Переход на доверенные ПАК в КИИ с учётом опыта построения аппаратно-программной платформы Эльбрус

Трушкин Константин Александрович

ЧТО ТАКОЕ ЭЛЬБРУС?

Инженерная школа С.А. Лебедева

Непрерывная традиция

Технологический суверенитет без компромиссов

Ведущие специалисты по микроэлектронике в России

Высокая экономическая эффективность разработки

АО «МЦСТ» — кузница кадров для российской микроэлектроники



>400 ЧЕЛОВЕК В ШТАТЕ

33 ГОДА НА РЫНКЕ

СИСТЕМООБРАЗУЮЩЕЕ ПРЕДПРИЯТИЕ

Идеальный ПАК для КИИ

- **Функционально надёжный, отказоустойчивый**
- **Информационно защищённый (если требуется)**
- **С российским жизненным циклом (как минимум, с длительной поддержкой)**
  - **Разработка, происхождение основных технологий**
  - **Производство ключевой ЭКБ**
  - **Производство изделия в целом**
- **С достаточной (под спецзадачу) производительностью**
- **Масштабируемый (по мере роста нагрузки)**
- **Удобный для поддержки и развития (программистам, администраторам, …)**
- **С высокой экономической эффективностью**
- **С уникальными/конкурентными свойствами, с экспортным потенциалом**

(ПАК) – комплекс радиоэлектронной продукции (РЭП) и программного обеспечения (ПО), работающих совместно для выполнения одной или нескольких **специальных задач**, функционально-технические характеристики которого определяются исключительно совокупностью ПО и РЭП и не могут быть реализованы при их разделении

Терминология согласно ТК167

- **Доверенность** – это документированное (гарантированное, подтвержденное) **свойство** изделия соответствовать установленным требованиям **функциональности (работоспособности, надежности, стойкости к условиям эксплуатации) и безопасности (функциональной, технологической и информационной)**
- ***Доверенность … обеспечивается*** *достоверностью, информативностью и полнотой* ***информации*** *об изделии, полученных из рационального (т.е. необходимого и достаточного) сочетания данных о действующих системах менеджмента качества и информационной безопасности* ***в ходе его стадий жизненного цикла и/или результатах тестирования и испытаний*** *изделий.*
- **Функциональная безопасность (ФБ)** – состояние защищенности изделия от угроз нанесения вреда жизни и здоровью персонала, а также значимого* ущерба объектам КИИ вследствие отказа изделия.
- **Технологическая безопасность (ТБ)** – состояние защищенности изделия от угроз нарушения процессов его жизненного цикла
- **Информационная безопасность (ИБ)** – состояние защищенности изделия от угроз нарушения функциональности вследствие компьютерных атак

Где мы находися сейчас?

- Основа существующих ПАК – зарубежные процессоры (x86 в основной части)
- Значительная доля ОС в ПАК – Windows

- Понятие «Доверенный ПАК» введено Постановлением Правительства №1912 от 14.11.2023 г.
- **Требования к аппаратуре:** ППП№719 от 17 июля 2015 г. (Реестр Минпромторга)
- **Требования к ПО:** ППП№1236 от 16 ноября 2015 г. (Реестр Минцифры)
- **Требования к ИБ – при необходимости, наличие сертификата ФСТЭК или ФСБ,** решаются наложенными средствами и программными СЗИ (сертифицированными по требованиям ФСТЭК), которые опираются на аппаратные свойства недоверенных процессоров.
- **Требования к ФБ для ДПАК** отсутствуют, есть ведомственные требования (например, в РЖД или Росатоме)

Основа доверенности находится в АПП

Аппаратно-программная платформа (АПП)

- Архитектура системы команд процессора
- Логический дизайн ядра процессора
- Компиляторы
- Операционные системы

Логический и физический дизайн процессора

Конструкция СВТ и т.п.



