УДК 621.391

Радиоконтроль служебных параметров сигналов Bluetooth

Фаустов И. С., Токарев А. Б., Сладких В. А.,
Козьмин В.А., Крыжко И. Б.

Постановка задачи: *Бурный рост использования беспроводных технологий требует развития средств контроля за устройствами и сетями передачи данных и, в частности, за беспроводными персональными сетями стандарта Bluetooth. Пассивный радиоконтроль Bluetooth устройств с произвольными MAC-адресами представляет собой сложную задачу, т.к. произвольность как адресной, так и служебной части пакетов данных препятствует применению классической корреляционной обработки, а недостаток априорной информации, необходимой для дескремблирования битового потока, осложняет задачу построения анализатора сетей Bluetooth на базе цифрового радиоприемного устройства.* ***Целью работы*** *является разработка способа обнаружения сигналов Bluetooth и определения их служебных параметров, а также построение на этой основе программно-аппаратного анализатора сетей Bluetooth.* ***Новизна:*** *предложенный способ отличается от известных способностью одновременно обнаруживать сигналы для произвольного набора Bluetooth-передатчиков и декодировать их служебные параметры без необходимости обмена запросами-ответами между анализатором и устройствами Bluetooth.* ***Практическая значимость:*** *предложенный способ может быть применен для построения анализатора сигналов Bluetooth на базе цифрового радиоприемного устройства с полосой одновременной обработки сигналов от 1 МГц. Способ реализован на базе цифровых радиоприемных устройствах семейства АРГАМАК, которые применяются в системах поиска и локализации несанкционированных источников радиоизлучений в контролируемых объектах.*

Ключевые слова: *Bluetooth, WPAN, пассивный радиоконтроль, цифровое радиоприемное устройство, обнаружение сигналов, служебные параметры сигналов.*

Введение

В последнее время широкое распространение получили беспроводные персональные сети (WPAN – Wireless personal area network). Радиус действия таких сетей может варьироваться от нескольких десятков сантиметров до нескольких десятков метров. Беспроводные персональные сети могут быть развернуты с использованием различных сетевых технологий, среди которых одной из наиболее распространенных является IEEE 802.15.1 (Bluetooth).

Технология Bluetooth, обеспечивающая передачу данных со скоростью до 3 Мбит/с, стала первой технологией, позволяющей организовывать WPAN. Спецификация Bluetooth была разработана группой Bluetooth Special Interest Group (Bluetooth SIG) 1989 г. и продолжает активно развиваться. Стоит отметить, что последние выпуски спецификации (5.0, 5.1, 5.2) нацелены на расширение спек-

Библиографическая ссылка на статью:
Фаустов И. С., Токарев А. Б., Сладких В. А., Козьмин В. А., Крыжко И. Б. Радиоконтроль служебных параметров сигналов Bluetooth // Системы управления, связи и безопасности. 2021. № 3. С. 135-151. DOI: 10.24412/2410-9916-2021-3-135-151

Reference for citation:
Faustov I. S., Tokarev A. B., Sladkikh V. A., Kozmin V. A., Kryzhko I. B. Radio monitoring of Bluetooth signals service parameters. *Systems of Control, Communication and Security*, 2021, no. 3, pp. 135-151 (in Russian). DOI: 10.24412/2410-9916-2021-3-135-151

тра применении технологии низкого энергопотребления (BLE – Bluetooth Low Energy) в области интернета вещей.

Стек протоколов Bluetooth предполагает использование свободного от лицензирования ISM (Industry, Science and Medicine) диапазона 2,4 – 2,4835 ГГц [1]. В этом диапазоне также могут работать устройства использующие иные технологии, такие как Wi-Fi (IEEE 802.11) или ZigBee (IEEE 802.15.4). Совмещение нескольких беспроводных технологий в одном диапазоне осложняет процедуру обнаружения сигналов стандарта IEEE 802.15.1.

Отметим, что диапазон 2,4 – 2,4835 ГГц является свободным от лицензирования, но в некоторых случаях использование устройств для передачи информации может быть ограничено, например, в пределах контролируемого объекта. Задачей радиоконтрольных служб в подобных условиях является выявление несанкционированных радиоизлучений любого происхождения, что требует от них умения анализировать наблюдаемые в контролируемых полосах частот сигналы и идентифицировать их источники.

В [2] предложен подход к идентификации Bluetooth устройств, основанный на использовании программно-определяемого радио; при этом показаны уязвимости протокола при формировании заголовков пакетов, позволяющие получить две части MAC-адреса ведущего устройства. В этой работе также представлены алгоритмы обработки бит, соответствующих заголовкам принятых пакетов, и результаты работы этих алгоритмов, однако недостаточно детализированы способы обнаружения сигналов и осуществления частотно-временной синхронизации.

В [3, 4] предложен способ эффективного приёма сигналов с гауссовской частотной манипуляцией (GFSK – Gaussian Frequency-Shift Keying) в каналах с частотно-селективными замираниями, а также коррекции частотной расстройки, характерной для Bluetooth-передатчиков. Однако предлагаемый подход ориентирован на оптимизацию приёма сигналов конкретного устройства; обобщить этот подход для эффективного обнаружения сигналов, формируемых набором передатчиков оказывается проблематично.

Целью данной работы является разработка способа обнаружения сигналов всех доступных в точке приёма Bluetooth-передатчиков, определения их служебных параметров и построение на его основе аппаратно-программного анализатора сетей Bluetooth.

Структура сигналов стандарта Bluetooth

По стандарту IEEE 802.15.1 для передачи сигналов Bluetooth могут использоваться семьдесят девять каналов шириной 1 МГц. Современные цифровые радиоприемные устройства систем радиоконтроля (РК) с полосой одновременного обзора в десятки мегагерц [5, 6], позволяют принимать параллельно несколько или даже сразу все каналы Bluetooth, однако обработка в каждом канале одинакова и может осуществляться независимо от других, поэтому далее сосредоточимся на анализе сигналов в отдельном канале.

Передача данных по стандарту IEEE 802.15.1 производится с использованием дуплексной схемы с временным разделением. Длительность одного вре-

менного слота равна 625 мкс; каждый четный временной интервал зарезервирован для передачи ведущим устройством, а нечетный – ведомым. Передача должна начинаться с началом слота, при этом допускается неопределенность, равная ±20 мкс.

Передача информации осуществляется пакетами. Длительность пакетов варьируется в зависимости от типа и может охватывать один, три или пять временных слотов. Для передачи данных используются 79 частотных каналов (в Японии, Франции и Испании – лишь 23 частотных канала) с центральными частотами, измеряемыми в мегагерцах

$$f_C = 2402 + k, \quad (1)$$

где $k = 0,...,78$ – индекс канала. Смена канала осуществляется 1600 раз в секунду по псевдослучайной последовательности частот, которая определяется исходя из значения MAC-адреса ведущего устройства (BD_ADDR), при этом текущее значение частоты в последовательности определяется значением счетчика часов ведущего устройства (CLKN). В момент сопряжения ведомое устройство получает MAC-адрес ведущего устройства и синхронизирует с ним значение счетчика CLKN. Если пакет занимает несколько временных слотов, то центральная частота канала остается неизменной. В начале каждого пакета спецификация допускает смещение Δf центра спектра от f_C на ±75 кГц; дальнейшие допустимые смещения несущей частоты от начального значения представлены в таблице 1 [1].

