УДК 681.3.06:519.248.681 **DOI:10.30837/rt.2020.2.201.07**

И.Е. АНТИПОВ, д-р техн. наук, Т.А. ВАСИЛЕНКО

ИДЕНТИФИКАЦИЯ МОБИЛЬНЫХ УСТРОЙСТВ ПО ОСОБЕННОСТЯМ СПЕКТРОВ ИХ СИГНАЛОВ

Введение

Стремительное развитие Wi-Fi сетей охватывает все сферы человеческой деятельности. Принцип построения беспроводных сетей несет в себе не только преимущества в виде свободного перемещения в зоне покрытия, достаточной скорости передачи данных и низкой стоимостью развертывания, но и множество уязвимостей и угроз. Стандартные меры защиты не обеспечивают должной безопасности [1, 2]. По данным лаборатории Касперского [3] любая Wi-Fi сеть с шифрованием WPA или WPA2 может подвергнуться атаке с переустановкой ключа.

Учитывая множество недостатков и уязвимостей, позволяющих злонамеренным воздействиям успешно преодолеть системы защиты информации, актуальным следует считать исследования, направленные на комплексное обеспечение безопасности, использование дополнительных параметров для обнаружения несанкционированного доступа и выявления злоумышленников.

Анализ литературных данных и постановка задач

Ранее авторами была разработана модель принятия решений об аномальном состоянии Wi-Fi сетей [4]. В работе были предложены методы для минимизации недостатков существующих систем обнаружения. С помощью этой модели проблема определения границы решается путем использования элементов нечеткой логики, а проблема адаптивности сети – путем учета параметров, влияющих на состояние сети, в том числе местоположение пользователей [5]. Главной проблемой в обеспечении безопасности остается задача идентификации абонентских Wi-Fi устройств (ноутбуков, планшетов, мобильных телефонов, видеокамер и т.д.), так как злоумышленники ради получения выгоды активно совершенствуют методы несанкционированного подключения. Для идентификации и аутентификации в основном используют SSID, PIN, MAC-адрес, пароли и секретные ключи. Было бы уместным рассмотреть идентификацию пользователей по еще одному параметру – спектральному составу их сигналов. Предполагается, что по заранее известным спектрам мобильных устройств, хранящихся в базе, можно идентифицировать пользователей беспроводной сети.

В работе [6] авторы с помощью многоспектрального анализа идентифицируют сигналы на известном фоне. Способ основан на использовании нормированных калиброванных спектров фона и возможных объектов и использовании процедуры ортогонализации, при которой находится модуль ортогональной проекции к векторам фона, и объектов в расширенном многомерном пространстве. Несмотря на практическую значимость исследований [6], для беспроводных сетей они не применимы, так как рассчитаны для обнаружения физических объектов.

Для идентификации телевизионных станций на частотах от 40 до 60 МГц [7] в своих исследованиях автор использует нестабильность частоты. Гетеродин приемника был синхронизирован с выходом термостатированного опорного источника частоты (опорный источник синтезатора частоты Ч6-31, нестабильность 10^{-8} (1 Гц на 100 МГц). При времени измерения в 0,1 с (отраженный от метеорного следа сигнал) и использовании счетного метода оценки частоты погрешность составляет 10 Гц. Для идентификации станций (ТВ радиопередатчиков) погрешности в 10 Гц было достаточно.

В открытой литературе фактически отсутствуют исследования, связанные с идентификацией устройств по спектральным характеристикам сигнала. Работы [6, 7] не имеют прямого отношения к беспроводным Wi-Fi сетям, которые имеют ряд своих особенностей. Следо-

вательно, необходимы дополнительные исследования, направленные на идентификацию беспроводных устройств в сети Wi-Fi по спектральному анализу их сигналов.

Цель и задача исследования

Цель исследования – оценка применимости детального анализа спектра сигналов, излучаемых устройствами, подключенными к беспроводным сетям, для их идентификации.

Для достижения поставленной цели необходимо решить следующие задачи:

– экспериментально измерить спектры беспроводных устройств, подключенных к сети Wi-Fi;

– проанализировать полученные результаты и оценить возможность использования спектра для идентификации мобильных устройств.

Материалы и методы исследования для измерения частотного спектра устройств, подключенных к беспроводной сети

Стандарт IEEE 802.11 определяет параметры спектра Wi-Fi канала (рис. 1.) [8].