ПРОЦЕССОРЫ ЭЛЬБРУС

4 поколения микропроцессоров за 10 лет



Эльбрус-4С
65нм

3 поколение

50 GFLOPS
4 ядра
0.75 ГГц

2013



Эльбрус-8С
28нм

4 поколение

250 GFLOPS
8 ядер
1.3 ГГц

2015



Эльбрус-8СВ
28нм

5 поколение

580 GFLOPS
8 ядер
1.5 ГГц

2018



Эльбрус-16С
16нм

6 поколение

1.5 TFLOPS
16 ядер
2.0 ГГц

2021



Эльбрус-2С3
16нм

6 поколение

0,18 TFLOPS
2 ядра
2.0 ГГц
3D GPU+codec

2022



Эльбрус-12С
16нм

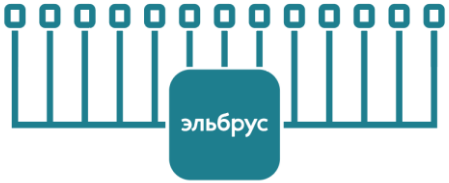
6 поколение

1 ,1 TFLOPS
12 ядер
2.0 ГГц

2022

от серверов и супер-ЭВМ до ноутбуков и встраиваемых ЭВМ

ОСОБЕННОСТИ АРХИТЕКТУРЫ ЭЛЬБРУС



ПАРАЛЛЕЛЬНАЯ ВЫСОКОПРОИЗВОДИТЕЛЬНАЯ АРХИТЕКТУРА

до 25 ОДНО ЯДРО ВЫПОЛНЯЕТ ДО 25 ОПЕРАЦИЙ В ТАКТ



Secure by design

ТЕХНОЛОГИЯ БЕЗОПАСНЫХ ВЫЧИСЛЕНИЙ

Превосходит требования CISA

>70% ЗАЩИЩАЕТ ОТ >70% АТАК НА ДАННЫЕ В ПАМЯТИ



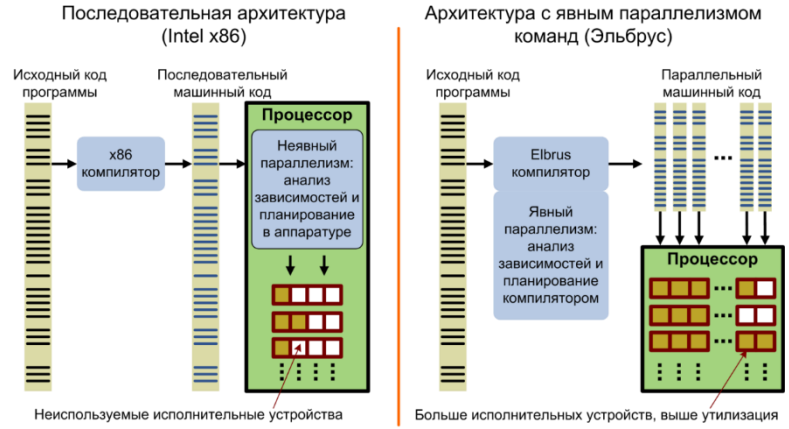
ДВОИЧНАЯ СОВМЕСТИМОСТЬ С X86, X86-64

>80% КПД WINDOWS ВНУТРИ ВИРТУАЛЬНОЙ МАШИНЫ >80%

Принципы архитектур: RISC vs. Эльбрус





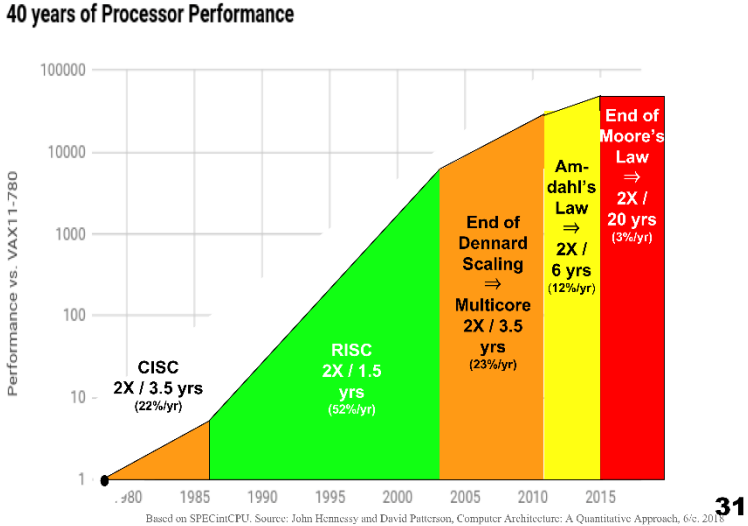


Перенос части работы по распараллеливанию на компиляцию

