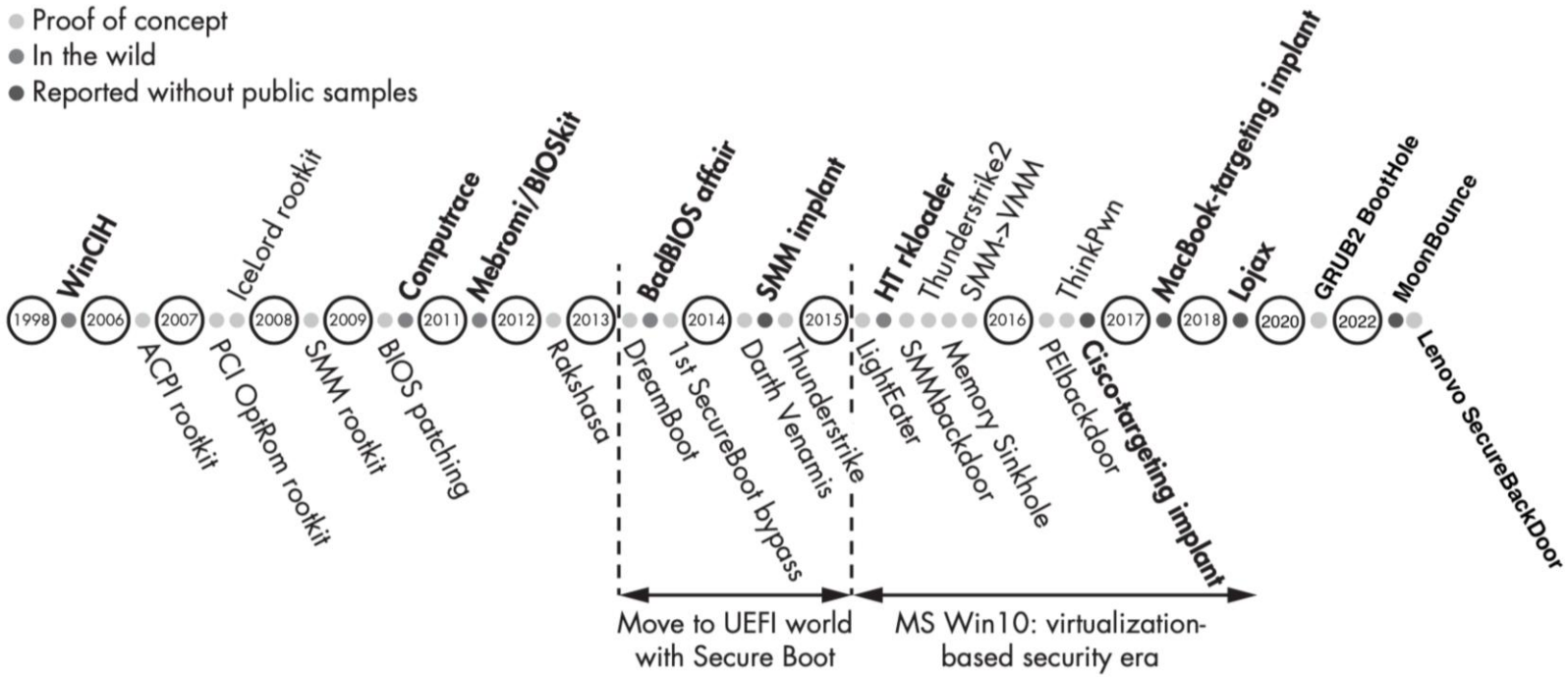
# Безопасная загрузка ядра Linux в UEFI окружении

проблемы и перспективы

С.К. Митрофанов <sk.mitrofanov@ispras.ru>
В.Ю. Чепцов <cheptsov@ispras.ru>
М.Ю. Кричанов <krichanov@ispras.ru>
А.В. Хорошилов <khoroshilov@ispras.ru>

