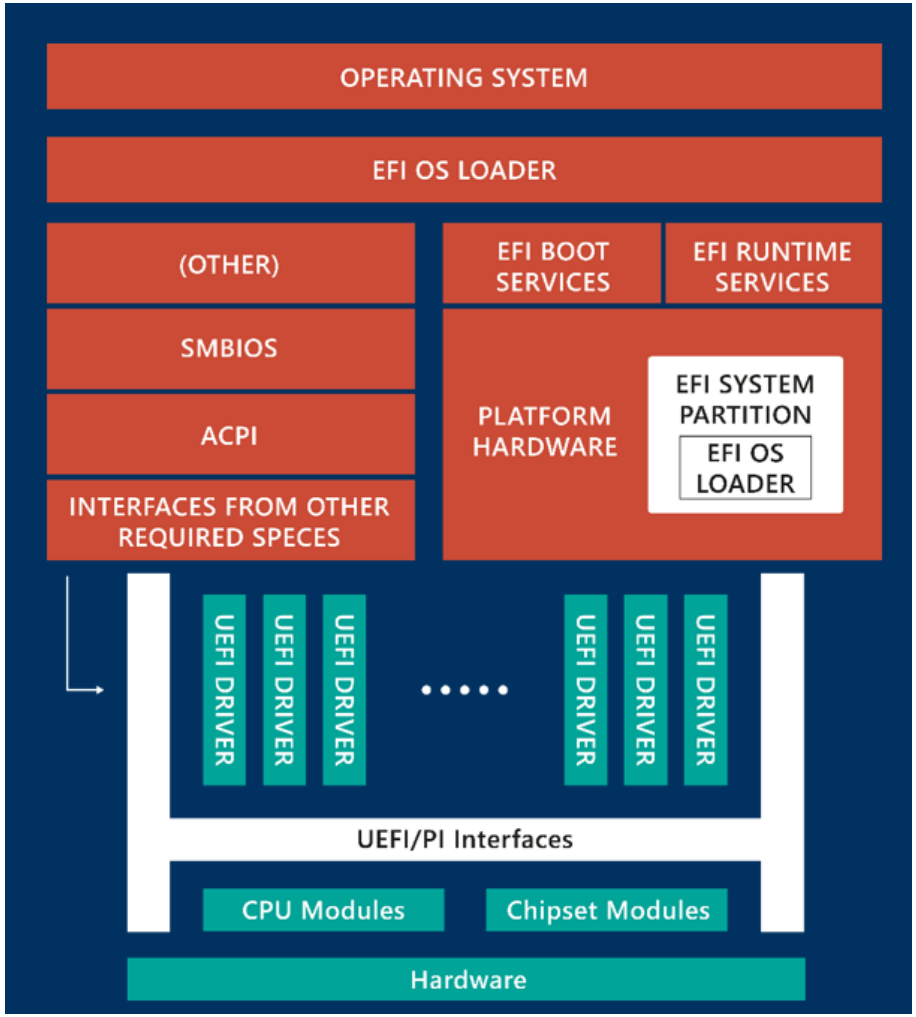
ViPNet SafeBoot

Что было? Что стало? Что будет?

Иван Кадыков
Руководитель направления

С чего всё началось?



Архитектура UEFI BIOS

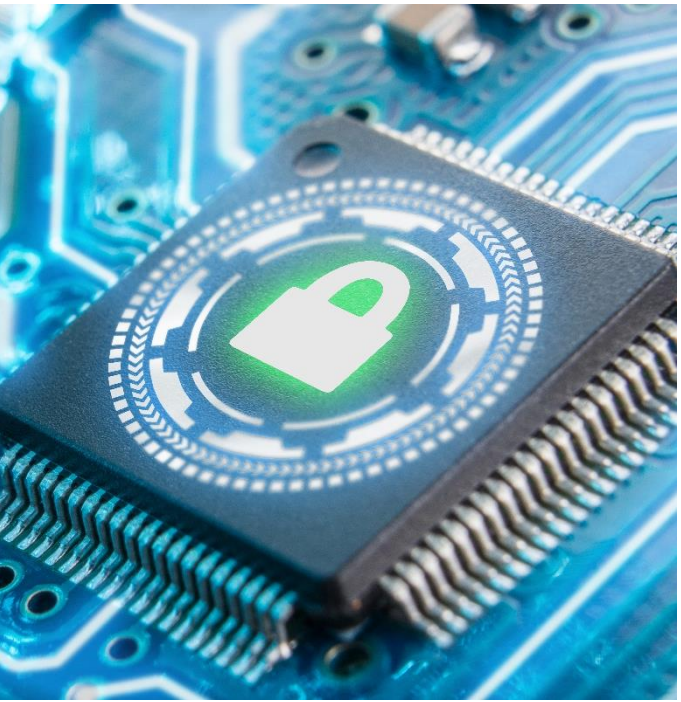
А что «там» с безопасностью?

