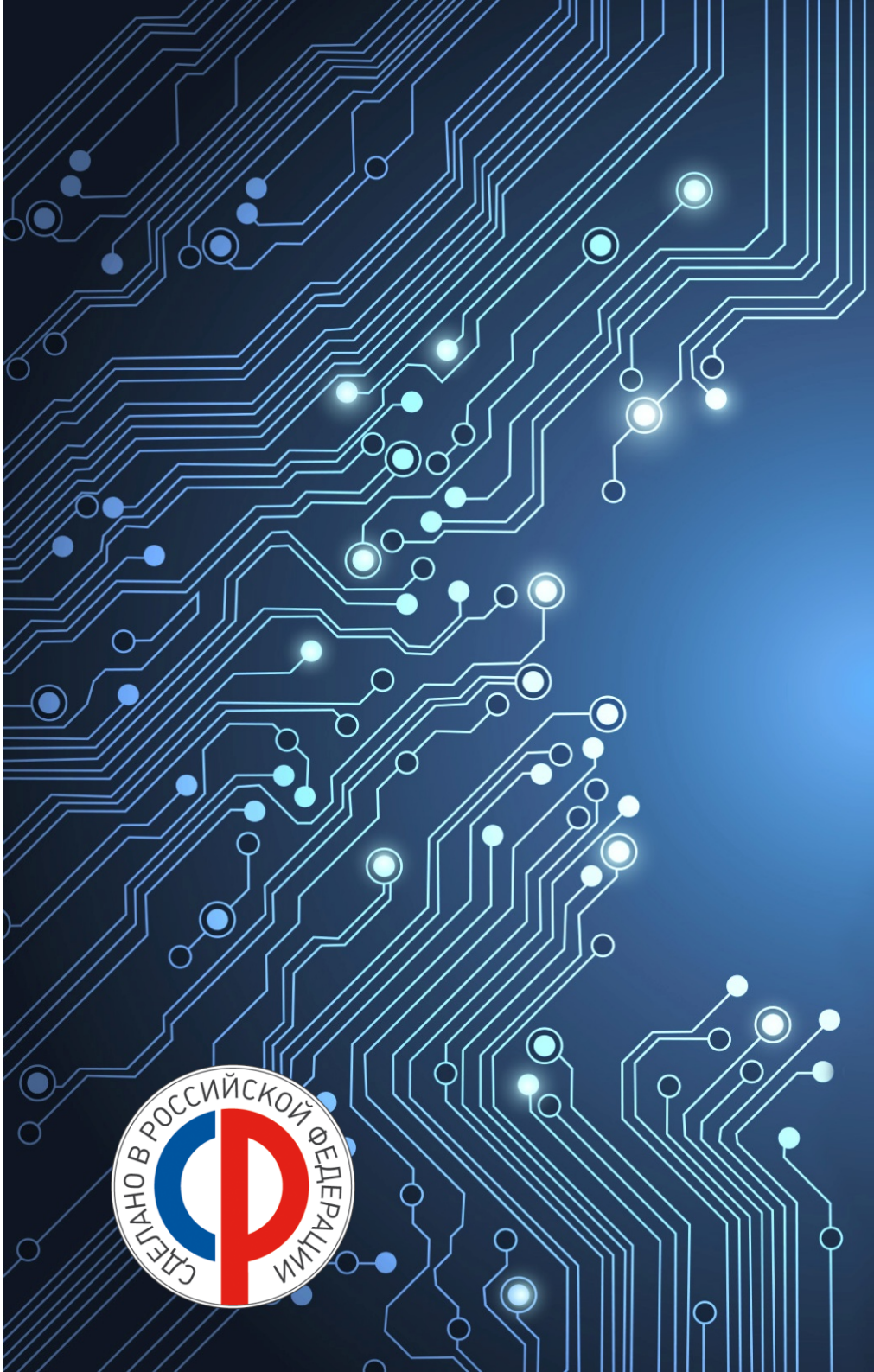


Доверенная система как основа построения безопасной инфраструктуры

Александр Чибисов
Руководитель направления
Департамент развития бизнеса

О КОМПАНИИ KRAFTWAY

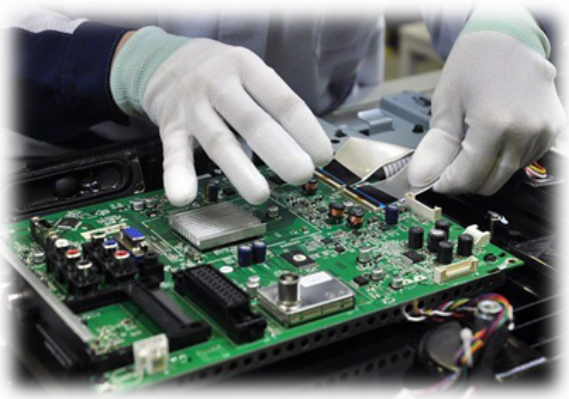
- Российская ИТ- компания, основана в 1993 году
- Производственно-логистический комплекс в городе Обнинск
- Линия поверхностного монтажа печатных плат
- Независимый испытательный центр – НИЦ СПЕЦТЕСТ
- Сеть представительств во всех регионах РФ и авторизованных сервисных центров (более 260)

КОМПЕТЕНЦИИ КОМПАНИИ

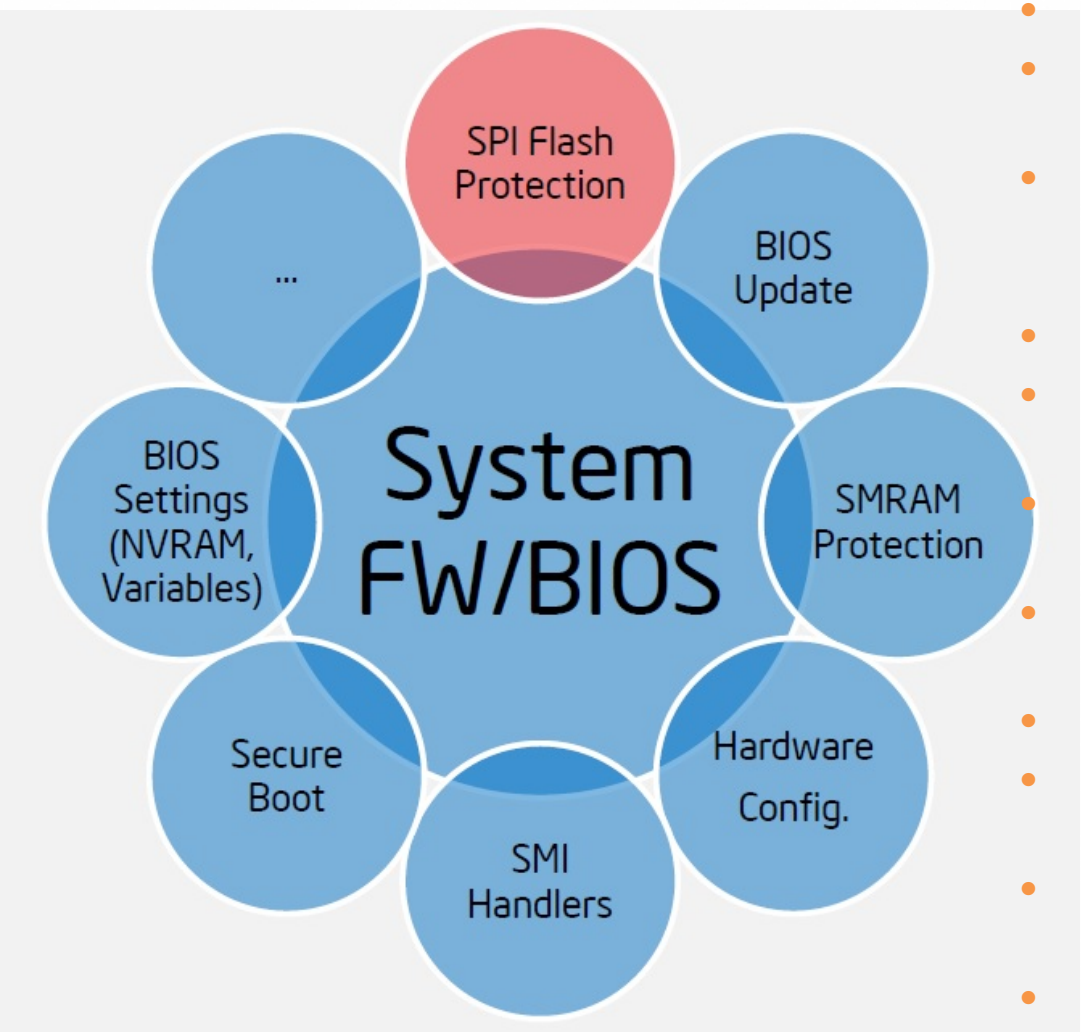
- **Разработка схемотехники печатных плат и вспомогательных узлов ПК**
  (шасси, системы электропитания, системы охлаждения и т.д.)
- **Разработка периферийного оборудования**
  (мониторы, ИБП, камеры видеонаблюдения)
- **Разработка встроенного микропрограммного обеспечения**
  (прошивки материнских плат и микроконтроллеров)
  собственных и на основе лицензионных и/или открытых исходных кодов
- **Разработка программного обеспечения**
  - мониторинг и управление ИТ-инфраструктурой
  - сбор и обработка информации о событиях безопасности
  - централизованное управление пользователями и приложениями
- **Разработка средств защиты информации**
- **Разработка изделий в защищенном исполнении**

