КЛОС – конфигурируемая линейка операционных систем

Семейство операционных систем КЛОС

И. Б. Бурдонов, А. С. Косачёв, А. К. Петренко,
А. В. Хорошилов, В. Ю. Чепцов

ИСП РАН

Москва, ISPRASOPEN-2025, 10 декабря 2025

Новая волна развития ОС

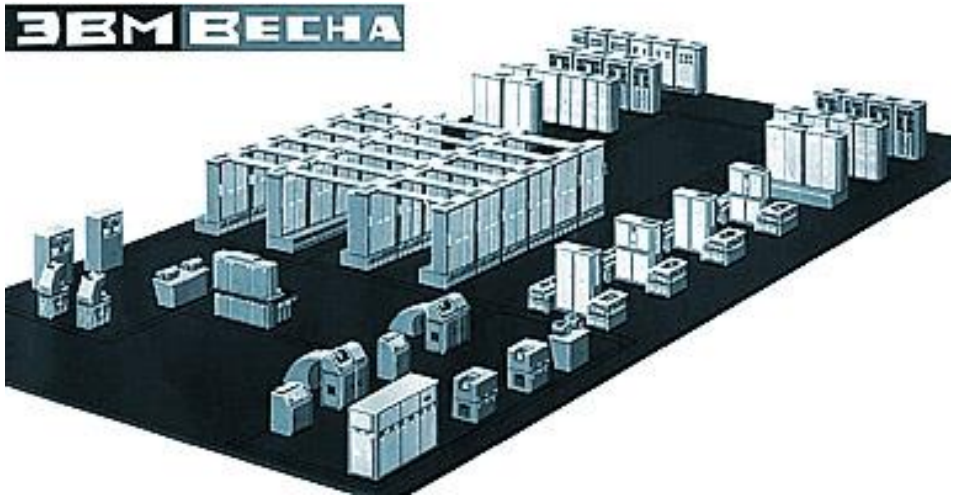
Факторы, определяющие направление исследований и разработок:

Возможности	Требования
Новые аппаратные платформы	Производительность
Новые методы и средства моделирования и верификации	Надёжность и безопасность
Зрелые процессы разработки	Экономия ресурсов

Технологический суверенитет ⟶ Отечественный программно-аппаратный стек

ИСП РАН

Первые отечественные ЭВМ с развитой системой прерываний



«Весна» — 1965 г.

БЭСМ-6 — 1967 г.

Первые отечественные ОС

Весна — 1965-1972

ОС «Весна» — 1966 г.

М. Р. Шура-Бура

В.С. Штаркман

БЭСМ-6 — 1968-1987

ОС ДТ-68

Л. Н. Королев

А. Н. Томилин

ОС НД-70

В. П. Иванников

ИСП РАН

Микроядерные ОС

Концепция новой архитектуры ОС начинает складываться 60-70-е года XX века.

- *В. П. Иванников. «Использование кластеров в операционной системе» ДАН СССР, 1977, Т. 237, № 2, стр. 2800–2833.*
- *В. П. Иванников. Проблемы операционных систем многомашинных вычислительных комплексов и реализация операционных системы АС-6-БЭСМ-6: Автореф. дис. на соиск. учен. степ. д. ф.-м. н. : 01.01.10, 1979.*

Термин «микроядерная ОС» появился гораздо позже, в 1981 году.

- *Rashid, Richard; Robertson, George. "Accent: A communication oriented network operating system kernel". SOSP '81 Proc. of the 8th ACM symposium on Operating systems principles. Pacific Grove, California, USA. pp. 64–75. doi: 10.1145/800216.806593*