Таблица 1 – Допустимое смещение несущей частоты

Длительность пакета, мкс	Допустимое отклонение центральной частоты сигнала от начального значения, кГц
625	±25
1875	±40
3125	±40

Приемопередатчики Bluetooth сигналов используют для передачи данных гауссовскую частотную манипуляцию с девиацией частоты от 115 до 175 кГц [1, 7], либо фазовую манипуляцию двух типов: π/4-DQPSK (π/4-differential quadrature phase shift keying) и 8DPSK (8-differential phase shift keying). Интервал передачи одного символа не зависит от используемой схемы модуляции и равен $T_S = 1$ мкс. Битовая скорость в случае использования GFSK равна 1 Мбит/с, а использование фазовой манипуляции позволяет достигнуть битовой скорости в 2 Мбит/с для π/4-DQPSK и 3 Мбит/с – для 8DPSK [1].

Обобщенная структура пакетов данных отражена на рис. 1 (исключением являются пакеты ID (identity) и FHS (Frequency hop synchronization) используемые в процедурах inquiry и page). Следует иметь в виду, что что при использовании технологии Enhanced Data Rate (EDR), предполагающей применение фазовой манипуляция, код доступа к каналу/устройству (CAC – Channel Access Code) и заголовок (Packet header), формируемый на уровне логического транс-

порта (logical transport), по-прежнему использует гауссовскую частотную манипуляцию для обеспечения обратной совместимости устройств [1].

Поскольку разрабатываемый способ обработки радиосигналов должен быть пригоден для обнаружения сигналов стандарта Bluetooth, излучаемых устройствами с произвольными MAC-адресами, то он должен базироваться на элементах пакетов, которые остаются неизменными (предсказуемыми) независимо от излучающего их устройства. Подобных элементов мало, т.к. большинство полей пакетов, представленных на рис. 1, зависит либо от пересылаемой информации, либо от MAC-адресов устройств.

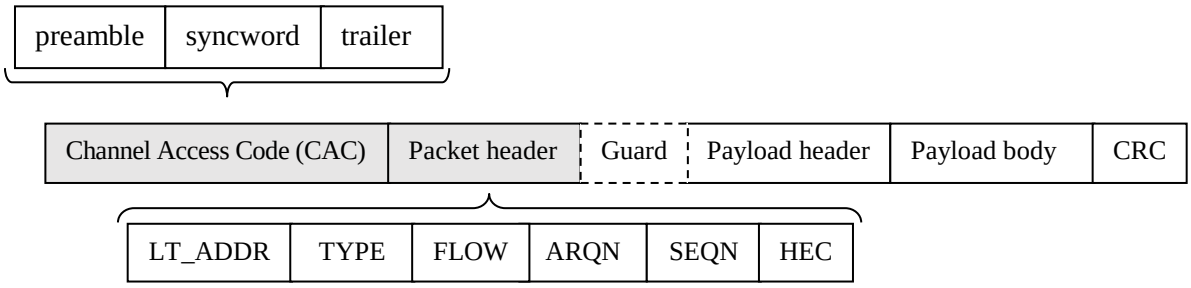


Рис. 1. Обобщенная структура пакета

В частности, содержимое поля CAC зависит от младших бит адреса передатчика lower address part (LAP). Процедура формирования входящего в CAC поля syncword предусматривает, помимо прочего, дополнение адресной части LAP последовательностью 001101 или 110010 в зависимости от старшего бита LAP (эти добавленные биты образуют 7-элементную последовательность Баркера, что позволяет улучшить автокорреляционные свойства пакета) и использование помехоустойчивого кодирования кодом Боуза-Чоудхури-Хоквингема (БЧХ) длиной 64. Более детальную информацию о формировании поля CAC можно найти в спецификации [1]; для разработки анализатора существенно лишь то, что код доступа к каналу обязан соответствовать одному из $M = 4$ возможных вариантов, представленных в таблице 2. Таким образом в пакете, формируемом устройством стандарта IEEE 802.15.1 с неизвестным LAP, из всего поля CAC предсказуемыми оказываются лишь преамбула (preamble), последовательности Баркера и трейлер (trailer) – последовательность чередующихся нулей и единиц, расположенная после последовательности Баркера.

Последовательность бит в заголовке пакета также зависит от передаваемой информации и адресов взаимодействующих устройств. Заголовок начинается логическим транспортным адресом LT_ADDR, который имеется у каждого активного устройства в пикосети и является идентификатором для ведомых устройств, и заканчивается 8-ми битной контрольной суммой HEC, при формировании которой используются старшие биты upper address part (UAP) ведущего устройства. А именно, контрольная сумма формируется с использованием регистра сдвига с обратными связями, полином которого $g(x) = x^8 + x^7 + x^5 + x^2 + x + 1$, где в качестве инициализирующего значения используется UAP ведущего устройства. Подобная структура заголовка позволяет

сосуществовать двум различным сетям даже при условии того, что код доступа к каналу у них одинаков.

Отметим, что заголовок в неявном виде содержит информацию о UAP ведущего устройства, но при отслеживании сетевого трафика «со стороны» в пассивном режиме значение счетчика часов $CLKN_{6-1}$ остается неизвестным. Это служит препятствием для того, чтобы на основании расчета контрольный суммы получить UAP. Подробнее об этом будет говорится при рассмотрении процедуры декодирования информационных бит.

Таблица 2 – Возможные комбинации бит кода доступа к каналу (CAC)

Номер варианта	Преамбула	Проверочные биты кода	LAP	Фрагмент последовательности Баркера	Трейлер
$m = 1$	1, 0, 1, 0	c_0=1, $c_1, \ldots, c_{33}$	$a_0, \ldots, a_{22}, a_{23}$=0	0, 0, 1, 1, 0, 1	0, 1, 0, 1
$m = 2$	0, 1, 0, 1	c_0=0, $c_1, \ldots, c_{33}$	$a_0, \ldots, a_{22}, a_{23}$=0	0, 0, 1, 1, 0, 1	0, 1, 0, 1
$m = 3$	1, 0, 1, 0	c_0=1, $c_1, \ldots, c_{33}$	$a_0, \ldots, a_{22}, a_{23}$=1	1, 1, 0, 0, 1, 0	1, 0, 1, 0
$m = 4$	0, 1, 0, 1	c_0=0, $c_1, \ldots, c_{33}$	$a_0, \ldots, a_{22}, a_{23}$=1	1, 1, 0, 0, 1, 0	1, 0, 1, 0

Таким образом, для подключенных друг к другу Bluetooth устройств наличие информации о коде доступа к физическому каналу позволяет им уверенно обнаруживать «свои» сигналы на фоне помех и радиосигналов иных стандартов за счет хороших корреляционных свойств битовой последовательности CAC. Если же задачей системы РК является ответ на вопрос, имеются ли в окрестности точки приёма хоть какие-то Bluetooth-устройства, то предсказуемыми оказываются лишь отдельные довольно короткие фрагменты битовых последовательностей, что усложняет задачу обнаружения сигналов.

