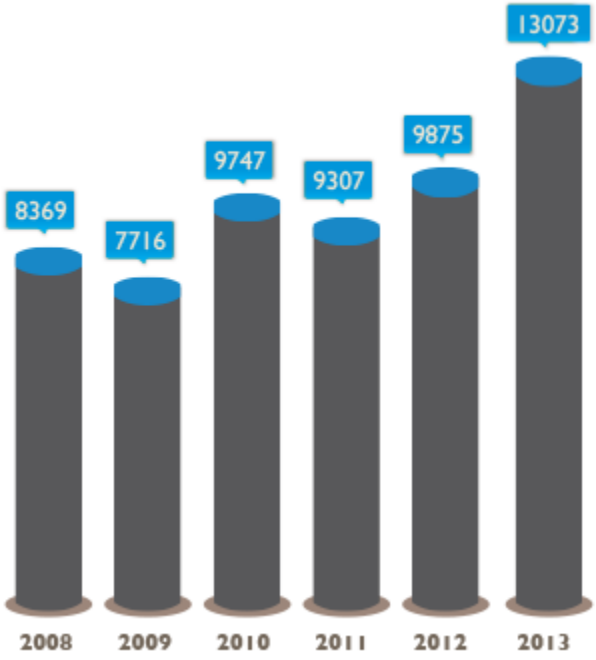
БЕЗОПАСНЫЙ ПРОЦЕССОР КАК СПОСОБ РЕШЕНИЯ ПРОБЛЕМЫ УЯЗВИМОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Д.П. Зегжда, Д.А. Москвин, А.В. Никольский

Проблема уязвимостей ПО



Количество уязвимостей

Использование уязвимостей по векторам атак

из Интернета | **из локальной сети** | **с локального компьютера**

**по данным secunia.com*

Подходы к устранению уязвимостей ПО

Обновления кода

- Высокая надежность
- Неотменяемость

- Низкая оперативность
- Невозможность исправить все ошибки

Устранение причин

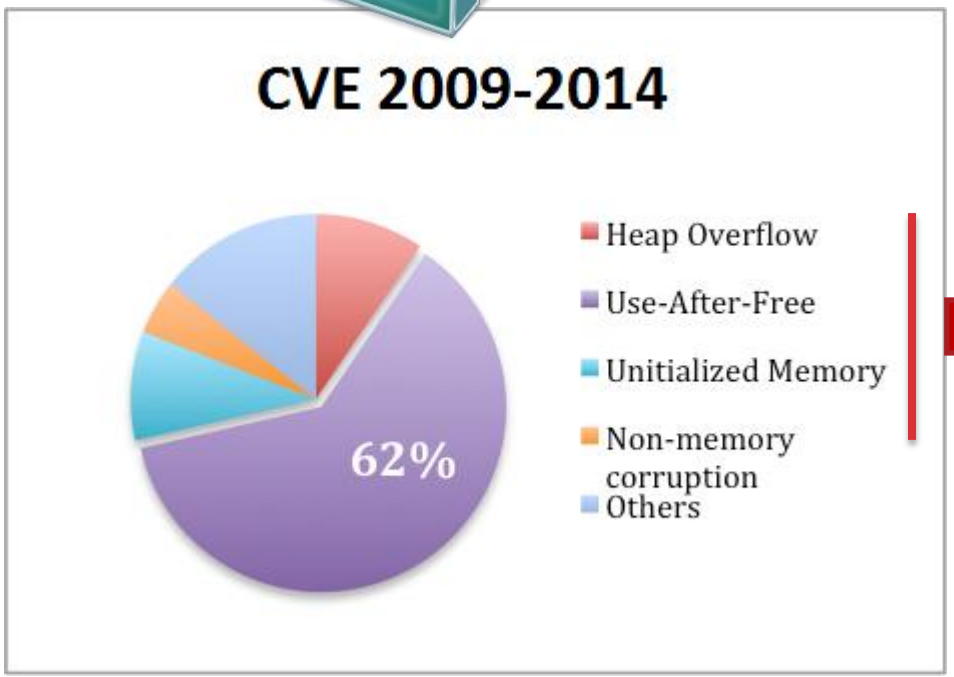
Использование дополнительных механизмов и средств защиты

