УДК 004.31, 004.4

Астапенко Г. Ф., Кучинский П. В., Новик М. И., Ращеня Н. А.

# БАЗОВАЯ МОДЕЛЬ АППАРАТНО-ПРОГРАММНОЙ ПЛАТФОРМЫ ЗАЩИЩЕННОГО АРМ АБОНЕНТА

Научно-исследовательское учреждение «Институт прикладных физических проблем имени А.Н. Севченко» Белорусского государственного университета Минск, Республика Беларусь

Представлены результаты исследований и разработки основных модулей аппаратно-программной платформы безопасного автоматизированного рабочего места (АРМ) абонента системы обработки конфиденциальных данных. Задачей является разработка гибкой защищенной системы, которая может легко перенастраиваться на варианты мобильного персонального ассистента и автономного встроенного устройства обработки и передачи мультимедийных конфиденциальных данных.

**Архитектура аппаратной платформы**

На рисунке 1 приведена общая схема состава предлагаемой аппаратной платформы. В качестве основы аппаратуры (процессорного блока) был выбран многоядерный процессор TI TDA4VM [1].

Система на чипе (SoC) TDA4VM является частью платформы архитектуры Multicore SoC. Система спроектирована как устройство с низким энергопотреблением, высокой производительностью и высокоинтегрированной архитектурой, обеспечивающей значительное улучшение вычислительной мощности, графических возможностей, обработки видео и изображений, виртуализации. Кроме того, эта SoC поддерживает самые современные функции функциональной безопасности.

Некоторые из основных отличительных характеристик устройства:

• 64-разрядная архитектура с поддержкой виртуализации и когерентной памяти, в которой используются все вычислительные возможности 64-разрядного процессора.

• Полностью программируемые промышленные коммуникационные подсистемы, обеспечивающие новые стандарты гигабитных чувствительных ко времени сетей.

• Интеграция аппаратных ускорителей обработки машинного зрения для удовлетворения обширных требований к обработке при низком энергопотреблении для приложений машинного зрения.

• Интеграция цифрового сигнального процессора (DSP) с фиксированной и плавающей запятой нового поколения, который значительно увеличивает мощность при решении широкого круга общих задач обработки сигналов.

• Надежная архитектура защищенности с изолированным контроллером безопасности, управляющим всеми безопасными конфигурациями, с высокопроизводительной схемой обмена сообщениями клиент-сервер между защищенным контроллером и всеми ядрами.

Одним из основных вариантов использования аппаратной платформы является выполнение функций процессорного блока мобильного персонального компьютерного ассистента (ПКА) и автономного встроенного устройства обработки и передачи мультимедийных конфиденциальных данных.

Особенностью предлагаемой архитектуры на (рисунок 1) является ее гибкость (в том числе применение в качестве процессорного блока как TDA4VM [1], так и AM438x [2]). Если предполагается использовать ПКА в качестве мобильного компьютера, имеется возможность подключить к процессорному блоку мини-дисплей, камеру, аудио систему, а также подсоединиться к сети Ethernet. Если ПКА применяется как компактное мобильное устройство, предоставляется возможность использовать ЖК-дисплей с сенсорным экраном, X16 клавиатуру, сотовый модем и/или WiFi адаптер. Если необходимо использовать ПКА в качестве автономного встроенного модуля (например, в инфраструктуре IoT), то имеется возможность подключить к процессорному блоку ряд вспомогательных сенсорных плат и датчиков через соответствующие коннекторы.

