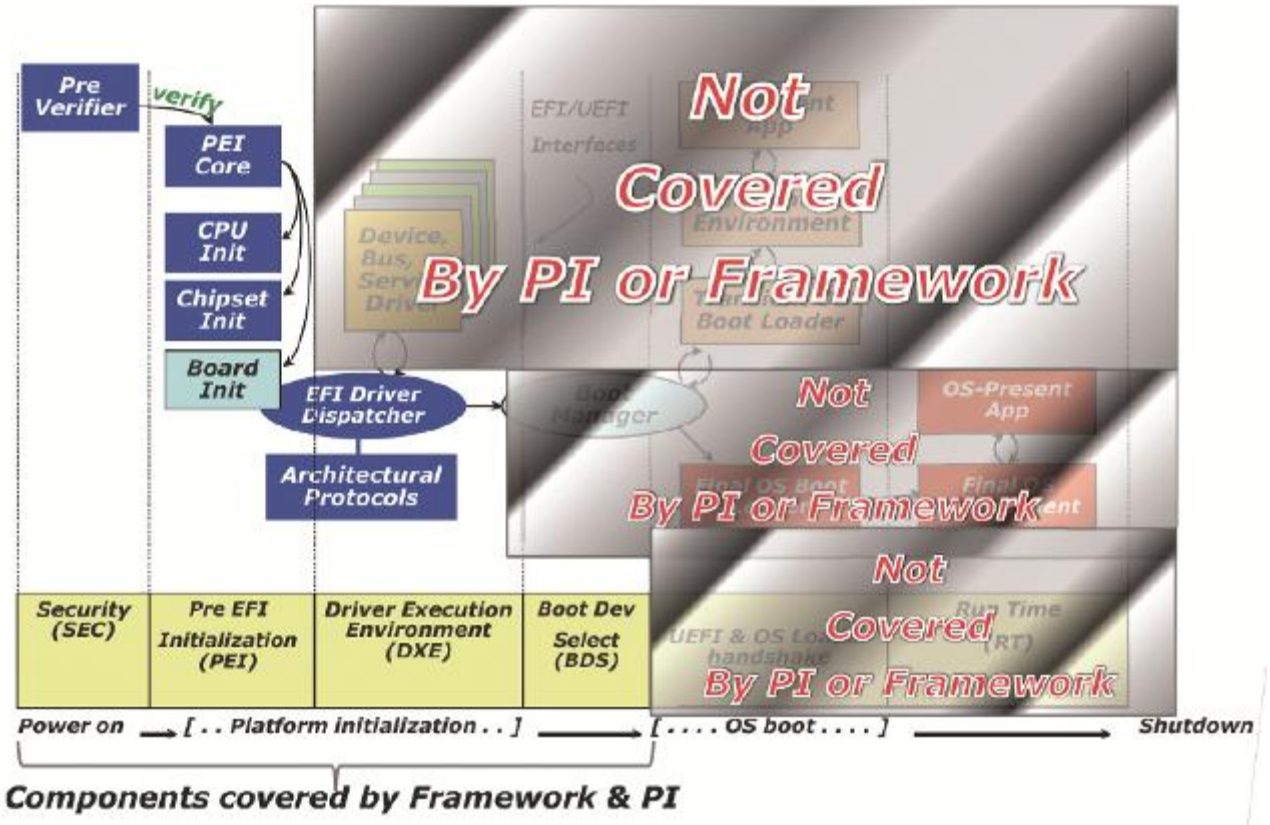

Рисунок 1.6 – Components covered by PI

Помітним аспектом PI є участь різних членів Форуму UEFI. Ці учасники представляють споживачів та виробників технології PI. Кінцевим споживачем компонента PI є постачальник системної плати, включаючи такі компанії, як Apple, Dell, HP, IBM, Lenovo та багато інших. Виробники компонентів PI включають виробників загальної інфраструктури, таких як незалежні постачальники BIOS (IBV), такі як AMI, Insyde, Phoenix та інші. І, нарешті, постачальники, що виробляють набори мікросхем, процесори та інші апаратні пристрої, такі як AMD, ARM та Intel, вироблятимуть драйвери для відповідного обладнання. Якби лише один постачальник мав доступ до

всіх джерел та інтелектуальної власності для створення платформи, реалізація зі статичним зв’язком була б ефективнішою. Але в двадцять першому столітті з різними учасниками апаратного та програмного забезпечення в обчислювальній індустрії програмні технології, такі як PI, є ключовими для ведення бізнесу.

Стосовно UEFI Forum, який є відповідальним за створення специфікацій для UEFI та PI. Також, форум має певну ієрархію, та складається з таких команд:

- UCST (UEFI Configuration sub-team) – Відповідає за всі матеріали, пов’язані з конфігурацією, і відповідає за створення конфігурації UEFI, широко відомої як HII, яка міститься в специфікації UEFI;
- UNST (UEFI Networking sub-team) – Відповідальний за всі матеріали, пов’язані з мережею. Команда відповідала за оновлення/включення матеріалів, пов’язаних з мережею, до специфікації UEFI, зокрема мережевої інфраструктури IPv6;
- USHT (UEFI Shell sub-team) – Відповідає за всі матеріали, пов’язані з командною оболонкою. Команда відповідала за створення специфікації UEFI Shell і продовжує підтримувати вміст у міру розвитку технологій;
- USST (UEFI Security sub-team) – Відповідальний за всі матеріали, пов’язані з безпекою. Команда була за додаткову інфраструктуру безпеки в специфікації UEFI.

На рисунку 1.7 показано, як елементи PI еволюціонують в UEFI. Ліва половина діаграми з SEC, PEI і DXE описана специфікаціями PI, а область специфікації UEFI відповідальна за BDS, UEFI+OS Loader handshake та RT [8].

UEFI має широкий набір учасників. До них належать:

- постачальники операційних систем, які створили інсталятори ОС і середовища виконання на основі UEFI;
- постачальники BIOS, які надають реалізації UEFI;
- виробники платформ, наприклад багатонаціональні корпорації, які

постачають платі, сумісні з UEFI;

- незалежні постачальники програмного забезпечення, які створюють програми та діагностику UEFI;

- незалежні постачальники обладнання, які створюють драйвери для своїх адаптерних карт;

- власники платформ, будь то користувач домашнього ПК або корпоративна IT-компанія, яка повинна адмініструвати систему на основі UEFI.

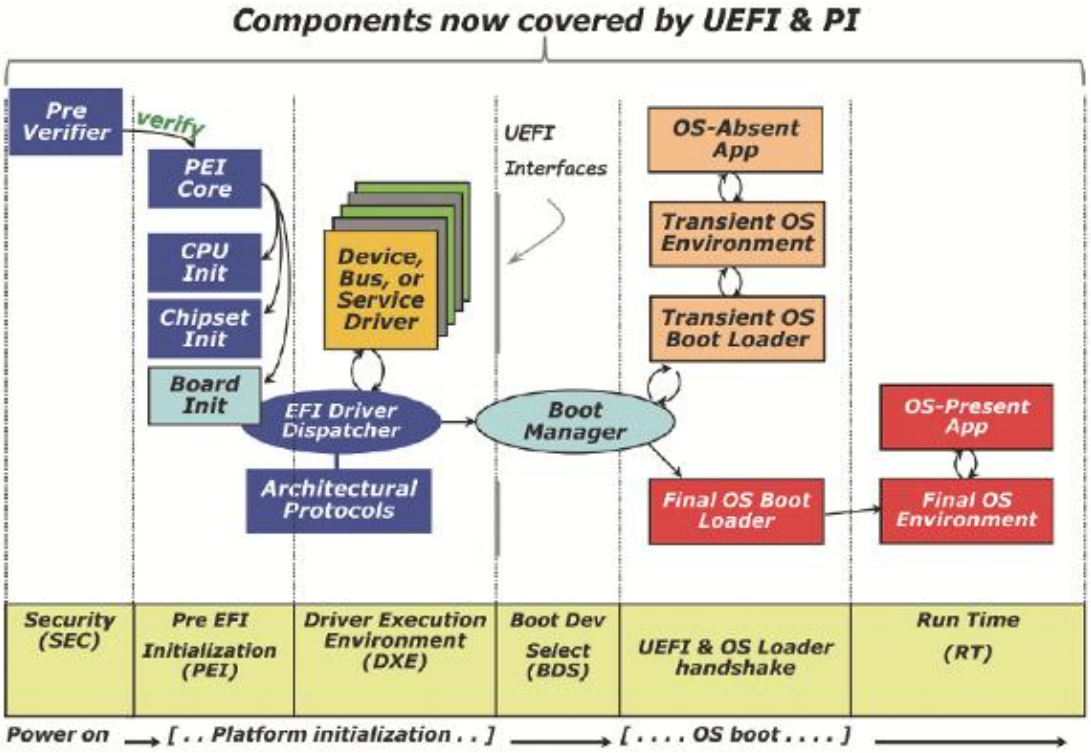

Рисунок 1.7 – Components covered by both UEFI and PI

PI відрізняється від UEFI в тому сенсі, що компоненти PI поставляються під повноваженнями виробника платформи і зазвичай не розширюються третіми сторонами. UEFI, з іншого боку, має змінний розділ файлової системи, змінні завантаження, список завантаження драйверів, підтримку доступних опцій ПЗУ в адаптерах хост-шини (HBA). Таким чином, PI і UEFI пропонують різні питання щодо безпеки.

1.5 Принцип роботи UEFI

UEFI описує програмний інтерфейс до платформи. Платформа включає материнську плату, чіпсет, центральний процесор та інші компоненти. Завантажувачі ОС, діагностика та інші програми, необхідні системі для виконання та взаємодії програм, включаючи драйвери та програми UEFI. UEFI також являє собою чисту специфікацію інтерфейсу, з якою взаємодіють драйвери та програми. Ці архітектурні аспекти включають набір об’єктів та інтерфейсів, описаних у специфікації UEFI. На рисунку 1.8 можна побачити інтерфейс налаштувань в UEFI [6].

Рисунок 1.8 – Settings in UEFI menu

Як і в Legacy BIOS, процесор починає виконувати першу інструкцію в кінці адресного простору за адресою 0xFFFFFFF0. Ця інструкція – стрибок на першу фазу ініціалізації платформи – SEC, яка відповідає за:

- обробку всіх подій перезапуску платформи;
- створення тимчасового сховища пам’яті;
- служіння коренем довіри до системи;
- передачу інформації до PEI Foundation.

Процесори x64/x86 запускаються в 16-бітному реальному режимі, і в процесі первинної ініціалізації BSP перетворюється на 32-бітовий захищений режим. Потім відбувається оновлення мікрокоду всіх доступних процесорів. Слідом відбувається обробка події включення. Під цим мається на увазі агрегація інформації про стани обладнання, щоб на наступній фазі деякі модулі могли зробити висновки про загальний стан платформи.

Під час фази SEC не відбувається ініціалізація оперативної пам’яті, натомість вільний кеш процесора позначається як нескиданий, і він перетворюється на тимчасову оперативну пам’ять. Такий режим називається No-eviction Mode (NEM). У виділеній пам’яті створюється стек, що дозволить модулям із наступних фаз використовувати стекові мови програмування до ініціалізації основної оперативної пам’яті. Далі відбувається ініціалізація всіх прикладних процесорів (AP) із надсиланням ним спеціальної послідовності міжпроцесорних переривань (IPI). Послідовність Init IPI→Start-up IPI пробуджує прикладний процесор і запускає на ньому самотестування (BIST). Результати тестування записуються та передаються далі для аналізу. В кінці фази Security необхідно знайти розділ Boot Firmware Volume (BFV), на якому розташовується код наступної фази, а також по можливості знайти інші, неосновні, розділи з кодом (FV). Щоб виправдати назву фази Security та стати коренем довіри, під час виконання цієї фази код, який очікує управління, може бути перевірений на відсутність несанкціонованих змін та шкідливих частин програми. Фаза попередньої ініціалізації (PEI), описана в специфікаціях PI Architecture, викликається досить рано в процесі завантаження. Зокрема, після попередньої обробки на етапі безпеки (SEC) будь-яка подія перезапуску машини викликає фазу PEI. Фаза PEI спочатку працює з платформою в стані зародження, використовуючи лише ресурси

процесора, такі як кеш процесора, стек викликів для розсилки модулів ініціалізації Pre-EFI (PEIM), які відповідають за:

- ініціалізацію деякого постійного доповнення пам’яті;
- опис пам’яті в блоках Hand-Off (HOBs);
- опис розташування томів мікропрограм у HOB;
- передачу керування у фазу середовища виконання драйвера (DXE).

Завдання фази Pre-EFI Initialization полягає у збиранні інформації про підключені пристрої та підготовку мінімально необхідної кількості обладнання для запуску процесу повної ініціалізації. За своїм задумом фаза PEI має бути легковажною, оскільки пам’ять процесорного кешу обмежена. Крім цього, у фазі PEI може відбуватися відновлення після збою, тому є потреба розміщувати код фази PEI у більш відмовостійкому сховищі.

Перед фазою DXE фаза Pre-EFI Initialization (PEI) відповідає за ініціалізацію постійної пам’яті в платформі, щоб фаза DXE могла бути завантажена та виконана. Стан системи в кінці фази PEI передається на фазу DXE через список незалежних від позиції структур даних, які називаються блоками передачі даних (HOB). HOB детально описані в Специфікації ініціалізації платформи. У фазі DXE є кілька компонентів:

- DXE Foundation;
- диспетчер DXE;
- набір драйверів DXE.

Завдання фази Driver Execution Environment (DXE) зводиться до ініціалізації пристроїв, що залишилися. До моменту старту фази DXE процесор і основна пам’ять вже готові до роботи, а на драйвери DXE не накладаються суворі обмеження споживаних ресурсів. Аналогічно PEI Foundation у цій фазі є власне ядро - DXE Foundation. Ядро створює необхідні інтерфейси та завантажує три види DXE сервісів:

- UEFI Boot Services - сервіси часу завантаження;
- UEFI Runtime Services - сервіси часу виконання;
- DXE Services – спеціальні сервіси, необхідні ядру DXE.

Після ініціалізації сервісів розпочинає роботу DXE Dispatcher. Він знаходить та завантажує DXE драйвери, які, у свою чергу, завершують ініціалізацію обладнання. Серед безлічі драйверів, що завантажуються на процесорах x64/x86 варто приділити увагу драйверу System Management Mode Init (SMM Init). Цей драйвер готує все для роботи системного керування (System Management Mode, SMM). SMM – це особливий привілейований режим, який дозволяє призупинити виконання поточного коду та виконати програму із захищеної області пам’яті SMRAM у власному контексті.

Додатково відзначимо модуль Compatibility Support Module (CSM), який забезпечує сумісність із Legacy та дозволяє завантажувати ОС без підтримки UEFI. Після ініціалізації всього обладнання настає час вибору завантажувального пристрою.

Фаза вибору завантажувального пристрою (BDS) реалізується як частина архітектурного протоколу BDS. DXE Foundation передасть управління архітектурному протоколу BDS після того, як усі драйвери DXE, чиї залежності були задоволені, будуть завантажені та виконані диспетчером DXE. Фаза BDS відповідає за наступне:

- ініціалізація консольних пристроїв;
- завантаження драйверів пристроїв;
- спроба завантажити та виконати вибір завантаження.

