Александр Калачев (г. Барнаул)

ДЛЯ МОБИЛЬНЫХ СТРАЖЕЙ: БЕСПРОВОДНОЙ СТАНДАРТ BLUETOOTH LOW ENERGY В СИСТЕМАХ БЕЗОПАСНОСТИ

Учет прихода работников и проверка прав доступа. Автоматическая блокировка оборудования или предупреждение об опасности на промышленном объекте. Слежение за маленьким ребенком в местах скопления людей. Установление местонахождения владельца багажа. Все эти задачи решают ***мобильные системы охраны, контроля и безопасности*** *на базе* ***беспроводных модулей BlueGiga*** *стандарта* ***Bluetooth Low Energy (BLE).***

Пожалуй, одной из наиболее часто встречающихся в повседневной жизни беспроводных сетевых технологий (после сотовой связи) является Bluetooth. Благодаря относительно высоким скоростям передачи данных и неплохим энергетическим показателям технология Bluetooth получила широкое распространение в мобильных электронных устройствах, персональных компьютерах, ноутбуках, беспроводных наушниках, гарнитурах, мультимедийных центрах. Стандарт позволяет поддерживать достаточно разветвленную и сложную сеть устройств. Однако, для применения в сенсорных сетях классический Bluetooth подходит мало из-за значительного для автономных источников питания энергопотребления вследствие особенностей работы стека протоколов.

Технология Bluetooth Low Energy (BLE) [1-3] – Bluetooth 4.0 является технологией беспроводной связи для ближних коммуникаций, разработанной группой Bluetooth Special Interest Group (SIG). В отличие от предыдущих стандартов – Bluetooth 2.0, Bluetooth 2.1 + EDR, Bluetooth 3.0, стандарт BLE изначально ориентирован на применение в системах сбора данных, мониторинга с автономным питанием. В отличие от технологий сенсорных сетей, таких как, ZigBee, 6LoWPAN или Z-Wave, ориентированных на разветвленные распределенные сети с многочисленными передачами данных между узлами сети, Bluetooth Low Energy рассчитан на топологии типа «точка-точка» и «звезда». Основными областями применения BLE являются устройства обеспечения безопасности, управления электроприборами и отображения показаний, датчики с батарейным питанием, домашние медицинские приборы, спортивные тренажеры.

Успех предыдущих версий Bluetooth, подтвержденный массовым применением беспроводных интерфейсов данных стандартов в большом количестве устройств, в том числе – рассчитанных на обычного потребителя, позволяет ожидать аналогичной ситуации и с устройствами, поддерживающими стандарт BLE. В частности IEFT 6LoWPAN Working Group рассматривает BLE как одну из значительных составляющих т.н. «Интернета вещей» (Internet of Things) и разрабатывает спецификацию, позволяющую транслировать пакеты IPv6 посредством BLE [2, 3].

Компания **BlueGiga** является одной из первых компаний, которая начала внедрять технологию Bluetooth Low Energy в своих устройствах. Однорежимные устройства (single-mode) выпускаются с 2010 года, а с 2011 года – и двухрежимные (dual-mode). Ассортимент устройств с технологией Bluetooth Low Energy от BlueGiga позволяет строить на их основе решения для самых различных секторов рынка встраиваемых беспроводных устройств:

- спортивное оборудование и аксессуары – измерители пульса, шагомеры, регистраторы ритма – выполненные в виде наручных часов, браслетов;
- датчики – температуры, влажности, присутствия;
- системы сбора и отображения данных;
- бытовые медицинские устройства – весы, тонометры, глюкометры, датчики температуры, дистанционные устройства вызова (в частности, т.н. «радионяни»);
- устройства бытовой электроники – пульты и консоли управления, беспроводные устройства ввода (мыши, клавиатуры, графические планшеты);
- средства автоматизации – части систем домашней автоматики, в частности, шлюзы между домашней сенсорной сетью и мобильными телефонами с Bluetooth;
- информационные устройства – распространение информации о помещениях, объектах, отделах посредством широковещательных сообщений.

Отдельно можно выделить возможность применения BLE-модулей BlueGiga в устройствах обеспечения безопасности. Это могут быть тревожные кнопки, бесконтактные ключи, выполненные в виде отдельных брелоков или функционирующие на базе мобильных телефонов.

Ряд задач может быть решен на основе обнаружения присутствия других BLE-устройств в радиусе действия сигнала центрального узла. К таким решениям относятся устройства-сигнализаторы, позволяющие обнаруживать удаление владельца от сумочек, багажа, кошельков, портмоне со встроенным BLE-модулем и сигнализирующее ему и окружающим (при необходимости) о потере владельца. Модули серий **BLE111, BLE112** благодаря своим компактным размерам, низкому профилю и малому потреблению позволяют встраивать сигнализирующие устройства непосредственно в предметы (карманы сумочек, корочки кошельков и записных книжек, стенки портфелей). Будучи встроенными в браслеты или брелоки, подобные устройства помогут, к примеру, не потерять ребенка в местах с большим скоплением людей (рынки, вокзалы, супермаркеты, аэропорты). Как бы это ни казалось странным, но такая проблема существует.

Аналогичным образом BLE-устройства могут служить для учета времени прихода/ухода работников: они устанавливаются на входе или выдаются по приходу на работу. Возможна также реализация систем мониторинга присутствия:

- в случае офисного применения – проверка прав доступа работника к дан-

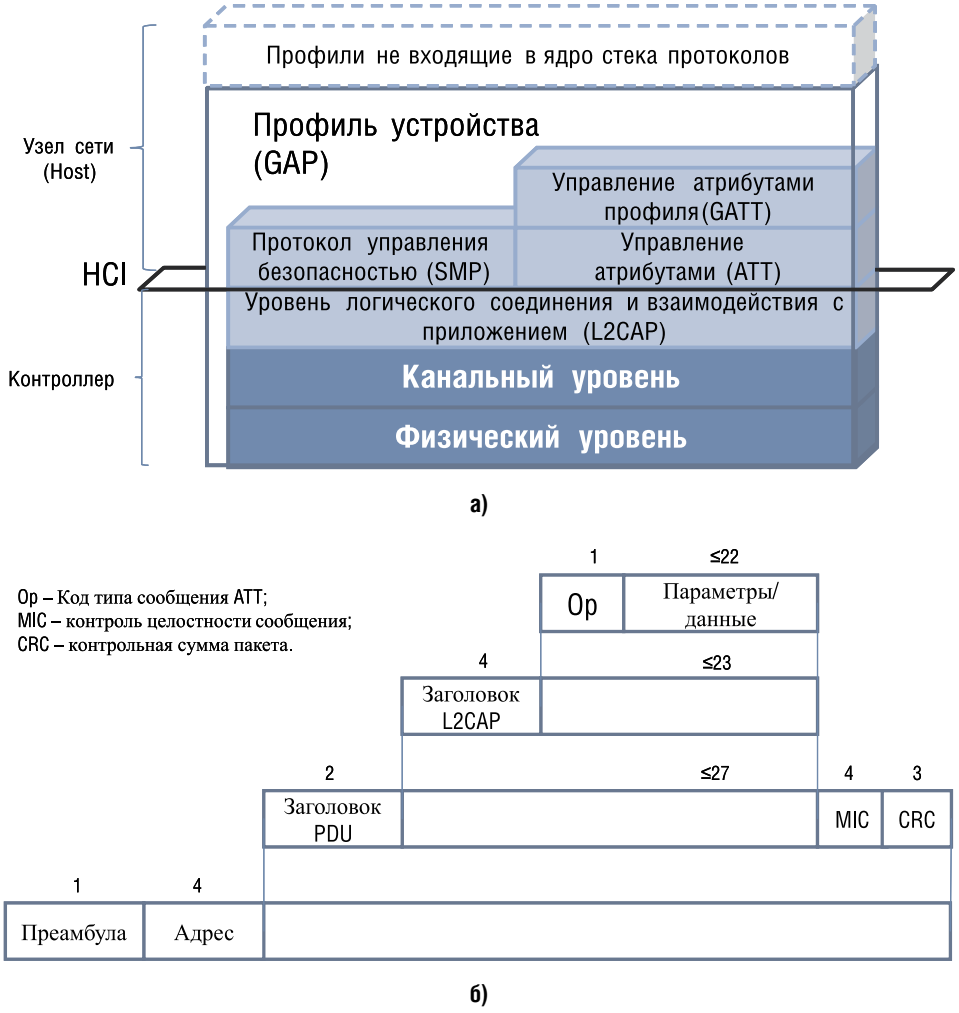

Рис. 1. **Структура стека протоколов Bluetooth Low Energy (BLE) – а) и пакета данных BLE – б)**

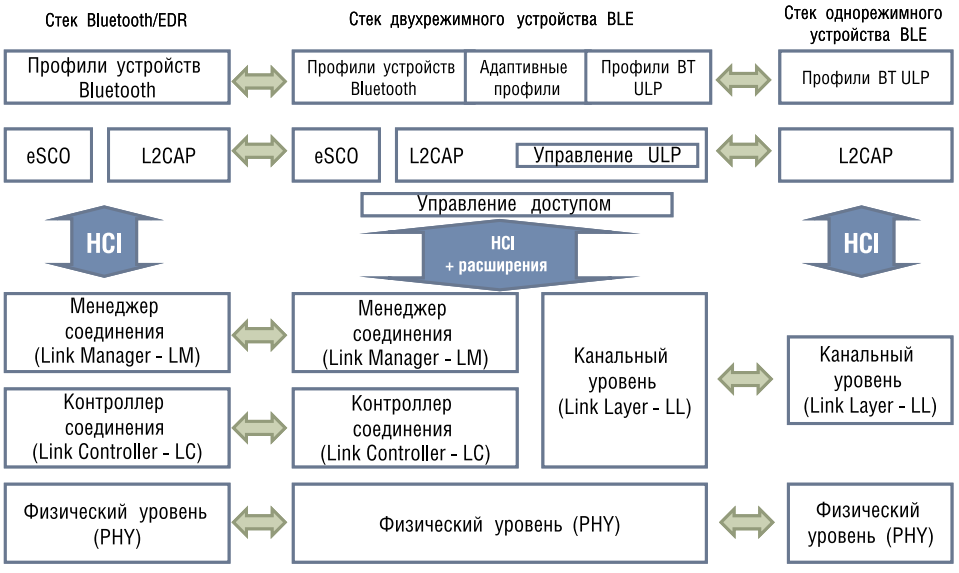

Рис. 2. **Схема взаимодействия между однорежимными, двухрежимными устройствами и классическими Bluetooth-устройствами**

ному компьютеру или информации, автоматическая блокировка-разблокировка системы в целях предотвращения несанкционированного доступа к информации, учет нахождения на рабочем месте (что полезно при внутреннем расследовании инцидентов, связанных с нарушением политики информационной безопасности компании);

• в промышленном применении – автоматическая блокировка/разблокировка оборудования для защиты от несанкционированного включения (например, на время проведения ремонтных или регламентных работ) или выключения;

• в строительной отрасли, при погрузочно-разгрузочных работах – для сигнализации нахождения в опасной зоне или индикации присутствия человека в зоне проведения работ.

Немаловажной областью применения BLE-устройств могут стать автомобильные системы. При помощи специальных BLE-брелоков или непосредственно со смартфона, оснащенного Bluetooth, возможно управление и настройка ряда автомобильных систем, начиная от личных настроек водителя (климат, предпочтительная радиостанция) до дополнительного уровня противоугонной системы. Таким уровнем может быть блокировка запуска автомобиля в отсутствии BLE-устройства (или любого из предварительно зарегистрированных устройств хозяина с Bluetooth) в радиусе действия BLE-узла, находящегося в автомобиле.

Ниже рассмотрим ключевые особенности стека протоколов Bluetooth Low Energy и BLE-устройств, поставляемых BlueGiga.

Стек протоколов Bluetooth Low Energy

Структура стека

Как и классический стек протоколов Bluetooth, стек BLE состоит из двух основных частей: контроллера (Controller) и узла сети (Host). Контроллер включает в себя физический и канальный уровень и часто реализуется в виде системы-на-кристалле (СнК) с интегрированным беспроводным трансивером. Часть стека, именуемая узлом сети реализуется программно на микроконтроллере приложений и включает в себя функциональность верхних уровней: уровень логической связи (Logical Link Control – LLC), протокол адаптации (Adaptation Protocol – L2CAP), протокол атрибутов (Attribute Protocol – ATT), протокол атрибутов профилей устройств (Generic Attribute Profile – GATT), протокол обеспечения безопасности (Security Manager Protocol – SMP), протокол обеспечения доступа к функциям профиля устройств (Generic Access Profile (GAP). Взаимодействие между верхней и нижней частями стека осуществляется интерфейсом Host Controller Interface (HCI). Дополнительная функциональность прикладного уровня может быть реализована поверх уровня узла сети. На рисунке 1 представлена структура стека протоколов BLE [1, 3].

Несмотря на то, что некоторые функции контроллера BLE заимствованы у классического Bluetooth, они не совместимы между собой, т.е. устройство, поддерживающее только BLE (однорежимное устройство – single-mode

device) не сможет взаимодействовать с устройством, поддерживающим только Bluetooth 2.x/3.0. Для осуществления взаимодействия между ними хотя бы одно из устройств должно поддерживать оба стека протоколов (двухрежимное устройство – dual-mode device).

Однорежимные устройства обладают наименьшим потреблением и в основном представляют собой конечные исполнительные устройства. Двухрежимные устройства предполагают возможность периодического получения энергии, располагаются на различных мобильных устройствах, а также могут функционировать и как обычные Bluetooth-устройства. Схема взаимодействия между однорежимными, двухрежимными устройствами и классическими Bluetooth-устройствами представлена на рисунке 2 [1, 4].

