Доверенная загрузка в сетях с доступом к разнокатегорийной информации

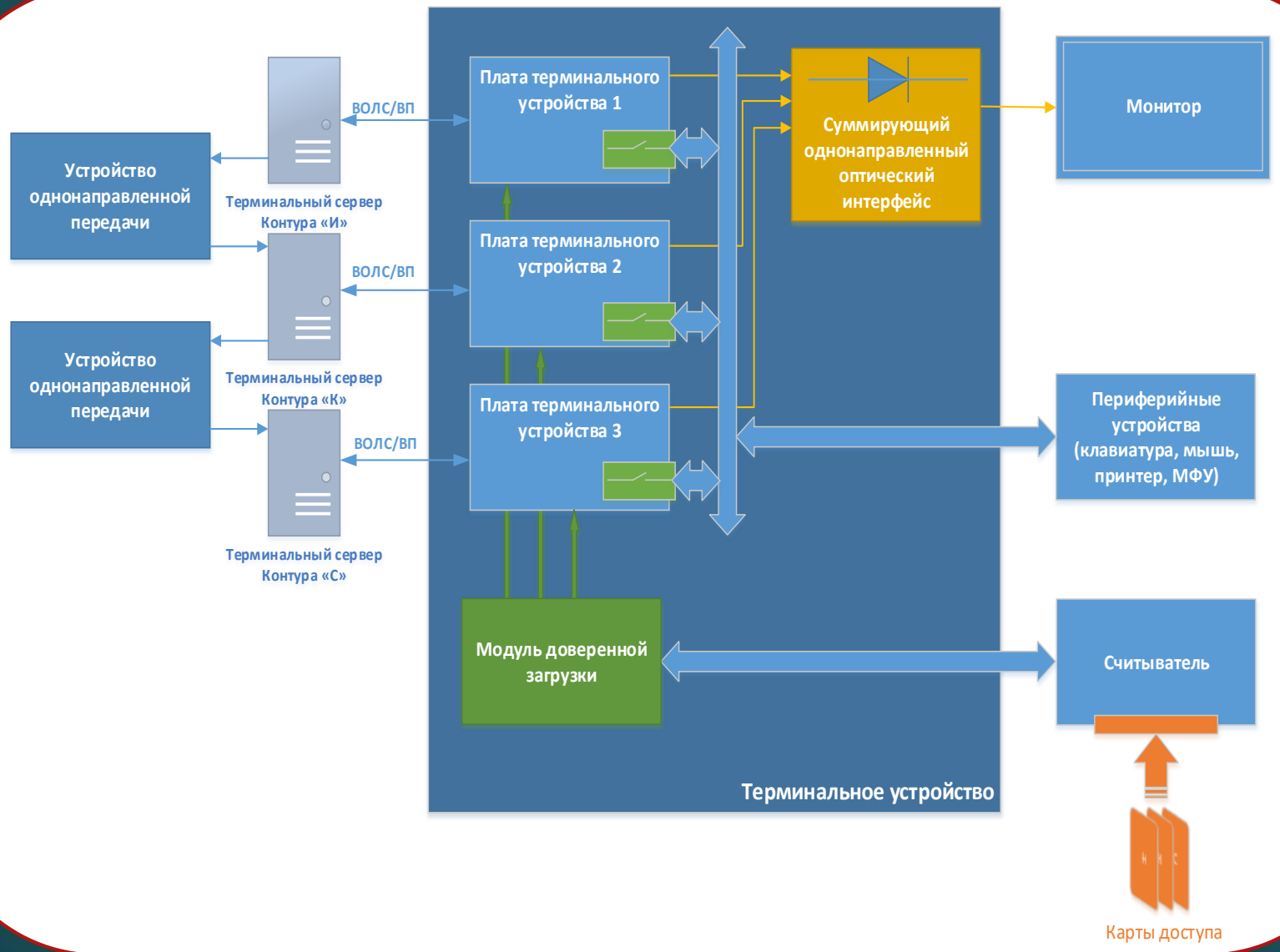
Дмитрий Холопов
holopov@swemel.ru

Антон Черников
chernikov@swemel.ru

Цели и задачи работы

- Создание возможности доступа пользователя к разнокатегорийной информации с одного рабочего места;
- Обеспечение контроля функционирования устройства от момента включения до старта операционной системы;
- Защита от утечки информации, обусловленной наличием аппаратных буферов в оборудовании.

