Доверенная платформа

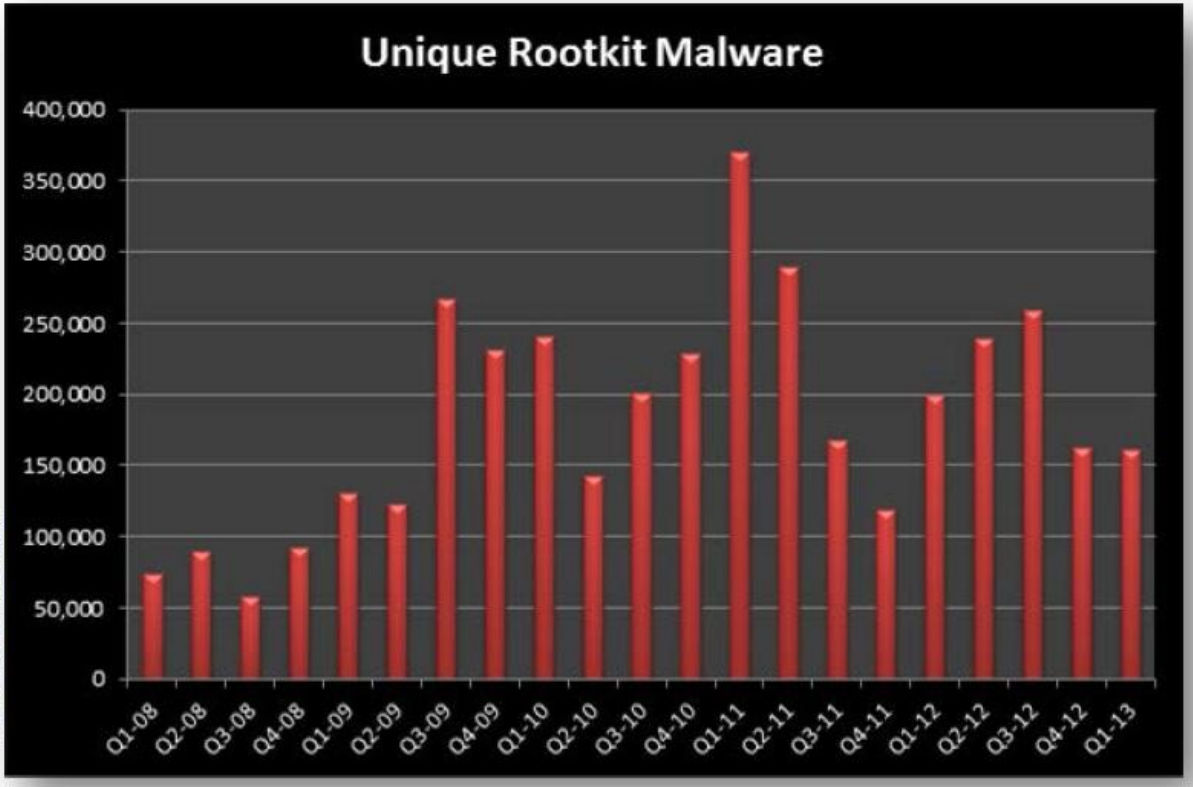
Практика создания СВТ с интегрированными СЗИ