Пошуком завантажуваних областей на пристроях займається Boot Manager. На деяких картах розширення, наприклад, на мережних картах і RAID-контролерах, може бути власний BIOS, званий Option ROM, або OpROM. Вміст OpROM пристроїв запускаються відразу після виявлення, а після виконання керування повертається до Boot Manager. Усі розділи, на яких знаходяться завантажувані області, зберігаються в пам’яті менеджера завантаження та впорядковуються відповідно до порядку завантаження. Якщо жодна програма не знайшлася, Boot Manager може викликати диспетчер DXE, на випадок якщо за час пошуків диспетчер завантажив

додаткові драйвери і менеджеру завантаження можуть відкритися нові пристрої.

Після опитування всіх пристроїв та пошуку областей завантаження Boot Manager починає завантажувати в порядку пріоритету завантаження. У загальному випадку управління передається до UEFI-додатку, який починає виконувати свою логіку. Однак для систем із сумісністю з Legacy режимом у списку завантажувальних областей може знайтися накопичувач з розміткою MBR і доведеться звертатися до CSM, модуля підтримки сумісності. Модуль CSM дозволяє запускати операційні системи, які не підтримують UEFI. Для завантаження таких ОС модуль CSM емулює оточення, яке потрапляє ОС:

- завантажує Legacy-драйвер;
- завантажує Legacy BIOS;
- переводить відеовиведення у сумісний з Legacy режим;
- створює у пам’яті необхідні для Legacy структури даних, відсутні в UEFI;
- завантажує драйвер CompatibilitySmm для роботи SMM у Legacy.

Нагадаємо, що в Legacy-режимі завантаження ОС починається в 16-бітному режимі, тоді як у UEFI все працює в 32-бітному режимі. CSM запускає Legacy-завантажувач у 16-бітному режимі та за необхідності забезпечує зв’язок з 32-бітними UEFI-драйверами.

Початок завантаження ОС чи Legacy-завантажувача призводить до початку фази Run Time(RT). У цій фазі всі послуги DXE (крім UEFI Runtime Services) перестають бути доступні. Вміст фази RT може бути різним. Тут може бути звичний по Legacy завантажувач ОС - наприклад, GRUB2 або Windows Boot Manager, який переводить процесор у 64-бітний режим і запускає ОС. Але можуть бути й самостійні програми або відразу ядро операційної системи. Ядро Linux, починаючи з версії 3.3, за наявності прапора CONFIG_EFI_STUB перетворюється на звичайну UEFI-додаток і може бути запущено з UEFI без використання сторонніх завантажувачів. Як і у випадку з Legacy BIOS, завантажувачеві або самому ядру необхідно

перевести процесор в 64-бітовий режим, завантажити всі драйвера, налаштувати планувальник і запустити init. Init, своєю чергою, запускає процеси у просторі користувача, після чого з’являється вікно логіна в ОС.[9]

Фаза After Life (AL) складається з постійних драйверів UEFI, які використовуються для збереження стану системи під час впорядкованого вимкнення ОС, сну, режиму глибокого сну або перезапуску.

1.6 Порівняння BIOS та UEFI при еволюційному розвитку

BIOS існує вже давно і еволюціонував мало. Навіть у комп’ютерів з ОС MS-DOS, випущених 1980-х, був BIOS. Звичайно, з часом BIOS таки змінювався і покращувався. Розроблялися його розширення, зокрема, ACPI, Advanced Configuration and Power Interface (удосконалений інтерфейс керування конфігурацією та живленням). Це дозволяло BIOS простіше налаштовувати пристрої та більш досконало керувати живленням, наприклад, йти в сплячий режим. Але BIOS розвинувся не так сильно, як інші комп’ютерні технології з часів MS-DOS. У традиційного BIOS досі є серйозні обмеження. Він може завантажуватись лише з жорстких дисків об’ємом не більше 2,1 Тб. Зараз вже повсюдно зустрічаються диски на 3 Тб, і з них комп’ютер із BIOS не завантажиться. Це обмеження BIOS MBR. BIOS повинен працювати у 16-бітному режимі процесора і йому доступний лише 1 Мб пам’яті[10]. Він має проблеми з одночасною ініціалізацією декількох пристроїв, що веде до уповільнення процесу завантаження, під час якого ініціалізуються всі апаратні інтерфейси та пристрої.

UEFI замінює традиційний BIOS на PC. На існуючому PC неможливо поміняти BIOS на UEFI. Потрібно купувати апаратне забезпечення, яке підтримує UEFI. Більшість версій UEFI підтримують емуляцію BIOS, щоб ви могли встановити і працювати зі застарілою ОС, яка очікує на наявність BIOS замість UEFI - так що зворотна сумісність у них є. Новий стандарт обходить обмеження BIOS. Прошивка UEFI може вантажитися з дисків

об’ємом понад 2,2 Тб – теоретична межа для них становить 9,4 зеттабайт. Це приблизно втричі більше за всі дані, що містяться в сьогоднішньому Інтернеті (рисунок 1.9).

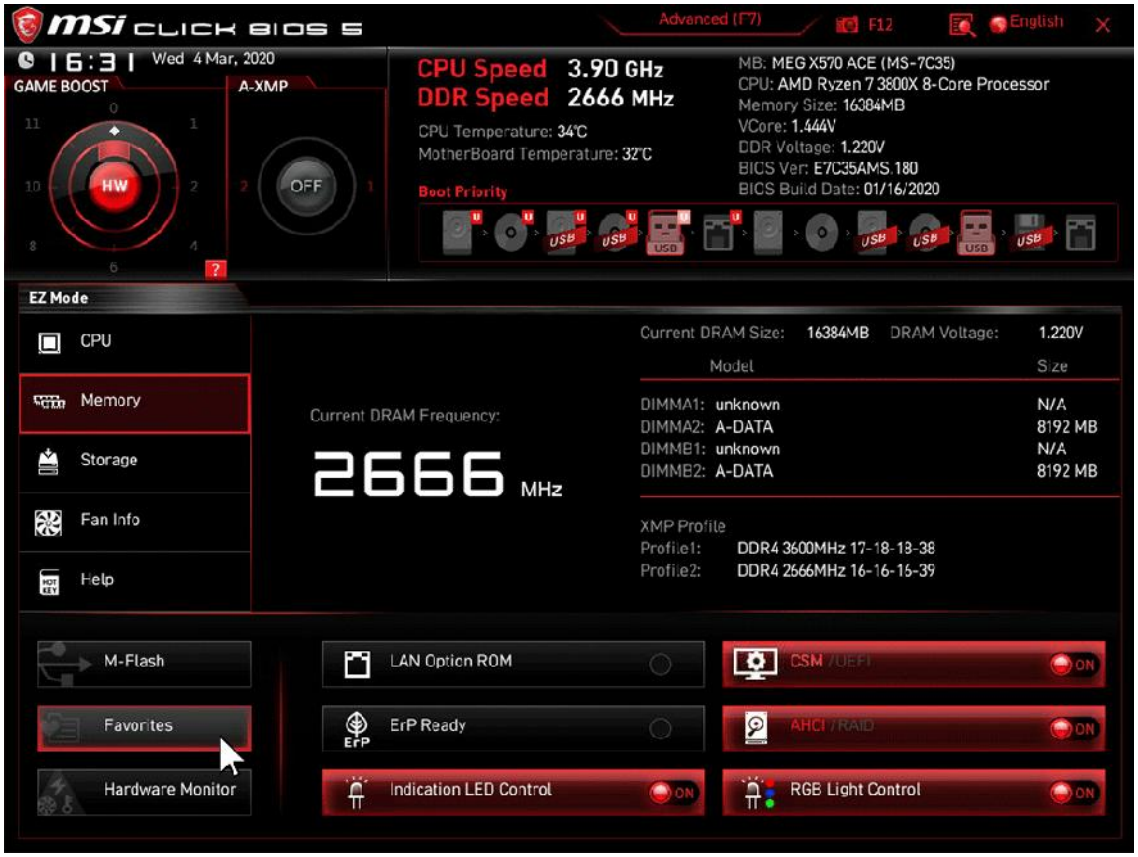

Рисунок 1.9 – UEFI interface

UEFI підтримує такі обсяги через використання розбивки на розділи GPT замість MBR. Також у неї стандартизований процес завантаження, і вона запускає програми EFI, що виконуються замість коду, розташованого в MBR. UEFI може працювати в 32-бітному або 64-бітному режимах і його адресний простір більше, ніж у BIOS - а значить, швидше завантаження. Також це означає, що екрани налаштування UEFI можна зробити красивішими, ніж у BIOS, включити туди графіку та підтримку миші. Але це необов’язково. Багато комп’ютерів досі працюють з UEFI з текстовим режимом, які виглядають і працюють так само, як старі екрани BIOS.

У UEFI вбудовано багато інших функцій. Вона підтримує безпечний

запуск Secure Boot, в якому можна перевірити, що завантаження операційної системи не змінила жодна шкідлива програма. Вона може підтримувати роботу по мережі, що дозволяє проводити віддалене налаштування та налагодження.

У випадку з традиційним BIOS для налаштування комп’ютера необхідно сидіти прямо перед ним. І це не просто заміна BIOS. UEFI - це невелика операційна система, що працює над прошивкою PC, тому вона здатна набагато більше, ніж BIOS. Її можна зберігати у флеш-пам’яті на материнській платі або завантажувати з жорсткого диска або мережі. У різних комп’ютерах буває різний інтерфейс та властивості UEFI. Все залежить від виробника комп’ютера, але основні можливості однакові у всіх.

2 ПРОГРАМНІ МЕТОДИ ПОШУКУ ТА УСУНЕННЯ НЕСПРАВНОСТЕЙ

Несправності в комп’ютері можуть виникни завдяки багатьом причинам, але треба виділити основні: встановлення невірних режимів роботи компонентів комп’ютера та поломки одного з декількох його компонентів. Ідеальним варіантом пошуку причини нестійкої роботи комп’ютера є така послідовність дій:

- перевірка Defaults CMOS Setup у розділі CMOS Setup Utility. Це дозволить завантажити значення усіх параметрів, вибраних заводом-виробником материнської плати як найоптимальніші;
- коректне встановлення усіх необхідних компонентів комп’ютеру;
- перевірка драйверів, видалення та оновлення;
- тестування компонентів комп’ютера різними програмами типу SiSoft Sandra Pro, Dr. Hardware тощо (рисунок 2.1, 2.2).

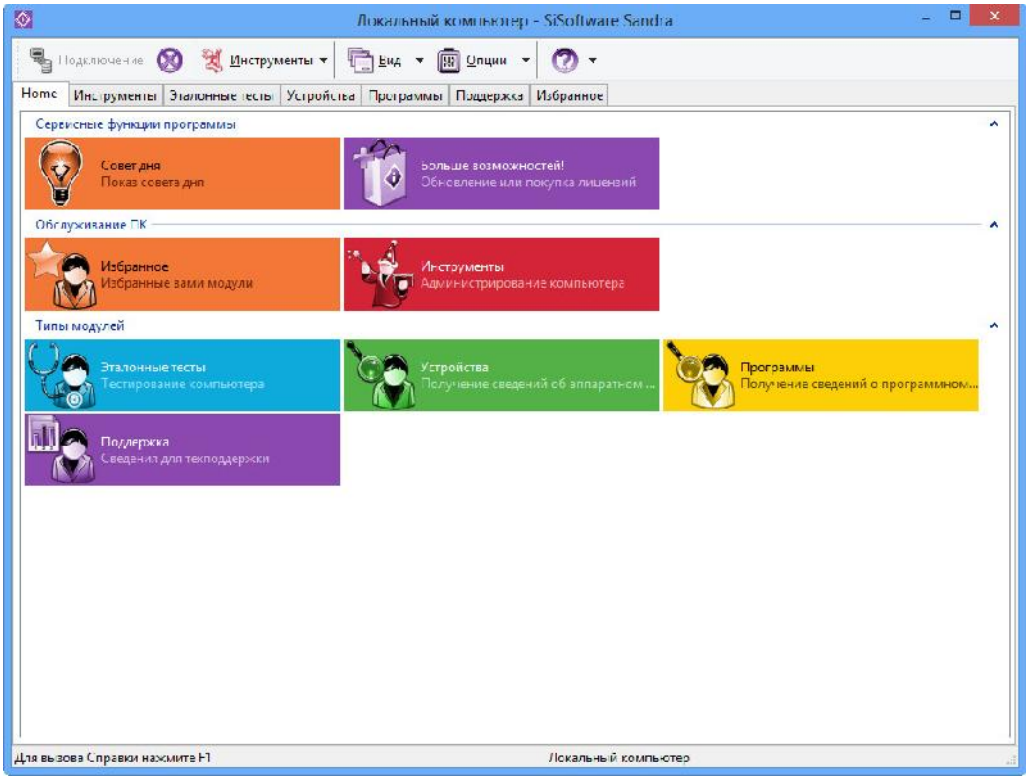

Рисунок 2.1 – Головне вікно застосунку SiSoft Sandra Pro

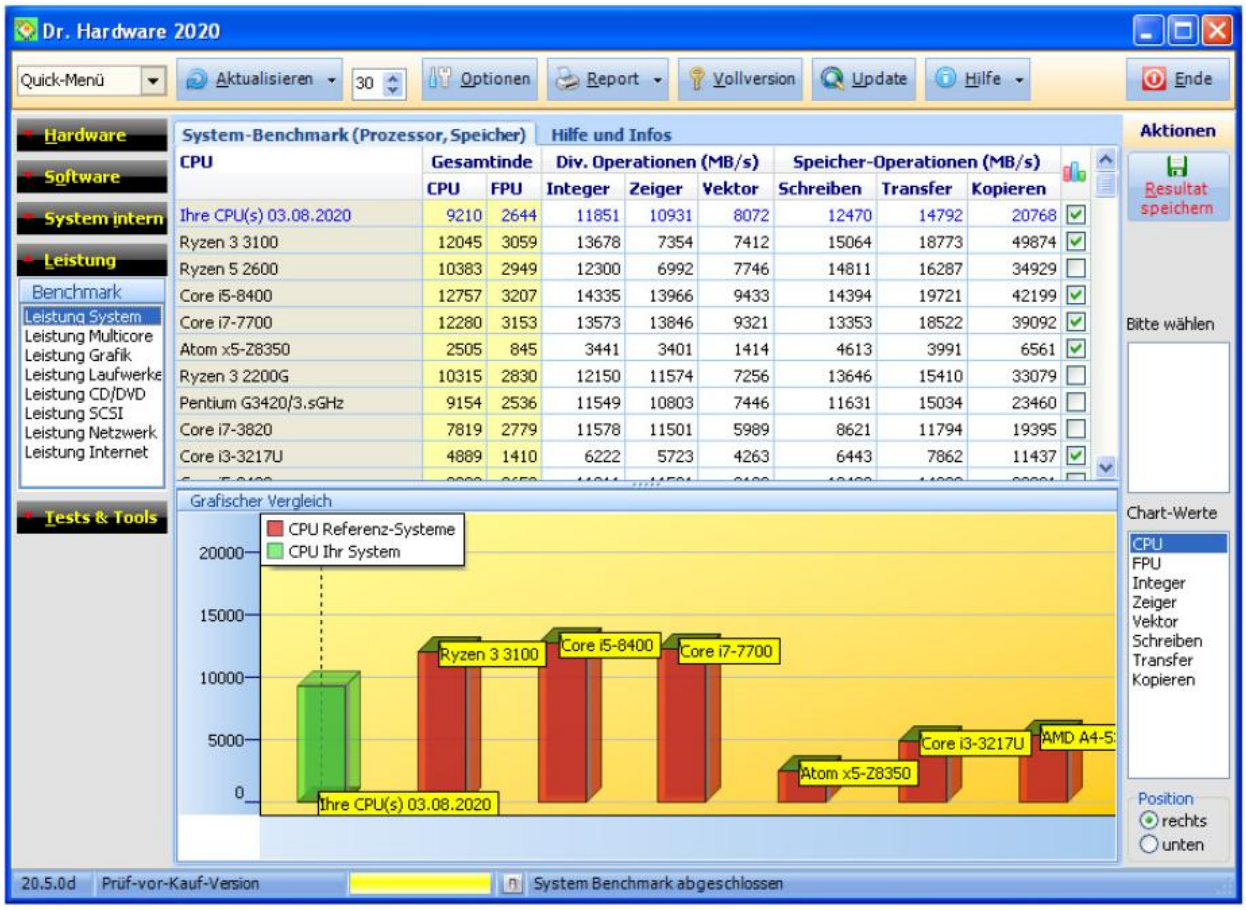

Рисунок 2.2 – Головне вікно застосунку Dr. Hardware

Зазвичай вже на цьому етапі виявляються компоненти, що нестабільно працюють. Слід пам’ятати, що неявні проблеми як зависання комп’ютера чи несанкціонованої перезавантаження найчастіше виникають через нестабільно працюючої материнської плати. Всі інші компоненти здебільшого ламаються відразу.

