УДК 004.7

Ю.И. Стародубцев, Е.В. Сухорукова, А.С. Корсунский, Т.Н. Масленникова, А.В. Вершенник

ЗАДАЧА ОБНАРУЖЕНИЯ НЕСАНКЦИОНИРОВАННО УСТАНОВЛЕННЫХ РАДИОЭЛЕКТРОННЫХ УСТРОЙСТВ И СПОСОБ ЕЕ РЕШЕНИЯ

Стародубцев Юрий Иванович, *доктор военных наук, профессор, окончил Кемеровское высшее военное командное училище связи, Военную академию связи им. С.М. Буденного. Заслуженный деятель науки РФ, академик Российской Академии военных наук, Академии безопасности и правопорядка, Российской Академии естественных наук, Арктической академии, почетный работник высшего профессионального образования. Профессор ВАС. Имеет монографии, учебные пособия, статьи и изобретения в области защиты информационного ресурса систем военной связи и АСУ в условиях информационной войны. [e-mail: vas@mail.ru].*

Сухорукова Елена Валерьевна, *кандидат технических наук, окончила Новочеркасский военный институт связи, адъюнктуру ВАС им. С.М. Буденного. Преподаватель кафедры «Безопасность информационно-телекоммуникационных систем специального назначения» ВАС им. С.М. Буденного. Имеет статьи и изобретения в области информационной безопасности. [e-mail: sukhorukova_lena@mail.ru].*

Корсунский Андрей Сергеевич, *кандидат технических наук, окончил факультет радиосвязи Ульяновского филиала Военного университета связи, адъюнктуру ВАС им. С.М. Буденного. Главный специалист ФНПЦ АО «НПО «Марс». Имеет статьи и изобретения в области радиоэлектронной защиты, безопасности связи и информации, а также передачи информации по беспроводным каналам связи информационно-телекоммуникационных систем. [e-mail: aksspb@mail.ru].*

Масленникова Татьяна Николаевна, *кандидат технических наук, окончила радиотехнический факультет Ульяновского политехнического института. Начальник научно-исследовательской лаборатории ФНПЦ АО «НПО «Марс». Имеет труды и публикации в области информационного обеспечения автоматизированных систем специального назначения. [e-mail: mars@mv.ru].*

Вершенник Алексей Васильевич, *окончил Ставропольское высшее военное инженерное училище связи, Военную академию РВСН. Преподаватель кафедры «Безопасность информационно-телекоммуникационных систем специального назначения» ВАС им. С.М. Буденного. Имеет статьи и изобретения в области информационной безопасности. [e-mail: alex14121972@mail.ru].*

Аннотация

Современный этап развития российского общества характеризуется существенным возрастанием роли и актуальности проблем обеспечения безопасности во всех сферах жизнедеятельности. Одной из основных задач в этой области становится борьба с промышленным (экономическим) шпионажем, который ведется с целью завоевания рынков сбыта, исключения технологических прорывов конкурентов, срыва переговоров по контрактам, перепродажи фирменных секретов и т. д. Одними из самых распространенных технических средств съема информации являются радиоизлучающие закладные устройства. Однако существующие средства контроля не перекрывают возможностей, заложенных в совре-

менных радиозакладных устройствах. В статье рассмотрена задача определения несанкционированно установленных радиоэлектронных устройств систем негласного съема информации, используемых в целях шпионажа, и предложен способ ее решения. Предлагаемый способ относится к области радиомониторинга электронного оборудования в контролируемой зоне и обеспечивает обнаружение сигналов в условиях отсутствия априорных сведений об их параметрах, а также позволяет определить основную частоту работы.

Ключевые слова: информационная безопасность, устройства негласного съема информации, радиозакладки.