Ренат Юсупов
Старший вице-президент

kraftway
ТЕХНОЛОГИИ БЕЗОПАСНОСТИ

Москва, 2014

ОЦЕНКА УРОВНЯ УГРОЗ



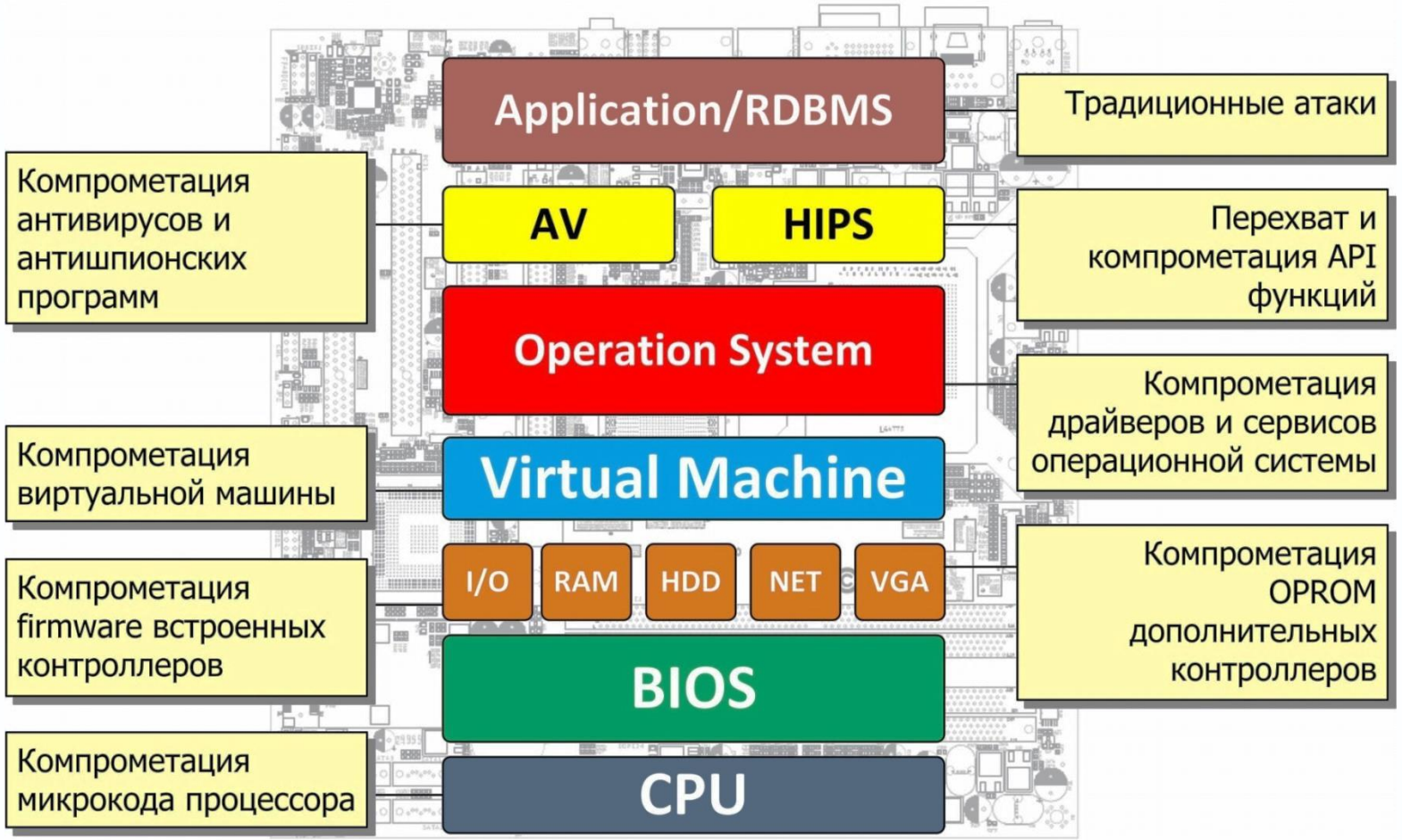
Source: McAfee

Rootkit Family	Binaries	%
Koutodoor	452,042	21%
TDSS	389,216	18%
Farfli	167,895	8%
MBR	162,605	8%
Caxnet	106,860	5%
Prosti	80,887	4%
DNS Changer	74,010	3%
Cutwail	32,560	2%
LDPinch	18,590	1%
Other rootkit samples	635,040	30%
Total	**2,119,705**	**100%**

Угрозы, уязвимости, инструменты защиты для x86 платформ

Угрозы	Уязвимости	Intel - McAfee, Microsoft, TCG	Kraftway
Загрузка нештатной ОС	подмена CMOS, MBR, GPT	Secure boot	Secure boot, Kraftway Secure Shell
Отключение/обход СЗИ	НДВ в BIOS, SMI режим	Secure boot, measured boot, MS ELAM	Загрузка из KSS
Изменение параметров/ конфигурации СЗИ	доступ к SPI, хранилищу EFI, MBR, GPT	шифрование McAfee Data Protection	защита SPI Flash, Рутокен TPM, Анкад АПМДЗ, Аладдин Secure microSD
Обход функций СЗИ	ловушки SMI, гипервизор в BIOS	McAfee microhypervisor	модуль KSS - гипервизор

АКТУАЛЬНАЯ МОДЕЛЬ УГРОЗ ДЛЯ КОМПРОМЕТАЦИИ BIOS



kraftway
ТЕХНОЛОГИИ БЕЗОПАСНОСТИ

Использование НДВ в BIOS

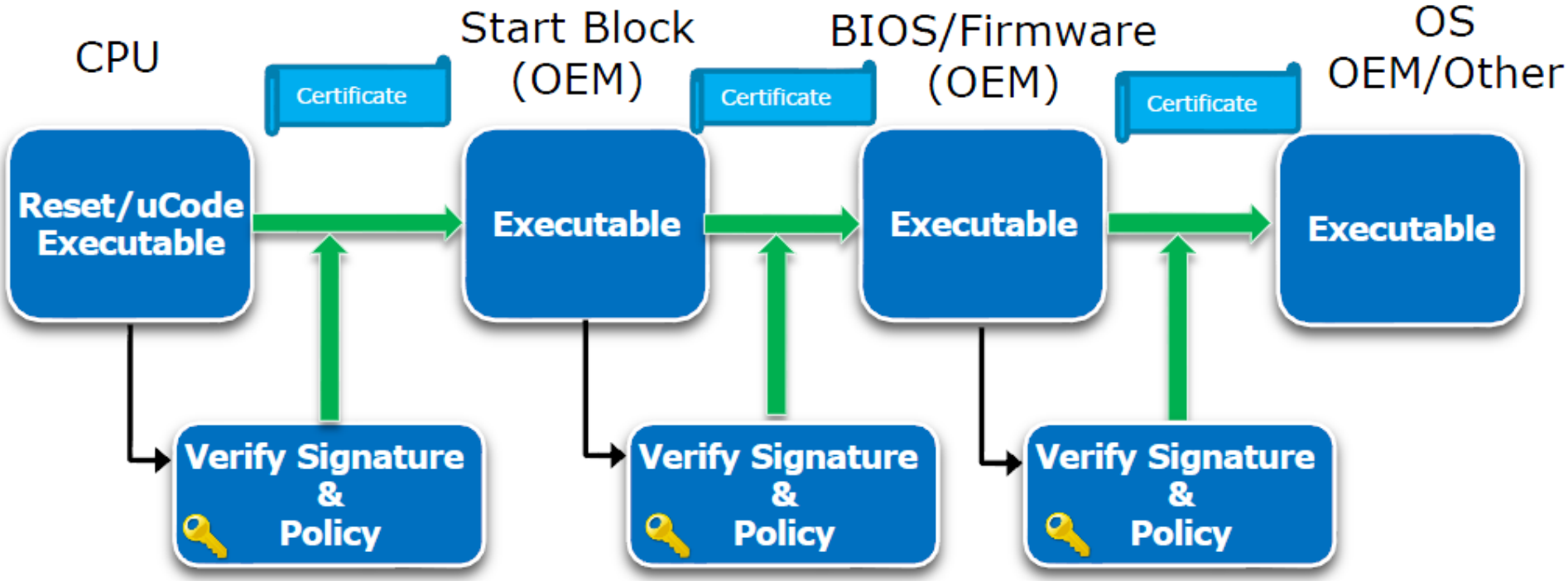
Утилиты из каталога АНБ сезона 2008-2009