Якщо несправність локалізувати не вдається, найкращим варіантом буде перевірка всіх комплектуючих на справному комп’ютері. Тобто досліджувані компоненти встановлюються в комп’ютер, що нормально працює.

Коли комп’ютер не піддається налаштуванню програмними методами або взагалі не завантажується, послідовність дій користувача має бути такою:

- вимкнення комп’ютеру та від’єднання від системного блоку всіх пристроїв;

- зняття кришки з системного блоку і видалення пилу, що накопичився;

- перевірка якості встановлення усіх плат розширення та модулів пам’яті у слотах;

- перевірка якості кріплення з’єднувальних шлейфів та роз’ємів живлення;

- обнулення вмісту CMOS-пам’яті.

Якщо комп’ютер, як і раніше, не вмикається, потрібне відключення від материнської плати усіх пристроїв, крім ЦП. Після цього, підключення комплектуючих. Після підключення кожного пристрою 0fслід увімкнути комп’ютер і перевірити його працездатність. Спочатку орієнтуватися можна буде лише за звуковими сигналами, що видаються системним динаміком, тому перевірте його підключення до материнської плати. Якщо комп’ютер не вмикається навіть у мінімальному комплекті, причина несправності криється в блоці живлення, або в материнській платі, або в ЦП.

2.1 Програма Power-On Self-Test

POST (Power-On Self-Test) – самотестування після включення. При включенні перевіряються апаратні вузли комп’ютера за допомогою програм, які ініціалізуються BIOS системної плати. POST та аналогічні функції, присутні у всіх сучасних електронних пристроях, наприклад, КПК, планшетах, смартфонах та ін.

Скорочений тест POST:

- перевірка цілісності програми BIOS у постійній пам’яті (ПЗП) за допомогою контрольної суми;

- пошук та включення основної частини системних шин, контролерів та підключених пристроїв (відеокарти, дисководів тощо), а також виконання програм, що входять до BIOS пристроїв для самоініціалізації;

- підрахунок обсягу оперативної пам’яті (ОЗП) та перевірка 1-го

сегмента (64 кілобайт).

Повний тест POST:

- тест регістрів процесора CPU;
- тест контрольної суми ПЗП;
- тест системного таймера та порту звукової сигналізації;
- перевірка контролера прямого доступу до пам’яті;
- перевірка регенератора оперативної пам’яті;
- перевірка нижньої області ОЗУ для проектування резидентних програм у BIOS;
- запуск резидентних програм;
- перевірка стандартного графічного адаптера (VGA);
- перевірка оперативної пам’яті;
- перевірка основних пристроїв уведення;
- перевірка CMOS;
- перевірка основних портів LPT/COM;
- перевірка накопичувачів дисководів (CD або DVD-привід);
- перевірка накопичувачів жорстких дисків (HDD);
- самотестування функціональних підсистем BIOS;
- передача керування завантажувачу.

2.1.1 Принцип роботи POST

Моніторинг старту здійснюється за допомогою спеціальних плат – контролерів стану порту 0080h. На рисунку 2.3 зображена одна з так званих POST-плат, які призначені для захоплення діагностичних кодів та їх наглядного відображення на цифровому індикаторі, що дозволяє виконувати ранню діагностику до запуску операційної системи.

Рисунок 2.3 – POST-плата

У деяких комп’ютерних системах для діагностичних цілей використовується порт із номером, відмінним від 0080h. Так, у системних платах із архітектурою EISA для діагностичних цілей використовується порт 0300h. Останнім часом виробники серйозніше стали ставитися до ідеї загальної стандартизації, так що особливих проблем ви не відчуватимете, адже старі комп’ютери зустрічаються дедалі рідше.

Існують три основні типи POST-плат:

- плати, які вимагають своєї роботи установки замість BIOS материнської плати, точніше замість мікросхеми, інший мікросхеми, що містить діагностичні програми. Наприклад, у такий спосіб працює технологія Lite BIOS. Індикація процесу діагностики зазвичай здійснюється на звичайній POST-платі. Коди, природно, будуть характерними для застосовуваної технології;

- "натуральні" POST-плати, що відображають інформацію, до якої їм вдається отримати доступ. За допомогою таких плат визначають вузол, в якому стався збій (наприклад, якщо це підсистема оперативної пам’яті, слід змінити модуль пам’яті, використовуваний слот і т. п.);

- плати, здатні емулювати частину функцій будь-якого вузла

материнської плати (наприклад, PHD PCI). Такі плати дозволяють отримати докладнішу інформацію про стан компонентів ПК, тимчасово обійтися без відеоконтролера, провести повну перевірку накопичувачів тощо.

2.1.2 Послідовність звукових сигналів

Як правило, для визначення того компонента, який викликає проблему, необхідно лише порахувати кількість сигналів, що видаються системним динаміком. У таблиці 2.1 наведено звукові сигнали та описи помилок, що видаються BIOS AMI.

Таблиця 2.1 – Звукові сигнали AMI BIOS

Сигнал	Опис
1 короткий	Помилок не виявлено
2 коротких	Помилка парності ОЗП
3 коротких	Помилка в перших 64Кб ОЗП
4 коротких	Несправність системного таймеру
5 коротких	Проблеми з CPU
6 коротких	Помилка ініціалізації контролеру клавіатури
7 коротких	Проблеми з материнською платою
8 коротких	Помилка пам’яті відеокарти
9 коротких	Контрольная сума BIOS невірна
10 коротких	Помилка запису в CMOS
11 коротких	Помилка кешу, розташованого на материнській платі
1 довгий, 1 короткий	Проблеми з блоком живлення
1 довгий, 2 коротких	Помилка відеокарти (Mono-CGA)
1 довгий, 3 коротких	Помилка відеокарти (EGA-VGA)
1 довгий, 4 коротких	Відсутність відеокарти
1 довгий, 8 коротких	Проблеми з відеокартою або монітор не підключений

Продовження таблиці 2.1

Сигнал	Опис
3 довгих	ОЗУ – тест зчитування/запису завершено з помилкою
Відсутній та пустий екран	Несправний процесор
Неперервний	Несправність блока живлення або перегрів комп’ютера

У таблиці 2.2 зображені звукові сигнали для Award BIOS.

Таблиця 2.2 – Звукові сигнали Award BIOS

Сигнал	Опис
1 короткий	Успішний POST
2 коротких	Незначні помилки
3 довгих	Помилка контролеру клавіатури
1 короткий, 1 довгий	Помилка ОЗП
1 довгий, 2 коротких	Помилка відеокарти
1 довгий, 3 коротких	Помилка клавіатури
1 довгий, 9 коротких	Помилка при зчитувані з ПЗП
Повторювальний короткий	Проблеми з ОЗП чи блоком живлення
Повторювальний довгий	Проблеми з ОЗП
Непреривний	Проблеми з блоком живлення

2.2 Візуальна інформація про несправності

Цей спосіб POST користується на додаток до звукових сигналів, якщо відеосистема комп’ютера справна. При цьому на екрані з’являється повідомлення, що коротко описує несправність, і код помилки. За кодом несправність можна вивчити детальніше, скориставшись документацією до материнської плати або BIOS. За допомогою текстових повідомлень

комп’ютер інформує лише про незначні помилки. Перелік можливих текстових повідомлень:

- 8042 Gate A20 Error - Не вдається проініціалізувати контролер клавіатури (цифра 8042 позначає тип мікросхеми, що зазвичай використовується для даного контролера, A20 позначає номер адресної лінії, яка зазвичай використовується для організації роботи клавіатури). Перезавантажте комп’ютер за допомогою кнопки RESET на системному блоці або на деякий час ви ключите комп’ютер. Якщо несправність після цього не зникла, швидше за все доведеться замінити материнську плату;

- Address Line Short - Виявлено коротке замикання однієї чи кількох ліній адресної шини. Уважно огляньте материнську плату, попередньо знявши всі плати розширення і відключивши з’єднувальні шлейфи. При необхідності витягніть її з корпусу, щоб переконатися, що під нею немає металевих предметів, шматків припою, які можуть відвалитися від самої плати при неякісному паянні. Можна спробувати "про пилососити" материнську плату звичайним пилососом, щоб видалити всі можливі шматочки припою (думаю, все-таки краще таким ось нетрадиційним чином "реанімувати" плату, ніж міняти її);

- BIOS ROM Checksum Error - В результаті проходження програми діагностики POST виявлено помилку в контрольній сумі вмісту мікросхеми BIOS, роботу комп’ютера при цьому було зупинено. Якщо на материнській платі використовується так звана технологія Dual - BIOS , то спробуйте відновити вміст мікросхеми. Для того щоб дізнатися, як правильно це зробити, прочитайте документацію на вашу материнську платню. А якщо ні, то для відновлення інформації в BIOS вам доведеться скористатися програматором. У разі повторної появи цієї помилки спробуйте замінити акумулятор, що живить мікросхему CMOS-пам’яті, яка є логічною частиною BIOS (при тестуванні програма діагностики POST розглядає її як єдине ціле з основною мікросхемою BIOS). Причиною може послужити деструктивний вплив якогось вірусу (наприклад, Worm. Magistr) (рисунок 2.4);

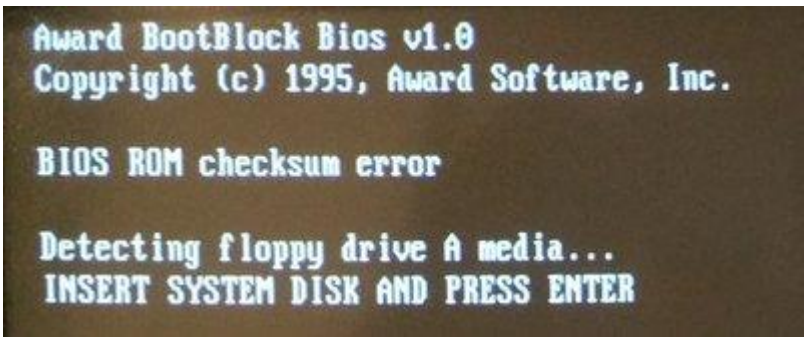

Рисунок 2.4 – BIOS ROM checksum error

- BIOS Update For Installed CPU Failed - Виникла помилка при спробі оновлення мікрокоду центрального процесора. Це може статися через невідповідність версії BIOS материнської плати та конкретної моделі центрального процесора. При цьому спроба BIOS виправити помилки, що фактично не існують, в архітектурі ядра процесора (для чого функція BIOS Update і призначена) може призвести до появи нових, у тому числі і фатальних помилок. Поверніть колишню версію BIOS або знайдіть в Інтернеті більш нову версію, що "прошита" в даний момент, швидше за все, цей недолік в ній вже виправлений;

- Bad PnP Serial ID Checksum – В результаті проходження самодіагностики програмою POST була виявлена помилка в контрольній сумі ідентифікатора одного з пристроїв Plug and Play. Перевірте якість встановлення всіх плат розширення. Щоб переконатися в якості контакту, витягніть і знову встановіть усі плати. Якщо таким чином не вдається усунути появу повідомлення, доведеться замінити "винний" у цьому пристрої;

- Boot Error – Press <F1> To Retry – Програма самодіагностики POST не виявила жодного завантажувального диска. Запустіть програму CMOS Setup Utility і перевірте значення всіх параметрів, які стосуються встановлених на комп'ютері жорстких дисків і дисководів. За необхідності перевірте надійність кріплення всіх з'єднувальних шлейфів та роз'ємів живлення жорстких дисків та дисководів;

- Bus Time-Out NMI At Slot X – Плата розширення, встановлена в слоті розширення номер X, не реагує на немаскируемое переривання протягом тривалого часу, до речі, що має чималий пріоритет серед всіх процесів, що відбуваються всередині комп'ютера. Спробуйте перезавантажити комп'ютер за допомогою кнопки RESET на системному блоці або на деякий час вимкнути його. Дійсно для шини EISA;

- Cache Memory Bad – Помилка ініціалізації кеш-пам'яті. Якщо на вашому комп'ютері вона виконана у вигляді окремих модулів (кеш-пам'ять 3-го рівня), спробуйте змінити модулі або хоча б витягнути їх і встановити назад, попередньо очистивши від пилу всі роз'єми. Якщо кеш-пам'ять інтегрована в центральний процесор, тоді вам доведеться, як мінімум, перевірити якість його охолодження (для тих процесорів, які виконані в конструктиві Slot I/A, слід перевіряти рівень нагріву саме для мікросхем кеш-пам'яті, розташованих на процесорній платі). Якщо перелічені заходи не дають жодного штибу, швидше за все, доведеться змінювати сам процесор, хоча не виключено, що неполадка зникне після перезавантаження за допомогою кнопки RESET на системному блоці або вимкнення комп'ютера на деякий час;

- Cache Memory Bad, Do Not Enable Cache – Помилка ініціалізації кеш-пам'яті, кеш-пам'ять вимкнена. Якщо на вашому комп'ютері вона виконана у вигляді окремих модулів (кеш пам'ять 3-го рівня), спробуйте поміняти модулі або хоча б витягнути їх і встановити назад, попередньо очистивши всі роз'єми від пилу. Якщо кеш-пам'ять інтегрована в центральний процесор, тоді вам доведеться, як мінімум, перевірити якість його охолодження (для тих процесорів, які виконані в конструктиві Slot I/A, слід перевіряти рівень нагрівання саме для мікросхем кеш-пам'яті, розташованих на процесорній платі). Якщо перелічені заходи не дають жодного штибу, швидше за все, доведеться змінювати сам процесор, хоча не виключено, що неполадка зникне після перезавантаження за допомогою кнопки RESET на системному блоці або вимкнення комп'ютера на деякий час;

- CH-2 Timer Error – Виникла помилка під час ініціалізації другого таймера. Дане повідомлення може з’явитися тільки в тому випадку, якщо на материнській платі встановлено два таймери. Спробуйте на деякий час вимкнути комп’ютер або перезавантажити його за допомогою кнопки RESET на системному блоці. Повідомлення може бути викликане некоректною роботою деяких периферійних пристроїв, тому на час діагностики відключіть все зайве від системного блоку;

- CMOS Battery Failed – Розрядився акумулятор, що живить мікросхему CMOS-пам’яті (є ймовірність, що несправність виникла через поганий контакт у ланцюгу живлення). Встановіть новий акумулятор. За потреби "продзвоніть" пробником усі контакти в ланцюзі живлення;