Радиоконтроль сетей Bluetooth

Задачей радиоконтроля устройств Bluetooth является максимально быстрый поиск всех имеющихся на контролируемом объекте устройств соответствующего стандарта. Кратковременность этой процедуры не позволяет отслеживать естественные процессы установления взаимосвязей между устройствами, поэтому контроль требует применения специфичных действий, позволяющих ускорить получение необходимой идентификационной информации.

Существует несколько способов контроля сетей Bluetooth [8], но все они сводятся к двум базовым концепциям: активный и пассивный радиоконтроль. Активный способ может быть осуществлен с помощью любого стандартного адаптера и предполагает отправку запроса всем устройствам, находящимся в анализируемой области. При получении такого запроса устройства отправляют в ответ всю необходимую для идентификации информацию. Полученные ответы позволят составить список устройств в данной области, однако в этот список попадут лишь устройства, которые не находятся в «приватном» режиме (т.к. в этом режиме отправка ответа на широковещательный запрос не производится).

Еще одна разновидность активной атаки («paging attack» [8]) позволяет выявлять наличие устройства с известным MAC-адресом. Суть этой атаки заключается в отправке не широковещательного пакета, а пакета, предназначен-

ного для определенного устройства. Такой пакет может быть сформирован по известному LAP устройства. Этот метод по обнаружению устройства с заранее известным MAC-адресом позволяет выявить наличие устройства даже в том случае, если устройство находится в «приватном» режиме.

Пассивный контроль заключается в отслеживании трафика между двумя устройствами. Устройства будут взаимодействовать друг с другом с помощью определенного кода доступа к каналу. Код доступа к каналу несет информацию о LAP. Кроме того, информацию об устройстве можно было бы получить на этапе сопряжения двух устройств, перехватив пакет FHS, однако такое событие происходит довольно редко.

Пассивный контроль требует бóльших ресурсов и менее эффективен, чем активный [8], однако использование пассивного способа на контролируемом объекте в некоторых случаях является единственным вариантом. Отметим, что в результате анализа служебных параметров есть возможность получить не только LAP, но и UAP ведущего устройства. Именно данный вариант контроля устройств и сетей Bluetooth взят за основу в текущей работе.

Поиск, обнаружение и временная синхронизация

В качестве исходных данных будем использовать выборки значений случайного процесса на входе приемника системы РК длительностью не менее 126 мкс (это длительность наиболее коротких из пакетов данных с идентификационной информацией, а ID-пакеты, используемые в процедурах inquiry и page, в рамках данной работы анализироваться не будут, так как их содержимое не позволяет каким-либо образом идентифицировать излучающее их устройство).

Процедура пассивного радиоконтроля Bluetooth сигналов начинается с поиска пакетов, соответствующих стандарту IEEE 802.15.1, и с установления моментов появления подобных пакетов на входе приемника РК. Потребность выявлять сигналы с произвольными кодами доступа к каналу препятствует применению классической корреляционной обработки. С другой стороны, ситуация, когда известной является преамбула и фрагмент сигнала, включающий последовательность Баркера с трейлером, является достаточно типичной для методов распознавания образов, поэтому поисковую процедуру будем искать как оконную операцию, результатом которой является оценка положения образа в массиве данных.

Представим обрабатываемые дискретные сигналы в виде векторов $\boldsymbol{x}$ в многомерном пространстве, размерность N которого равна количеству отсчетов в выборке. Образ – это односвязное множество векторных сигналов расположенных в N-мерном пространстве вокруг эталона $v^{(m)}$, определяемого априорными данными. При поиске образов в пространстве сигналов пространство сигналов E^N разбивается на $M+1$ попарно несовместных множеств: $E_0, E_1, ..., E_M : E_i \cap E_j = \varnothing$ для всех $i \neq j$. $\bigcup_{i=0}^{M} E_i = E^N$. Если же $x \in E_0$, то считается, что вектор $\boldsymbol{x}$ попал в область «неопределенности», то есть ни один из искомых образов с ним не ассоциируется.

Учитывая, что приемопередатчики стандарта Bluetooth используют для формирования радиосигналов гауссовскую частотную манипуляцию, в качестве эталонов целесообразно использовать сигналы, регистрируемые на выходе частотного дискриминатора приёмника РК, на вход которого поступает отфильтрованный сигнал отдельного Bluetooth-канала. В настоящей работе для фильтрации использовался рассчитанный минимаксным методом по алгоритму Паркса-Макклелана КИХ-фильтр с полосой пропускания $B = 1,6$ МГц, переходной полосой 1 МГц и уровнем подавления сигналов 80 дБ (для уверенного подавления близких по частоте сигналов в сложной радиообстановке, порождаемой большим количеством выходящих в эфир устройств). При низком уровне помех уровень подавления можно уменьшить, чтобы понизить порядок фильтра и сократить вычислительные затраты на фильтрацию.

На входе частотного дискриминатора действуют выборки квадратурных составляющих принимаемого случайного процесса $I(t_i)$ и $Q(t_i)$, где $i = 1,...,N$. Текущую фазу колебания можно определить по ним как

$$\varphi(t_i) = arctg\left(\frac{Q(t_i)}{I(t_i)}\right), \quad (2)$$

а для осуществления частотной демодуляции достаточно рассчитать последовательность значений x_i, выражаемых в радианах в секунду и определяемых разностью значений фазы

$$x_i = \frac{\varphi(t_{i+1}) - \varphi(t_i)}{t_{i+1} - t_i}, \quad (3)$$

где следует скорректировать фазовые углы при переходе через π, дополняя их значениями ±2π, чтобы убрать разрывы фаз.

Сформировав на основе априорной информации об отсчетах преамбулы-трейлера совокупность эталонных векторов $v^{(m)}$ $m = 1,...,M$, определяющих совокупность подлежащих распознаванию образов, далее необходимо для реально наблюдаемых на выходе частотного дискриминатора данных проанализировать расстояния $d_j^{(m)}$ между имеющим длительность поля САС фрагментом вектора $\boldsymbol{x}$, стартующим с отсчета x_j (j – индекс, соответствующий проверяемой гипотезе о моменте начала пакета), и эталонами $v^{(m)}$

$$d_j^{(m)} = \left\| v^{(m)} - \frac{2\pi}{\mu}\boldsymbol{x}_j \right\|^2 = \sum_{i=1}^{5\cdot n}\left[v_i^{(m)} - \frac{2\pi}{\mu} x_{j+i} \right]^2 + \sum_{i=1}^{11\cdot n}\left[v_{5\cdot n+i}^{(m)} - \frac{2\pi}{\mu} x_{61\cdot n+j+i} \right]^2, \quad (4)$$

где n – количество отсчетов на один символ битовой последовательности в предположении, что используемая частота дискретизации ровно в n раз превышает $1/T_S$.