- IRATEMONK – модифицированная прошивка MBR для запуска программы кражи данных;
- SWAP – перепрошивка модифицированными версиями BIOS и HPA HDD для получения удалённого доступа;
- IRONCHEF – SMI функция модифицированного BIOS для передачи информации через встроенную закладку – радиопередатчик;
- DEITYBOUNCE – SMI функция в модифицированном BIOS для удалённого доступа до загрузки ОС;
- JETPLOW, HALLUXWATER, FEEDTROUGH, SOUFFLETROUGH, GOURMETTROUGH – эксплойты в модифицированном BIOS для Cisco, Huawei, Juniper.

Угрозы, уязвимости, инструменты защиты

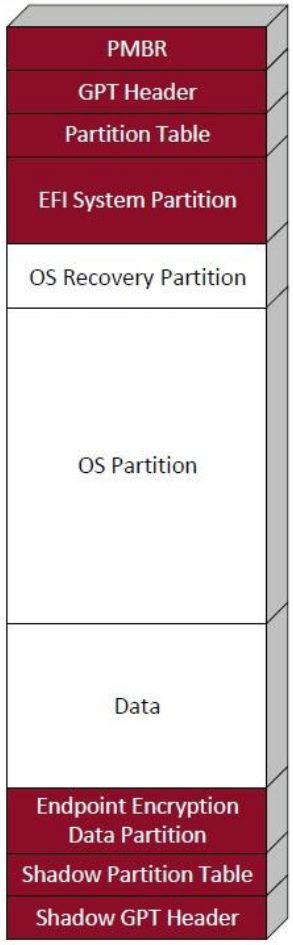
Угрозы	Уязвимости	Intel - McAfee, Microsoft, TCG	Kraftway
Загрузка нештатной ОС	подмена CMOS, MBR, GPT	**Secure boot**	Secure boot, Kraftway Secure Shell
Отключение/обход СЗИ	НДВ в BIOS, SMI режим	**Secure boot, measured boot, MS ELAM**	Загрузка из KSS
Изменение параметров/ конфигурации СЗИ	доступ к SPI, хранилищу EFI, MBR, GPT	**шифрование McAfee Data Protection**	защита SPI Flash, Рутокен TPM, Анкад АПМДЗ, Аладдин Secure microSD
Обход функций СЗИ	ловушки SMI, гипервизор в BIOS	**McAfee Deepsafe micro-hypervisor**	модуль KSS - гипервизор

Режим SECURE BOOT.