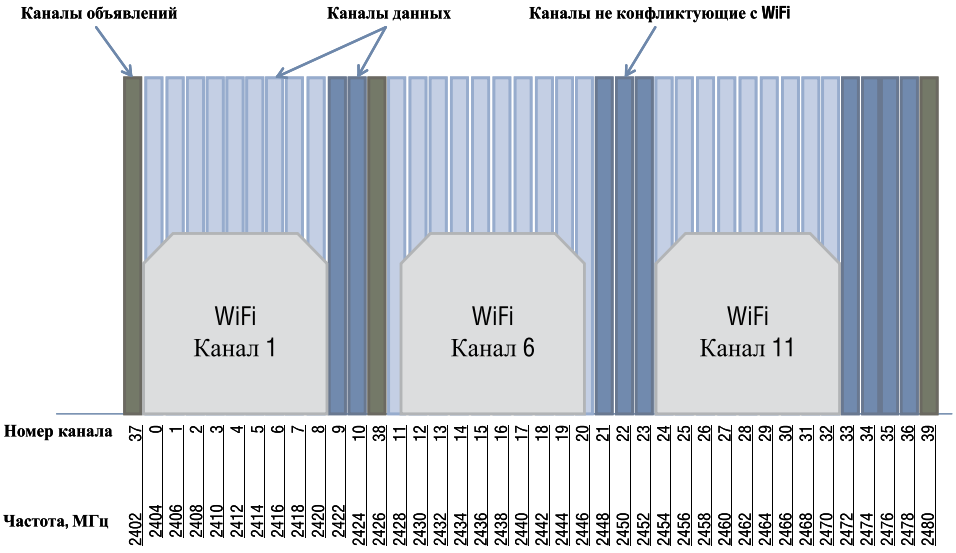

Рис. 3. **Соотношение частотных каналов BLE и каналов IEEE 802.11**

Физический уровень

Устройства BLE работают в диапазоне 2,4 ГГц. В стандарте определено 40 частотных каналов с расстоянием в 2 МГц между каналами. На физическом уровне применена GFSK-модуляция (Gaussian Frequency Shift Keying) с индексом модуляции в пределах от 0,45 до 0,55, что позволяет уменьшить пиковое потребление энергии. Скорость передачи на физическом уровне 1 Мбит/с. В стандарте BLE чувствительность приемника определена как уровень сигнала на приемнике, при котором частота битовых ошибок (Bit Error Rate – BER) достигает уровня 10-3. Она должна составлять -70 дБм или лучше.

Выделяют два типа каналов – каналы объявления и каналы данных. Каналы объявления используются для поиска устройств, установления соединения, широковещательных передач, тогда как каналы данных используются для двунаправленного обмена между устройствами.

Для каналов объявления выделено три частотных канала в центре полосы, что минимизирует перекрытие с каналами 1, 6 и 11 стандарта IEEE 802.11. Остальные 37 каналов используются для обмена данными. Для снижения влияния помех, многолучевого распространения, а также снижения влияния соседних устройств при обмене данными происходит скачкообразное переключение частоты (рис. 3) [1].

Канальный уровень

В BLE для передачи широковещательных пакетов применяются каналы объявления. Любое устройство, передающее пакеты по данным каналам, называется объявителем. Передача пакетов по каналам объявлений происходит только в течение специальных выделенных интервалов времени, называемых событиями объявлений. Во время этих событий устройство-объявитель передает пакеты объявлений последовательно по каждому из трех каналов. Устройства, единственной функцией которых является прием пакетов объявлений, называются сканерами [3].

Двунаправленный обмен между BLE-устройствами возможен только после установления соединения между ними. Создание нового соединения между двумя устройствами является асимметричной процедурой, в течение которой устройство-объявитель по каналам объявления сигнализирует о своей готовности к соединению, в то время как другое устройство (инициатор соединения) прослушивает данные каналы. Когда инициатор обнаруживает нужное устройство, он может послать запрос на установление соединения (Connection Request) объявителю, который устанавливает между ними соединение. С этого момента устройства могут осуществлять обмен по каналам данных. Пакеты, относящиеся к установленному соединению, будут отмечены сгенерированным случайным образом 32-битным кодом доступа.

Также как и в классическом варианте Bluetooth, в BLE для установленного соединения одно из устройств выступает в качестве ведущего (master), второе – ведомого (slave). В ходе процедуры установления соединения – инициатор и объявитель, соответственно. Ведущее устройство может поддерживать несколько соединений с ведомыми, в то время как ведомое устройство может иметь только одно подключение – к ведущему. Таким образом, BLE-устройство одновременно может принадлежать только одной пико-сети. В этом кроется еще одно отличие BLE от Bluetooth – в последнем случае ведомое устройство в свою очередь могло выступать в качестве ведущего устройства своей собственной пико-сети.

Для экономии энергии ведомое устройство по умолчанию находится в спящем состоянии, периодически просыпаясь для проверки наличия пакетов данных от ведущего. Ведущий определяет для своих ведомых устройств моменты времени, в которые ведомый просыпается для прослушивания канала, регулируя тем самым доступ устройств к среде передачи по схеме разделения времени (Time Division Multiple Access – TDMA). Ведущее устройство также задает ведомым схему переключения частотных каналов. Параметры соединения передаются в сообщении запроса на установление соединения и могут быть обновлены при необходимости (например при смене схемы переключения каналов для устранения перекрытия с частотными каналами других устройств).

После установления соединения физический канал передачи данных разделяется на неперекрывающиеся временные интервалы, называемые событиями соединения (connection events) или фреймами. В течение фрейма все пакеты передаются по одному частотному каналу. Каждый фрейм начинается с передачи пакета ведущим устройством. В том случае, если ведомое устройство получило пакет, оно должно послать пакет-подтверждение. В то же время подтверждения от ведущего устройства ведомому не требуется. Между двумя последовательными пакетами должен быть выдержан интервал времени не менее 150 мкс – т.н. межкадровый интервал (Inter Frame Space – IFS).

До тех пор, пока между ведущим и ведомым продолжается обмен пакетами, событие соединения (или фрейм обмена) считается открытым. В пакетах данных, в случае необходимости дальнейшего обмена, установлен бит More Data (MD). Если ни одно из устройств не имеет данных для передачи, событие соединения

Таблица 1. **Сервисы и уровни безопасности, определенные в стеке протоколов BLE [3]**

Режим	Уровень безопасности	Тип соединения (Pairing)	Шифрование	Проверка целостности	Уровень стека
LE Security Mode 1	Уровень 1	Нет	Нет	Нет	Канальный уровень (Link Layer)
	Уровень 2	Без аутентификации	Есть	Есть	
	Уровень 3	Аутентификация	Есть	Есть	
LE Security Mode 2	Уровень 1	Без аутентификации	Нет	Есть	Уровень ATT (ATT Layer)
	Уровень 2	Аутентификация	Есть	Есть	

будет закрыто, и ведомое устройство уже не должно прослушивать канал до начала следующего фрейма. Другими причинами, приводящими к закрытию события соединения, являются два последовательно принятых пакета с ошибками, неверный адрес устройства в пакете. Для контроля битовых ошибок в пакете после поля данных следует поле 24-битной контрольной суммы.