Отечественные микроядерные ОС

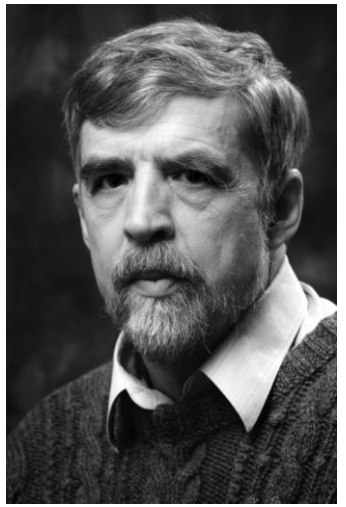
КЛОС (АС-6, 1975), **КЛАСТОС** (БЕСТА, 1980-е)

ИСП РАН

Основные разработчики КЛОС

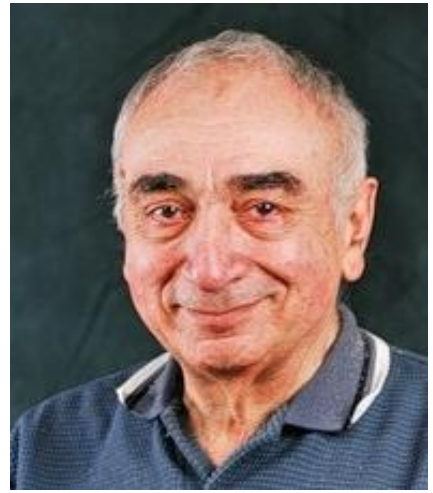
Виктор Иванников
Игорь Бурдонов
Александр Косачев





Герман Копытов
Сергей Кузнецов
Сергей Гайсарян





ИСП РАН

Развитие КЛОС в 2000-е годы

- Исследование и верификация ОС «Багет» (ОС-2000/3000).
- Изучение стандарта ARINC 653 – требования пространственной и временной изоляции, реализация обработки ошибочных ситуаций, детерминированное выполнение приложений даже при наличии отказов отдельных процессов.

Академик В. Б. Бетелин

- Развитие открытого проекта РОК — экспериментальной микроядерной ОСРВ с поддержкой ARINC 653.

ИСП РАН

Развитие КЛОС в 2010-е годы

- 2015 — Постановка задачи построения семейства ОС. Лаврищева Е.М., Петренко А.К. Моделирование семейств программных систем. Труды ИСП РАН, том 28, вып. 6, 2016, стр. 49-64. DOI:10.15514/ISPRAS-2016-28(6)-4

Академик Е.А. Федосов

- 2016 — Начало работ совместно с ГосНИИАС JetOS – микроядерная ОСРВ с поддержкой ARINC 653 и обеспечением требований DO-178C для программных систем с уровнем критичности «А».

ИСП РАН

Развитие КЛОС в 2020-е годы

- 2020— Начало разработки специальной микроядерной ОСРВ в интересах государственного заказчика.

Семейство космических аппаратов ИБИС

ИСП РАН

КЛОС

КЛОС — это технологический стек по созданию встраиваемых операционных систем жёсткого реального времени с поддержкой многоядерности, повышенных требований к безопасности (КТ-178С) и защищённости (РБПО).