- Оперативность
- Защита от неизвестных уязвимостей

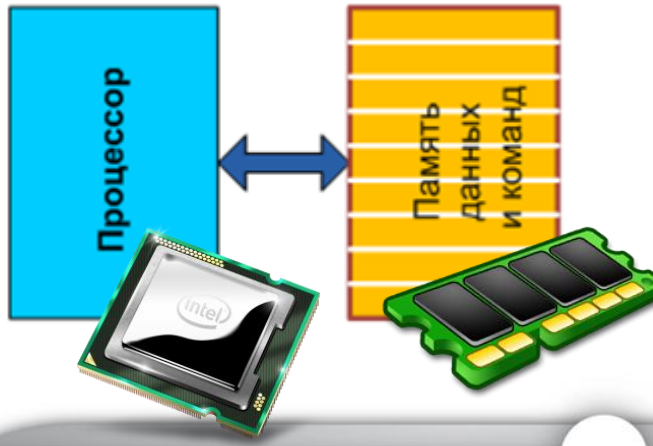
- Необходимость постоянного контроля
- Возможные ошибки

Предотвращение последствий

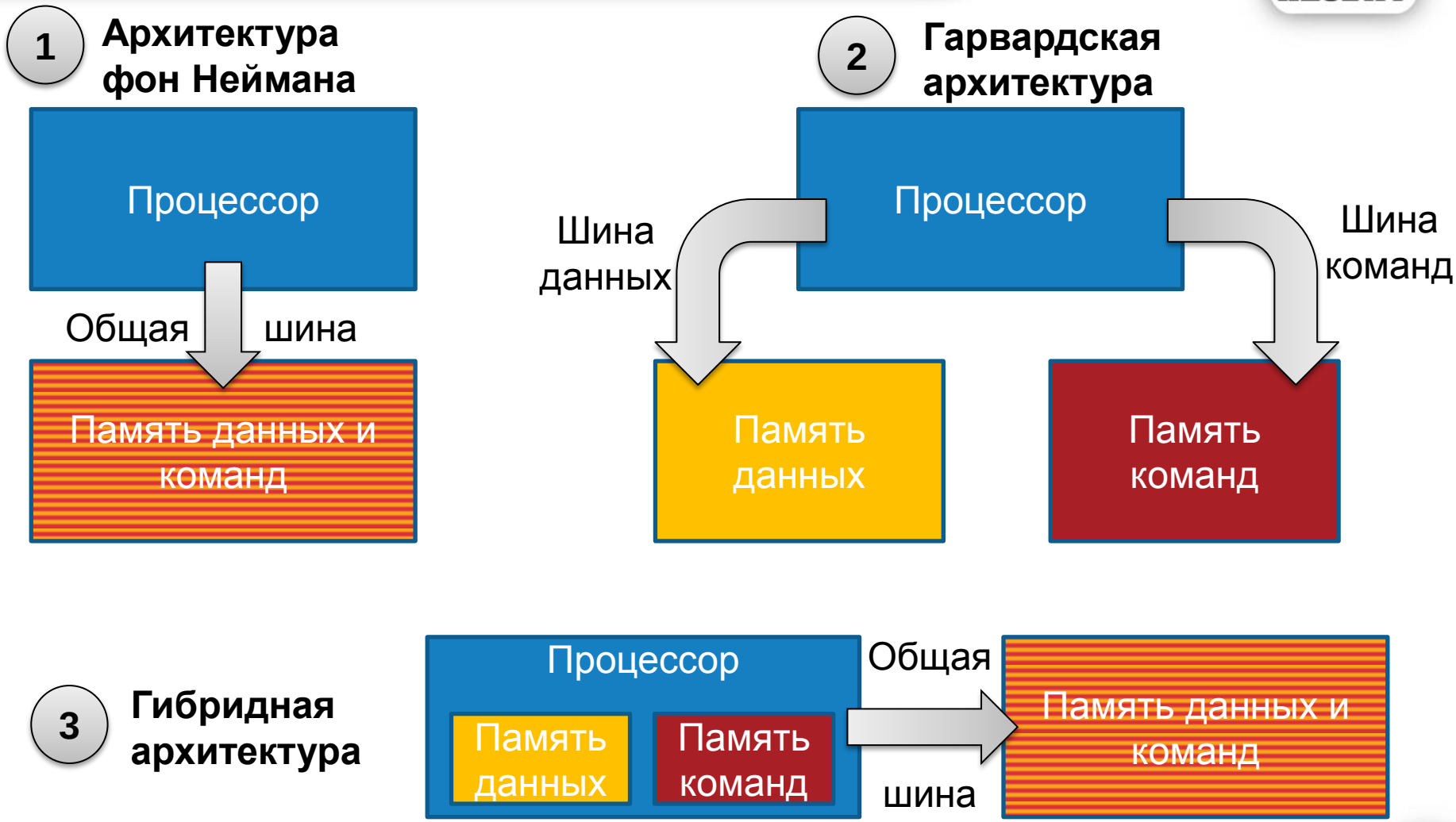
Уязвимости как следствие недостатков архитектуры ЭВМ