В (4) первая сумма учитывает соответствующие эталону $v^{(m)}$ четыре символа преамбулы вместе с «c_0», вторая сумма учитывает «a_{23}» вместе с последовательностью Баркера и трейлером, а μ – величина индекса модуляции, которая может быть на практике неизвестна или варьироваться. Как следствие,

формально определение значения $\mu^{(m)}$, соответствующего минимуму расстояния $d^{(m)}$, где $m=1,...,M$, является вариационной задачей, но в рамках текущего исследовании условимся не рассматривать решение такой задачи и полагать, что индекс модуляции является константой.

Наиболее вероятный момент $j_{н.в.}^{(m)}$ появления эталона $v^{(m)}$ на входе приёмника РК соответствует минимуму расстояния $d_j^{(m)}$, так что физически алгоритм синхронизации построен на отыскании участка с минимальной разностной энергией между принятым и эталонным сигналами. Если значение решающей функции $d_j=\min\limits_m d_j^{(m)}$, где $m=1,...,M$, превышает пороговое значение h на всем анализируемом интервале, выносится решение об отсутствие пакета. Значение h подбирается эмпирически. Если для некоторого отсчета j_0 выполняется неравенство $d_{j_0}<h$, выносится решение о наличии сигнала. Итоговая оценка момента начала пакета определяется положением минимума решающей функции, на интервале, соответствующего длительности САС:

$$j_{н.в.}=\arg\min_j d_j,\ j=j_0,...,j_0+n\cdot 72. \qquad (5)$$

На рис. 2 представлена функция $d(t_i)$, полученная при частоте дискретизации $f_д=20$ МГц и отношении сигнал-шум (ОСШ) $q=10$ дБ для сформированного случайным образом пакета при различных значениях расстройки Δf между реальной центральной частотой сигнала и её номинальным значением. В подобных условиях при расстройках вплоть до максимально допустимой в соответствии со стандартом $\Delta f=75$ кГц минимум решающей функции хотя и имеет тенденцию к увеличению при росте Δf, но остается уверенно различимым на фоне шумов.

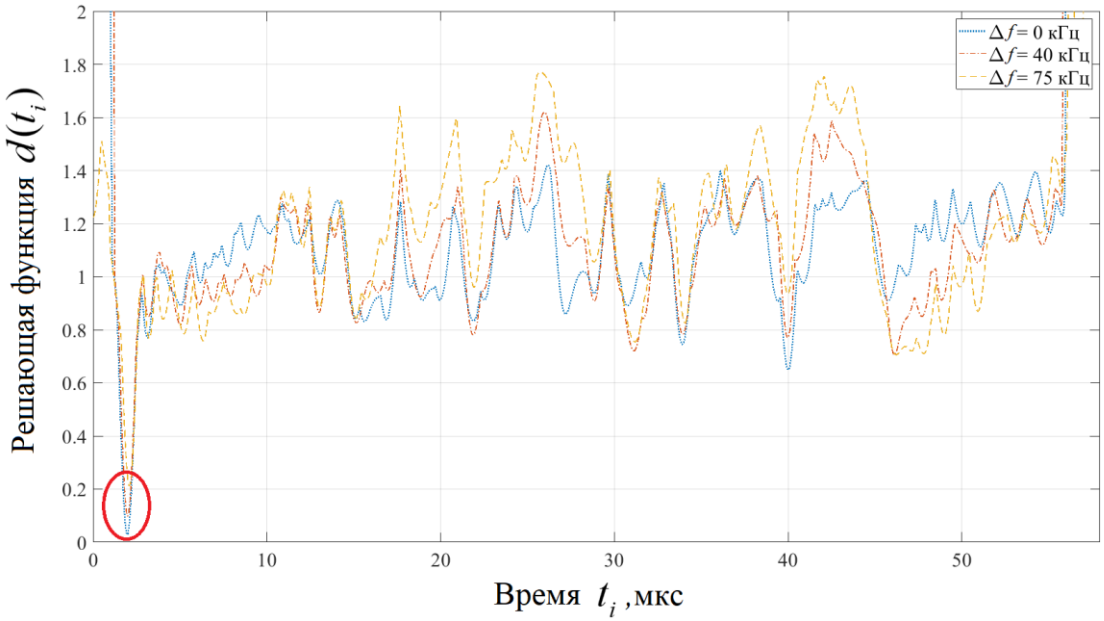


Рис. 2. График функции $d(t_i)$ при $q=10$ дБ, $f_д=20$ МГц

Следует отметить, что на практике частоту дискретизации по сравнению с значением $f_д = 20$ МГц можно заметно снизить; высокая частота дискретизации удобна при моделировании лишь тем, что упрощает визуальный контроль границ символов битовой последовательности. Однако при повышенной частоте дискретизации увеличивается размер буфера, необходимого для хранения и обработки исходной выборки, а нормированная полоса пропускания фильтра $B/f_д$ уменьшается, что вызывает завышение требуемого порядка фильтра. С другой стороны, понижение частоты дискретизации приводит к росту погрешности синхронизации во временной области, что влечет резкое снижение качества работы по мере приближения частоты дискретизации к 1 МГц; в связи с этим не следует понижать частоту дискретизации ниже $f_д = 4$ МГц. Диаграммы на рис. 3 демонстрируют поиск момента начала Bluetooth-сигнала при частоте дискретизации $f_д = 4$ МГц и указывают на сохранение работоспособности алгоритма при подобном 5-кратном понижении частоты дискретизации.

