Использование аппаратно-программной платформы «Эльбрус» в информационно-защищённых применениях в промышленности

Трушкин Константин Александрович
АО «МЦСТ»

О компании АО МЦСТ

1948 — Образован ИТМиВТ им. Лебедева

1992 — Образовано АО «МЦСТ» группой специалистов ИТМиВТ

2001 — Первый микропроцессор МЦСТ-R150 (150 МГц)

2007 — Первый микропроцессор серии Эльбрус (300 МГц) и ВК на его базе

2021 — МП Эльбрус-16С, производительность 0.75 Тфлопс

Сервер 4хЭ-16С , 3 Тфлопс – план (Q4)

Штат 450 человек

(5 ДТН, 40 КТН, 40 студентов, 9 аспирантов)

R&D 340 человек

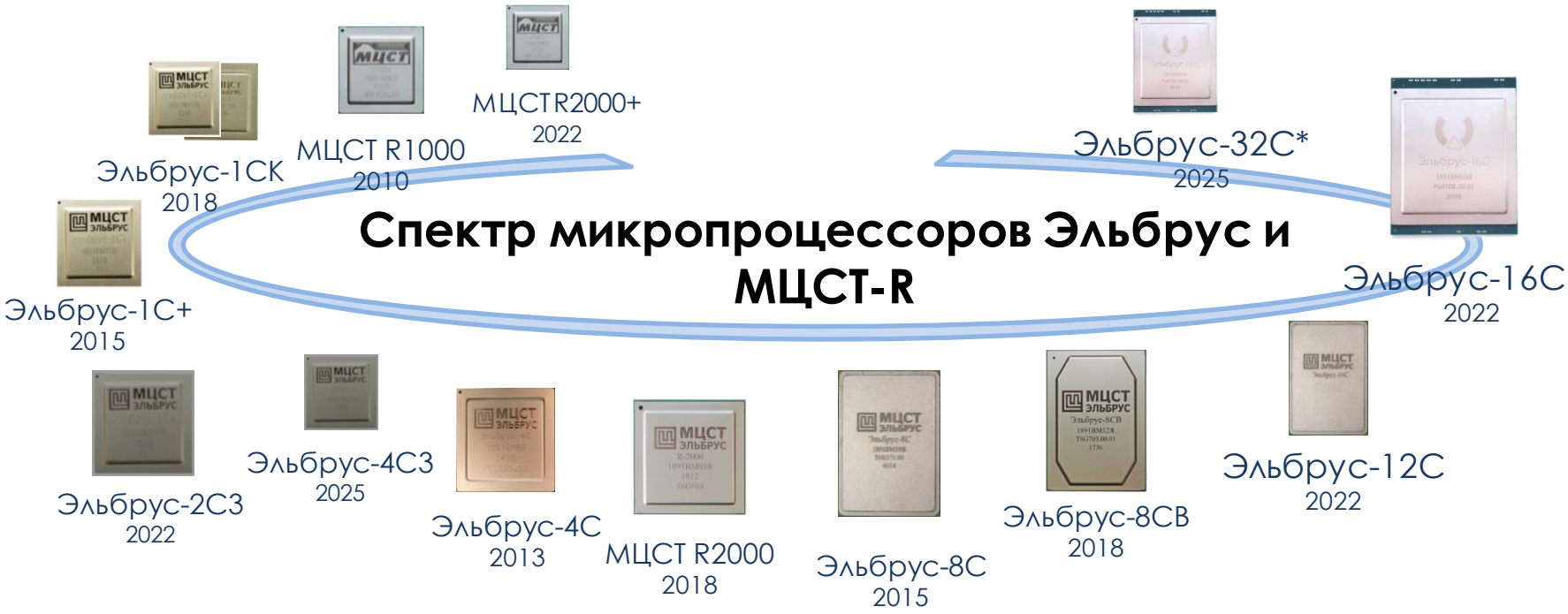
Кафедра в МФТИ, договор с МИФИ

АО «МЦСТ» - разработчик и поставщик для ВС РФ в рамках государственного оборонного заказа, как по прямым государственным контрактам с Минобороны России, так и по кооперации с головными разработчиками/изготовителями ВК на основе МП «Эльбрус» и базового ПО собственной разработки для образцов ВВТ. Основные области применения - зенитные ракетные системы ПВО, ПКО и развитие системы ПРО, СПРН, ККП, АСУ СН, ГАК и БИУС ВМФ, в современных и перспективных авиационных комплексах фронтовой и дальней авиации, в автоматизированных системах специального управления, оснащение органов управления МО.

Отечественные Аппаратно-Программные Платформы МЦСТ

Встраиваемые микропроцессоры

Серверные микропроцессоры



Настольные микропроцессоры

Серверные микропроцессоры

эльбрус

Возможности архитектуры Эльбрус

Параллельная энергоэффективная архитектура

- 25 скалярных оп. за такт за счет явного параллелизма (микро)операций
- Микрооперации планирует российский оптимизирующий компилятор
- Возможности для оптимизации программистами
- Высокая однопоточная производительность

Эффективная двоичная совместимость с Intel x86, x86-64

- Аппаратно-программная технология динамической двоичной трансляции
