ИНТЕГРИРОВАННАЯ БЕЗОПАСНОСТЬ, КАК ЧАСТЬ ЖИЗНЕННОГО ЦИКЛА ДОВЕРЕННОЙ СРЕДЫ

Корольков Сергей
Компания «ТрастЛаб»

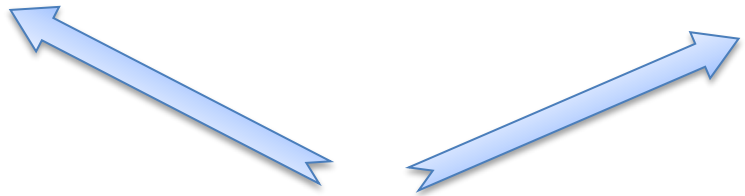
ИНТЕГРИРОВАННАЯ БЕЗОПАСНОСТЬ

Угрозы

- Уязвимости прошивок и АО
- Утечки через встроенное ПО и СФ блоки
- НДВ в АО и встроенном ПО
- Манипулирование параметрами работы

Возможности

- Доверенная загрузка и корень доверия
- Изолированная среда для критических функций
- Безопасная среда для СКЗИ
- Защищенное хранение данных
- Контроль работы на аппаратном уровне
- Мониторинг и управление



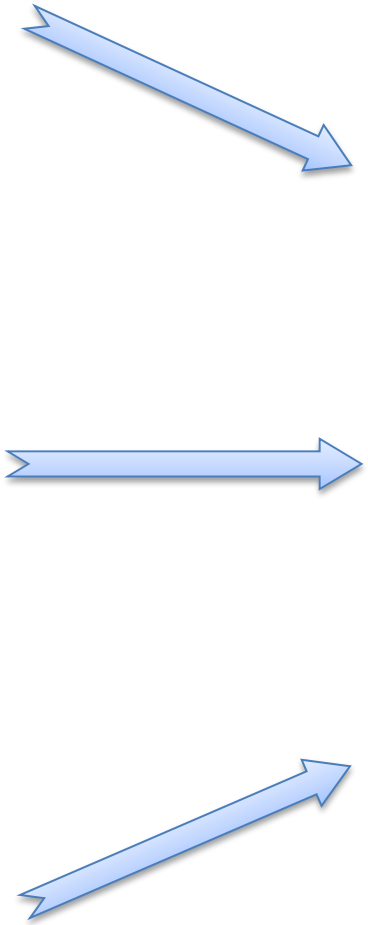
Развитие технологий

- Информационные системы «теряют» границы
- Все взаимодействует со всеми
- Рост и развитие интегрированных возможностей
- Автономные системы и «умные» устройства
- Смещение в сторону аппаратных возможностей

Интегрированная безопасность как предметная область

ОБЛАСТЬ ИНТЕГРИРОВАННОЙ БЕЗОПАСНОСТИ

- Реализация функций безопасности
  - Корень доверия
  - Доверенная загрузка
  - Среда для критических функций
  - Криптомодули
  - Доверенное хранилище
  - Контроль состояния
  - Отключение недоверенных блоков
- Служебные функции
  - Управление критическим АО
  - Удаленное управление
  - Мониторинг
- ЖЦ в процессе эксплуатации
  - Обновления
  - Вывод из эксплуатации



ПО пользователя

- Пользовательские приложения
- API и сервисы
- Драйверы
- Пользовательская ОС
- Загрузчик пользовательской ОС

Встроенное ПО

- UEFI/BIOS
- Опциональные приложения безопасности
- **Приложения безопасности**
- API и сервисы (опционально)
- Драйверы (опционально)
- ОС (опционально)
- Начальный загрузчик устройства

Служебное АО

- AMT/IMM и др.
- Служебные ядра СнК
- **ARM TZ**
- **TPM**
- **Криптомодули, RNG**
- **OTP, eFuse, таймеры и др.**