- CMOS Battery State Low – Розрядився акумулятор, що живить мікросхему CMOS-пам’яті (є ймовірність, що несправність виникла через поганий контакт у ланцюгу живлення). Встановіть новий акумулятор. За потреби "продзвоніть" пробником усі контакти в ланцюзі живлення;

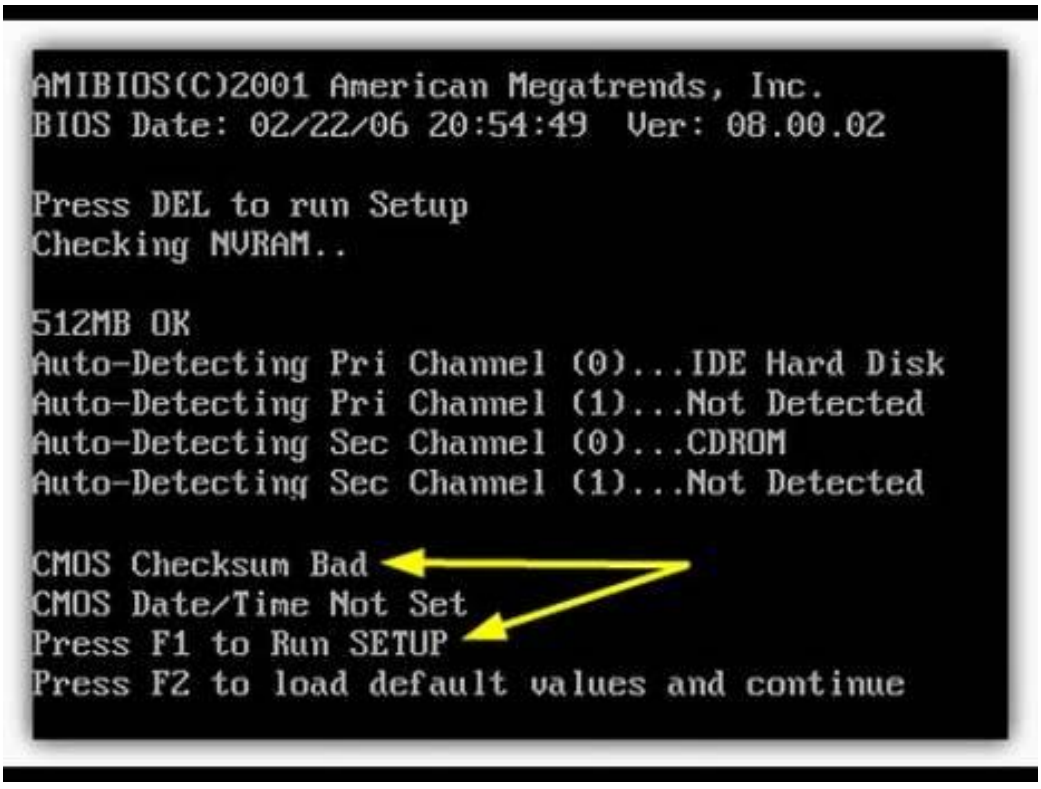

Рисунок 2.5 – CMOS Checksum Bad

- CMOS Checksum Bad – Під час проходження самодіагностики програмою POST було виявлено помилку у контрольній сумі вмісту CMOS-пам’яті. Швидше за все, несправність виникла через розрядку акумулятора, що живить мікросхему CMOS-пам’яті. Замініть акумулятор, запустіть програму CMOS Setup Utility та завантажте оптимальні значення для всіх параметрів. Якщо помилку усунути не вдалося, перевірте всі контакти в ланцюзі живлення. Причиною неполадки може стати деструктивний вплив якогось вірусу (наприклад, Worm. Magistr). (рисунок 2.5);

- CMOS Checksum Error - Під час проходження самодіагностики програмою POST було виявлено помилку у контрольній сумі вмісту CMOS-пам’яті. Швидше за все, несправність виникла через розрядку акумулятора, що живить мікросхему CMOS-пам’яті. Замініть акумулятор, запустіть програму CMOS Setup Utility та завантажте оптимальні значення для всіх параметрів. Якщо помилку усунути не вдалося, перевірте всі контакти в ланцюзі живлення. Причиною неполадки може стати деструктивний вплив якогось вірусу (наприклад, WinClH 95 або l. Worm. Magistr);

- CMOS Checksum Failure - Під час проходження самодіагностики програмою POST було виявлено помилку у контрольній сумі вмісту CMOS-пам’яті. Швидше за все, несправність виникла через розрядку акумулятора, що живить мікросхему CMOS-пам’яті. Замініть акумулятор, запустіть програму CMOS Setup Utility та завантажте оптимальні значення для всіх параметрів. Якщо помилку усунути не вдалося, перевірте всі контакти в ланцюзі перевірити встановлення модулів оперативної пам’яті в слотах. Якщо модулі не підтримують контроль парності, запустіть програму CMOS Setup Utility і вимкніть усі опції, які дозволяють подібний контроль. Повідомлення може з’являтися при проблемах з роботою пристроїв, інтегрованих у материнську плату або процесор. У цьому випадку несправність усувається заміною або материнської плати, або процесора;

- Press ESC Перейти до Memory Test - Повідомлення з’являється на екрані монітора у випадку, коли опція на кшталт Quick Power On Self Test

перебуває у вимкненому стані. Пропонується за допомогою натискання < Esc > пропустити потрійне тестування оперативної пам’яті;

- Press Fl To Disable NMI, F2 To Reboot - Стався збій у роботі контролера переривань. Швидше за все, система не може ідентифікувати пристрій, який подав запит на переривання, що не маскується. Пропонується або заборонити використання переривання NMI невідомим пристроєм (клавіша < F1>) і продовжити роботу, або перезавантажити комп’ютер (клавіша < F 2>);

- Press TAB to Show POST Screen - Деякі виробники замінюють стандартний логотип на власний. Після натискання клавіші TAB ви можете переглянути оригінальний логотип Phoenix BIOS замість логотипу виробника материнської плати, що відображається за замовчуванням;

- Primary Boot Device Not Found - Не знайдено перший завантажувальний диск. Це повідомлення з’являється лише з BIOS , що дозволяє встановити кілька можливих варіантів завантаження. Наприклад, якщо в якості першого завантажувального пристрою вказаний дисковод для гнучких дисків, повідомлення може з’явитися при спробі завантаження з вставленою несистемною дискетою. Запустіть програму CMOS Setup Utility і встановіть завантаження з жорсткого диска;

- Primary Input Device Not Found - Призначений первинний пристрій введення інформації не виявлено;

- Primary Master Hard Disk Fail - Програма тестування виявила збій у роботі жорсткого диска, підключеного до першого каналу IDE (primary) і встановленого як master-диск. Спробуйте перезавантажити комп’ютер за допомогою кнопки RESET на системному блоці. Якщо несправність з’явилася знову, перевірте сполучний шлейф та роз’єм живлення відповідного жорсткого диска. В іншому випадку знадобиться заміна вінчестера;

- IDE Controller Resource Conflict - Контролер IDE намагається використовувати вже зайняті ресурси комп’ютера. Найчастіше ця проблема виникає після спроби включити другий канал контролера після тривалої

роботи з відключеним каналом. Запустіть програму CMOS Setup Utility та увімкніть режим оновлення конфігурації пристроїв. Якщо несправність усунути не вдалося, з'ясуйте, з яким пристроєм конфліктує контролер IDE і зробіть для нього ручне налаштування розподілу ресурсів;

- RAM Parity Error - Checking For Segment - Стався серйозний збій під час роботи оперативної пам'яті — помилка парності. Перевірте, чи підтримують встановлені модулі пам'яті контроль парності. Якщо ні, то запустіть програму CMOS Setup Utility і вимкніть усі опції, які стосуються цієї функції. Якщо модулі пам'яті підтримують контроль парності, спробуйте перезавантажити комп'ютер за допомогою кнопки RESET на системному блоці. При повторній появі помилки, швидше за все, потрібно замінити несправний модуль пам'яті;

- Real Time Clock Error - Виникла критична помилка під час роботи годинника реального часу. Запустіть програму CMOS Setup Utility та встановіть нормальні значення дати та часу. Якщо помилка з'явилася знову, швидше за все, доведеться замінити материнську плату;

- Real Time Clock Failure - Виникла критична помилка під час роботи годинника реального часу. Запустіть програму CMOS Setup Utility та встановіть нормальні значення дати та часу. Якщо помилка з'явилася знову, швидше за все, доведеться замінити материнську плату;

- Resuming From Disk, Press TAB to Show POST Screen - Дане повідомлення з'являється на ноутбуках з Phoenix BIOS, коли користувач намагається перезавантажити (вимкнути) комп'ютер, що знаходиться в сплячому режимі. Після натискання клавіші <ТаЬ> комп'ютер перетворюється на нормальний режим роботи, після чого його можна перезавантажити або вимкнути;

- SMART Failure Predicted on Primary Master - Вбудована діагностика жорсткого диска, підключеного до першого каналу IDE як master-диск, говорить про наявність проблем з надійністю його роботи (рисунок 2.6);

Рисунок 2.6 – SMART Failure Predicted on Hard Disk

- SMART Failure Predicted on Primary Slave - Вбудована діагностика жорсткого диска, підключеного до першого каналу IDE як slave-диск, говорить про наявність проблем із надійністю його роботи;

- SMART Failure Затверджено на Secondary Master - Вбудована діагностика жорсткого диска, підключеного до другого каналу IDE як master-диск, говорить про наявність проблем з надійністю його роботи;

- SMART Failure Predicted on Secondary Slave - Вбудована діагностика жорсткого диска, підключеного до другого каналу IDE як slave-диск, говорить про наявність проблем з надійністю його роботи;

- Secondary Master Hard Disk Fail - Програма тестування виявила збій у роботі жорсткого диска, під ключеного до другого каналу IDE (secondary) і встановленого як master-диск. Спробуйте перезавантажити комп'ютер за допомогою кнопки RESET на системному блоці. Якщо несправність з'явилася знову, перевірте з'єднувальний шлейф та роз'єм живлення відповідного жорсткого диска. В іншому випадку знадобиться заміна вінчестера.);

- Secondary Slave Hard Disk Fail - Програма тестування виявила збій у роботі жорсткого диска, під ключеного до другого каналу IDE (secondary) і встановленого як slave-диск. Спробуйте перезавантажити комп'ютер за

допомогою кнопки RESET на системному блоці. Якщо несправність з’явилася знову, перевірте з’єднувальний шлейф та роз’єм живлення відповідного жорсткого диска. В іншому випадку знадобиться заміна вінчестера;

- Service Processor Not Properly Installed - Помилка ініціалізації контролера керування сервером;

- Should Be Empty But EISA Board Found - При ідентифікації плати розширення EISA виявлено невідповідність даних, зазначених у BIOS, дійсним характеристикам. Запустіть програму EISA Configuration Utility та перевірте значення всіх параметрів;

- Should Have EISA Board But Not Found - Плата розширення EISA не відповідає запитам системи. Запустіть програму EISA Configuration Utility і перевірте значення всіх параметрів. Якщо несправність усунути не вдається, швидше за все доведеться замінити відповідну плату розширення;

- Slot Not Empty - Виявлено невідому плату розширення на шині EISA. Запустіть EISA Configuration Utility та встановіть правильні параметри плати;

- Start Unit Request Failed - BIOS контролера SCSI не може надіслати команду Start Unit Command одному з пристроїв, підключених до контролера. У BIOS контролера слід опцію Send Start Unit Command встановити у значення "Вимкнено" (No);

- Software Port NMI Inoperational - Не працює програмний порт немаскованого переривання NMI. Спробуйте на деякий час вимкнути комп’ютер. Якщо несправність вуст поранити не вдається, швидше за все доведеться замінити материнську плату;

- Software Port NMI - Не працює програмний порт немаскованого переривання NMI. Спробуйте на деякий час вимкнути комп’ютер. Якщо несправність вуст поранити не вдається, швидше за все доведеться замінити материнську плату;

- State Battery CMOS Low - Розрядився акумулятор, що живить мікросхему CMOS-пам’яті (є ймовірність, що несправність виникла через

поганий контакт у ланцюгу живлення). Встановіть новий акумулятор. Якщо повідомлення все одно є, перевірте якість контактів;

- Static Device Resource Conflict - Плата розширення на шині ISA, яка не підтримує стандарт Plug and Play, намагається використовувати ресурси, вже зайняті іншим пристроєм. У більшості випадків проблему можна вирішити тільки вручну на будівництво режиму роботи нерпр-плати розширення;

- System Battery Is Dead - Розрядився акумулятор, що живить мікросхему CMOS-пам’яті (є ймовірність, що несправність виникла через поганий контакт у ланцюгу живлення). Встановіть новий акумулятор. Якщо повідомлення все одно є, перевірте якість контактів;

- System Battery Is Dead - Replace And Run Setup - Розрядився акумулятор, що живить мікросхему CMOS-пам’яті (є ймовірність, що несправність виникла через поганий контакт у ланцюгу живлення). Встановіть новий акумулятор. Якщо повідомлення все одно є, перевірте якість контактів;

- System Cache Error - Помилка ініціалізації кеш-пам’яті. Якщо на вашому комп’ютері вона виконана у вигляді окремих модулів (кеш-пам’ять 3-го рівня), спробуйте змінити модулі або хоча б витягнути їх і встановити назад, попередньо очистивши від пилу всі роз’єми. Якщо кеш-пам’ять інтегрована в центральний процесор, тоді вам доведеться, як мінімум, перевірити якість його охолодження (для тих процесорів, які виконані в конструктиві Slot I/A, слід перевіряти рівень нагріву саме для мікросхем кеш-пам’яті, розташованих на процесорної плати). Якщо перелічені заходи не дають жодного штибу, швидше за все, доведеться змінювати сам процесор, хоча не виключено, що неполадка зникне після перезавантаження за допомогою кнопки RESET на системному блоці або вимкнення на деякий час;

- Checksum Bad - Виявлено помилку в контрольній сумі вмісту пам’яті CMOS. Швидше за все, несправність виникла через розрядку акумулятора,

що живить мікросхему CMOS-пам’яті. Замініть акумулятор, запустіть програму CMOS Setup Utility та встановіть правильні значення всіх параметрів. Якщо помилку усунути не вдалося, перезапишіть вміст BIOS (це можливо лише у випадку встановлення Flash-пам’яті);

- System Device Resource Conflict - Плата розширення на шині ISA, яка не підтримує стандарт Plug and Play, намагається використовувати ресурси, вже зайняті іншим пристроєм. У більшості випадків проблему можна вирішити тільки вручну на будівництво режиму роботи нерпр-плати розширення;

- System Halted, (Ctrl-Alt-Del) To Reboot - Система зупинила свою роботу. Для перезавантаження комп’ютера пропонується натиснути клавішу < Ctrl >+< Alt >+< Del > ("теплий старт"). Повідомлення найчастіше виникає при спробі доступу будь-якої програми до обладнання, минаючи засоби операційної системи. Якщо операційна система не допускає подібних дій, комп’ютер припиняє свою роботу з виведенням на екран монітора цього повідомлення;

- System RAM Failed At Offset: XXXX - Помилка ініціалізації основної пам’яті. Спробуйте на деякий час вимкнути комп’ютер і перевірте якість установки модулів пам’яті в слотах. Якщо несправність усунути не вдається, швидше за все, доведеться замінити модулі пам’яті;

- System Time Error - Помилка системного таймера;