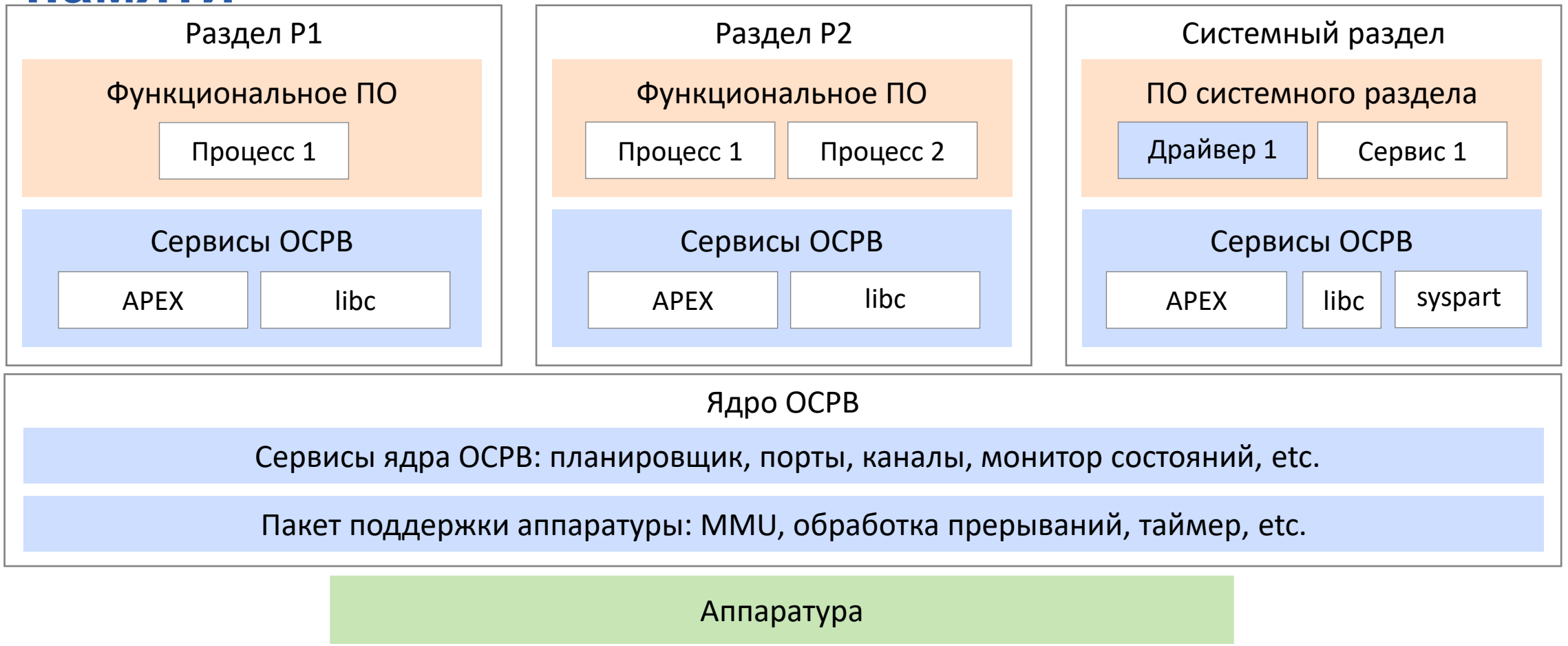
В КЛОС обеспечивается пространственная (по памяти) и временна́я (по гарантиям времени отклика) изоляция функционального и системного программного обеспечения. Накладные расходы со стороны ОСРВ минимизированы за счёт статического конфигурирования памяти и непериодических таймеров с квантованием.

Ключевые особенности

- Детерминированное выполнение приложений разных производителей на одном устройстве с изоляцией по времени и пространству.
- Выполнение драйверов устройств в изолированном окружении с пониженным уровнем привилегий для повышения безопасности и защищённости.
- Поддержка симметричной (SMP) и асимметричной (AMP) многоядерности для минимизации влияния параллельного кода.
- Отказ одного приложения не влияет на другое приложение. Централизованный мониторинг отказов (HMON).
- Гибкие требования к аппаратуре. Широкий набор поддерживаемых архитектур. eMMC, Ethernet, i2c, MAVLink, NVRAM (FRAM, EEPROM), ONFI NAND, Parallel и SPI NOR, PCI, RTC, SATA, SpaceWire, SPI, VirtIO, ГОСТ Р 52070-2003 (МКИО), UART, SPI NOR и др.
- Реализация API стандартов ARINC 653 P1 и P2, ISO/IEC 9899 (C) и 14882 (C++), GlobalPlatform TEE и других государственных отраслевых стандартов.