Для нового события соединения ведущий и ведомый используют новый частотный канал, заданный в карте переключения каналов. Время между началом двух последовательных событий соединения задается параметром *connInterval,* является кратным 1,25 мс и может лежать в пределах от 7,5 мс до 4 с. Вторым важным параметром для пико-сети BLE является параметр *connSlaveLatency,* определяющий количество последовательных фреймов, в течении которых ведомое устройство не прослушивает канал и может на это время отключить трансивер. Данный параметр является целым числом в пределах от 0 до 499, которое не должно превышать контрольного интервала супервизора – параметр *connSupervisionTimeout.* Параметр *connSupervisionTimeout* может принимать значения в диапазоне от 100 мс до 32 с. Его назначение – обнаружение потери соединения с устройством из-за ухудшения качества канала связи или перемещения его за пределы досягаемости [3].

На канальном уровне для управления потоком данных действует механизм остановки и ожидания (stop-and-wait mechanism) на основе т.н. кумулятивного подтверждения, служащего одновременно и оповещением об ошибке. Заголовок каждого пакета, передаваемого по каналам данных, содержит два однобитных поля, называемых порядковым номером и следующим ожидаемым порядковым номером (Sequence Number (SN) и Next Expected Sequence Number (NESN) соответственно). SN идентифицирует пакет, тогда как NESN показывает, какой пакет ожидается от устройства, с которым установлено соединение. Если пакет устройством принят успешно, поле NESN в его следующем пакете будет увеличено, и такой пакет одновременно будет считаться пакетом подтверждения. В противном случае, если устройство обнаруживает ошибку (не сходится контрольная сумма), полю NESN в принятом пакете нельзя доверять, и устройство, принявшее такой пакет, повторяет отправку своего последнего пакета, что на стороне приемника в такой ситуации будет воспринято как сообщение об ошибке.

L2CAP

Протокол L2CAP в BLE является упрощенной и оптимизированной версией соответствующего протокола в Bluetooth 2.x/3.x. В BLE основной задачей L2CAP является мультиплексирование данных трех протоколов (ATT, SMP, Link Layer) для соединения канального уровня. Отвечает за установление логического соединения. Не производится сегментирования пакетов или сборки пакетов, т.к. максимальная полезная нагрузка L2CAP в BLE составляет 23 байта.

ATT

Определяет коммуникационные сообщения между двумя устройствами, выступающими в контексте данного протокола в качестве клиента и сервера.

Сервер поддерживает набор атрибутов, представляющих собой структуру данных, позволяющую получать доступ к информации, управляемой протоколом GATT. Роли клиента и сервера определяются протоколом GATT и не зависят от роли устройства в соединении (ведущий/ведомый).

Клиент посредством запросов может получить доступ к атрибутам сервера. Кроме того, сервер посылает клиенту два типа сообщений, содержащих атрибуты:

- уведомления, не требующие подтверждения;
- индикаторы, на которые клиент обязан ответить.

Клиент также может послать серверу команды на изменение значений атрибутов.

GATT

Протокол GATT определяет среду исполнения, используемую ATT для обнаружения сервисов и обмена характеристиками между устройствами. Характеристика в данном случае представляет собой набор данных, включающих в себя значения и свойства. Данные, относящиеся к сервисам и характеристикам, сохраняются в атрибутах.

К примеру, сервер с работающим сервисом «температурный датчик» может быть связан с характеристикой «температура», которая используется для описания датчика, а другой атрибут может применяться для хранения результатов измерений.

Вопросы безопасности BLE

BLE предлагает несколько сервисов безопасности для защиты данных, передаваемых между парой соединенных устройств. Большинство из поддерживаемых сервисов могут быть описаны в терминах двух режимов: LE Security Mode 1 и LE Security Mode 2. Эти режимы обеспечивают сервисы безопасности на канальном уровне и уровне ATT, соответственно [3].

Канальный уровень BLE поддерживает шифрование и аутентификацию на основе алгоритма Cipher Block Chaining-Message Authentication Code (CCM) и блочного шифра AES-128. При использовании в соединении шифрования и аутентификации, к полезной нагрузке (PDU) добавляется четырехбайтное сообщение проверки целостности Message Integrity Check (MIC), после чего поля PDU и MIC шифруются.

Также возможна передача аутентификационных данных поверх нешифрованного соединения канального уровня. В данном случае на уровне ATT к полезной нагрузке добавляется 12-байтная сигнатура. Сигнатура вычисляется путем использования алгоритма AES-128 как блочного шифра. Одним входом алгоритма является счетчик, позволяющий предотвратить атаки типа повтора сообщений. Если приемнику удается верифицировать сообщение, считается, что оно пришло от достоверного источника.

В дополнение к описанным сервисам, BLE поддерживает механизм, называемый приватным (или частным) адресом, который позволяет устройству использовать множество часто меняемых адресов. Этот механизм снижает угрозу отслеживания BLE-устройства по его адресу. Приватные адреса генерируются на основе публичного адреса устройства путем его шифрования с

использованием ключа, полученного от доверенного устройства.

Каждый режим безопасности предусматривает наличие нескольких уровней, применяемых в зависимости от типа соединения пары устройств (таблица 1).

Логическое соединение устройств (pairing) происходит в три этапа. На первом этапе соединенные на канальном уровне устройства объявляют свои доступные возможности ввода-вывода, и на основе их принимается решение о методе взаимодействия на втором этапе.

Целью второго этапа является генерация короткоживущего ключа (Short-Term Key – STK), который будет использован на третьем этапе для обеспечения безопасности передачи распространения ключевой информации. На втором этапе устройства первоначально договариваются о временном ключе (Temporary Key – TK) при помощи одного из методов:

- Out Of Band;
- Passkey Entry;
- Just Works.

Метод Out Of Band (передача вне полосы) предполагает передачу временного ключа по альтернативным каналам, например, используя NFC. В методе Passkey Entry ключ задает пользователь в виде последовательности из шести цифр. Когда применение обоих методов невозможно, используется метод Just Work, хотя он не поддерживает проверку аутентификаций, и не защищен от атаки типа «посредник» (Man In The Middle – MITM).

На базе ключа TK и случайных чисел, генерируемых каждым из узлов, создается STK, что является завершением второго этапа.

На третьем этапе каждая из конечных точек соединения может передать другой конечной точке до трех 128-битных ключей, называемых Long-Term Key (LTK), Connection Signature Resolving Key (CSRK) и Identity Resolving Key (IRK).

LTK используется для генерации 128-битного ключа для шифрования и аутентификации на канальном уровне, CSRK – для подписи данных на уровне ATT, а IRK – для генерации частных адресов.

Протокол управления безопасностью Security Manager Protocol (SMP), работающий поверх фиксированного канала уровня L2CAP, отслеживает выполнение всех трех этапов.

