infotecs

ViPNet SafeBoot

Давайте разберёмся…

UEFI – повышает безопасность компьютера

UEFI – повышает возможности атаки на компьютер

Повышает безопасность…

Secure boot (UEFI Spec)

- Безопасная загрузка
- Проверка загружаемых модулей

Measured boot

- Использование TPM модуля
- Журналирование всех стадий загрузки и изменений

Повышает возможность атаки…

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

Поэтому желательно использовать МДЗ

infotecs

… НО НЕ ВСЕ ЗАМКИ ОДИНАКОВЫ, ОНИ РАЗЛИЧАЮТСЯ…

ТЕХНИЧЕСКИ:

1. Аппаратно-программные выполненные на платах расширения PCI-E, mini PCI-E, M2.
2. Программные в виде модулей устанавливаемых в UEFI BIOS

ПО СЕРТИФИКАЦИИ:

1. Сертификация ФСТЭК - средства доверенной загрузки (СДЗ)*
   - Уровня базовой системы ввода-вывода
   - Уровня платы расширения
2. Сертификация ФСБ – аппаратно-программные модули доверенной загрузки (АПМДЗ)

*ещё бывают уровня загрузочной записи, но мы их не рассматриваем…

Ключевой набор возможностей для МДЗ

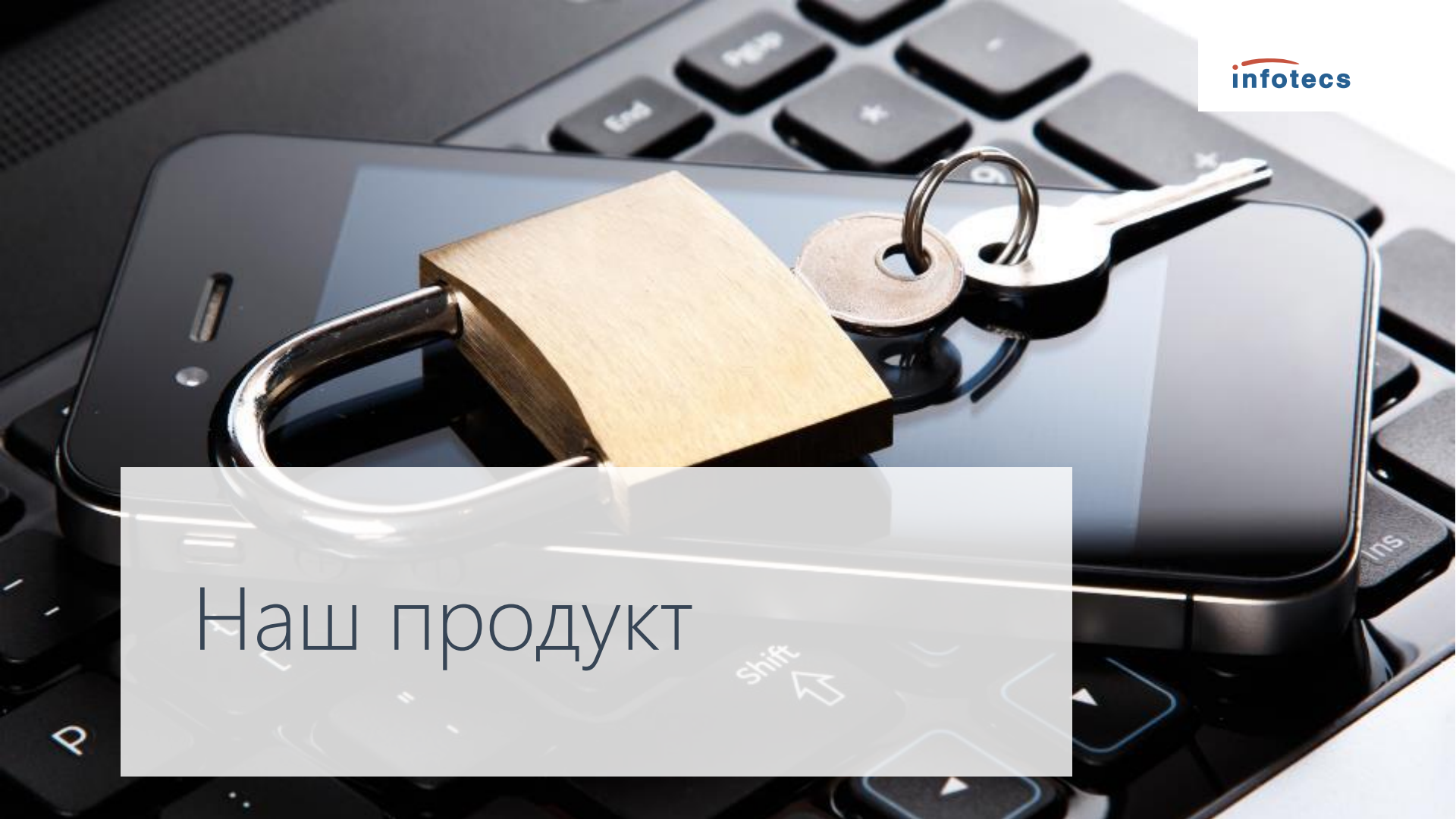
Разграничение доступа

Доверенная загрузка штатной ОС

Контроль целостности ОС и программной среды

Контроль целостности аппаратных составляющих

Ведение внутреннего журнала аудита событий



Наш продукт

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.

