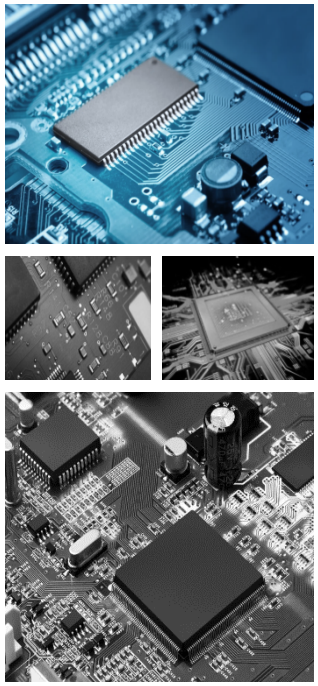
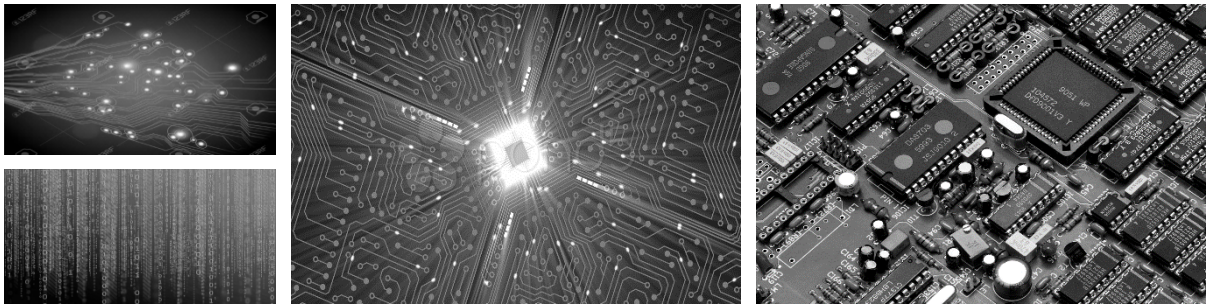