- ДТ любых операционных систем в кодах x86/x86-64 Windows , Linux, QNX и т.д
- ДТ приложений в кодах x86/x86-64, функционирующих в среде Linux
- Производительность до 80% от нативной (изначально в кодах Эльбруса)

Информационная защищённость

- Российский BIOS (сертифицирован ФСБ)
- Защищённость против ряда кибератак «из коробки»
- Технология безопасных вычислений
  - Аппаратная защита целостности структуры памяти программы
  - Отладка приложений на скорости ~80% от базовой (в незащищённом режиме)
  - Гарантированное обнаружение атак, нарушающих структуру памяти

Универсальные микропроцессоры «ЭЛЬБРУС»

Логические и электрические схемы аппаратуры, средства разработки, BIOS, операционная система (ОС, ОПО) созданы/портированы в России, имеются в исходных кодах.

От 1-го поколения произв-ть выросла в 300 раз

Эльбрус-1С+
40нм

4 поколение

- –25 GFLOPS
- –1 ядро
- –1 ГГц
- –2 MB L2
- –3D GPU

2015

Эльбрус-8С
28нм

4 поколение

- –250 GFLOPS
- –8 ядер
- –1.3 ГГц
- –16 MB L3
- –DDR3

2015

Эльбрус-8СВ
28нм

5 поколение

- –580 GFLOPS
- –8 ядер
- –1.5 ГГц
- –SIMD-128
- –DDR4

2018

Эльбрус-16С
16нм

6 поколение

- –1.5 TFLOPS
- –16 ядер
- –2.0 ГГц
- –Виртуализация
- –48 MB L2 + L3
- –SoC
- –8 каналов DDR4

2022 - серия
проходит испытания
Завершение исп-й 2021

Эльбрус-2С3
16нм

6 поколение

- –0,18 TFLOPS
- –2 ядра
- –2.0 ГГц
- –Виртуализация
- –2 MB L2 на ядро
- –SoC мобильный
- –3D GPU+codec

2022 – серия
проходит испытания
Завершение исп-й 2022

Эльбрус-12С
16нм

6 поколение

- –1 ,1 TFLOPS
- –12 ядер
- –2.0 ГГц
- –Виртуализация
- –36 MB L2 + L3
- –SoC, 2 кан. DDR4
- –Доступная цена

2023 – серия
инж образец - 2022

Красным – качественные изменения

эльбрус

Программная экосистема

- Собственные средства разработки:

- Fortran2003, C11, C++17 -> 20
- Совместим с **gcc**, в разработке **llvm** back-end

