пламенное горение происходит по всей глубине ограждений. Расположение горючих материалов, их параметры и газодинамические процессы определяют динамику выгорания помещения.

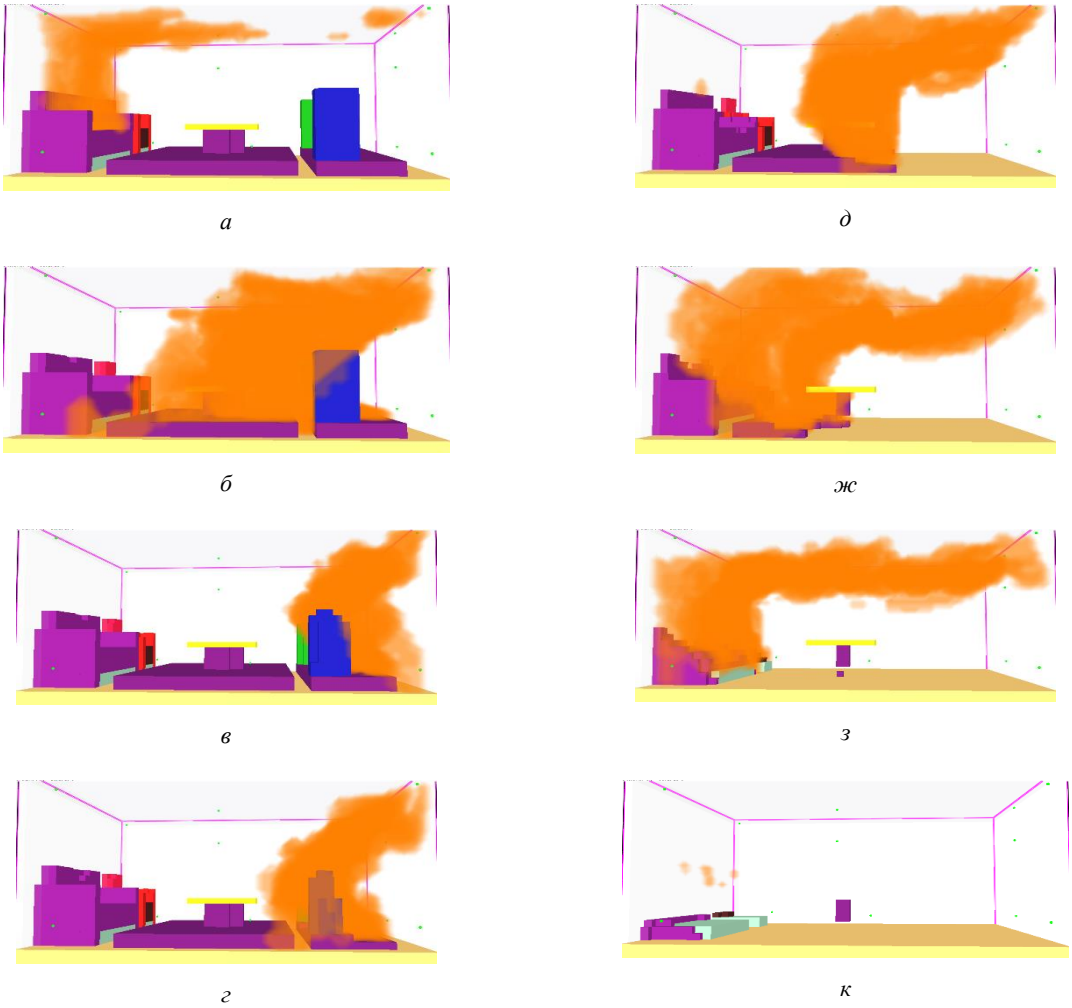

Рисунок 4 – Картины расположения пламенного горения на 99 (*а*), 117 (*б*), 150 (*в*), 186 (*г*), 363 (*д*), 489 (*ж*), 585 (*з*), 786 (*к*) секундах быстрого пожара

Литература

1. Karlsson, B. Enclosure fire dynamics / B. Karlsson, J. G. Quintiere. – CRC Press LLC, 2000. – 317 p.

2. Drysdale, D. Fn introduction for fire dynamics / D. Drysdale. – Third edition : Willey, 2011. – 551 p.

3. Fire Dynamics Simulator (Version 5) Technical Reference Guide Volume 1: Mathematical model, NIST Special Publication 1018-5 / K. McGrattan [et al.]. – MA : Gaithersburg, 2009. – 94 p.