- Time-Out Failure During - Слід перевірити наявність та правильність підключення термінаторів на SCSI-шині, а також правильність підключення інформаційних кабелів. Можливо, один із пристроїв SCSI несправний;

- Type Display CMOS Mismatch - У BIOS неправильно вказано тип системного монітора. Запустіть програму CMOS Setup Utility і введіть правильні характеристики монітора (у старих материнських платах для цього може знадобитися перемикання відповідної перемички);

- Uncorrectable ECC DRAM Error - Під час роботи оперативної пам’яті DRAM виникла серйозна помилка, яка може бути виправлена системою

корекції ECC. Повідомлення може виникнути при серйозних проблемах роботи модулів пам’яті з підтримкою режиму ECC (корекція одиночних помилок і виявлення множинних). Спробуйте на деякий час вимкнути комп’ютер. Якщо несправність усунути не вдається, швидше за все, доведеться замінити модулі пам’яті;

- Unknown PCI Error - Виникла невідома помилка під час роботи пристроїв на шині PCI. Спробуйте на деякий час вимкнути комп’ютер. Другим кроком усунення несправності можна порекомендувати послідовну заміну PCI-плат розширення. Якщо локалізувати проблему не вдається, швидше за все доведеться замінити материнську плату;

- Update Failed - Оновлення інформації про конфігурацію пристроїв Plug and Play закінчилося невдачею. Швидше за все, проблема в низькій напрузі мікросхеми. Спробуйте замінити акумулятор. Якщо це не допомогло, ваша материнська плата замінюється;

- Update OK! - Оновлення інформації про конфігурацію пристроїв Plug and Play пройшло успішно. Повідомлення зазвичай з’являється під час встановлення нового обладнання;

- Wrong Board In Slot - Встановлена плата EISA некоректно відповідає запитам системи. Запустіть програму EISA Configuration Utility та перевірте значення всіх параметрів. Якщо несправність усунути не вдається, швидше за все, доведеться замінити відповідну плату;

- X: Drive Error - Диск x: не відповідає запитам системи. В першу чергу перевірте якість підключення з’єднувального шлейфу та гнізда живлення. Якщо все підключено нормально, запустіть програму CMOS Setup Utility та перевірте встановлені параметри жорсткого диска (найкраще скористатися пунктом HDD Auto Detection). Іноді помилка з’являється при збоях таблиці розділів диска. В цьому випадку достатньо переформатувати диск;

- X: Drive Failure - Диск x: не відповідає запитам системи. В першу чергу перевірте якість підключення з’єднувального шлейфу та гнізда

живлення. Якщо все підключено нормально, запустіть програму CMOS Setup Utility та перевірте встановлені параметри жорсткого диска (найкраще скористатися пунктом HDD Auto Detection). Іноді помилка з’являється при збоях таблиці розділів диска. У цьому випадку достатньо переформатувати диск.

2.3 Узагальнений алгоритм пошуку несправностей та діагностики

На рисунку 2.7 представлений узагальнений алгоритм виявлення чи діагностіки несправностей.

Технічна діагностика вивчає методи отримання і оцінки діагностичної інформації, діагностичні моделі і алгоритми прийняття рішень. Метою технічної діагностики є підвищення надійності та ресурсу комп’ютерних систем. Як відомо, найважливішим показником надійності є відсутність відмов під час експлуатації технічної системи. Технічна діагностика завдяки ранньому виявленню дефектів і несправностей дозволяє усунути подібні відмови в процесі технічного обслуговування, що підвищує надійність і ефективність експлуатації, а також дає можливість експлуатації комп’ютерних систем відповідального призначення за станом.

Теоретичним фундаментом для вирішення основного завдання комп’ютерної діагностики слід вважати загальну теорію розпізнавання образів. Комп’ютерна діагностика вивчає алгоритми розпізнавання щодо завдань діагностики, які зазвичай можуть розглядатися як завдання класифікації.

Алгоритми розпізнавання в технічній діагностиці частково ґрунтуються на діагностичних моделях, що встановлюють зв’язок між станами технічної системи та їх відбиттям у просторі діагностичних сигналів. Важливою частиною проблеми розпізнавання є правила прийняття рішень (вирішувальні правила).

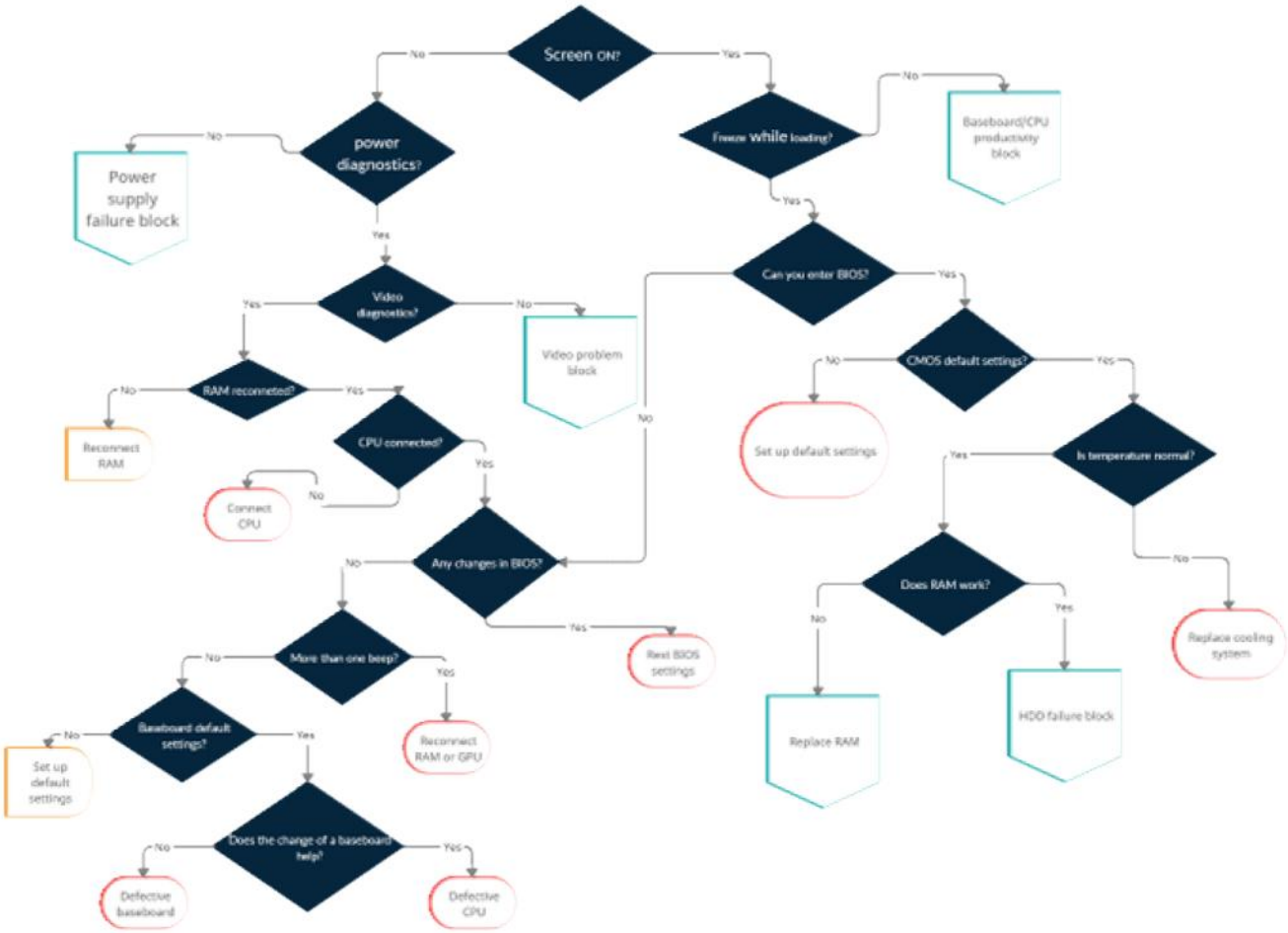

Рисунок 2.7 – Блок-схема алгоритму

3 ПРОГРАМНА МОДЕЛЬ ТА СЕРЕДОВИЩЕ МОДЕЛЮВАННЯ

3.1 Програмний застосунок взаємодії користувача з BIOS

Застосунок має бути у вигляді віконної програми із зручним інтерфейсом для кращого та швидкого використання. Саме це було головною метою створення застосунку, бо якщо користувачу потрібно дізнатись щось про певну функцію базової системи введення-виведення, треба шукати інформацію в інтернеті чи в книжках, що не дуже зручно та займає багато часу. Але саме застосунок допоможе в цьому, а ще існує відображення головних даних про операційну систему на BIOS. Головною метою застосунку було створення зручного інтерфейсу користувача задля швидкої взаємодії із застосунком. Вся програма розподілена на 4 головні частини, які доступні через кнопки. Застосунок має такі компоненти:

- Main;
- Features;
- Beep codes;
- FAQ.

За допомогою мови розмітки користувальницького інтерфейсу QML, вдалося зробити кожен елемент застосунку спеціальним. Основний ухил був на бірюзовий та чорний кольори. Для застосунка було вирішено використати мінімалістичний стиль, але з деякими графічними елементами. Саме завдяки можливості зміни кожного елемента можна кастомізувати застосунок так, як потрібно розробнику, та задавати будь-які кольори та анімації.

Щодо функціоналу застосунку, головною метою якого було спрощення розуміння базової системи введення-виведення та її функцій, було запропоновано надання суттєвої інформації щодо операційної системи та базової системи введення-виведення, а також перевірка стану безпеки UEFI чи BIOS.

Розділ Features містить у собі найбільш загальні функції, які користувач

може мати на певній материнській платі, та детальний опис цих функцій, щоб користувач мав більше уявлення щодо їх використання**.** Наступний розділ, який має назву POST, містить у собі таблиці апаратних сигналів головних виробників. Завдяки цьому розділу користувач може дізнатись причину несправності та уживати необхідних заходів. Найпоширеніші питання щодо базової системи введення-виведення чи питань стосовно апаратних проблем користувач може знайти у розділі “FAQ”.

Після запуску застосунку, можна побачити головне вікно застосунку, на якому розташовано 4 кнопки, завдяки яким користувач може взаємодіяти із застосунком як необхідно. Задля отримання загальної інформації треба натиснути на кнопку “Main” (рисунок 3.1).

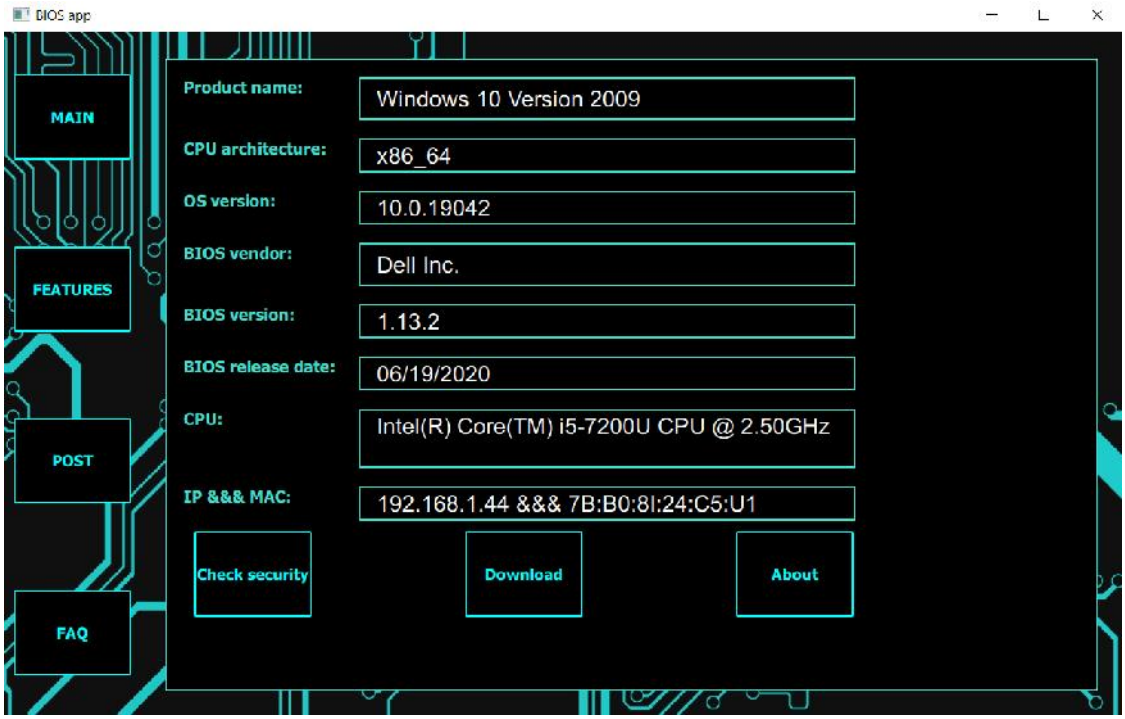

Рисунок 3.1 – Інтерфейс додатку

В цьому розділі можна дізнатись основну інформацію, таку як версія BIOS та операційної системи, IP користувача, інформацію про CPU та стан налаштувань BIOS. Після натискання кнопки “Check security”, з’явиться діалогове вікно, де буде відображено стан найголовніших з точки зору

безпеки налаштувань (рисунок 3.2).

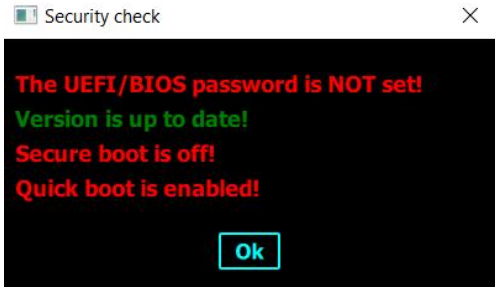

Рисунок 3.2 – Перевірка налаштувань безпеки

Після натискання кнопки “Features” користувач може дивитися інформацію про різні функції базової системи введення-виведення (рисунок 3.3). Цей програмний модуль розбитий на такі підпункти:

- Standard CMOS Features;
- Advanced BIOS Features;
- Integrated Peripherals;
- Power Management Setup;
- PnP/PCI Configuration;
- PC Health Status;
- Frequency/Voltage Control.

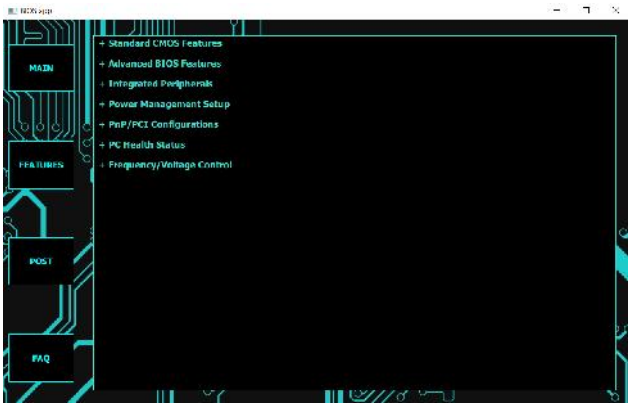

Рисунок 3.3 – Перелік підрозділів функцій BIOS у розділі Features

У цих розділах описані загальні функції найголовніших виробників базової системи введення-виведення (рисунок 3.4). Після запуску BIOS, користувач може не побачити усі вкладинки, тому треба бути пильним щодо використання різноманітних функцій. Кожен розділ містить майже усі функції. Також, користувач може обрати потрібну йому функцію, та детальний опис буде відображено.

