Импортозамещение. Российская доверенная вычислительная техника как основа построения безопасной инфраструктуры

Александр Игнатовский
Руководитель направления
Департамент развития бизнеса

СДЕЛАНО В РОССИЙСКОЙ ФЕДЕРАЦИИ

kraftway®
РОССИЙСКИЕ ТЕХНОЛОГИИ

О КОМПАНИИ KRAFTWAY

- Одна из крупнейших российских ИТ- компаний, основана в 1993 г.
- Уникальный производственно - логистический комплекс в городе Обнинск;
- Линия поверхностного монтажа печатных плат;
- Независимый испытательный центр – НИЦ СПЕЦТЕСТ.
- Сеть представительств и авторизованных сервисных центров во всех регионах РФ (более 260)

ТЕКУЩЕЕ СОСТОЯНИЕ РОССИЙСКОЙ РАДИОЭЛЕКТРОНИКИ В СФЕРЕ ПРОИЗВОДСТВА СВТ

СИЛА

- ✓ Государственный курс на импортозамещение;
- ✓ Повышение внимания к вопросами обеспечения информационной безопасности
- ✓Наличие в России производственных предприятий микро- и радиоэлектроники и дизайн-центров

СЛАБОСТЬ

- ✓Абсолютное доминирование иностранных производителей СВТ;
- ✓Технологическое отставание в области производства и разработки российской ЭКБ;
- ✓Высокая стоимость отечественной ЭКБ, в следствие ограниченного спроса и объема производства

ВОЗМОЖНОСТИ

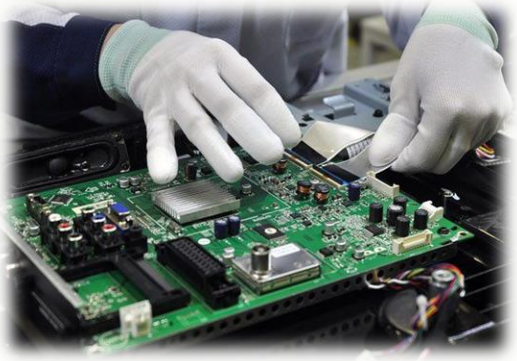
- ✓Внедрение технологий, позволяющих использовать импортную элементную базу для создания российских доверенных СВТ
- ✓Интеграция Российских средств защиты информации на уровень платформы;
- ✓Разработка и производство СВТ с использованием отечественной элементной базы;

УГРОЗЫ

- ✓Угроза введения ограничений на импорт СВТ в Россию;
- ✓Угроза наличия НДВ и различных уязвимостей в импортном оборудовании на уровне аппаратной платформы;
- ✓Угроза заражения вредоносным ПО нового типа (компрометация на уровне прошивок)

