МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний аерокосмічний університет ім. М. Є. Жуковського

«Харківський авіаційний інститут»

Факультет радіоелектроніки, комп'ютерних систем та інфокомунікацій

Кафедра комп'ютерних систем, мереж і кібербезпеки

**Лабораторна робота № 1**

з «Операційні системи»

(назва дисципліни)

на тему: «Засоби BIOS і EFI, а також програмні засоби віртуалізації»

Виконав: студент 2 курсу групи № 525Б

напряму підготовки (спеціальності)

системне програмування Озеров О.І.

(прізвище й ініціали студента)

Прийняв: к.т.н., доцент кафедри 503

Морозова Ольга Ігорівна

(посада, науковий ступінь, прізвище й ініціали)

Національна шкала: \_\_\_\_\_\_\_\_\_\_

Кількість балів: \_\_\_\_\_

Оцінка: ECTS \_\_\_\_\_

Харків – 2019

## **Цель**:

1. Изучение средств инициализации системы и доступа к аппаратному

обеспечению BIOS и EFI.

2. Изучение программных средств виртуализации.

## **Постановка задачи:**

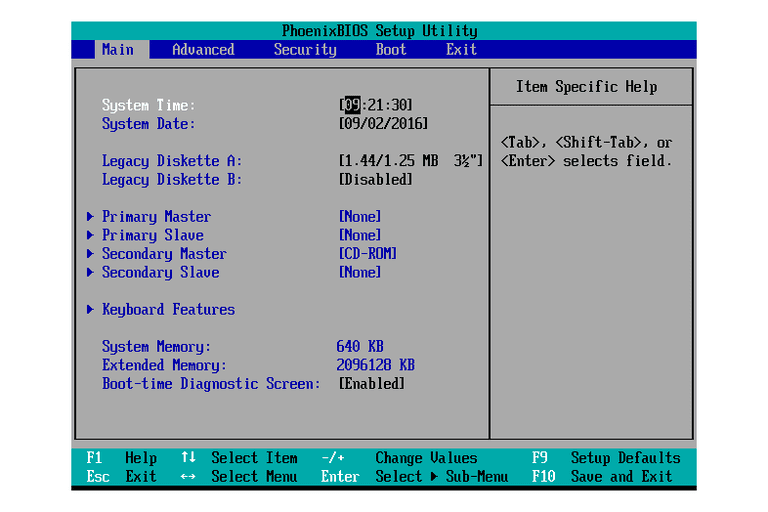
1. Ознакомиться с принципом функционирования средств BIOS-Setup и EFI

shell.

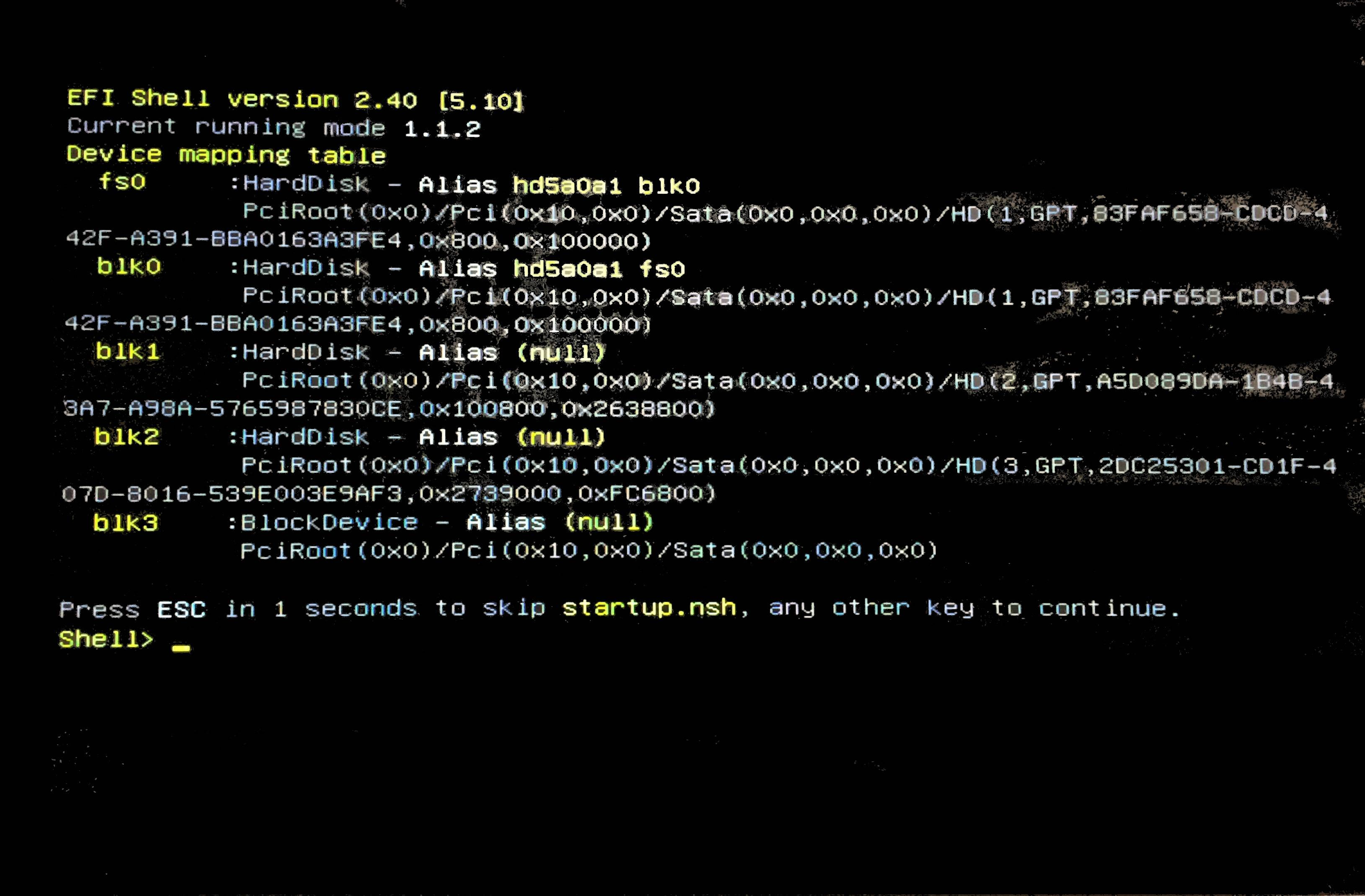
2. Ознакомиться cо средством виртуализации Oracle VM VirtualBox.