THE PROBLEM OF DETECTING ELECTRONIC DEVICES INSTALLED WITHOUT AUTHORIZATION AND THE METHOD OF ITS SOLUTION

Iurii Ivanovitch Starodubtsev, *Doctor of Military Sciences, Professor; graduated from Kemerovo Higher Military Command School of Communications and the Marshal Budjonny Military Academy of Signal Corps; Honored Worker of Science of the Russian Federation, Academician of the Russian Academy of Military Sciences, Security Forces Academy, Russian Academy of Natural Sciences, Arctic Academy of Sciences; Honored Worker of Higher Professional Education, Professor of Military Communications Academy; an author of monographs, manuals, articles, and inventions in the field of information-resources security of military communication systems and computer-aided control systems in infowar contexts. e-mail: vas@mail.ru.*

Elena Valerievna Sukhorukova*, Candidate of Engineering; graduated from Novocherkassk Military Communications Institute; finished his post-graduate studies at the Marshal Budjonny Military Academy of Signal Corps; Lecturer at the Department 'Security of Information and Telecommunication Systems of Social Purposes' of the Marshal Budjonny Military Academy of Signal Corps; an author of articles and inventions in the field of information security. e-mail: sukhorukova_lena@mail.ru.*

Andrei Sergeevich Korsunskii, *Candidate of Engineering; graduated from the Faculty of Radio-Communications at Ulyanovsk Branch of the Military Communications University; finished his post-graduate studies at the Marshal Budjonny Military Academy of Signal Corps; Chief Specialist at FRPC JSC 'RPA 'Mars'; an author of articles and inventions in the field of radioelectronics protection, communications, and information security as well as data transmission through wireless communication channels in information telecommunication systems. e-mail: aksspb@mail.ru.*

Tatiana Nikolaevna Maslennikova, *Candidate of Engineering; graduated from the Faculty of Radioengineering of Ulyanovsk Polytechnic Institute; Head of a research-and-development laboratory at FRPC JSC 'RPA 'Mars'; an author of papers and publications in the field of information support of special-purpose computer-aided systems. e-mail: mars@mv.ru.*

Aleksei Vasilievich Vershennik, *graduated from Stavropolsk Higher Military Engineering School of Communications and Military Academy of the Strategic Missile Forces, Lecturer of the Department 'The Security of Information Telecommunications Systems of Special Purposes' of Marshal Budjonny Military Academy of Signal Corps; an author of articles and inventions in the field of information security. e-mail: alex14121972@mail.ru.*

Abstract

The modern development of the Russian society is characterized with the great increase of the role and actuality of security assurance problems in all spheres of life. One of the major problems is industrial (economic) counterespionage. Such types of espionages are carried in order to sweep market, prevent technological breakthroughs of contestants, wreck negotiations on contracts, resale corporate secrets, etc. One of the most widespread technological tools for information retrieval is a radio eavesdropping device. However, existing control devices do not address capabilities of modern radio eavesdropping devices. The article considers the problem of detection of radio devices installed without authorization in information retrieval systems. Such devices are used for espionage. The method for solving the aforesaid problem is also offered. The method is concerned with the field of radio monitoring of electronic devices in a supervised zone, provides detection of signals in conditions of absence of prior information about their parameters and also allows to define the base frequency of performance.

Key words: information security, eavesdropping devices, radio eavesdropping device.

Введение

В настоящее время проблема обеспечения информационной безопасности (ИБ) резко обострилась с развитием конкуренции в среде свободного предпринимательства. Как показывают исследования, масштабы промышленного шпионажа постоянно растут. По экспертным оценкам, на долю экономического шпионажа приходится 60% потерь предприятия от недобросовестной конкуренции [1].

Существуют разнообразные средства радиоконтроля обследуемых помещений: от простейших индикаторов

электромагнитного поля до сложных автоматизированных комплексов [2]. Для выявления излучающих в эфир радиозакладок необходимо определить возможный диапазон их работы и используемые виды модуляции и закрытия. Как следует из анализа существующих радиозакладных устройств, диапазон их работы достаточно широк и имеет тенденцию к продвижению в более высокие диапазоны. Так в настоящее время специальные технические средства в России чаще всего работают в диапазоне частот 415...420 МГц. Однако в эксплуатации можно встретить большое количество радиозакладных устройств диапазона 20...2000 МГц. Кроме того, существенное изменение претерпели и виды модуляции, используемой в них. В наиболее профессиональных устройствах используют такие сложные сигналы, как шумоподобные или с псевдослучайной перестановкой несущей частоты [3].