Ключевые возможности

1. Строгая двухфакторная аутентификация
   - Поддержка токенов – Rutoken ЭЦП, Rutoken Lite, JaCarta PKI, Guardant ID
   - Возможность входа по сертификату ГОСТ

2. Запрет загрузки ОС с внешних носителей
   - Выбор одного доверенного загрузчика

Ключевые возможности

Контроль целостности

- UEFI BIOS
- MBR на носителях информации
- Таблиц ACPI, SMBIOS, карты распределения памя
- Файловых систем FAT32, NTFS, EXT2, EXT3, EXT4
- Ресурсов конфигурационного пространства PCI/I
- CMOS (содержимого энергонезависимой памяти
- Контроль завершенности транзакций - NTFS, EXT EXT4

Ключевые возможности

1. Регистрация событий безопасности
2. Возможность создания шаблонов настройки для удобства ввода в строй парка компьютеров и серверов с установленным ViPNet SafeBoot
3. Защита от обхода и самотестирование
4. Возможность программного обновления замка

Сертификат!!!

- Сертифицирован по требованиям руководящих документов к средствам доверенной загрузки уровня базовой системы ввода-вывода **второго** класса и возможность использования в ИСПДн до У31 включительно и в ГИС до 1-го класса защищенности включительно.

- Набор мер прописан в формуляре

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 средств 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.К004) - 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

Настоящий сертификат внесен в Государственный реестр сертифицированных средств защиты информации
14 ноября 2017 г.

Соответствие и актуальность

Какие требования приказов закрывает?

- (ГЛАВНОЕ) УПД.17 – «Обеспечение доверенной загрузки средств вычислительной техники» - актуально для классов 1-2 ИСПДн и ГИС
- Требования подсистемы идентификации и аутентификации, регистрации событий безопасности.
- Частично закрывает обеспечение целостности ИС и ИСПДн, управление доступом

Почему актуально?

- Можно установить множество средств защиты в ОС, но если есть возможность загрузки с внешнего носителя, то все труды и вложения напрасны.

Банк угроз – что можно закрыть?

В БДУ ФСТЭК имеется

29 угроз

в полной или косвенной мере относящиеся 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

