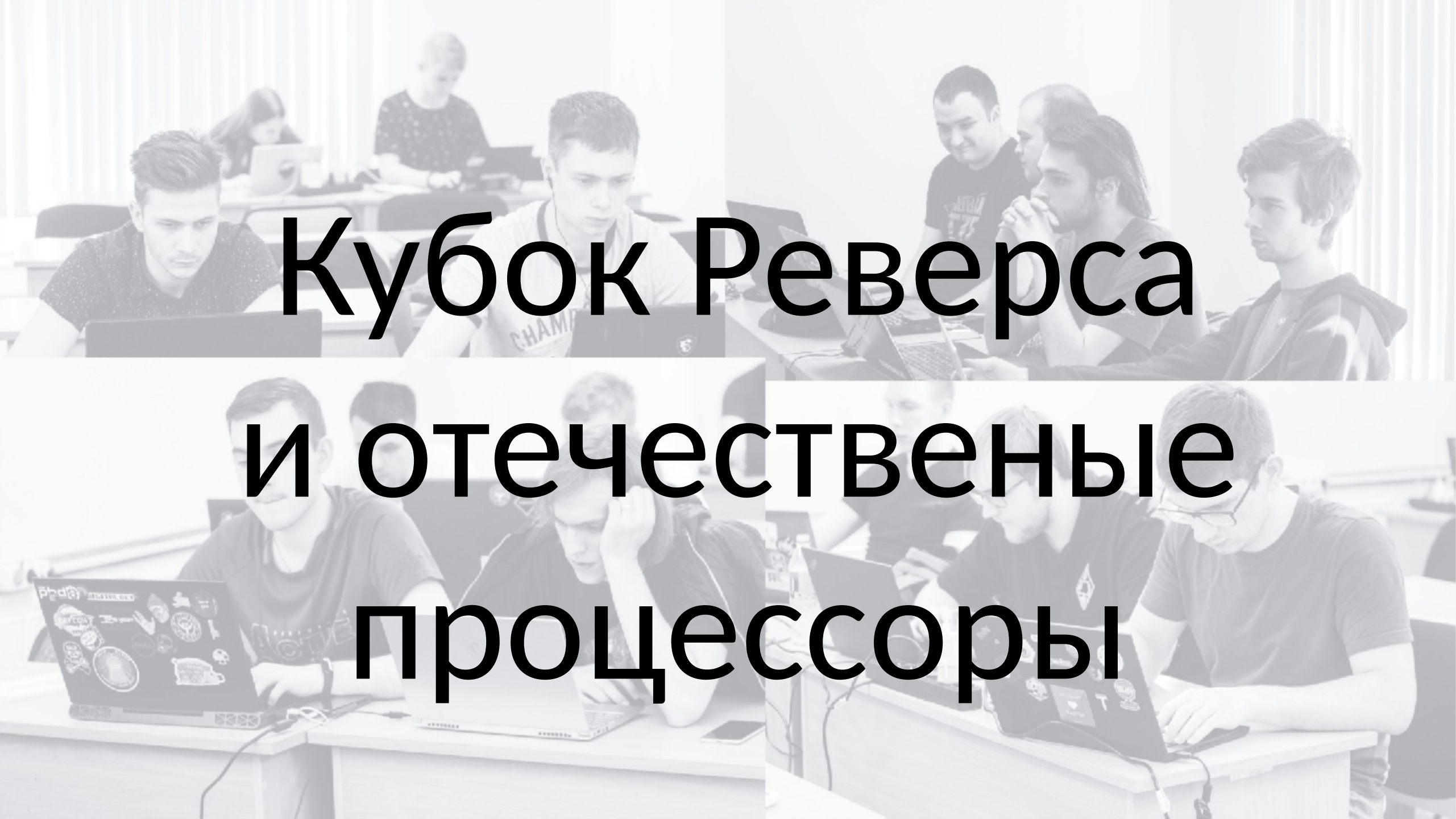