- Java 8, 11
- Mono 5.16, (2021: 6.12), .NET Core 3.1.8
- NodeJS: 12.16.3

- Библиотека EML ~ 1500 функций

- Двоичный транслятор system / application

- Дистрибутивы

  - Ядра: 5.4. и более ранние. Версии для Эльбрус, x86-64, SPARC
  - Более 5000 программных пакетов
  - Арх.-зависимые фрагменты и оптимизации

- **+ Экосистема проприетарного российского ПО**

Программная экосистема

Lotos	Энстрим
ЗОСРВ «Нейтрино-Э»	СВД Встраиваемые системы
Эльбрус Линукс	МЦСТ
Ось	НЦИ
Роса Линукс	Роса

СУБД Линтер	Релекс
СУБД РЕД БД	РЭД СОФТ
СУБД PostgresPro	Postgres Professional

СЭД Дело	ЭОС
СЭД Бюрократ	ИВК

OpenSCADA	OpenSorce/ИНЭУМ
MasterSCDA	ИНСАТ

Электронный Архив	ЭлАР

Аналитика LuxBI	LuxMS

ВКС ТруКонф
ВКС НИПС
ВКС IVA/Масштаб

ГИС Панорама
ГИС Горизонт

Спектр ВТ на базе МП Эльбрус

Настольные ПК

Моноблоки, терминалы

Бортовые и промышленные компьютеры

Планшеты

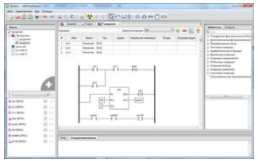
Кластеры и СуперЭВМ

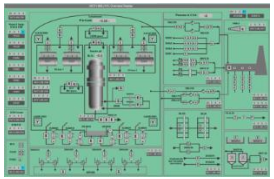
Серверы общего назначения

Системы хранения данных

Ноутбуки

Управляющие вычислительные комплексы СМ1820М





Серийно выпускаемая более 10 лет и постоянно обновляемая линейка управляющих вычислительных комплексов (серверы, стойки сбора данных, серверы) для построения верхнего уровня системы управления технологическими объектами.

Резервированные решения с дублированными вычислительными блоками (как стойки, так и АРМ).

Класс безопасности по НП-001-15: 3Н
Управляющие вычислительные комплексы проходят испытания на вибрацию, ЭМС и т.д.

Работа под управлением ОСРВ Эльбрус или ОС Linux.

Программирование логики объекта на языках стандарта МЭК61131-3 (САПР Beremiz, MasterSCADA-4D).
Решение по визуализации: SCADA-Elbrus, MasterSCADA 4D, Sematic WinCC.
Поддержка СУБД: PostgreSQL, Oracle.

Изделия такого типа работают в системах АСРК на энергоблоках Калининской, Белоярской, Ростовской, Ленинградской АЭС,
Тяньваньской АЭС, АЭС Куданкулам, а также в ряде других систем на объектах атомной промышленности.

Уровень технологий Эльбрус в СХД

НТ НОРСИ-ТРАНС

RAIDIX

AERODISK faster, higher, safer

BAUM UNIFIED DATA STORAGE

BITBLAZE

Послед. чтение	5.7 ГБайт/с
Послед. запись	2.7 ГБайт/с
IOPS, чтение	1.4 млн
IOPS, запись	0.7 млн
Корпоративный функционал	Есть
Гипер-конвергентность	Есть
Хранение ФЗ-374	Есть
Уровень 2021 г.	Mid range
Уровень 2022 г.	High End

DEPO

РСК

ОТВ

АРГО ИСТ

Уровень технологий Эльбрус в ЦОД и НРС

ФГБУ НИИ Восход
- ЦОД для ГИС «МИР» для обработки паспортно-визовых документов нового поколения (ПВДНП) с инфраструктурой и сервисом, 24x7
- Национальный удостоверяющий центр (НУЦ)

Первый пример ГИС на росс. процессорах

Обработано
10.5 млн документов

МВД России
- Серверы Эльбрус для ЦАФАП - **400+** шт во всех регионах России

Хранение, обработка, анализ видеопотока
Первая высоконагруженная система на российских процессорах