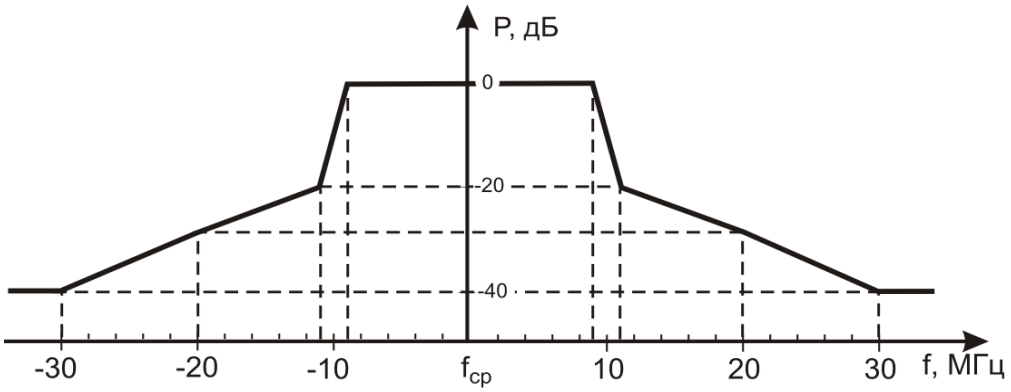

Рис. 1. Спектральная маска каналов Wi-Fi

Все стандарты беспроводной Wi-Fi сети, начиная с 802.11a, имеют OFDM (Orthogonal frequency-division multiplexing – мультиплексирование с ортогональным частотным разделением каналов) модуляцию [8]. На рис. 2 представлена схема OFDM модулятора.

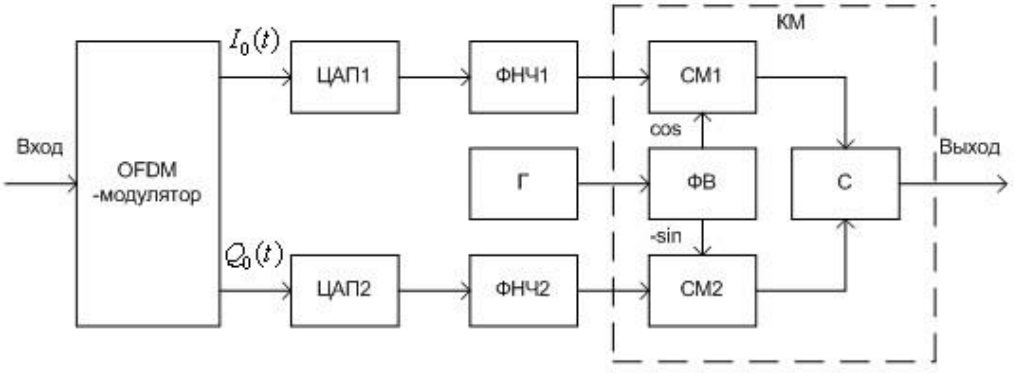

Рис. 2. Схема OFDM модулятора

При реализации OFDM на компьютерной модели спектр получается таким, как показан на рис. 3. Можно сделать вывод, что спектр получается:

- симметричным относительно средней частоты;
- практически равномерным в пределах +/- 25 МГц от средней частоты;
- резко убывающим за пределами +/- 25 МГц от средней частоты.