Архитектура фон Неймана



Архитектура фон Неймана VS Гарвардская архитектура



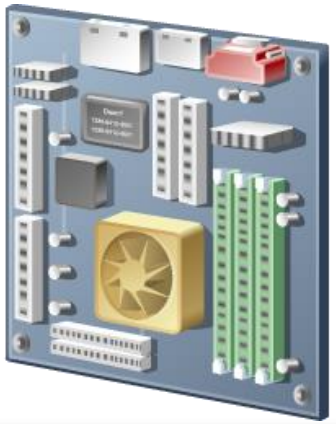
Архитектура фон Неймана VS Гарвардская архитектура (2)

		**Характеристика**
		Производительность
		Безопасность
		Стоимость
		Поддержка современных технологий разработки приложений

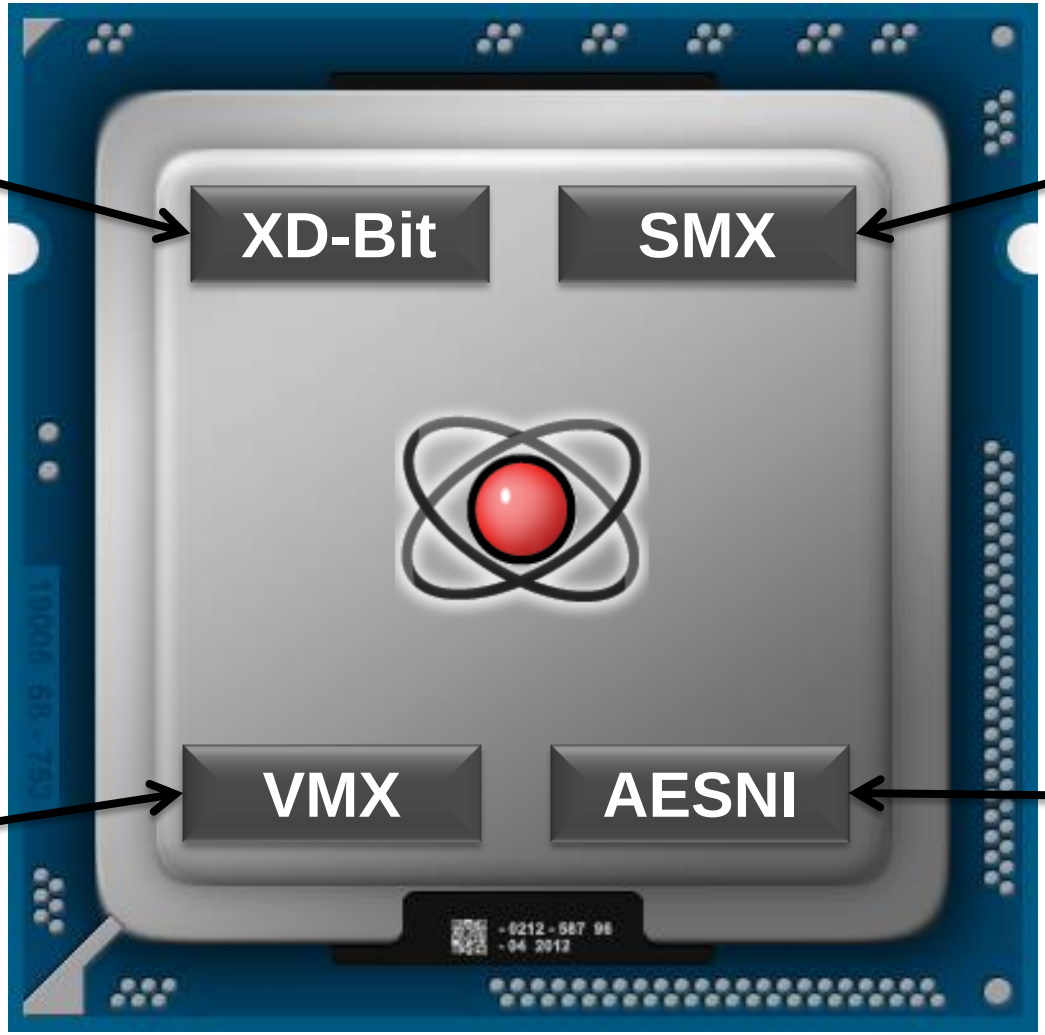
Аппаратные технологии защиты от уязвимостей ПО