Реализация виртуализованной среды на текущих процессорах Эльбрус

ЦИАМ
- СуперЭВМ с процессорами Эльбрус **50 Тфлопс**

Первая супер-ЭВМ на росс. процессорах с СЖО

Инженерный расчет RANS и RANS/ILES методами с высокой сходимостью

Микропроцессор «ЭЛЬБРУС-32С»

- > 3 TFLOPS (FP64) / 6 TFLOPS (FP32) / 12 TFLOPS (FP16) 4x
- 32…64* ядра Эльбрус v6 @ >=2 ГГц (арх 7-го поколения) >2x
- Система команд - крипто- и нейропримитивы, гибкость
- Виртуализация – развитие
- Технология безопасных вычислений - развитие
- Объём кэш-памяти >=64 MB 2x
- >= 6 каналов памяти DDR5 1.5…2x
- >= 4 ТБ на процессор 4x
- >= 64 PCIe 5.0 lanes 4x
- NVMe/SATA, Ethernet 10…100*, USB >=3.1
- Многопроцессорность (2S-4S* конфигурации)
- Шина CXL 2.0 – для интерконнекта и акселераторов
  - NVMe nex-gen, Mellanox, Ангара, СМПО, нейропроцессоры
- <=6 нм FinFET, ~600 мм^2, ~30В транзисторов

Крупные облачные ЦОД

Супер-ЭВМ

Кластеры с общей памятью

Стенды для отладки ПО

Гибридные вычисления

СХД гиперконвергентные

СХД классические High-end

*возможность определяется в ходе проектирования

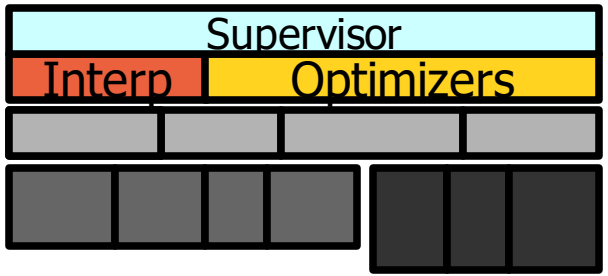
Зелёным – улучшение в разах относит. Эльбрус-16С

Технология двоичной трансляции x86/x86-64

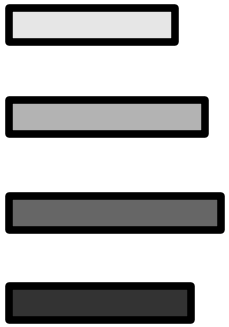
Двоичная трансляция кодов x86

Многоуровневая оптимизирующая трансляция

Чаще = темнее



Откомпилированные регионы



Интерпретатор исполняет редкий код

Более 3 исполнений — шаблонная компиляция

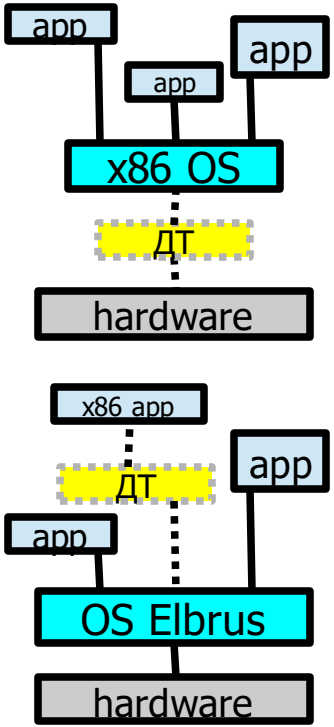
Более 2500 исполнений — легкая оптимизация