1. **Различие между принципом работы BIOS и EFI**

**Пример BIOS:**

****

**Пример EFI:**

****

BIOS считывает информацию с первого сектора жесткого диска, где содержится главная загрузочная запись (MBR) и выбирает загрузочное устройство, где находится операционная система. Поскольку BIOS – это очень старая система, работающая с середины 1970-х гг, то она до сих пор работает в 16-битном режиме. Это обстоятельство ограничивает количество информации, которое может быть прочитано из системной ROM (постоянной памяти компьютера).

EFI выполняет ту же задачу, но делает это немного по-другому. Она хранит всю информацию об инициализации и начальной загрузке системы в специальном файле, находящемся на жестком диске в особом разделе ESP (EFI System Partition). Кроме того, ESP содержит загрузочные программы операционной системы, установленной на компьютере.

EFI в перспективе предназначена для полной замены BIOS и предлагает много новых функций и улучшений, которые не могут быть реализованы в BIOS:

1. **Отсутствие ограничений объема разделов и их количества.**Для хранения информации о жестком диске БИОС использует главную загрузочную запись (MBR), в то время как EFI – так называемую GPT (GUID partition table). Основная разница между ними состоит в том, что MBR использует 32-битные элементы, что позволяет системе иметь лишь 4 физических раздела диска, а каждый раздел может быть размером не более 2 терабайт. Что же касается GPT, то она имеет 64-битные элементы, что позволяет системе иметь до 128 разделов размером до зеттабайта (1021 байт).
2. **Скорость и производительность.** Поскольку технология EFI не зависит от конкретной платформы, то она способна уменьшить время загрузки и увеличить скорость работы компьютера, особенно в том случае, если в системе установлены объемные жесткие диски.
3. **Безопасность.** Самым большим преимуществом EFI по сравнению с БИОС является безопасность. Она реализуется при помощи технологии Secure Boot (безопасный запуск), поддерживаемой операционной системой Windows 8. Поскольку Secure Boot имеет возможность запрашивать цифровую подпись у загрузочных программ, то интерфейс EFI позволяет использовать во время загрузки только аутентифицированные драйверы и службы. Secure Boot контролирует процесс загрузки до тех пор, пока операционная система полностью не загружена. Это дает гарантию того, что во время загрузки в компьютер не проникнет вредоносное ПО.
4. **Обратная совместимость.** Для обратной совместимости большинство реализаций EFI на компьютерах архитектуры PC также поддерживают режим Legacy BIOS для дисков с MBR. Для этого в EFI существует функция CSM (Compatibility Support Module, модуль поддержки совместимости). В случае диска с MBR загрузка производится в том же режиме, что и в системах на основе BIOS. Также возможна загрузка систем на основе BIOS с дисков, имеющих GPT.
5. **Поддержка сетевой загрузки.** EFI может осуществлять загрузку через сеть при помощи технологии Preboot eXecution Environment (PXE). Эта технология поддерживает основные сетевые протоколы, такие, как IPv4 и IPv6, UDP, DHCP и TFTP. Также поддерживается загрузка с загрузочных образов, хранящихся в сетевых хранилищах данных.
6. **Менеджер загрузки.**В стандарте EFI менеджер загрузки определяется как инструмент, предназначенный для загрузки операционной системы и всех необходимых драйверов. Загрузчики операционной системы хранятся в файлах, к которым может осуществляться доступ со стороны встроенного ПО. EFI поддерживает файловые системы FAT32, а также FAT16 и FAT12 для съемных носителей. EFI не зависит от загрузочных секторов, хотя ESP отводит для них место в целях обратной совместимости. Загрузчики автоматически определяются программным обеспечением EFI, что позволяет осуществлять загрузку со съемных носителей.