ПРОБЛЕМЫ ИМПОРТОЗАВИСИМОСТИ

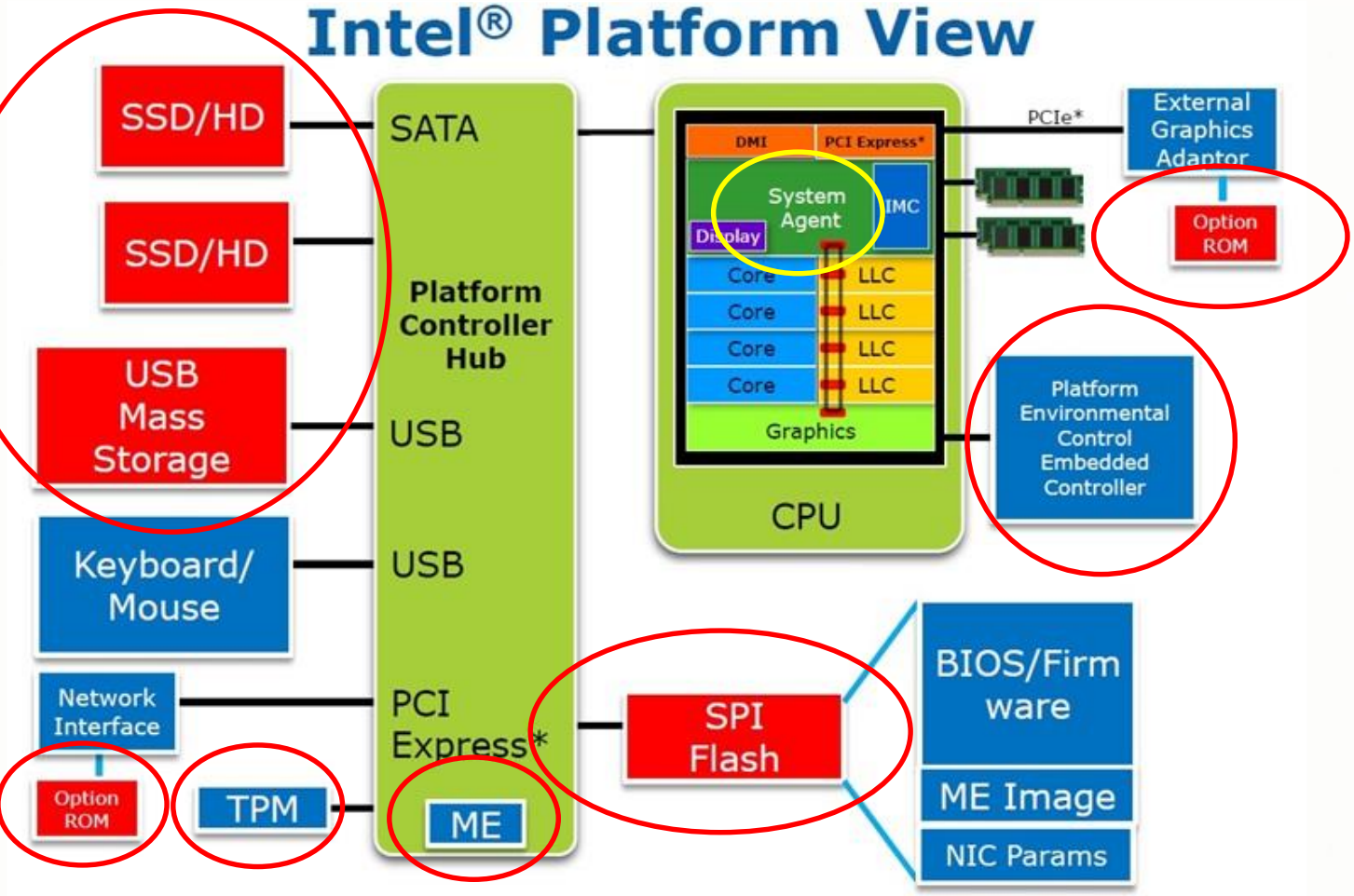
Высокий уровень «импортозависимости» в области ИТ-отрасли является серьезной угрозой устойчивости функционирования информационных систем.