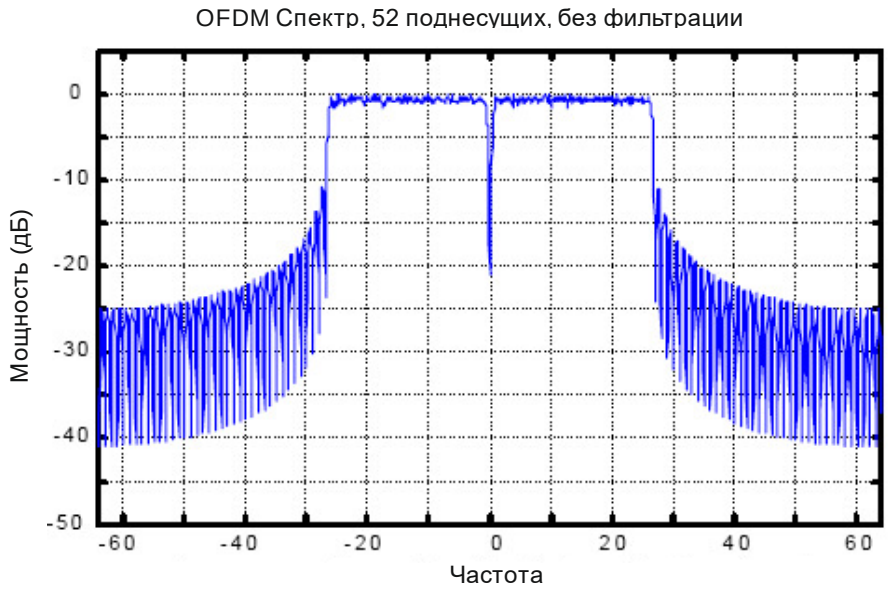

Рис. 3. Спектр OFDM сигнала

В реальных условиях спектр может отличаться от идеального:
- из-за особенностей схемы или программного кода, реализующей модуляцию;
- неидентичности элементов схем, различных задержек в них;
- зависимости параметров схем от напряжения питания и температуры;
- особенностей схем выходных каскадов передатчиков и выходных фильтров;
- различий в конструкциях антенн и корпусов оборудования.

Это может приводить к следующим отклонениям:
- несимметричности спектра;
- нестабильности средней частоты сигнала;
- возникновению аномалий в спектре в виде «горбов» или «провалов»;
- возникновению высших гармоник и т. д.

Анализ технической документации, находящейся в открытом доступе, к сожалению, не позволил найти какие-либо численные значения указанных отклонений для выпускаемого Wi-Fi оборудования. (Возможно, они не предназначены для открытой публикации, возможно, их действительно нет.) Сложности возникли даже при поиске электрических принципиальных схем Wi-Fi передатчиков, по которым можно было бы сделать вывод об их характеристиках.

Поэтому в дальнейшем нам придется ориентироваться только на собственные экспериментальные исследования.

Для измерения спектра устройств, подключенных к Wi-Fi сети, был выбран анализатор спектра Signal Hound USB-SA44B – цифровой анализатор спектра и измерительный приемник диапазона от 1 до 4,4 ГГц с предварительным ВЧ усилителем. Основой Signal Hound является узкополосный приемник с преобразованием ПЧ сигнала в цифровую форму с максимальной полосой пропускания в 250 кГц. Он принимает до 2 МБ квадратурных данных каждую секунду, которые затем могут быть отображены в графическом виде. Блок-схема, приведенная на рис. 4 [9], отображает главные элементы структуры устройства. Подавление зеркального канала выполняется смешиванием верхней и нижней боковой полос и дальнейшей математической обработкой.

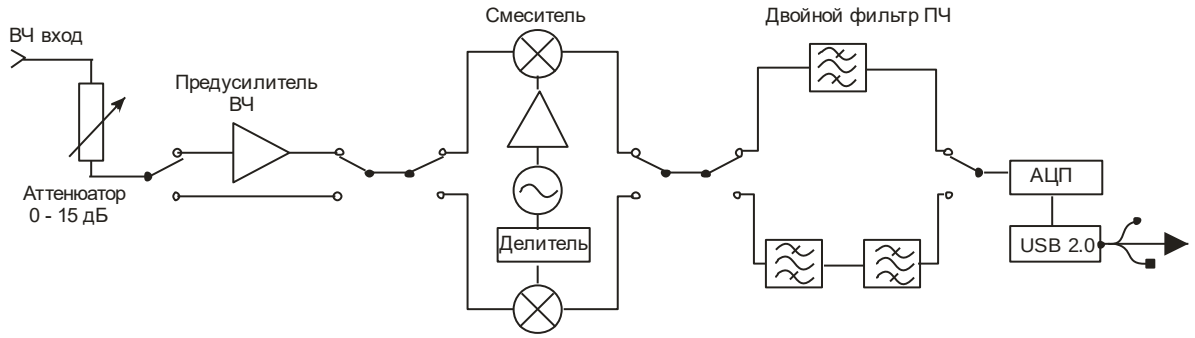

Рис. 4. Упрощенная блок-схема анализатора спектра SignalHound USB-SA44B

Экспериментальные исследования по измерению спектра мобильных устройств, подключенных к беспроводной Wi-Fi сети

Экспериментальные исследования проводились на кафедре Компьютерной радиоинженерии и систем технической защиты информации Харьковского национального университета радиоэлектроники. Для измерений были взяты пять различных мобильных устройств, которые подключались к одной и той же точке доступа. На каждом из устройств запускалось одно и то же приложение (web-браузер) и одна и та же задача – воспроизведение одного и того же видеофайла из Интернета.

