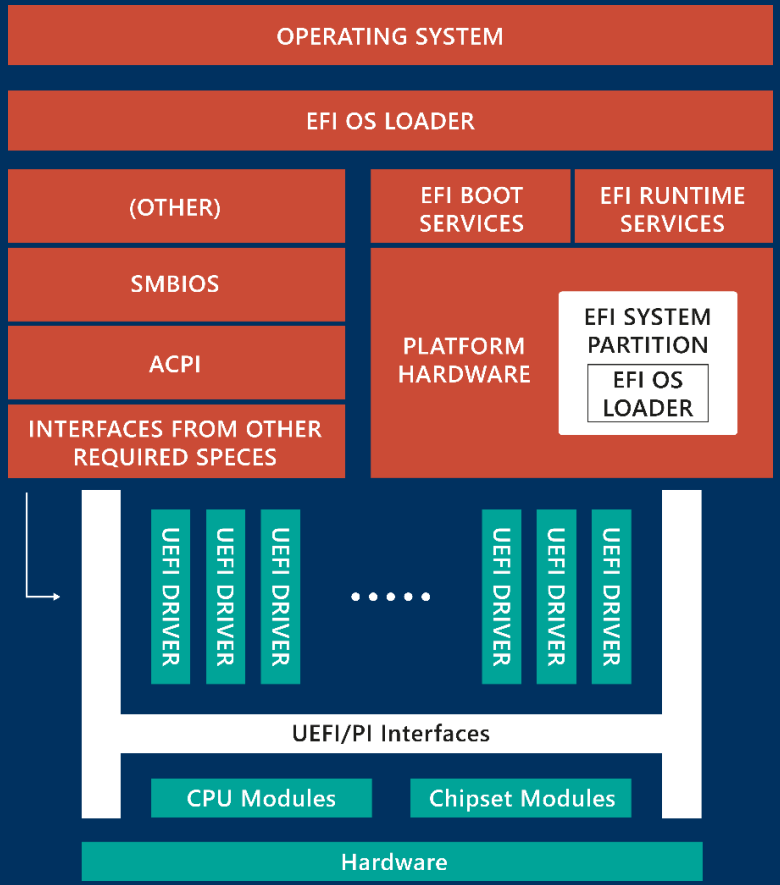
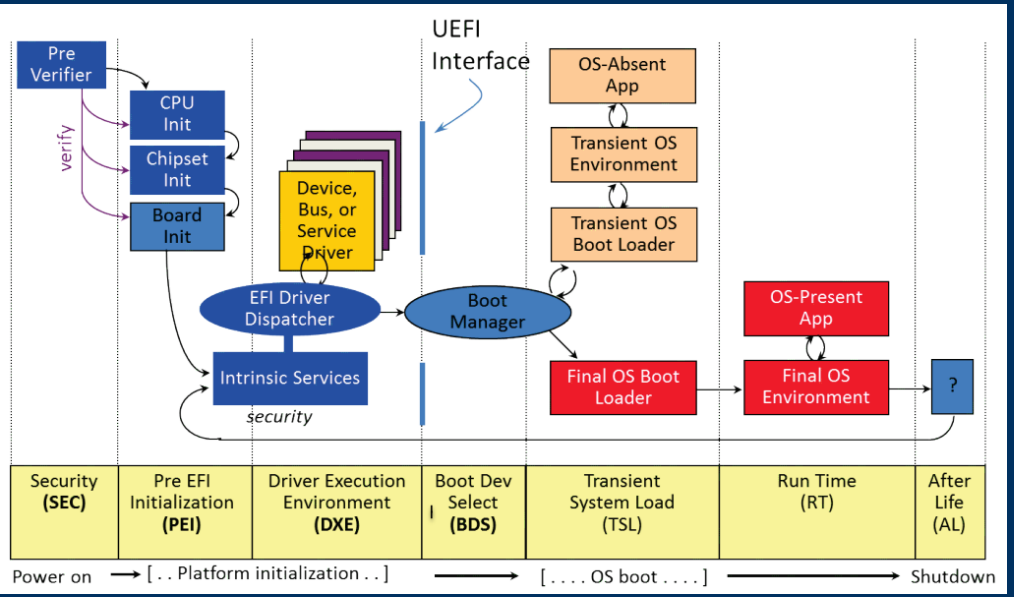
Практика организации доверенной загрузки. Разбор первых опытов внедрения ViPNet SafeBoot

Как устроен UEFI BIOS и насколько защищён?