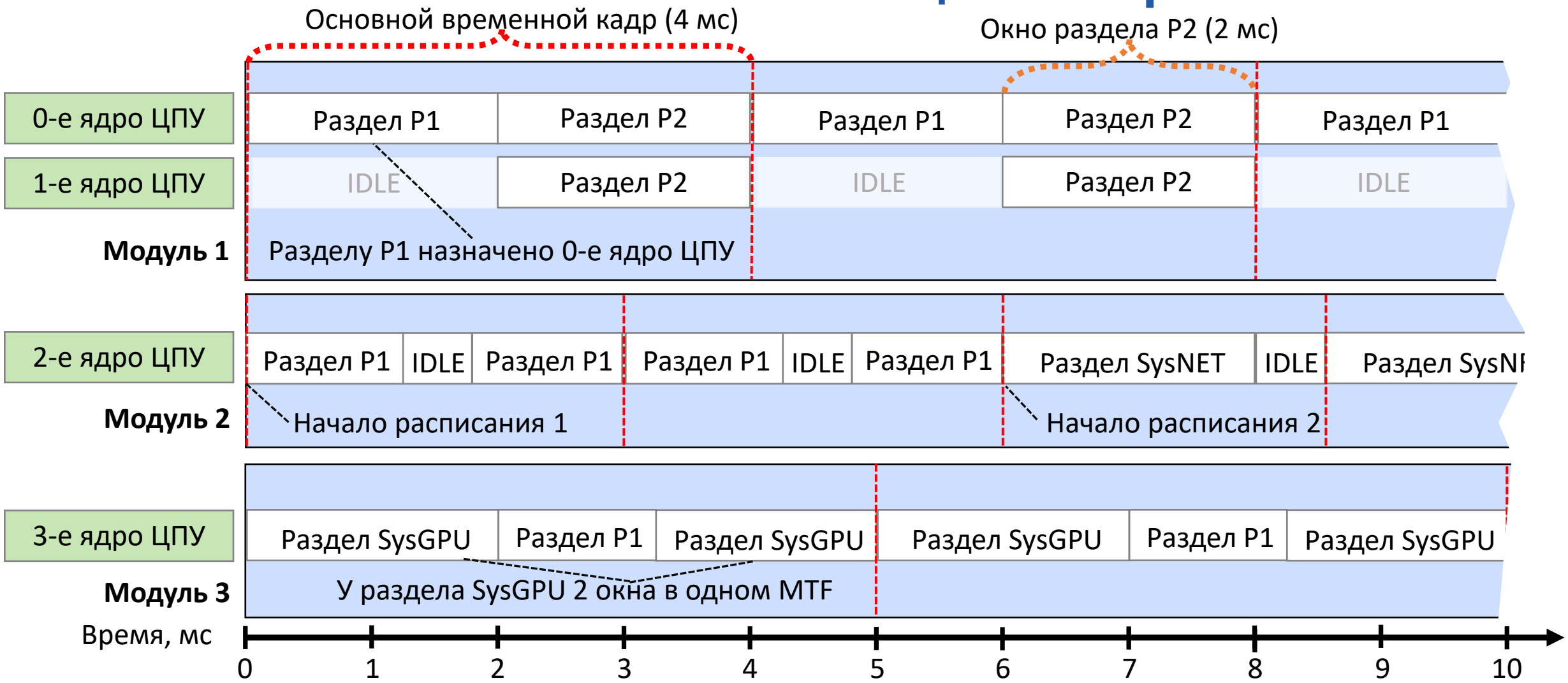
ИСП РАН

Механизмы обеспечения изоляции по памяти



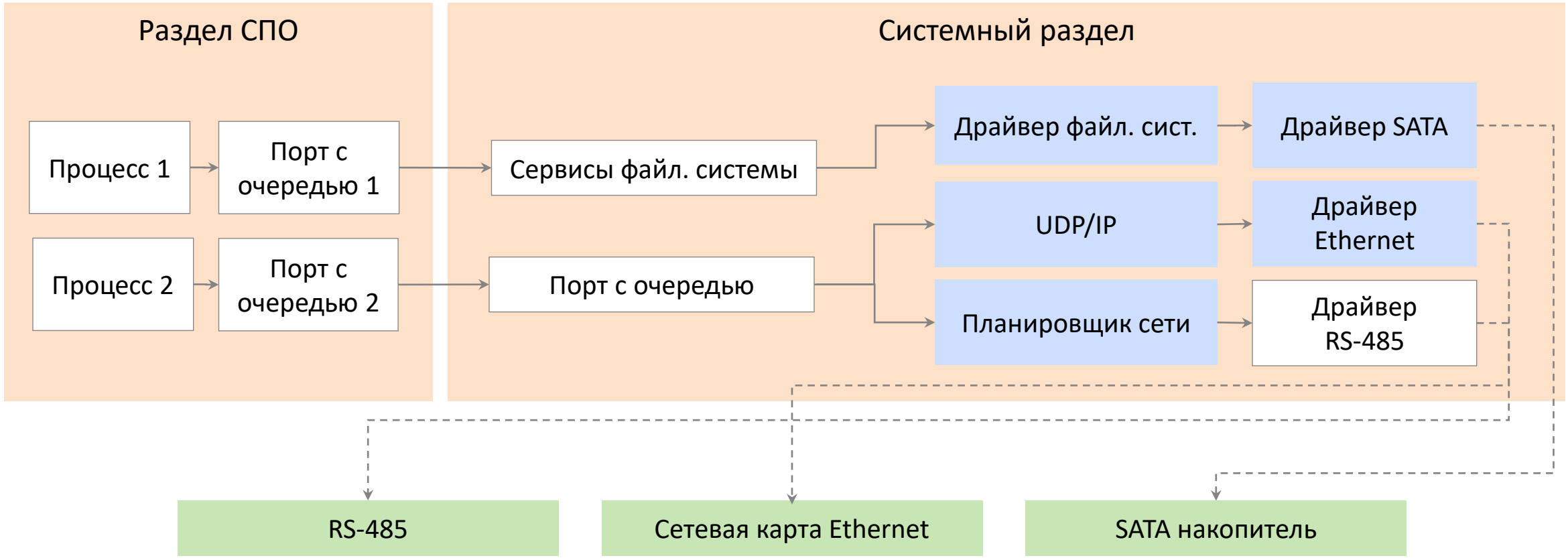
- Разделы изолированы по времени и пространству.
- Выделенные разделам ресурсы определены заранее на уровне конфигурации.
- Основная работа с оборудованием выполняется с пониженными привилегиями.

Механизмы обеспечения изоляции по времени



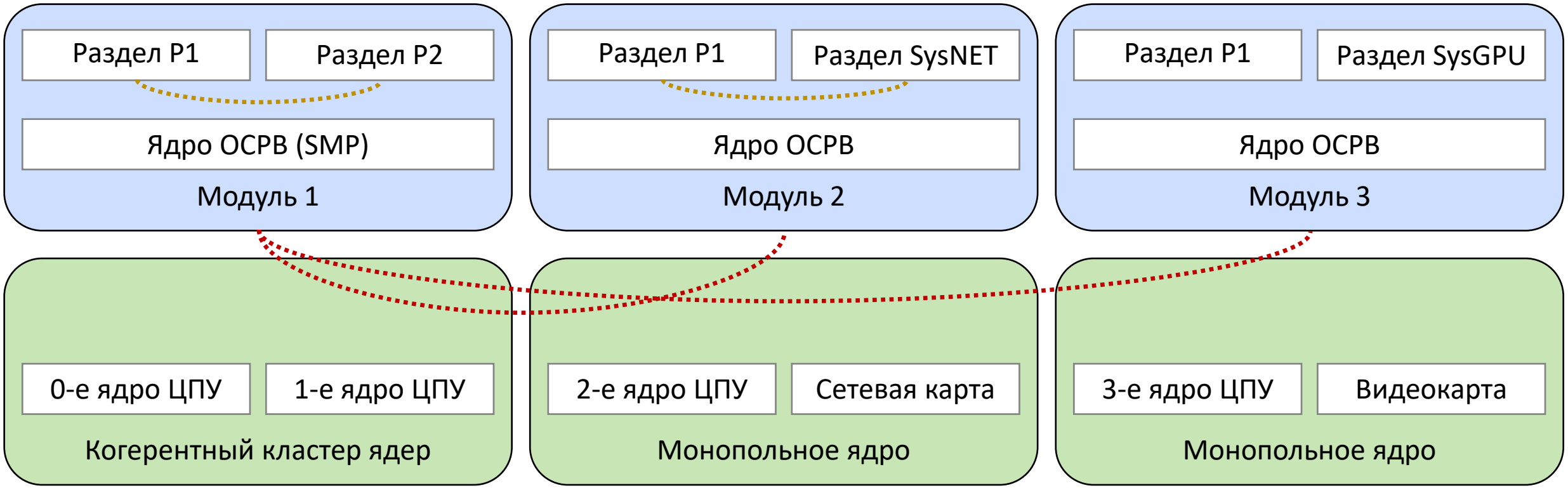
- Расписания распределяют время по окнам между разделами в рамках модуля.
- Окна расписания повторяются каждый основной временной кадр.
- Ядра ЦПУ назначаются разделу в рамках расписания.