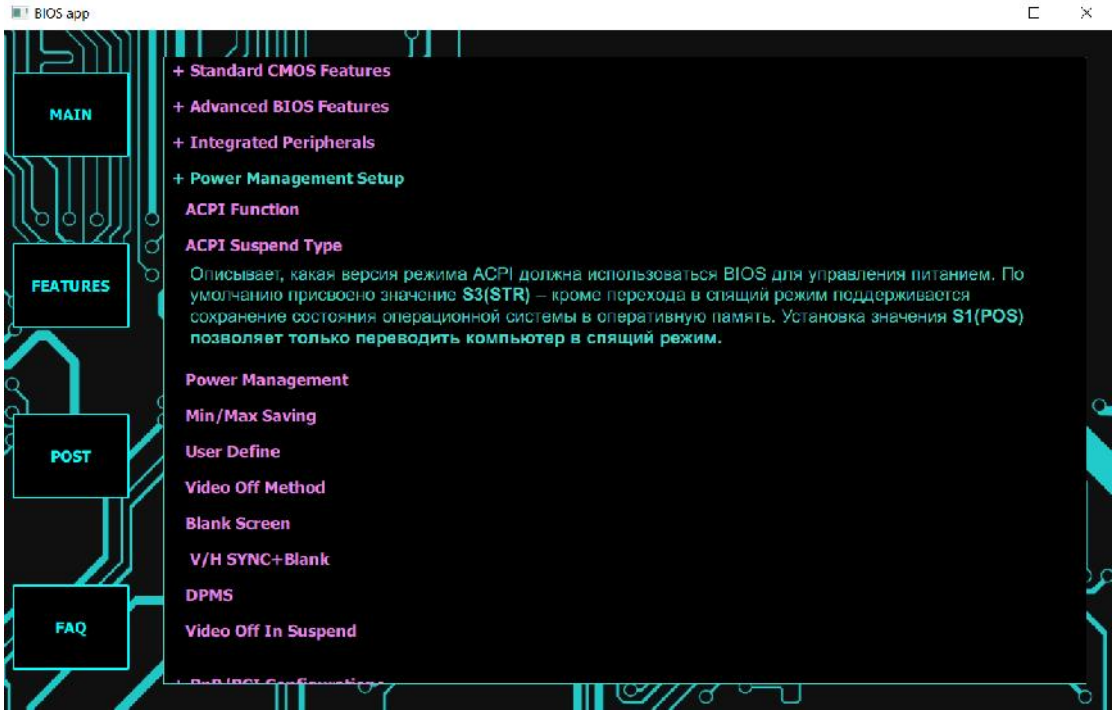

Рисунок 3.4 – Опис параметру ACPI Suspend Type у розділі Features

Завдяки різним кольорам можна відрізняти розділ від функції. У застосунку використано бірюзовий колір щодо розділу, а фіолетовий – функцій. Якщо трапляються апаратні поломки, комп’ютер оповіщає користувача про них звуковими сигналами (рисунок 3.5). Саме після натискання кнопки POST, користувач перейде до розділу, де будуть відображені звукові сигнали найпоширеніших виробників BIOS чи ноутбуків. Завдяки цьому розділу користувачу буде простіше виявити поломку та вжити необхідних заходів. Останньою функцією застосунку є перегляд найпоширеніших питань щодо базової системи введення-виведення чи апаратних проблем, а також поетапне вирішення цих проблем. Після

натискання на кнопку FAQ, користувач може побачити перелік питань.

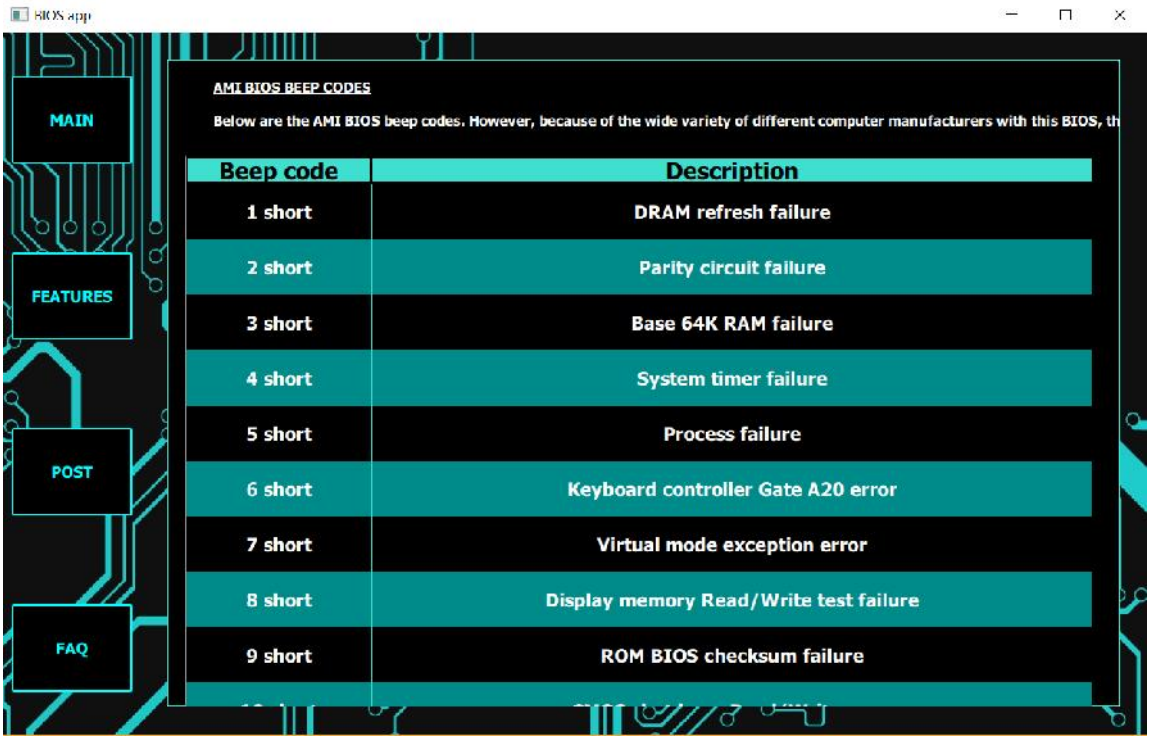

Рисунок 3.5 – Таблиця помилок на прикладі AMI BIOS у розділі POST

Саме після цього, користувач може дивитись відповіді на різноманітні питання. Зробити це можливо по натисканні на потрібне користувачу питання.

3.2 Середовище моделювання

3.2.1 Фреймворк tianocore

Tianocore EDK II — це еталонна реалізація UEFI від Intel. EDK II — це сучасне, багатофункціональне, кросплатформне середовище розробки мікропрограми для специфікацій UEFI та PI, яке є відкритим вихідним кодом з використанням BSD+Patent. TianoCore EDK II — це стандартна загальна реалізація сервісів UEFI. Код EDK II був інтегрований в інші проекти.

Частиною TianoCore є оболонка UEFI, наприклад, якщо певний постачальник UEFI не підтримує функцію оболонки UEFI, можна використовувати оболонку UEFI від TianoCore. У червні 2004 року Intel оголосила, що випустить «Основний код» свого Extensible Firmware Interface (EFI), наступника 16-розрядного x86 PC BIOS, за ліцензією з відкритим вихідним кодом. Цей Основний код, розроблений Intel як частина коду проекту під назвою Tiano, був реалізацією EFI для Intel. Це переросло в EDK, EDK II та інші проекти з відкритим кодом. Специфікації EFI були представлені на форумі United EFI як частина оригінальних специфікацій UEFI, які були прийняті більш ніж 200 компаніями і поставлялися на мільйони обчислювальних пристроїв. Форум UEFI не підтримує жодної конкретної реалізації, але TianoCore розроблено для реалізації специфікацій UEFI та UEFI PI.

3.2.2 Платформи та пакети

Це платформи, які зараз підтримуються EDK II, згруповані за постачальником процесора, а не за постачальником платформи.

- AMD: Cello, Overdrive, Overdrive 1000;
- Ampere: Mt.Jade;
- ARM: Juno, SGI family;
- Beagle Board;
- Hisilicon: D03, D05, D06, HiKey, HiKey960;
- Intel;
- Marvell;
- Raspberry Pi 3/4.

Проект EDK II складається з пакетів. Супроводжувачі для кожного пакета перераховані нижче:

- UefiCpuPkg - надає модулі та бібліотеки ЦП, сумісні з UEFI;
- ArmVirtPkg - емуляція UEFI для процесорів ARM;

- ArmPkg - пакет процесора ARM;
- ArmPlatformPkg;
- CryptoPkg - Пакет для модулів криптографії;
- FatPkg;
- InterFsp2Pkg - надає компонент для створення двійкового файлу FSP;
- IntelFsp2WrapperPkg - надає компонент для використання двійкового файлу FSP;
- MdePkg - надає всі визначення, бібліотечні класи та екземпляри бібліотек;
- NetworkPkg - надає мережеві модулі, які відповідають специфікації UEFI 2.4;
- OvmfPkg - спрямований на підтримку мікропрограми для віртуальних машин за допомогою edk2;
- ShellPkg - надає всі визначення для EFI та UEFI Shell;
- SecurityPkg - Надає функції безпеки, які відповідають галузевим стандартам TCG/UEFI;
- MdeModulePkg - надає модулі, які відповідають галузевим стандартам UEFI/PI;
- RedfishPkg - є ефективним і безпечним рішенням для кінцевих користувачів для віддаленого налаштування конфігурацій платформи UEFI за допомогою Redfish RESTful API;
- EmulatorPkg – дозволяє увімкнути емуляцію UEFI в середовищі ОС;
- EmbeddedPkg - надає заголовки та бібліотеки, які відповідають галузевим стандартам EFI/PI;
- DynamicTablesPkg - надає механізми для зменшення кількості зусиль, необхідних для перенесення мікропрограм на нові платформи. Метою є забезпечення реалізації, здатної генерувати таблиці мікропрограм із зовнішнього джерела;
- FmpDevicePkg - забезпечує реалізацію екземпляра Firmware Management Protocol, який підтримує оновлення пристроїв зберігання

мікропрограм за допомогою капсул UEFI;

- SignedCapsulePkg - надає підписану капсулу в EDKII для підтримки безпечного рішення для оновлення та відновлення капсули.

Однак, одним з найважливіших для нас пакетів є EmulatorPkg. EmulatorPkg забезпечує середовище, де середовище UEFI може емулюватися в середовищі ОС, де повністю сумісне з UEFI середовище неможливе. Наприклад, запуск під ОС, де процес ОС містить середовище емуляції UEFI. Задля емуляції середовище, потрібно скачати фреймворк tianocore, та збудувати пакет для емуляції.

На прикладі ОС Kali Linux, зробимо такі кроки (рисунок 3.6 – 3.13):

```
cd tianocore/edk2/EmulatorPkg
build.sh
build.sh run
```