Архитектура UEFI BIOS





Фазы инициализации платформы

(SEC) – reset vector

(PEI) – первичная инициализация

(DXE) – общая инициализация

(BDS) – выбор загрузчика

ТЕХНО 2020 infotecs ФЕСТ

А что «там» с безопасностью?

Так ли безопасен UEFI BIOS с привнесёнными функциями безопасности?

Модель угроз – нарушитель

- Нарушитель имеет физический доступ
  - Нарушитель высокого уровня (умеет работать с программатором)
  - Нарушитель среднего уровня (нет программатора, но знает, как всё устроено)
  - Нарушитель низкого уровня (~~уборщица~~)
- Нарушитель имеет удалённый доступ….

Модель угроз – ключевые векторы атаки

- Загрузка нового кода или модификация исходного кода UEFI BIOS
- Изменение загрузчика, атаки на SecureBoot (bootkit)
- Возможность загрузки с внешнего носителя

Заблуждения

Пароль на UEFI BIOS = безопасность

- Сброс пароля на персональных компьютерах не занимает много времени
- На ноутбуках необязательно сбрасывать пароль через батарейку – есть решение - https://bios-pw.org/

Заблуждения

Secure Boot это почти безопасно

- Shim – подписанный загрузчик (можно найти на github)
- UEFI Shell + загрузчик Clover
- Очередь загрузки можно поменять в переменной EFI «BootOrder»

Резонансные, успешно реализованные атаки

LoJax – первый известный UEFI руткит

Уязвимость загрузчика операционной системы

- CVE-2020-10713. Опубликована 29 июля 2020 компанией Eclypsium. Уязвимость напрямую связана с доверенной загрузкой операционных систем.
- Уязвимости подвержены практически все операционные системы, использующие Secure Boot (загрузчик GRUB2).
- Проблему быстро не решить(!)

ViPNet SafeBoot не использует ни Secure Boot, ни загрузчик GRUB2, ни загрузчик shim.

Изображение взято с сайта https://eclypsium.com/2020/07/29/theres-a-hole-in-the-boot/

Malware - MosaicRegressor

- Найден в начале октября 2020.
- Полный отчёт от АО «Лаборатория Касперского».
- Код malware основан на malware от Hacking Team bootkit.
- Задачи:
  - Сбор информации и документов с компьютера, архивация материалов и отправка на удалённый сервер.
  - Получение вредоносного кода от удалённого сервера и выполнение этого кода.

Банк угроз

ТЕХНО 2020 infotecs фест

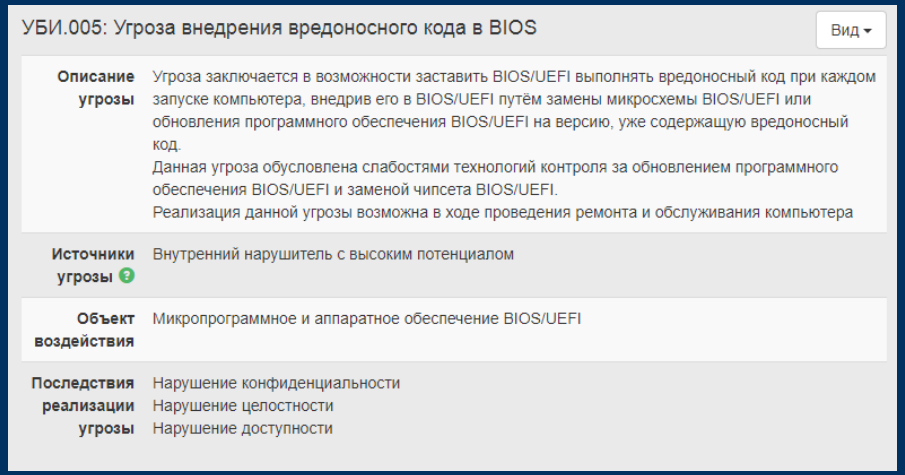
29 угроз

в полной или косвенной мере относящиеся к угрозам BIOS/UEFI BIOS

Угроза
УБИ.004: Угроза аппаратного сброса пароля BIOS
УБИ.005: Угроза внедрения вредоносного кода в BIOS
УБИ.008: Угроза восстановления аутентификационной информации
УБИ.006: Угроза внедрения кода или данных
УБИ.009: Угроза восстановления предыдущей уязвимой версии BIOS
УБИ.013: Угроза деструктивного использования декларированного функционала BIOS
УБИ.018: Угроза загрузки нештатной операционной системы
УБИ.023: Угроза изменения компонентов системы
УБИ.024: Угроза изменения режимов работы аппаратных элементов компьютера
УБИ.030: Угроза использования информации идентификации/аутентификации, заданной по умолчанию
УБИ.032: Угроза использования поддельных цифровых подписей BIOS
УБИ.035: Угроза использования слабых криптографических алгоритмов BIOS
УБИ.039: Угроза исчерпания запаса ключей, необходимых для обновления BIOS
УБИ.045: Угроза нарушения изоляции среды исполнения BIOS

