УДК 004.451(043.2)

Спецификация UEFI и мультизагрузка компьютеров в учебных классах

Ганжа В. А.[1], Сидорик В. В.[2],
[1]Белорусский государственный университет информатики и радиоэлектроники,
[2]Белорусский национальный технический университет

В настоящее время любой специалист IT-сферы — программист, преподаватель вуза, менеджер производства часто вынуждены по роду своей деятельности работать одновременно с несколькими операционными системами. Из экономических соображений в компьютерных классах учреждений образования на одних и тех же компьютерах выгодно развертывание различных операционных систем. В этой связи актуальна проблема мультизагрузки современных операционных систем на одном персональном компьютере.

В данной работе сравниваются возможности загрузки из BIOS через MBR, уже уходящей, с набирающей популярность загрузкой через прошивку UEFI (Unified EFI — Extensible Firmware Interface). Имеется неуклюжий перевод этого термина на русский — «Унифицированный расширяемый интерфейс прошивки».

Этот стандарт активно развивается усилиями международного сообщества [1] при общем курировании Intel [2]. Последняя, сентябрьская, версия спецификации UEFI 2.7A в виде обширного 2500-страничного документа находится здесь [3]. Спецификация UEFI массово внедряется во все вновь выпускаемые материнские платы, поэтому на данный момент найти новый компьютер с традиционным BIOS практически невозможно.

Теоретическая часть

UEFI загрузка операционной системы значительно отличается от загрузки BIOS через MBR. Разберем это несколько подробнее.

UEFI определяет интерфейс между операционной системой и микрокодом прошивки, или интерфейс, располагающийся «поверх» аппаратных компонентов компьютера. В самом названии UEFI определение «расширяемый интерфейс» говорит о том, что это модульная система, которая может функционально легко расширяться и модернизироваться. UEFI по сравнению с BIOS не ограничено только лишь персональными компьютерами архитектуры x86–64, но и претендует на всеплатформенный стандарт. Основное назначение EFI — замена устаревающей технологии BIOS и связанных с ней ограничений.

Основная задача EFI — корректно инициализировать оборудование и передать управление загрузчику операционной системы. В этом плане задача не сильно отличается от задачи традиционного BIOS, но алгоритмы принципиально другие. UEFI можно считать виртуальной платформой, которая предоставляет интерфейсы к оборудованию.

Каковы же истинные причины, которые привели к попыткам замены стандартного BIOS на что-то принципиально новое. На схеме (*рис. 1*) показан алгоритм работы при включении питания и инициализации системы.

UEFI осуществляет загрузку в несколько этапов как бы на нескольких уровнях: сначала перебираются загрузочные записи прошивки, а затем происходит переход к системному раздела ESP (EFI System Partition), где записаны загрузчики. А затем загрузчик на EFI-разделе активирует ОС, которая может быть локализована на каком-то внешнем носителе. Заметим, что «физиче-