Достижение большего параллелизма при меньшей мощности

RISC-V

End of Growth of Performance?



Процессоры RISC подошли к пределу
У Эльбруса есть шанс преодолеть его

Технология безопасных вычислений (ТБВ)

- Защита от ошибок программиста:
  - неинициализированные данные
  - выход за границы объектов

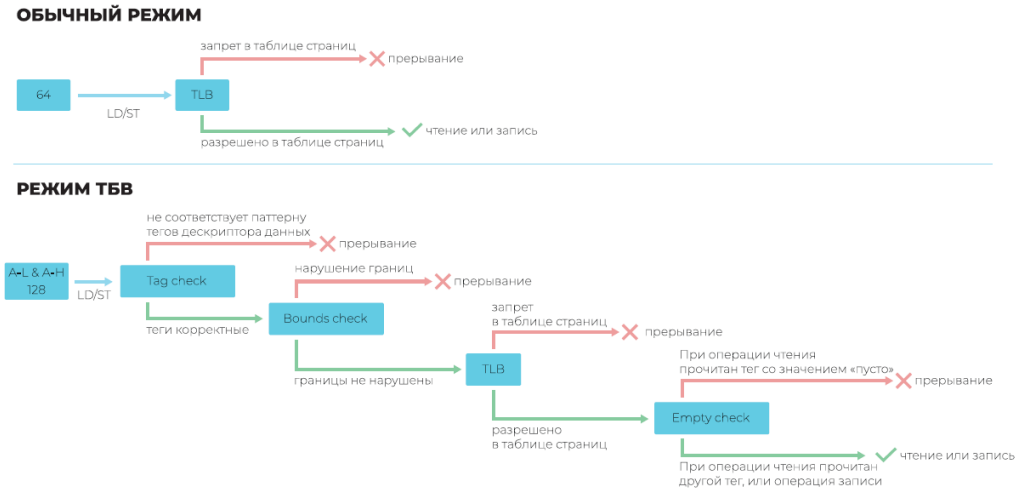
    (защита от Spectre!)
  - обращение к освобождённой памяти
- Защита от эксплуатации ошибок (уязвимостией) злоумышленником:
  - Переполнение буфера (buffer overflow)
  - use-after-free

  (они – источник >70% атак по данным ARM)
- Изоляция недоверенного модуля / защита от утечек информации через библиотеки
  - межмодульная защита
- Рост производительности труда программистов в несколько раз

ИСПОЛЬЗОВАНИЕ ДЕСКРИПТОРОВ ВМЕСТО УКАЗАТЕЛЕЙ



АППАРАТНЫЙ КОНТРОЛЬ ОБРАЩЕНИЙ ЧЕРЕЗ ДЕСКРИПТОРЫ










National Cyber Security Centre
a part of GCHQ

Australian Government
Australian Signals Directorate
ACSC Australian Cyber Security Centre

Communications Security Establishment
Canadian Centre for Cyber Security
Centre de la sécurité des télécommunications
Centre canadien pour la cybersécurité