Уязвимым местом BLE на текущий момент является незащищенность ни одного из реализованных в нем методов установления соединения от пассивного прослушивания. Однако, в следующих версиях BLE планируется использование эллиптической криптографической

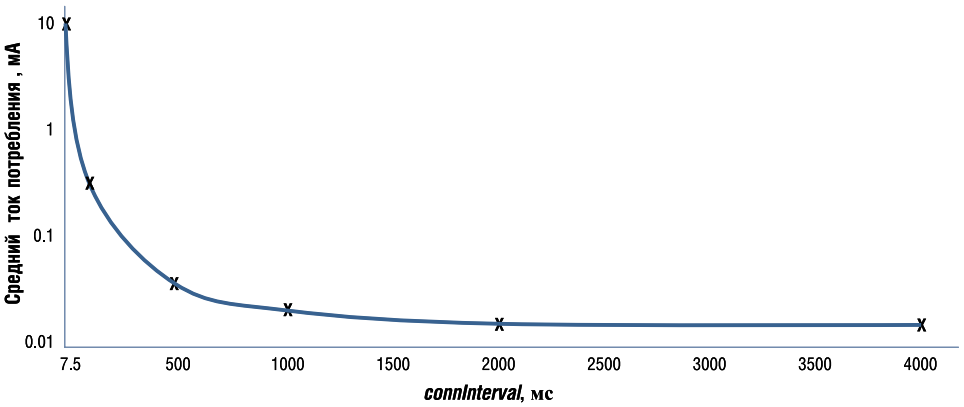

Рис. 4. **Средний ток потребления BLE-устройства в режиме ведомого (узел построен на базе СнК CC2450, *connSlaveLatency=0*)**

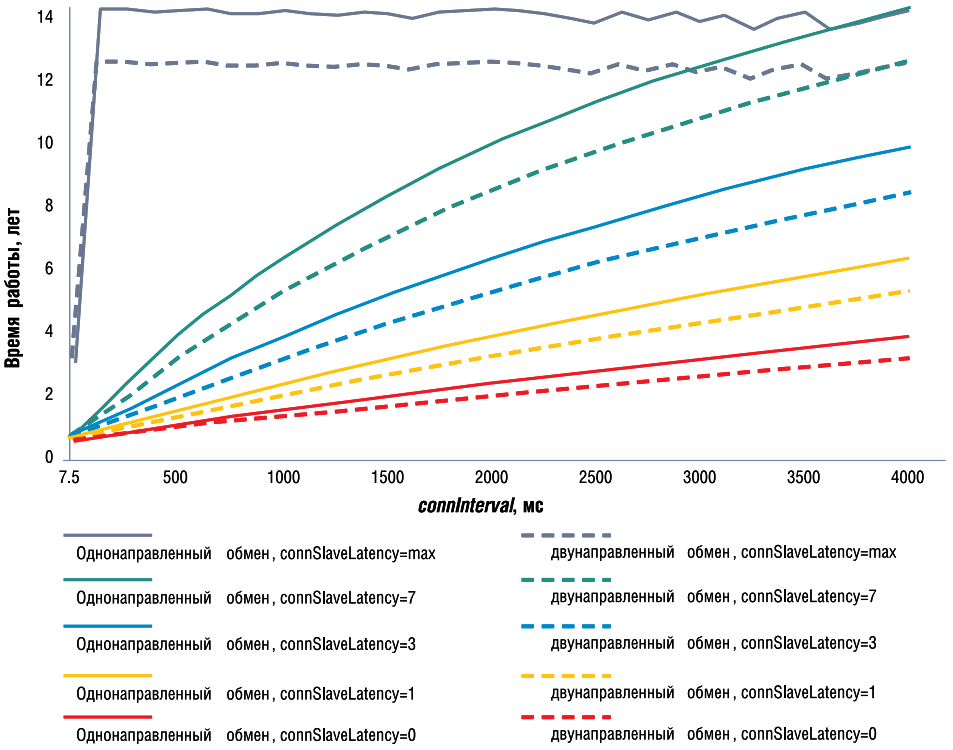

Рис. 5. **Теоретические оценки времени автономной работы BLE-устройства на основе CC2540 (от батареи емкостью 230 мАч в режиме ведомого устройства при уровне ошибок равном 0 и максимальном значении *connSlaveLatency*)**

кривой и алгоритма обмена открытыми ключами (алгоритм Диффи-Хэлмана).

Уровень GAP и профили приложений

Протокол GAP определяет роли устройств, режимы и процедуры обнаружения устройств и сервисов, управление установлением соединения и безопасностью. В BLE GAP выделяет четыре роли для контроллера – широковещательный, наблюдатель, периферийный и центральный.

Широковещательный узел может только передавать пакеты по каналам объявления и не поддерживает соединение с другими устройствами. Наблюдатель способен только прослушивать каналы объявлений, в частности, способен принимать пакеты, передаваемые широковещательным узлом. Центральные узлы представляют собой устройства, способные поддерживать несколько соединений, в то время как периферийные – это простые устройства, способные поддерживать одно соединение с центральным узлом. Роли центрального и периферийного узла предполагают, что устройство способно выполнять функции, соответственно, ведущего или ведомого . Устройство может поддерживать несколько ролей, но одновременно активной может быть только одна из них.

Поверх GAP могут быть построены дополнительные профили приложений, обеспечивающие необходимую пользователю функциональность. В BLE поддерживается иерархия профилей – профиль

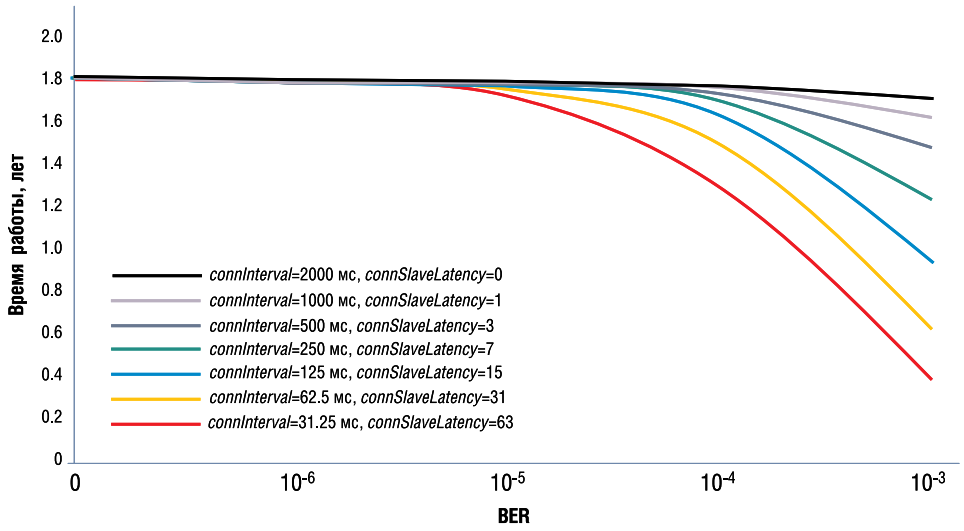

Рис. 6. **Теоретические оценки времени автономной работы BLE-устройства на основе CC2540 (от батареи емкостью 230 мАч в режиме ведомого устройства при различном уровне ошибок и различных значениях параметров *connInterval* и *connSlaveLatency*)**

верхнего уровня может использовать функции профиля низкого уровня.

Эксплуатационные характеристики BLE

Одним из важных показателей, определяющих возможность применения технологии беспроводной связи в той или иной задаче, является энергопотребление узлов сети, работающей по данной технологии. Этот показатель будет определять время автономной работы устройств, и, соответственно, схему технического обслуживания сети.

Для устройств BLE потребление будет зависеть от роли устройства в соединении и параметрах соединения, в частности от *connInterval, connSlaveLatency, connSupervisionTimeout,* а также от качества связи.