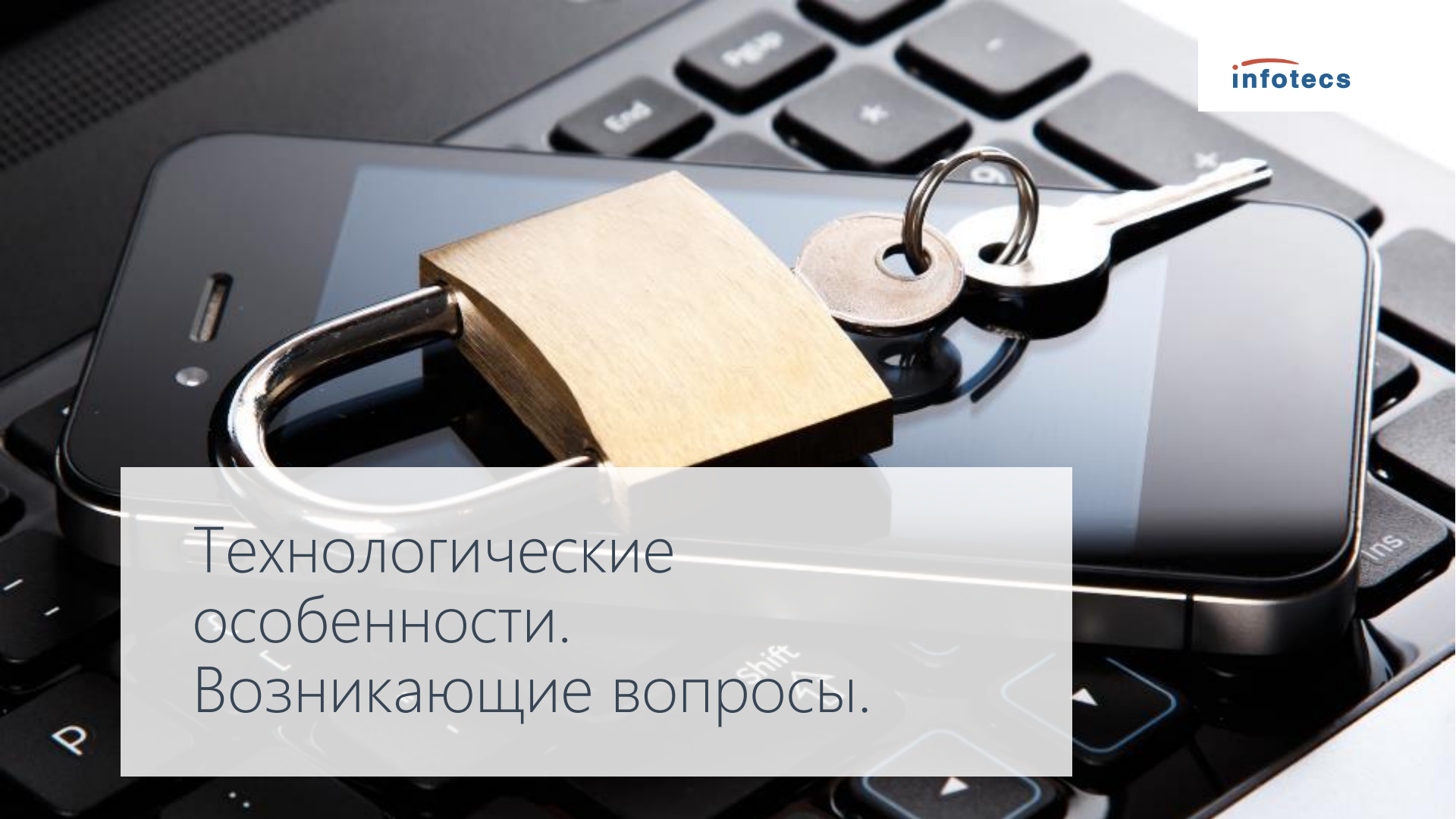
Схема лицензирования

- Лицензия на рабочую станцию (коробочная лицензия) – требуется приобрести количество лицензий равное количеству рабочих станций, на которые будет установлен ViPNet SafeBoot.

- CD-диск (установочный комплект) с формуляром - по количеству рабочих станций на которые будет установлен SafeBoot (прикладывается формуляр с голографической наклейкой ФСТЭК России)

Наши преимущества

1. Отсутствие «железной составляющей»:
   - ✓ Меньше цена продукта
   - ✓ Экономия на логистике
2. Поддержка UEFI BIOS на различных платформах, в отличии от конкурентов
3. Возможность установки в BIOS виртуальных машин
4. Использование шаблонов настройки для упрощения ввода в эксплуатацию
5. Уверенность в вендоре с успешной 25-летней историей



Технологические особенности. Возникающие вопросы.

Что даём на тест?

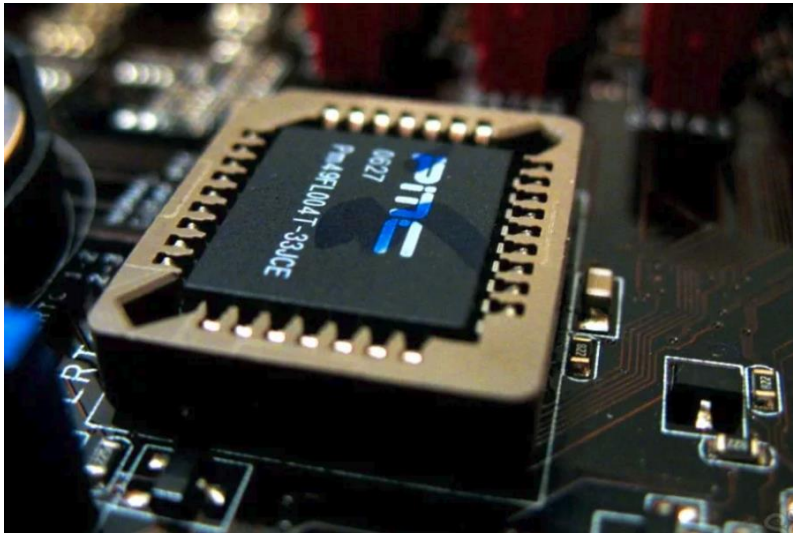
UEFI BIOS – среда для многих незнакомая и похожа на «дремучие джунгли». Для передачи на тест есть простое компромиссное решение.

Передача установленного ViPNet SafeBoot в виртуальную машину (можно без ОС ~25 Мб)

Другие варианты…

Передача непосредственно самого модуля для собственноручной установки:

- ✓ При помощи специальной утилиты*
- ✓ При помощи программатора



Мы сотрудничаем с производителями

В настоящий момент мы активно работаем с:

- ✓ Аквариус
- ✓ Depo Computers
- ✓ Lenovo
- ✓ YADRO
- ✓ Getac

В перспективе:

- ✓ Hewlett Packard Inc
- ✓ Acer
- ✓ Dell
- ✓ NPP MAYAK

В феврале релиз 1.3

- ✓ Специальная утилита для простоты погружения МДЗ в BIOS
- ✓ Поддержка аутентификации через LDAP/AD
- ✓ Контроль целостности реестра
- ✓ Дополнительные методы аутентификации (без PKI)
- ✓ Поддержка новейших платформ
- ✓ Быстрое формирование списков контролируемых ресурсов


infotecs
Спасибо!