Область интегрированной безопасности

ДОВЕРИЕ vs БЕЗОПАСНОСТЬ vs ЖИЗНЕННЫЙ ЦИКЛ

Доверенная система:

система, которая в изменяющихся условиях функционирует так, как она была запроектирована без ухудшения характеристик защищенности и устойчивости (в том числе к атакам)

Доверенное

- Безопасность процедур разработки
- Глубина верификации (сертификации)
- Достаточность функции безопасности
- Отсутствия ограничений на использование

Безопасное

- Устойчивое к атакам
- Доверено загруженное
- Целостные критические компоненты
- Верифицированное состояние

Российское

- Возможности глубокой верификации
- Отсутствие ограничений на использование

Доверенный жизненный цикл

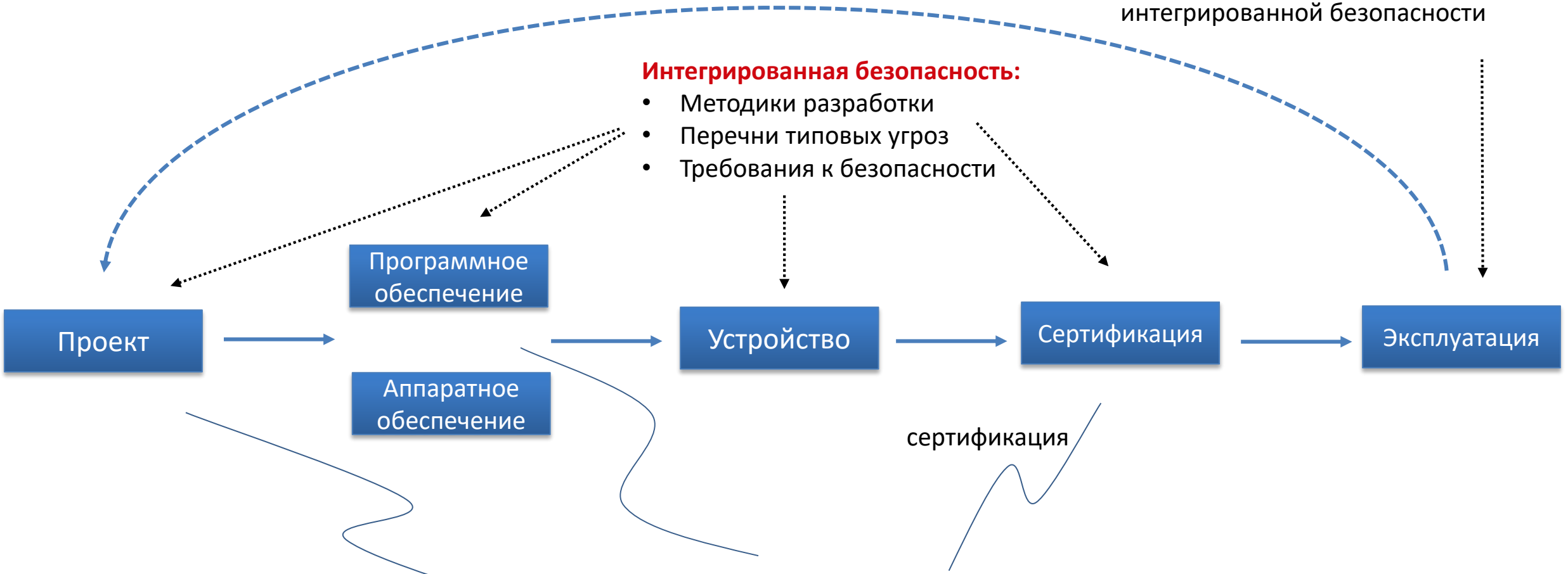
ЖИЗНЕННЫЙ ЦИКЛ

Приказ №239, №17…

- Требования к задействованию средств интегрированной безопасности

Интегрированная безопасность:

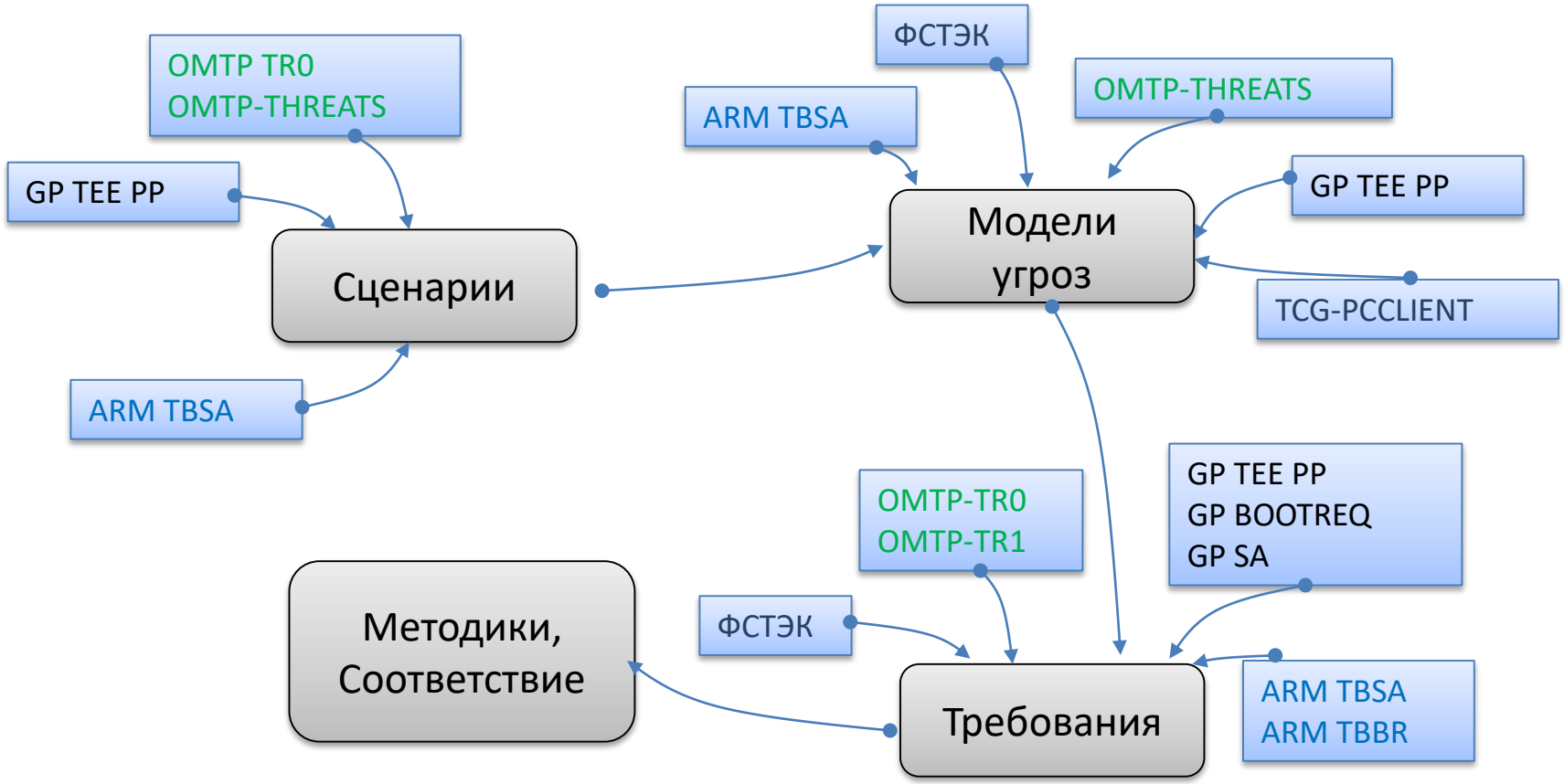
- Методики разработки
- Перечни типовых угроз
- Требования к безопасности



Требования к доверию:

- Требования к разработке
- Проверка программного обеспечения
- Проверка аппаратного обеспечения