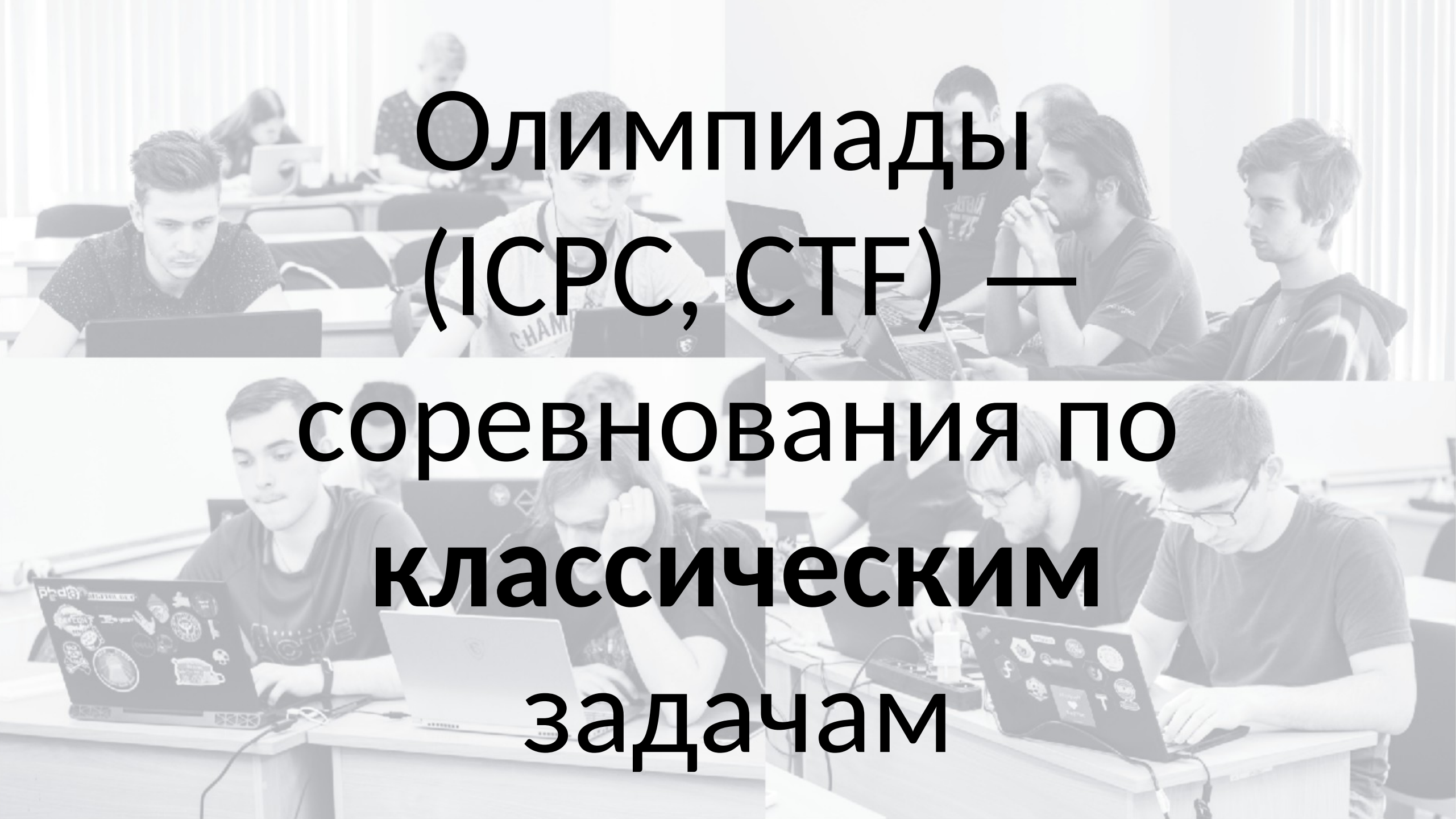