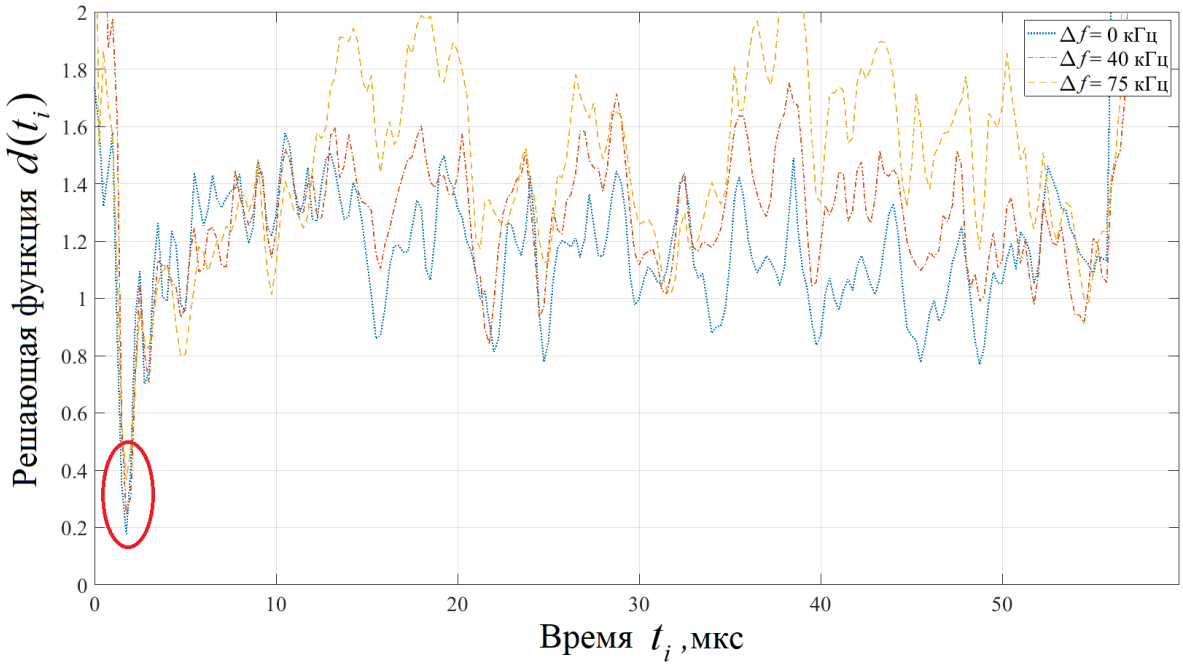


Рис. 3. График функции $d(t_i)$ при $q = 10$ дБ, $f_д = 4$ МГц

Частотная синхронизация и демодуляция символов

После обнаружения сигнала и установления временной синхронизации необходимо по принимаемому сигналу определить последовательность информационных бит. Существуют различные методы приема сигналов с гауссовской частотной манипуляцией [9, 10]; методы, инвариантные к амплитуде входного сигнала, могут обеспечить меньшую вероятность возникновения битовой ошибки (BER – Bit error rate) при одинаковом отношении сигнал/шум [9, 11]. С учетом этого, для каждого символа будем накапливать сигнал с выхода частотного дискриминатора на интервале передачи одного бита $T_S = 1$ мкс и сравнивать полученный результат с пороговым значением γ:

$$z_k = \frac{1}{n}\sum_{k=0}^{n} x_{j_{н.в.}+n\cdot k} \underset{H_1}{\overset{H_0}{\lessgtr}} \gamma, \quad (k = 0,...,K-1), \tag{6}$$

где n – количество отсчетов на один символ; K– количество декодируемых символов.

При отсутствии частотной расстройки оптимальным пороговым значением в (6) оказывается $\gamma = 0$. Для адаптации же порога γ к неизвестному частотному смещению Δf несущей частоты от номинала можно использовать следующий подход. Значения, поступающие с выхода частотного дискриминатора на интервале длительности пакета, упорядочиваются по возрастанию и определяется среднее арифметическое среди 10-20% наибольших и 10-20% наименьших значений, которое является достаточно точной оценкой частотной расстройки пакета. Отметим, что использовать просто среднее арифметическое всех принятых значений не рекомендуется, так как несовпадение числа нулей и единиц в принятом пакете будет при этом порождать погрешность оценивания [9], в то время как предложенная оценка сохранит свою высокую точность.

Предложенный способ демодуляции при частоте дискретизации $f_o = 20$ МГц обеспечивает заданную стандартом [1] величину $BER \le 10^{-3}$ при отношении сигнал/шум близком к $q = 3$ дБ. Влияние частоты дискретизации на процесс демодуляции можно проследить по рис. 4.