ИСП РАН

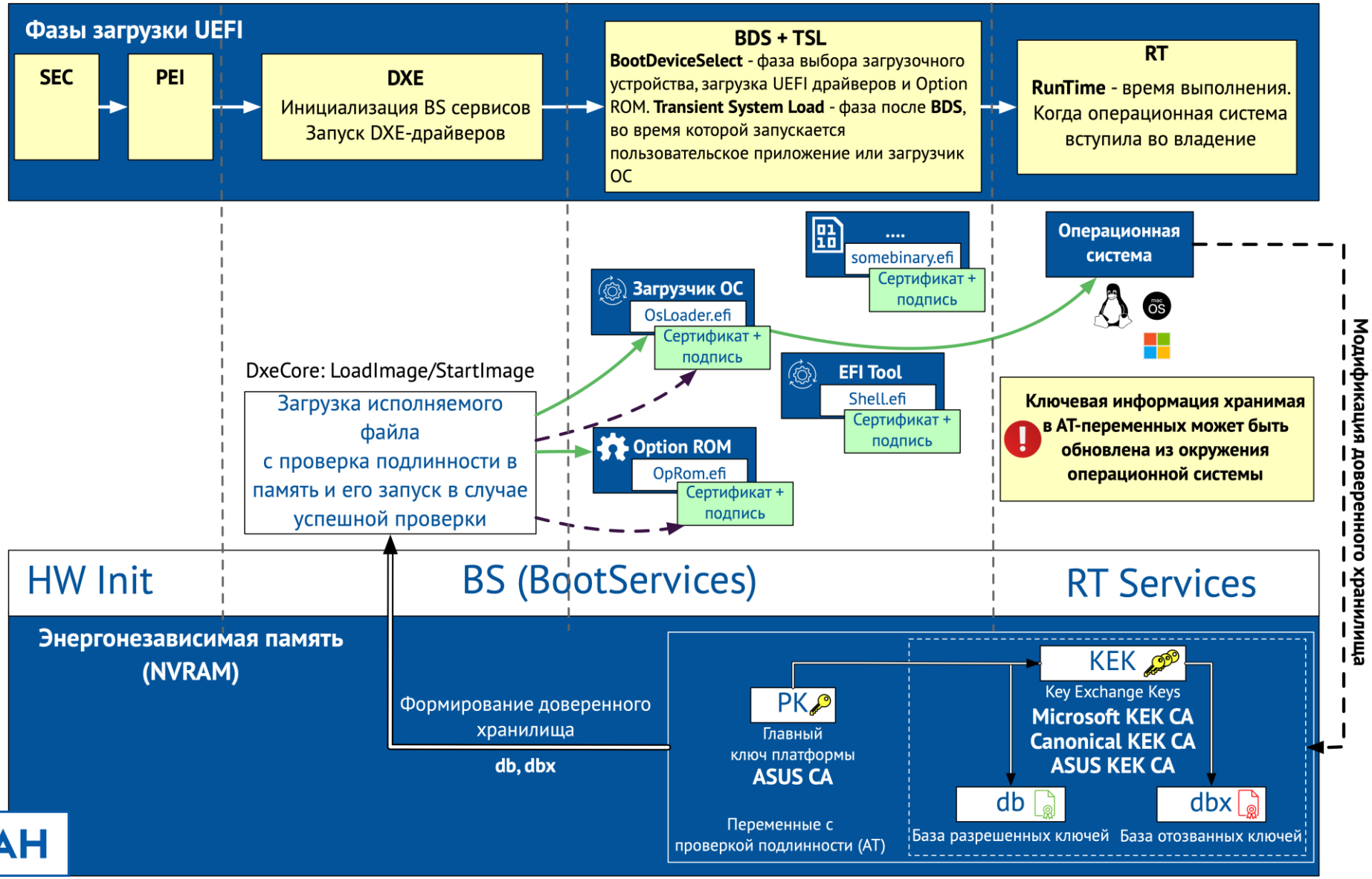
# Введение


**Михаил Кричанов, Виталий Чепцов**
Повышение безопасности прошивок с виртуальными машинами UEFI при помощи снапшотов и сокращения поверхности атаки