- Так ли безопасен UEFI BIOS с привнесёнными функциями безопасности?

Модель угроз – ключевые векторы атаки

- Установка вредоносного кода в хранилище основной прошивки и последующий запуск
- Изменение настроек UEFI в NVRAM
- Перехват данных
- Атаки на SecureBoot (отключение или обход)
- Возможность загрузки с внешнего носителя

Ноябрь 2016 года



В свет вышла первая версия программного модуля доверенной загрузки ViPNet SafeBoot.

Главной и отличительной чертой была возможность установки **в любой UEFI BIOS** (любого производителя) спецификации 2.3.1.

ViPNet SafeBoot

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

Решаемые задачи ViPNet SafeBoot

Сертификат № 3823

Сертификат получен год спустя после релиза – 14.11.2017 г.

По требованиям к средствам доверенной загрузки уровня базовой системы ввода-вывода второго класса.

СИСТЕМА СЕРТИФИКАЦИИ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 3823

Выдан 14 ноября 2017 г.
Действителен до 14 ноября 2020 г.

Настоящий сертификат удостоверяет, что **программный комплекс «Программный модуль доверенной загрузки ViPNet SafeBoot»**, разработанный и производимый ОАО «ИнфоТеКС» в соответствии с техническими условиями ФРКЕ.00180-01 97 01 ТУ, является программным средством доверенной загрузки уровня базовой системы ввода-вывода, соответствует требованиям документов «Требования к средствам доверенной загрузки» (ФСТЭК России, 2013) и «Профиль защиты средства доверенной загрузки уровня базовой системы ввода-вывода второго класса защиты. ИТ.СДЗ.УБ2.ПЗ» (ФСТЭК России, 2013) при выполнении указаний по эксплуатации, приведенных в формуляре ФРКЕ.00180-01 30 01 ФО.

Сертификат выдан на основании результатов сертификационных испытаний, проведенных испытательной лабораторией ООО «ЦБИ» (аттестат аккредитации от 11.04.2016 № СЗИ RU.0001.01БИ00.Б004) - техническое заключение от 28.07.2017, экспертного заключения от 12.10.2017 органа по сертификации ФАУ «ГНИИИ ПТЗИ ФСТЭК России» (аттестат аккредитации от 05.05.2016 № СЗИ RU.0001.01БИ00.А002).

Заявитель: ОАО «ИнфоТеКС» (ИНН 7710013769)
Адрес: 127287, г. Москва, Старый Петровско-Разумовский проезд, д. 1/23, стр. 1
Телефон: (495) 737-6192

Контроль маркирования знаками соответствия сертифицированной продукции и инспекционный контроль её соответствия требованиям документов, указанных в настоящем сертификате, осуществляется испытательной лабораторией ООО «ЦБИ».

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ

В. Лютиков

Хронология событий

2017

Ключевые события

- Официальный релиз версий 1.1. и 1.2
- Окончена сертификация 1.0

2018

Ключевые события

- Официальный релиз версии 1.4
- Передача на контроль изменений версии 1.4

2019

Ключевые события

- Официальный релиз версий 1.3
- Передача на контроль изменений версии 1.3
- Завершение котроля изменений для версии 1.3

2020

Ключевые события

- Официальный релиз версии 2.0
- Завершение котроля изменений для версии 1.4
- Передача на сертификацию версии 2.0 – для продления сертификата