Механизмы обеспечения изоляции драйверов устройств



ИСП РАН

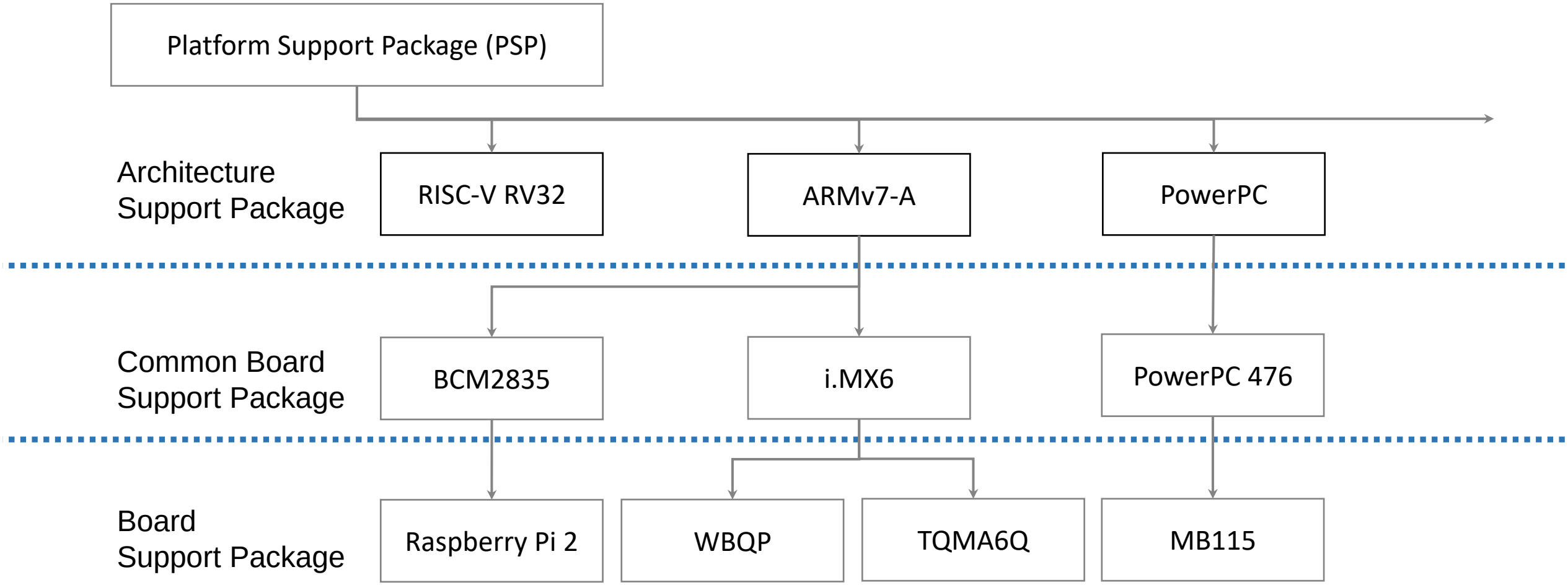
Механизмы обеспечения изоляции в многоядерном режиме



