РусКрипто XXVIII научно-практическая конференция

Компания Актив

Обеспечение доверенной среды обновления микропрограммы в условиях дефицита аппаратных ресурсов

Инновационный метод поэтапной перезаписи
как стандарт надежности и экономии ресурсов.

Дмитрий Овтин

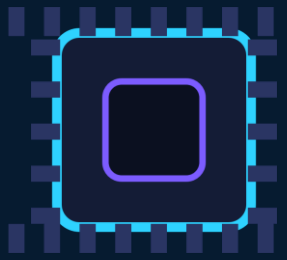
Инженер-программист,
Компания «Актив»

Специфика Bare Metal систем и вызовы обновления

Ключевые особенности и ограничения

- Отсутствие ОС: минимум сервисов, нет файловой системы, нет диспетчера задач.
- Выполнение кода в бесконечном цикле (main loop) с обработкой прерываний.
- Сбой при записи во FLASH может превратить устройство в «кирпич».
- Главное ограничение: малый объём FLASH не позволяет держать «лишний» образ прошивки.

Интуиция риска



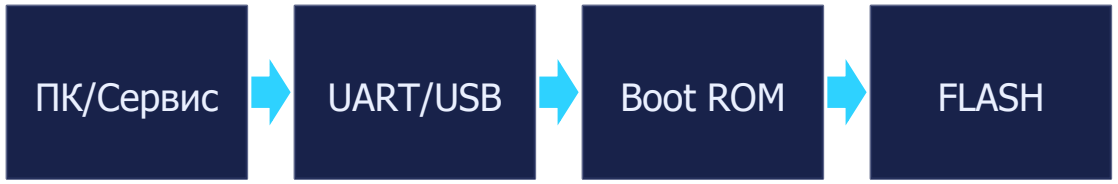
```
main()
while(1) {
  …
}
```

При ошибке записи FLASH → потеря кода

Традиционные методы: In-System Programming (ISP)

Суть

Программирование через встроенный заводской загрузчик (например, UART / USB).



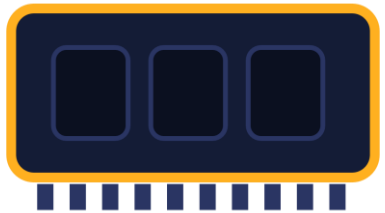
Минусы

- Требует физического присутствия (манипуляции с выводами BOOT).
- Система находится в режиме offline.
- Часто требуется полное стирание чипа.

Вывод: ISP надёжен, но плохо подходит для удалённых и частых обновлений.

Стратегии IAP: выполнение из RAM и внешняя память

RAM Execution



Функции записи копируются в ОЗУ и выполняются оттуда.

Минус:
катастрофически низкая отказоустойчивость при сбое питания — FLASH может содержать повреждённый образ.

External Storage

Использование внешней микросхемы памяти для хранения образа.

Минусы:
- дополнительные аппаратные ресурсы
- длительный простой (downtime)
- при копировании образа

Двухбанковая архитектура (Dual Bank)

Идея

Разделение FLASH-памяти на два идентичных блока: Банк 1 и Банк 2.

Банк 1 (текущий)

Банк 2 (новый)

Преимущества:

- Бесшовное обновление (в т.ч. OTA).
- Возможность отката на предыдущую версию.

Критический минус: требуется удвоение объёма FLASH.

Почему это не работает на малой FLASH

На контроллерах с ограниченным объёмом памяти двухбанковая схема физически невозможна:

- нет места под второй полный образ
- требуется переход на более дорогие МК.

Решение: метод разделения на две части (патент)

Суть подхода:

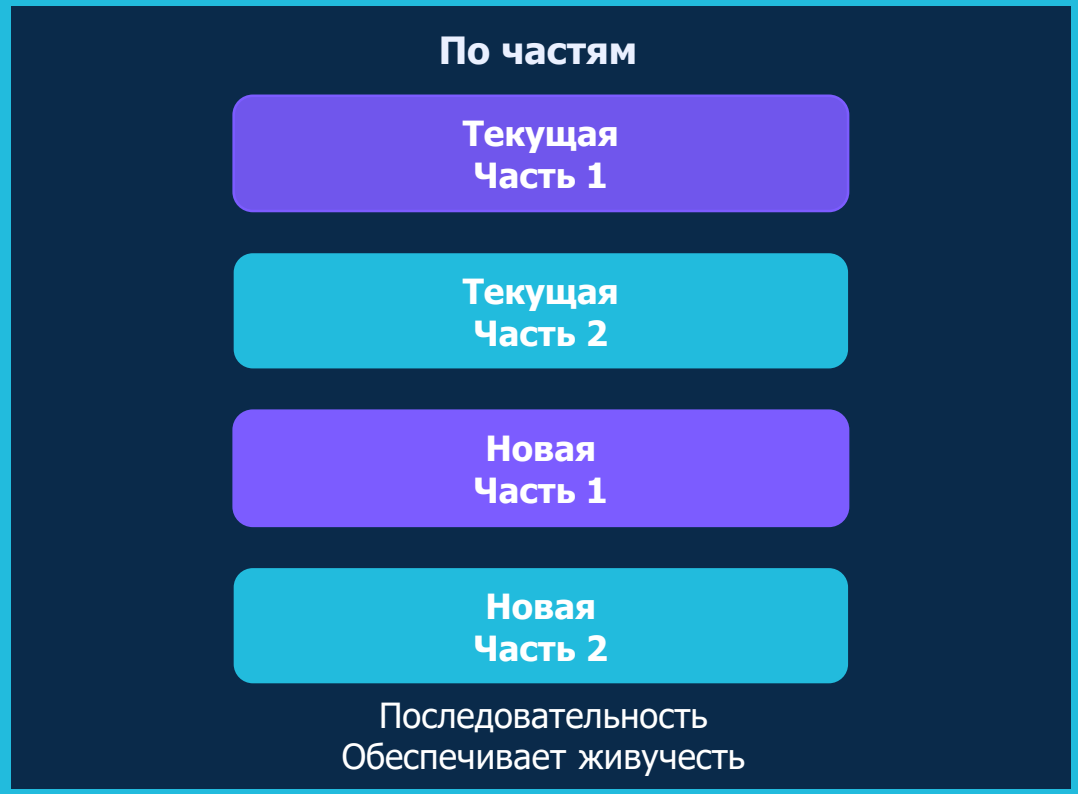
- Поэтапная запись новой прошивки по частям с частичным сохранением текущей в процессе.
- Устройство всегда сохраняет минимально достаточный код для продолжения обновления.
- Цель: безопасное обновление при существенно ограниченных ресурсах FLASH.

Интеллектуальная собственность.

Метод защищён патентом (RU2845340C1).

Ключевая идея: *«обновляться, не теряя возможность обновляться».*

Наглядно:



Распределение FLASH-памяти в методе

4 функциональные области:

1. Загрузчик (первичное программирование).
2. Первая часть текущей прошивки (базовый функционал).
3. Вторая часть текущей прошивки (основной функционал).
4. Пользовательские данные.

Карта памяти (пример логики)

Важно: объём под «временную область» получается за счёт очищения части 2 на первом этапе.

Процесс обновления: стадия 1

Стадия 1	Стадия 2	Стадия 3

Стадия 1: Загрузка новой первой части микропрограммы

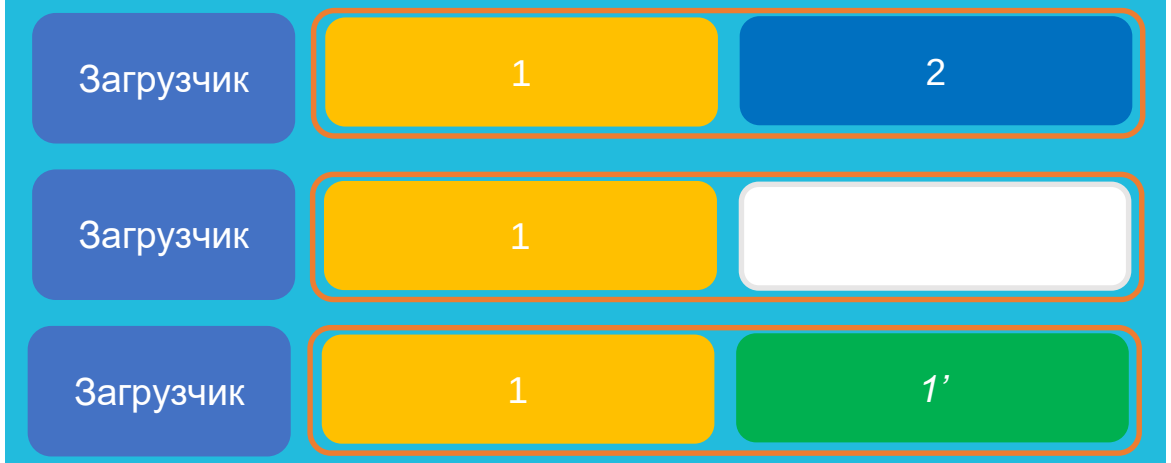
Очистка области второй части прошивки силами первой части (минимальный код обновления всегда доступен).