2021

Ключевые события

- Выпуск версии 2.1

Ключевые изменения в функциональности

ViPNet SafeBoot 1.3

- Возможность аутентификации пользователей на LDAP/AD сервере
- КЦ Реестра Windows

ViPNet SafeBoot 1.4

- Поддержка JaCarta-2 ГОСТ
- Поддержка работы с сертификатами MS CA в AD
- Деморежим и режим неактивности

ViPNet SafeBoot 2.0

- Новый графический интерфейс
- Защита на уровне SMM (System Management Mode)

Выпущен релиз 2.1

- Защита от Malware в UEFI BIOS
- Активация защиты на платформах AMD
- Поддержка токена Rutoken S
- Поддержка работы со считывателями смарт-карт – ACR38, JCR721, ASEDrive IIIe
- Поддержка SSO для входа в операционную систему и ViPNet SafePoint v.1.2
- Подготовка и доработка механизмов удалённого управления для интеграции с EndPoint Protection
- Умный экспорт-импорт БД ViPNet SafeBoot
- Поддержка сенсорных экранов, реализация сенсорной клавиатуры под UEFI
- Базовая поддержка ARM-архитектуры

«Виды» ViPNet SafeBoot

- Сертифицированная версия 1.4

- Официальная версия 2.0 (проходит сертификацию)
- Ожидания по сертификации апрель 2021

ViPNet SafeBoot MC

Своё управляющее приложение ViPNet SafeBoot MC:

- получение информации о наличии ViPNet SafeBoot на рабочей станции/сервере;
- получение информации об установленной версии ViPNet SafeBoot;
- получение IP-адреса устройства, на котором установлен ViPNet SafeBoot;
- удалённая загрузка лицензий в СДЗ, с возможностью группового лицензирования;
- удалённая регистрация лицензий на сервере лицензирования;
- удалённая выгрузка журналов ViPNet SafeBoot, с возможностью групповой выгрузки.

В данный момент SafeBoot MC встраивается в ViPNet EndPoint Protection.

В реестре отечественного ПО

Главная / Заявления / ViPNet SafeBoot

ViPNet SafeBoot

Сведения о правообладателях программного обеспечения

российская коммерческая организация

Название организации	ОТКРЫТОЕ АКЦИОНЕРНОЕ ОБЩЕСТВО "ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И КОММУНИКАЦИОННЫЕ СИСТЕМЫ"
ИНН	7710013769

Сведения об исключительном праве

Собственная разработка

История изменений

30 Марта 2017	Заявление зарегистрировано
30 Марта 2017	Заявление размещено на сайте
3 Апреля 2017	Назначен ответственный эксперт
3 Апреля 2017	Передано на экспертизу

Заявление о включении в реестр

Дата подачи:
16 Марта 2017

Дата регистрации:
30 Марта 2017

Статус:
Включено в реестр

Заявляемый класс программного обеспечения:
Системы мониторинга и управления, Средства обеспечения информационной безопасности

Сайт правообладателя:
http://infotecs.ru/product/vipnet-safeboot.html

Ссылка на приказ МКС:
Ссылка
Экспертное заключение:
Ссылка

Почему средства доверенной загрузки так необходимы?

Задачи и потребности заказчиков. Compliance

Задача - соответствие требованиям ФСТЭК России по защите ИСПДн, ГИС, АСУ ТП и КИИ – выполнение полного комплекса мер по защите.

Необходимость использования прописана в мерах защиты по первому и второму классу:

- В ИСПДн и ГИС – УПД.17
- В АСУ ТП и КИИ – УПД.3

29 угроз

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

Угроза	Угроза
УБИ.004: Угроза аппаратного сброса пароля BIOS	УБИ.053: Угроза невозможности управления правами пользователей BIOS
УБИ.005: Угроза внедрения вредоносного кода в BIOS	УБИ.072: Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS
УБИ.008: Угроза восстановления аутентификационной информации	УБИ.087: Угроза несанкционированного использования привилегированных функций BIOS
УБИ.006: Угроза внедрения кода или данных	УБИ.090: Угроза несанкционированного создания учётной записи пользователя
УБИ.009: Угроза восстановления предыдущей уязвимой версии BIOS	УБИ.108: Угроза ошибки обновления гипервизора
УБИ.013: Угроза деструктивного использования декларированного функционала BIOS	УБИ.121: Угроза повреждения системного реестра
УБИ.018: Угроза загрузки нештатной операционной системы	УБИ.123: Угроза подбора пароля BIOS
УБИ.023: Угроза изменения компонентов системы	УБИ.124: Угроза подделки записей журнала регистрации событий
УБИ.024: Угроза изменения режимов работы аппаратных элементов компьютера	УБИ.129: Угроза подмены резервной копии программного обеспечения BIOS
УБИ.030: Угроза использования информации идентификации/аутентификации, заданной по умолчанию	УБИ.144: Угроза программного сброса пароля BIOS
УБИ.032: Угроза использования поддельных цифровых подписей BIOS	УБИ.145: Угроза пропуска проверки целостности программного обеспечения
УБИ.035: Угроза использования слабых криптографических алгоритмов BIOS	УБИ.150: Угроза сбоя процесса обновления BIOS
УБИ.039: Угроза исчерпания запаса ключей, необходимых для обновления BIOS	УБИ.152: Угроза удаления аутентификационной информации
УБИ.045: Угроза нарушения изоляции среды исполнения BIOS	УБИ.154: Угроза установки уязвимых версий обновления программного обеспечения BIOS
	УБИ.179: Угроза несанкционированной модификации защищаемой информации

БДУ ФСТЭК России

При аттестации рабочих мест необходимо учитывать БДУ ФСТЭК. Использование ViPNet SafeBoot поможет решить вопрос с закрытием угроз, связанных с BIOS/UEFI BIOS.

Уязвимость загрузчика операционной системы

CVE-2020-10713:опубликована 29 июля 2020 года 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 года.

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.

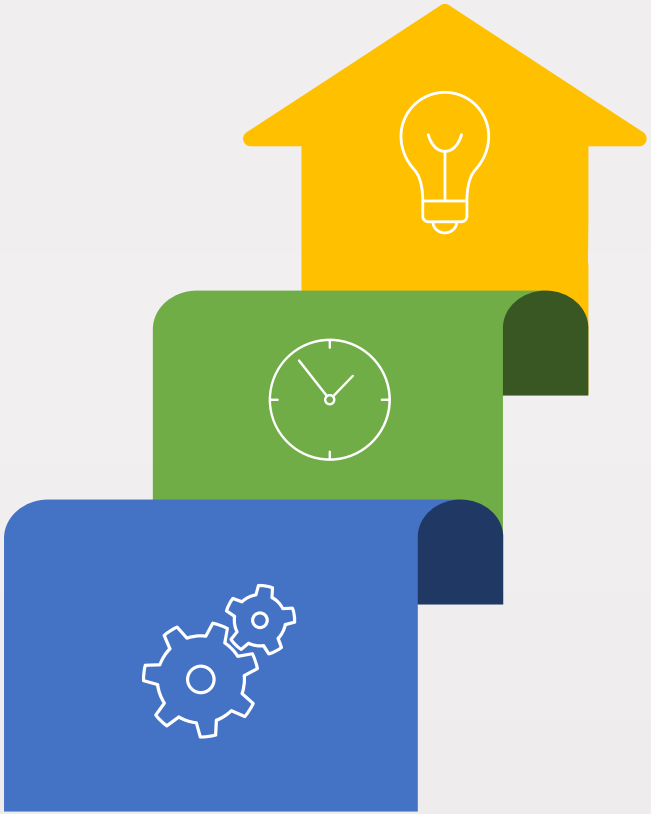
Сопровождение. Техническая помощь

ViPNet SafeBoot – не обычный замок

- Замок без аппаратной составляющей
- Его нельзя потрогать
- Для него не нужны слоты PCI, PCI-E, mini PCI-E, M2

Для ViPNet SafeBoot нужен UEFI BIOS спецификации 2.3.1 и выше.

Самостоятельное предварительное тестирование



Шаг 3

Передача установщика с необходимыми инструкциями для установки.