Кубок Реверса

и отечественные
процессоры



Олимпиады
(ICPC, STF) —

соревнования по
классическим
задачам

Следующий шаг развития —
специализированные
соревнования



Следующий шаг развития —
специализированные
соревнования

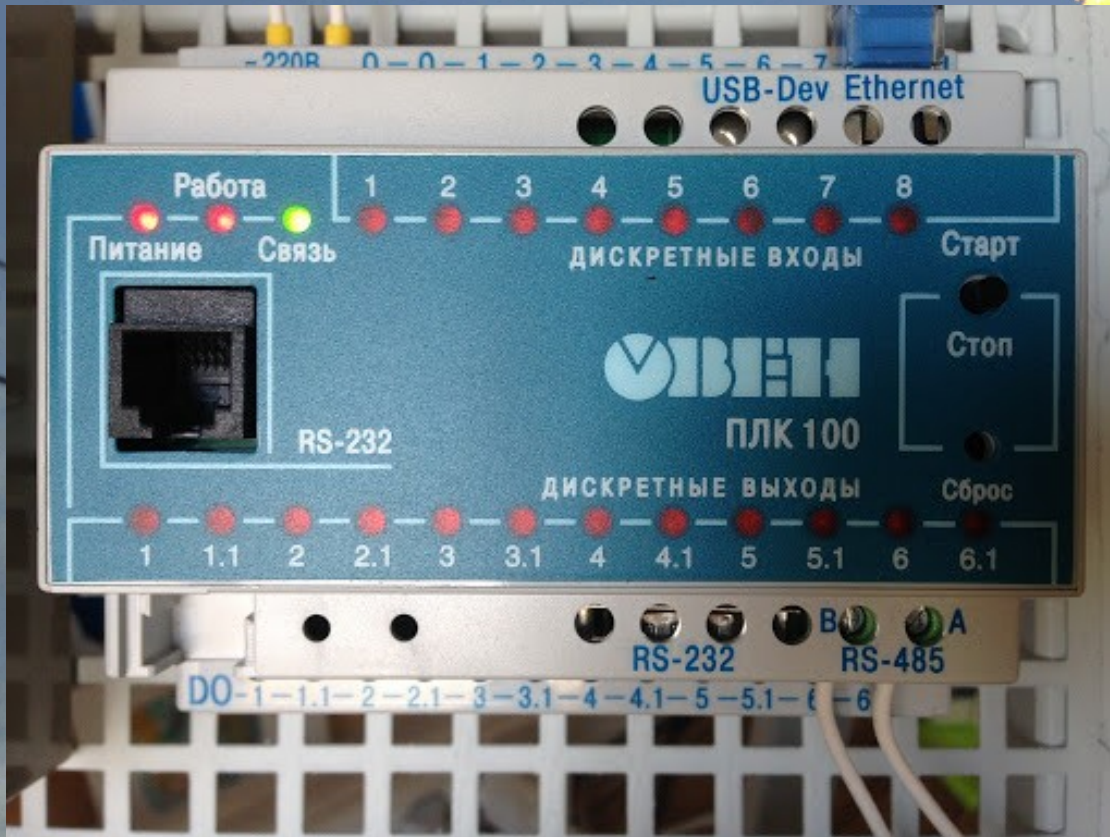


A photograph of an industrial facility, likely a refinery or chemical plant, featuring several tall distillation columns and complex piping. A large, bright orange flame is visible rising from one of the central structures. The sky is blue with some clouds.

Информационная безопасность промышленных объектов

Industrial CTF

Kaspersky Industrial CTF, Противостояние на PHDays



25

Даниил Григорян
(Академия ФСО)

Владимир Лебедев
(ТГУ, Томск)

Полина Соколова
(СПбГУ)

Сильнейшая команда



VIM (МФТИ)
Эдгар Казиахмедов, Клим Киреев

Зачем кубок реверса?

Обратная разработка, реинжиниринг

- Задаём стандарт подготовки специалистов
- Требуем широкий кругозор, умение быстро строить модели и исследовать архитектуру
- Развитие учебных курсов университетов

Почему отечественные процессоры?

- Для широко распространённых архитектур есть готовые инструменты.
- Нужны специалисты для импортозамещения
- Новые архитектуры — новые возможности, выход из тупика.

Проблемы

3 основных блока проблем, обнаруженных при подготовке и проведении соревнований

1. При анализе статистики соревнований
2. При общении с участниками во время разборов задач (в конце каждого соревновательного дня)
3. При поиске партнёров, который оказался на удивление сложной задачей

1

Статистика

Кубок Реверса

1 обладатель кубка
10 победителей
25 финалистов
139 участников
520 заявок на участие
более 20 академий и
университетов России

ИТ

25 000 выпуск
15 000 в т.ч. прогр.
уже работают
500 000 в России
2 000 000 в Китае
3 000 000 в Индии
4 000 000 в США

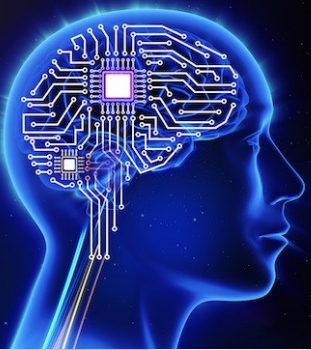
?

Разборы задач

- Отсутствует системная подготовка
- Решают только те задачи, которые знают как решать — нет элементарных навыков исследовательской работы
- Не допускают даже мысль о собственной разработке программ
- Разработчики задач из промышленности не представляют как ставить задачу

Поиск партнёров

- Работодатели не видят никакого смысла в сотрудничестве с университетами
- Они сами организуют обучение и абсолютно удовлетворены его результатами
- Кадровые агентства не знают что такое реверс, обратный анализ и реинжиниринг
- Фонды поддержки образования не хотят финансировать то, чего нет в учебных планах



Кубок Реверса 2020

Региональный тур

- Установление контактов с работодателями
- Отбор участников для финала
- Поиск талантов

Финальный тур

- Организация сообщества
- Формирование рейтингов
- Усиление мотивации

Планы

1. Факультативы + КПК по реверс-инжинирингу ARM, Байкал-М, Эльбрус, безопасности промышленных контроллеров, ОС AstraLinux и т. п. в МФТИ

2. Финал в апреле-мае (по эпидемической обстановке)

ОСНОВНЫЕ ВЫВОДЫ

Необходимо:

1. Создать клубы реверса по возможности при больших университетах
2. Обеспечить клубы программами подготовки и практическими задачами
3. Привлечь к преподаванию сотрудников предприятий-работодателей
4. Проводить ежегодные соревнования