ОБЩЕДОСТУПНЫЕ МИРОВЫЕ ПРАКТИКИ



Имеются наработки по анализу угроз и требований в области интегрированной безопасности

АКТИВНОСТЬ АССОЦИАЦИИ «ДОВЕРЕННАЯ ПЛАТФОРМА»

Высокотехнологичные аппаратные угрозы

- Угроза компрометации передаваемых по внешней шине данных
- Угроза компрометации данных внутреннего ОЗУ
- Угроза НСД ко внутренним ресурсам SoC
- Угроза установки зонда внутрь SoC
- Угроза НДВ в коде лицензируемых блоков SoC
- Угроза установки зонда внутрь SoC

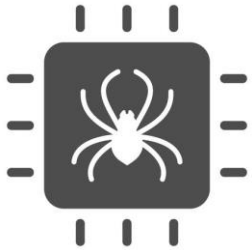
...

Внешние аппаратные угрозы

- Угроза манипуляция параметрами производительности
- Угроза искажения данных в ОЗУ
- Угроза утечки информации через LED
- Угроза подмены внешних Flash карт
- Угроза утечки информации через LCD (и др. DMA)
- Угроза вредоносного контроллера на шине
- Угроза обхода защиты путем отключения внешнего питания
- Угроза обхода защиты путем ограничения параметров питания

...

Угрозы встроенного ПО



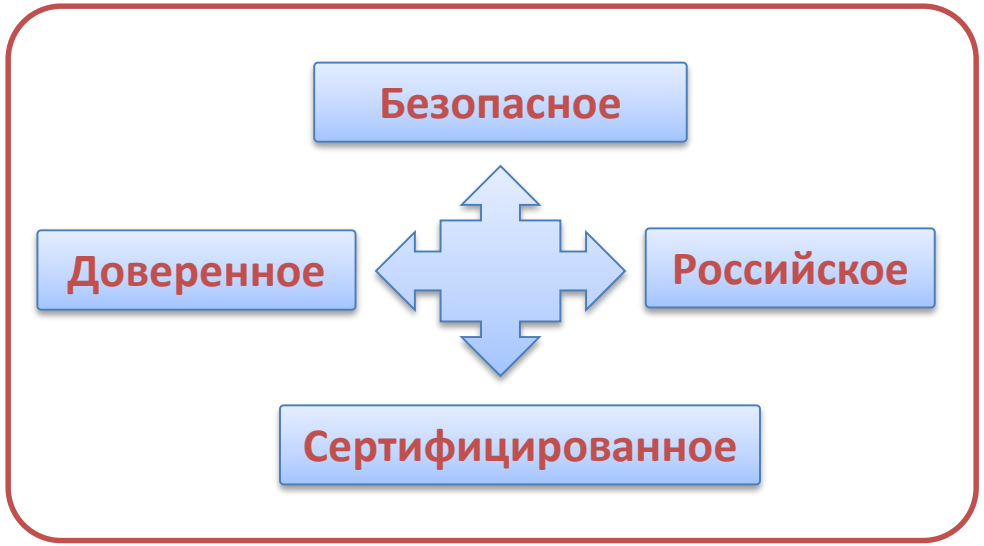
- Угрозы реализации уязвимостей ПО
- Угроза искажения данных периферийных устройств
- Угрозы нарушения процедур обновления
- Угроза НСД к данным и буферам обмена
- Угрозы невозможности обновления
- Обхода изоляции памяти
- Угрозы обхода процедур загрузки
- Утечки данных нетрадиционным путем

...

НМД ДОВЕРЕННЫЙ ЖИЗНЕННЫЙ ЦИКЛ

Назрела необходимость регулирования вопросов доверенного жизненного цикла:

- Структурирование вопросов разработки доверенной ЭКБ
- Нормативное регулирование в области интегрированной безопасности
- Гармонизация с НМД в области доверия
- Гармонизация с регуляторными документами по импортозамещению



Вопросы