Способ обнаружения несанкционированных устройств

Быстрое развитие широкополосных (ШП) и сверхширокополосных (СШП) технологий определили следующие их преимущества:

- способность переносить значительно большее количество информации об объекте исследования;
- низкая средняя излучаемая мощность, которая обычно не превышает единиц-десятков милливатт и определяется дальностью и скоростью передачи информации;
- скрытная работа линии связи благодаря низкой спектральной плотности мощности на единицу полосы частот; электромагнитная совместимость с узкополосными системами, работающими в той же полосе частот;
- высокая скорость передачи информации;
- эффективная борьба с многолучевым распространением за счет временной селекции прямых и переотраженных сигналов или корреляционного приема;
- минимум радиочастотных цепей в приемнике/передатчике (отсутствие высокочастотных генераторов, смесителей, умножителей и пр.);
- простота конструкции [4].

Это существенно усложняет задачу поиска радиозакладных устройств, использующих ШП- и СШП-сигналы. Поэтому появляется необходимость разработки как новых методов и способов их обнаружения, так и создания соответствующих технических средств.

В настоящее время не существует однозначного определения СШП-сигнала.

Так, под СШП-сигналом понимают сигнал, показатель широкополосности которого удовлетворяет условию [5]:

$$\mu_{\min} \le \mu < 2,$$

где показатель широкополосности и задается соотношением:

$$\mu = \frac{\Delta f}{f_0} = 2\frac{f_{\max} - f_{\min}}{f_{\max} + f_{\min}},$$

где $f_0, f_{\min}, f_{\max}$ – средняя, минимальная и максимальная частоты функции спектральной плотности (ФСП) одномерного преобразования Фурье (ОПФ) $S(f)$ данного сигнала $s(t)$; $\Delta f = f_{\max} - f_{\min}$ – ширина полосы частот сигнала.

В то же время, согласно определению, введенному комиссией управления перспективных военных научно-исследовательских и опытно-конструкторских работ Министерства Обороны США, $\mu_{\min} = 0{,}25$, а $f_{\min}$ и $f_{\max}$ следует находить по уровню –20 дБ уменьшения ФСП относительно главного максимума.

Кроме того, определение Федеральной комиссии США, появившееся в 2002 году, предлагает считать $\mu_{\min} = 0{,}20$, а $f_{\min}$ и $f_{\max}$ определять по уровню –10 дБ, причем ширина полосы частот, занимаемая СШП-сигналом, должна удовлетворять условию $\Delta f \ge 500$ МГц.

К сигналам, которые могут использоваться в СШП-радиосистемах, относятся гауссовы импульсы, радиоимпульсы, импульсы Эрмита, хаотические сигналы, линейные частотно-модулированные сигналы, многочастотные сигналы [6].

Малая спектральная плотность и псевдослучайность характеристик СШП-сигнала делают очень сложным его обнаружение.

Авторами статьи предлагается способ, позволяющий обнаружить устройства, использующие СШП-сигналы, в условиях отсутствия априорных сведений об их параметрах, а также определить их основную частоту работы.

Заявленный способ заключается в следующих действиях [7]:

Сигналы от несанкционированно установленных радиоэлектронных устройств (НУРЭУ) систем негласного съема информации должны рассматриваться как случайные процессы в условиях неизвестности их параметров.

Для обнаружения таких сигналов, как правило, используются способы автокорреляционного приема, когда опорное напряжение формируется из принятого сигнала путем различных преобразований, обусловленных видом принимаемого сигнала, в частности, из самого сигнала, в линии задержки.

Для обнаружения СШП-сигнала с априорно неизвестными параметрами предлагается применить сходную идею, только в качестве опорного канала использовать один из каналов фильтрации в выбранной паре [8, 9].

Алгоритм работы предлагаемого способа заключается в следующем (рис. 1).

СШП-сигнал поступает на m параллельно включённых полосовых фильтров (ПФ) (бл. 1, 2, рис. 1), со взаимопримыкающими полосами пропускания одинаковой величины, причем ширина полосы пропускания ПФ гораздо меньше ширины спектра сигнала $\Delta wn\phi << \Delta wc$. В целях сокращения времени обнаружения переключение между выходами ПФ и входами преобразователей частоты (ПЧ) предлагается осуществлять при помощи коммутатора [10], то есть предлагается обрабатывать выделенные сигналы не всеми m ПФ, а случайно выбранными i парами из них.

Количество выбираемых пар каналов фильтрации в каждом отдельном случае может быть разным и определяется заданными временем и вероятностью обнаружения.