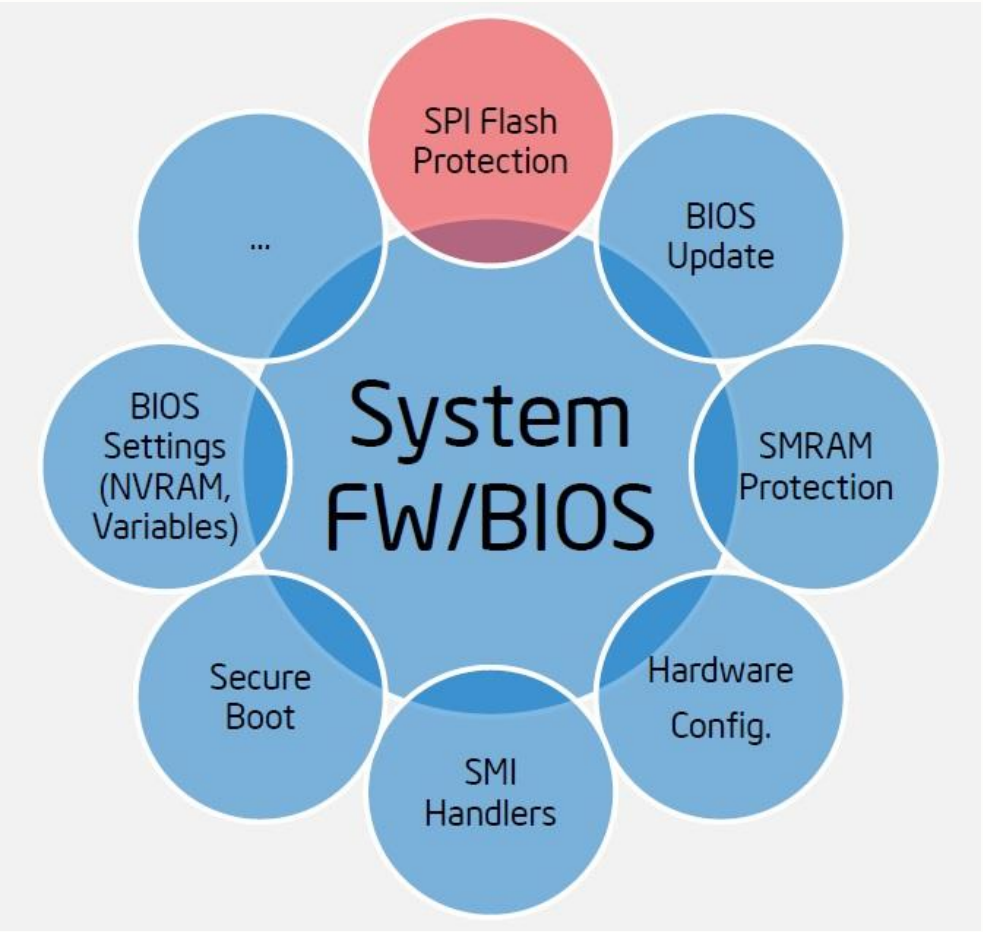
Подавляющее большинство используемых вычислительных систем построено на компонентах импортного производства. Нельзя исключать возможность наличия в них закладок, недекларированных возможностей и скрытых каналов управления,

ПОЗВОЛЯЮЩИХ ОБОЙТИ ЛЮБЫЕ НАЛОЖЕННЫЕ СРЕДСТВА ЗАЩИТЫ

ФИЗИЧЕСКАЯ МОДЕЛЬ УЯЗВИМОСТЕЙ X86 ПЛАТФОРМ



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).

ОСНОВНЫЕ ЭЛЕМЕНТЫ ДОВЕРЕННОЙ ПЛАТФОРМЫ

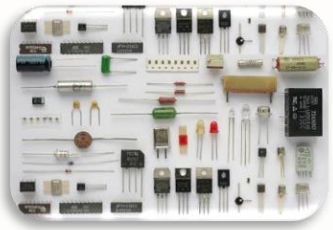
Достаточная доверенность:

Абсолютная доверенность:

kraftway
РОССИЙСКИЕ ТЕХНОЛОГИИ

ПРОБЛЕМЫ ИМПОРТОЗАМЕЩЕНИЯ

На сегодняшний день локально производится более 70% простейшей компонентной базы



При этом импортозамещение в области управляющей логики для платформы x86 **стремится к нулю.**

Перенос ПО на любую другую архитектуру и его оптимизация для достижения сопоставимого с x86 быстродействия является трудоёмким и дорогостоящим процессом.

Полная локализация производства компонентной базы на территории России не является выполнимой задачей на ближайшие годы

ПРОБЛЕМЫ ИМПОРТОЗАМЕЩЕНИЯ

Использование отечественных процессоров в критически важных системах на данный момент не может полностью решить проблемы технологической независимости.