Предотвращение выполнения данных (Data Execution Prevention, DEP)

Технология доверенной загрузки (Trusted Execution Technology, TXT)

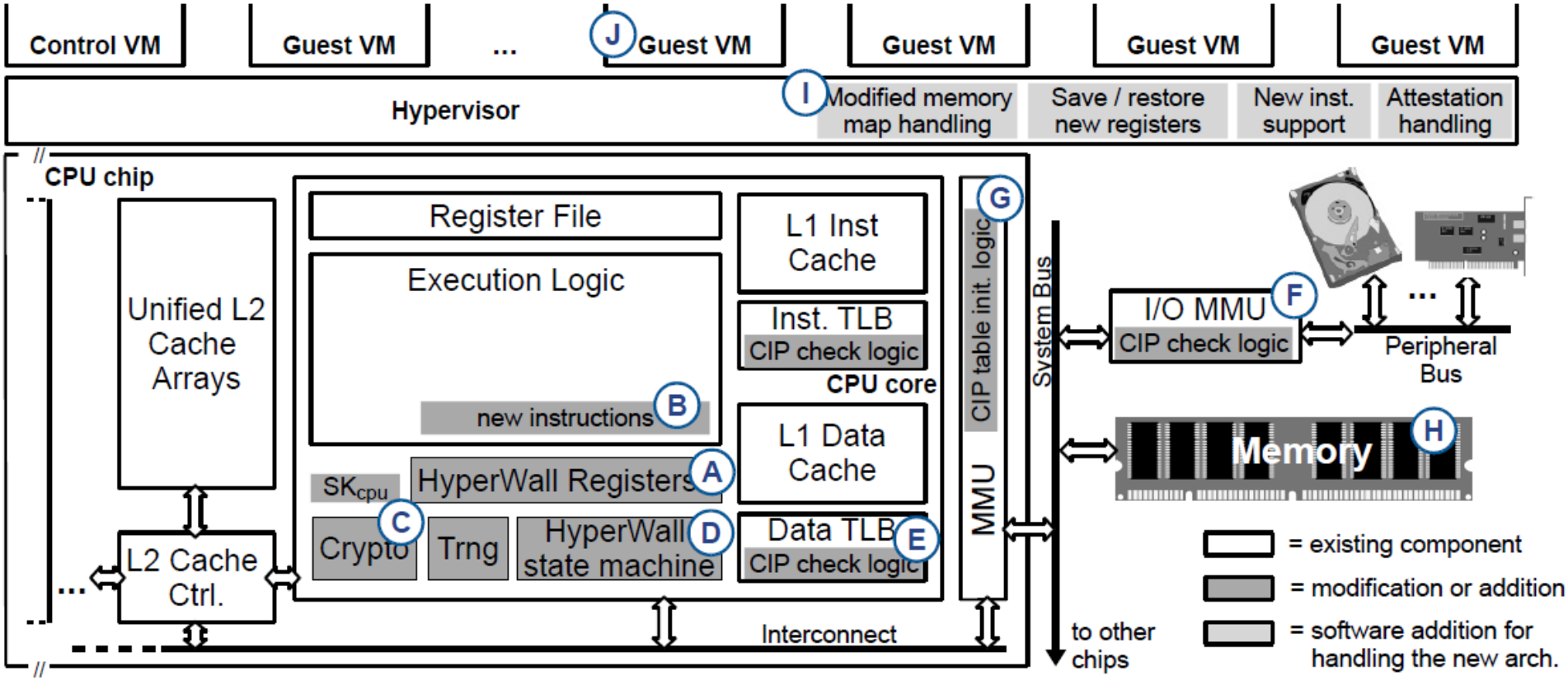


Расширения x86-процессоров



Независимые от ПО аппаратные технологии защиты

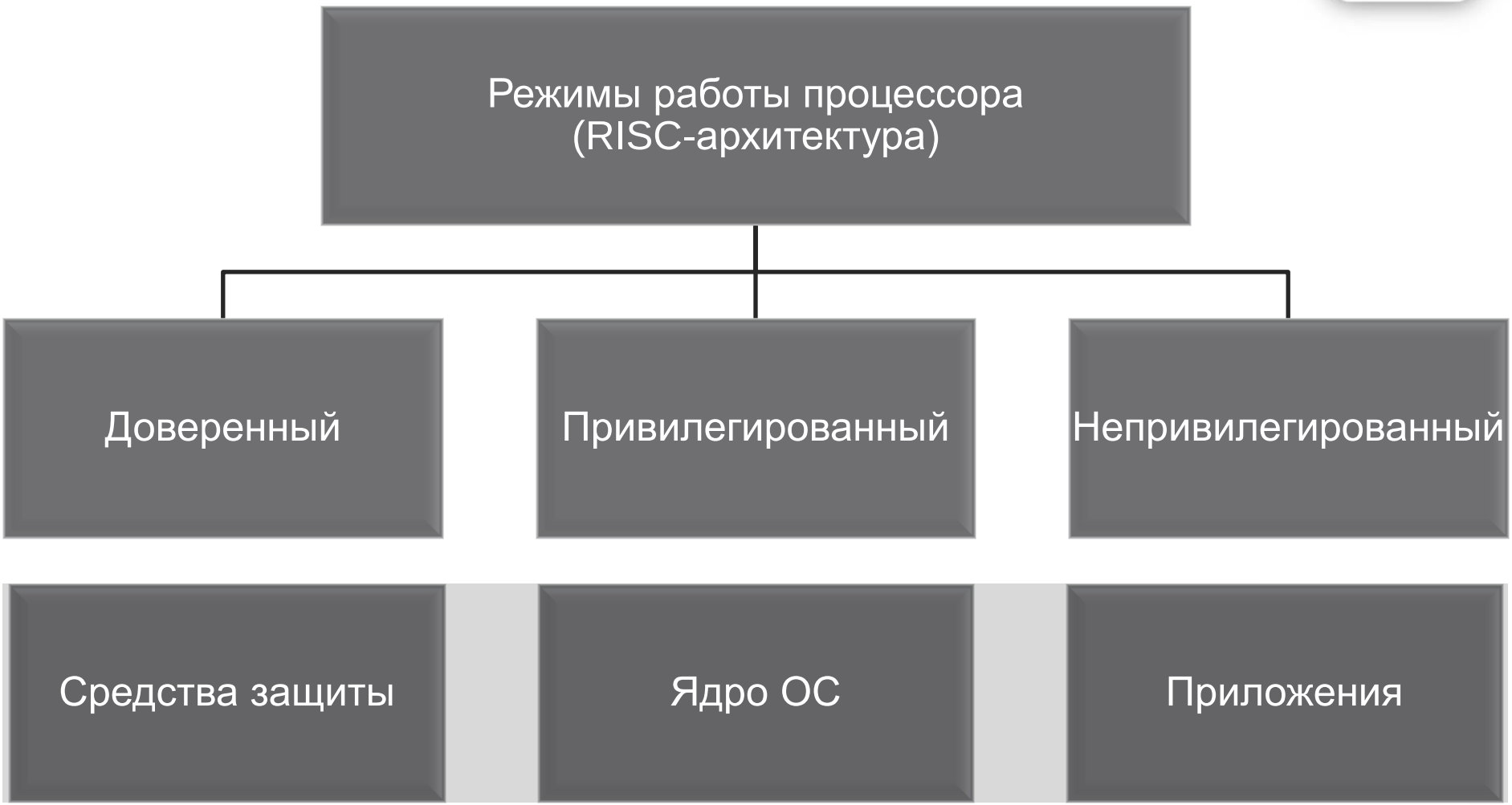
HyperWall



Российские процессоры

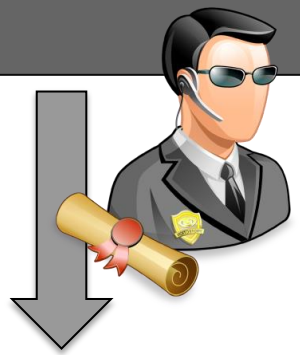
Процессор	Baikal M (M/S)	Эльбрус-8С
Архитектура	ARM (Cortex A-57)	Эльбрус (x86-совместима)
Такт. частота	2 ГГц	1,3 ГГц
Кол-во ядер	8	8
Техн. процесс	28 нм	28 нм
ОС	Мод. Linux	Эльбрус (мод. Linux)
Безопасность	???	Поддержка режима защищённых вычислений с особым аппаратным контролем целостности структуры памяти

Требования к безопасному процессору (1)



Требования к безопасному процессору (2)

Доверенный режим



Привилегированный режим

Непривилегированный режим

Гарвардская архитектура

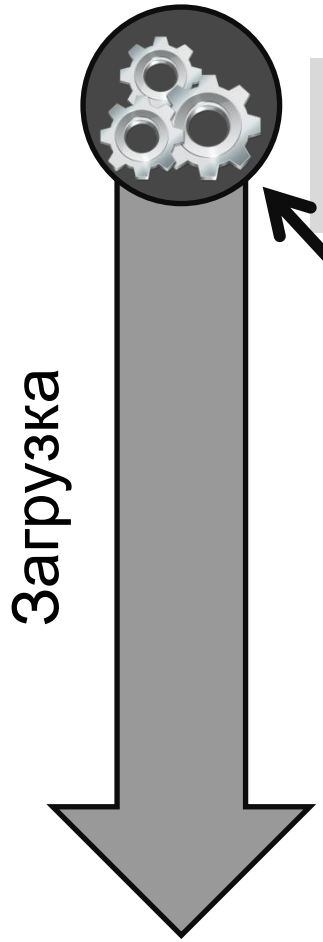
Архитектура фон Неймана

Требования к безопасному процессору (2)

Доверенный режим	Привилегированный режим	Непривилегированный режим

Гарвардская архитектура	Архитектура фон Неймана

Требования к безопасному процессору (3)



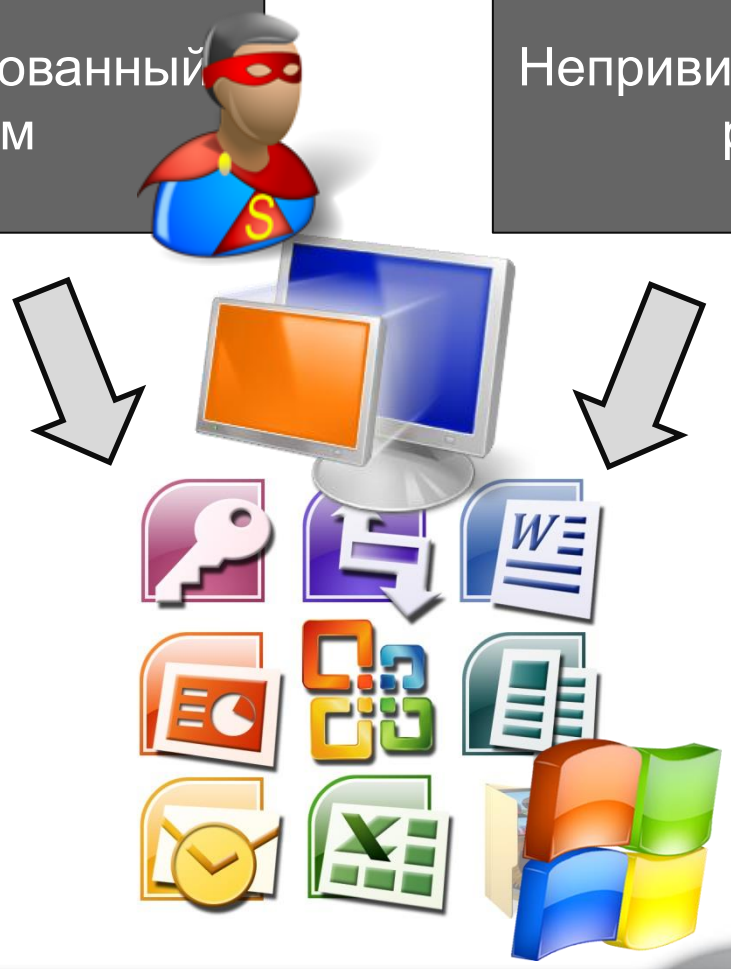
- первая инструкция –
  в защищенном режиме

Криптопроцессор

Требования к безопасному процессору (4)

Привилегированный режим

Непривилегированный режим



Реализуемость требований

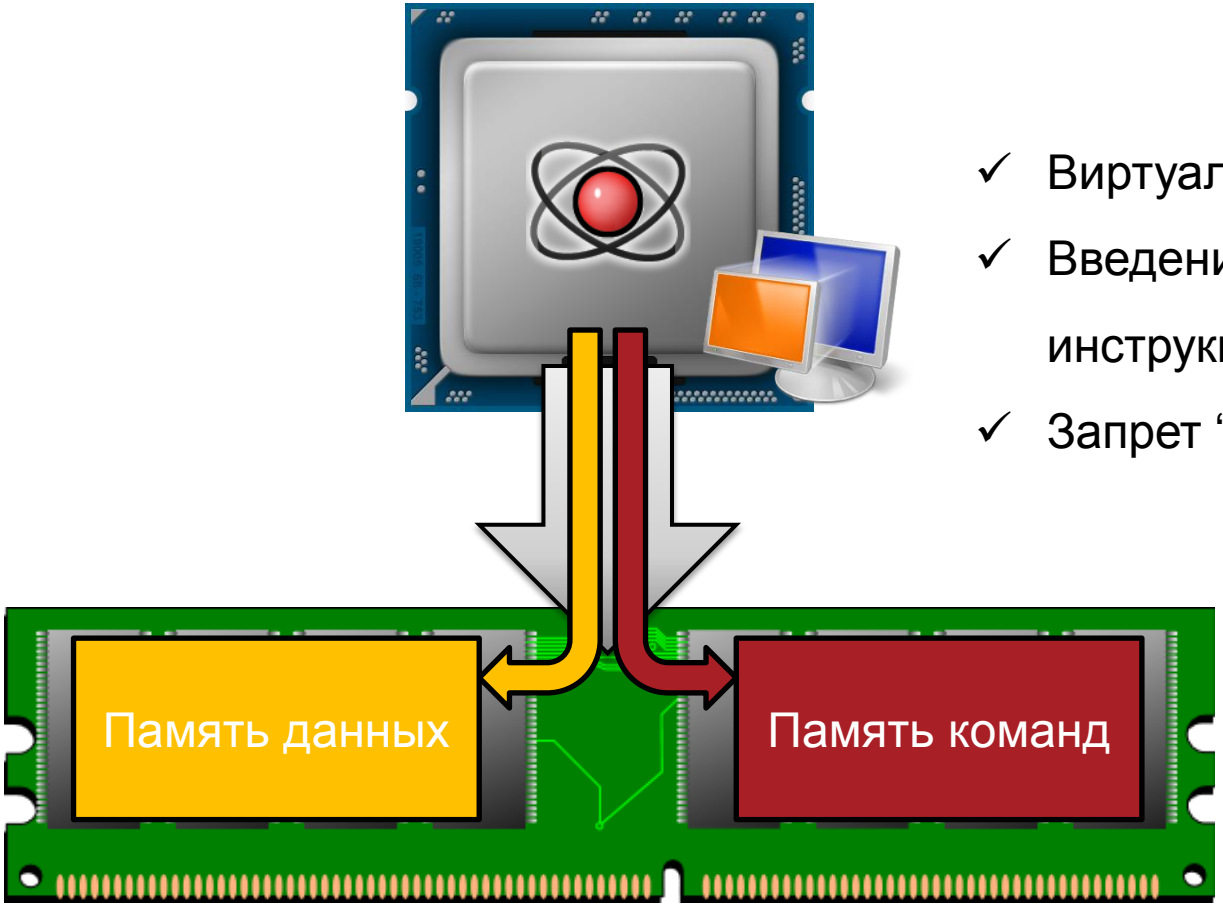
В процессорах ARC поддерживается Гарвардская архитектура

В процессорах Intel — аппаратная виртуализация

В ARM —два режима и сокращенный набор команд

Требования непротиворечивы

Применение виртуализации



- ✓ Виртуализация доступа к памяти
- ✓ Введение нового набора инструкций
- ✓ Запрет “лишних” режимов


НОВЫЕ БЕЗОПАСНЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ
НЕОБИТ