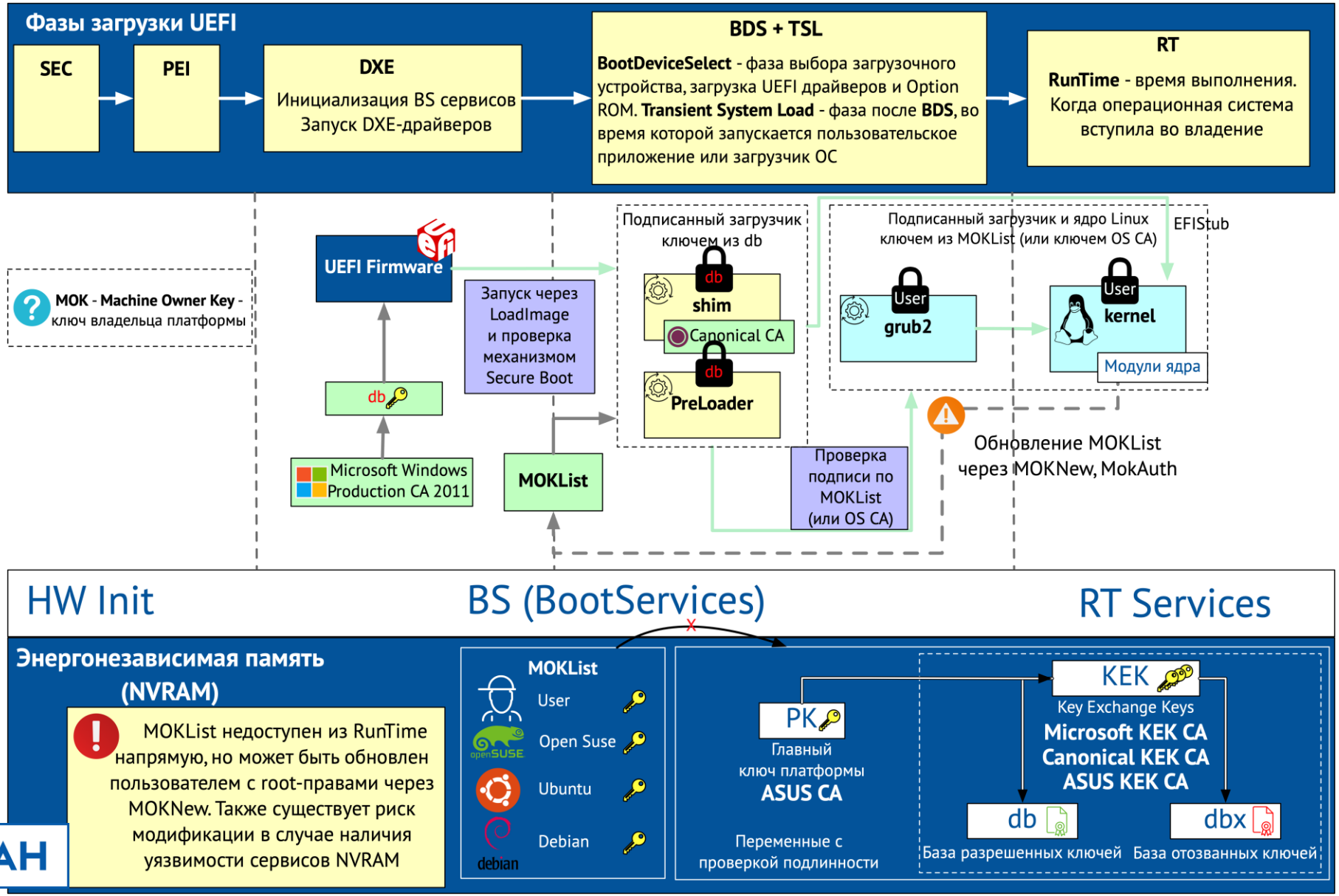
ИСП РАН

# UEFI Secure Boot




ИСП РАН

# Linux Secure Boot

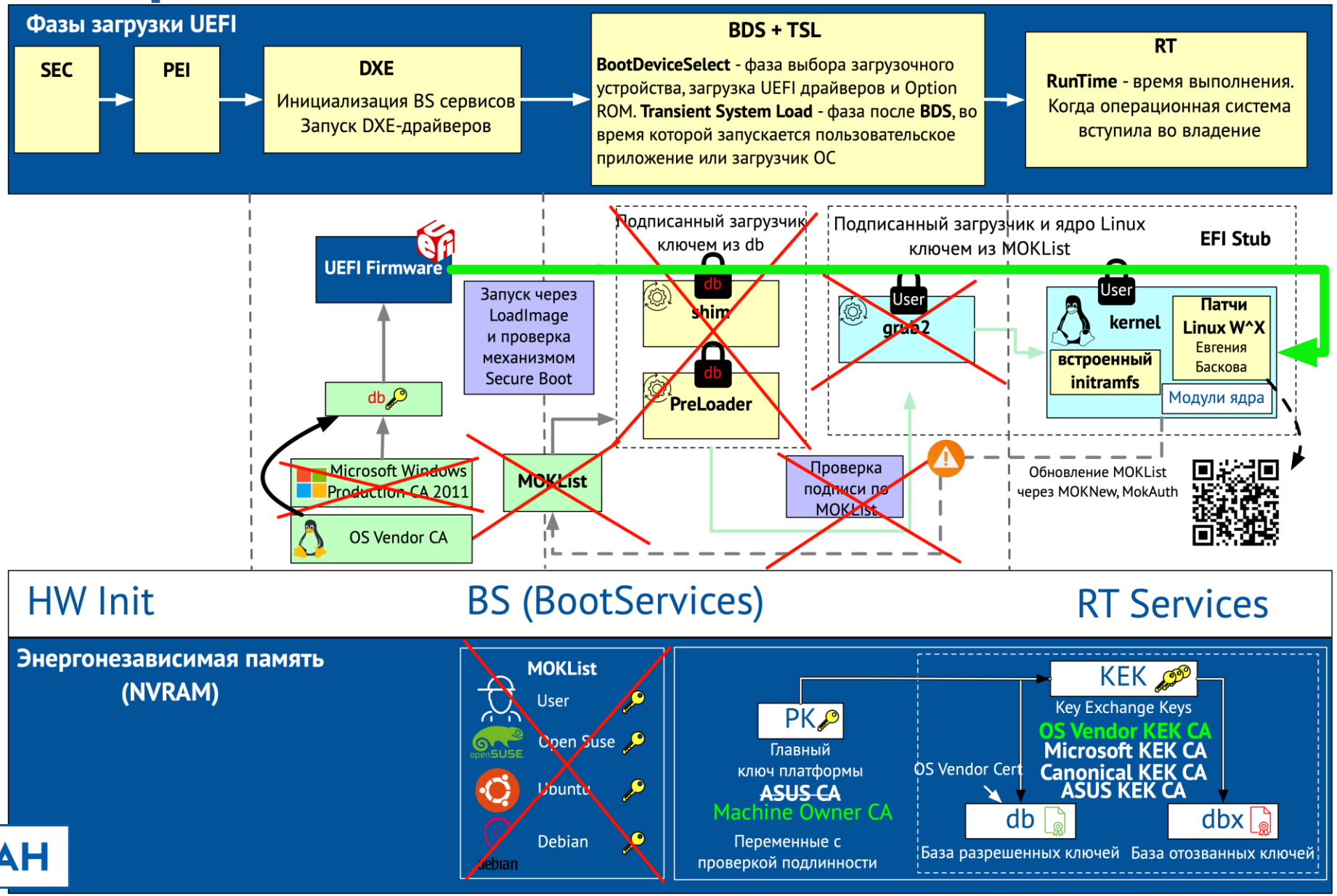



ИСП РАН

# В чем проблема?

- Бесконечный список доверенного ПО, порождаемый сертификатами **Microsoft** и **Canonical** через **shim**.
- Медленный отзыв уязвимых версий и связанные с этим проблемы; проблема разрастания **dbx**.
- Ключ владельца аппаратуры (**MOK**), хранится как **Boot Services** переменная, и может быть изменён на произвольный любым пользователем с правами **root**.
- Аргументы загрузки ядра хранятся на изменяемой файловой системе (в конфигурации загрузчика, прим. grub.cfg), в **NVRAM** переменной загрузочной записи (**Boot####**) или редактируются прямо из загрузчика, позволяя получить **root**-доступ.
- Цепочка доверия заканчивается на модулях ядра и не проверяет ни файловую систему начальной загрузки (**initrd**), ни какие-либо пользовательские программы.

# Решение проблемы «здесь и сейчас»

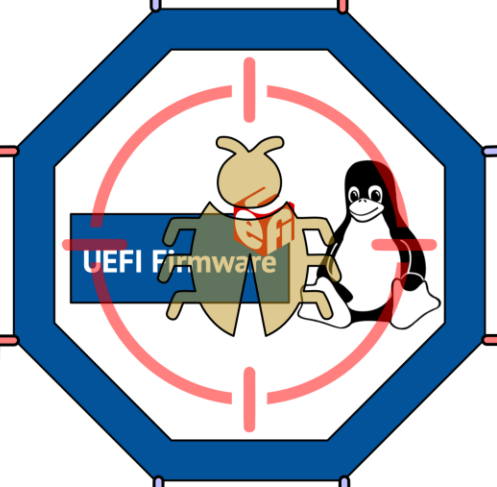



ИСП РАН

# Но... Есть архитектурные проблемы прошивки

- Отсутствует проверка типа накопителя и его физического расположения в устройстве.
- Отсутствует привязка экземпляра установленной операционной системы к экземпляру оборудования (запрет на запуск ОС с накопителя на другой аппаратной платформе).
- Отсутствуют политики безопасности для разделения на режимы сервисной (**recovery mode**) и обычной загрузки (**normal boot**).
- Отсутствует механизм безопасных версий загрузчика с прозрачным запретом предыдущих версий загрузчика после запуска более новых.
- Отсутствует темпоральность параметров безопасной загрузки (операционная система может менять список доверенных ключей на лету), приводящая к большой поверхности атаки, которая сейчас и ранее приводила к **полной компрометации устройства**.
- Используемый механизм подписи переусложнён необходимостью детальной обработки **PE/COFF** файлов и не расширяем, а его реализация содержит не исправленные по сей день уязвимости.

# Поверхность атаки




## Нарушение целостности ОС изнутри

Компрометация цепочки загрузки
**/boot/***, **vmlinuz**, **initrd** ...

## Нарушение статической целостности ОС извне

Подмена накопителя данных с последующей перезагрузкой
(диск с виртуальной машиной, диск физический HDD и т.д. )

## Запуск скомпрометированного ПО

Утечка сертификата – подпись вредоносного ПО.
Сброс настроек UEFI приводит к очистке **dbx**

## Нарушение динамической целостности ОС извне

Атаки TOCTOU.
**Пример**: SATA Hotplug с целью прохождения проверки целостности дистрибутива ОС.
Если для физической машины можно исправить повесив пломбу, то в системе виртуализации защититься в случае компрометации не выйдет.