Federal Office for Information Security

National Cyber Security Centre
Ministry of Justice and Security
certnz
National Cyber Security Centre
PART OF THE GCSB

Изменение баланса рисков кибербезопасности: принципы и подходы для обеспечения безопасности на этапе разработки и безопасности по умолчанию

Публикация: 13 апреля 2023

В США рекомендуется:

переходить на безопасные языки
или использовать технологии CHERI – прямой аналог ТБВ Эльбрус

It is possible that Astra Linux developers have fewer opportunities for a wider base of individuals to test and secure their code. Those could be areas for the United States and its allies to press the advantage in cyberspace.

https://www.cfr.org/blog/russias-becoming-more-digitally-isolated-and-dependent-china

Эльбрус-2С3: процессор для резервного контура

- Система на кристалле
- Производительность - до 192/96 Gflops;
- Количество ядер – 2, архитектура Эльбрус v6
- Тактовая частота – 2 ГГц;
- ОЗУ – DDR4-3200, 2 канала
- PCI-Ex. 3.0 x 16
- Встроенное видео с 3D ускорением, video codec
- Потребляемая мощность 10-25 Вт;
- Технология – 16 нм;

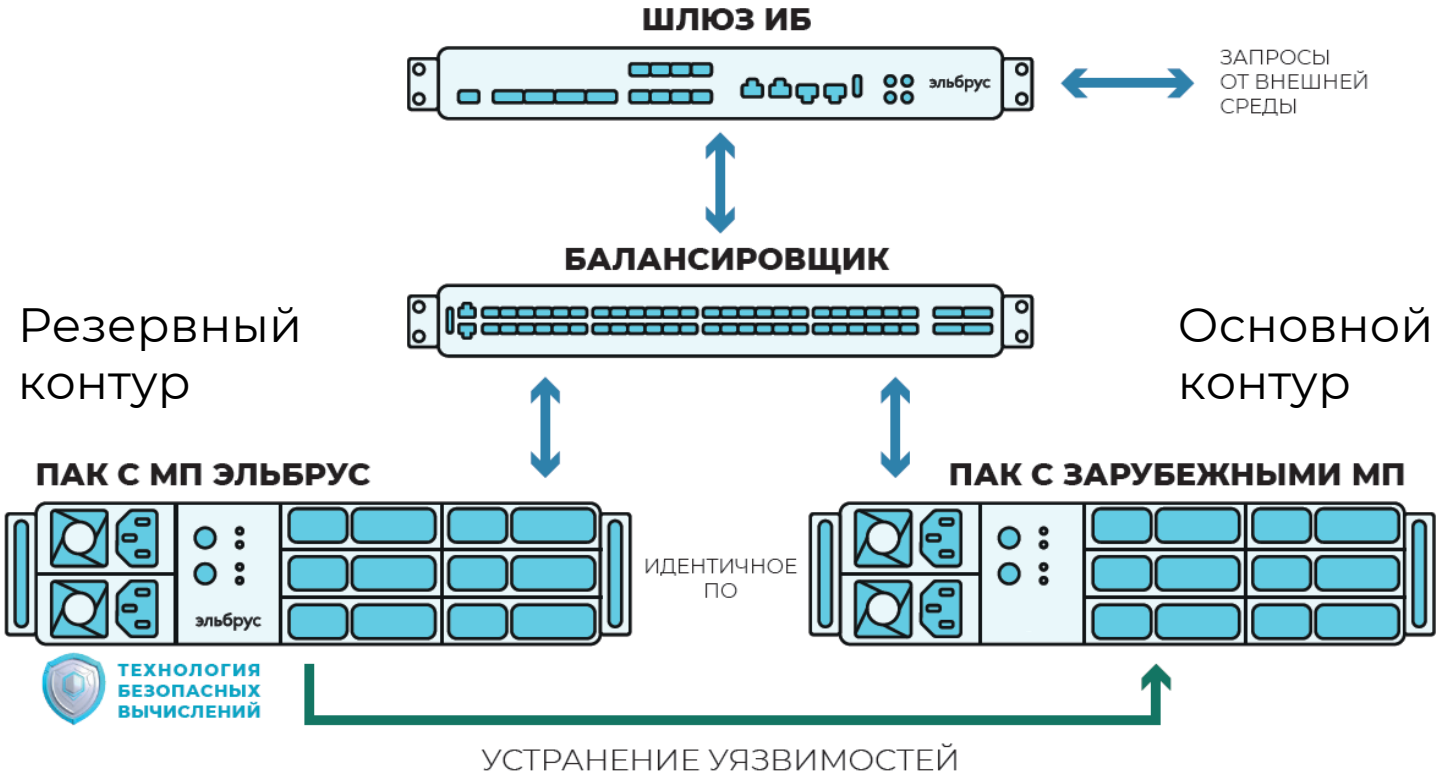


Разработка: *комплексный проект по ПП109 (через Минпромторг)*

Статус: *наличие на складах значительных запасов*

Предназначение: *пилотные проекты, стенды для переноса ПО на платформу Эльбрус, поиск ошибок в ПО через технологию безопасных вычислений, шлюзы информационной безопасности*

ГЕТЕРОГЕННЫЕ ОТКАЗОУСТОЙЧИВЫЕ ПАК



Дорожная карта перевода ПАК для КИИ на ОАПП Эльбрус



Выводы

- Платформа Эльбрус имеет потенциал стать основой создания ПАК для КИИ
- Технологии платформы Эльбрус позволяют обеспечить постепенное внедрение через ДТ x86 и повысить киберстойкость / надёжность ПАК через применение ТБВ
- Запаса процессоров Эльбрус достаточно для портирования ПО и пилотных проектов