## **История возникновения технологии**

Технология EFI BIOS изначально была разработана компанией Intel. Сейчас стандарт EFI разрабатывается организацией EFI Forum.

Первоначальной мотивацией для разработки EFI были ограничения BIOS, такие, как 16-битный процессорный режим, 1 МБ адресуемого пространства памяти, что было неприемлемо для серьезных серверных платформ, таких, как Itanium. Попытка устранить эти проблемы в 1998 г. первоначально получила название Intel Boot Initiative, а затем была переименована в EFI.

В 2005 году Intel приостановила развитие стандарта EFI на версии 1.10 и передала его Unified EFI Forum, которая развила стандарт в версию EFI. При этом владельцем исходного стандарта EFI BIOS продолжает оставаться Intel, выдающая лицензии на продукты, основанные на технологии EFI. Версия EFI 2.1 была выпущена в январе 2007 г. В ней были добавлены возможности шифрования данных, сетевой аутентификации и технология User Interface Architecture. Текущая версия стандарта EFI 2.4 была принята в июле 2013г.

## **Критика EFI**

В адрес EFI порой высказывается критика, в частности со стороны поборников информационных прав. Например, компьютерный эксперт Рональд Г. Миних, один из разработчиков альтернативной открытой технологии загрузки Coreboot, осуждает EFI как попытку ограничить возможность пользователя полностью контролировать свой компьютер. Кроме того, он считает, что эта технология не решает ни одной из застарелых проблем традиционного BIOS, в частности, потребности в двух драйверах – одного для встроенного ПО, другого – для операционной системы.

## **Заключение**

EFI – это технология, которая имеет как немало преимуществ, так и недостатки. На сегодняшний день она еще не распространена повсеместно и не поддерживается всеми компьютерами и другими устройствами. Наличие встроенного в EFI менеджера загрузки означает, что отпадает необходимость в отдельных загрузчиках. Кроме того, эта технология может работать совместно с BIOS(в режиме совместимости — Legacy BIOS) и независимо от нее. При этом BIOS по-прежнему может использоваться там, где не требуется хранить большие объемы данных, а проблема безопасности не является чрезвычайно актуальной.

## **2. Сценарии использования виртуальных машин**

Выполнение нескольких ОС на одном компьютере

Виртуальная машина обеспечивает одновременную работу нескольких операционных систем на одном компьютере с Windows или Linux. Создавайте виртуальные машины с операционными системами Linux и Windows, а также с другими средами серверов, настольных или планшетных компьютеров, с настраиваемыми виртуальными сетями и средствами моделирования состояния сети. Эти виртуальные машины можно использовать для разработки и тестирования приложений, создания архитектуры решения, демонстрации продукта и т. д.

Возможности разработки и тестирования на любой платформе

ВМ поддерживает сотни операционных систем и работает с облачными и контейнерными технологиями, такими как Docker и Kubernetes.

Подключение к VMware vSphere

Безопасное подключение к серверам vSphere, [ESXi](https://www.vmware.com/ru/products/esxi-and-esx.html) или к другим серверам на платформе Workstation дает возможность управлять виртуальными машинами и физическими узлами. Общая платформа обеспечивает максимальную производительность и дает возможность без труда переносить виртуальные машины с локального компьютера и на него.

Защита и изоляция сред

Безопасно выполняйте второй настольный компьютер с другими параметрами конфиденциальности, средствами и конфигурациями сети или используйте средства для изучения уязвимостей операционных систем. Workstation предоставляет один из наиболее безопасных гипервизоров в отрасли, а также поддерживает мощные возможности для профессионалов в области ИТ-безопасности.

## **3. Создание ВМ**

Процесс создания виртуальной машины представлен на скриншотах ниже:

