Аппаратные способы защиты информации для микроконтроллеров в архитектуре RISC-V

OSDay 2026

Константин Невидин

Июнь 2026

Syntacore™
RISC-V cores and tools

Содержание доклада

- Архитектура RISC-V: профили, базовые операции, расширения и прочее.
- Аппаратные возможности защиты информации
- Факторы, влияющие на применимость аппаратных возможностей

© 2026 Syntacore. All trademarks, products,
and brand names belong to their respective owners

RISC-V история, архитектура 1

2010 г. Зарождение — американский университетский проект.
Профессор Дэвид Паттерсон и Крсте Асанович.

Цель: создать открытую и свободную архитектуру набора команд (ISA) на принципах Reduced Instruction Set Computing.

Мотивы

- Альтернатива проприетарным архитектурам (ARM, x86) без лицензионных ограничений.
- Поддержка академических исследований и быстрого прототипирования.
- Обеспечение **модульности** (базовый набор + опциональные расширения) и **масштабируемости** (от микроконтроллеров до суперкомпьютеров).

2014 г. — публикация первой официальной спецификации RISC-V.

- Быстрое признание в академической среде (использование в учебных курсах).
- Рост интереса индустрии: внедрение в коммерческих продуктах и встраиваемых системах. Активное международное сообщество разработчиков.
- Участие крупных компаний и стартапов в развитии экосистемы. Применение в IoT, микроконтроллерах, высокопроизводительных процессорах и др.

Открытость и свобода использования — основа инноваций и широкого распространения RISC-V по всему миру

© 2026 Syntacore. All trademarks, products, and brand names belong to their respective owners

RISC-V история, архитектура 2

Архитектура строится по принципу «ядро + модули»:

RV32I — 32-битная целочисленная базовая система команд.

RV64I — 64-битная версия (наиболее распространена в серверах и десктопах).

RV128I — перспективная 128-битная реализация.

I — целочисленные операции, это обязательный базовый профиль

M — целочисленное умножение и деление.

A — атомарные операции (для многозадачности).

F — арифметика с плавающей точкой (одинарная точность).

D — арифметика с плавающей точкой (двойная точность; требует F).

C — сжатые инструкции (16-битные) для экономии памяти.

Q — арифметика четверной точности (расширение D).

B — битовые операции (опционально).

V — векторные операции (для HPC, AI).

© 2026 Syntacore. All trademarks, products, and brand names belong to their respective owners

RISC-V на рынке микроконтроллеров

Основные применения:

- **Интернет вещей**
- **АСУ-ТП, промышленная** электроника
- Продвинутые **медицинские устройства**
- **Автомобильная электроника**
- **Искусственный интеллект (AI Edge)**
- **Безопасность** (датчики дыма, системы контроля пожаробезопасности, взлома и прочее — это очень большой рынок)

© 2026 Syntacore. All trademarks, products, and brand names belong to their respective owners

RISC-V на рынке

2022
более **10** млрд ядер

2024
62,4 млрд ядер*

2025
14% рынка процессорных ядер*
28% рынка процессоров IoT**

2027
25 млрд ускорителей AI*

2028
20 млрд процессоров для рынка IoT***

* Semico Research, December 2021
** Counterpoint Technology Market Research, September 2021
*** Omdia Research, May 2023

До 16%

вырастет доля RISC-V ядер в полупроводниковых IP к 2027 году.

Некоторые примеры:

- 650 млн RISC-V ядер отгружены Qualcomm для mobile, automotive, extended reality и IoT продуктов
- Более 7 млн штук продаж смартфона Pixel 6 от Google, содержащего чип безопасности на RISC-V

© 2026 Syntacore. All trademarks, products, and brand names belong to their respective owners

Безопасность микроконтроллеров

Уязвимости в ПО (firmware)

- Недостаточная валидация данных
- Ненадлежащая обработка исключений
- Использование устаревших библиотек

Атаки на аппаратуру

- Атаки по побочным каналам
- Glitch-атаки
- Декорпусирование

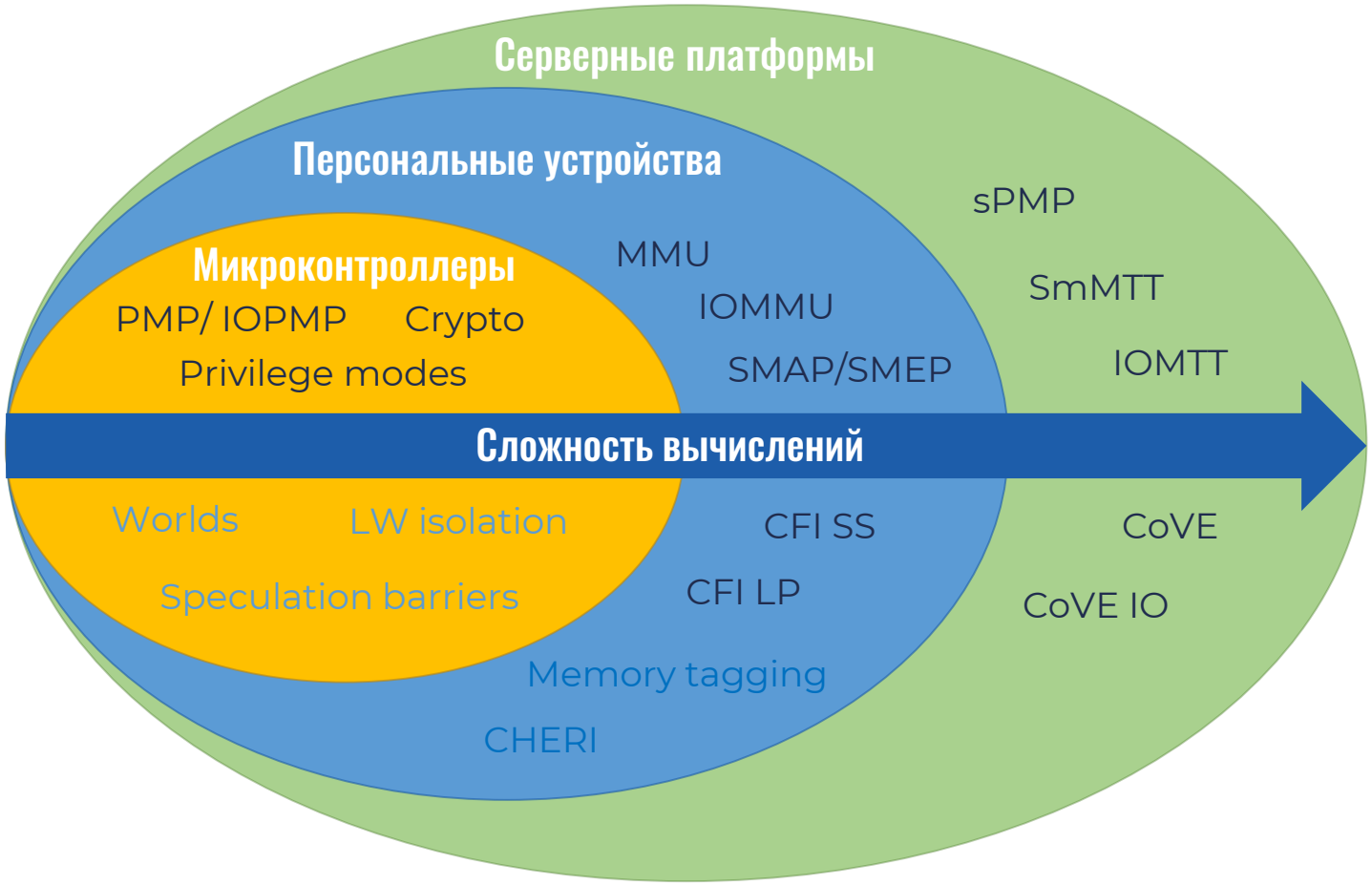
Уязвимости в коммуникационных протоколах

База уязвимостей (Common Weakness Enumeration)

CWE-1429, CWE-441, CWE-1194, CWE-1319, CWE-1201, CWE-1257, CWE-1419, CWE-1193, CWE-1320, CWE-1299, CWE-1393, CWE-1391, CWE-1252, CWE-1392, CWE-1423, CWE-1332, CWE-1318, CWE-1247, CWE-1384, CWE-1343, CWE-1300, CWE-1432

© 2026 Syntacore. All trademarks, products, and brand names belong to their respective owners

Развитие средств защиты в архитектуре RISC-V



PMP — Physical Memory Protection

IO — input/output

MMU — Memory management unit

SMAP/SMEP — Supervisor Memory Access/Execution Prevention

CHERI — Capability Hardware Enabled RISC-V Instructions

CFI — Control flow integrity

SS — Shadow Stack

LP — Landing pads

sPMP — Supervisor mode PMP

SmMTT — Supervisor mode Memory Tracking Table

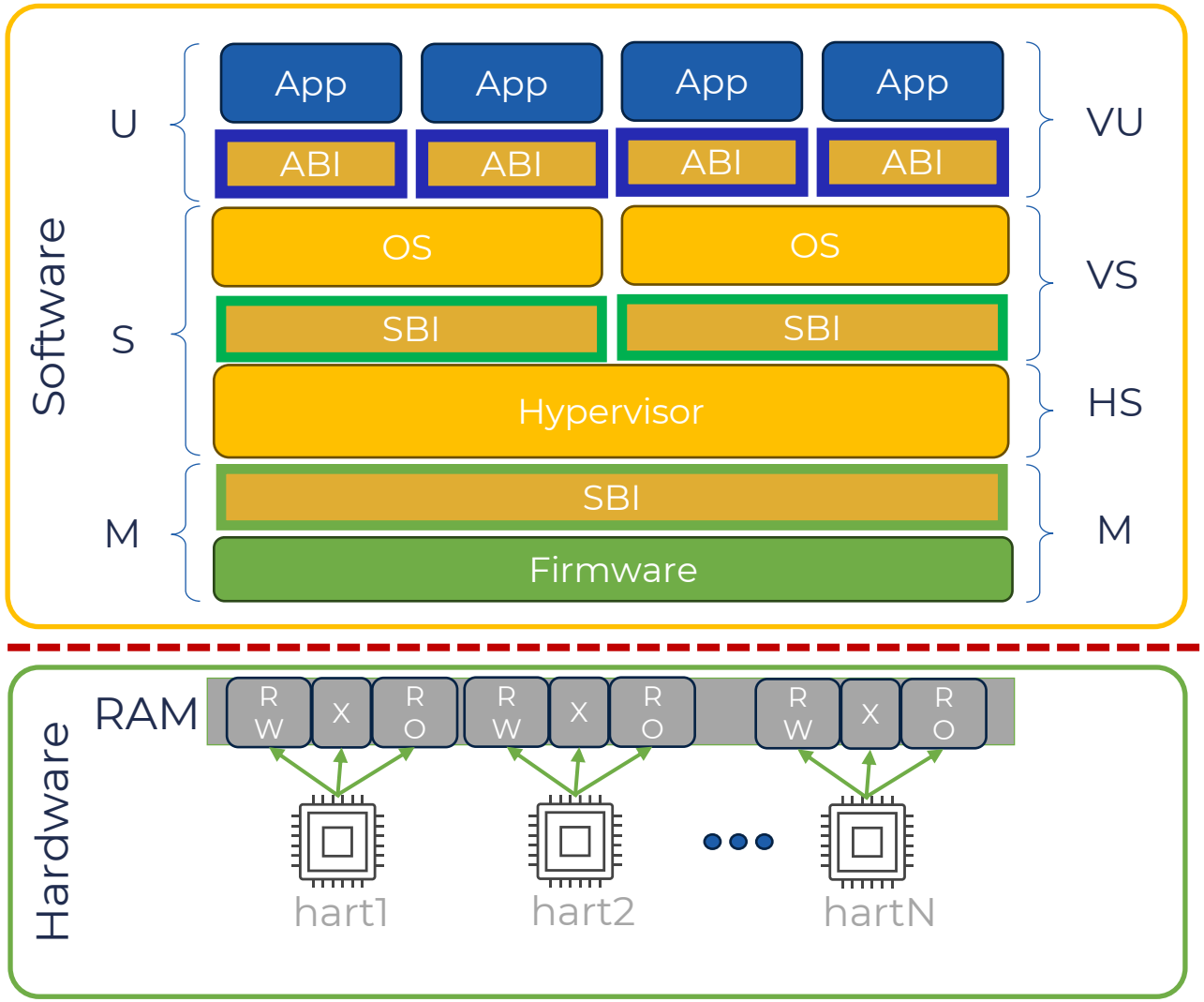
CoVE — Confidential VM Extension

LW Isolation — lightweight isolation

Syntacore™ RISC-V cores and tools

© 2026 Syntacore. All trademarks, products, and brand names belong to their respective owners

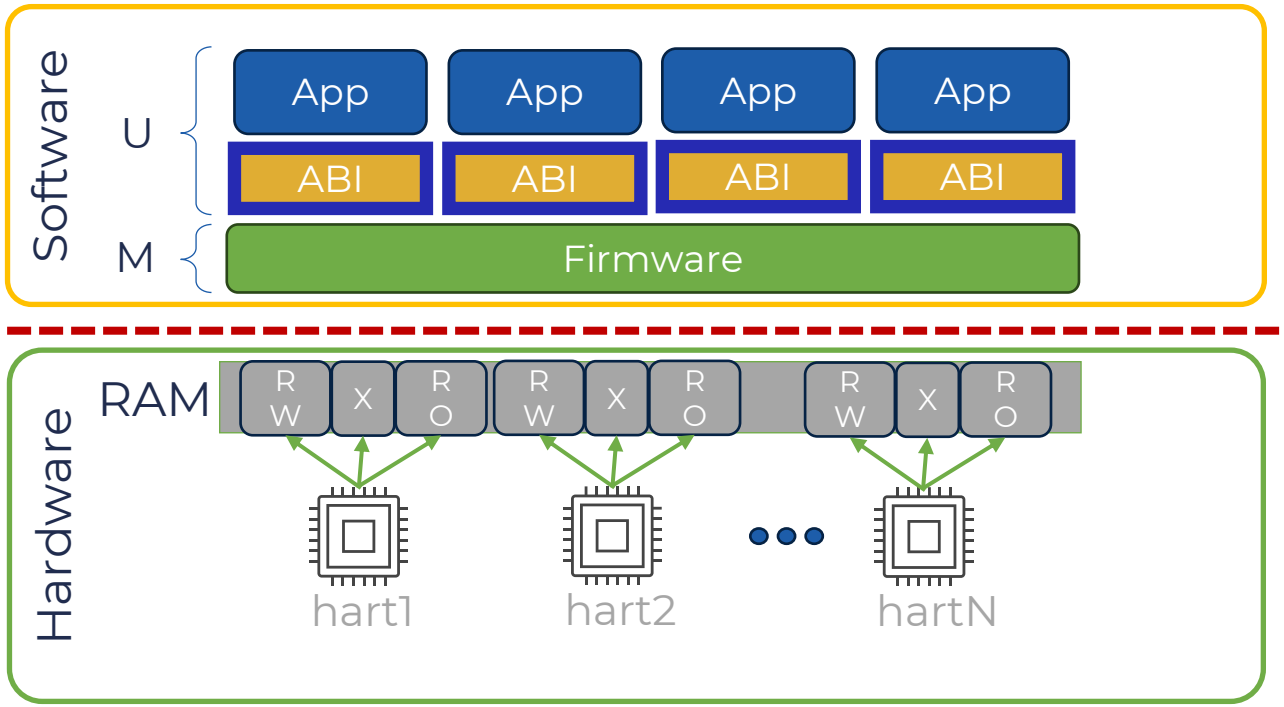
Уровни привилегий



- Простейший режим
  - Machine
    или
  - Machine – User
- Невиртуальный режим:
  - Machine – Supervisor – User
- Виртуальный режим:
  - M – HS – VS – VU

© 2026 Syntacore. All trademarks, products, and brand names belong to their respective owners

Уровни привилегий микроконтроллеров

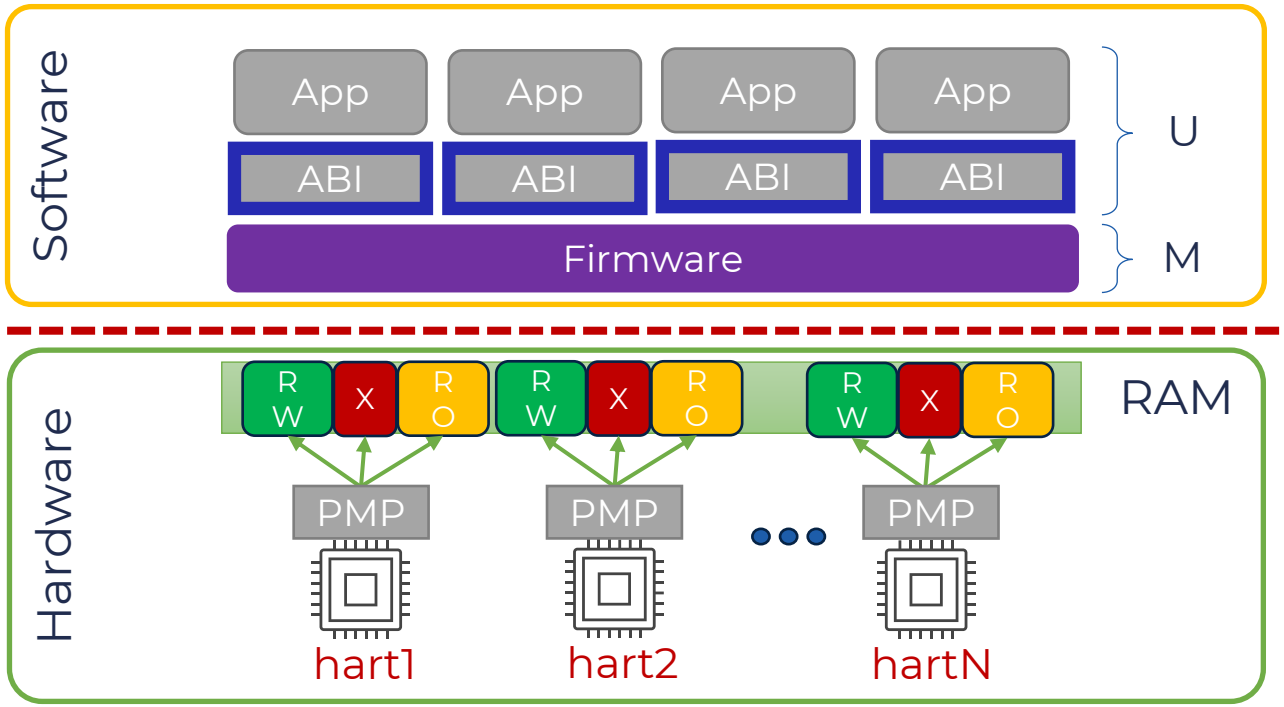


- Простейший режим
  - Machine
    или
  - Machine – User

Syntacore™ RISC-V cores and tools

© 2026 Syntacore. All trademarks, products, and brand names belong to their respective owners

Защита физической памяти — PMP



PMP проверки применяются в следующих случаях:

- U-режим — RAM/MMIO
- M-режиме — RAM/MMIO со сменой режима привилегий на S или U.

PMP: Поддерживается до 64 регионов.

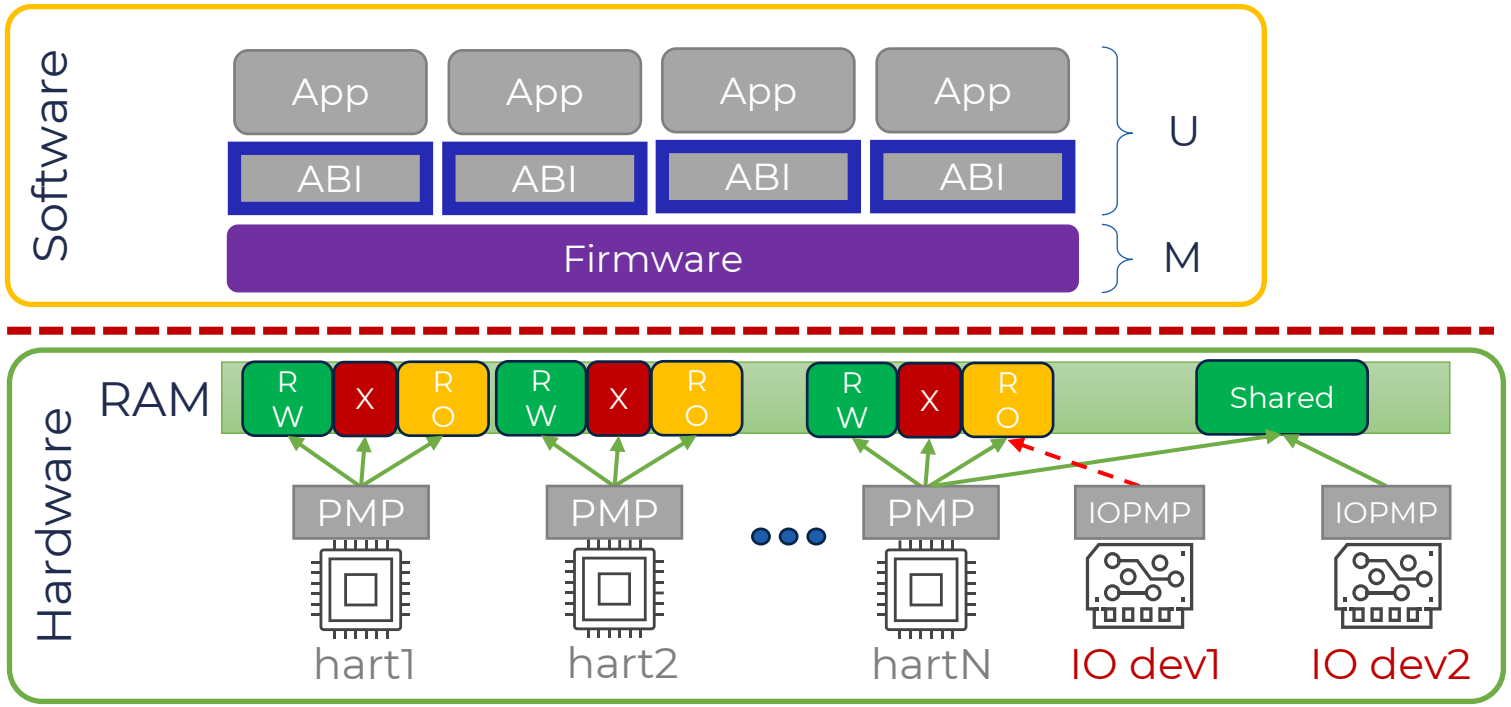
Note: Различные реализации могут поддерживать 0, 16 или 64 PMP записи

smepmp: запрет доступ из M-режима, таким образом даже программное обеспечение в M-режиме не может получить доступ к регионам в S/U режимах.

smap/smep: запрет доступ из S-режима, таким образом программное обеспечение в S-режиме не может получить доступ к регионам в U режимах.

© 2026 Syntacore. All trademarks, products, and brand names belong to their respective owners

Защита памяти от злонамеренного доступа со стороны вешних устройств — IOPMP



Request Role-ID, **RRID** — уникальный идентификатор для

- инициатора шины
- группы инициаторов шины с одинаковыми правами доступа

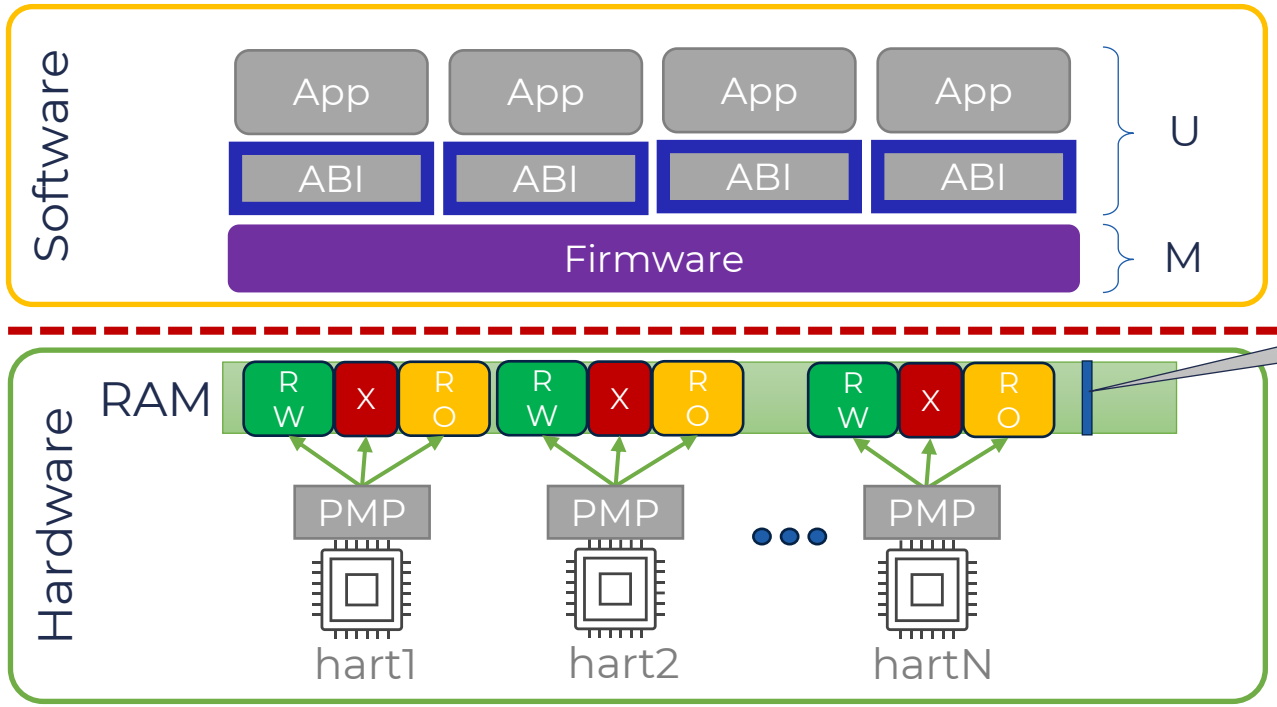
Экземпляр IOPMP может поддерживать до **65 535** источников.

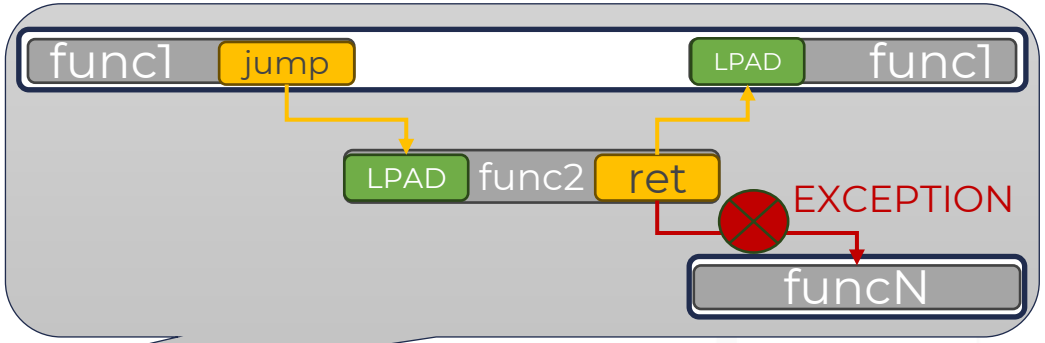
Полная модель IOPMP поддерживает до **63** доменов памяти.

Syntacore™ RISC-V cores and tools

© 2026 Syntacore. All trademarks, products, and brand names belong to their respective owners

Целостность потока управления — Landing pads

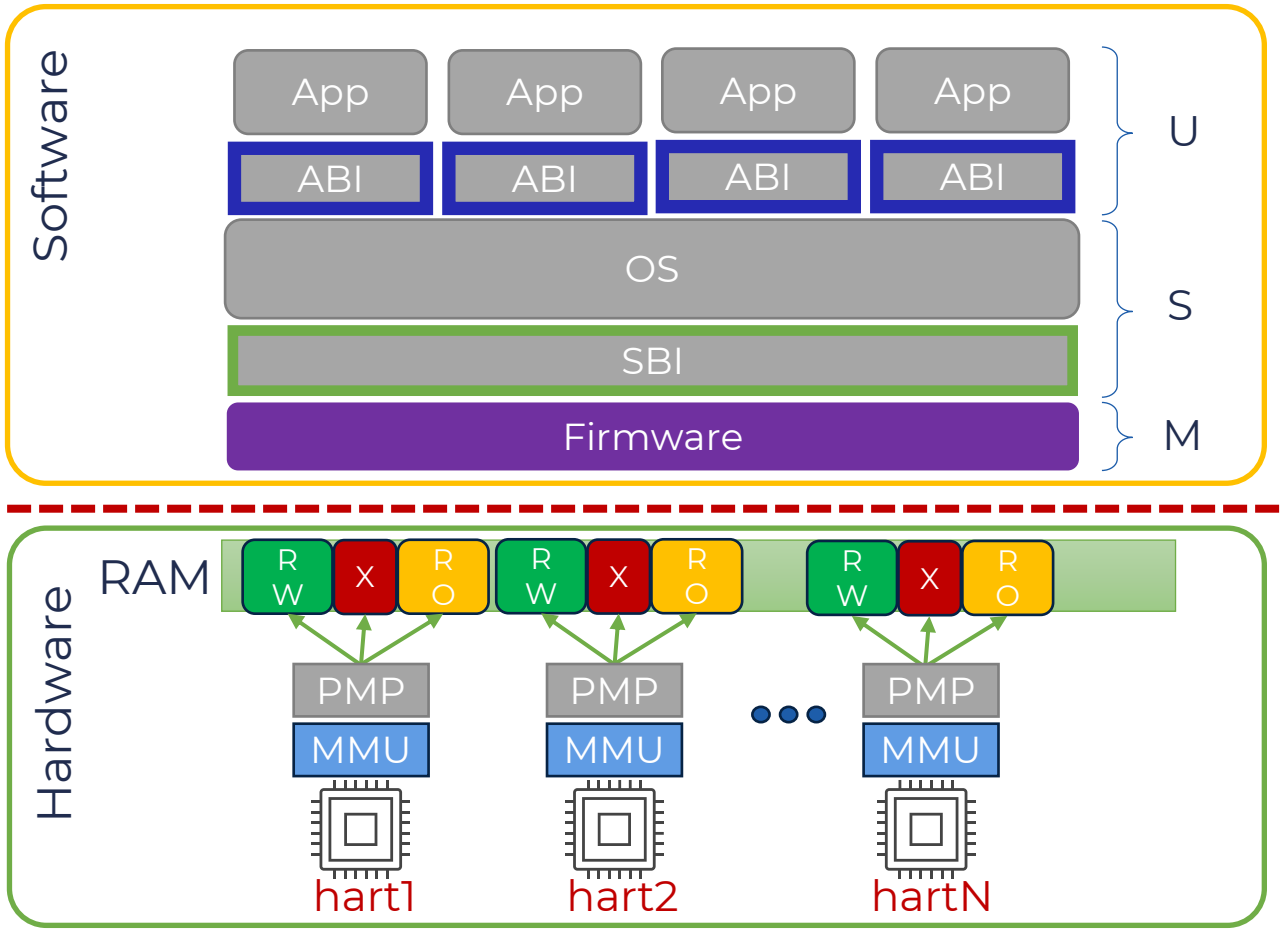




- Инструкция **LPAD** используется для обозначения законных точек перехода для инструкций вызова и косвенного перехода в коде приложения.
- Компиляторы выдают инструкцию **LPAD** в качестве первой инструкции функции, получающей адрес, а также для любых целей косвенного перехода.
- Hart отслеживает ожидаемое состояние landing pad (**ELP**), которое обновляется с помощью *indirect_call* или indirect_*jump*, чтобы проверить наличие команды **LPAD** в целевой ветке.
- Если инструкция в целевой точке не является корректной **LPAD**, то возникает ***исключение***.

© 2026 Syntacore. All trademarks, products, and brand names belong to their respective owners

Поддержка виртуальной памяти — MMU



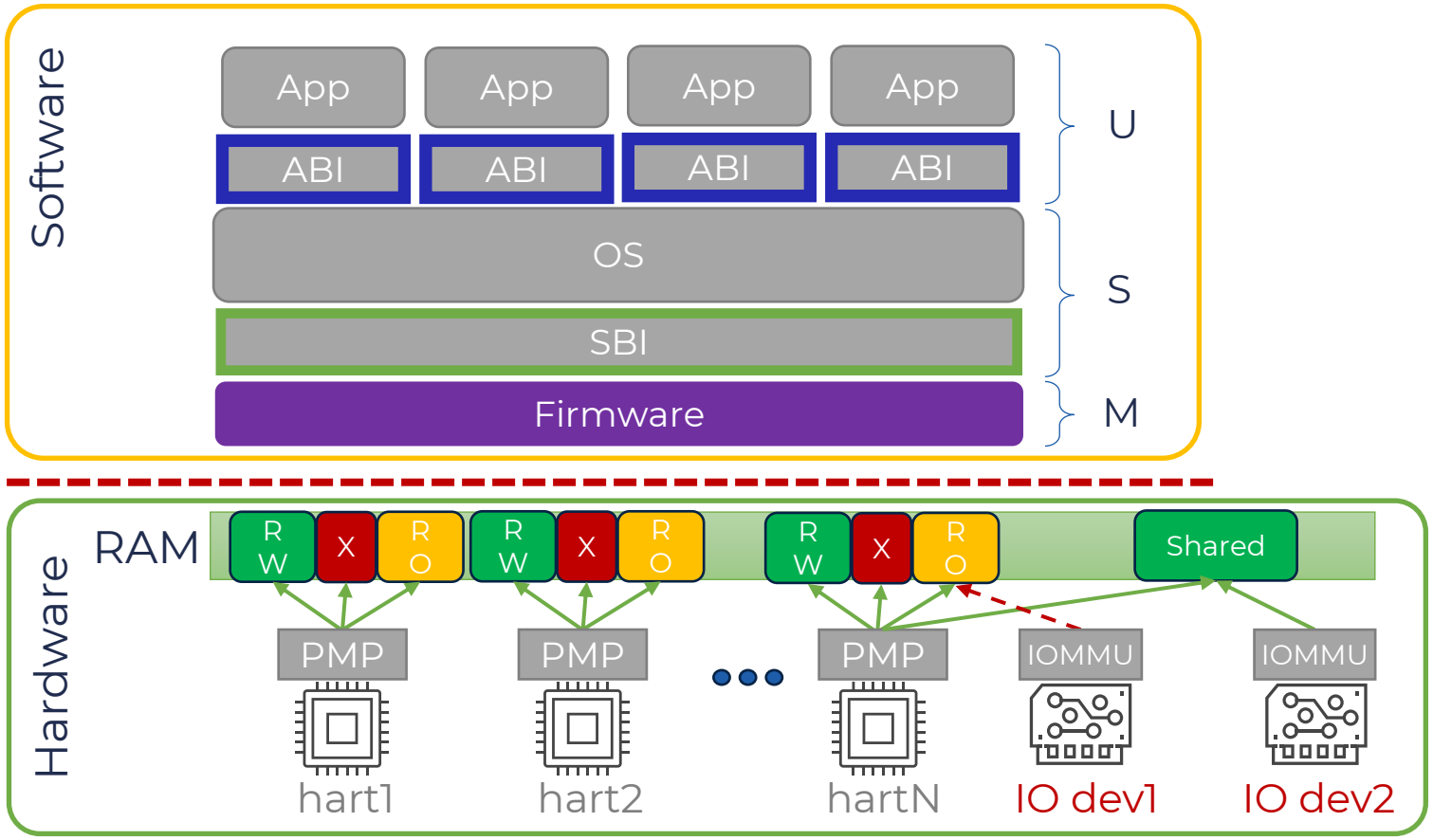
SV39 — 39bit виртуальное адресное пространство
SV48 — 48bit
SV57 — 57bit

39 = 9 + 9 + 9 +12

G — global mapping accessible in all VSpaces
U — accessible by U-mode
X/W/R — page Read/Write/Execute
V — page valid

Syntacore™ RISC-V cores and tools
© 2026 Syntacore. All trademarks, products, and brand names belong to their respective owners

Защита виртуальной памяти от злонамеренного доступа со стороны вешних устройств — IOMMU

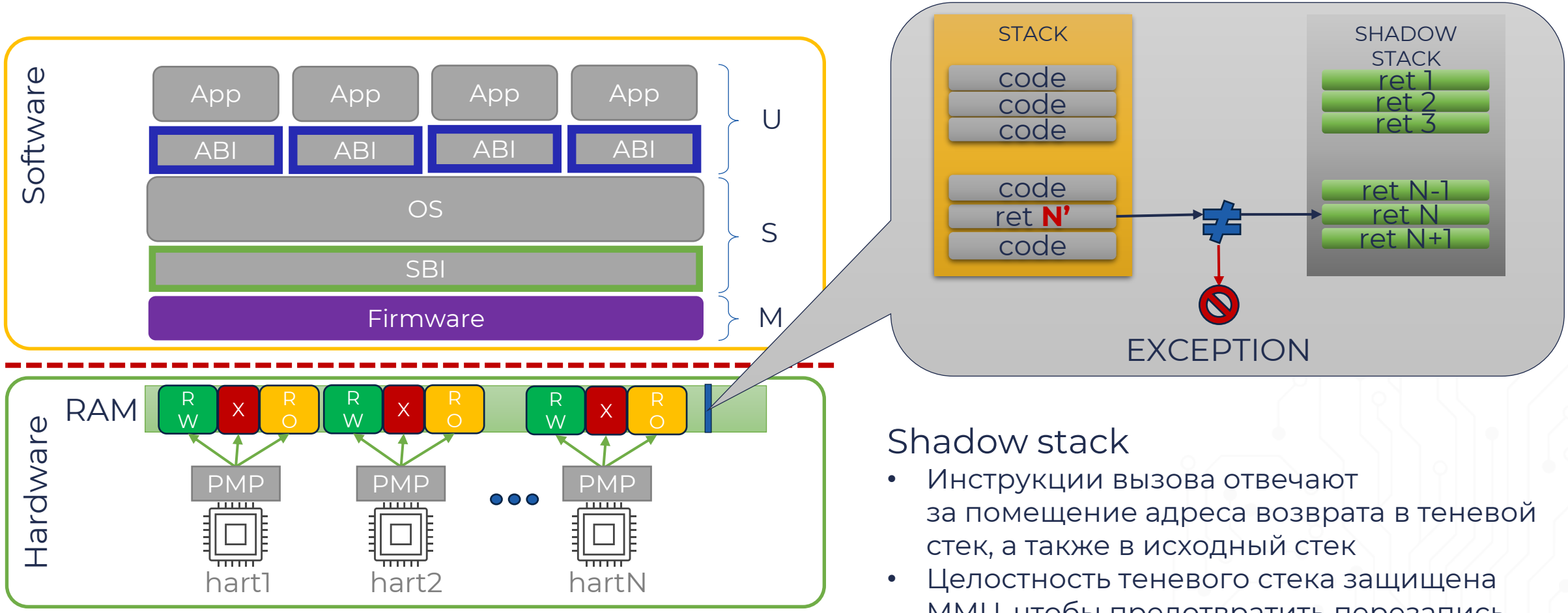


- IOMMU использует двухэтапный процесс трансляции адресов для трансляции IOVA в SPA и обеспечения защиты памяти для DMA.
- IOMMU использует те же форматы таблиц страниц, которые используются MMU hart для трансляции адресов первого и второго этапов

Syntacore™ RISC-V cores and tools

© 2026 Syntacore. All trademarks, products, and brand names belong to their respective owners

Целостность потока управления – Shadow stack



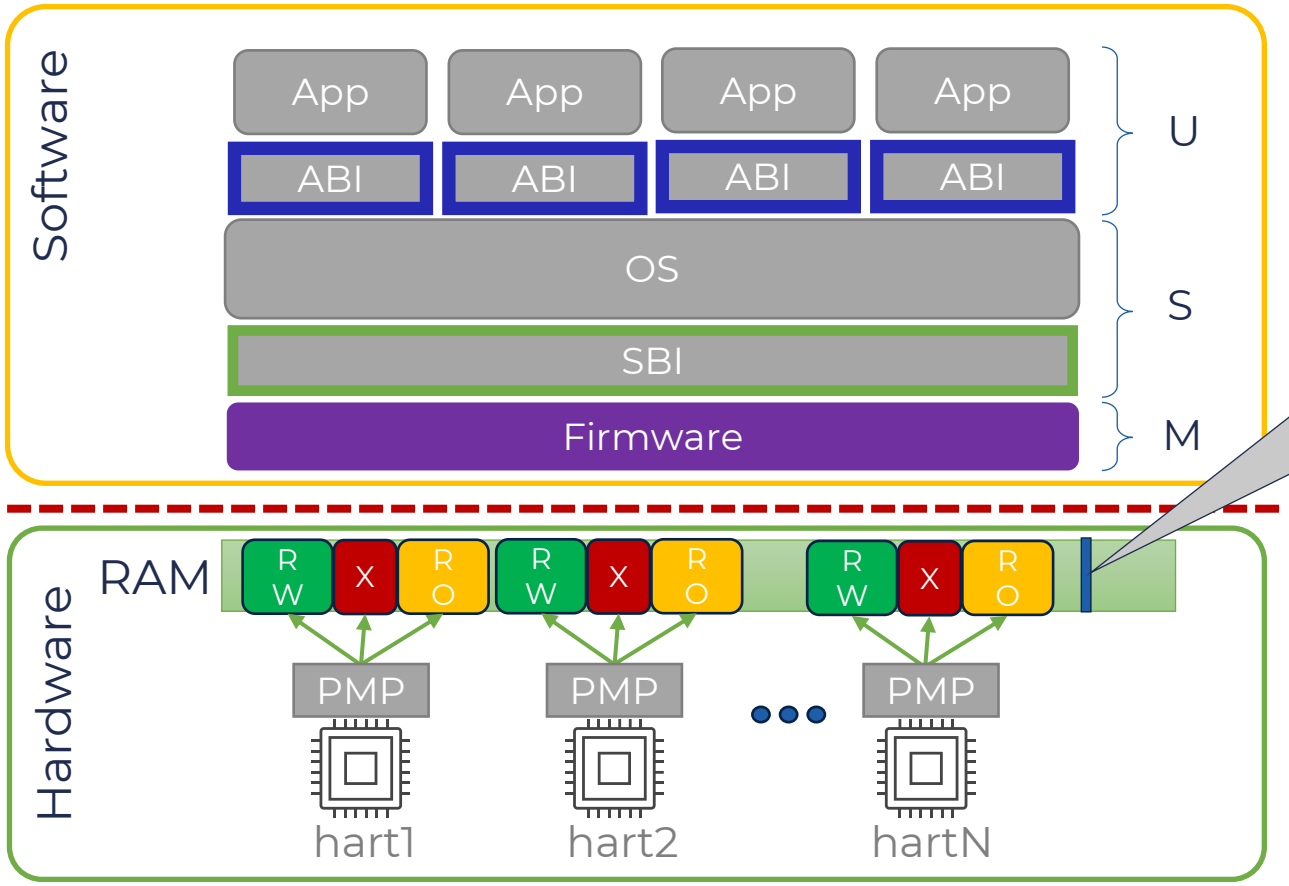
Shadow stack

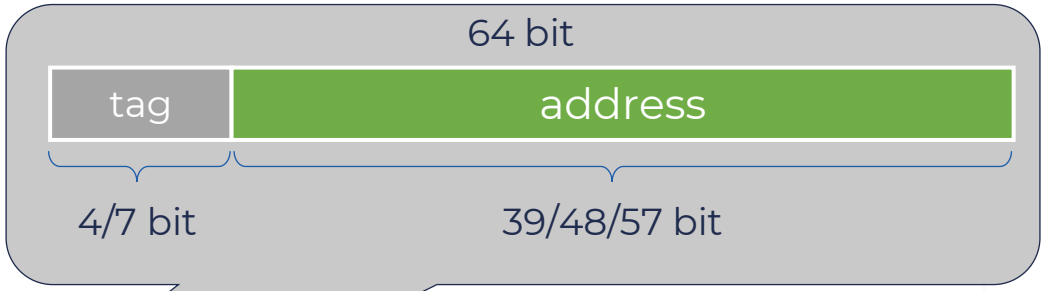
- Инструкции вызова отвечают за помещение адреса возврата в теневой стек, а также в исходный стек
- Целостность теневого стека защищена MMU, чтобы предотвратить перезапись злоумышленником находящихся в нем обратных адресов

Syntacore™ RISC-V cores and tools

© 2026 Syntacore. All trademarks, products, and brand names belong to their respective owners

RISC-V Memory tagging





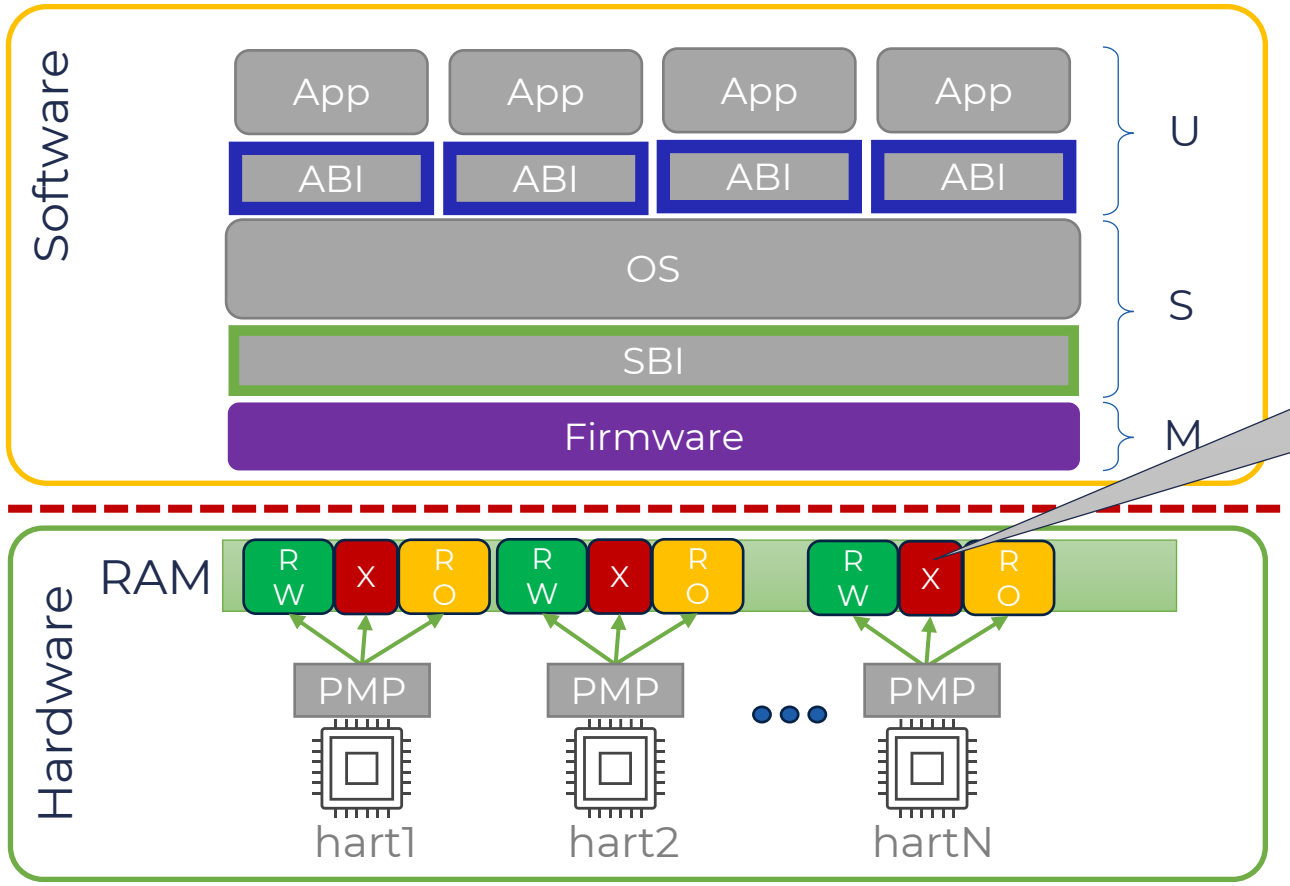
- Схема с «замком и ключом».
- Памяти присваивается тег памяти (замок).
- Каждому указателю в неиспользуемых верхних битах присваивается тег указателя (ключ).
- Каждый доступ в память — проверка валидности тега (отпирание замка).

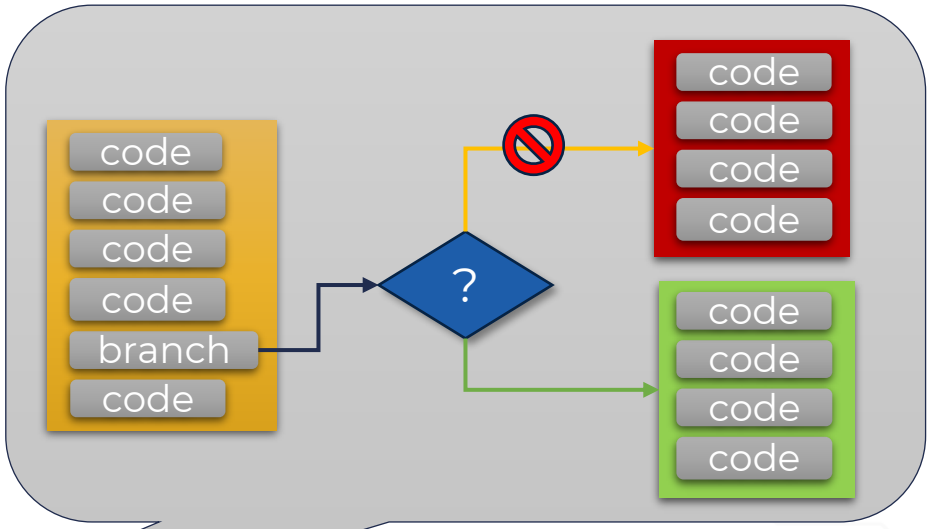
Зависит от Pointer masking, работает только для 64 bit и в виртуальной памяти, работает с zimop.

Syntacore™ RISC-V cores and tools

© 2026 Syntacore. All trademarks, products, and brand names belong to their respective owners

RISC-V Speculation barriers Zisb

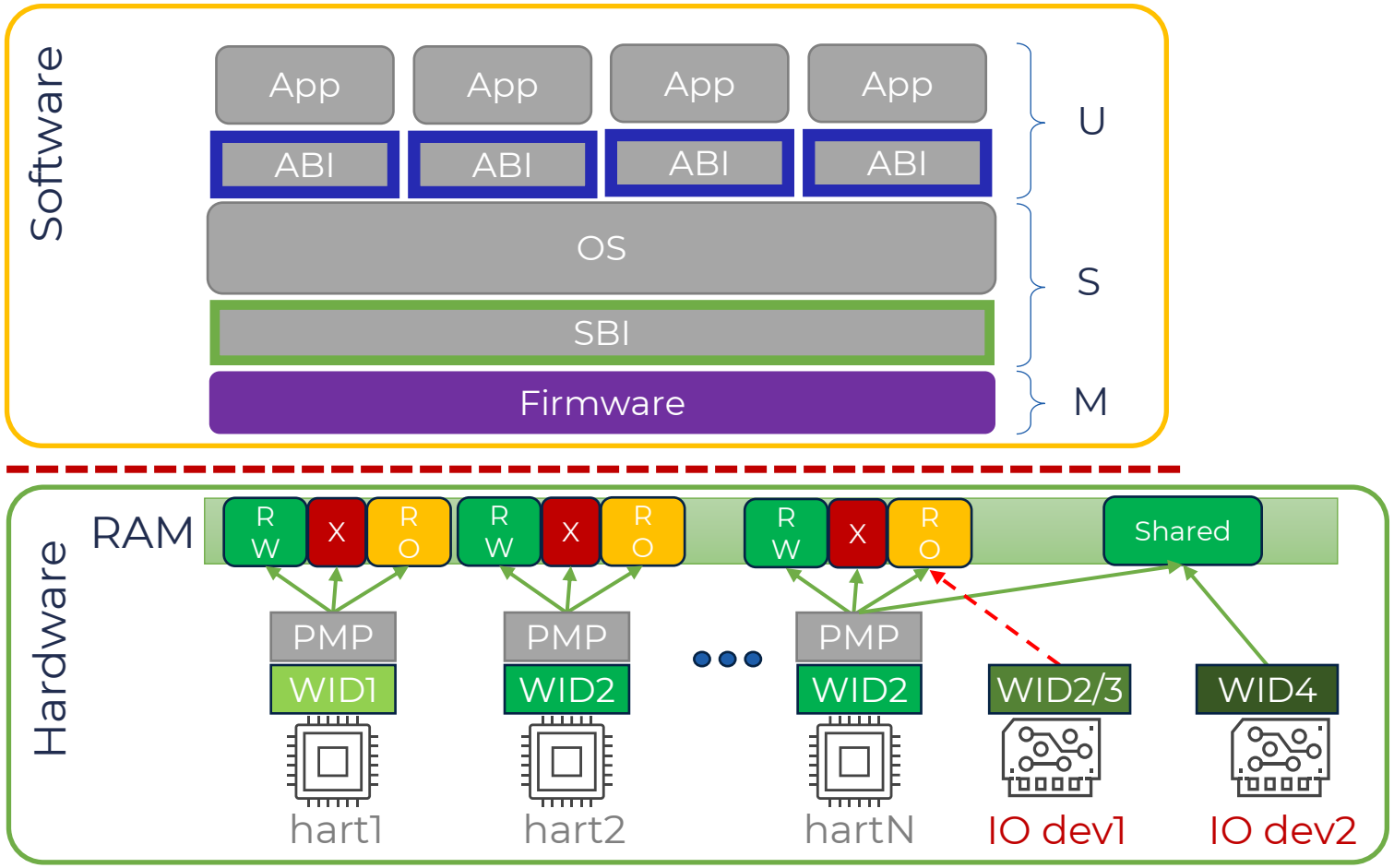




1. Позволяют разработчикам явно контролировать границы спекуляций в CPU-конвейерах.
2. Предотвращают утечки данных через побочные каналы (side channels) при транзиентном выполнении инструкций.
3. Не сбрасывают и не очищают предсказания, а дополняют существующие техники, например, маркировку предсказателей информацией о режиме привилегий.
4. Запрещают использование предсказаний, созданных в одном домене, при выполнении кода в другом домене.

© 2026 Syntacore. All trademarks, products, and brand names belong to their respective owners

RISC-V Worlds — изоляция в мирах

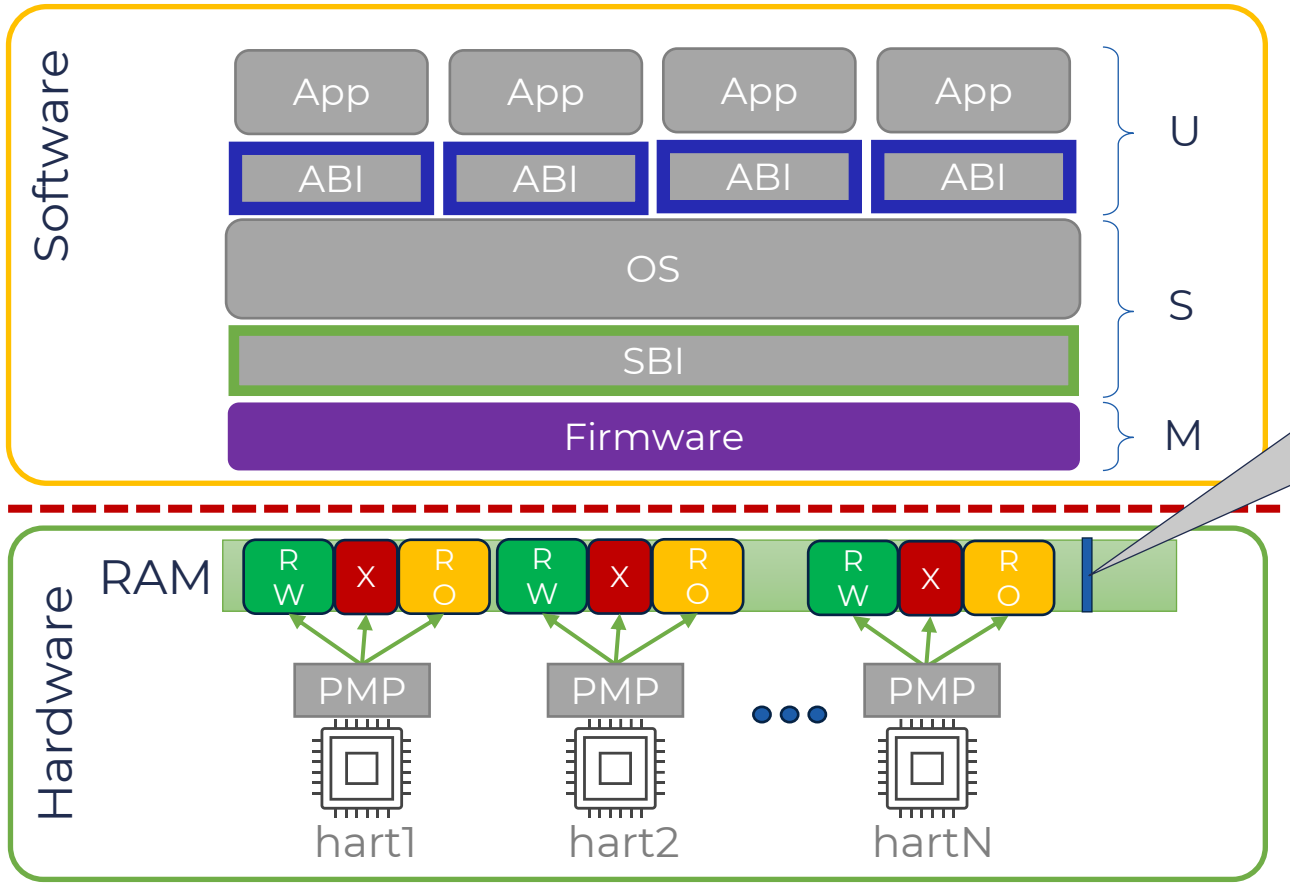


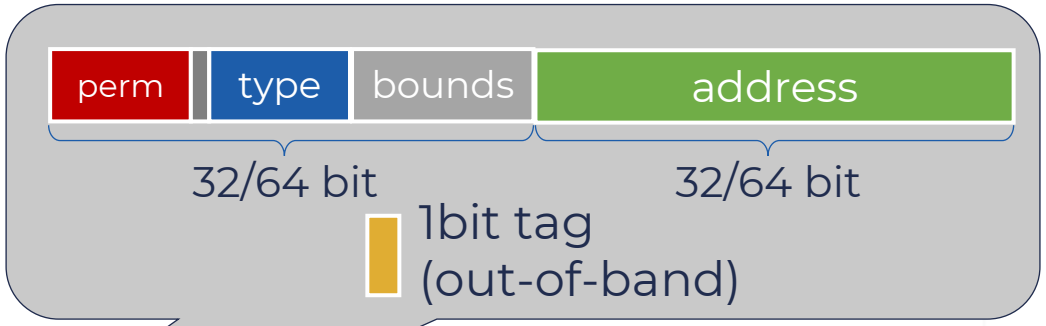
- WIDs – 2/8 штук достаточно
- Распределение контекстов агентов и ресурсов по мирам выполняется до или во время сброса/загрузки
- Распределение по мирам не меняется динамически во время работы системы.

Syntacore™ RISC-V cores and tools

© 2026 Syntacore. All trademarks, products, and brand names belong to their respective owners

CHERI — Capability Hardware Enhanced RISC-V Instructions





- Дополнительные 32/64 бита для адреса с разрешениями, типом объекта и границами.
- Любая capability с **tag** != 1 не может быть разыменована — она инвалидна

Основа безопасности метода:

- **Provenance (Происхождение)** — *capability* можно создать только из уже существующей *capability*
- **Monotonicity (Монотонность)** — невозможно создать *capability* с доступами превосходящими родительскую *capability*

Syntacore™ RISC-V cores and tools
© 2026 Syntacore. All trademarks, products, and brand names belong to their respective owners

Факторы, влияющие на применимость аппаратных функций

Что влияет на применимость аппаратных функций безопасности:

- Сложность реализации в железе — размер блока в kGates.
  - Аппаратные блоки могут быть очень большими – рост размера кристалла – цена выше.
- Поддержка аппаратных функций в софте
  - Некоторые аппаратные функции требуют поддержку в компиляторах, библиотеках, загрузчиках.
- Влияние на производительность системы —
  - классический компромисс **скорость-безопасность**.

© 2026 Syntacore. All trademarks, products, and brand names belong to their respective owners

Заключение

- RISC-V архитектура подходит методологии применения микроконтроллеров.
- RISC-V уже содержит аппаратную поддержку функциональности, покрываемой микроконтроллерами.
- RISC-V предлагает аппаратную защиту информации и продолжает активно развиваться в этой области.
- RISC-V микроконтроллеры уже активно представлены на рынке.
- Рыночная доля аппаратуры на базе RISC-V будет расти и дальше.

Спасибо за внимание!

Вопросы?