Более 200000 исполнений — агрессивная оптимизация

Коды Elbrus в процессе работы системы двоичной трансляции

+ База кодов
+ Отдельный поток для трансляции

Двоичная трансляция кодов x86



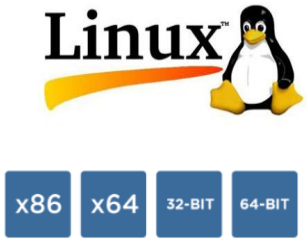
- Трансляция кодов x86 поддержана в двух режимах:
  - Полная эмуляция машины x86
  - Эмуляция x86-приложения в нативном окружении
- В аппаратуре были реализованы
  - Поддержка трансляции адресного пространства эмулируемой x86-машины
  - Поддержка модели памяти x86
  - Эффективная поддержка точных и асинхронных прерываний x86
  - Поддержка быстрых переходов между участками оптимизированного кода

Вся аппаратная поддержка повышения производительности задействована в ДТ

Миграция ПО на платформу Эльбрус через ДТ

Исходное ПО для платф. Windows

Перевод на стек ПО для платф. Linux/x86



Постепенный перенос ПО на арх. Эльбрус

ПОРТИРОВАНИЕ

Перенос всех приложений на арх. Эльбрус

МЦСТ ЭЛЬБРУС

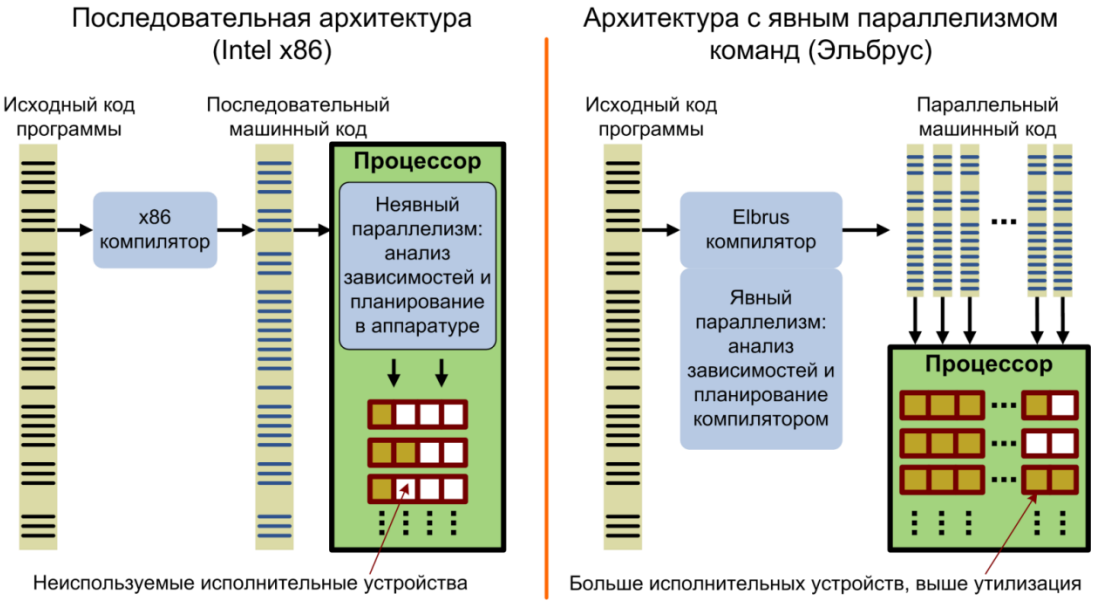
ДТ + Виртуализация Эльбрус-16С

С помощью двоичной трансляции (ДТ) можно ускорить внедрение российской ВТ, не дожидаясь портирования всего стека ПО

Вопросы информационной безопасности

Принципы архитектур: RISC vs. VLIW (Эльбрус)