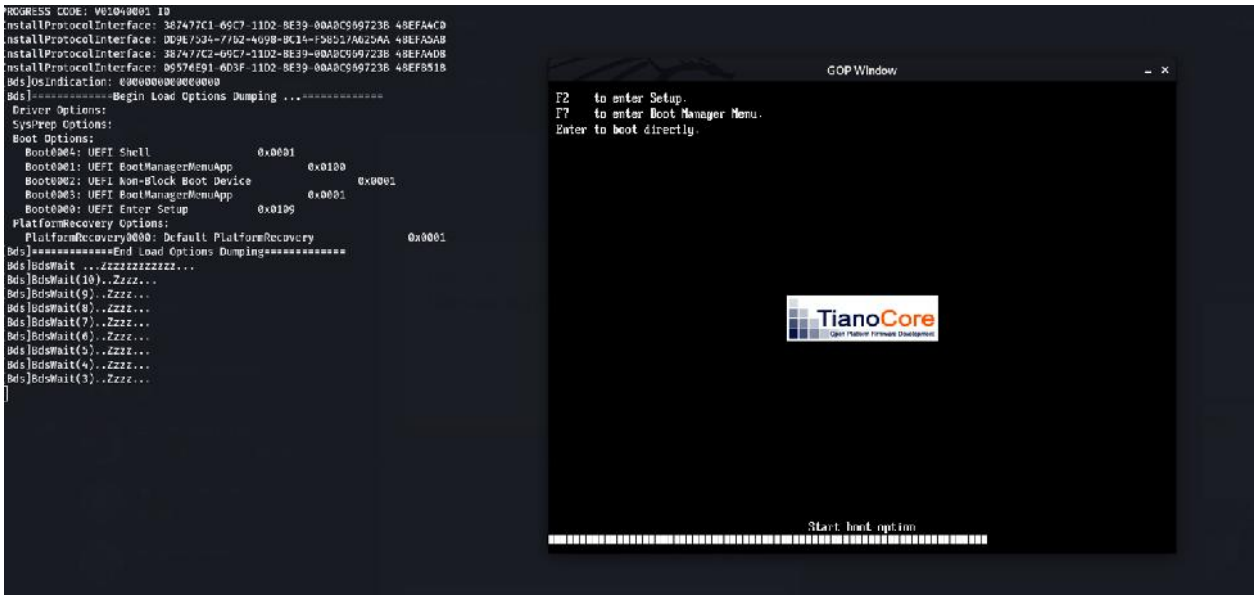

Рисунок 3.6 – Початок емуляції

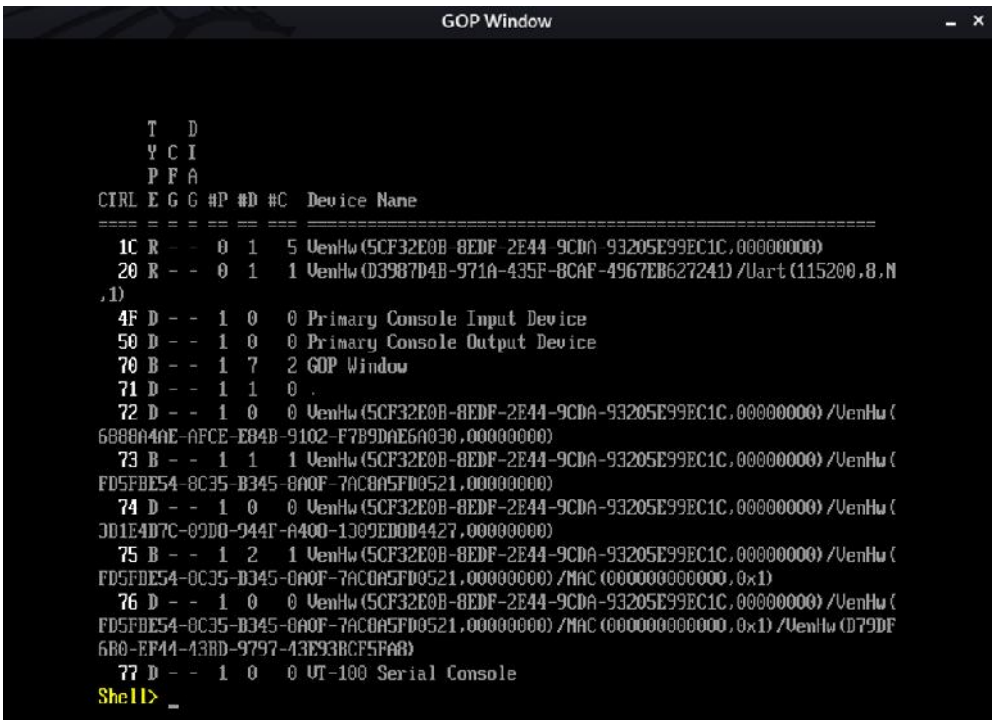

Рисунок 3.7 – Відображення списку пристроїв, якими керують драйвери UEFI

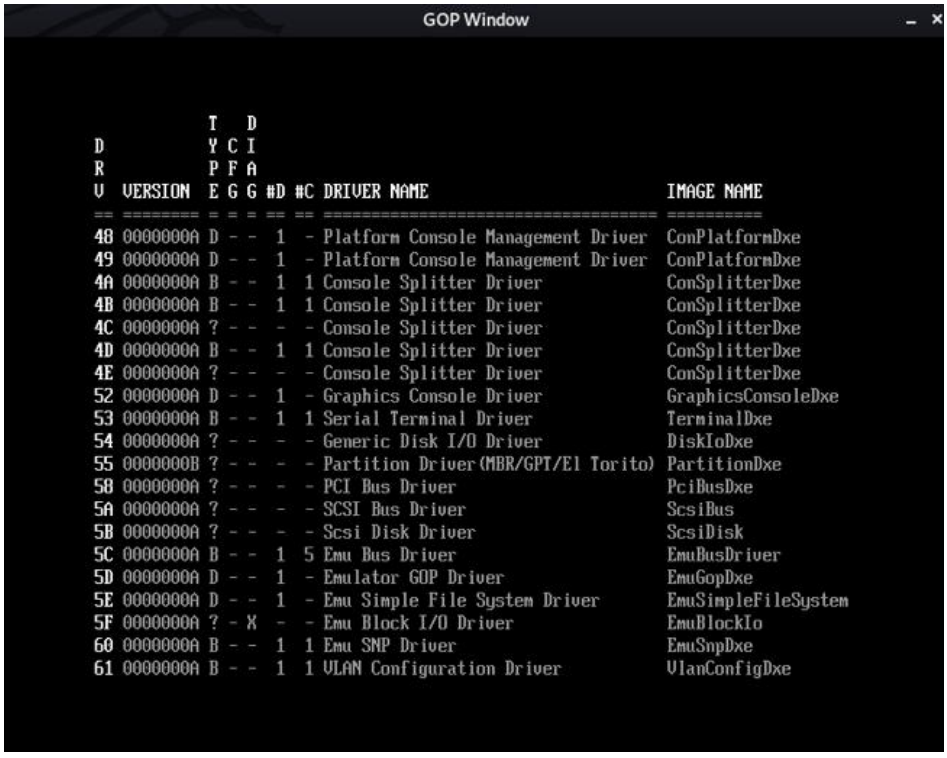

Рисунок 3.8 – Відображення списку інформації для драйверів, які відповідають моделі драйвера UEFI

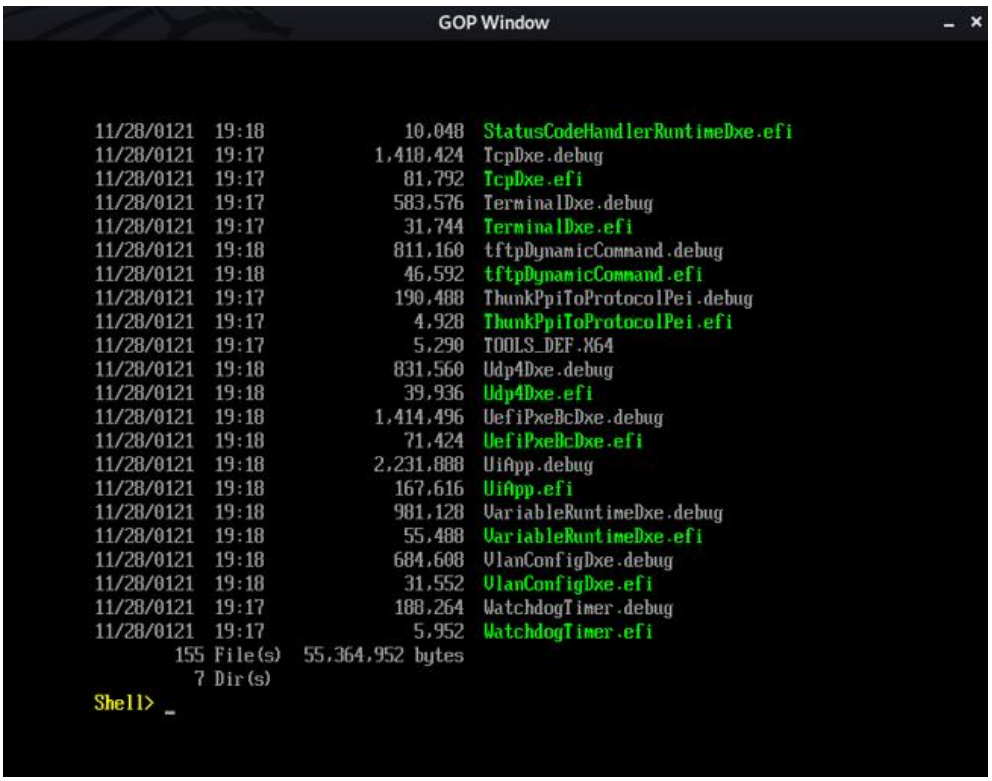

Рисунок 3.9 – Відображення списку файлів одного з приводів

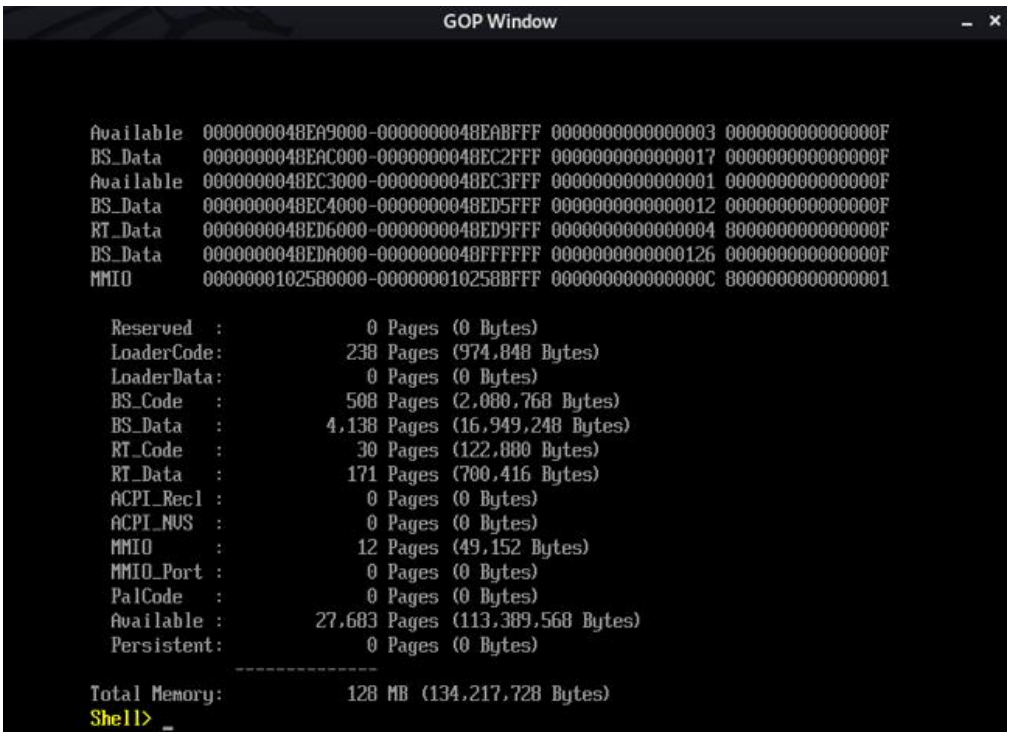

Рисунок 3.10 – Відображення карти системної пам’яті

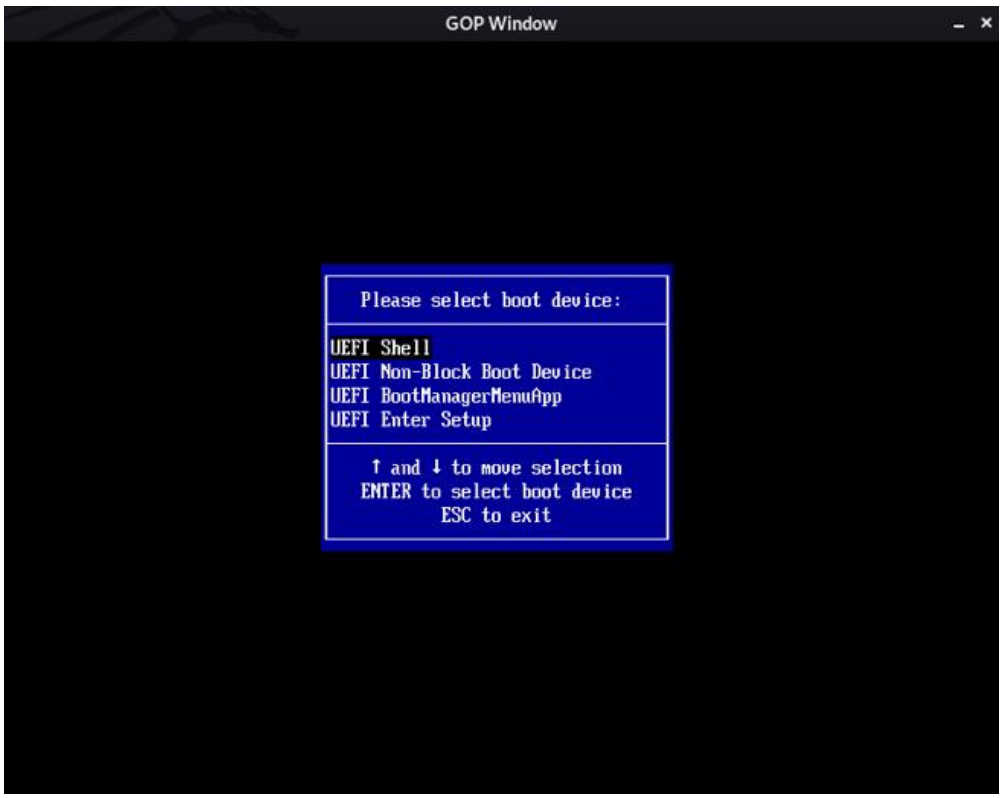

Рисунок 3.11 – Відображення вибору девайса для загрузки

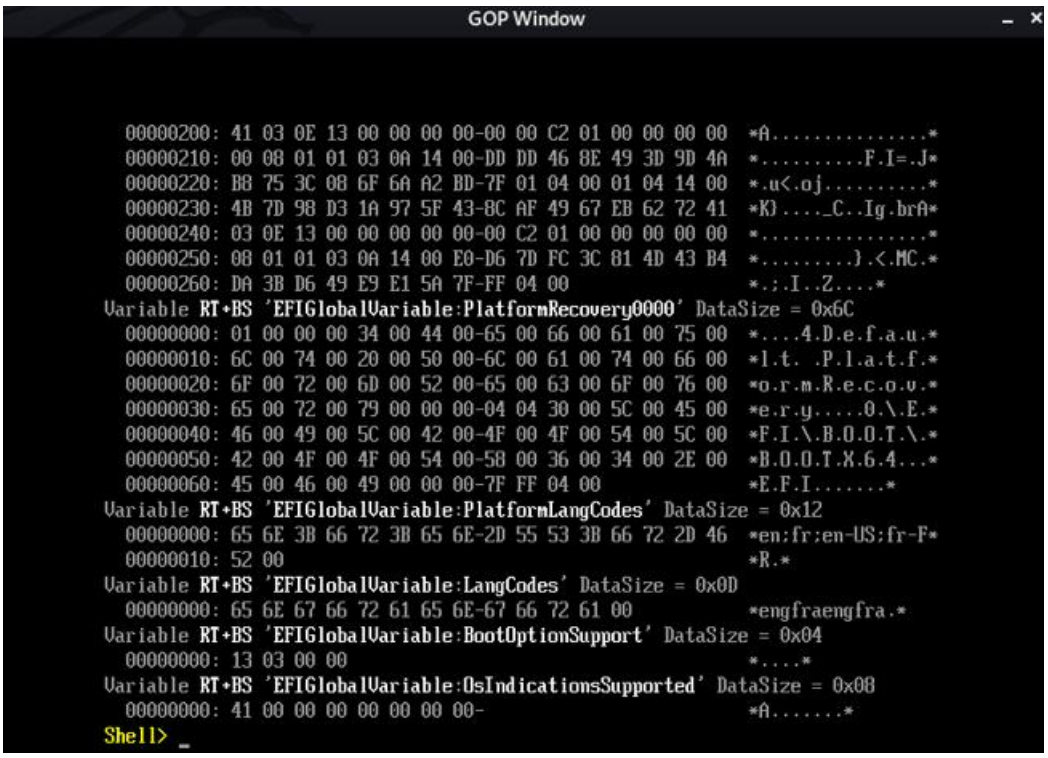

Рисунок 3.12 – Відображення стану змінних UEFI

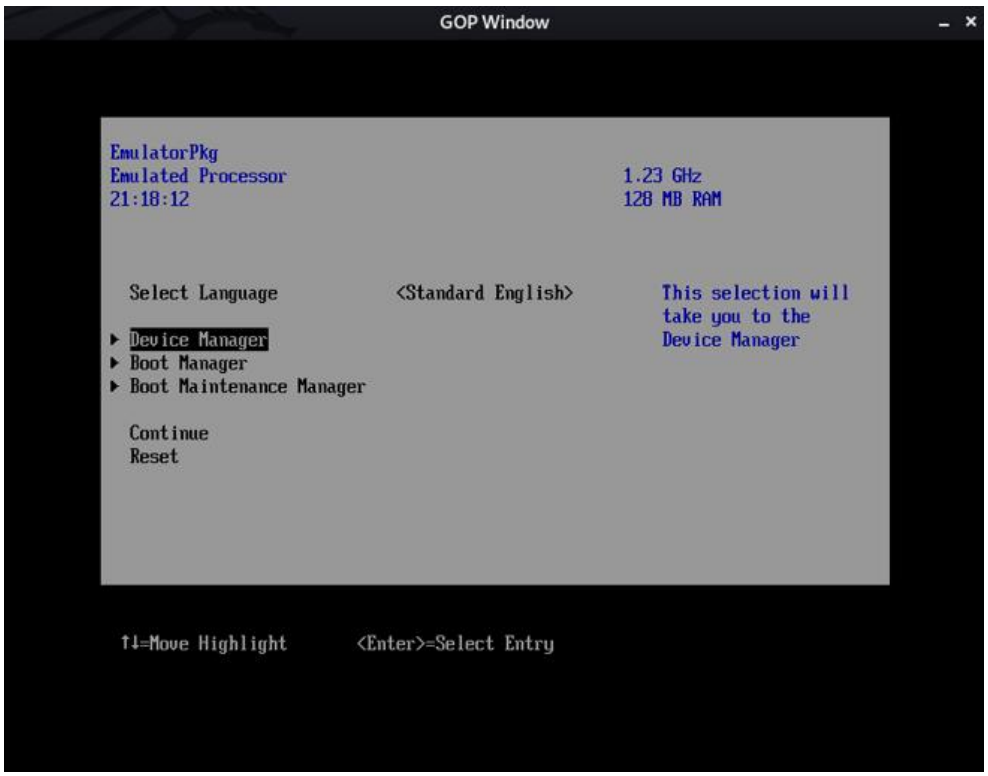

Рисунок 3.13 – Відображення головного екрану BIOS за допомоги емуляції

4 РЕКОМЕНДАЦІЇ ЩОДО НАЛАШТУВАННЯ ПАРАМЕТРІВ BIOS

4.1 Протокол Secure Boot

Основна мета Secure Boot — запобігти будь-кому виконанню несанкціонованого коду в середовищі перед завантаженням; таким чином, тільки код, який відповідає політиці цілісності платформи дозволено виконуватися. Ця технологія є дуже важливо для платформ з високою надійністю, і також часто використовується на вбудованих пристроях і мобільних платформах, оскільки це дозволяє постачальникам обмежувати платформи до програмного забезпечення, схваленого постачальником, наприклад iOS на iPhone або Windows 10.