Среднее энергопотребление узла в режиме ведомого в зависимости от величины *connInterval* представлено на рисунке 4 [3].

В [3] также представлены результаты теоретического анализа времени автономной работы BLE-устройства в качестве ведомого в зависимости от интервала следования событий связи connInterval и уровня битовых ошибок (BER) (рисунки 5 и 6, соотвестственно).

Данные результаты, хотя и представляют максимальные оценки времени работы BLE-устройств, но показывают, что BLE вполне подходит для сенсорных устройств с автономным питанием, и среднее потребление BLE-устройств вполне сравнимо с потреблением устройств, «традиционных» для сенсорных сетей.

Сравнительные характеристики технологий BLE, Bluetooth, ZigBee, 6LoWPAN, Z-Wave представлены в таблице 2 [1, 3].

Области применения BLE

Безусловно, большая часть областей применения Bluetooth может быть успешно заменена или дополнена устройствами BLE, что продлит срок службы устройств за счет более эффективного управления энергопотреблением. В частности, возможно применение двухрежимных устройств BLE в мобильных телефонах, планшетных компьютерах, ноутбуках. Однорежимные устройства могут применяться в качестве беспроводного интерфейса датчиков с батарейным питанием, применяющихся как отдельно, так и в составе других

Таблица 2. **Некоторые сравнительные характеристики технологий BLE, Bluetooth, ZigBee, 6LoWPAN, Z-Wave**

Параметр	ZigBee	6LoWPAN (поверх IEEE802.15.4)	Z-Wave	BLE	Bluetooth
Частотный диапазон, МГц	868/915/2400	–	868/908, 2400 (не все версии устройств)	2400	2400
Битовая скорость, кбит/с	20/40/250	–	9.6/40, 200	1000	<721 (v1.2), 3000(v2+EDR), <24000(v3+HS)
Тип модуляции сигнала	BPSK/BPSK/O-QPSK	–	BPSK	GFSK	GFSK(v1.2), GFSK/4-DQPSK/8DPSK (v2+EDR), 802.11 (v3+HS)
Метод расширения спектра	DSSS	–	Нет	FHSS (ширина канала 2 МГц)	FHSS (ширина канала 1 МГц)
Чувствительность приемника, дБм	-92 или лучше для 868/915 МГц; -85 или лучше для 2400 МГц	–	-101	<-70 -87…93	-90
Выходная мощность передатчика, дБм	-32…0	–	-20…0	-20…10	20/4/0 (класс 1/2/3)
Размер данных пакета, байт	До 127	–	До 64	От 8 до 47	До 358
Адресация	16- и 64-бит MAC, 16-бит идентификатор сети	16- и 64-бит MAC, 128-бит адрес IPv6	32-бит идентификатор дома; 8-бит адрес узла	48-бит открытый адрес Bluetooth или случайный адрес	48-бит открытый адрес Bluetooth
Типовые требования к реализации стека протоколов	45…128 кбайт ПЗУ; 2,7…12 кбайт ОЗУ	~24 кбайт ПЗУ; ~3,6 кбайт ОЗУ	32…64 кбайт ПЗУ; 2…16 кбайт ОЗУ	~40 кбайт ПЗУ; ~2,5 кбайт ОЗУ	~100 кбайт ПЗУ; ~30 кбайт ОЗУ

Рис. 7. **Внешний вид двухрежимного BLE-модуля BT111**

устройств — в часах, пульсометрах, шагомерах, домашних тонометрах, термометрах и тому подобных устройств.

В составе мобильных устройств BLE может быть использован для управления домашней автоматикой, устройствами освещения или охраны, как минимум, в пределах одного помещения. Для управления устройствами в пределах всего дома возможно использование BLE в качестве шлюза между управляющим устройством и сетью домашней автоматики.

Низкое энергопотребление и более устойчивая работа в условиях большого количества аналогичных устройств в ряде случаев позволяет рассматривать BLE как альтернативу устройствам NFC, в частности RFID-меткам. Но более интересен вариант использования BLE совместно с NFC. В этом случае первые обеспечивают больший радиус устойчивой работы и большое количество совместно работающих устройств, а вторые служат для установления логического соединения между парой устройств, обеспечивая более высокий уровень безопасности за счет меньшего радиуса действия.

Модули Bluetooth Low Energy компании BlueGiga

На данный момент BlueGiga предлагает серии BLE-устройств [5, 6]:

- модуль BT111 Bluetooth Smart Ready HCI Module;
- USB-устройство BLED112 Bluetooth low energy dongle;
- модуль BLE112 Bluetooth low energy module.

Модуль BT111

BT111 предназначен для приложений, в которых необходима работа и с классическими Bluetooth-устройствами, и с устройствами Bluetooth Low Energy, и представляет собой миниатюрный модуль поверхностного монтажа со встроенной антенной (рис. 7).

При выходной мощности до 8 дБм модули BT111 могут поддерживать соединение на расстоянии порядка 100 м в пределах прямой видимости. Чувствительность приемника составляет -89 дБм.

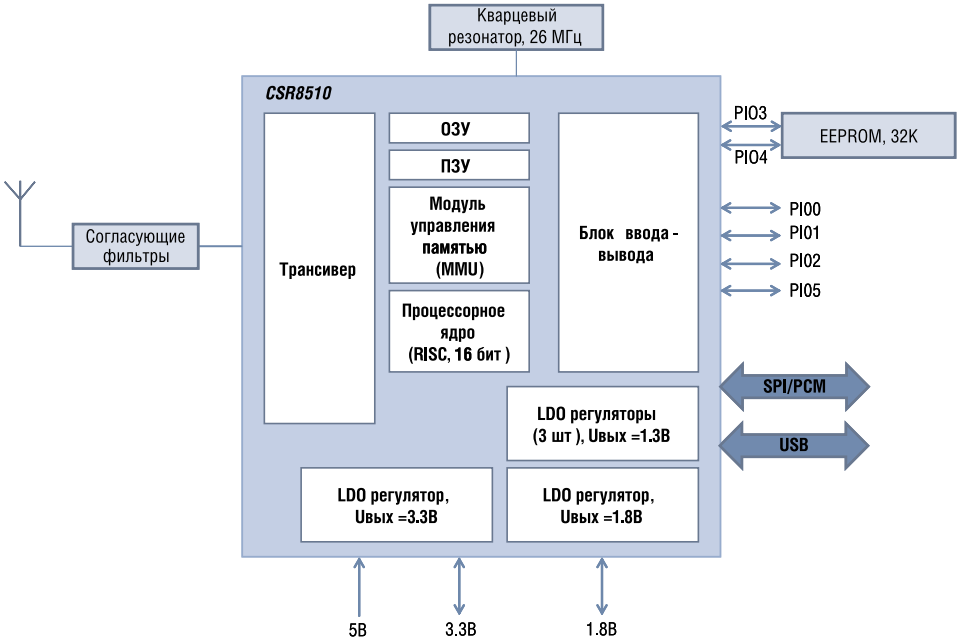

Рис. 8. **Структурная схема BLE модуля BT111**

В основе BT111 лежит беспроводная система-на-кристалле CS8510 [7], содержащая Bluetooth-трансивер, 16-битный RISC-микроконтроллер с достаточно эффективной схемой управления энергопотреблением и распределением памяти. Ядро микроконтроллера при поддержке контроллера прерываний и таймера исполняет стек протоколов Bluetooth, а также отслеживает беспроводной интерфейс и интерфейс к хост-контроллеру. Встроенный в CS8510 LDO-регулятор позволяет модулю работать в диапазоне напряжений от 1,8 до 3,6 В.