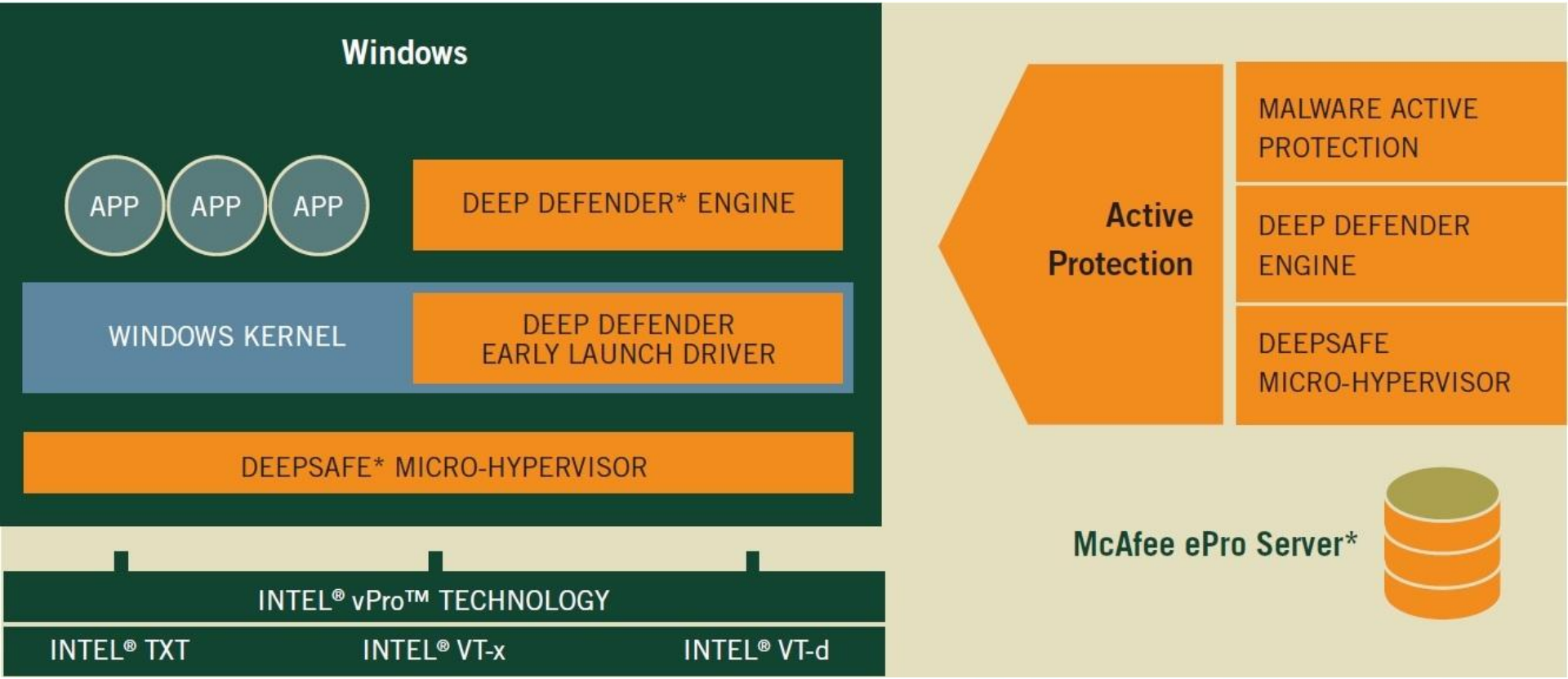
- Загружаются только подписанные модули
- Режим UEFI с запуском ТОЛЬКО подписанного загрузчика OS
- Работает только с TPM

Недостатки шифрования дисков на примере McAfee Endpoint Protrction



- Protective MBR, GPT Headers и Partition Tables не могут быть зашифрованы:
  - Данные из этих областей необходимы до расшифровки диска
  - Диск не может быть распознан как GPT
- EFI System Partition не может быть зашифрована:
  - Содержит некоторые драйверы и запускаемые файлы UEFI
- Незашифрованные локальные конфигурационные файлы и копии важных областей.

Метод защиты за пределами ОС. Скрытая VM.



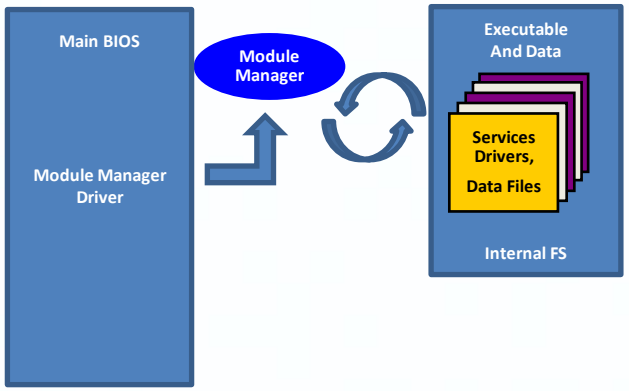
kraftway
ТЕХНОЛОГИИ БЕЗОПАСНОСТИ

Угрозы, уязвимости, инструменты защиты

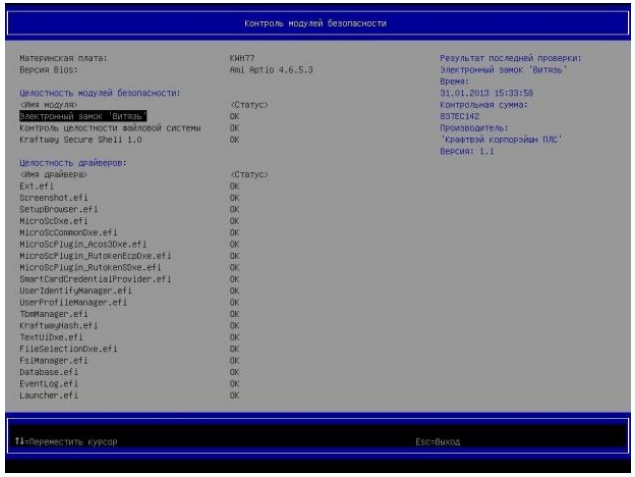
Угрозы	Уязвимости	Intel - McAfee, Microsoft, TCG	Kraftway
Загрузка нештатной ОС	подмена CMOS, MBR, GPT	Secure boot	**Secure boot, Kraftway Secure Shell**
Отключение/обход СЗИ	НДВ в BIOS, SMI режим	Secure boot, measured boot, MS ELAM	**загрузка СЗИ из KSS**
Изменение параметров/ конфигурации СЗИ	доступ к SPI, хранилищу EFI, MBR, GPT	шифрование McAfee Data Protection	**защита SPI Flash, Рутокен TPM, Анкад АПМДЗ, Аладдин Secure microSD**
Обход функций СЗИ	ловушки SMI, гипервизор в BIOS	McAfee microhypervisor	**гипервизор - модуль KSS**