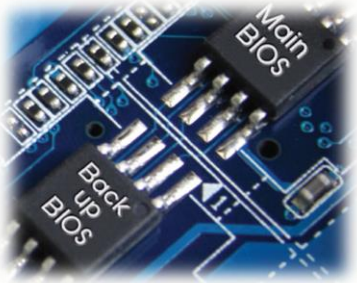
Процессоры производятся по определённому технологическому процессу, привязанному к конкретной зарубежной фабрике, поскольку в России таких микроэлектронных производств не существует.

Соответственно, контроль производства таких процессоров находится за пределами РФ и всегда существует риск санкционных ограничений

КОНЦЕПЦИЯ ПОСТРОЕНИЯ ДОВЕРЕННОЙ ПЛАТФОРМЫ НА НЕДОВЕРЕННОЙ КОМПОНЕНТНОЙ БАЗЕ ИМПОРТНОГО ПРОИЗВОДСТВА.

Превентивная модель защиты:

- Обеспечение изначальной целостности и неизменности среды функционирования (UEFI)



Непрерывная модель безопасности:

- Использование принципа «цепочек доверия» (проверка каждого запускаемого компонента, с использованием технологии цифровых сертификатов)
- Непрерывный контроль операций ввода/вывода с внешними ресурсами (локальными и сетевыми)

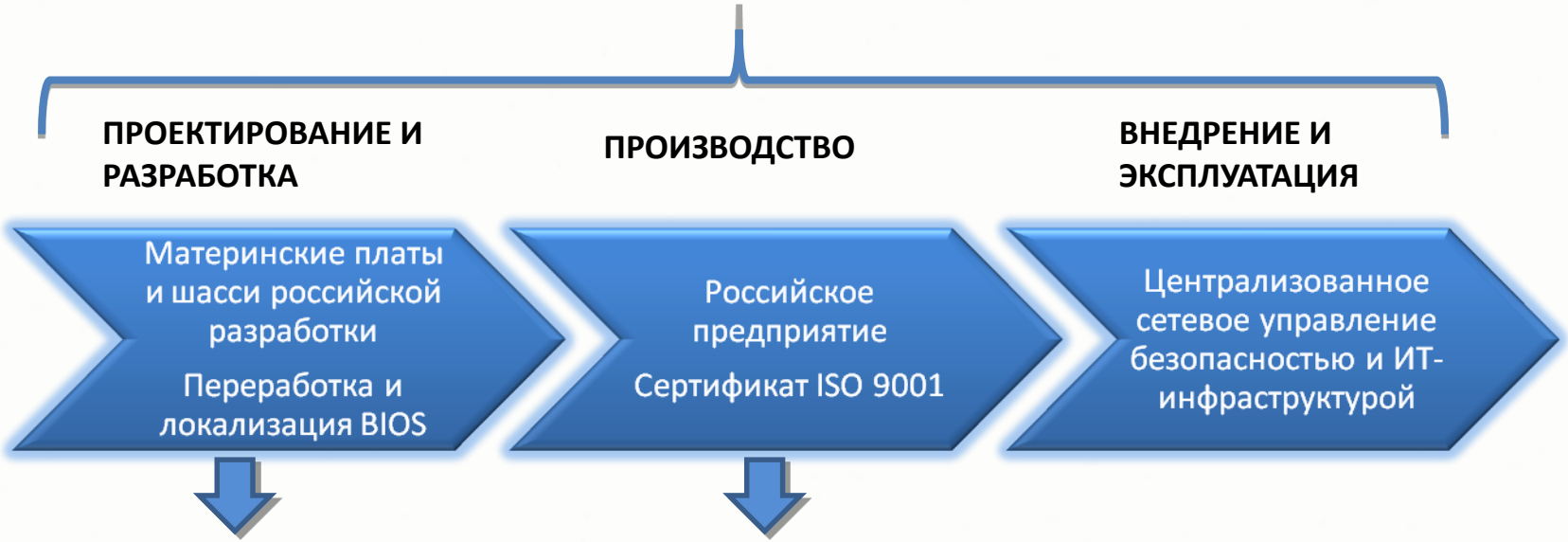
Разделение среды функционирования СЗИ и стандартных приложений