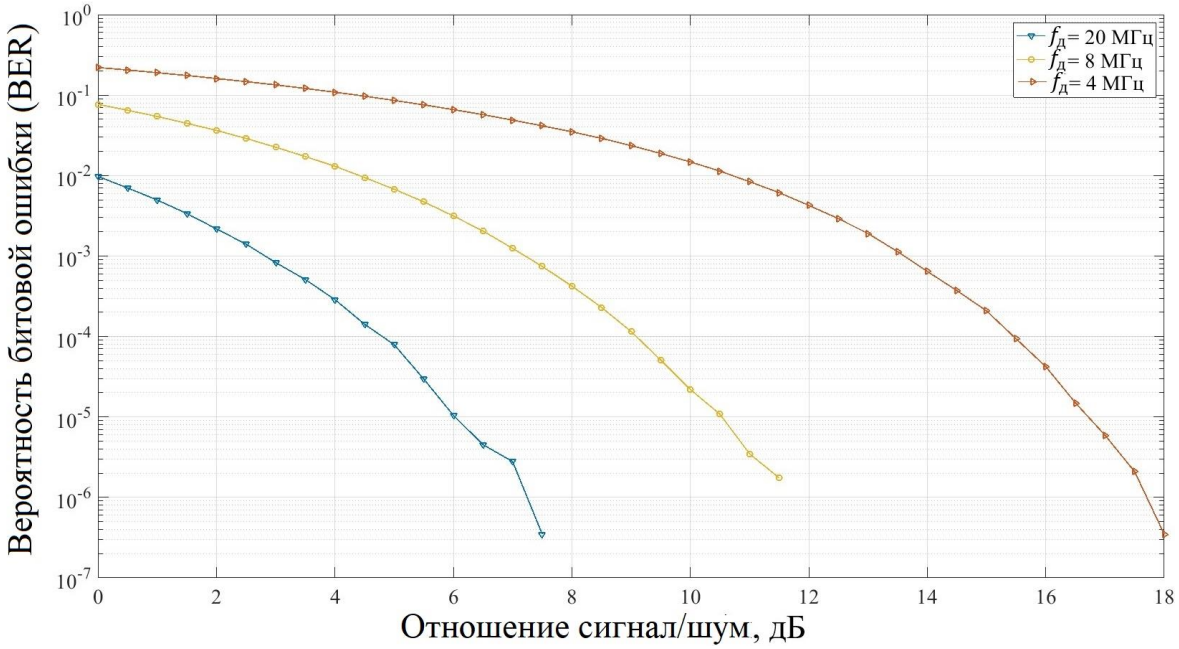


Рис. 4. Зависимость вероятности битовой ошибки
от отношения сигнал/шум

Декодирование информационных бит

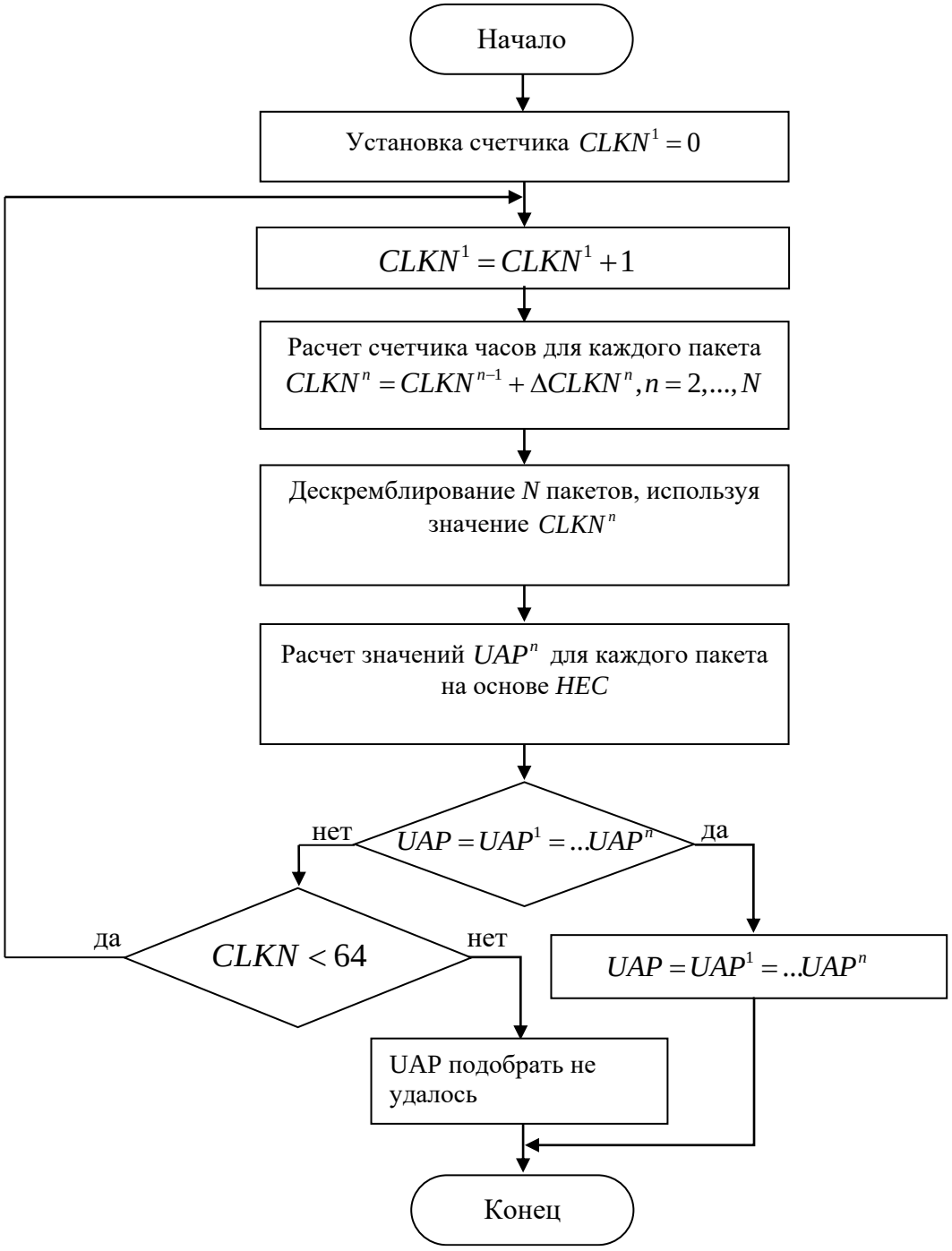
После получения битового потока следует декодировать код БЧХ и исправить ошибки в кодовом слове (если они есть). Различные методы декодирования БЧХ кодов представлены в работах [12, 13]. В случае синдромного декодирования, оптимальным способом является использование алгоритма Бер-

лекэмпа-Месси или Евклида для решения ключевого уравнения [12, 13]. Так как код систематический, то получить LAP можно, взяв соответствующие биты кодового слова. Затем осуществляется декодирование заголовка, например, с помощью мажоритарного декодирования [14]. После мажоритарного декодирования необходимо дескремблировать полученный битовый поток, соответствующий заголовку. Алгоритм дескремблирования представляет собой операцию «XOR» входного битового потока с псевдослучайной последовательностью, формируемой регистром сдвига с обратными связями, полином которого $g(x) = x^7 + x^4 + 1$. Инициализирующие значение такого регистра зависит от неизвестного системе РК текущим значением счетчика часов ведущего устройства $CLKN_{6-1}$ [1], что препятствует выполнению дескремблирования, принятый пакет – единственный. Однако, при регистрации и совместной обработке нескольких пакетов для получения информации о функционировании сети можно воспользоваться перебором значений $CLKN_{6-1}$ до тех пор, пока UAP не будет совпадать для всех N принятых пакетов. Блок-схема соответствующего алгоритма получения UAP показана на рис. 5. После получения UAP и декодирования заголовка следует извлечь информацию из полей LT_ADDR, тем самым получив информацию о ведомых устройствах сети.

Возможные результаты работы алгоритма декодирования заголовков пакетов показаны в табл. 3. Для удобства двоичные данные представлены в таблице в шестнадцатеричном виде. Приведенные результаты показывают успешность подбора счетчика $CLKN_{6-1}$ по 15-ти пакетам, что в представленном примере позволило извлечь информацию об UAP ведущего устройства, типы передаваемых пакетов и логический транспортный адрес LT_ADDR.

Таблица 3 – Декодирование заголовков пакетов

Время получения пакета, мкс	whitening header packet	$CLKN_{6-1}$	UAP	TYPE	LT_ADDR
5227	adbc	1c	90	POLL	1
5852	347f4	1d	90	NULL	1
95228	1150a	2c	90	POLL	1
95854	16942	2d	90	NULL	1
97730	20a86	30	90	3-DH5	1
100854	3692e	35	90	NULL	1
155230	f098	c	90	POLL	1
155855	8cd0	d	90	NULL	1
185231	1482e	3c	90	POLL	1
185856	2a266	3d	90	NULL	1
216481	3225a	2e	90	3-DH5	1
219606	21c9e	33	90	NULL	1
277731	3ef14	10	90	3-DH5	1
280856	28cbc	15	90	NULL	1
312107	31eb8	7	90	NULL	1



* $CLKN^n$ значение счетчиков часов $CLKN_{6-1}$, где n – номер пакета

Рис. 5. Алгоритм получения UAP

Минимальное количество пакетов, на основании которого возможно однозначно определить инициализирующее значение скремблера $CLKN_{6-1}$, зависит от ряда случайных факторов. Практическая апробация показывает, что для успешного декодирования, как правило, желательно иметь не менее 10 пакетов данных. Использование приемника с максимально широкой полосой одновременного обзора способствует сокращению времени накопления требуемого комплекта пакетов, однако процедура радиоконтроля может оказаться довольно

быстрой даже при сборе информации в не слишком широком диапазоне частот. Так, приведенные в табл. 3 данные получены при использовании приемника, контролирующего параллельно лишь 24 из 79 каналов Bluetooth на протяжении ~0.3 с. Этого оказалось достаточно для правильного определения 4 байтов MAC-адреса ведущего устройства (UAP и LAP) и выяснения количества активных устройств в анализируемой пикосети.

Пример работы анализатора

Разработанный способ обработки сигналов реализован в программно-аппаратном анализаторе сигналов Bluetooth на базе панорамного цифрового радиоприемного устройства семейства АРГАМАК [5] с полосой одновременной обработки сигналов 24 МГц, изображенного на рис. 6. Анализатор обеспечивает выявление и идентификацию работающих в диапазоне 2,4 ГГц и на нестандартных частотах устройств IEEE 802.15.1. Анализатор осуществляет обнаружение сигналов Bluetooth, частотно-временную синхронизацию, демодуляцию (приведение к битовому потоку), анализ служебных параметров протокола, а также определение идентификаторов активных устройств.