## Откат к уязвимой версии программного обеспечения

Запуск уязвимой версии ОС.
Отсутствие механизма отзыва версий

## Подмена ОС на недоверенную

Запуск ОС отличной от разрешенной, например, запуск ОС Windows в обход политики безопасности, в том числе, с внешнего накопителя

## Компрометация прошивки через ее сервисы

**SMM** модули, сервисы **NVRAM**, ...

## Запуск с недоверенного носителя

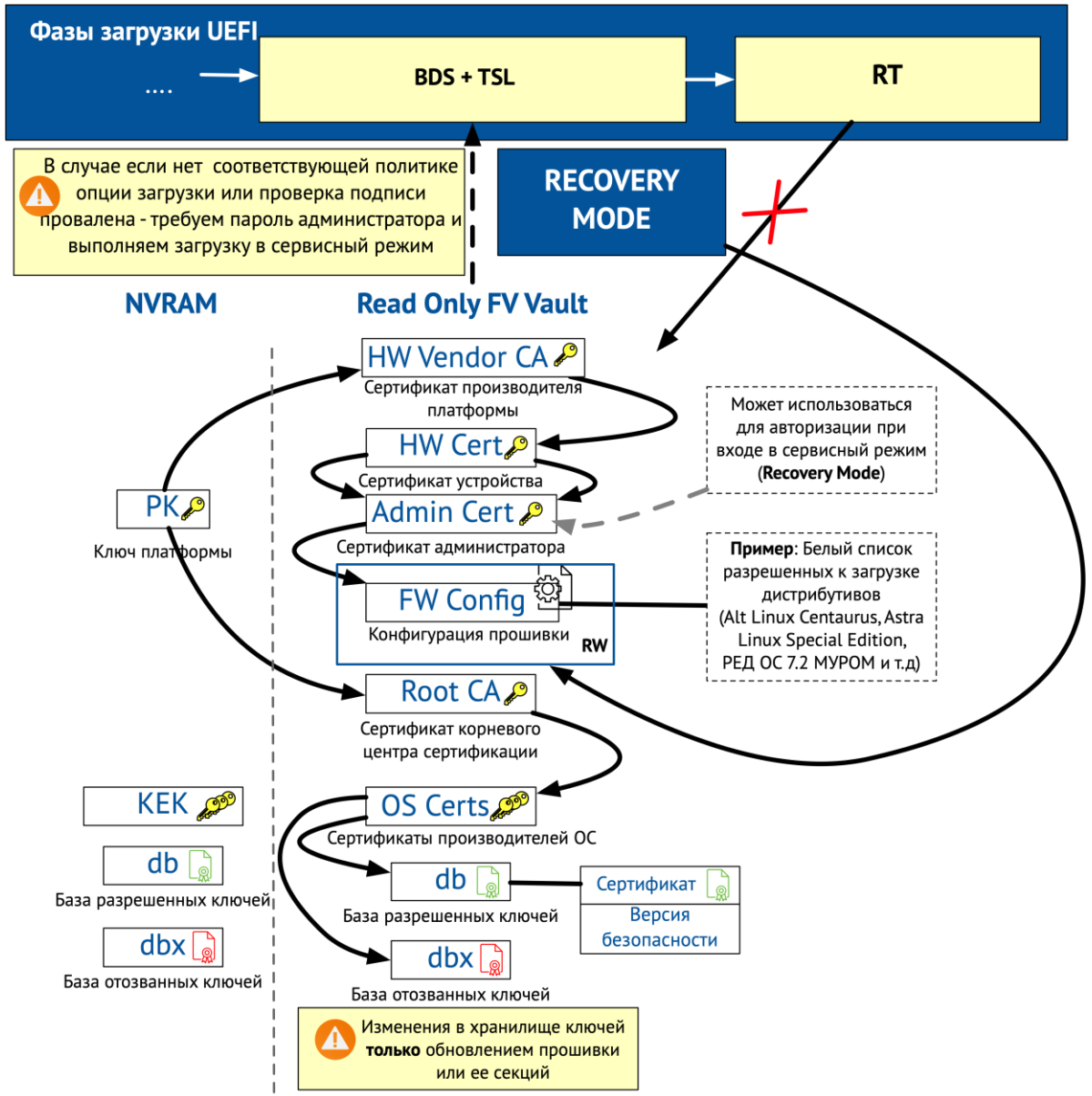
Клонирование ОС с модифицированными файлами
и параметрами, использование ее в качестве загрузочной

В рамках существующей реализации:

- – возможно частичное исправление
- – невозможно исправить

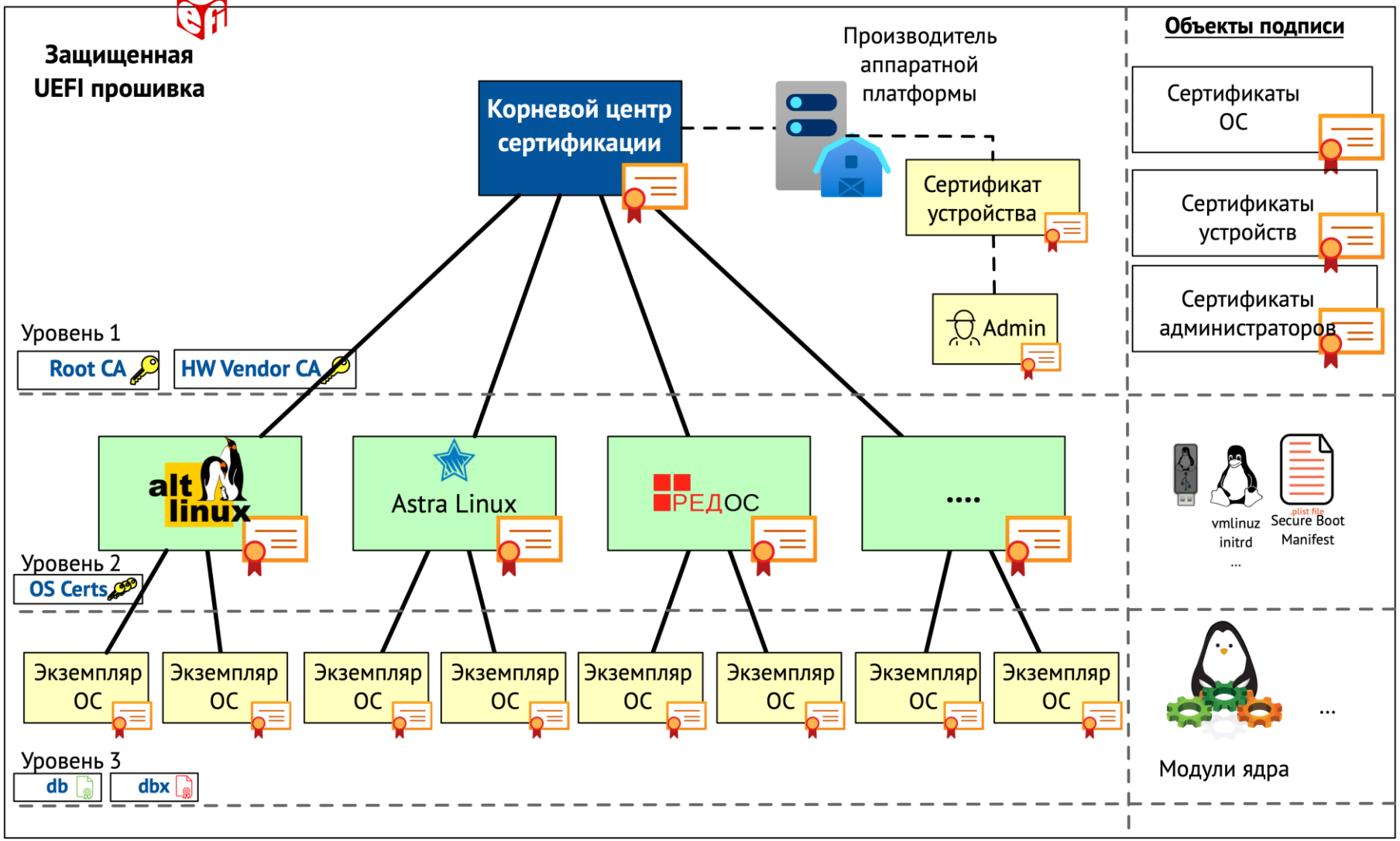
ИСП РАН

# Концепция механизма безопасной загрузки ОС




ИСП РАН

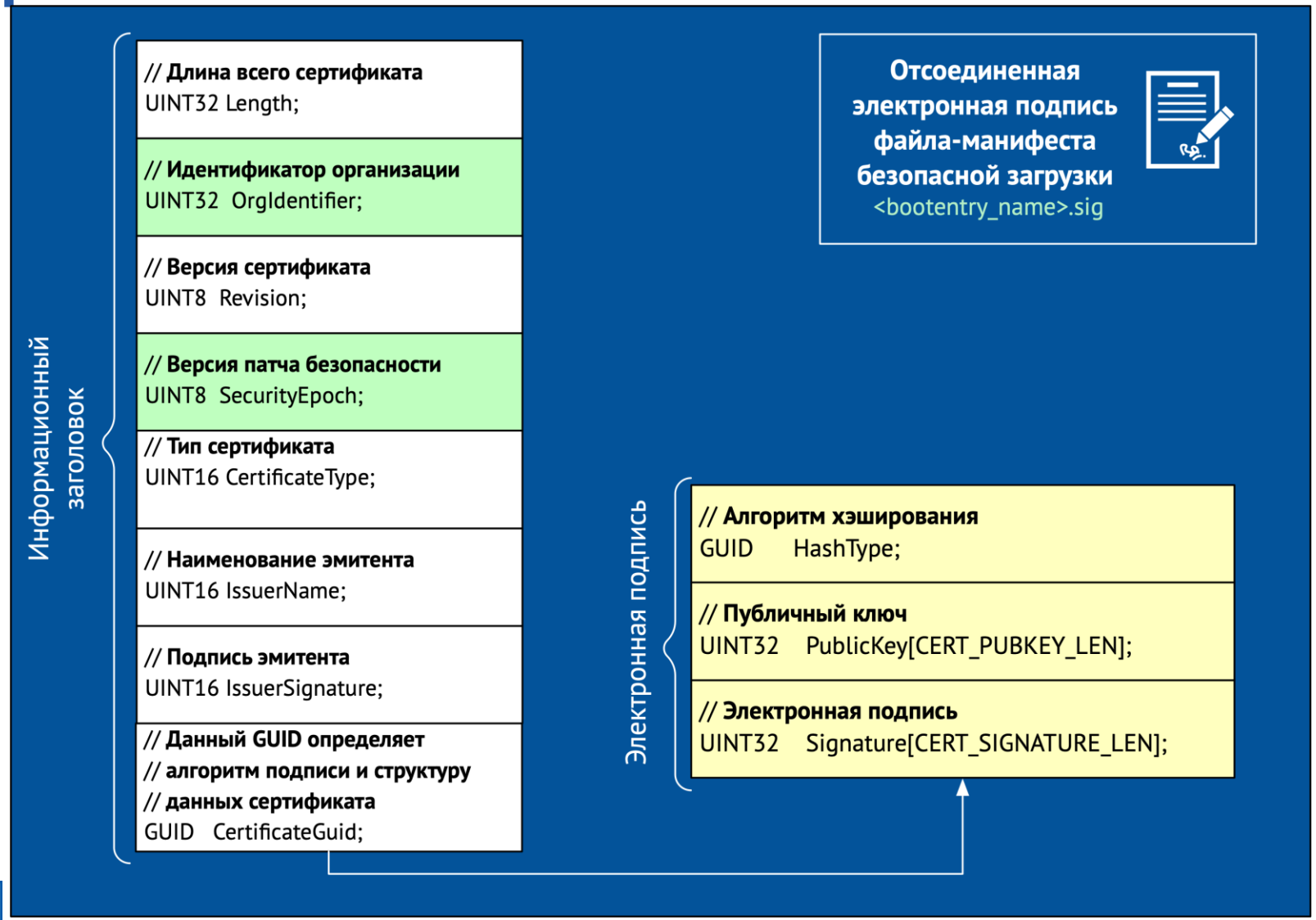