- Интеграция в архитектуру x86 на стадии проектирования дополнительного независимого аппаратного **ВЫЧИСЛИТЕЛЬНОГО МОДУЛЯ ДОВЕРИЯ**
- Перенос функций СЗИ в “МОДУЛЬ ДОВЕРИЯ”
- Обеспечение приоритета исполнения приложений безопасности над остальными функциями платформ

kraftway
РОССИЙСКИЕ ТЕХНОЛОГИИ

ПОДХОД К ВЫПУСКУ ДОВЕРЕННОЙ ПРОДУКЦИИ

Доверенная платформа: контроль всех стадий жизненного цикла продукта / решения

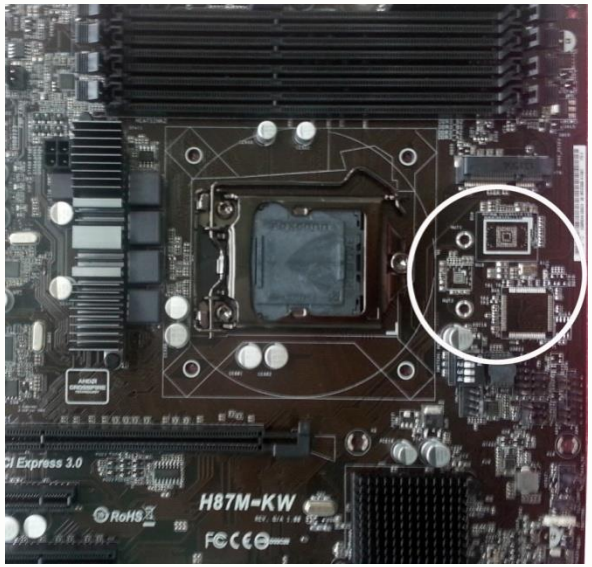


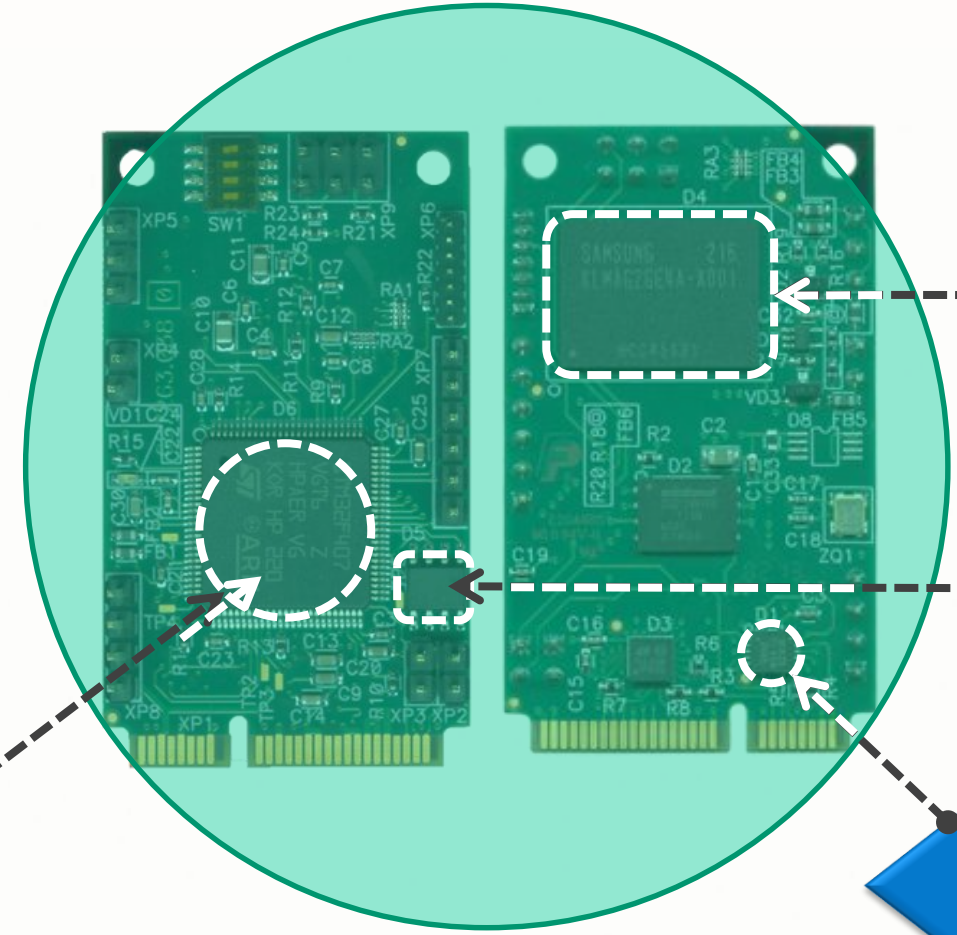
- **Интеграция в схемотехнику платформы аппаратного модуля доверия**
- **Разработка СЗИ функционирующих в защищённой неизменяемой среде модуля доверия**