Рис. 6. Цифровое радиоприемное устройство семейства АРГАМАК

В цифровом радиоприемном устройстве осуществляется прием, цифровая фильтрация и формирование комплексной выборки сигнала, которая подается на ЭВМ, где производится дальнейшая обработка, включая декодирование пакетов на канальном уровне (link layer), определяемом спецификацией Bluetooth [1].

Пример работы анализатора показан на рис. 6, где помимо представленных в табл. 2 данных видны результаты анализа и других сетей Bluetooth, зафиксированных во всем диапазоне работы.

В качестве аппаратной базы могут использоваться и другие цифровые приемники, обеспечивающие формирование комплексной выборки сигнала в

полосе частот одновременного обзора не менее 1 МГц с частотой дискретизации не менее 2 МГц.

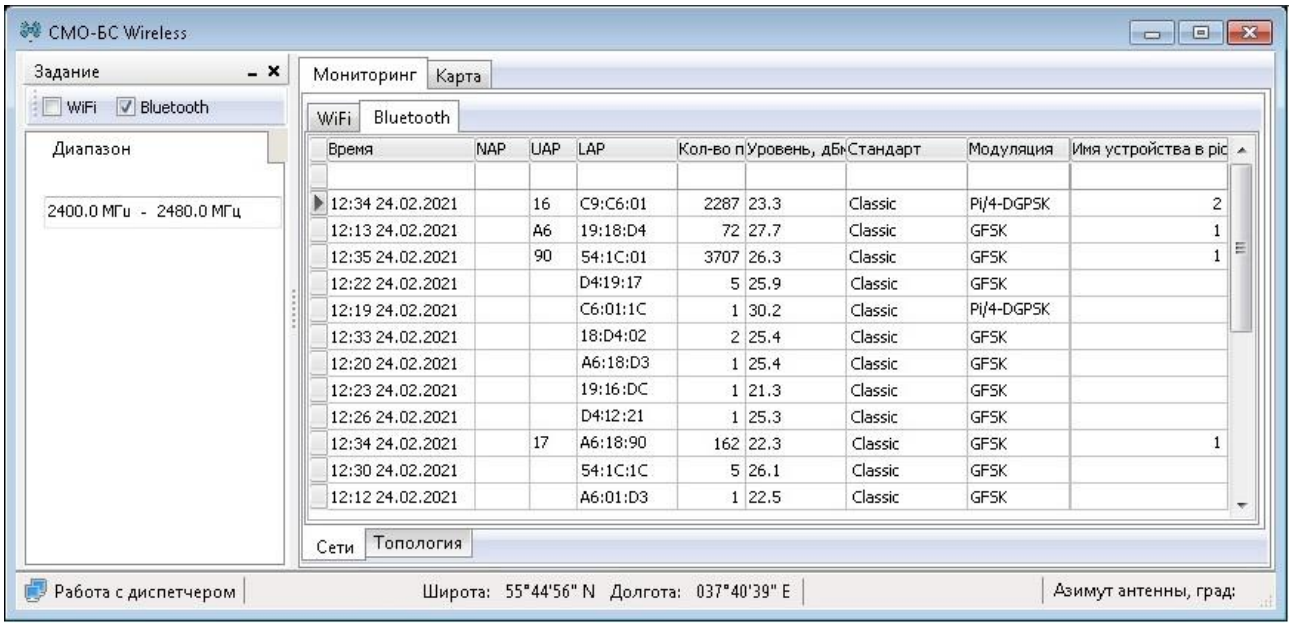


Рис. 6. Окно с результатами работы анализатора

Выводы

Разработанный способ анализа радиосигналов предназначен для пассивного радиоконтроля устройств и сетей Bluetooth. Элементом новизны представленного решения является одновременное обнаружение сигналов произвольного набора Bluetooth-передатчиков. При допускаемой стандартом частотной расстройке, не превышающей 75 кГц, уверенное обнаружение и анализ сигналов обеспечивается при отношениях сигнал-шум $q \geq 3$ дБ. Также к элементам новизны относится предложенный алгоритм декодирования служебных параметров сигналов, базирующийся на совместной обработке набора обнаруженных пакетов данных.

Рассмотренный способ анализа радиосигналов Bluetooth может быть реализован на основе цифровых радиоприемных устройств с полосой одновременной обработки сигналов от 1 МГц. В статье приведен пример анализатора радиосигналов Bluetooth на базе цифрового радиоприемного устройства семейства АРГАМАК с полосой 24 МГц, используемого в системах дистанционного обнаружения и локализации источников несанкционированных радиоизлучений в контролируемых объектах.

Литература

1. Bluetooth SIG, Specification of the Bluetooth System // Bluetooth SIG, Version 5.1, 21 January. 2019. – 2985 p.

2. Cominelli M., Gringoli F., Patras P., Lind M., Noubir G. Even Black Cats Cannot Stay Hidden in the Dark: Full-band De-anonymization of Bluetooth Classic Devices // IEEE Symposium on Security and Privacy. 2020. P. 534-548.

3. Tibenderana C., Weiss S. Efficient and Robust Detection of GFSK Signals under Dispersive Channel, Modulation Index and Carrier Frequency Offset Conditions // EURASIP Journal on Applied Signal Processing. 2005. P. 2719-2729.

4. Tibenderana C., Weiss S. A Low-Complexity High-Performance Bluetooth Receiver // IEE Colloquium on DSP enabled Radio, United Kingdom. 2003. P. 426-435.

5. Рембовский А. М., Ашихмин А. В., Козьмин В. А., Автоматизированные системы радиоконтроля и их компоненты / под ред. А. М. Рембовского. – М.: Горячая линия-Телеком, 2017. – 424 с.

6. Rembovsky A. M., Ashikhmin A. V., Kozmin V. A., Smolskiy S. M. Radio Monitoring Automated Systems and Their Components. – Springer, 2018. – 467 p.

7. Staszewski R. B. All-Digital Frequency Synthesizer in Deep-Submicron CMOS. – Wiley-Interscience, 2006. – 261 p.

8. Gehrmann C., Persson J., Smeets B. Bluetooth Security. – Artech House, 2004. – 209 p.

9. Robinson C. Optimisation of Bluetooth wireless personal area networks. – Durham theses, Durham University, 2004. – 157 p.

10. Schiphorst R., Hoeksema F., Slump K. Bluetooth Demodulation Algorithms and their Performance in Proc // Karlsruhe Workshop on Software Radios, 2002. P. 99-106.

11. Варакин Л. Е. Теория систем сигналов. – М.: Сов. радио, 1978. – 304 с.

12. Blahut R. E. Theory and Practice of Error Control Codes. – Addison Wesley, 1983. – 500 p.

13. Sweeney P. Error control coding. From theory to practice. – Wiley, 2002. – 252 p.

14. Морелос-Сарагоса Р. Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение. – М.: Техносфера, 2005. – 320 с.

References

1. Bluetooth SIG, Specification of the Bluetooth System // Bluetooth SIG, Version 5.1, 21 January. 2019. – 2985 p.

2. Cominelli M., Gringoli F., Patras P., Lind M., Noubir G. Even Black Cats Cannot Stay Hidden in the Dark: Full-band De-anonymization of Bluetooth Classic Devices. *IEEE Symposium on Security and Privacy*, 2020, pp. 534-548.