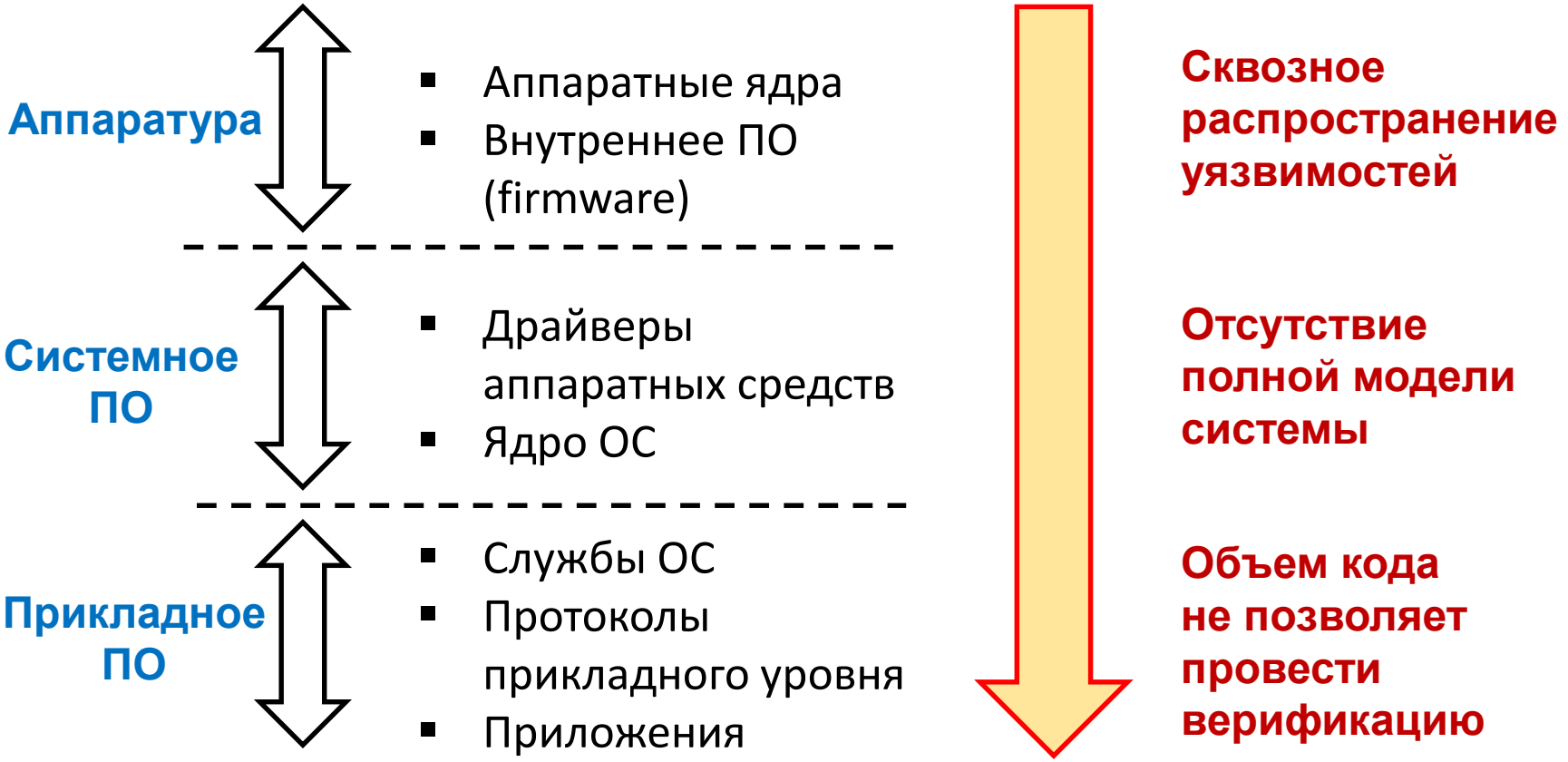


Базовые технологии проектирования доверенных вычислительных систем

г. Санкт-Петербург,
23 марта 2017 г.

Борис Кривошеин
Исполнительный директор ООО «ИнЧип Технологии»

Программно-аппаратный стек и угрозы безопасности



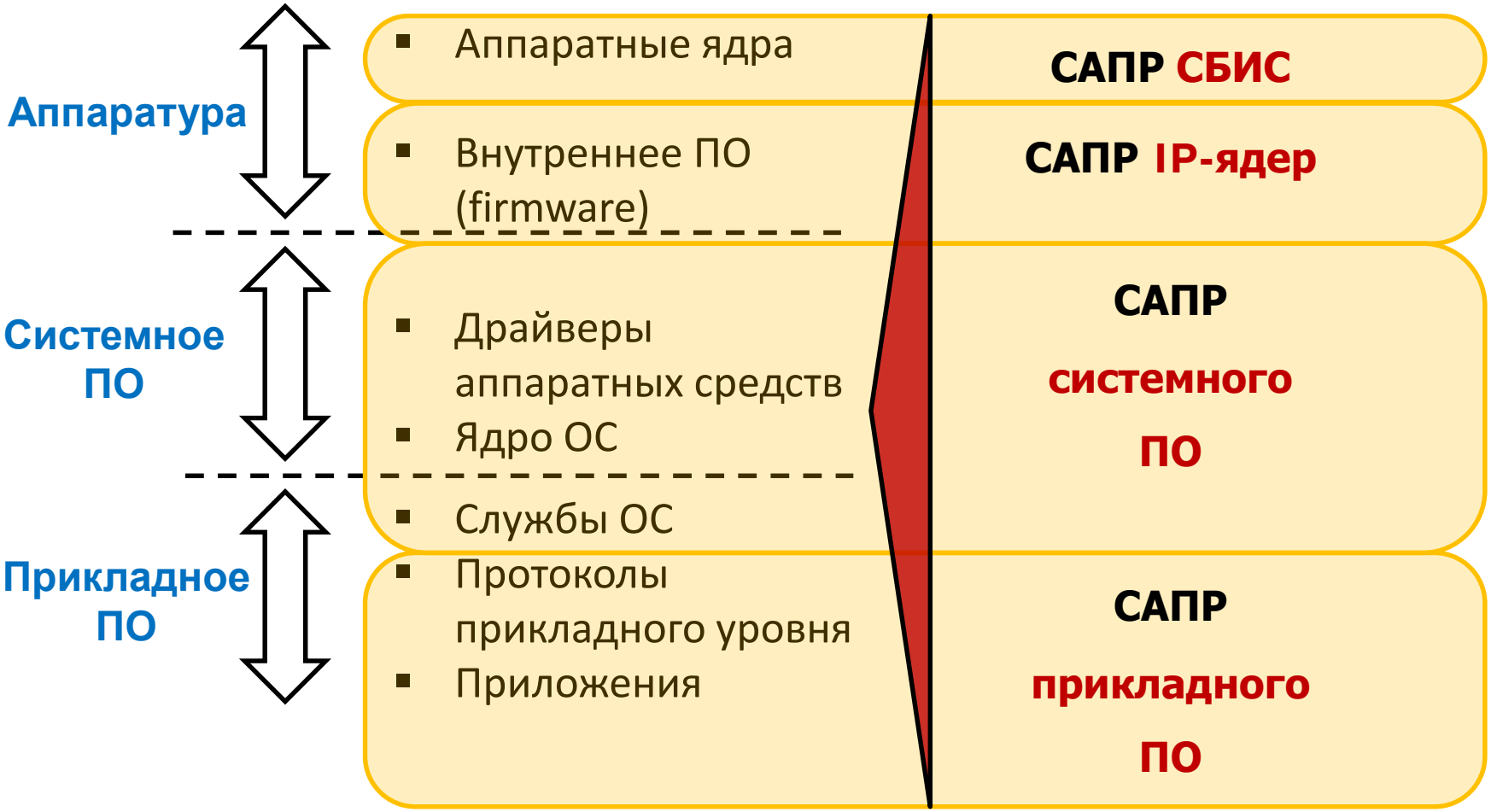
Оценочный уровень доверия к ПО *(ОУД/SEL 1-7)* – факты:

- SEL 4 – большинство операционных систем (… Windows 10)
- SEL 5 – библиотеки модулей защиты информации
- SEL 6 – ОС РВ «Integrity-178B», отдельные программные модули
- SEL 7 – Микроядро ОС «seL4», аппаратные элементы защиты

«Открытое ПО»:

- В основном – без оценки уровня доверия
- Некоторые реализации – до уровня SEL 4
- Отдельные исключения – до SEL 7, но для единственной версии без обновлений

Корневой элемент доверенности: средства разработки



Угрозы безопасности со стороны САПР

- Теоретическая возможность – обоснована в 80-х годах XX века *(Reflections on Trusting Trust, Ken Thompson, 1984)*

- Атаки с использованием САПР – реальность в XXI веке
  - Инцидент с внедрением в исходный код компилятора ОС FreeBSD на серверах компании кода для получения несанкционированного доступа к транслированному ПО - 19.09.2012 г. (обнаружено 11.11.2012 г.)

- Не декларированные возможности САПР – правило, а не исключение
  - Инцидент с транслятором Visual Studio C++ 2015 (Update 2, Win 7/10)

Вход:

```
#include "stdafx.h"
#include <iostream>
int main()
{
   return 0;
}
```

Выход:

вызов функции “**telemetry_main_invoke_trigger**”

Компоненты доверенной среды проектирования

- Средства описания, моделирования и анализа архитектуры системы
- Средства безопасной интеграции доверенных компонентов системы
- Средства автоматического синтеза кода из спецификаций системного уровня
- Средства автоматизированного тестирования кода с контролем покрытия
- Средства проверки временных ограничений в системах реального времени
- Средства верификации кода с учетом требований безопасности
- Средства применения аппаратных механизмов защиты целевой платформы
- Средства автоматизированного контроля и документирования процессов разработки, отладки и верификации ПО
- Средства визуализации модели системы, ее компонентов и атрибутов
- Средства реализации защиты интеллектуальной собственности

Контакты

ООО «ИнЧип Технологии»
Россия
105005 Москва
ул. Радио 24 к.1
T +7 499 281 65 63
E contact@inchip.tech
http://www.inchip.tech