ОБОЛОЧКА БЕЗОПАСНОСТИ 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 расширяется, легко портируется;
- Все данные и модели хранятся в защищенной встроенной файловой системе.
- Централизованный дистанционный мониторинг и и управление функциями безопасности через Kraftway Security Center



kraftway
ТЕХНОЛОГИИ БЕЗОПАСНОСТИ

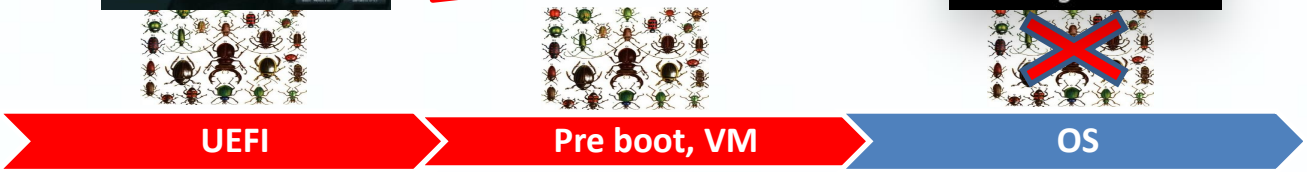
КОНЦЕПЦИЯ ПОСТРОЕНИЯ ДОВЕРЕННЫХ ПЛАТФОРМ

1. Превентивная модель защиты:
   - непрерывный контроль ключевых объектов и функций.
2. Непрерывная модель безопасности:
   - использование принципа «цепочек доверия» (пример – «secure boot»).
3. Интеграция СЗИ в типовую функциональность платформ:
   - совместимость СЗИ и платформ на уровне проектирования;
   - динамическая настройка на актуальную модель угроз.
4. Разделение среды функционирования СЗИ и стандартных приложений
   - перенос части функций СЗИ и систем управления в BIOS и доверенные виртуальные машины.
5. Приоритет исполнения приложений безопасности над остальными функциями платформ

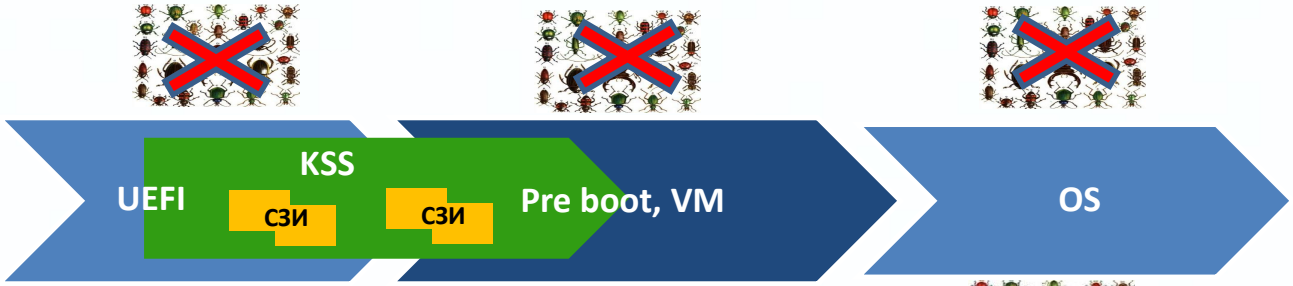
ТЕХНОЛОГИЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ KRAFTWAY

Между включением компьютера и запуском СЗИ существует окно, когда никто не контролирует загружаемые драйверы и приложения.

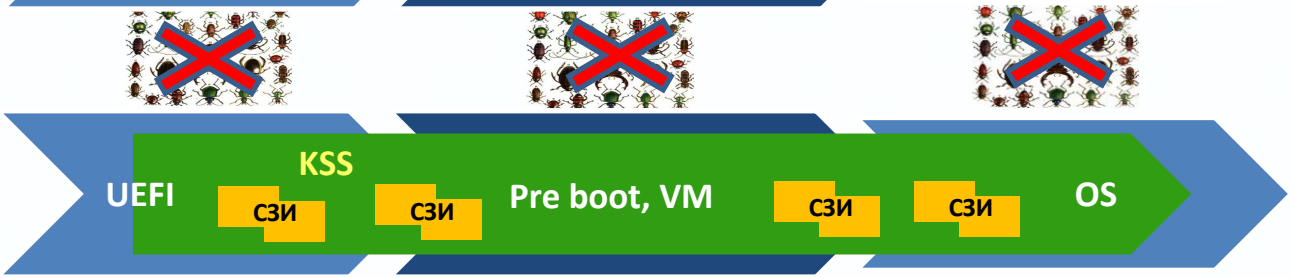
ВНИМАНИЕ
РЕАЛЬНАЯ УГРОЗА



Запуск устройства в режиме превентивной защиты UEFI + Pre boot



Запуск устройства в режиме превентивной защиты цикла использования



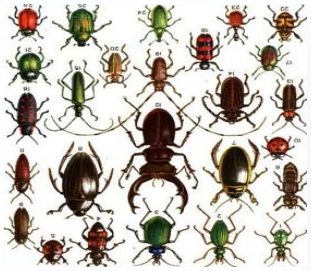
KSS – оболочка безопасности Kraftway Secure Shell
СЗИ – средства защиты информации