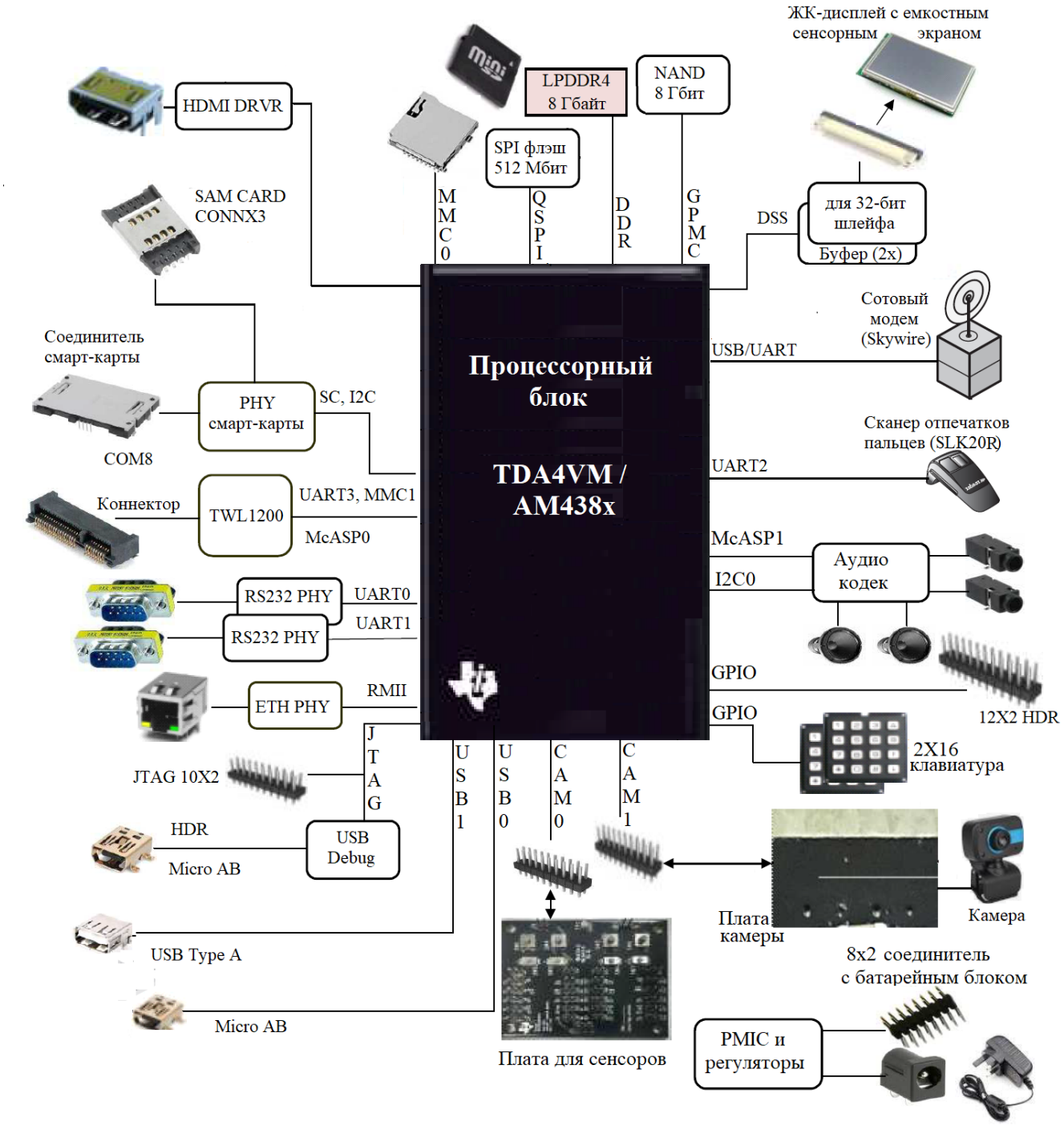


Рисунок 1 – Блок-схема варианта аппаратной реализации персонального ассистента

**Реализация схем безопасности встроенной системы**

Хотя интегральные схемы (ИС), такие как микроконтроллеры (MCU), процессоры и устройства беспроводной связи, не представляют собой законченное решение для защиты приложения, они могут предоставить строительные блоки, которые можно использовать для включения функций безопасности в приложение. Можно разделить эти функции на ряд категорий [3], относящиеся к приложениям. Эти категории – «средства обеспечения безопасности». В зависимости от ресурсов, которые нуждаются в защите, и точек уязвимости, рассматриваются все соответствующие средства обеспечения безопасности, с последующим выбором функции безопасности на уровне применяемого устройства и отдельного модуля для разработки соответствующего механизма защиты. На рисунке 2 представлена структура безопасности.


Рисунок 2 – Структура безопасности встроенной системы.

Необходимо отметить, что особенностью предлагаемого построения аппаратно-программных компонент обеспечения безопасности встроенной системы является их распределенный, полуавтономный режим функционирования, позволяющий отслеживать уязвимости и реализовывать блокирующие функции для отдельных модулей, работающих в системе.

Список литературы

1. J721E DRA829/TDA4VM Processors. Technical Reference Manual, TI. – 2022. – 3513p.
2. Sitara AM438x processor: tamper protection. TI. – 2017. – 7p
3. Sitara Processor Security: Embedded processor security. TI. – 2019. – 10 p.