Secure Boot доступний у трьох формах, які залежать від рівня ієрархії процесу завантаження, в якій він застосовується:

- безпечне завантаження ОС - реалізовано на рівні завантажувача ОС.
- перевіряє компоненти, завантажені завантажувачем ОС, такі як ядро ОС і драйвери для завантаження;
- безпечне завантаження UEFI - реалізовано в прошивці UEFI. Перевіряє драйвери та програми UEFI DXE, додаткові ПЗУ та завантажувачі ОС;
- безпечне завантаження платформи - перевіряє мікропрограму ініціалізації платформи.

Комп’ютери, на яких працює застарілий BIOS або модуль підтримки сумісності (CSM), слід перевести в режим UEFI. Також, буває так, коли поточні платформи підтримують завантаження UEFI, але переваги безпеки зводяться нанівець, якщо їх не ввімкнути. Попередній стандарт завантаження за своєю суттю є небезпечним, що залишає можливість зловмисному програмному забезпеченню вставлятися в процес завантаження. Деякі виробники BIOS дозволяють «подвійний» режим або «комбо» режим, який

намагається розумно перемикатися між застарілою версією та UEFI. Хоча цей режим зручний, він не є безпечним. Безпечне завантаження має бути ввімкнено на всіх кінцевих точках і налаштовано на аудит модулів мікропрограми, пристроїв розширення та образів ОС, що завантажуються.

Secure Boot слід налаштувати, якщо це необхідно, щоб відповідати потребам організацій та їх допоміжного апаратного та програмного забезпечення, тим паче, що більшість утиліт налаштування BIOS та багато інтерфейсів керування BMC дозволяють замінити ключі та сертифікати Secure Boot. Налаштування Secure Boot дозволяє адміністраторам реагувати на певні вразливості, не чекаючи оновлення BIOS. Прикладом може бути виправлення списку відкликання безпеки UEFI, який можна оновити вручну для уразливостей grub2/shim, таких як BootHole, та додаткових розкритих CVE.

Налаштування Secure Boot дозволяє адміністраторам зменшити вектори атаки:

- видалення стандартного сертифіката UEFI CA від Microsoft із бази даних Secure Boot;
- встановлення сигнатур або хешів певного завантажувача ОС, що використовується. Це запобігає завантаженню будь-якої іншої ОС;
- вимкнення завантаження в середовищах ОС, які можуть надати користувачеві розширений доступ;
- відключення зовнішніх портів (SATA, USB, тощо);
- запобігання зміни порядку завантаження.

4.1.1 Захист від буткітів за допомогою Secure Boot

Буткіт DreamBoot був першим публічним буткітом для підтвердження концепції, орієнтованим на системи на основі UEFI. У системі UEFI без Secure Boot цей букіт працює наступним чином:

- автор буткіту замінює оригінальний завантажувач UEFI Windows,

bootmgfw.efi, на шкідливий завантажувач bootx64.efi у завантажуваному розділі;

- шкідливий завантажувач завантажує оригінальний bootmgfw.efi, виправляє його, щоб отримати контроль над завантажувачем Windows winload.efi, і виконує його;

- шкідливий код продовжує виправляти системні модулі доки досягає ядра операційної системи, минаючи механізми захисту ядра (наприклад, політику підписання коду в режимі ядра), призначені для запобігання несанкціонованого виконання коду в режимі ядра.

Така атака можлива, оскільки за замовчуванням завантажувач ОС не автентифікується в процесі завантаження UEFI. Мікропрограмне забезпечення UEFI отримує місцезнаходження завантажувача ОС із змінної UEFI, яка для платформ Microsoft Windows розташована за адресою EFI\Microsoft\Boot\bootmgfw.efi у розділі завантаження. Зловмисник із системними привілеями може легко замінити або змінити завантажувач.

Однак, коли Secure Boot ввімкнено, ця атака більше неможлива. Оскільки Secure Boot перевіряє цілісність образів UEFI, що виконуються під час завантаження, а завантажувач ОС є одним із виконуваних файлів, перевірених під час завантаження, Secure Boot перевірить підпис завантажувача щодо баз даних db і dbx. Шкідливий завантажувач не підписаний належним ключем підпису, тому він потенційно не пройде перевірки та не виконуватиметься (залежно від політики завантаження). Це один із способів захисту Secure Boot від буткітів.

4.2 Параметр прискорення запуску операційної системи

Однією з ключових цілей обчислювальних платформ є швидкість реагування. Час завантаження BIOS є ключовим фактором реагування, який виробники OEM, кінцеві користувачі та постачальники ОС просять надати розробникам мікропрограми. Тут увага приділяється часу запуску системи

(параметр Fast Boot) та часу відновлення. BIOS традиційної архітектури Intel працював протягом багатьох років щоб розробити для себе завантаження з будь-якої конфігурації, яку може виявити платформа, щоразу, коли вона завантажується, вона працює, щоб заново відкривати все, що може, про зміну конфігурації машини, яка могла статися, коли вона була вимкнена. Однак це також призвело до збільшення часу завантаження понад 30 секунд лише для BIOS. При належному налаштуванні та обладнанні побутова електроніка або вбудований комп’ютерний пристрій, що ввімкнено, можуть легко завантажитися менш ніж за дві секунди. Зазвичай для цього потрібне індивідуальні жорстко запрограмовані рішення або рішення на основі політики, що може коштувати кількох місяців оптимізації.

Деякі системи обмінюють безпеку на швидкість, дозволяючи Fast Boot пропускати вимірювання або перевірку певних частин мікропрограми. Fast boot або мінімальне завантаження мінімізує час завантаження, пропускаючи численні перевірки, які можуть включати або не включати перевірки Secure Boot. Швидкість завантаження має пріоритет над деякими функціями безпеки та/або додатковими функціями та підтримкою периферійних пристроїв під час завантаження. Зловмисне програмне забезпечення, як LoJax, може проскочити в деяких системах. Fast Boot зазвичай увімкнено на споживчих пристроях. Якщо для Fast Boot можна налаштувати перемикач, вимкнення Fast Boot зазвичай призводить до повного завантаження, бо багато систем робочих станцій налаштовані в режимі Fast Boot, який пропускає перевірки фаз PEI, DXE і BDS завантаження UEFI

4.3 Адміністрування BIOS

4.3.1 Налаштування паролю

Мікропрограмне забезпечення має бути захищено за допомогою набору паролів адміністратора, що відповідають можливостям пристрою та варіанту

використання. Специфікація UEFI забезпечує підтримку пароля через ідентифікатор користувача та HII. Паролі адміністратора на більшості платформ обмежують доступ до параметрів конфігурації BIOS, які контролюють безпечне завантаження UEFI та інші функції безпеки платформи.

Таким чином, якщо пароль не захищений, BIOS не захищений і платформа не захищена. Паролі мікропрограми повинні відповідати тим же галузевим вимогам, що й паролі ОС (складність, довжина, повторне використання тощо). Можливо, додайте 2-й фактор, наприклад, безпечний ключ тощо. Слабкі або повторно використані паролі все ще залишаються проблемою, яка вимагає від кожної організації встановити політику створення та відстеження паролів. Паролі за замовчуванням є небезпечними паролями, оскільки вони фактично те ж саме, що і відсутність пароля. Хакер може заблокувати вашу власну систему або внести непомітні зміни до безпеки. Деякі уряди вирішують це за допомогою регламенту: вимагання унікального пароля за замовчуванням для кожного пристрою або змушення користувачів встановлювати власний пароль під час першого підключення.

4.3.2 Встановлення оновлень

Мікропрограмне забезпечення має оновлюватися регулярно та розглядатися так само важливо, як оновлення операційної системи та програм. UEFI надає стандартні механізми для передачі оновлень мікропрограми (так звані капсули) до BIOS. Як і інше програмне забезпечення в системі, мікропрограмне забезпечення може потребувати регулярних оновлень, оскільки виявляють проблеми з безпекою та випускають виправлення безпеки.

Задля оновлення BIOS під час безпечного завантаження потрібно:

- скопіювати підписаний файл зображення капсули у визначене специфікацією UEFI місце для зберігання капсул (наприклад,

/EFI/UpdateCapsules);

- запустити оновлення BIOS, встановивши змінну OsIndicationsUEFI з наступним перезавантаженням;

- під час завантаження BIOS перевірити, чи встановлено OsIndicationsis і чи є файл капсули;

- перевірити підпис капсули за допомогою ключа HPE (інтегрованого в BIOS). Якщо перевірка пройшла успішно, викликати флеш-програму в капсулі, щоб оновити BIOS. Коли оновлення BIOS завершено, образ капсули видаляється, а OsIndicationsvariable очищається, і виконується апаратне скидання.

Задля перевірки цілісності мікропрограми та конфігурації безпечного завантаження слід використовувати модуль довіреної платформи (TPM). Trusted Computing Group (TCG) надає специфікації, які надають додаткові можливості безпеки поверх безпечного завантаження UEFI. BIOS використовує TPM для вимірювання мікропрограми та конфігурації безпечного завантаження та передає це в операційну систему.

Завантажувачі ОС із підтримкою TPM перевіряють, що вимірювання під час завантаження відповідають записаним вимірюванням. Приклади включають: завантажувачі Microsoft, Trusted SHIM, Trusted GRUB, Tboot і TPM-rEFInd. Зі сторони звичайних користувачів, проблемою оновлення може бути відсутність сповіщень про доступні прошивки, не кажучи про безпеку виконання цього процесу.

4.4 Вирішення проблеми

Враховуючи вищезгадані етапи, можна затвердити що неправильно сконфігурована система являє собою ґрунтом для взлому. Враховуючи загальне зменшення випадків злому після переходу з BIOS до UEFI, не можливо не помітити значну кількість проблем із-за місконфігурації. Саму тому, у програмний додаток було впроваджено деяких змін. Замість

перевірки тільки актуальної версії, були додані перевірки стану паролю, Secure та Fast Boot.

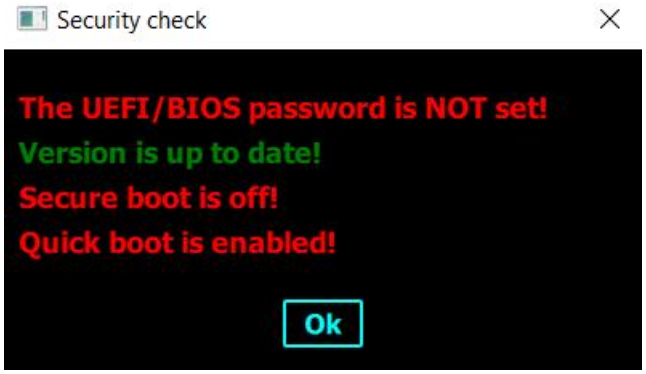

Рисунок 4.1 – Приклад місконфігурації

Завдяки цим перевіркам, користувач, може перевірити стан налаштувань BIOS/UEFI, та змінити їх, при необхідності.

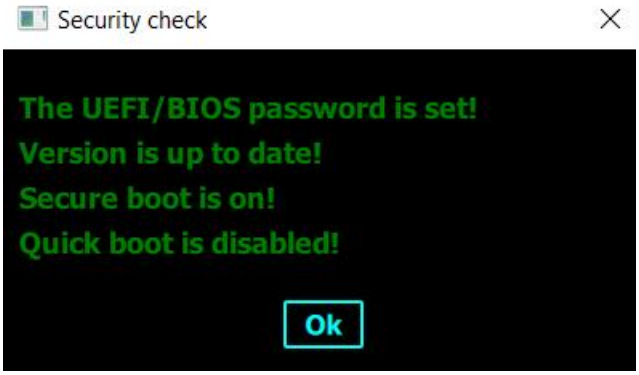

Рисунок 4.2 – Приклад правильної конфігурації

ВИСНОВКИ

В результаті виконання кваліфікаційної роботи було проведено аналіз методів управління комп’ютерних систем BIOS та UEFI, який включав у себе принципи роботи обох систем, різниця між системами. На основі недоліків однієї з систем був описан перехід від цієї системи до більш нової, покращення налаштувань конфігурацій даних систем, та оновлення програмного застосунку задля допомоги звичайному користувачеві перевірки найважливіших налаштувань зі сторони кібербезпеки.

В роботі був описан детальний процес загрузки комп’ютера та усіх його компонентів. Від подачі живлення до старту роботи операційної системи. Детально описані найрізноманітніші варіанти помилок різних виробників BIOS, як звукових, під час проходження Power-On Self Test, так і текстові для найбільш популярних виробників, була описана еволюція однієї з систем, порівняння зломів даних систем, та підтвердження того, що місконфігурація може звести все нанівець.

Опис кожної з систем відображає важливість та актуальність теми, бо саме оболонка між апаратним та програмним забезпеченням містить ключові функції забезпечення роботоздійності будь-яких приладів. Перехід від BIOS до UEFI майже завершено, але все ще багато користувачів використовують стару систему, саме тому було вирішено все щез зачепити систему BIOS. Також були описані різні додатки задля аналізу різних компонентів комп’ютеру та винайдено узагальнений алгоритм пошуку несправностей цих компонентів.

Нажаль, безпека описаних систем в небезпеці, бо за останні пару років було винайдено багато руткітів, які дозволяють проникати у середину системи, та завдавати значних змін на рівні конфігурації системи та навіть після запуску операційної системи, саме тому дуже важливо зрозуміти як працює система, та запобігти атак у майбутньому.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1 Блог системного администратора [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://poznyaev.ru/blog/programmnoe-obespechenie/tri-programmy-dlya-obnovleniya-bios#GIGABYTE_BIOS.

2 BIOS [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/BIOS.

3 Стартовые процедуры Boot Block [Електронний ресурс] . – 2020. – Режим доступу до ресурсу: http://icbook.com.ua/post/_award6/iboot.html.

4 Award BIOS File Structure [Електронний ресурс] . – 2020. – Режим доступу до ресурсу: https://sites.google.com/site/pinczakko/award-bios-file-structure.

5 UEFI [Електронний ресурс]. – 2019. – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/UEFI.

6 Unified Extensible Firmware Interface [Електронний ресурс] . – 2020. – Режим доступу до ресурсу: https://en.wikipedia.org/wiki/Extensible_ Firmware_Interface.

7 UEFI - Унифицированный расширяемый микропрограммный интерфейс [Електронний ресурс] . – 2020. – Режим доступу до ресурсу: http://datadump.ru/uefi/.

8 UEFI boot: how does that actually work, then? [Електронний ресурс] . – 2020. – Режим доступу до ресурсу: https://www.happyassassin.net/posts/2014/01/25/uefi-boot-how-does-that-actually-work-then/.

9 UEFI FAQS [Електронний ресурс] . – 2020. – Режим доступу до ресурсу: https://uefi.org/faq.

10 UEFI BIOS file device, part two: UEFI Firmware Volume and its contents [Електронний ресурс] . – 2020. – Режим доступу до ресурсу: https://sudonull.com/post/125061-UEFI-BIOS-file-device-part-two-UEFI-Firmware-Volume-and-its-contents.