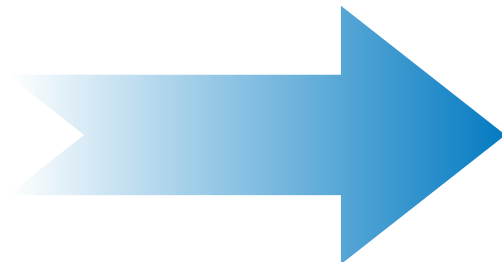
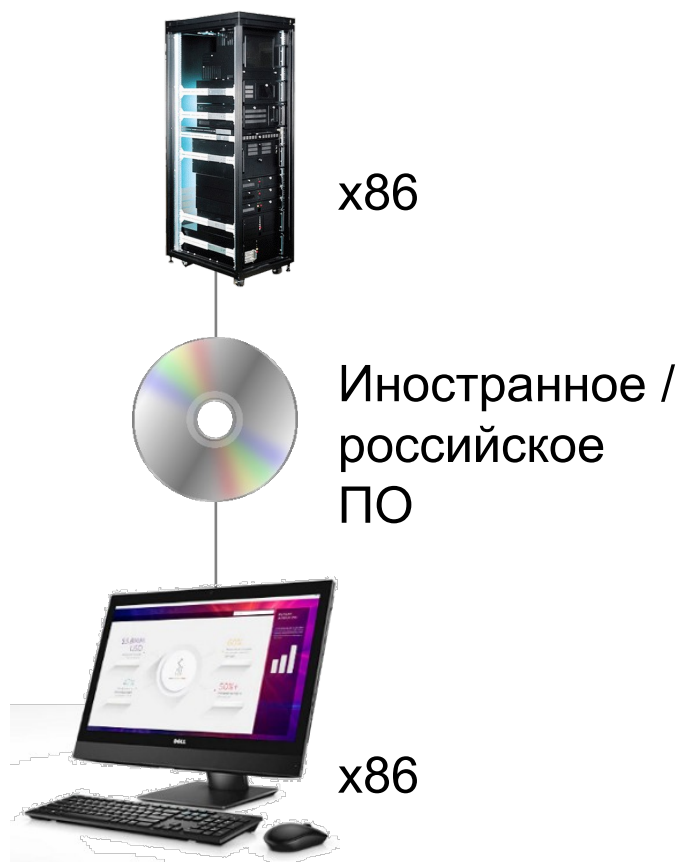
**Процессоры Baikal – платформа
безопасных отечественных
решений**



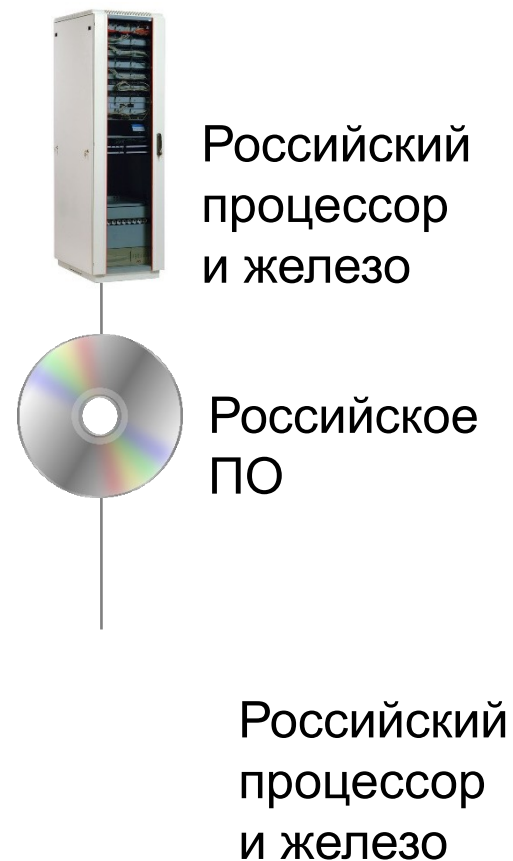


Требования регуляторов к инфраструктуре

2021 год



2024 год





О компании



Сегодня в компании работает **140** человек,
из них **85** инженеров и разработчиков

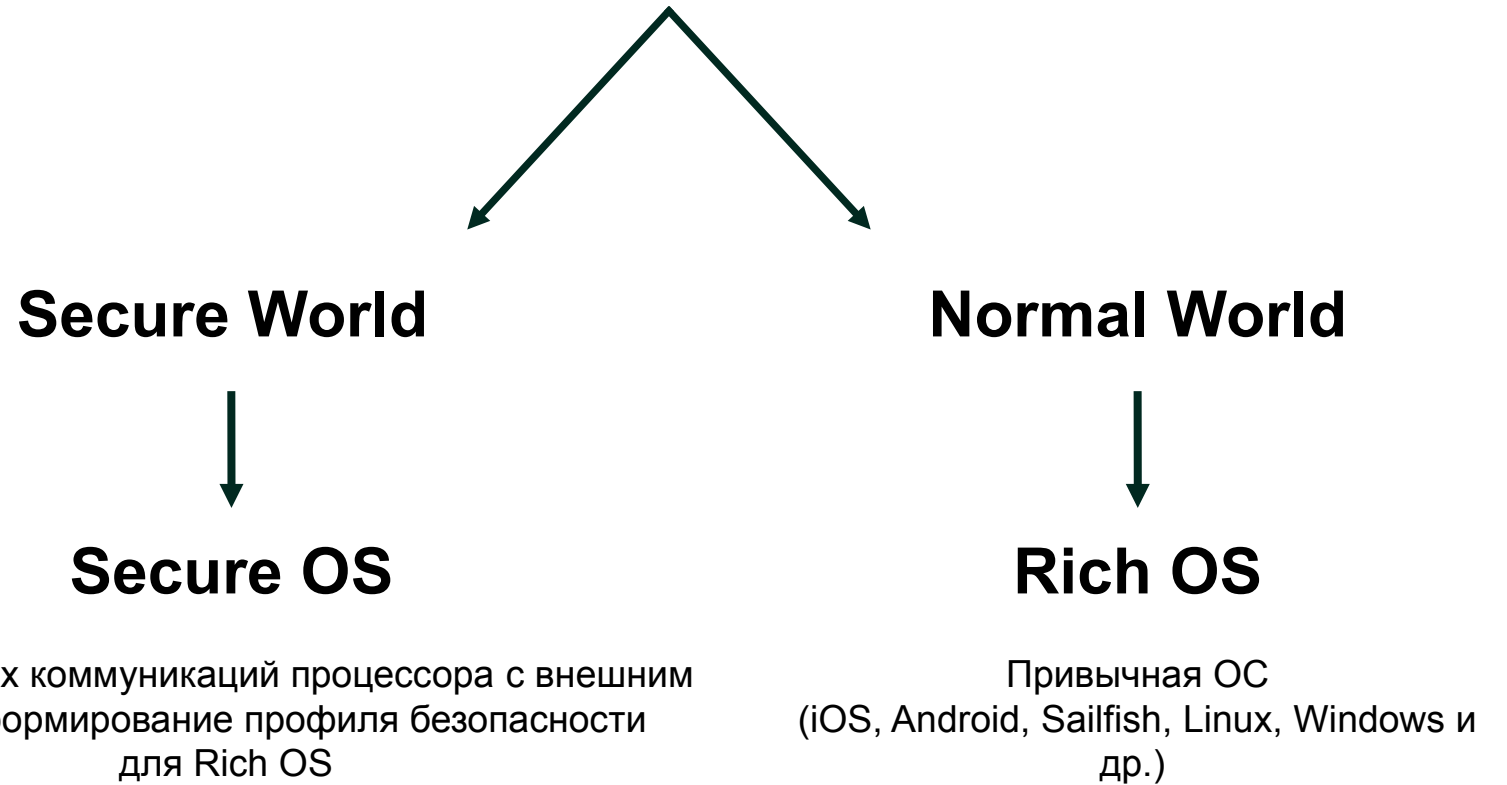




System Management Mode для ARM



Arm Security Extensions = Arm TrustZone





System Management Mode для ARM

1 Загрузчик получает управление сразу после включения питания, стартует Secure OS

2 Secure OS загружает "гостевую" Rich OS

3 Secure OS может контролировать все приложения, и сама Rich OS узнать об этом не может

Управление обменом с периферией производится через TrustZone





Продукты компании



Baikal-T

Массовое
производство

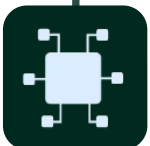
- 28 нм
- 2 ядра MIPS P5600
- Частота 1,2 ГГц



Телекоммуникационное
оборудование



Системы
хранения данных



Встраиваемые
системы



Baikal-M

Массовое
производство

- 28 нм
- 8 ядер Arm Cortex-A57
- 8 ядер Arm Mali T628
- Частота 1,5 ГГц



Настольные
ПК и моноблоки



Мини-серверы



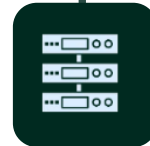
Промышленные
системы



Baikal-S

Производство – Q2 22
Образцы – Q4 21

- 16 нм
- 48 ядер Arm Cortex-A75
- Частота 2 ГГц



Серверы



Системы
хранения данных



Суперкомпьютерные
системы



Baikal-L

Производство – Q2 23
Образцы – Q4 22

- 12 нм
- 4 ядра Arm Cortex-A710
- Частота до 2,5 ГГц



Ноутбуки



Промышленные
планшеты



Baikal-T



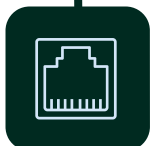
Baikal-T

Серийный продукт

- 25×25 мм, BGA
- Рабочая температура 0...+70 °C*



Встраиваемые системы и интернет вещей



Коммуникационные устройства



Промышленные и встраиваемые системы

2 ядра
MIPS Warrior P5600

1,2 ГГц
рабочая частота

5 Вт
энергопотребление

8 Гб DRAM
32-bit DDR3-1600

2 × SATA
6G

4 × PCIe
PCIe Gen 3

3 × Ethernet
2 × 1 Гбит; 1 × 10 Гбит

28 нм
техпроцесс



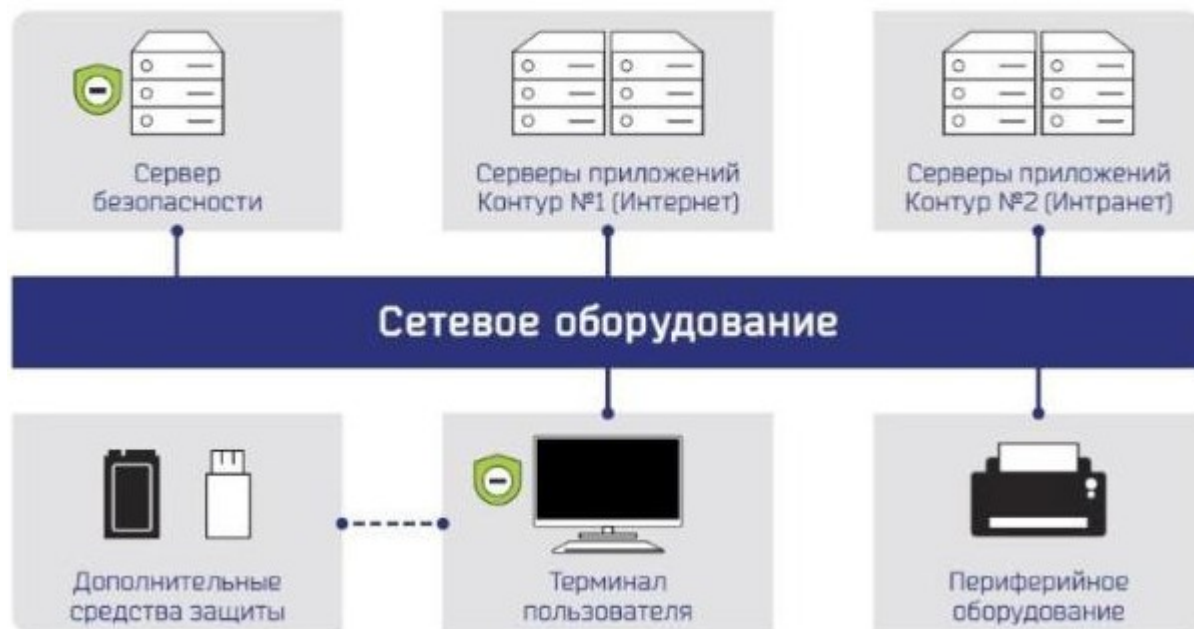
Интегральная микросхема второго уровня, относится к продукции, произведённой на территории РФ согласно ПП РФ от 17 июля 2015 г. № 719

- 32-битная архитектура MIPS
- Возможность применения в устройствах с повышенным уровнем безопасности
- Широкий набор интегрированных коммуникационных интерфейсов



Примеры готовых безопасных решений на Baikal-T

Программно-аппаратный комплекс «Тринити»



Обеспечивает обработку информации в замкнутой и доверенной аппаратно-программной среде.

Возможности:

- усиленная аутентификация пользователей и идентификация оборудования в системе;
- масштабируемая система с высоким уровнем информационной безопасности;
- централизованное управление всей ИТ-инфраструктурой и аудит всей системы;
- многоуровневая система разграничения доступа к конфиденциальной и открытой информации;
- защита всех каналов и сессий
- с помощью СКЗИ;
- аудит всей системы;
- многоконтурный режим работы пользователя.



Примеры готовых безопасных решений на Baikal-T

Программно-аппаратный комплекс «Горизонт-Т»



Предназначен для виртуализации и защиты виртуальных систем и состоит из Сервера E-Class, терминальных станций «Таволга-Терминал 2BT1» в качестве тонких клиентов и ПО «Горизонт -ВС».

Использует аппаратную платформу и ПО, включенное в реестр отечественного ПО Минкомсвязи РФ.

Отличительная особенность платформы виртуализации – интегрированное взаимодействие гипервизора и «тонкого клиента» со специальным аппаратным модулем идентификации и контроля доверенной среды, обеспечивающим дополнительную защиту от несанкционированного доступа к данным и программному обеспечению.



Baikal-M



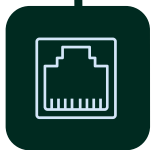
Baikal-M

Серийный продукт
300+ тыс. в 2022 году

- Техпроцесс 28 нм
- 40×40 мм, BGA
- Рабочая температура 0...+70 °C*



Настольные
ПК и моноблоки



Коммуникационные
устройства



Промышленные
и встраиваемые
системы

8 ядер

Arm® Cortex™-A57

1,5 ГГц

рабочая частота

35 Вт

энергопотребление

2,5K

разрешение видео
2560×1440 (WQHD)*

8 ядер GPU

Arm® Mali™-T628

3 × PCIe

PCIe Gen 3

6 × USB

2 × 3.1 Gen 1; 4 × 2.0

128 Гб DRAM

64-bit DDR4-2400*



Интегральная микросхема второго уровня, относится к продукции, произведённой на территории РФ согласно ПП РФ от 17 июля 2015 г. № 719

- 64-битная архитектура Armv8-A
- Технология доверенной загрузки
- Динамическое управление рабочими частотами и энергопотреблением CPU

* Указанные характеристики могут отличаться от фактических





Примеры готовых безопасных устройств на Baikal-M

Моноблок Depo Neos Twin M524



Двухконтурный защищенный комплекс. Обеспечивает одновременную безопасную работу сотрудников с информацией ограниченного доступа и открытой информацией. Два независимых вычислительных узла размещены в корпусе моноблока, поддерживающего мгновенное переключение между контурами.