kraftway
ТЕХНОЛОГИИ БЕЗОПАСНОСТИ

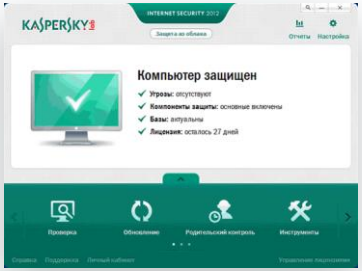
KSS. ВСТРАИВАЕМЫЕ РЕШЕНИЯ

- **«Kaspersky Antivirus for UEFI»:** программный модуль компании «Kaspersky Lab»;
- **«Встраиваемый модуль безопасности TSM (Trusted Security Module)»:** программный комплекс идентификации и аутентификации в UEFI компании «Аладдин Р.Д.»;
- **«Secure microSD»:** программно-аппаратный модуль компании «Алладин Р.Д.»;
- **«Рутокен ЭЦП TPM»:** программно-аппаратный модуль компании «Актив»;
- **«АПМДЗ-И/МП»:** интегрированный на МВ программно-аппаратный модуль доверенной загрузки компании «Анкад»;
- **«Комплект доверенного сеанса»:** модуль защиты программно-аппаратного комплекса компании S-Terra CSP .

KSS. ЗАЩИТА ОТ ROOT-/BOOTKIT

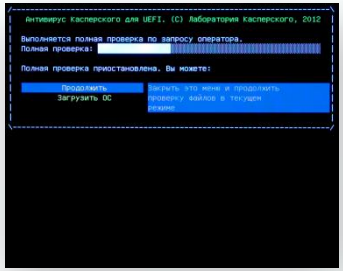


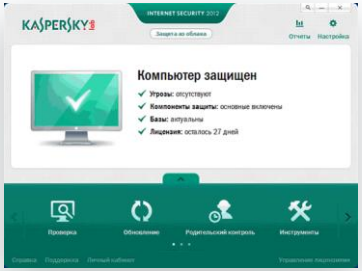


ВНИМАНИЕ
РЕАЛЬНАЯ УГРОЗА

Между включением компьютера и запуском антивирусной программы существует окно, когда никто не контролирует загружаемый драйверы и приложения. Boot-kit и root-kit приложения активно используют его для заражения системы.

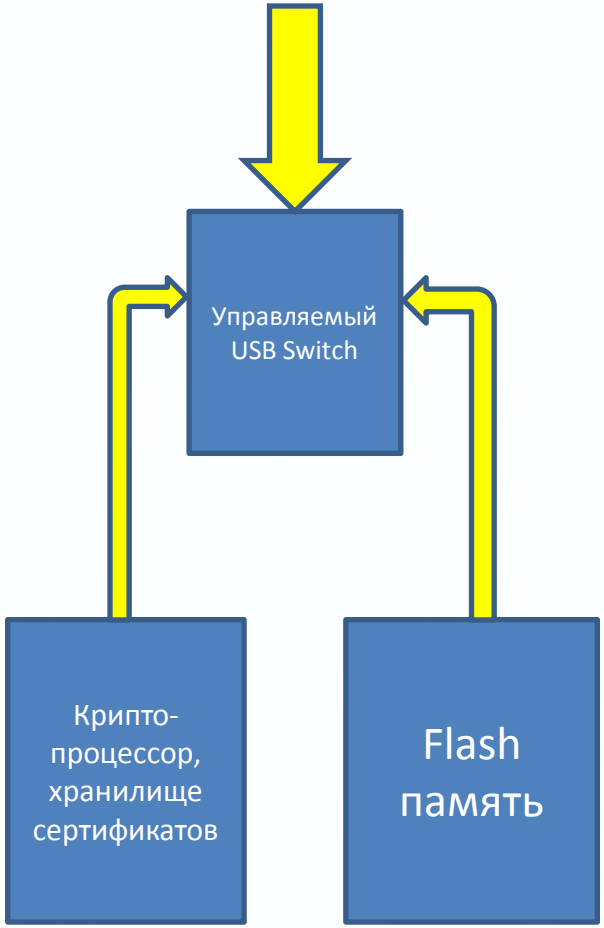
АНТИВИРУС KASPERSKY ДЛЯ UEFI: ЗАЩИТА ДО ЗАГРУЗКИ ОС

Запуск предварительной антивирусной проверки в момент загрузки позволяет проверить все файлы, которые будут использоваться в процессе загрузки ОС и обеспечить защиту от функционирования вредоносного кода.

РУТОКЕН ЭЦП TPM.
СЕРТИФИЦИРОВАННЫЙ TPM.