Загрузка первой части новой прошивки во временную (очищенную) область.

Далее выполняется:
проверка целостности и подлинности

Только после успешной верификации двигаемся дальше.

Последовательность действий



Процесс обновления: стадия 2

Стадия 1 | **Стадия 2** | Стадия 3

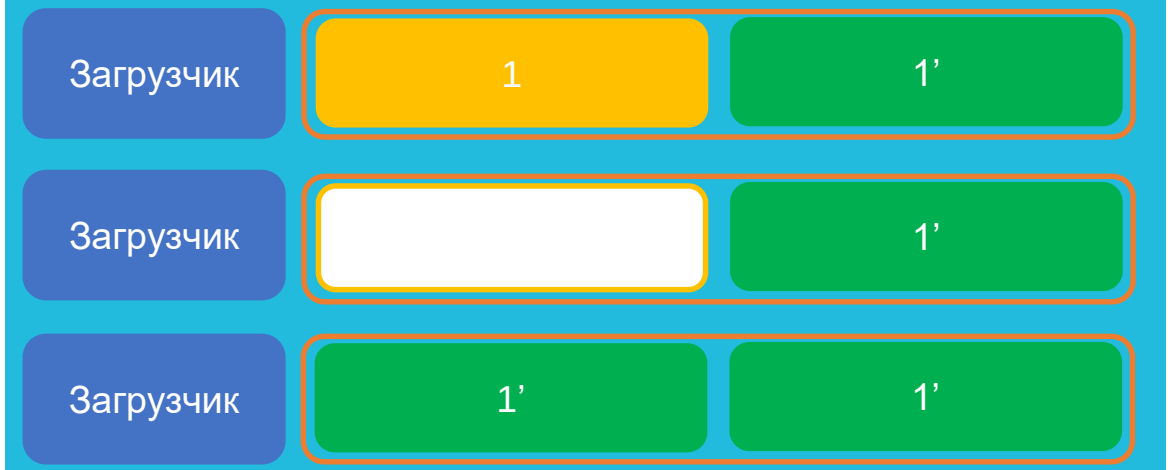
Стадия 2: Установка новой первой части

Управление передается загрузчику.

Копирование новой первой части на свое место.

Критично: загрузчик — минимальный и максимально проверенный компонент.