Угроза
УБИ.053: Угроза невозможности управления правами пользователей BIOS
УБИ.072: Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS
УБИ.087: Угроза несанкционированного использования привилегированных функций BIOS
УБИ.090: Угроза несанкционированного создания учётной записи пользователя
УБИ.108: Угроза ошибки обновления гипервизора
УБИ.121: Угроза повреждения системного реестра
УБИ.123: Угроза подбора пароля BIOS
УБИ.124: Угроза подделки записей журнала регистрации событий
УБИ.129: Угроза подмены резервной копии программного обеспечения BIOS
УБИ.144: Угроза программного сброса пароля BIOS
УБИ.145: Угроза пропуска проверки целостности программного обеспечения
УБИ.150: Угроза сбоя процесса обновления BIOS
УБИ.152: Угроза удаления аутентификационной информации
УБИ.154: Угроза установки уязвимых версий обновления программного обеспечения BIOS
УБИ.179: Угроза несанкционированной модификации защищаемой информации

Подробнее об угрозах

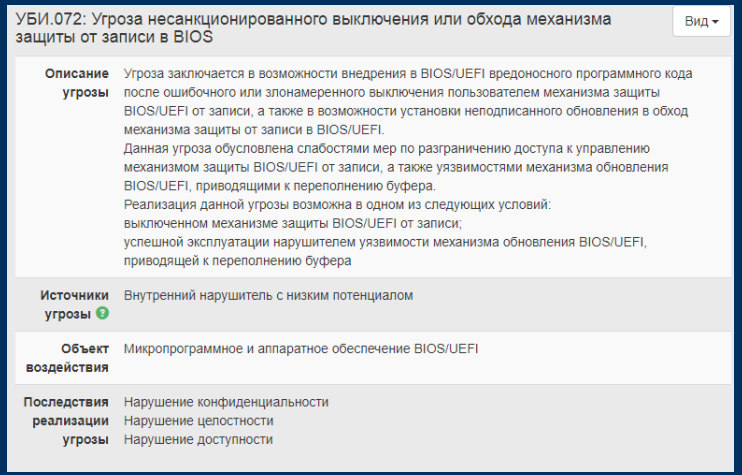


УБИ.005: Угроза внедрения вредоносного кода в BIOS

Вид

Описание угрозы	Угроза заключается в возможности заставить BIOS/UEFI выполнять вредоносный код при каждом запуске компьютера, внедрив его в BIOS/UEFI путём замены микросхемы BIOS/UEFI или обновления программного обеспечения BIOS/UEFI на версию, уже содержащую вредоносный код. Данная угроза обусловлена слабостями технологий контроля за обновлением программного обеспечения BIOS/UEFI и заменой чипсета BIOS/UEFI. Реализация данной угрозы возможна в ходе проведения ремонта и обслуживания компьютера
Источники угрозы	Внутренний нарушитель с высоким потенциалом
Объект воздействия	Микропрограммное и аппаратное обеспечение BIOS/UEFI
Последствия реализации угрозы	Нарушение конфиденциальности Нарушение целостности Нарушение доступности

Угроза внедрения вредоносного кода в BIOS



УБИ.072: Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS

Вид

Описание угрозы	Угроза заключается в возможности внедрения в BIOS/UEFI вредоносного программного кода после ошибочного или злонамеренного выключения пользователем механизма защиты BIOS/UEFI от записи, а также в возможности установки неподписанного обновления в обход механизма защиты от записи в BIOS/UEFI. Данная угроза обусловлена слабостями мер по разграничению доступа к управлению механизмом защиты BIOS/UEFI от записи, а также уязвимостями механизма обновления BIOS/UEFI, приводящими к переполнению буфера. Реализация данной угрозы возможна в одном из следующих условий: выключенном механизме защиты BIOS/UEFI от записи; успешной эксплуатации нарушителем уязвимости механизма обновления BIOS/UEFI, приводящей к переполнению буфера
Источники угрозы	Внутренний нарушитель с низким потенциалом
Объект воздействия	Микропрограммное и аппаратное обеспечение BIOS/UEFI
Последствия реализации угрозы	Нарушение конфиденциальности Нарушение целостности Нарушение доступности

Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS

ViPNet SafeBoot

ViPNet SafeBoot

Высокотехнологичный программный модуль доверенной загрузки, устанавливаемый в UEFI BIOS различных производителей. Предназначен для защиты компьютеров и серверов (в т.ч. и сервероввиртуализации) от современных угроз НСД, связанных с загрузкой ОС и атак на сам BIOS.