Линия МЦСТ-R

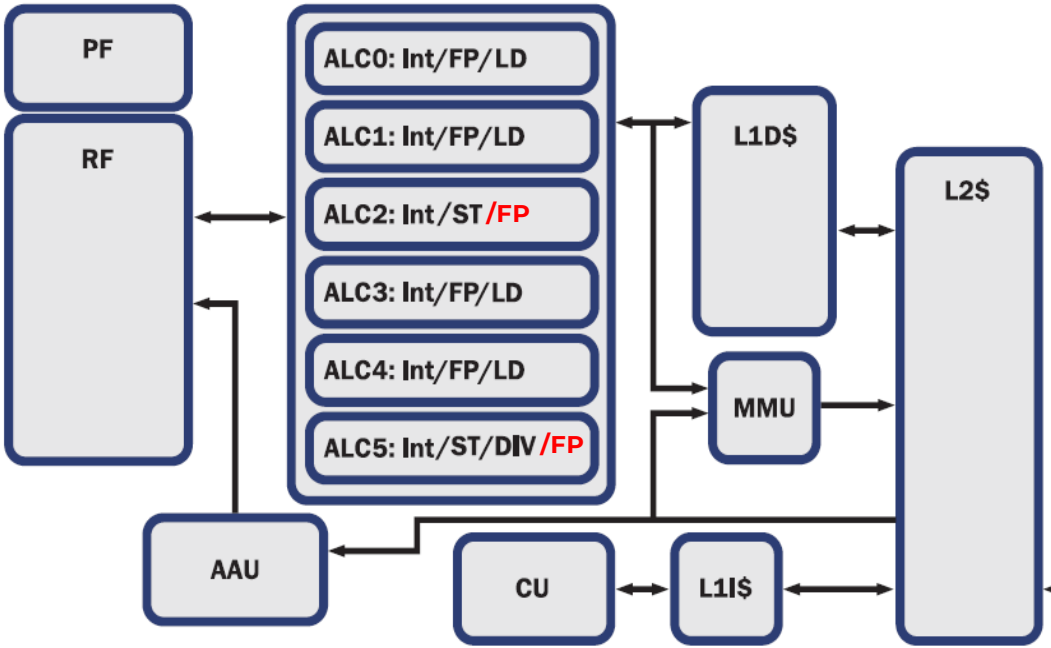


Перенос части работы по распараллеливанию на компиляцию

Достижение большего параллелизма при меньшей мощности

Линия Эльбрус

Микропроцессоры Эльбрус – архитектура ядра



RF *- универсальный регистровый файл*

PF *- регистровый файл для однобитных предикатов*

ALC0...ALC5 *- каналы исполнения*

MMU *- Устройство управления памяти*

L1D$ *- кэш-память данных 1го уровня*

L1I$ *- кэш-память инструкций 1го уровня*

L2$ *- кэш-память 2го уровня*

CU *- устройство управления*

AAU *- устройство предварительной подкачки данных*

RF – 256 80/128 - битных регистров с тегами, из них до 128 с программным переименованием

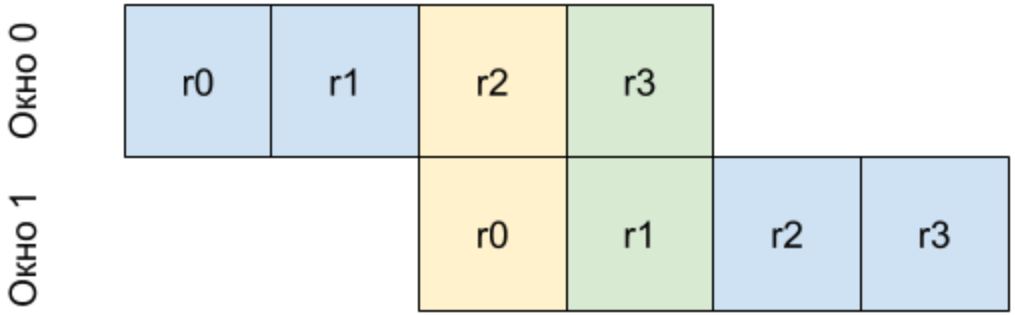
PF – 32 1-битных регистра для хранения предикатов с тегами и программным переименованием

