Лабораторная №1 Изучение безопасности UEFI BIOS на базе платформ Intel

Цель данной работы – ознакомление с базовой архитектурой UEFI BIOS и их механизмами защиты. Лабораторная выполняется в парах по 2 человека под платформу Intel (объединяемся с обладателями ноутбуков и или ПК на Intel).
В рамках лабораторной требуется выполнить следующие действия и описать в отчете подробно все дальнейшие выполняемые действия со скриншотами:

1. Изучить процесс загрузки ЭВМ на базе UEFI BIOS в соответствии со спецификацией https://uefi.org/sites/default/files/resources/UEFI_Spec_2_8_final.pdf
2. Получить образ UEFI BIOS вашего ПК/Ноутбука с официального сайта производителя.
3. С использованием утилиты UEFITool открыть образ UEFI BIOS https://github.com/LongSoft/UEFITool
4. Определить модульный состав и точку входа для всех фаз функционирования UEFI BIOS.
5. С помощью утилиты **CHIPSEC** https://github.com/chipsec/chipsec определить конфигурацию LPC/SPI-устройства
6. Определить поддержку технологий Intel Boot Guard, Intel BIOS Guard, Secure Boot и их конфигурацию. Сделать предположение о корректности заданной производителем конфигурации данных технологий.
7. В модульном составе UEFI BIOS выявить модуль Setup
8. С помощью утилиты **Universal-IFR-Extractor** https://github.com/LongSoft/Universal-IFR-Extractor извлечь IFR-информацию из Setup-модуля.
9. Выявить скрытые опции настройки UEFI BIOS через NVRAM-переменные
10. Сделать вывод о безопасности UEFI BIOS на исследуемой платформе.

Состав отчета

1. Электронный вид, печатаем только титул
2. Формулировка задания
3. Описание исследуемой платформы
4. Описание характеристик UEFI BIOS (версия, размер, производитель, состав и назначение регионов)
5. Подробно со скриншотами описание проделанной работы.

Доп. литература:

1. Цикл статей «О безопасности UEFI»:
    a. https://habr.com/ru/post/266935/
    b. https://habr.com/ru/post/267197/
    c. https://habr.com/ru/post/267237/
    d. https://habr.com/ru/post/267491/
    e. https://habr.com/ru/post/267953/
    f. https://habr.com/ru/post/268135/
    g. https://habr.com/ru/post/268423/
2. Fractured Backbone: Breaking Modern OS Defenses with Firmware Attacks https://www.youtube.com/watch?v=ryKy9LvmSIs
3. CHIPSEC Platform Security Assessment Framework https://www.blackhat.com/docs/us-14/materials/arsenal/us-14-Bulygin-CHIPSEC-Slides.pdf https://telegra.ph/Pentest-UEFI-Ocenivaem-zashchishchennost-proshivki-UEFI-s-pomoshchyu-CHIPSEC-08-31
4. BIOS Guard: https://www.youtube.com/watch?v=kSQVGFbTfqE

5. Boot Guard: https://www.youtube.com/watch?v=8M5KqGmbnE4