Решаемые задачи ViPNet SafeBoot

ТЕХНО 2020 infotecs фест

Организация доверенной загрузки

Контроль целостности

- UEFI BIOS
- MBR
- Таблицы ACPI, SMBIOS, карты распределения памяти
- Файлов
- CMOS

Разграничение доступа

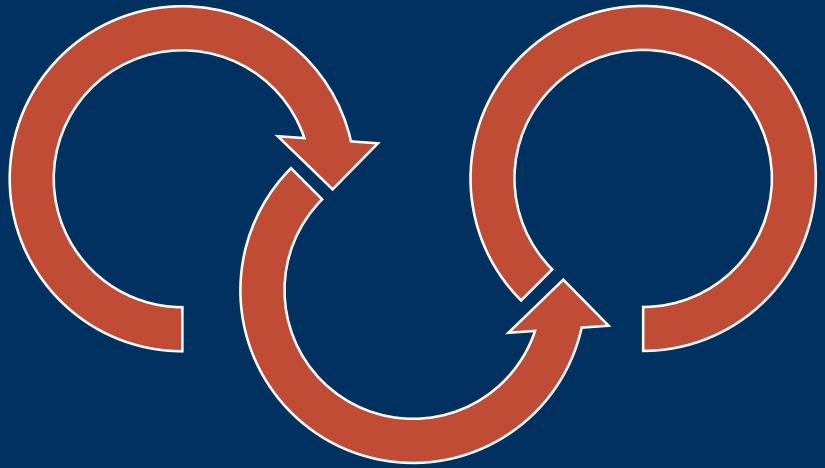
- Двухфакторная аутентификация
- Авторизация в AD/LDAP

Диагностика. Установка. Настройка.

Ключевые вопросы – на которые отвечаем

Где взять продукт?

Где взять необходимые инструменты?



Как установить?

ViPNet SafeBoot

Высокотехнологичный программный модуль доверенной загрузки уровня UEFI BIOS

Документация

Документация на продукты ViPNet представлена в виде zip-архивов или непосредственно в виде pdf-файлов. Для просмотра документации Вам понадобится бесплатная программа Adobe Acrobat Reader. Вы ее можете скачать с сайта компании Adobe. При скачивании документации просим вас обращать внимание на указанный номер версии. Эксплуатируемая вами версия продуктов ViPNet может отличаться от представленной на сайте версии документации. Выберите продукт для получения перечня доступной по нему документации:

Документация	Версия	Размер
Таблица совместимости ViPNet SafeBoot с платформами	от 19.06.2019	28.93 Kb
Комплект документации для ViPNet SafeBoot	1.3 от 13.11.2018	4.5 Mb
Диагностическая утилита – получение информации о UEFI BIOS-компьютера	1.1.38 от 19.06.2019	1.9 Mb