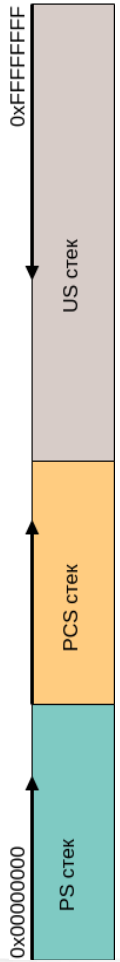
Красным указаны изменения для архитектуры в.4/в.5 (Эльбрус-8С/8СВ)

Незащищённый (обычный) режим

- Три различных стека
  - USER Stack – классический стек для автоматических переменных и параметров, доступный из процедуры
  - PROCEDURE Stack – стек регистров для откачки и подкачки при вызовах процедур (выделении регистровых окон), доступный из процедуры
  - PROCEDURE CHAIN Stack – стек связующей информации – адреса возврата, **не**доступный из процедуры

Структура стеков делает невозможными атаки типа ROP





История: что решала защита в архитектуре Эльбрус-1,2,3?

- Низкая производительность труда
- Аксиома: В каждой программе есть хотя бы одна ошибка
  - Программные ошибки есть потенциальные уязвимости
  - Программная ошибка – то же, что НДВ для атаки
- Отладка кода занимает слишком много времени/усилий
- Тезисы Б.А.Бабаяна:
  - Существующие компьютеры неудобны для работы программистов
  - Компьютер должен быть простым для программирования
  - Языки высокого уровня снижают количество ошибок
  - «Правильный» компьютер не должен позволить исполняться «неправильной» программе

История: МВК «Эльбрус-1,2»

Могли работать как в защищенном, так и в обычном режиме
- Боевой режим – защищенный
- В переходный период допускалась работа в обычном режиме

Все ПО было написано «от нуля»

Fortran и Эль-76

Практически отсутствовали проблемы совместимости
- Полная обратная совместимость (защищенный режим → незащищенный)
- Несовместимость на уровне трансляции из-за более строгой типизации

Легкая отладка
- Отладчиком пользовались только разработчики ОС
- На прикладном уровне отладчик не требовался

Технология безопасных вычислений

- Защита от ошибок программиста:
  - неинициализированные данные
  - контроль границ объектов
  - обращение к освобождённой памяти
- Защита от эксплуатации ошибок злоумышленником:
  - Переполнение буфера (buffer overflow)
  - use-after-free
- Изоляция недоверенного модуля / защита от утечек информации через библиотеки
  - межмодульная защита
- Рост производительности труда программистов в несколько раз

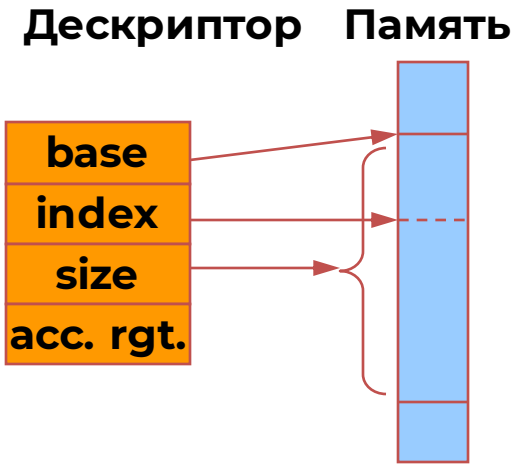
Ошибки с системах АСУ ТП, связанные с неправильной работой с памятью - Отчёт Positive Technologies, 2016

В каждой тысяче строк кода содержится минимум одна ошибка

В ядре Linux содержится 20+ млн строк кода

Для индустриальных приложений безопасность - главная характеристика после корректности функционирования. ТБВ повышает оба KPI