Регистрация производилась на анализаторе спектра Signal Hound USB-SA44B, подключенном к компьютеру, на котором установлено программное обеспечение Spike (VSG version 1.0.4; Spike version 3.2.3).

Для каждого из мобильных устройств измерение проводилось в четырех положениях относительно приемной антенны (рис. 5) по четыре раза. Каждое измерение (накопление) спектральных отсчетов длилось около трех минут. Таким образом, всего было выполнено 80 измерений общей длительностью ~4 часов. Кроме того, проводились измерения при изменении температуры устройства.

1 2 3 4

Рис. 5. Положение устройства относительно приемной антенны

В результате каждого измерения программа формировала файл данных $P_L(f)$, f = 2,411 – 2,433 с шагом 2 кГц. Значение мощности на каждой частоте выражалось в относительных единицах (дБм). На рис. 6 представлены результаты измерений для двух устройств в разных положениях.

Для сравнения двух спектров вычислялась величина

$$D_{L1,L2} = \sqrt{\frac{1}{N}\sum_{n=1}^{N}\left(P_{L1}(f_n) - P_{L2}(f_n) + P_0\right)^2}, \quad (1)$$

где N – количество частот, P_0 – константа для учета различий в средней мощности двух сигналов, которая подбиралась вручную по минимуму D.

Константу P_0 пришлось ввести из-за того, что средняя мощность у разных устройств и даже у одного и того же устройства в разных положениях отличалась в пределах ± 10 дБ.

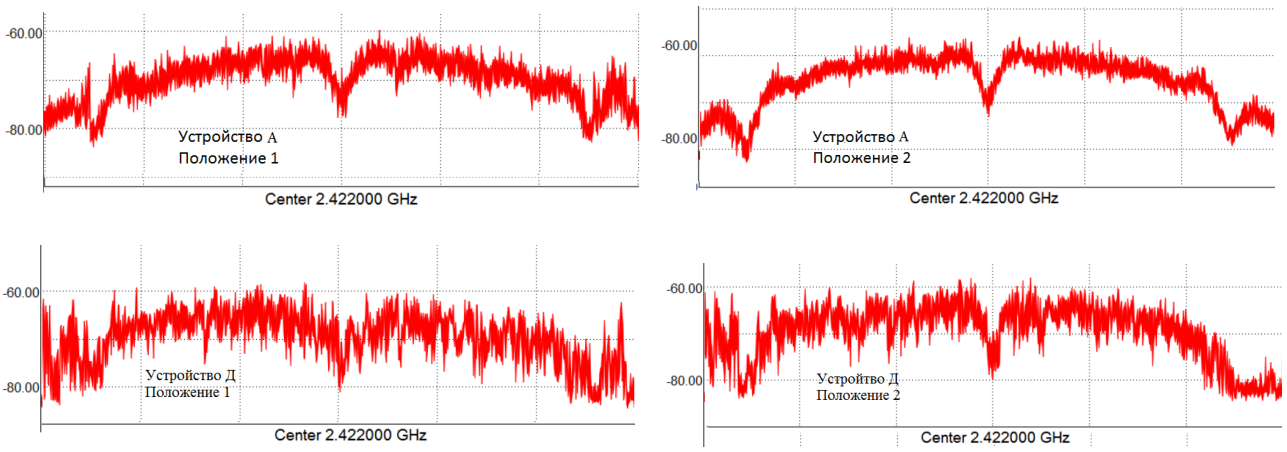

Рис. 6. Результаты измерений для двух устройств в разных положениях.

Все измерения, за исключением «Б», проводились при комнатной температуре. Серии измерений для разных устройств были обозначены:

А – Смартфон Redmi note 4X;

Б – Смартфон Redmi note 4X (тот же «А», но при температуре +5 ^{0}С.);

В – Смартфон Redmi note 4X, аналогичный «А», но другой экземпляр;

Г – Смартфон Meizu M5 Note;

Д – Смартфон Honor 09 Lite;

Е – Смартфон Meizu M6 Note;

Результаты измерений представлены в таблицах. В табл. 1 сопоставляются два разных смартфона одной модели в разных положениях, в табл. 2 один и тот же смартфон в разных положениях, в табл. 3 сравниваются два разных смартфона в разных положениях. В таблицах буква обозначает модель смартфона в соответствии с приведенными выше обозначениями, цифра – номер положения согласно рис. 5.