# Цепочка доверия



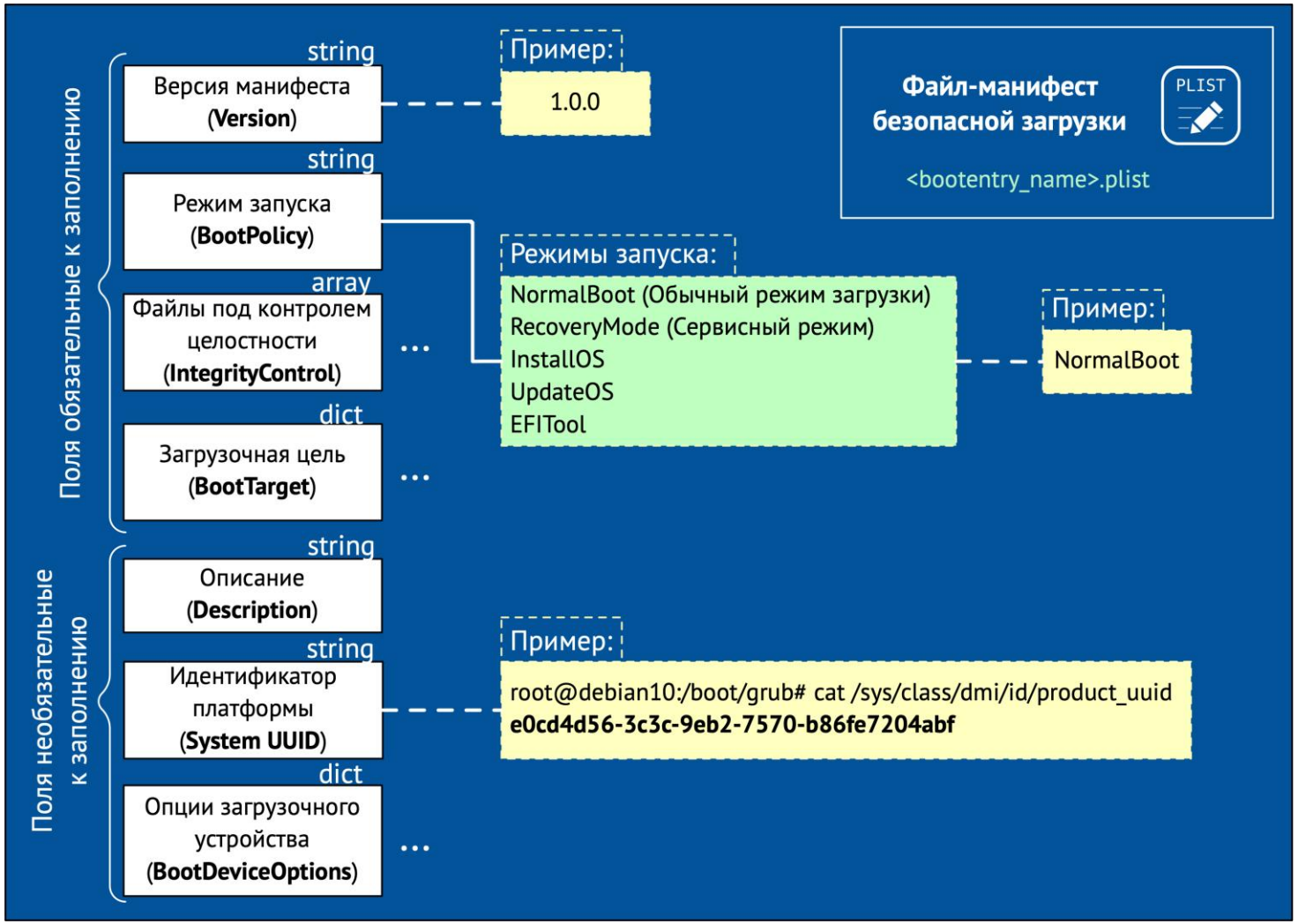
# Защищенный процесс загрузки


ИСП РАН

# Детали устройства механизма безопасной загрузки

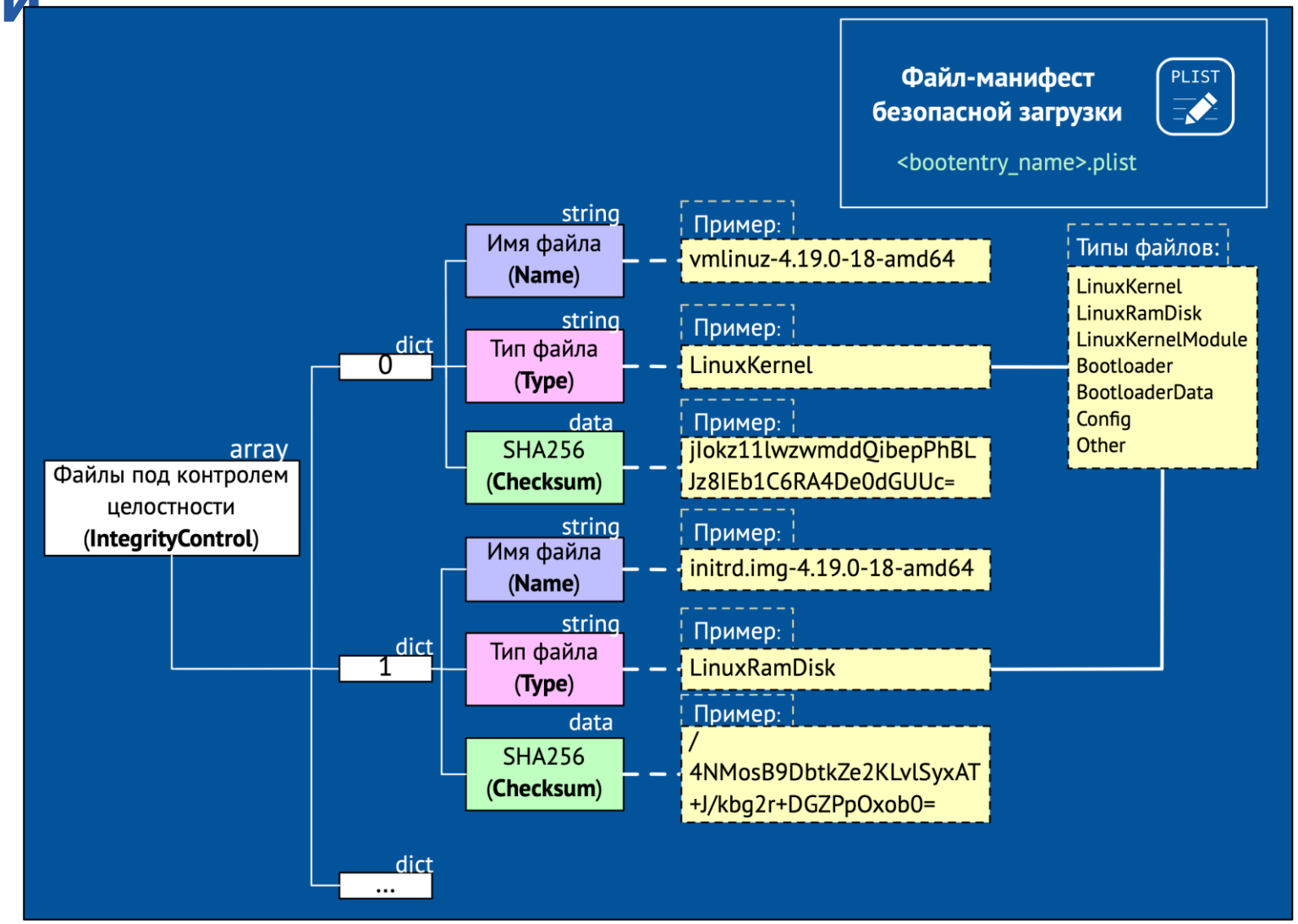