Разделы передают сообщения друг другу посредством:

- внутримодульных каналов в виде портов ARINC 653 в рамках своего кластера;
- межмодульных каналов в виде портов ARINC 653 в рамках нескольких кластеров;
- общих блоков памяти с явной настройкой когерентности доступа;
- каналов через сетевые устройства в виде портов ARINC 653 между разными вычислителями.

Структура пакета поддержки аппаратуры (PSP)



Поддерживаемые платформы

- ARMv7-A [Cortex-A7, Cortex-A9], e.g. NXP i.MX6 или Broadcom BCM2836
- ARMv7-M [Cortex-M4], e.g. ST STM32F429
- ARMv8-A [Cortex-A53, Cortex-A55], e.g. Rockchip RK3568
- MIPS32 [Мультикор, КОМДИВ], e.g. **НПЦ «Элвис»** 1892ВМ15АФ, **НИИСИ** 1890ВМ8Я, К5500ВК018
- PowerPC [e500v2, e500mc, 470S], e.g. NXP p1010, NXP p3041, **НТЦ Модуль** 476FP
- RISC-V [rv32 imafdc, Syntacore SCR5], e.g. **АО «НИИЭТ»** 1921ВК048
- x86 (IA-32) [Nehalem и новее]

Вычислитель должен обладать ≥ 2 МБ ОЗУ* и поддерживать атомарные инструкции.

Возможна доработка пакета поддержки аппаратуры на стороне заказчика и под конкретного заказчика.

** Ведутся работы по поддержке конфигураций с меньшими объёмами ОЗУ.*

ИСП РАН

Спасибо за внимание!

ИСП РАН

Инструменты для разработчика ПО

- Компиляторы Ada, C, C++, Modula 2 с поддержкой множества архитектур.
  GCC 14.3 и LLVM Clang 19. Безопасный компилятор.
- Динамические средства выявления ошибок с памятью и арифметикой.
  Санитайзеры LLVM: Address, Memory, Thread, Undefined Behavior.
- Статические анализаторы кода.
  Clang Static Analyzer. Clang Tidy. Анализ потребления стека. Svace.
- Средства сбора покрытия по коду.
  LLVM Covarge. GCOV. LLVM MC/DC, GCOV MC/DC, COVERest для MC/DC.
- Средства выявления узких мест производительности.
  Сэмплирующий профилировщик внутри OCPB (gprof).
- Средства ускорения процесса разработки.
  IDE на базе Eclipse или Theia. Интеграция в редакторы. Бинарная поставка кода.