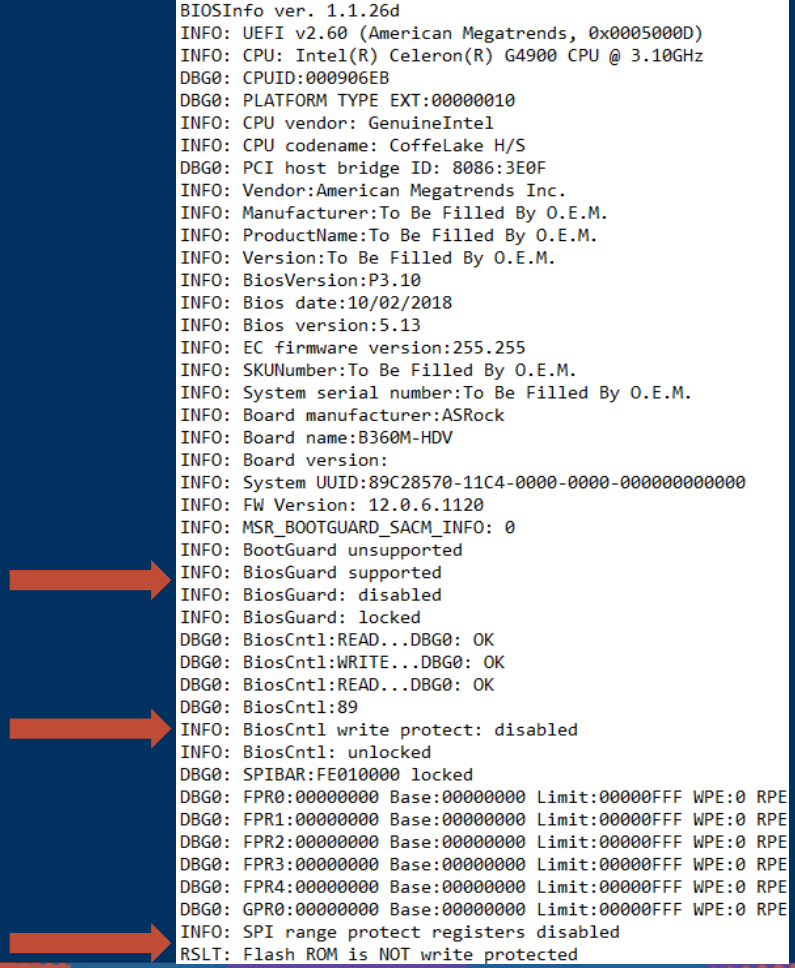
Инструменты для диагностики

Можно скачать с сайта:

- Таблица совместимости
- Документация
- Диагностическая утилита

ТЕХНО 2020 infotecs ФЕСТ

Начинаем



Пример отчёта

Можно пробовать устанавливать ViPNet SafeBoot программным путём.

Для этого необходим дистрибутив.

```
BIOSInfo ver. 1.1.38
INFO: UEFI v2.70 (American Megatrends, 0x0005000E)
INFO: CPU: Intel(R) Xeon(R) Gold 5118 CPU @ 2.30GHz
DBG0: CPUID:00050654
DBG0: PLATFORM TYPE EXT:00000020
INFO: CPU vendor: GenuineIntel
INFO: CPU codename: Skylake SP
DBG0: PCI host bridge ID: 8086:2020
INFO: Vendor:American Megatrends Inc.
INFO: Manufacturer:ASUSTeK COMPUTER INC.
INFO: ProductName:RS500-E9-RS4
INFO: Version:Rev 1.xx
INFO: BiosVersion:5102
INFO: Bios date:02/12/2019
INFO: Bios version:5.14
INFO: EC firmware version:255.255
INFO: System serial number:K1S0CG000075
INFO: Board manufacturer:ASUSTeK COMPUTER INC.
INFO: Board name:Z11PR-D16-DC Series
INFO: Board version:Rev 1.xx
INFO: System UUID:AEEBD332-CEF0-B276-480F-0C9D925BE819
INFO: MSR_BOOTGUARD_SACM_INFO: 400000000
INFO: BootGuard unsupported
INFO: BiosGuard supported
INFO: BiosGuard: disabled
INFO: BiosGuard: locked
DBG0: BiosCntl:AA
INFO: BiosCntl write protect: enabled
INFO: BiosCntl: locked
DBG0: SPIBAR:FE010000 locked
DBG0: FPR0:00000000 Base:00000000 Limit:00000FFF WPE:0 RPE:0
DBG0: FPR1:00000000 Base:00000000 Limit:00000FFF WPE:0 RPE:0
DBG0: FPR2:00000000 Base:00000000 Limit:00000FFF WPE:0 RPE:0
DBG0: FPR3:00000000 Base:00000000 Limit:00000FFF WPE:0 RPE:0
DBG0: FPR4:00000000 Base:00000000 Limit:00000FFF WPE:0 RPE:0
DBG0: GPR0:00000000 Base:00000000 Limit:00000FFF WPE:0 RPE:0
INFO: SPI range protect registers disabled
RSLT: Flash ROM is write protected
```

Пример отчёта

Запись приложения в UEFI BIOS заблокирована, НО:

- Можно провести исследование платформы для отключения защиты

```
INFO: BiosVersion:1.6.0
INFO: Bios date:05/16/2018
INFO: Bios version:1.6
INFO: EC firmware version:255.255
INFO: SKUNumber:0786
INFO: System serial number:9DHSTC2
INFO: Board manufacturer:Dell Inc.
INFO: Board name:0CWJTV
INFO: Board version:A00
INFO: System UUID:4C4C4544-0044-4810-8053-B9C04F544332
INFO: FW Version: 11.8.50.3460
INFO: MSR_BOOTGUARD_SACM_INFO: 30000007D
DBG0: TXT DIDVID:1B0068086
DBG0: TXT VER_EMIF:9D003000
DBG0: BG ERROR Code:00000000
DBG0: Acm Status:808F8003
DBG0: Boot Status:8000000000000000
DBG0: FWSTS4:00084000
DBG0: FWSTS5:00001F01
DBG0: FWSTS6:47C00BC9
DBG0: BootGuard profile: F:1 M:1 V:1 PBE:1 ENF:3
INFO: BootGuard profile 5 detected
INFO: BootGuard supported
INFO: BootGuard protection activated
INFO: System in Verified boot
INFO: System in Measured boot
INFO: Detected BootGuard profile:5
INFO: TPM inited
INFO: TPM type:TPM 2.0
INFO: BiosGuard supported
INFO: BiosGuard: enabled
INFO: BiosGuard: locked
DBG0: BiosCntl:AA
INFO: BiosCntl write protect: enabled
INFO: BiosCntl: locked
DBG0: SPIBAR:FE010000 locked
DBG0: FPR0:00000000 Base:00000000 Limit:00000FFF WPE:0 RPE:0
DBG0: FPR1:00000000 Base:00000000 Limit:00000FFF WPE:0 RPE:0
DBG0: FPR2:00000000 Base:00000000 Limit:00000FFF WPE:0 RPE:0
DBG0: FPR3:00000000 Base:00000000 Limit:00000FFF WPE:0 RPE:0
DBG0: FPR4:00000000 Base:00000000 Limit:00000FFF WPE:0 RPE:0
DBG0: GPR0:00000000 Base:00000000 Limit:00000FFF WPE:0 RPE:0
INFO: SPI range protect registers disabled
RSLT: Flash ROM is write protected
```


Пример отчёта

Всё защищено, необходимо обращаться к производителю

ViPNet SafeBoot

Руководство по установке

ТЕХНО 2020 infotecs фест

Диагностическая установка

Данная процедура проделывается после получения от ИнфоТеКС одобрения на программную установку.

ИСПОЛЬЗУЙТЕ ДОКУМЕНТАЦИЮ

```
ViPNet SafeBoot installation utility version:
1.4.0.27 (2019-05-22 12:44 MSK), release build (LegacyGui)

Installation package integrity verification...

Do you want to run ViPNet SafeBoot diagnostic mode?
Press 'q' to cancel or any other key to continue
```

Диагностическая установка

Данная процедура проделывается после получения от ИнфоТеКС одобрения на программную установку.