4. Fire Dynamics Simulator (Version 5). User's Guide, NIST Special Publication 1019-5 / K. McGrattan [et al.]. – MA : Gaithersburg, 2009. – 176 p.

УДК 004.31, 004.4

ПОРТАТИВНЫЙ ЗАЩИЩЕННЫЙ КОММУНИКАЦИОННЫЙ МОДУЛЬ

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

НИУ «Институт прикладных физических проблем имени А.Н. Севченко» БГУ
Минск, Республика Беларусь

Аннотация. Представлена базовая архитектура и аппаратно-программное обеспечение портативного защищенного коммуникационного модуля (ПЗКМ). Модуль позволяет взаимодействовать с другими ПЗКМ посредством беспроводного интерфейса WiFi-Direct в распределенной P2P сети, а также реализовать взаимодействие с персональным коммуникатором удаленной связи (например, смартфоном) для организации защищенных сессий в виртуальной частной (выделенной) сети. Базовая архитектура ПЗМК представляет собой модифицируемый и масштабируемый набор функциональных модулей, обеспечива-

ющих безопасное формирование, обработку и передачу мультимедийных данных. Программные компоненты ПЗКМ организованы в иерархическую структуру взаимодействия от верхнего прикладного уровня до уровня встроенной операционной системы.

Ключевые слова: информационная безопасность, криптографическая защита, защищенный коммуникационный модуль.

PORTABLE PROTECTED COMMUNICATION MODULE

Rashchenia N., Astapenko G., Kuchynski P., Novik M.

A.N. Sevchenko Institute of Applied Physical Problems BSU
Minsk, Belarus

Abstract. The basic architecture, hardware and software of the portable protected communication module (PPCM) are presented. The module interacts with the same modules via a WiFi-Direct wireless interface in a distributed P2P network, interacts with a personal remote communicator (for example, a smartphone) to organize secure sessions in a virtual private network. The basic architecture of the PPCM is a modifiable and scalable set of functional modules that ensure the safe formation, processing and transmission of multimedia data. The software components of the PPCM are organized in a hierarchical structure of interaction from the upper level of application software to the level of the embedded operating system.

Key words: information security, cryptographic protection, protected communication module.

Адрес для переписки: Ращеня Н.А., ул. Академика Курчатова, 7, г. Минск 220045, Республика Беларусь
e-mail: rashchenia@bsu.by

Архитектура портативного защищенного коммуникационного модуля (ПЗКМ). ПЗКМ представляет собой компактное устройство, которое в одном из прикладных применений может служить надежным, безопасным ассистентом пользователя при формировании, передаче и приеме конфиденциальной информации. На рис. 1 представлен функциональный состав основных компонентов ПЗКМ.

Ядром модуля является процессор TIAM4378 [1] на основе ARM архитектуры. Он содержит блоки обработки данных, их хранения, а также периферийный узел, осуществляющий интерфейс связи с внешними источниками и приемниками потоков данных и сигналов.

Несмотря на то, что внутри процессора находится встроенный криптомодуль, для повышения надежности и безопасности ПЗКМ содержит дополнительные аппаратные модули криптоускорителя и физического генератора случайных числовых последовательностей (ГСЧП). Модуль криптоускорителя реализует арифметические и алгебраические функции обработки больших чисел, а также операции над точками эллиптической кривой. Блок контроля доступа к критической информации дополнен устройством кнопочного набора ПИН-кода.

Для реализации беспроводного интерфейса на основе технологии WLAN используется комбинированный (WiFi/Bluetooth) чип TI – WL1835 MODCOM8B [2], а для реализации беспроводной связи ближнего поля (в пределах 10 см) (NFC) – чип TITRF7970A [3].

Для обеспечения средствами мультимедийной обработки данных ПЗМК содержит встроенные модули: аудио кодек, видео камера, LCD панель и сенсорный экран.