Принт-сервер



Первое защищенное решение для корпоративной печати на полностью российских компонентах с предустановленным ПО управления печатью «Мониторинг и Защита» на российском ядре собственной разработки компании. ПО обеспечивает безопасность и защиту конфиденциальных данных и мониторинг устройств: позволяет контролировать расход картриджей, отслеживать счетчики устройств, данные об объемах печати сотрудников.



Развитие экосистемы Операционные системы

Разработчик ПО

Операционная система

Статус



Astra Linux Special Edition

Доступна для рынка



«Альт Рабочая станция 9.1»
«Альт 8 СП»

Доступна для рынка



«РЕД ОС 7.2»

Доступна для рынка



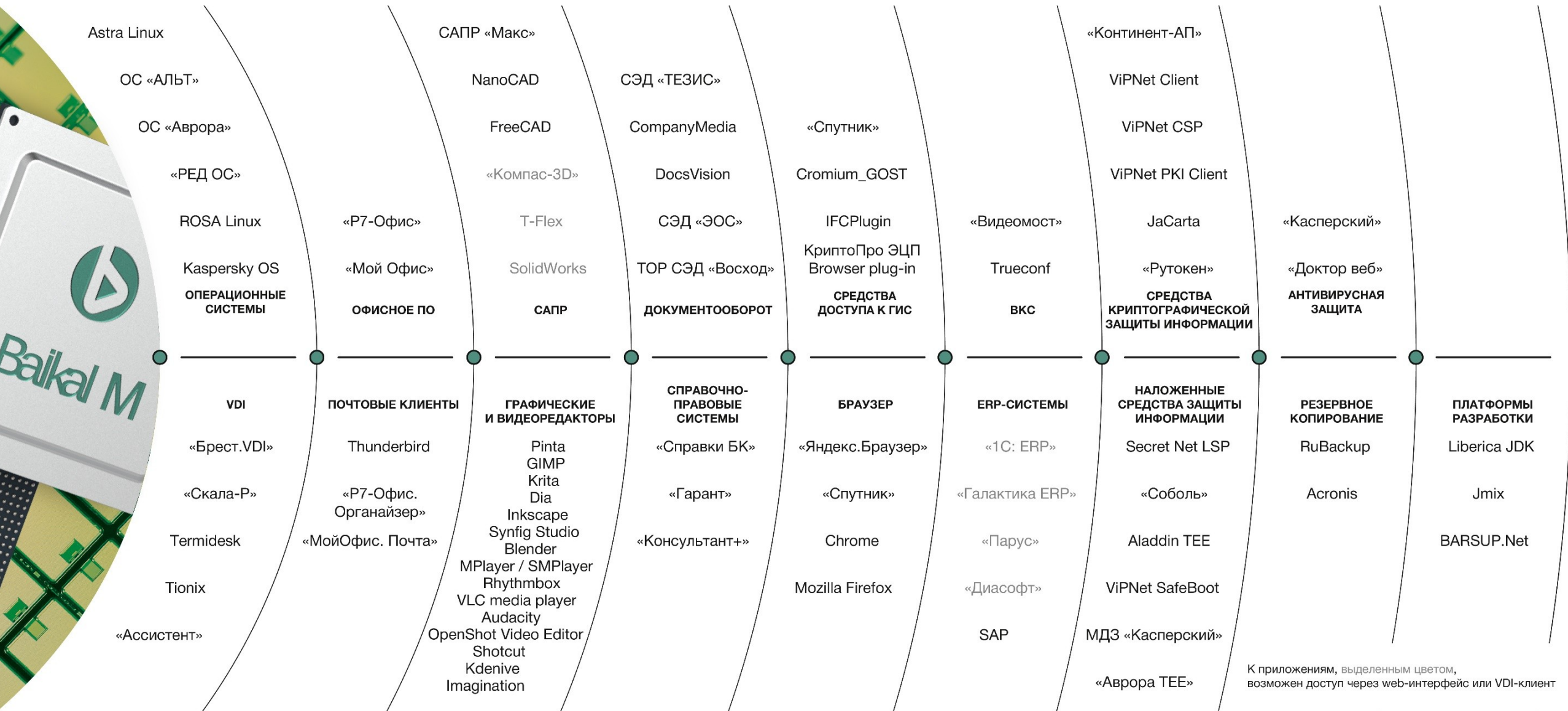
Операционная система «Аврора»
для электронных терминалов и киосков

Доступна для рынка



Развитие экосистемы Baikal-M

Прикладное ПО

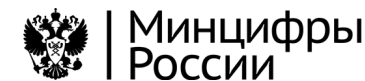




- Полностью российское защищенное решение
- Производительность на уровне западных аналогов
- Соответствие всем требованиям регуляторов рынка



Процессор Baikal-M



ОС и ПО из реестра
отечественного ПО



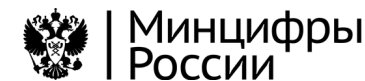
АРМ производства одного
из вендоров из реестра
Минпромторга