Технология безопасных вычислений МП Эльбрус

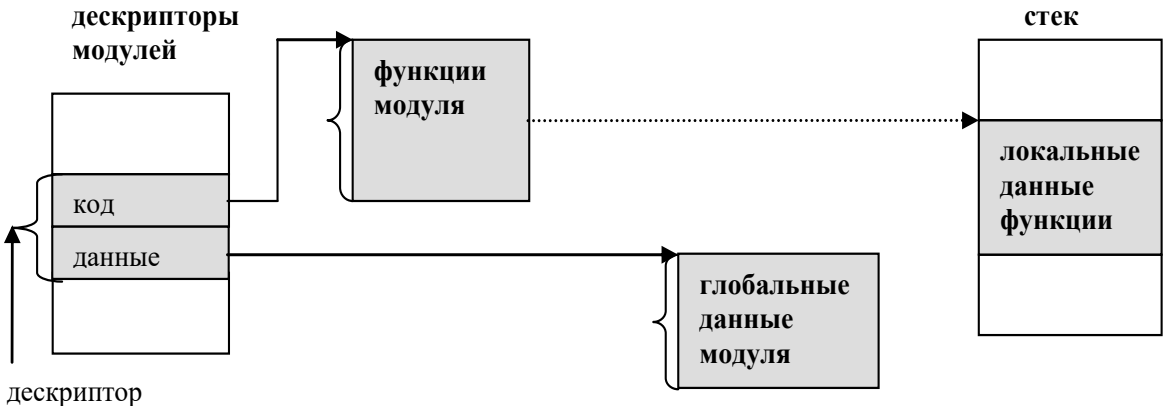


Все данные в процессоре и памяти сопровождаются дополнительным полем – «тегом», содержащим их тип (по 2 разряда на каждые 4 байта), хранящийся в ECC

Адресная информация всегда отличима от неадресной

- Размер «указателя» (дескриптора) - 128 бит
  - Адресная арифметика работает согласно стандарту
  - Запрещены операции преобразования целого в указатель
  - Можно генерировать дескрипторы подобъектов

Технология безопасных вычислений МП Эльбрус



- Контекстная защита: взаимодействие – только через законный интерфейс

  (с точки зрения семантики языка высокого уровня)

  - Параметры функций и возвращаемое значение
  - Глобальные переменные, проэкспортированные в модуль
  - Куча (heap)

Технология безопасных вычислений МП Эльбрус

Задача	Неинициали-зированные данные	Выход за границу массива	Привязка к свойствам аппаратной платформы	Отклонения от стандарта языка	Преобразо-вание целого в указатель	Запись в глобал указателя на локал
008.espresso	1			1		
023.eqntott	1			2		
052.alvinn						
056.ear				>20		
072.sc			<10			1
099.go		<10				
124.m88ksim						
126.gcc			<10	<10	<10	
129.compress	1	1	1			
130.li						>20
132.ijpeg	>20	<10	1	<10		
134.perl	1			>20		
147.vortex			<10			
164.gzip						1
175.vpr			1			<10
176.gcc			<10	<10	<10	
177.mesa	<10		<10			
179.art						
181.mcf						
183.equake						
186.crafty						<10
188.ammp						
197.parser			1			
252.eon						
253.perlbmk			<10	1	<10	
254.gap						
255.vortex			<10			
256.bzip2						
300.twolf	>20			<10	<10	
Всего проблем по числу задач	**7**	**3**	**11**	**9**	**4**	**5**

Задачи на языках C/C++ из стандартных пакетов SPEC CPU 92,95,2000

Направления совместных работ с Лабораторией Касперского

Текущие и перспективные продукты

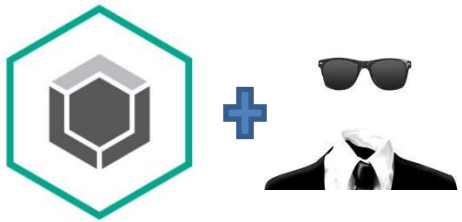
Готовность (выше-ниже)

Компьютеры Эльбрус + Kaspersky Endpoint Security – готово!

KasperskyOS, перенос на Эльбрус
– требует портирования

KasperskyOS, перенос на Эльбрус в защищённом режиме (ТБВ)
– требует портирования

Интеграция Kaspersky Endpoint Security в двоичный транслятор – требует R&D



эльбрус