Шаг 2

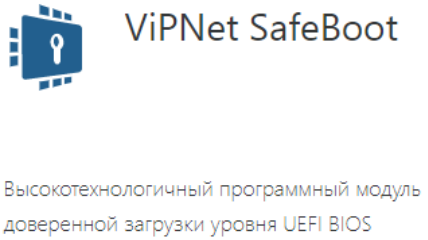
- Наши специалисты оценивают возможность установки.
- В некоторых случаях вам будет выслан дистрибутив ViPNet SafeBoot для организации диагностической установки («виртуальная» установка МДЗ), после чего лог надо отправить снова нам.
- В результате второго шага мы понимаем способ установки.

Шаг 1

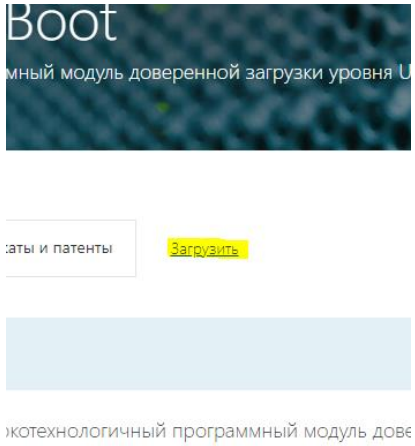
- Определяемся, какие платформы имеем или предполагаем к закупке.
- Скачиваем диагностическую утилиту с сайта https://infotecs.ru/product/vipnet-safeboot.html из раздела «Загрузить».
- Выполняете диагностику и отправляете нам полученный лог.

Где найти диагностическую утилиту

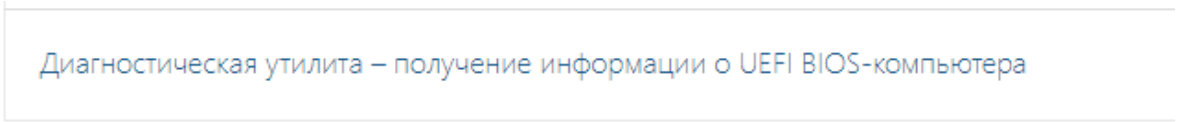
1.



2.



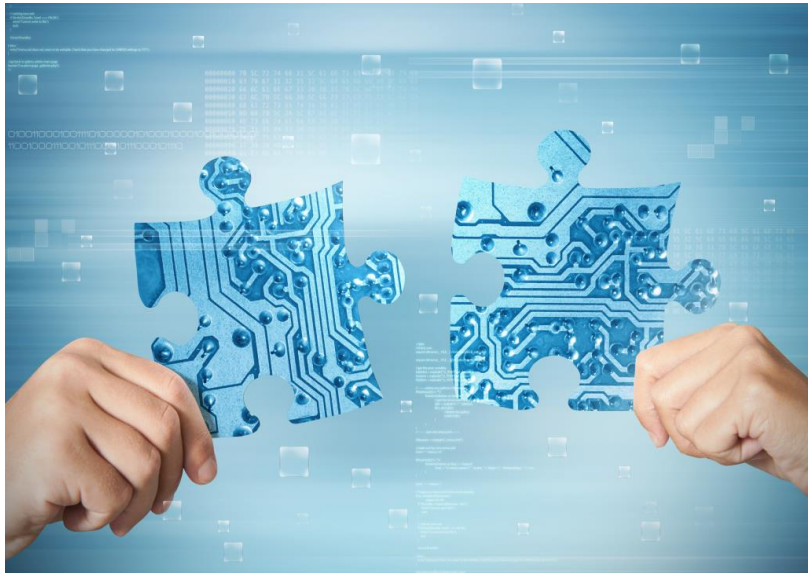
3.



Если компьютеры планируется закупать

- Начинаем общение с производителем платформ по выбранной платформе
- Мы уже работаем с:
  - Аквариус
  - Depo Computers
  - iRU
  - Getac
  - ТОНК
  - Dell
  - Lenovo
  - Asus
  - Acer
  - Рамэк
  - Advantech
  - Panasonic

Актуально для больших проектов!



«На десерт»

В ближайшее время будем работать над релизом 2.2

Ключевые фичи

- Доверенная загрузка по сети(HTTPBoot и PXE) с контролем целостности
- Развитие поддержки платформ с ARM-архитектурой
- Поддержка новых токенов – JaCarta LT и Guardant ID версии 2