- Полностью российское защищенное решение
- Аналог Intel Xeon Gold 2 поколения по производительности
- Развитая экосистема совместимого программного обеспечения серверного класса



Процессор Baikal-M



ОС и ПО из реестра
отечественного ПО



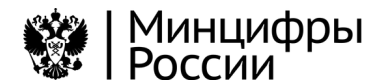
АРМ производства одного
из вендоров из реестра
Минпромторга



- Полностью российское защищенное решение
- Использование в качестве информационного терминала и терминала электронной очереди
- Соответствие всем требованиям регуляторов рынка



Процессор Baikal-M



ОС и ПО из реестра
отечественного ПО



Киоск производства
одного из вендоров из
реестра Минпромторга



Инфраструктура на отечественных процессорах





Развитие экосистемы

Антивирусные средства защиты информации



Kaspersky® Endpoint Security

Многоуровневая защита нового поколения
от всех типов киберугроз



Развитие экосистемы Средства криптографической защиты информации

Разработчик ПО	Название ПО	Назначение
 КОД безопасности	«Континент АП»	Клиентское приложение для защищенного доступа в корпоративную сеть с удаленных персональных компьютеров и смартфонов сотрудников
	ViPNet Client	Клиентское приложение для защиты сетевого трафика
	ViPNet CSP	Криптопровайдер, сертифицированный ФСБ РФ как средство криптографической защиты информации (СКЗИ) и электронной подписи
	ViPNet PKI Client	Универсальный клиент для работы в инфраструктуре открытых ключей
 Аладдин	JaCarta	JaCartaUSB-токены, смарт-карты и модули безопасности для промышленной автоматизации, M2M и IoT
 РУТОКЕН	«Плагин»	Электронные идентификаторы, смарт-карты и ПО



Развитие экосистемы Наложенные средства защиты информации

Разработчик ПО	Название ПО	Назначение
	«Соболь»	Программно-аппаратный комплекс для обеспечения доверенной загрузки ОС
	Secret Net LSP	Средство защиты информации от несанкционированного доступа для ОС семейства Linux
	ViPNet SafeBoot	Высокотехнологичный программный модуль доверенной загрузки уровня UEFI BIOS
	Aladdin Trusted Security Module (TSM)	Доверенная программно-аппаратная платформа с применением технологии TrustZone для Arm-процессоров: средство доверенной загрузки, доверенная среда исполнения (TEE), модуль СКЗИ и электронной подписи, инфраструктура управления ключами и устройствами
	Доверенная среда исполнения	Доверенная среда исполнения позволяет надежно изолировать выполнение критических операций, например, работу с криптографическими ключами или контроль целостности основной ОС на мобильных устройствах



Механизм плавной миграции на Baikal-M

Примеры замещаемого ПО



ПО, не требующее замещения





Механизм плавной миграции на Baikal-M

Эксперты Baikal Electronics разработали механизм плавной миграции, который позволит клиентам перейти на отечественное оборудование с минимумом затрат и без остановки рабочих процессов.

3 месяца
Базовый срок миграции

1 неделя



Анализ используемых заказчиком программно-аппаратных комплексов и разделение их на группы пользователей

2-3 недели



Выявление групп программного обеспечения:

- Общесистемное
- Прикладное
- Офисное
- Средства защиты информации
- Информационные системы



Выявление аппаратных групп:

- Автоматизированные рабочие места пользователей
- Серверные и СХД-группировки
- Периферийное оборудование
- Сетевое оборудование

2 недели



Формирование перечня уже имеющихся совместимых решений, при необходимости — подбор аналогов, а также способов их запуска

Определение оптимального для задач заказчика сценария применения решения: автономный, терминальный/VDI или гибридный

4 недели



Проведение пилотного проекта для выбранных групп пользователей, выявление проблемных зон и их устранение

2 недели



Подведение итогов пилотного проекта и формирование предложений по внедрению решений

Эльбрус

VLIW - сверхдлинное командное слово

1. Можно попробовать компилятор

<https://ce.mentality.rip/>

2. Физическая машина в музее Яндекса

Пример ассемблерного кода

square(int):

{ nop 5

setwd wsz = 0x4, nfx = 0x1, dbl = 0x0

return %ctpr3

 muls,3 %r0, %r0, %g16

}

{ ct %ctpr3

 sxt,3 0x2, %g16, %dr0

}

До 6 арифметико-логических операций за такт

{

 muls,3 %r0, %r0, %g16

 и другие в фигурных скобках

(Условия Бернстайна нужно выполнять)

 MIMD архитектура

}

Регистровый файл (256 регистров)

%g — глобальные регистры (32)

Помимо них доступны:

8 входных регистров

8 локальных регистров

8 выходных регистров

Предикаты

32 двухразрядных регистра.

1 разряд тип (диагностический/логический

1 разряд значение

Сохраняются с процедурой

Control Transfer Preparation

Может быть, я пойду туда ctp %ctpr3
... или сюда....ctp %ctpr2
....я определился, пойдём туда: ct %ctpr3