# Детали устройства механизма безопасной загрузки



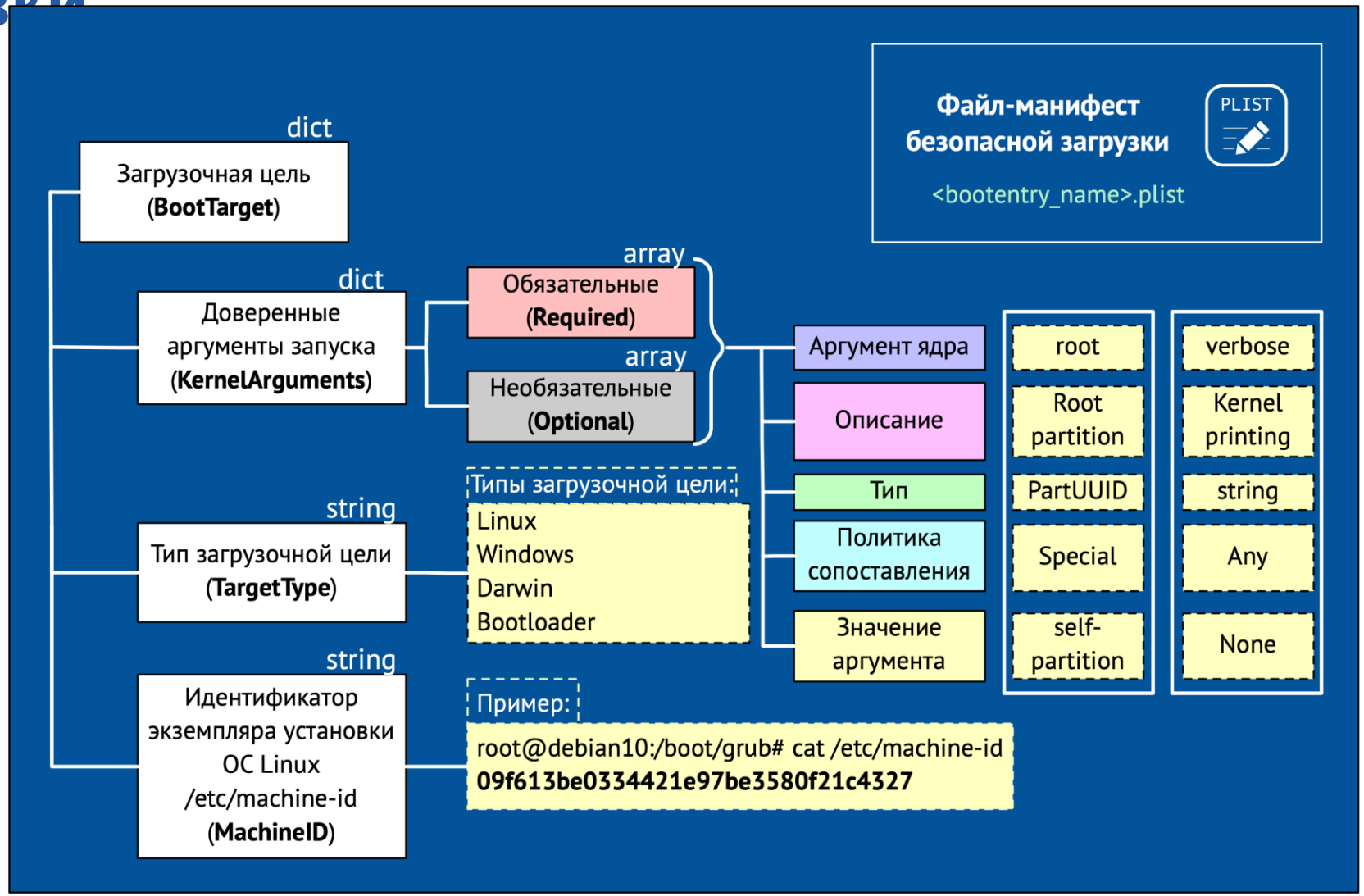

ИСП РАН

# Детали устройства механизма безопасной загрузки



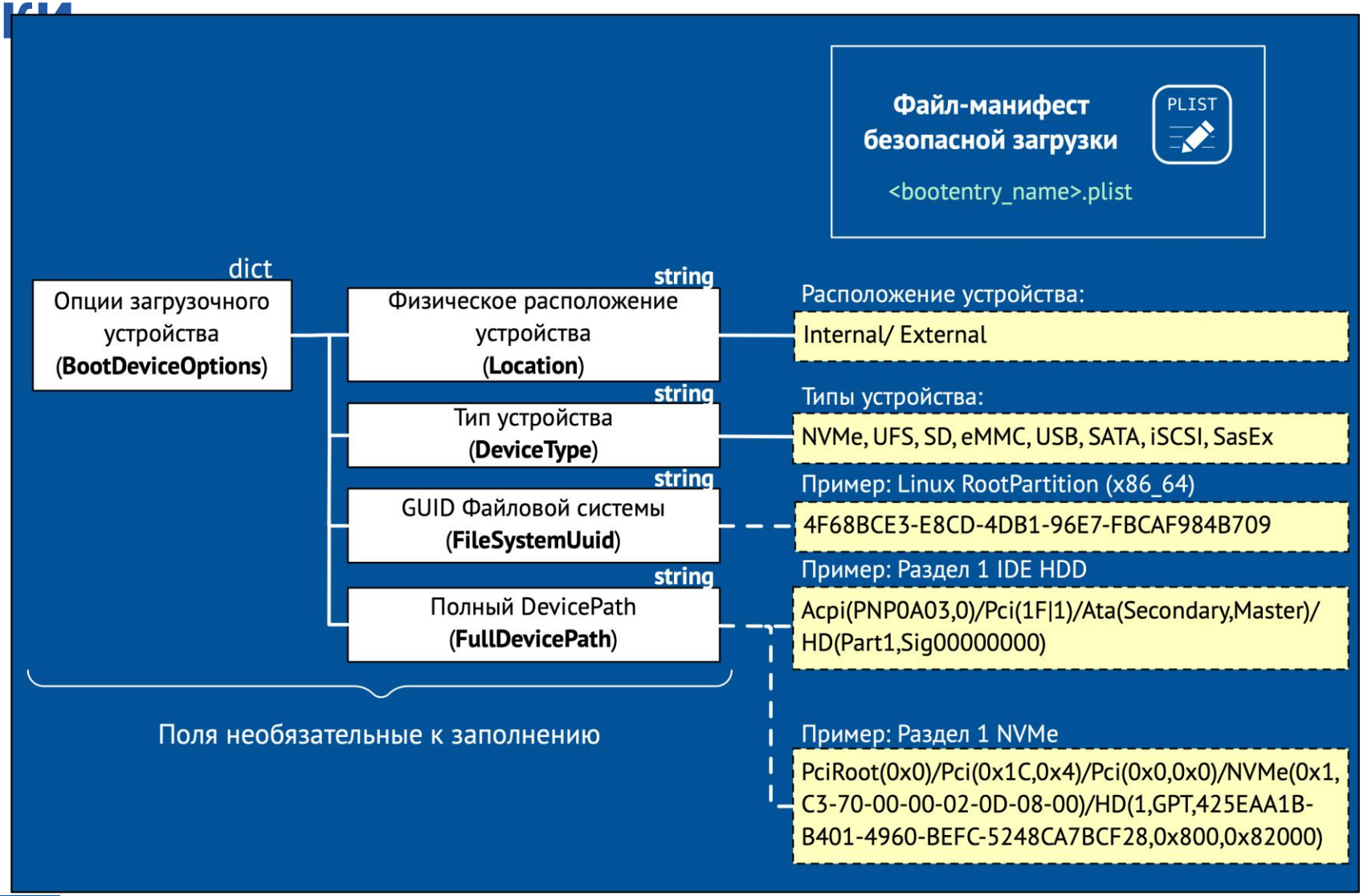

ИСП РАН