- **Поверхностный монтаж печатных плат**
- **Проведение в цикле производства специальных проверок и специальных исследований;**
- **Гарантия качества, сквозной 100% контроль продукции**

kraftway
РОССИЙСКИЕ ТЕХНОЛОГИИ

МОДУЛЬ ДОВЕРИЯ В МАТЕРИНСКИХ ПЛАТАХ КРАФТВЭЙ





Flash

BIOS

МП

ключ

kraftway
РОССИЙСКИЕ ТЕХНОЛОГИИ

СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ ИНТЕГРИРОВАННЫЕ В МОДУЛЬ ДОВЕРИЯ

- **Аппаратно-програмный модуль доверенной загрузки** обеспечивают защиту от несанкционированного доступа за счет двухфакторной аутентификации до старта операционной системы и запрет загрузки с внешних носителей
- **Средство контроля конфигурации** – обеспечивает контроль целостности программной и аппаратной среды компьютера.
- **Тонкий Гипервизор** – обеспечивает контроль потоков ввода/вывода и профилирование оборудования под конкретного пользователя.
- **Антивирус «Касперский для UEFI»** - обеспечивает своевременное обнаружение и блокирование вирусных атак до загрузки ОС.
- **Kraftway Security Center** – обеспечивает централизованное дистанционное управления средствами защиты на уровне BIOS (UEFI).

РАБОТА СЗИ В ТИПОВОЙ ВЫЧИСЛИТЕЛЬНОЙ СИСТЕМЕ

Включение ПК

Инициализация BIOS

Проверка оборудования (POST)