ПРОБЛЕМА ИМПОРТОЗАВИСИМОСТИ

- Высокий уровень «импортозависимости» в ИТ-отрасли является серьезной угрозой устойчивости информационных систем
- Большинство используемых вычислительных систем построено на компонентах импортного производства
- Применение наложенных средств защиты не исключает возможность осуществления низкоуровневых атак с применением закладок и скрытых каналов



ВЕКТОРЫ НИЗКОУРОВНЕВЫХ АТАК



- Наличие НДВ базового образа BIOS
- Несанкционированное изменение образа или части образа
- Исполнение неконтролируемого кода во встроенной памяти процессора и чипсета в процессе его инициализации
- Нарушение цепочки доверия при загрузке
- Перевод CPU в режим особых привилегий SMM
- Изменение загрузочной записи в MBR или GPT таблице
- Внедрение закладок при замене прошивок OEM-устройств
- Подмена сетевого загрузочного устройства
- Перехват управления OEM-устройств через НДВ OPROM
- Наличие НДВ специализированных контроллеров BMC, TPM
- Подмена драйверов и модулей UEFI загружаемых с диска из раздела EFI
- Модификация загрузчика выхода из состояния сна (BootScript)
- Перевод CPU в отладочный режим (DCI)

ТИПОВАЯ АРХИТЕКТУРА

Типовые компоненты с потенциальной уязвимостью

kraftway®
РОССИЙСКИЕ ТЕХНОЛОГИИ

АРХИТЕКТУРА ДОВЕРЕННОЙ СИСТЕМЫ

kraftway®
РОССИЙСКИЕ ТЕХНОЛОГИИ

ДОВЕРЕННАЯ ПЛАТФОРМА

- **Аппаратная часть:** снижает риск наличия закладок в аппаратной части
  - Проектирование и разработка материнских плат в России
  - Интеграция аппаратно-программных средств защиты на стадии проектирования
  - Локализация производства оборудования
  - Закупки компонентной базы большими партиями

- **Программная часть:** исключает риск НДВ на этапе загрузки системы
  - Переработка и локализация прошивок микроконтроллеров (BIOS, Firmware)
  - Интеграция средств защиты информации на самый низкий уровень (в аппаратную часть платформы и в прошивку BIOS)
  - Централизованное управление безопасностью и ИТ-инфраструктурой
  - Непрерывный контроль системы в процессе работы