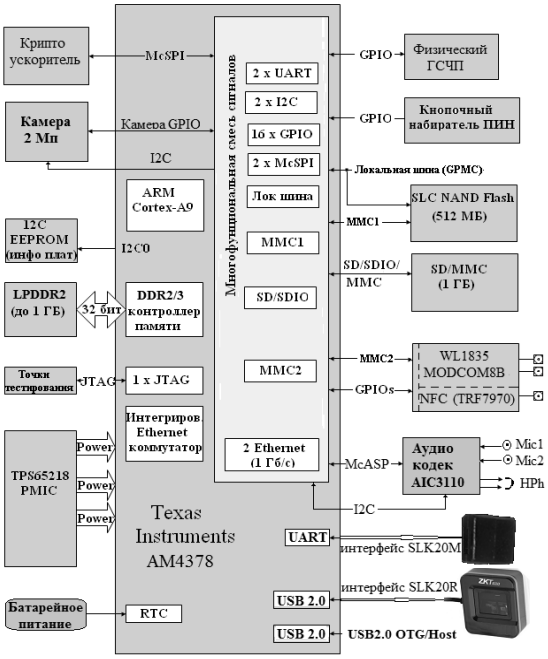

Рисунок 1 – Функциональные компоненты ПЗКМ

Для реализации сервиса безопасности процедур локальной и удаленной аутентификации ПЗКМ дополнен встроенным компонентом сканирования и обработки отпечатков пальцев SLK20M/SLK20R фирмы ZKTeco, взаимодействие с которым на аппаратном уровне осуществляется через последовательный интерфейс UART (115200 бит/с) – для SLK20M, или через интерфейс USB 2.0/1.1 – для SLK20R. Основными критериями выбора данных модулей среди других подобных моделей от различных производителей, являются: высокие технические характеристики; обеспечение программным инструментарием

(SDK) и соответствующей документацией; поддержка защиты от подделок отпечатков.

Алгоритмическое и программное обеспечение защищенной передачи данных. Для решения задач обработки и защищенного обмена мультимедийными данными разработано алгоритмическое и программное обеспечение (АПО).

Основой построения АПО является многоуровневый модульный принцип. На рис. 2 представлена иерархия уровней и состав АПО.

Рисунок 2 – Состав АПО

Верхний уровень – модули приложений, затем уровень модулей сценариев и конфигураций, третий уровень – специализированные прикладные библиотечные модули, четвертый – системное программное обеспечение (на основе TIAM437EVMSDK [4]), пятый уровень – встроенные аппаратно-программные компоненты.

ПЗКМ и отдельные модули АПО могут быть использованы, как базовые компоненты, при построении следующих законченных приложений:

Ethernet туннели. Создание и поддержка виртуальных защищенных туннелей передачи конфиденциальных данных между удаленными абонентами, используя открытую Internet-сеть.

VoIP. Поддержка обмена голосовыми сообщениями между удаленными абонентами, при этом генерация и хранение критической (ключевой) информации осуществляется в ПЗКМ.

IoT. Возможность поддержки и подключения к сети Интернета вещей для применения в различных прикладных сферах. При этом реализуется адаптация к уже существующей инфраструктуре и протоколам.

Сенсорный мониторинг. Аппаратно-программная поддержка беспроводных сенсорных сетей для сбора, агрегации и передачи данных.

Мультимедиа обмен. Реализация поддержки защищенного канала обмена мультимедийными данными, возможно в реальном времени.

WBAN (Wireless Body Area Network). Беспроводная передвижная портативная сеть может быть развернута на основе компонентов ПЗКМ для реализации, например, непрерывного мониторинга за состоянием здоровья человека (через соответствующие встроенные датчики).

Сценарии (реализуемые посредством командного языка bash) предназначены для:

– настройки и инициализации соответствующих приложению переменных среды исполнения;

– последовательного запуска цепочки модулей реализации требуемых задач для конкретного приложения.

Конфигурационные компоненты используются для статической предварительной настройки библиотечных модулей и сценариев для конкретного развертываемого приложения.

Специализированные прикладные библиотеки, как правило, представляющие собой отдельный законченный проект, обеспечивают прикладной интерфейс с приложениями и утилитой конфигурации, а также связь с соответствующими драйверами и утилитами системного программного обеспечения.

Литература

1. AM437x ARM Cortex-A9 processors – Technical Reference Manual [Электронный ресурс]. –Режим доступа: https://ti.com. – Дата доступа: 01.10.2021.

2. WL18xxMOD WiLink™ 8 Single-Band Combo Module – Wi-Fi®, Bluetooth®, and Bluetooth Low Energy (LE) [Электронный ресурс]. – Режим доступа: https://ti.com. – Дата доступа: 01.10.2021.

3. TRF7970A Multiprotocol Fully Integrated 13.56-MHz RFID and Near Field Communication (NFC) Transceiver IC [Электронный ресурс]. – Режим доступа: https://ti.com. – Дата доступа: 01.10.2021.

4. Processor SDK for AM437x Sitara Processors - Linux and TI-RTOS support, Version: 06.03.00.106 [Электронный ресурс]. – Режим доступа:ti.com. – Дата доступа: 01.10.2021.