3. Tibenderana C., Weiss S. Efficient and Robust Detection of GFSK Signals under Dispersive Channel, Modulation Index and Carrier Frequency Offset Conditions. *EURASIP Journal on Applied Signal Processing*, 2005, pp. 2719-2729.

4. Tibenderana C., Weiss S. A Low-Complexity High-Performance Bluetooth Receiver. *IEE Colloquium on DSP enabled Radio*, United Kingdom, 2003, pp. 426-435.

5. Rembovsky A. M., Ashikhmin A. V., Kozmin V.A. *Avtomatizirovannyye sistemy radiokontrolya i ikh komponenty* [Automated radio monitoring systems and their components]. Moscow, Hotline-Telecom, 2017. 424 p. (in Russian).

6. Rembovsky A. M., Ashikhmin A. V., Kozmin V. A., Smolskiy S. M. *Radio Monitoring Automated Systems and Their Components*. Springer, 2018. 467 p.

7. Staszewski R. B. *All-Digital Frequency Synthesizer in Deep-Submicron CMOS*. Wiley-Interscience, 2006. 261 p.

8. Gehrmann C., Persson J., Smeets B. *Bluetooth Security*. Artech House, 2004. 209 p.

9. Robinson C. *Optimisation of Bluetooth wireless personal area networks*. Durham theses, Durham University, 2004. 157 p.

10. Schiphorst R., Hoeksema F., Slump K. Bluetooth Demodulation Algorithms and their Performance in Proc. 2nd. *Karlsruhe Workshop on Software Radios*, 2002, pp. 99-106.

11. Varakin L. E. *Teoria sistem signalov* [Theory of signal systems]. Moscov, Sov. Radio, 1978. 304 p. (in Russian).

12. Blahut R. E. *Theory and Practice of Error Control Codes*. Addison Wesley, 1983. 500 p.

13. Sweeney P. *Error control coding. From theory to practice*. Wiley, 2002. 252 p.

14. Robert H. Morelos-Zaragoza. *The Art of Error Correcting Coding*. Wiley, 2002. 238 p.

15. Rembovsky A. M., Ashikhmin A. V., Kozmin V.A. *Radiomonitoring – zadachi, metody, sredstva* [Radio monitoring – tasks, methods, means]. Moscow, Hotline-Telecom, 2015. 640 p. (in Russian).

Статья поступила 5 марта 2021 г.

Информация об авторах

Фаустов Иван Сергеевич – инженер-программист. АО «ИРКОС». Область научных интересов: радиомониторинг, цифровая обработка сигналов. E-mail: faustov.97@bk.ru

Токарев Антон Борисович – доктор технических наук, доцент. Профессор кафедры радиотехники. Воронежский государственный технический университет. Профессор кафедры информационной безопасности и систем связи. Международный институт компьютерных технологий. Старший научный сотрудник научно-исследовательского сектора. АО «ИРКОС». Область научных интересов: широкополосный радиомониторинг, алгоритмы цифровой обработки сигналов. E–mail: TokarevAB@ircoc.vrn.ru

Сладких Владимир Александрович – кандидат технических наук. Начальник научно-исследовательского сектора. АО «ИРКОС». Область научных интересов: радиомониторинг, цифровая обработка сигналов. E–mail: sladkihva@ircoc.vrn.ru

Козьмин Владимир Алексеевич – кандидат технических наук, доцент. Директор по научной работе. АО «ИРКОС». Область научных интересов: алгоритмы радиомониторинга. E–mail: kv@ircoc.vrn.ru

Крыжко Игорь Борисович – кандидат технических наук, доцент. Доцент кафедры программного обеспечения и администрирования информационных систем. Воронежский государственный университет. Старший научный сотрудник научно-исследовательского сектора. АО «ИРКОС». Область научных интересов: алгоритмы радиомониторинга. E–mail: kryzhkoib@ircoc.vrn.ru

Адрес: 394024, Россия, г. Воронеж, Рабочий пр., д. 101б.

Radio monitoring of Bluetooth signals service parameters

I. S. Faustov, A. B. Tokarev, V. A. Sladkikh, V. A. Kozmin, I. B. Kryzhko

***Problem statement**: Rapid growth in the use of wireless technologies has seen a marked increase in the last decade. This entails the need to develop radio monitoring tools for devices and data networks, and, in particular, for wireless personal networks of the Bluetooth standard. Passive monitoring of Bluetooth signals with an unknown MAC-address cannot be implemented based on classical correlation processing. The task of network analyzing is complicated when trying to dewhitening a packet. The source information is not enough for decoding of link layer packet specified in the Bluetooth standard**. **Purpose**: The aim of the work is to develop algorithms for receiving Bluetooth signals and analyzing their service parameters, as well as to build a software and hardware analyzer of Bluetooth signals based on the developed algorithms. **Novelty:** the proposed method differs from the known ones by the ability to detect signals for random of Bluetooth transmitters and decode their service parameters without the need to exchange requests and responses between the analyzer and Bluetooth devices. **Practical relevance:** the proposed method can be used to build a Bluetooth signal analyzer on an SDR with a band of simultaneous signal processing from 1 MHz. The Bluetooth network analyzer, implemented on the basis of a digital radio receiver of the ARGAMAK family, serves as the basis for the device for searching and localizing unauthorized radio sources in controlled objects*

***Key words:** Bluetooth, WPAN, signal detection, passive radio monitoring, service parameters of signals.*

Information about Authors

Ivan Sergeevich Faustov – software engineer. JSC «IRCOS». Field of research: radio monitoring, digital signal processing. E-mail: faustov.97@bk.ru

Anton Borisovich Tokarev – Advanced Doctor of Engineering Sciences, docent. Professor of the Department of Radio Engineering. Voronezh State Technical University. Professor of the Department of Information Security and Communication Systems. International Institute of Computer Technology. Senior Researcher at the Research sector. JSC «IRCOS». Field of research: wideband radiomonitoring, digital signal processing algorithms. E–mail: tokarevab@ircoc.vrn.ru

Vladimir Alexandrovich Sladkikh – Ph.D. of Engineering Sciences. Head of the Research Sector. JSC «IRCOS». Field of research: radiomonitoring, digital signal processing. E–mail: sladkihva@ircoc.vrn.ru

Vladimir Alekseevich Kozmin – Ph.D. of Engineering Sciences, Docent. Director for scientific works. JSC «IRCOS». Field of research: Algorithms for Radio Monitoring. E–mail: kv@ircoc.vrn.ru

Igor Borisovich Kryzhko – Ph.D. of Engineering Sciences, Docent. Associate Professor of the Department of Software Development and Information Systems Administration. Voronezh State University. Senior Researcher at the Research sector. JSC «IRCOS». Field of research: Algorithms for Radio Monitoring. E–mail: kryzhkoib@ircoc.vrn.ru

Address: 394024, Russia, Voronezh, Rabochiy prospect, 101b.