CSR8510 дополнительно имеет SPI-, PCM- и USB (Full-speed 12 Мбит/с)-интерфейсы. Кроме того, доступны до четырех линий ввода-вывода, которые могут быть использованы в качестве линий индикаторов, в качестве входных линий, а также в режиме совместимости с Wi-Fi.

Помимо самой однокристальной системы CS8510 в состав BT111 входят: монопольная керамическая антенна, входной фильтр, EEPROM объемом 32 кбайта и кварцевый резонатор на 26 МГц. Структурная схема BT111 представлена на рисунке 8.

Антенна обеспечивает усиление порядка 0,5 дБм, радиочастотный фильтр позволяет уменьшать уровень помех модуля. Встроенная EEPROM может быть использована для хранения настроек модуля, таких как выходная мощность передатчика, конфигурация периферийных интерфейсов, настройки и идентификаторы USB, адрес Bluetooth.

BT111 может работать совместно с Wi-Fi-устройствами. Для этого предусмотрено три режима совместимости:

- Unity-3;
- Unity-3e;
- Unity+.

CS8510 обладает весьма впечатляющими объемами памяти и эффективной схемой управления ею. Так, модуль управления памятью поддерживает несколько кольцевых буферов для передачи данных между хост-контроллером и беспроводным интерфейсом при минимальном участии в этом процессорного ядра.

В CS8510 56 кбайт оперативной памяти разделятся между кольцевыми буферами для голосовых данных или для пакетов данных для каждого из поддерживаемых активных соединений. Встроенная постоянная память объемом 5 Мбайт предназначена для хранения прошивки стека протоколов, настроек модуля и кода прикладных программ.

Модуль BLE112

Модуль BLE112 (рис. 9) является однорежимным BLE-модулем, предназначенным для сенсорных систем и BLE-аксессуаров с батарейным питанием. BLE112 поддерживает практически все возможности устройств BLE — беспроводная передача данных, поддержка стека протоколов BLE и ряда профилей BLE-устройств, дополнительно присутствует возможность хранения пользовательских приложений. Таким образом,

Рис. 9. **Внешний вид модуля BLE112**

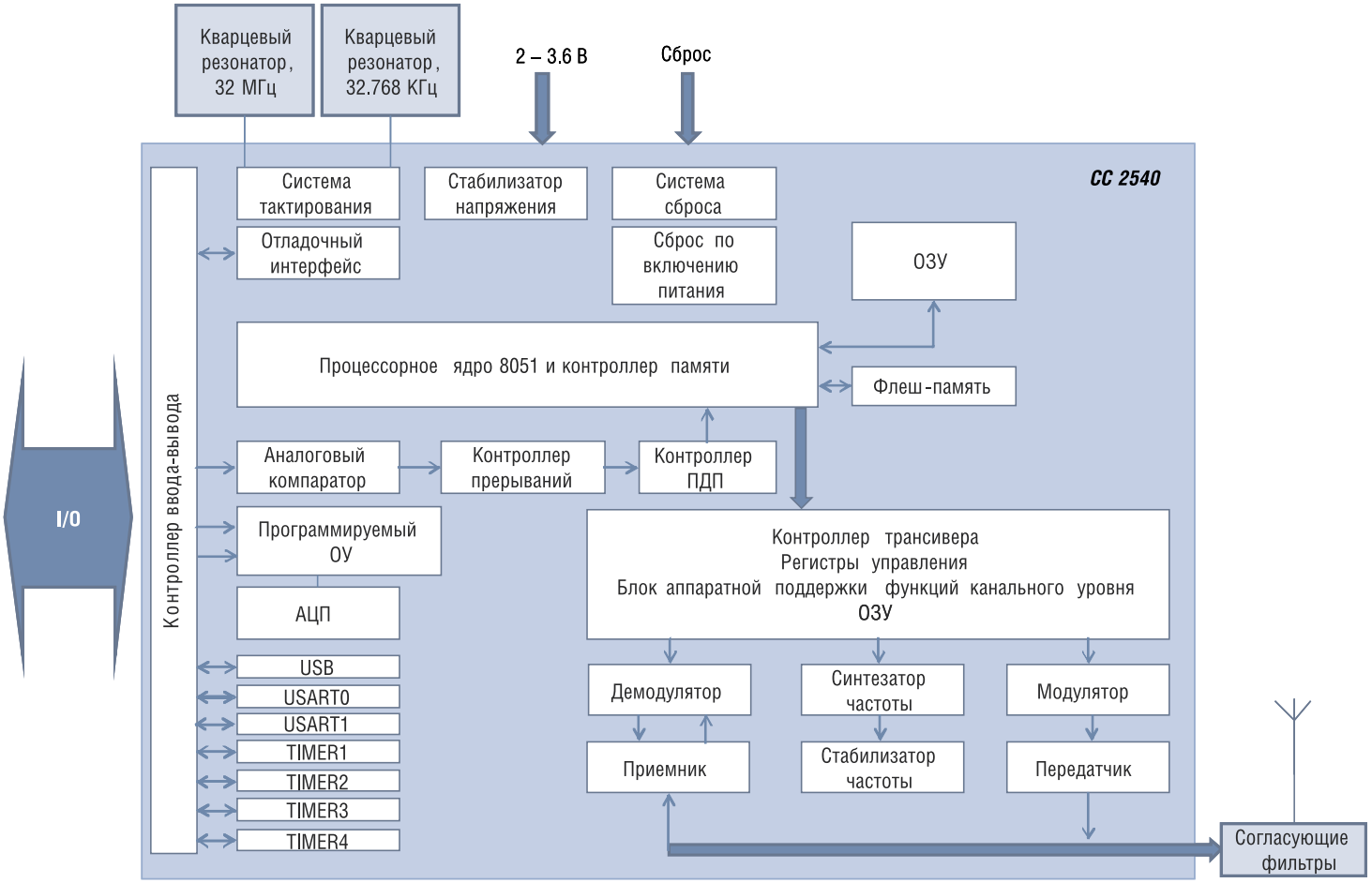

Рис. 10. **Структурная схема модуля BLE112**

возможна работа модуля BLE без внешнего контроллера.

BLE112 отличает достаточно низкое энергопотребление и широкий диапазон напряжений питания. Так он может напрямую работать от 3 В батарейки типа «монета» или от пары батареек типа AAA. В режиме сна модуль потребляет только порядка 400 нА, переход в активный режим осуществляется за доли миллисекунд, а в режиме передачи ток потребления составляет около 27 мА (при выходной мощности 0 дБм).

Трансивер BLE112 обеспечивает выходную мощность в пределах от -23 до 3 дБм и чувствительность по приему порядка -85…-91 дБм.