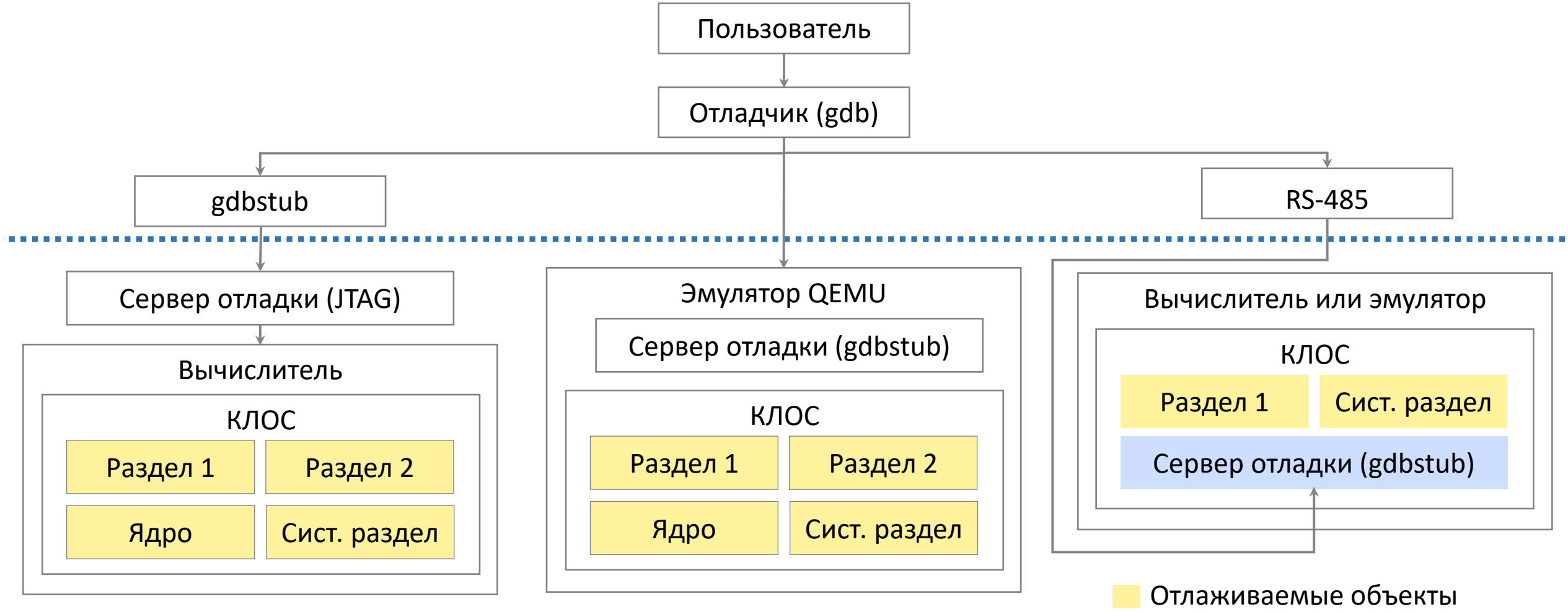
Существующие проекты

- JetOS — операционная система реального времени для гражданских авиалайнеров, построенных на архитектуре ИМА (интегрированной модульной авионики).
- Операционная система реального времени для космических аппаратов.
- TestOS — окружение для модульного тестирования программного обеспечения на целевой аппаратуре с целью проведения отработки ПО для ответственного применения.
- EmbetruOS — перспективная операционная система реального времени для энклавов и сопроцессоров, работающих в доверенном контуре вычислительной системы.
- Операционная система реального времени для доверенных БА.

Процессы интеграции, тестирования и отработки

- Встроенная система тестирования, которая позволяет проводить тестирование по единой схеме как на эмуляторе, так и на оборудовании.
- Поддержка инструментария для написания модульных (unit), интеграционных и полносистемных тестов, включая встроенные проверки и тестовые макросы.
- Расширенный набор инструментов поддержки создания доверенных программных систем, включая статический анализ (SVACE, KLEVER), сбор покрытия и динамическое инструментирование (LLVM Sanitizers, Race Hunter).
- Разработка сертифицированного пакета по КТ-178С по наивысшему уровню “А”.
- Обеспечение CI / CD / “непрерывного тестирования” (по запросу).
- Поддержка отладки на устройстве по единой схеме.

Сценарии интерактивной отладки



ИСП РАН

Требования к рабочей станции

- GNU/Linux дистрибутив на архитектуре x86_64 (например, Astra Linux 1.8 или Ubuntu 22.04), либо Apple macOS 10.12 или новее.
- Рекомендуется 4-ядерный процессор, 8 ГБ ОЗУ, 25 ГБ места на диске или лучше.
- Есть виртуальная машина в формате .ova (VirtualBox, VMware) для быстрого запуска и демонстрации возможностей.