Таблица 1

	В1	В2	В3	В4
А1	1,3	1,2	1,0	0,9
А2	1,1	1,0	1,3	1,5
А3	1,1	1,0	1,3	1,1
А4	1,2	1,2	1,3	1,3

Таблица 2

	В1	В2	В3	В4
В1	0	0,9	1,0	1,1
В2	0,9	0	0,6	0,7
В3	1,0	0,6	0	0,6
В4	1,1	0,7	0,6	0

Таблица 3

	Г1	Г2	Г3	Г4
А1	2,3	2,8	2,5	3,0
А2	3,2	3,7	2,9	2,6
А3	2,3	2,9	2,4	2,4
А4	2,6	3,0	3,0	2,9

Значения, усредненные по всем четырем положениям, для всех исследованных смартфонов приведены в табл. 4. Разброс значений в пределах каждого усреднения сопоставим с разбросом для одного и того же устройства (табл. 2).

Таблица 4

	А	Г	Д	Е
А	1,1	3,5	4,3	2,1
Г	3,5	1,5	4,4	3,4
Д	4,3	4,4	1,5	3,9
Е	2,1	3,4	3,9	1,2

Также было исследовано влияние температуры. В табл. 5 сравниваются спектры одного и того же смартфона при комнатной температуре и при температуре +5 ^{0}C без поправки на сдвиг частот. Затем для учета смещения частоты в выражение (1) была внесена поправка j,

$$D_{L1,L2} = \sqrt{\frac{1}{N}\sum_{n=1}^{N}\left(P_{L1}(f_n) - P_{L2}(f_{n+j}) + P_0\right)^2}\,, \qquad (2)$$

позволившая «сдвигать» спектр охлажденного устройства в исходное состояние. Эта поправка подбиралась вручную в пределах 2 – 3 единицы (4…6 кГц) для минимизации значения D. Сопоставление спектров после внесения поправки представлено в табл. 6.

Таблица 5

	Б1	Б2	Б3	Б4
А1	1,83	1,18	1,7	1,84
А2	2,85	1,9	1,37	1,38
А3	2,16	1,46	1,49	1,57
А4	2,57	1,66	1,58	1,65

Таблица 6

	Б1	Б2	Б3	Б4
А1	1,82	1,18	1,63	1,72
А2	2,26	1,9	1,25	1,17
А3	2,16	1,33	1,33	1,33
А4	2,57	1,66	1,4	1,43

Анализ результатов

Даже при визуальном анализе (рис. 6) можно сделать вывод, что спектр излучения у одного и того же устройства хоть и меняется при его повороте, но несущественно (в большей мере меняется мощность). Вместе с тем, спектр излучения у разных устройств заметно различается.

Обобщенные результаты измерений показаны в виде диаграммы на рис. 7.

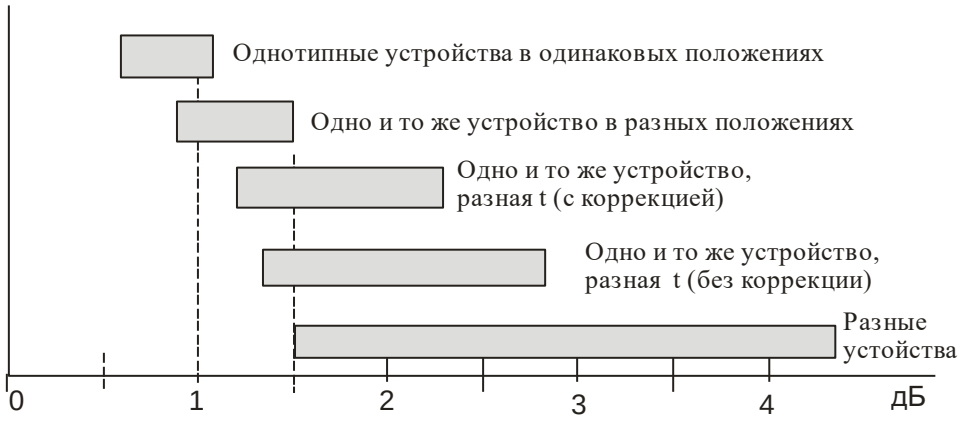

Рис. 7. Результаты измерений

На диаграмме показаны диапазоны значений, которые могут принимать средние квадраты разностей спектральных отсчетов для разных устройств. Из рисунка видно, что если значение разности оказывается меньше 1,5 дБ, то это однозначно одно и то же устройство. Если разность оказывается больше 2,8 дБ, то очевидно, что это разные устройства. Диапазон 1,5 – 2,8 дБ представляет собой область неопределенности – такие разности могут относиться как к одному и тому же устройству, так и к разным.