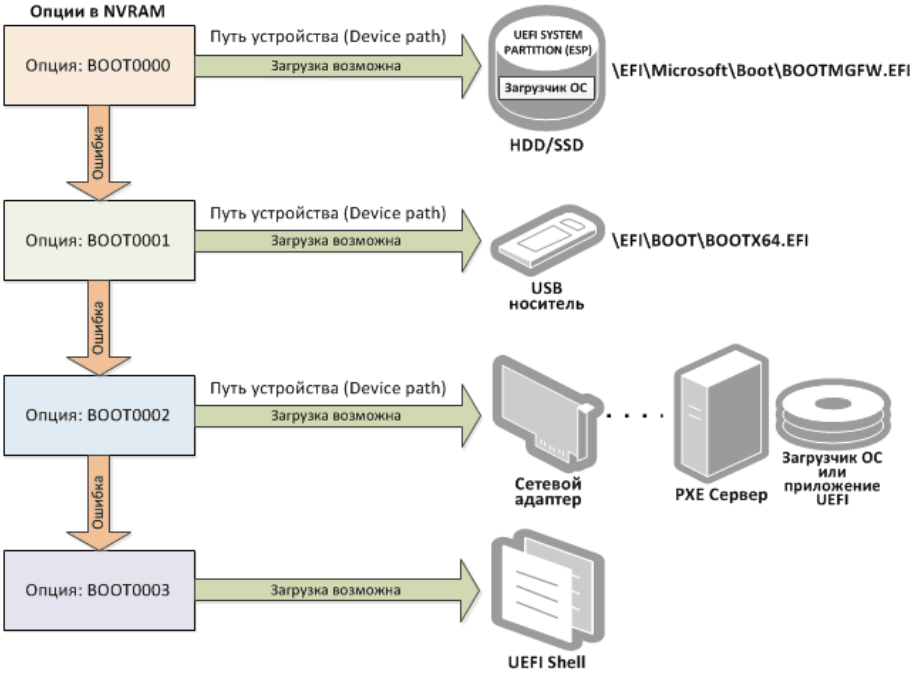

Рисунок 1 — Схема загрузки UEFI

ски» записи прошивки, указывающие путь к загрузчику устройства и файлы самого загрузчика устройства, находятся совсем в разных местах.

Записи прошивки хранятся в NVRAM (Non-Volatile RAM) — это микросхема на системной плате, а загрузчики операционных систем — это файлы с расширением.efi, хранящиеся на системном разделе EFI. Разбиение EFI может быть создано на любом внешнем GPT(GUID Partition Table)-носителе — HDD, SSD, DVD-диск USB-флешка; установщиком при инсталляции операционной системы

Экспериментальная часть

Некоторые описываемые положения авторам удалось реализовать и проверить на серийно выпускаемой аппаратуре. На *рисунке 2* показан графический интерфейс настроек системной платы с UEFI, которая использовалась авторами при написании данной работы. Работает мышь, нажав F12, создается скриншот.

В качестве испытательного полигона использовался настольный компьютер следующей конфигурации:

CPU:	Intel Core i7–7700K 4.2GHz Kaby Lake
RAM:	16 x 4 = 64 GB
Motherboard:	eVGA z270 Classified K
VideoCard:	geForce GTX 1060
SSD:	Samsung EVO pro 850512 Gb
SSD:	Samsung EVO pro 960500 Gb
HDD:	HDD Hitachi HGST 4000
HDD:	HDD Seagate ST3000DM001 Barracuda

Стандартные мышь, монитор, клавиатура и оптический DVD-привод.

Доступ к настройкам прошивки UEFI осуществляется через графический интерфейс с использованием мыши и очень напоминает традиционную работу с legacy BIOS. Доступ же к за-