# Детали устройства механизма безопасной загрузки



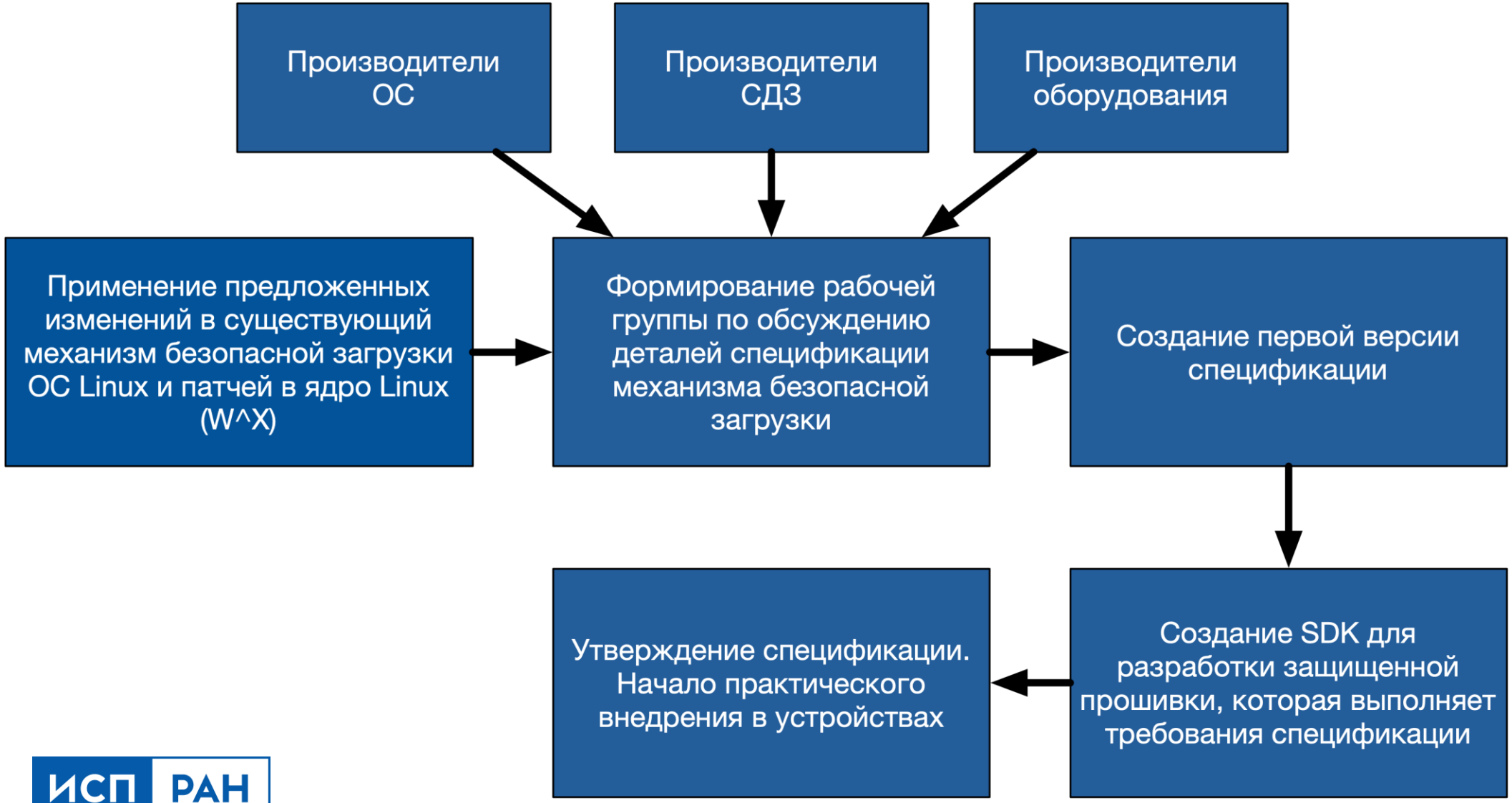

ИСП РАН

# Детали устройства механизма безопасной загрузки




ИСП РАН

# Заключение




ИСП РАН

# Спасибо за внимание!

ИСП РАН