Дополнительная обработка спектра, позволяющая учесть температурную поправку, сужает область неопределенности до 1,5 – 2,2 дБ. Если же исключить влияние температуры, то область неопределенности практически исчезает (остается точка вблизи 1,5 дБ).

Также следует отметить, что понижение температуры приводит не только к смещению средней частоты спектра, но и к изменению вида спектральной характеристики. По-видимому, от температуры изменяются характеристики элементов схемы передатчика.

Наличие высших (2-й и 3-й) гармоник в составе сигнала Wi-Fi передатчиков предполагалось, но экспериментально не выявлено, по крайней мере, пригодного для измерений уровня.

Результаты экспериментальных исследований по измерению спектра мобильных устройств говорят о применимости данного метода для идентификации мобильных устройств, что позволит качественно дополнить существующую модель обеспечения безопасности [4], уменьшив риски несанкционированных действий. Недостатком идентификации абонентов беспроводной сети по спектру излучаемого им сигнала является то, что спектры разных устройств, но одной и той же модели, имеют не слишком явные отличия, что может привести к ошибкам.

Выводы

1. При помощи анализатора спектра Signal Hound USB-SA44B, точки доступа и шести мобильных устройств экспериментально получены спектры для каждого устройства в четырех разных положениях. Одно устройство исследовалось при различных температурах.

2. Предложен метод сравнения спектров различных устройств путем вычисления среднего квадрата разности соответствующих спектральных отсчетов с учетом различий в средней мощности разных сигналов.

3. Экспериментально установлено сходство спектров Wi-Fi сигналов одного и того же устройства в разных положениях и существенные различия в спектрах излучения у разных устройств, что может быть использованы для их идентификации.

4. Установлен диапазон значений средних квадратов разностей спектральных отсчетов, который может соответствовать как одному и тому же устройству в разных положениях, так и разным устройствам. Для идентификации устройств в этом диапазоне необходимо осуществлять более детальный анализ спектра, либо использовать другие методы.

Дальнейшие исследование целесообразно развивать в направлении дополнительных методов анализа спектра мобильных устройств и экспериментальным исследованиям модели принятия решений об аномальном состоянии сети [4] с учетом рассмотренного параметра.

Список литературы:

1. Котов В. Д., Васильев В. И. Современное состояние проблемы обнаружения сетевых вторжений // Вестник Уфимского государственного авиационного технического университета. 2012. Т. 16, № 3 (48). С. 198–204.

2. Лось А. Б., Даниелян Ю. Ю. Сравнительный анализ систем обнаружения вторжений, представленных на отечественном рынке // Вестник Московского финансово-юридического университета. 2014. С. 181–187.

3. KRACK: ваш Wi-Fi больше не безопасен // Kaspersky daily. URL: https://www.kaspersky.ru/blog/krackattack/19022/

4. Антипов И. Е., Ященко Т. А., Насиф Н. Т. Применение нечеткой логики для повышения безопасности беспроводных сетей на базе технологии Wi-Fi // Радиотехника. 2011. № 165. С. 103–106.

5. Антипов И. Е., Василенко Т. А. Усовершенствование модели принятия решений об аномальном состоянии сети системой позиционирования // Восточно-европейский журнал передовых технологий. 2019. № 1/9 (97). С.6

6. Герус А. В., Савченко Е. В., Саворский В. П. Алгоритм распознавания акустических, оптических, электрических сигналов от слабых источников в присутствии известного фона // Журнал радиоэлектроники. 2017. №11. С. 1–13.

7. Кукуш В.Д. Совершенствование метеорной радиотехнической системы мониторинга динамических параметров атмосферы Земли по сигналам телевизионного вещания : дис. … канд. техн. наук. Харьков, 2012. 165 с.

8. Современные беспроводные сети: состояние и перспективы развития / И.А. Гепко, В.Ф. Олейник, Ю.Д. Чайка, А.В. Бондаренко. Киев : ЕКМО, 2009. 672 с.

9. Signal Hound USB-SA44B.Версия 2.11A .Инструкция пользователя. Test Equipment Plus, 2010. 39 с.

Харьковский национальный
университет радиоэлектроники

Поступила в редколлегию 11.03.2020