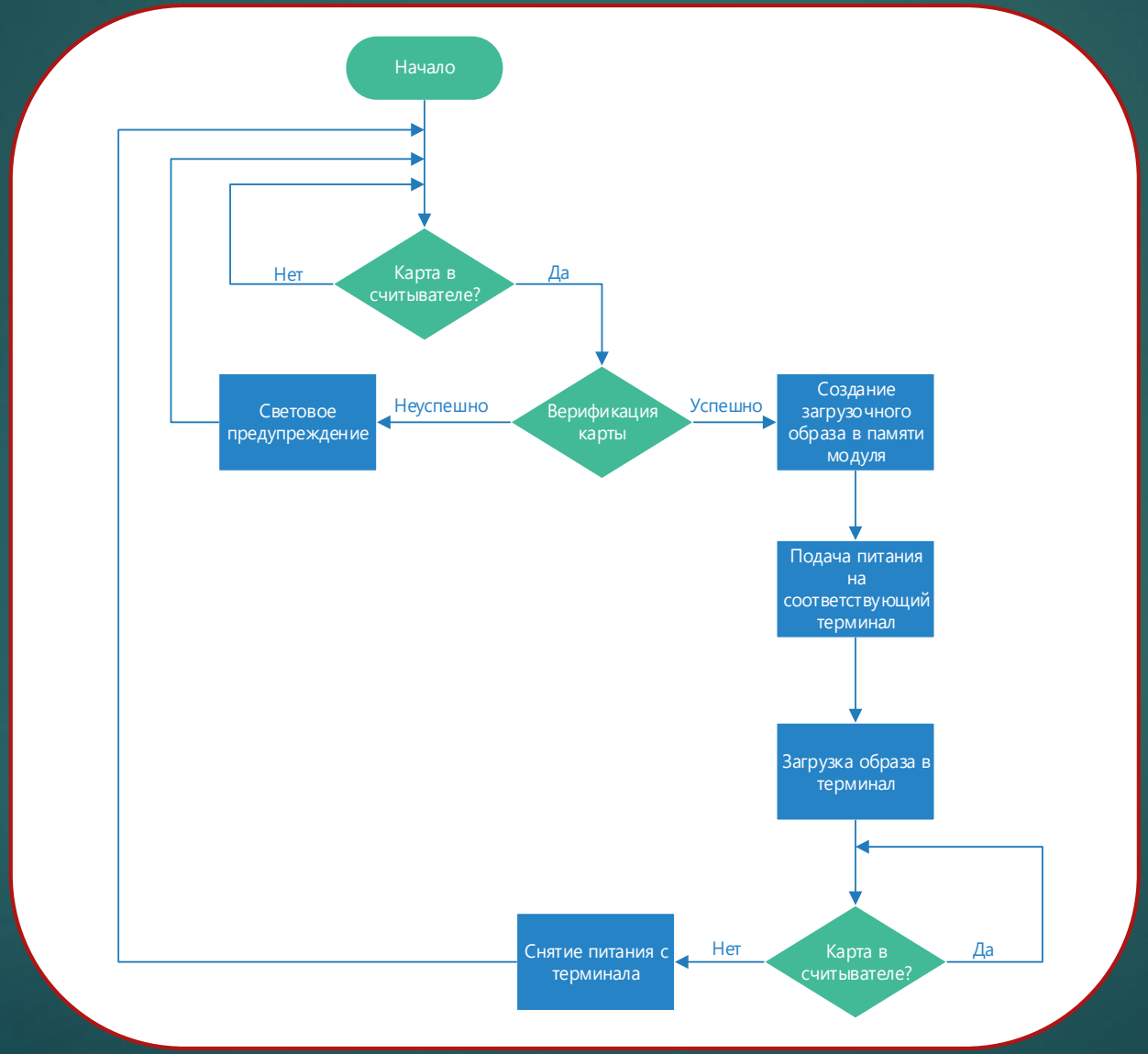
Блок-схема терминального устройства



Структура данных на карте

Карта не содержит загрузочный образ в «чистом» виде. Загрузочный образ формируется модулем доверенной загрузки на основании данных карты.