Инициализация PCI-устройств

Инициализация загрузчика ОС

Считывание начального загрузчика ОС

Аппаратное прерывание процедуры загрузки

Передача управления загрузчику ОС

Загрузка ОС

Запуск вредоносного кода

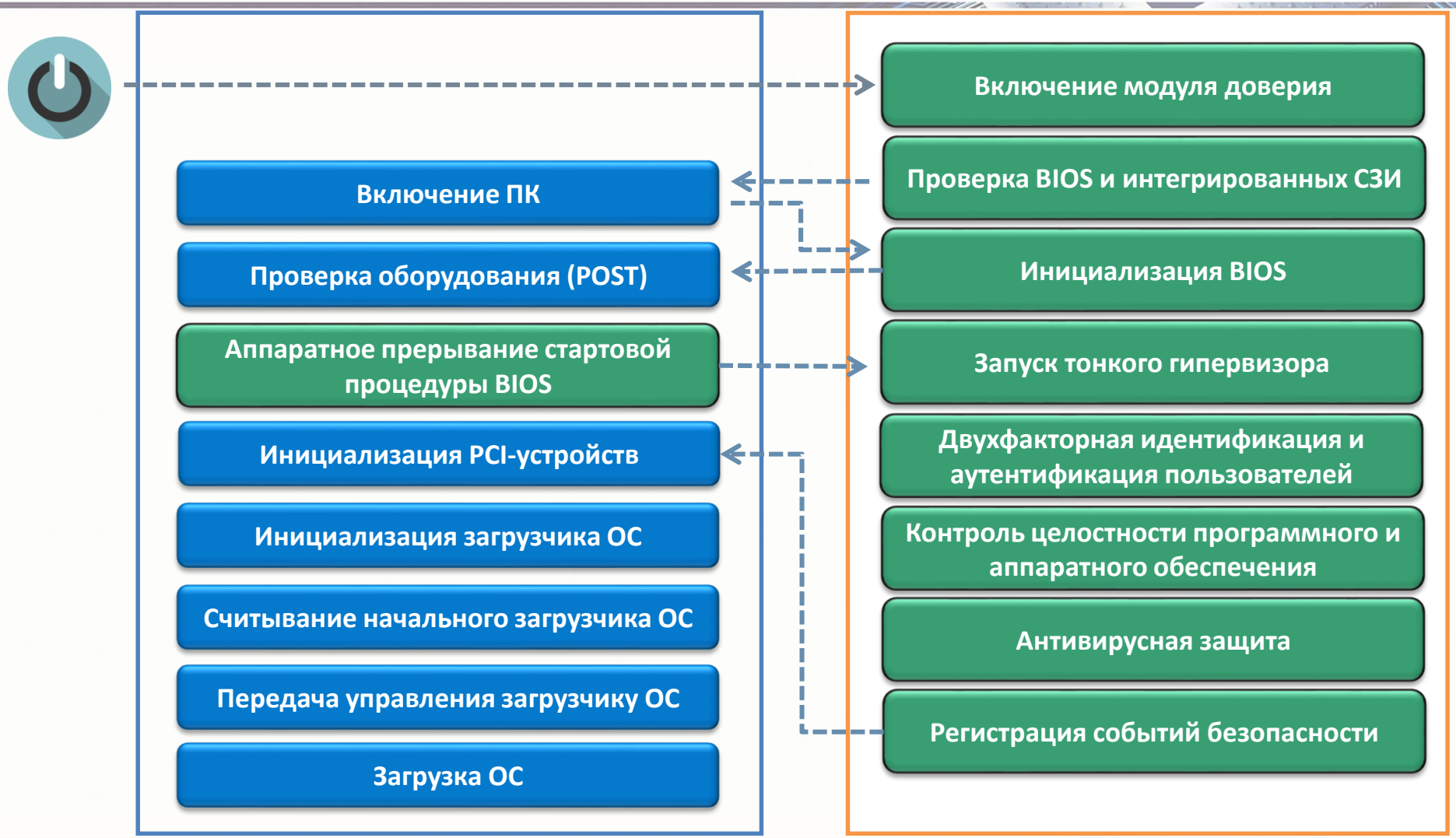
Внешнее (наложенное) СЗИ

Двухфакторная идентификация и аутентификация пользователей

Контроль целостности программного обеспечения

Регистрация событий безопасности

РАБОТА СЗИ В ДОВЕРЕННОЙ ВЫЧИСЛИТЕЛЬНОЙ СИСТЕ



kraftway
РОССИЙСКИЕ ТЕХНОЛОГИИ


Спасибо за внимание!
kraftway
РОССИЙСКИЕ ТЕХНОЛОГИИ