Последовательность действий



Процесс обновления: стадия 3

Стадия 1 | Стадия 2 | **Стадия 3**

Стадия 3: Загрузка новой второй части микропрограммы

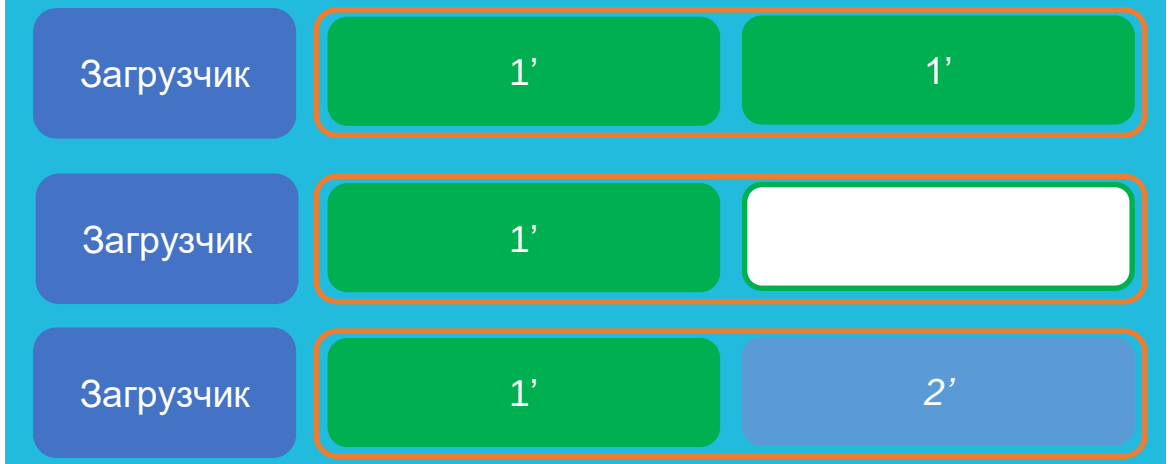
Обновленная первая часть загружает вторую часть новой прошивки.

После записи и проверки:

- переключение в обычный режим
- очистка статуса обновления
- продолжение работы устройства.

RUN

Последовательность действий

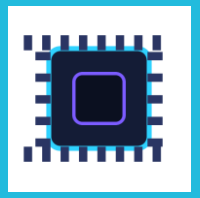


Преимущества двухэтапного метода

Что даёт метод:

- **Нет дублирования кода:**
  исключается избыточность функционала.
- **Экономия ресурсов:**
  уменьшается необходимый объём FLASH-памяти.
- **Безопасность:**
  устройство остаётся в режиме обновления до успешного завершения (невозможно «сломать»).
- **Гибкость:**
  исправление багов вплоть до уровня работы с периферией.

Фокус



Экономия FLASH

Живучесть при сбоях

Минимум downtime

Практический эффект: *выше надёжность → ниже стоимость железа и сопровождения.*

Защита подлинности прошивки

Подпись прошивки

Каждый файл обновления содержит электронную подпись, сформированную закрытым ключом производителя.

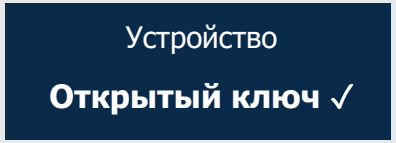
Прошивка не может быть подменена или повреждена без обнаружения.

Проверка на устройстве

На этапе производства в устройство загружается соответствующий открытый ключ для проверки подписи.

При получении обновления устройство проверяет подпись этим ключом.

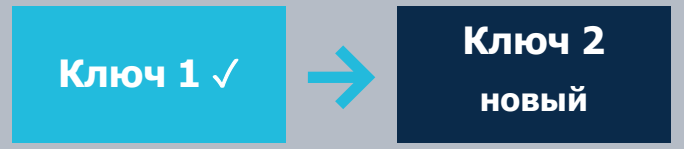
Если подпись не совпадает — обновление отклоняется.



Обновление ключа

До истечения срока действия ключа подписи обновления формируется новая ключевая пара и соответствующий открытый ключ доставляется пользователю в составе файла обновления.

Устройство проверяет, что новый открытый ключ подписан действующим ключом подписи обновления и только потом обновляет его.



Подпись по ГОСТ Р 34.10-2012. Цепочка доверия обеспечивает обновление ключей без физического доступа к устройству

Заключение

Живучесть

Поэтапная перезапись с сохранением минимального кода на каждом этапе.

Защита подлинности

ЭЦП по ГОСТ с цепочкой доверия для безопасного обновления ключей.

Экономия ресурсов

Нет дублирования кода, работает на МК с ограниченной FLASH-памятью.

Надёжное, запатентованное и оптимальное решение для обновления программы микроконтроллеров.

Спасибо за внимание!

ovtin@rutoken.ru
info@rutoken.ru

www.rutoken.ru
www.aktiv-company.ru

+7 495 925-77-90
+7 926 175-75-60

Дмитрий Овтин

Инженер-программист,
Компания «Актив»

КОМПАНИЯ АКТИВ

РусКрипто XXVIII НАУЧНО-ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