- **Крипто-процессор с поддержкой шифрования ГОСТ**
- **Защищенное хранилище сертификатов с неизвлекаемыми ключами**
- **Датчик случайных чисел**
- **Управляемый встроенным крипто-процессором USB Switch**
- **Отключаемая на аппаратном уровне FLASH память**
- **Привязка к платформе на уровне криптографических ключей**
- **Возможность использования в качестве защищенного хранилища для модулей UEFI**

ДОВЕРЕННЫЕ МАТЕРИНСКИЕ ПЛАТЫ KRAFTWAY

Тип продукции	М. плата Kraftway	CPU	BIOS и СЗИ	Год вып.	Кол-во
ПК	KWG43	Core2	Kraftway AWARD и Aladdin TSM	2010	> 50.000
ПК	KWQ67	iCore	Kraftway Insyde	2011	> 15.000
Тонкий клиент	KWN10	Atom PT	Kraftway AWARD и Aladdin TSM	2011	> 60.000
Тонкий клиент	KWN10D	Atom CT	Kraftway AMI, KSS, Aladdin TSM, Касперский KUEFI, Рутокен TPM	2012	> 10.000
ПК	KWH77	iCore	Kraftway AMI, KSS, Aladdin TSM, Касперский KUEFI, Рутокен TPM	2013	> 15.000
ПК, сервер	KWH87	iCore	Kraftway AMI, KSS, Aladdin TSM, Касперский KUEFI, Рутокен TPM, Анкад АПМДЗ-И/МП	2013	12/2013
Тонкий клиент	KWBS	Celeron	Kraftway AMI, KSS, Aladdin TSM, Касперский KUEFI, Рутокен TPM, Анкад АПМДЗ-И/МП	2014	02/2014
Сервер	KW…	2 Xeon	Kraftway AMI, KSS, Aladdin TSM, Касперский KUEFI, Рутокен TPM, Анкад/BMC	2014	2014