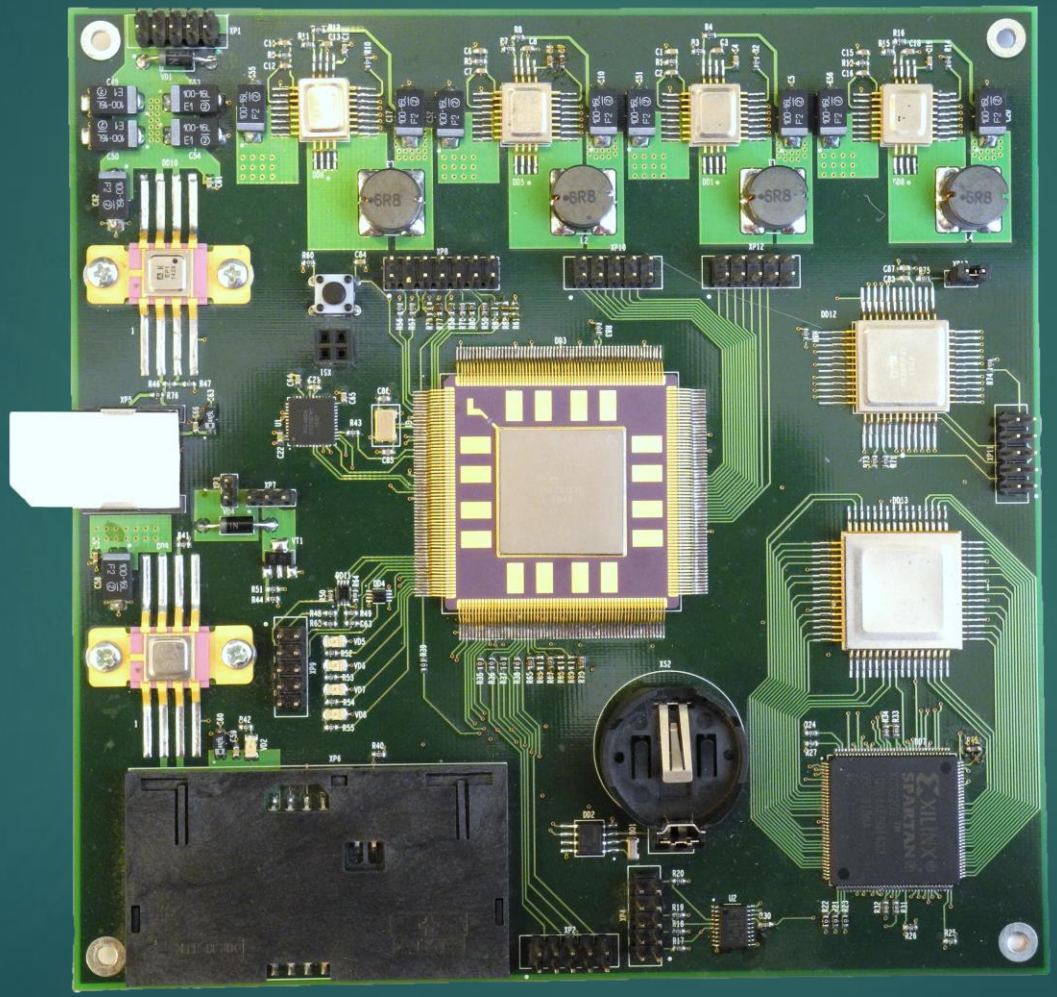
Алгоритм работы



Сложности в реализации

- Особенности интерфейса SPI;
- Отечественная компонентная база;
- Хранение ключевой информации;
- Проблемы объединения видеосигнала.

Модуль доверенной загрузки



МВП SWEMEL

Готовое изделие

МВП SWEMEL

Ключевые особенности

- Аппаратная защита от запуска терминального устройства без достоверной карты;
- Возможность использования подписанного зашифрованного загрузочного кода;
- Контроль целостности загрузочного кода до запуска терминала;
- Использование отечественной элементной базы:
  - ✓ Сертифицированный криптопроцессор Микрон
  - ✓ Микроконтроллер фирмы Миландр
- Автоматическое отключение терминала от сети электропитания при извлечении карты;
- Отсутствие скрытых энергонезависимых «карманов» памяти и дополнительных источников питания;
- Безопасное обновление загрузочного кода (вне защищаемого терминала);
- Устройство защищено патентами.

МВП SWEMEL

РОССИЙСКАЯ ФЕДЕРАЦИЯ

ПАТЕНТ

НА ПОЛЕЗНУЮ МОДЕЛЬ

№ 157843

ТЕРМИНАЛ С КОНТРОЛИРУЕМОЙ ЗАГРУЗКОЙ BIOS С ВНЕШНЕГО НОСИТЕЛЯ

Патентообладатель(ли): ***Закрытое акционерное общество "Многопрофильное внедренческое предприятие "СВЕМЕЛ" (ЗАО "МВП "СВЕМЕЛ") (RU)***

Автор(ы): ***см. на обороте***

Заявка № **2015113310**

Приоритет полезной модели **10 апреля 2015 г.**

Зарегистрировано в Государственном реестре полезных моделей Российской Федерации ***20 ноября 2015 г.***

Срок действия патента истекает **10 апреля 2025 г.**

Руководитель Федеральной службы по интеллектуальной собственности

Г.П. Ивлиев

МВП SWEMEL

Спасибо за внимание!

Контактная информация
Телефон:**(495) 926-7187**
Факс:**(499) 750-7065**
Эл. почта: **post@swemel.ru**
Адрес:**127254 г.Москва, Огородный проезд, д.5, стр.5**