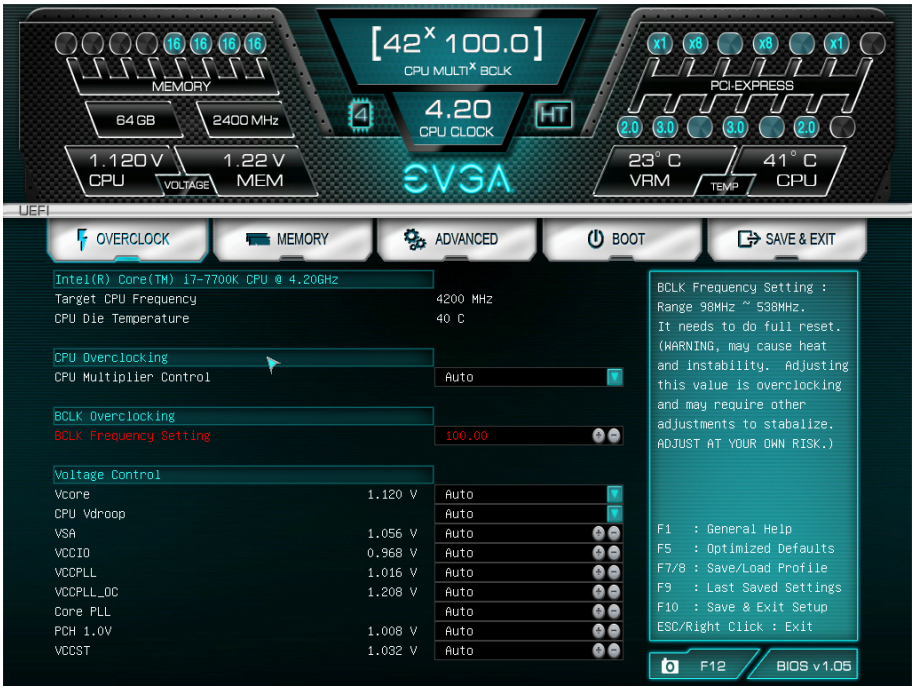

Рисунок 2 — Вид настроек прошивки UEFI мало чем отличается от обычного BIOS

грузочным записям UEFI возможен через Linux-утилиту **efibootmgr**, но во многих руководствах предупреждают о возможности получения непредсказуемого результата при использовании этой утилиты, особенно «на-запись». Авторы следовали этому совету и из соображений безопасности [4], использовали эту утилиту только «на-чтение». Ниже приведены некоторые результаты «на-чтение». Набрав в командной строке эту команду без ключей:

```
efibootmgr
BootCurrent: 0000
Timeout: 2 seconds
BootOrder: 0000,0002,0003
Boot0000* Booting z270
Boot0002* opensuse
Boot0003* Windows Boot Manager
```

получим отчет о трех имеющихся в прошивке загрузочных записях. От одной из этих записей система должна перейти на EFI-раздел и активировать там загрузчик, показано на *рисунке 3*.

В правой части рисунка, как и в привычном нам legacy BIOS, видим перечень возможных устройств, порядок последовательности которых может настраиваться пользователем. С этих устройств может осуществляется загрузка. Например, первым стоит (Boot Option #1)

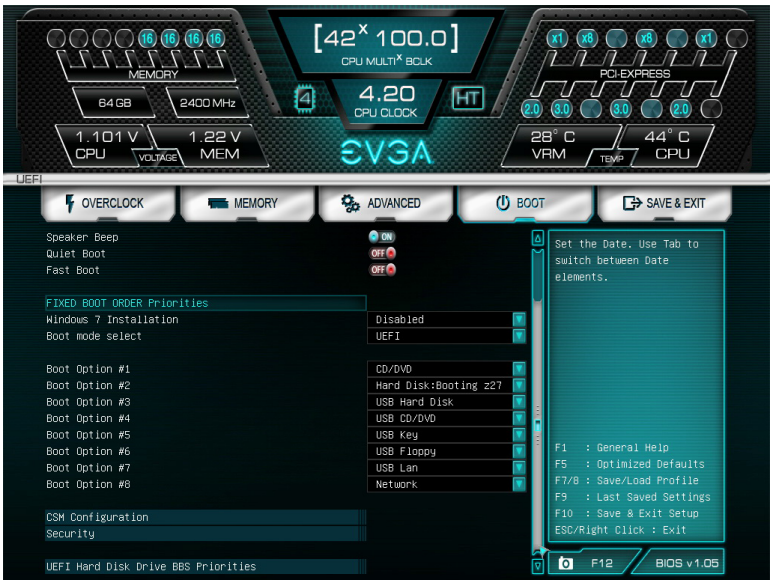

Рисунок 3 — Фрагмент окна настроек с порядком последовательности загружаемых устройств

запуск загрузчика с оптического привода, но если в привод не вставлен загрузочный DVD-диск, осуществляется переход ко второй записи (Boot Option #2) и включается загрузочная система EFI-раздела на Hard Disk: Booting. Эта ситуация отображена на *рисунке 4*, где виден список загрузчиков жесткого диска и три варианта загрузки.