BLE112 основан на BLE-процессоре от Texas Instruments CC2540 [8], и в дополнение к самому беспроводному процессору имеет встроенные кварцевые резонаторы на 32 МГц и на 32,678 КГц, обеспечивающие тактирование CC2540, согласующий фильтр и миниатюрную керамическую антенну. На печатной плате модуля предусмотрено также посадочное место для UFL-разъема, позволяющего подключать внешнюю антенну.

Структурная схема BLE112 представлена на рисунке 10.

CC2450 содержит высокопроизводительный микроконтроллер архитектуры 8051 с 8 кбайт оперативной памяти и

Рис. 11. **Внешний вид USB-BLE модуля BLED112**

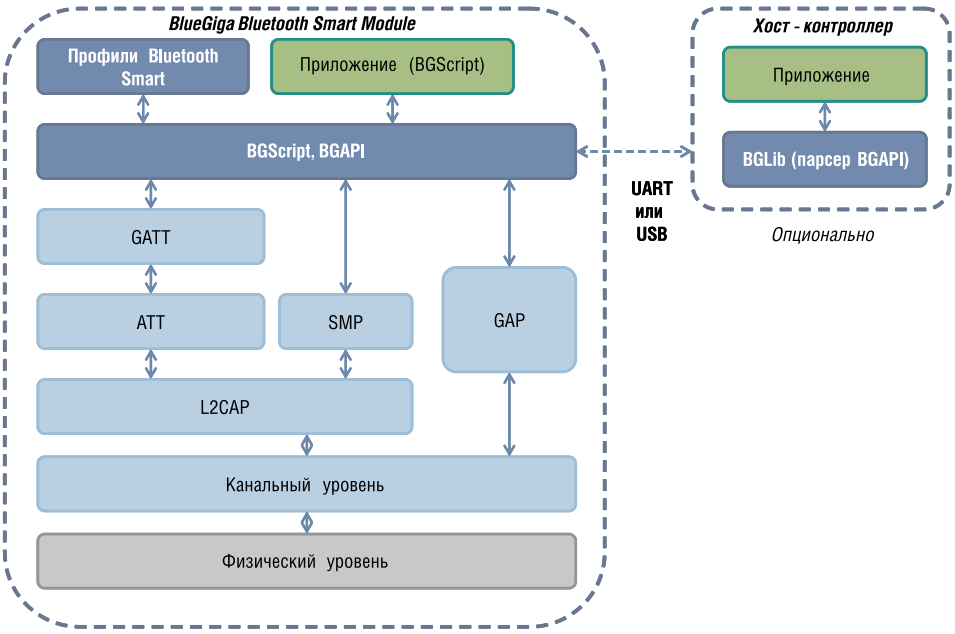

Рис. 12. **Структурная схема программного обеспечения, предоставляемого BlueGiga**

до 256 кбайт флеш-памяти с возможностью перепрограммирования самим устройством. Пятиканальный контроллер прямого доступа в память позволяет весьма эффективно организовать работу с периферийными устройствами и памятью, существенно экономя ресурсы процессорного ядра. Контроллер прерываний обслуживает до 18 каналов прерываний с четырьмя уровнями приоритета, включая прерывания от таймеров, периферийных устройств, линий ввода-вывода.

Набор периферийных устройств включает в себя:

- таймер с ультранизким потреблением, работающий от внешнего 32 кГц резонатора;
- сторожевой таймер;
- 40-битный таймер, используемый стеком протоколов BLE;
- 16-битный таймер с функциями счетчика, ШИМ-генератора и таймера;
- два 8-битных многофункциональных таймера (таймер/счетчик/ШИМ);
- два асинхронных последовательных интерфейса;
- модуль шифрования (AES128);
- 8-канальный АЦП с разрядностью от 7 до 12 бит и скоростями преобразования от 30 до 4 кГц и встроенным датчиком температуры;
- аналоговый компаратор.

Еще одним устройством, предлагаемым BlueGiga для приложений BLE, является USB-BLE модуль BLED112 (рис. 12). Сохраняя функциональность, аналогичную модулю BLE112 (за исключением возможностей ввода-вывода), он выполнен в формате USB-устройства и позволяет подключать другие BLE к персональному компьютеру. BLED112 может также выполнять роль виртуального COM-порта или USB-HID устройства.

BLED112 может также быть полезен при отладке и демонстрации приложений, использующих стек протоколов Bluetooth Low Energy.

Программное обеспечение

BlueGiga предоставляет ряд инструментов и сред для разработки BLE-приложений, а также для настройки модулей и отладки встроенного программного обеспечения.

Программный интерфейс **BGAPI™** совместно с библиотекой **BGLib™C-library** позволяет достаточно легко и эффективно использовать ресурсы модулей BlueGiga при помощи внешнего хост-контроллера (рис. 12).

Программный пакет Profile Toolkit™ позволяет производить разработку и отладку пользовательских приложений для BLE-модулей.

BGScript™ предназначен для быстрой разработки приложений без глубоких знаний особенностей работы стека протоколов, для отладки и тестирования логики работы приложений. Приложения на BGScript™ могут разрабатываться и для хост-контроллера и для самих модулей.

Заключение

Технология Bluetooth Low Energy представляется весьма перспективной технологией для сенсорных приложений, особенно связанных с тесным взаимодействием с пользователем. BLE имеет большой потенциал для широкого распространения, связанный в том числе с успехом классического Bluetooth.

Специализирующаяся на Bluetooth-устройствах компания BlueGige выпускает одно- и двухрежимные устройства BLE, включая модули поверхностного монтажа и USB-устройства, позволяющие благодаря компактным размерам и низкому энергопотреблению реализовывать приложения практически любых областей применения технологии BLE.

Литература

1. Bluetooth® low energy technology// *http://www.compel.ru/wordpress/wp-content/uploads/2012/04/Bluetooth_low_energy_technology.pdf*

2. Johanna Nieminen. Connecting IPv6 capable Bluetooth Low Energy sensors with the Internet of Things// *http://www.futureinternet.fi/seminar2012/Nieminen_IPv6_over_BTLE_300512.pdf*

3. Carles Gomez, Joaquim Oller and Josep Paradells. Overview and Evaluation of Bluetooth Low Energy: An Emerging Low-Power Wireless Technology. *http://www.mdpi.com/1424-8220/12/9/11734*

4. Flavia Martelli. Bluetooth® low energy. *http://www.chiaraburatti.org/uploads/teaching/handouts_WSNs_BT-LE.pdf*

5. Bluegiga – Bluetooth_Modules// *http://www.bluegiga.com/bluetooth-low-energy*

6. Виктор Алексеев. Новые модули Bluetooth 4.0 серии BLE производства Bluegiga.//Беспроводные технологии. 2011. №2. С. 16 – 22.

7. CSR8000™ Platform// *http://www.csr.com/products/54/csr8000-platform*

8. 2.4GHz Bluetooth® low energy System-on-Chip// *http://www.ti.com/lit/gpn/cc2540.*

Получение технической информации, заказ образцов, поставка –
e-mail: wireless.vesti@compel.ru