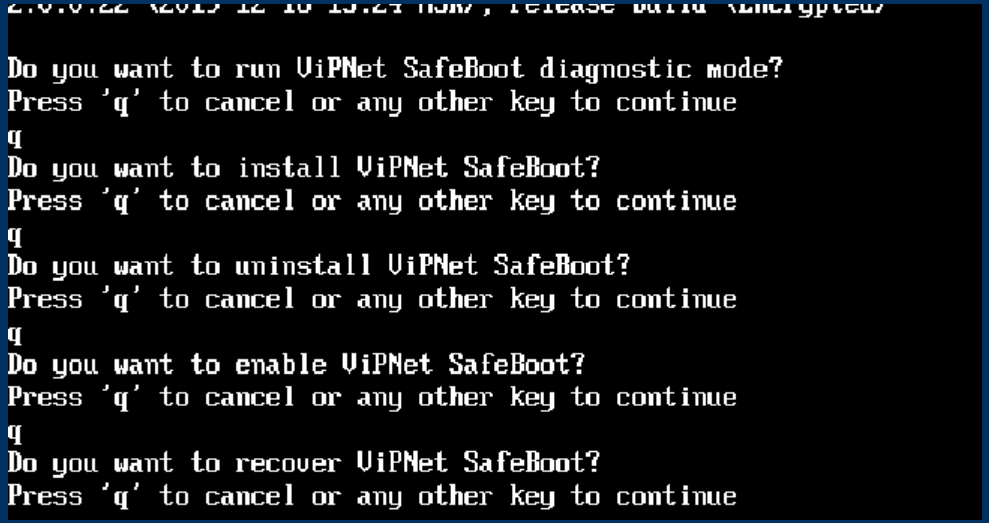
ИСПОЛЬЗУЙТЕ ДОКУМЕНТАЦИЮ

ТЕХНО 2020 infotecs фест

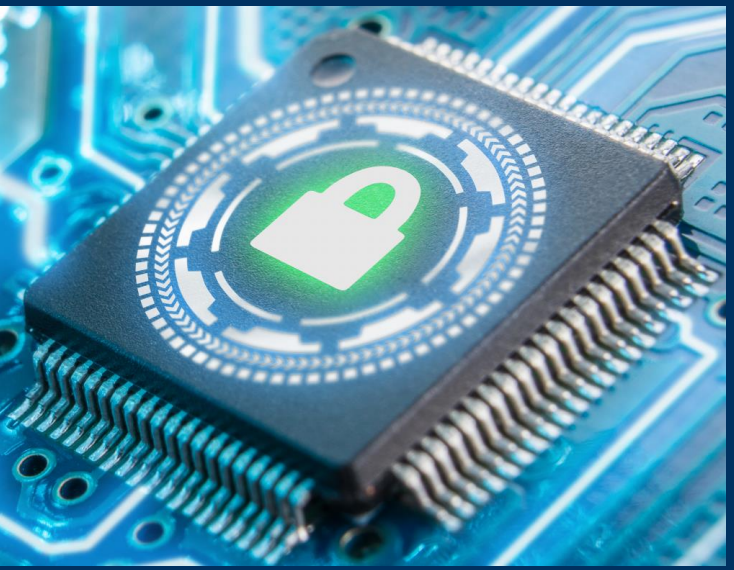
Установка

Продолжаем следовать документации

Дополнительные параметры установки



Пока идёт установка…



Если программная установка не возможна – начинаем общение с производителем платформы

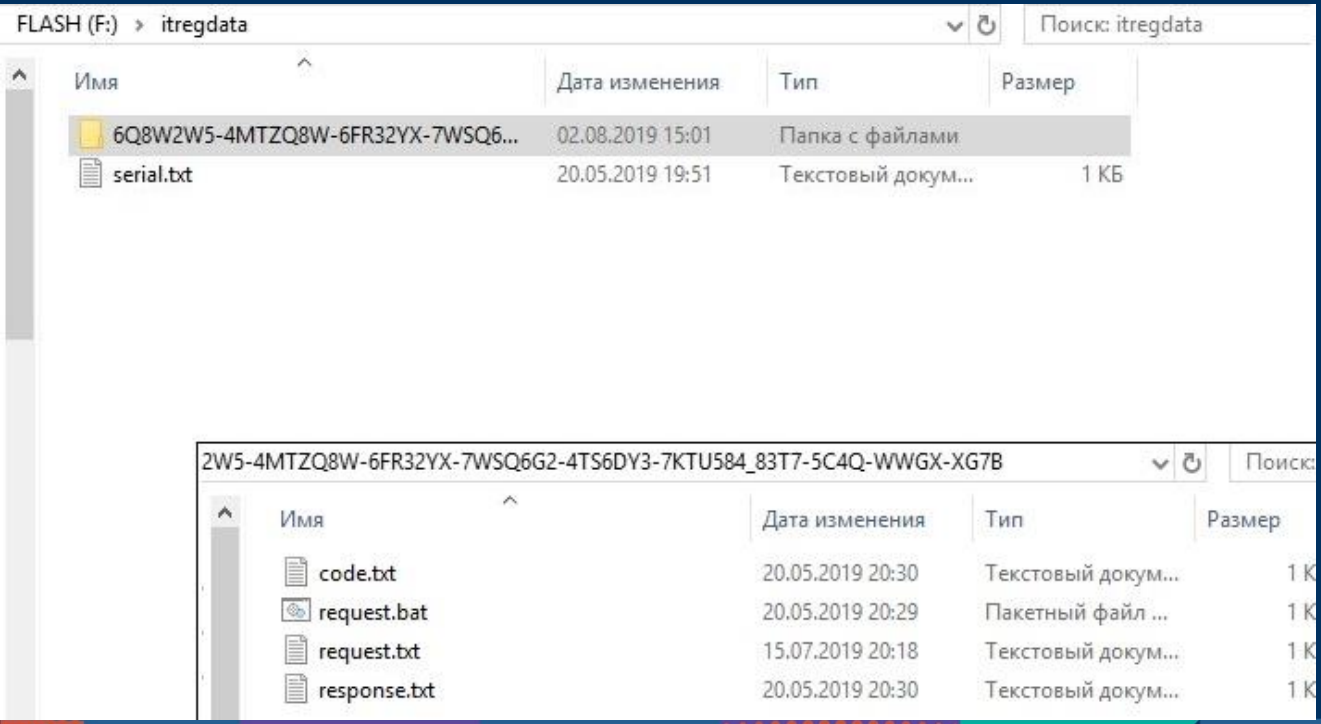
Основные шаги:

- Обсудить варианты встраивания ViPNet SafeBoot в UEFI BIOS
- Подготовить образ UEFI BIOS с ViPNet SafeBoot
- Подписать образ у производителя платформы
- Протестировать
- Установить на платформу штатными средствами обновления UEFI BIOS

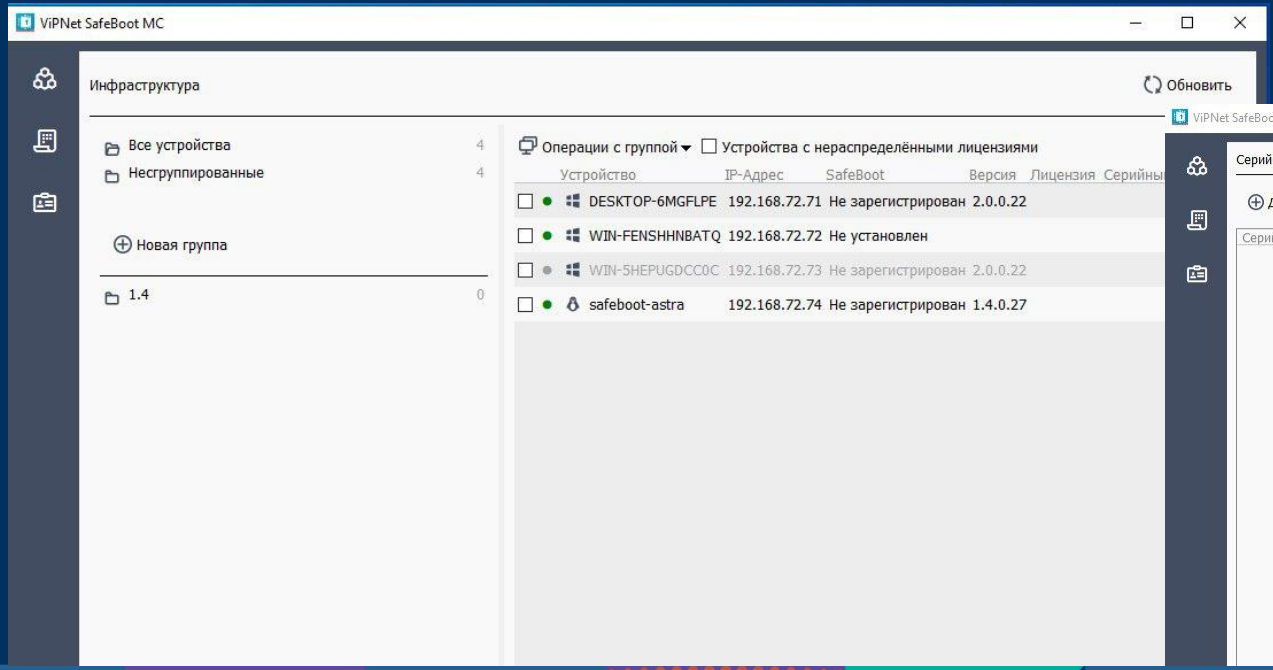
Регистрация ViPNet SafeBoot

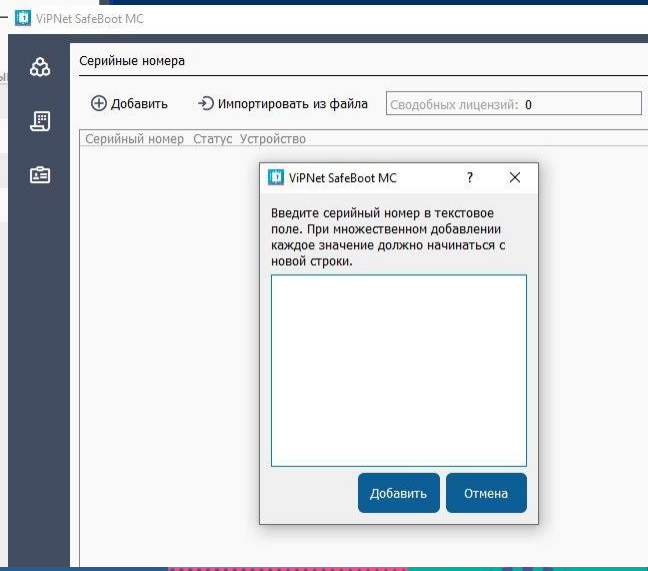
ТЕХНО infotecs 2020 ФЕСТ

Набор файлов при регистрации



Если у вас огромный парк компьютеров ViPNet SafeBoot MC





ТЕХНО 2020 infotecs Фест

ТЕХНО 2020 infotecs Фест

Спасибо за внимание!