- Необходимо стимулировать перевод ПО для КИИ на ОАПП Эльбрус
- Необходим комплекс/программа работ по созданию стеков ПО под КИИ со сниженными накладными расходами.
- **Ключевой фактор в создании ПАК для КИИ становится организационно-финансовый. Есть кадры, технологии, готовность работать!**

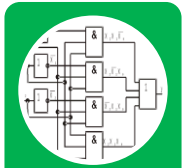
- Необходимо форсировать подготовку отечественных фабрик п/п и подложек, в том числе вести опережающее планирование разработки процессоров Эльбрус для них
- Для успешного создания доверенных ПАК необходима согласованная разработка процессоров, интерконнектов, SSD и других периферийных устройств, входящих в поверхность атаки и влияющих на производительность ПАК в целом.

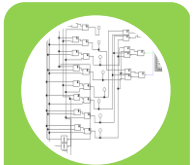
эльбрус

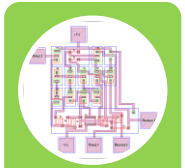
Цикл разработки и производства МП и других СБИС

САПР | САПР | САПР | САПР


ISA (система команд)


Логический дизайн ядра


Логический дизайн МП и корпуса (подложки)


Физический дизайн МП и корпуса (подложки)


Верификация помодульная, общая, программные тесты, sign-off


Производство кристаллов


Производство корпусов (подложек)


Разбраковка кристаллов и подложек


Сборка и тестирование микросхем, post-silicon validation


Разработка программного стека

МАРШРУТ ПРОЕКТИРОВАНИЯ АППАРАТНОЙ И ПРОГРАММНОЙ ЧАСТЕЙ ОАПП

Основа ОАПП – российское ядро. Использование российской ISA снимает юридические риски, которые возникнут при использовании зарубежной ISA

Российские фабрики: серийно 250…180 нм
Экспериментальные линии 130…90 нм
Перспектива – 28 нм (план Минпромторга)

Российские фабрики: керамические подложки делаем, органические – плохо.

Российские ОС и ПО: есть полностью соответствующие требованиям к ОАПП и критериям российского репозитория