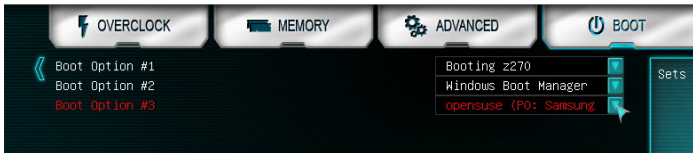

Рисунок 4 — Раскрывшийся список пункта UEFI Hard Disk Driver BBS Priorities

Если все же загрузочный DVD-диск вставлен в привод, то на экране появляется еще одна запись (*рис. 5*) о загрузочном устройстве на оптическом приводе: UEFI CDROM/DVD Driver BBS Priorities.

Если мы в этом меню «войдем» в эту запись, она раскроется и покажет в подменю варианты загрузки с устройства (Boot Option #1) оптического привода (рисунок 6). Скриншот на *рисунок 6* — это полная аналогия ситуации, изображенной на *рисунок 4*, где раскрыты варианты загрузки с жесткого диска (Boot Option #2).

Рисунок 5 — Окно настроек с двумя строками возможных загрузочных разделов EFI

Рисунок 6 — Раскрывшийся список пункта UEFI CDROM/DVD Driver BBS Priorities

Всего на *рисунках 3 и 5* показаны восемь записей (Boot Option #1 — #8). Все эти записи просматриваются прошивкой в порядке возрастания номера от первого до восьмого, и система передаст управление тому активному устройству, которое первым окажется в списке.

Следует отметить, что для успешной загрузки подключаемое в этот список оборудование должно иметь системный EFI раздел расположенный на носителе, отформатированном по правилам GPT. Мы подробно разобрали схему загрузки на втором этапе, когда система анализирует EFI раздел.

На первом этапе, когда UEFI осуществляет перебор загрузочных записей прошивки, используют утилиту управления загрузочными записями rEFInd [5] (*рис. 7*).

Рисунок 7 — Стартовое окно загрузчика rEFInd

Для использования этой утилиты есть две резонных причины. Во-первых, избежать использования опасной команды **efibootmgr**, во-вторых, исключить использование громоздкого Linux GRUB2. Утилита rEFInd при загрузке Linux-системы умеет обращаться непосредственно к ядру операционной системы, минуя GRUB2.

UEFI загрузка “Pro et contra”.

Достоинства:

— упростилась и стала предсказуемой организация загрузки нескольких ОС на одном компьютере;

— наконец, можно избавится от изрядно всем надоевшего, чрезвычайно громоздкого Linux загрузчика GRUB2;

— установщик ОС Microsoft при инсталляции не затирает чужие загрузочные записи.

Недостатки:

— UEFI загрузка сложна и ее настройка и организация силами обычного пользователя проблематична;

— пока нет единого стандарта и четко соблюдаемого всеми протокола, UEFI загрузку каждый производитель аппаратуры будет «понимать» и реализовывать немного по своему, отсюда возникают разночтения и нестыковки;

— система MBR — legacy BiOS еще долго будет востребована пользователями и отражение этого модуль CSM (Compatibility Support Module) в UEFI загрузке.

Литература

1. [Электронный ресурс]. — Режим доступа: http://www.uefi.org/. — Дата доступа: 10.09.2017.
2. [Электронный ресурс]. — Режим доступа: https://www.intel.com/content/ www/us/en/ architecture-and-technology/ unified-extensible-firmware-interface/efi-homepage-general-technology.html#. — Дата доступа: 11.09.2017.
3. [Электронный ресурс]. — Режим доступа: http://www.uefi.org/specifications. — Дата доступа: 15.09.2017.
4. Компьютерные сети. Информационная безопасность / В. А. Ганжа, В. В. Сидорик. Минск : БГУИР, 2014. — 128 с.
5. [Электронный ресурс]. — Режим доступа: http://www.rodsbooks.com/refind/ index.html. — Дата доступа: 10.09.2017.