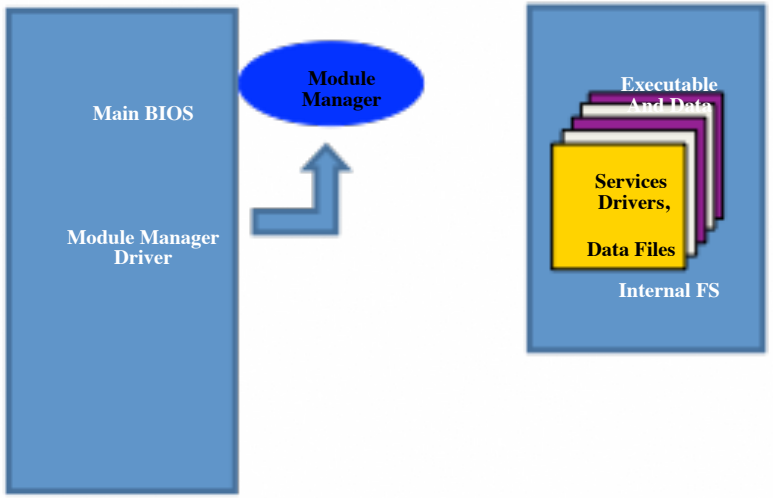
РАБОТА ДОВЕРЕННОЙ СИСТЕМЫ

- Включение ПК0
- Проверка оборудования (POST)
- Аппаратное прерывание стартовой процедуры BIOS
- Инициализация PCI-устройств
- Инициализация загрузчика ОС
- Считывание начального загрузчика ОС
- Передача управления загрузчику ОС
- Загрузка ОС

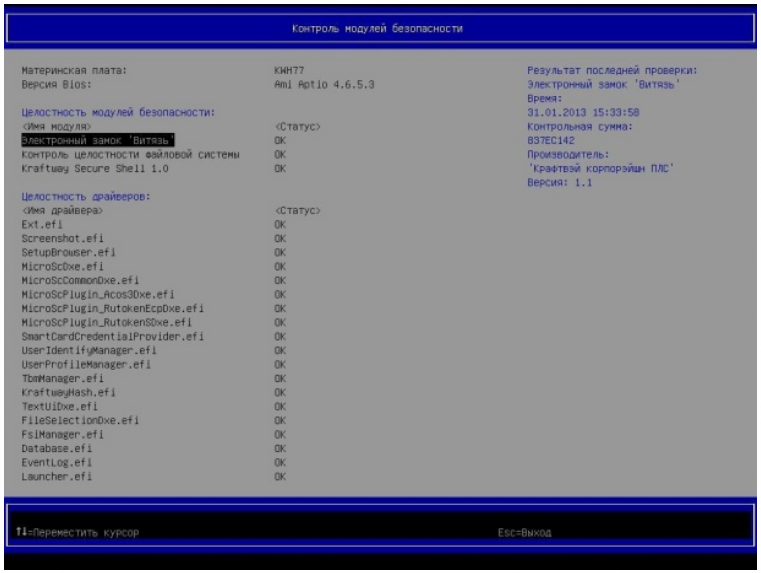
- Включение модуля доверия
- Проверка BIOS и интегрированных СЗИ
- Инициализация BIOS
- Запуск тонкого гипервизора
- Двухфакторная идентификация и аутентификация пользователей
- Контроль целостности программного и аппаратного обеспечения
- Антивирусная защита
- Регистрация событий безопасности

ОБОЛОЧКА БЕЗОПАСНОСТИ KRAFTWAY

Kraftway Secure Shell (KSS) – интегрированная в UEFI среда гарантированного и защищенного исполнения модулей безопасности до загрузки операционной системы



- Открытое API для интеграции модулей других производителей
- Модули безопасности реализованы в виде Plug-In
- Легко интегрируется и расширяется
- Все данные и модули хранятся в закрытой встроенной файловой системе



kraftway®
РОССИЙСКИЕ ТЕХНОЛОГИИ

ИНТЕГРИРОВАННЫЕ МОДУЛИ

- **Средство доверенной загрузки**
- защита от несанкционированного доступа за счет многофакторной аутентификации до старта ОС и запрет загрузки с внешних носителей
- **Средство контроля конфигурации**
- контроль целостности программной и аппаратной среды компьютера
- **Тонкий Гипервизор**
- контроль потоков ввода/вывода и профилирование оборудования под конкретного пользователя
- **Клиент Kraftway Security Center**
- централизованное управление интегрированными модулями на уровне BIOS (UEFI)

ВСТРАИВАЕМЫЕ РЕШЕНИЯ

- **«Встраиваемый модуль безопасности TSM»**
  программный комплекс
- **«Kaspersky Antivirus for UEFI»**
  программный модуль
- **«Secure microSD»**
  программно-аппаратный модуль
- **«Рутокен ЭЦП TPM»**
  программно-аппаратный модуль
- **«АПМДЗ-И/МП»**
  аппаратный модуль интегрированный на уровне МВ
- **«Комплект доверенного сеанса»**
  модуль защиты программно-аппаратного комплекса

Аладдин РД

KASPERSKY lab

компания Актив

На страже Вашей информации.

s•terra csp

Спасибо за внимание!

Александр Чибисов
Руководитель направления
Департамент развития бизнеса