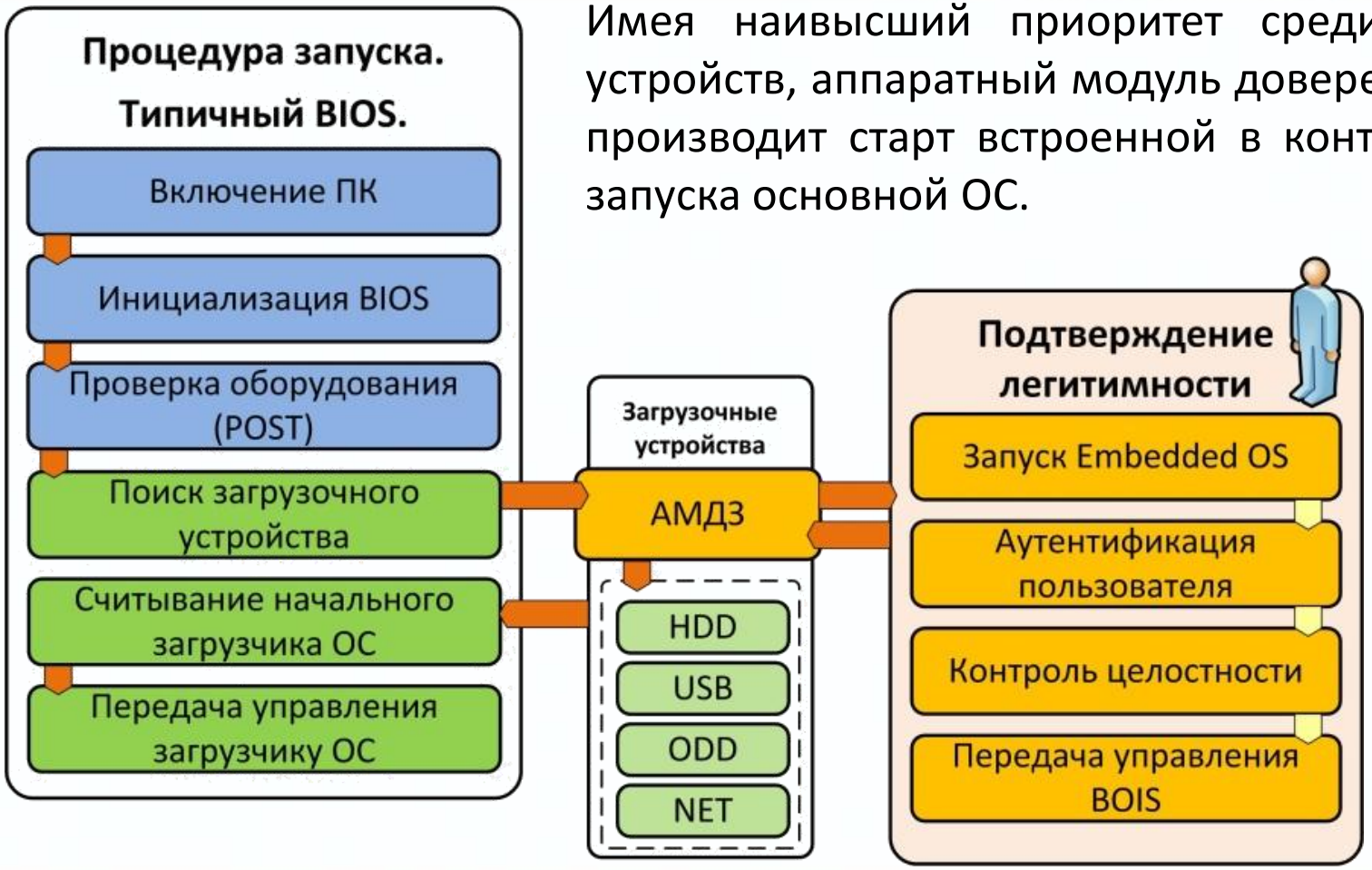
ВСТРАИВАНИЕ KRAFTWAY SECURE SHELL И СЗИ

Тип	Марка, модель	BIOS и СЗИ	Год
ПК	Fujitsu Esprimo	UEFI AMI, Kraftway KSS, ЭЗ «Витязь», Aladdin TSM, Касперский KUEFI, Рутокен TPM	2012
Моноблок (23.5”)	ECS Aura	UEFI AMI, Kraftway KSS, ЭЗ «Витязь», Aladdin TSM, Касперский KUEFI, Secure microSD	2013
Ноутбук (14”-17”)	MSI Classic Series	UEFI AMI, Kraftway KSS, ЭЗ «Витязь», Aladdin TSM, Касперский KUEFI, Secure microSD	2013
Сервер (2 CPU)	ASUS Z9PE	UEFI AMI, Kraftway KSS, ЭЗ «Витязь», Aladdin TSM, Касперский KUEFI, Рутокен TPM	2013
Планшет (7”-11”)	Windows based	UEFI AMI, Kraftway KSS, ЭЗ «Витязь», Aladdin TSM, Касперский KUEFI	03/2014

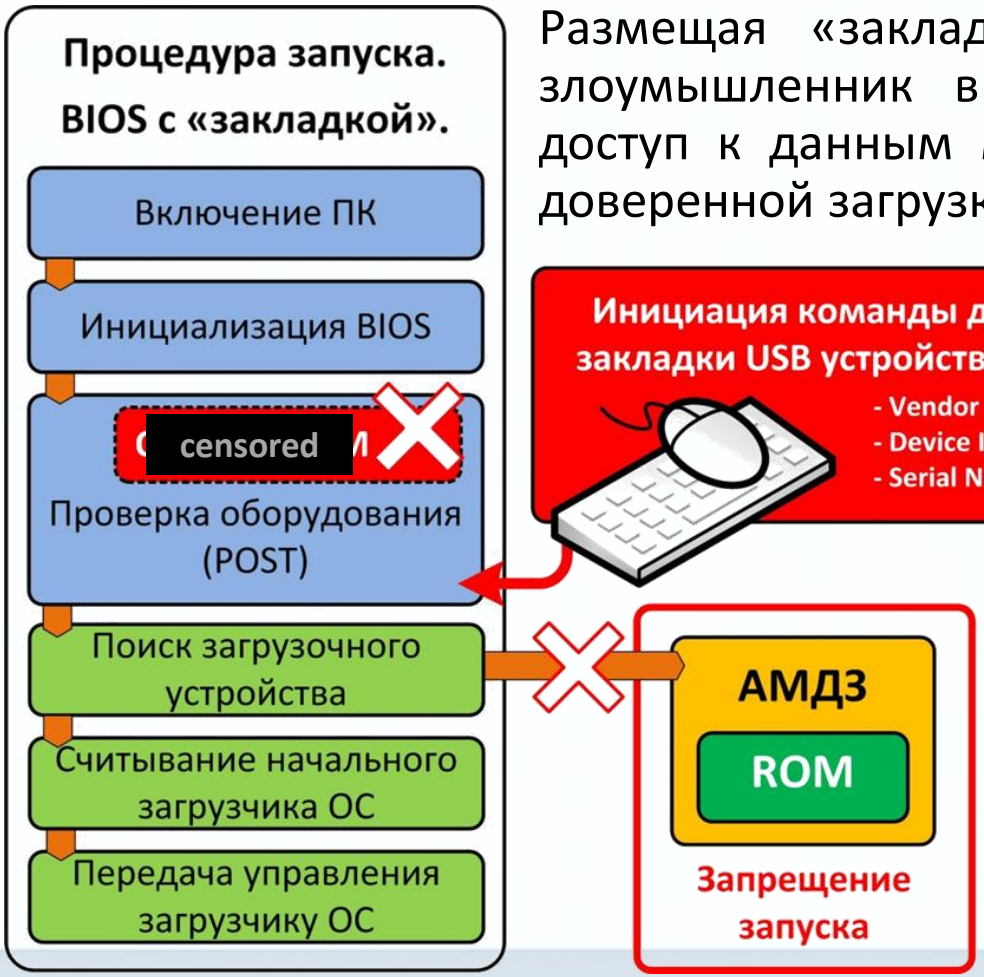

СПАСИБО ЗА ВНИМАНИЕ!
kraftway
ТЕХНОЛОГИИ БЕЗОПАСНОСТИ

СТАРТ СИСТЕМЫ С ТИПИЧНЫМ АПМДЗ

Имея наивысший приоритет среди загрузочных устройств, аппаратный модуль доверенной загрузки производит старт встроенной в контроллер ОС до запуска основной ОС.



НОВЫЕ УГРОЗЫ.
СИСТЕМЫ С МОДИФИЦИРОВАННЫМ BIOS



Размещая «закладку» в BIOS материнской платы, злоумышленник в любой момент может получить доступ к данным минуя защиту аппаратного модуля доверенной загрузки.

Ключ активации может иметь любое исполнение (мышь, токен, накопитель, клавиатура и т.д.).

После завершения действий злоумышленника система возвращается в исходное состояние, что не создаёт прецедентов для обращения в службу безопасности.

confidential

kraftway
ТЕХНОЛОГИИ БЕЗОПАСНОСТИ