Для снижения требований к быстродействию аналогово-цифровых преобразователей (АЦП) и других цифровых элементов сигналы с выхода фильтров перено-

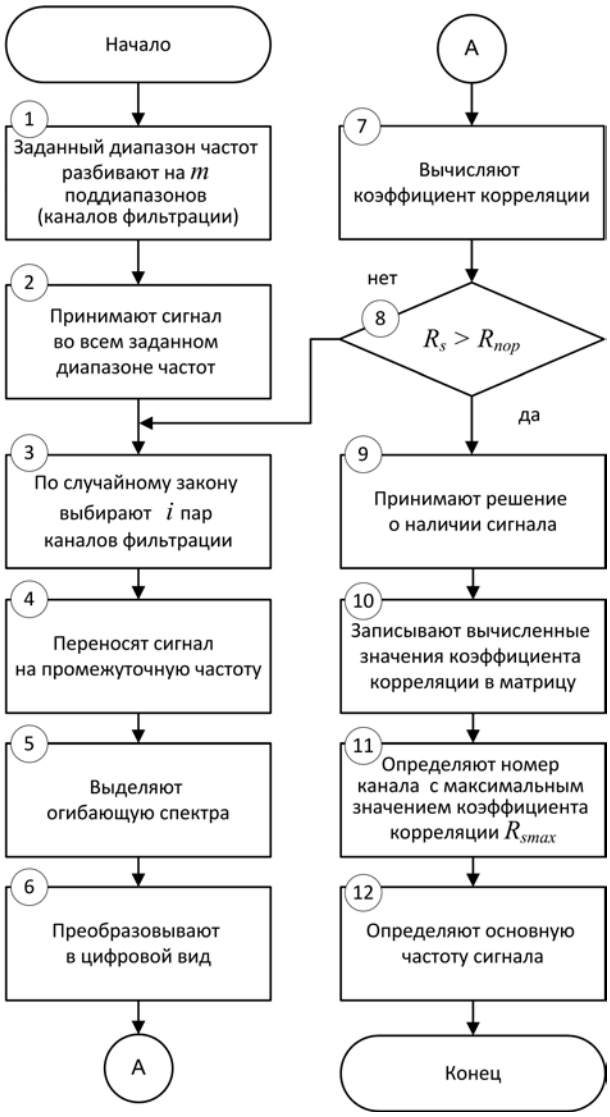

Рис. 1. Обобщенный алгоритм предлагаемого способа обнаружения сигналов

сят на промежуточную частоту. Далее выделяют огибающую спектра. При помощи АЦП сигналы дискретизируют во времени и квантуют по уровням (бл. 6, рис. 1).

Затем производят анализ степени взаимосвязи выбранных каналов фильтрации путем попарного вычисления коэффициента корреляции R_s по формуле 1 (бл. 7, рис. 1) [11]:

$$R_s = \frac{r_{ij}}{\frac{1}{N}\left[\sum_{n=0}^{N-1} x_i^2(n) \sum_{n=0}^{N-1} x_j^2(n)\right]^{1/2}}, \quad (1)$$

где $r_{ij} = \frac{1}{N}\sum_{n=0}^{N-1} x_i(n) x_j(n)$,

$x_i(n)$ – последовательность значений отсчетов сигналов в i –м канале фильтрации,

$x_j(n)$ – последовательность значений отсчетов сигналов в j –м канале фильтрации,

N – количество пар значений.

Вычисленное значение коэффициента корреляции сравнивают с порогом принятия решения (бл. 8, рис. 1), определяемое по критерию Неймана-Пирсона, т. к. при таком выборе порога априорные вероятности отсутствия или наличия сигнала не требуются [8].

При коэффициенте корреляции, превышающем пороговое значение ($R_s > R_{пор}$), принимают решение об обнаружении сигнала (бл. 9, рис. 1), вычисленные значения коэффициента корреляции R_s записывают в соответствующую номерам каналов ячейку предварительно сформированной матрицы (бл. 10, рис.1). Определение максимального значения данного коэффициента корреляции R_{smax} определяет основную частоту $f_{осн}$ сигнала.

Допустим, на m каналов фильтрации подается сигнал, спектр которого представлен на рисунке 2. Фрагмент матрицы с вычисленными значениями коэффициента корреляции по формуле (1) представлен на рисунке 3.

Для упрощения расчетов было взято нормированное значение огибающей спектра сигнала $S(f)$ от 0 до 1.

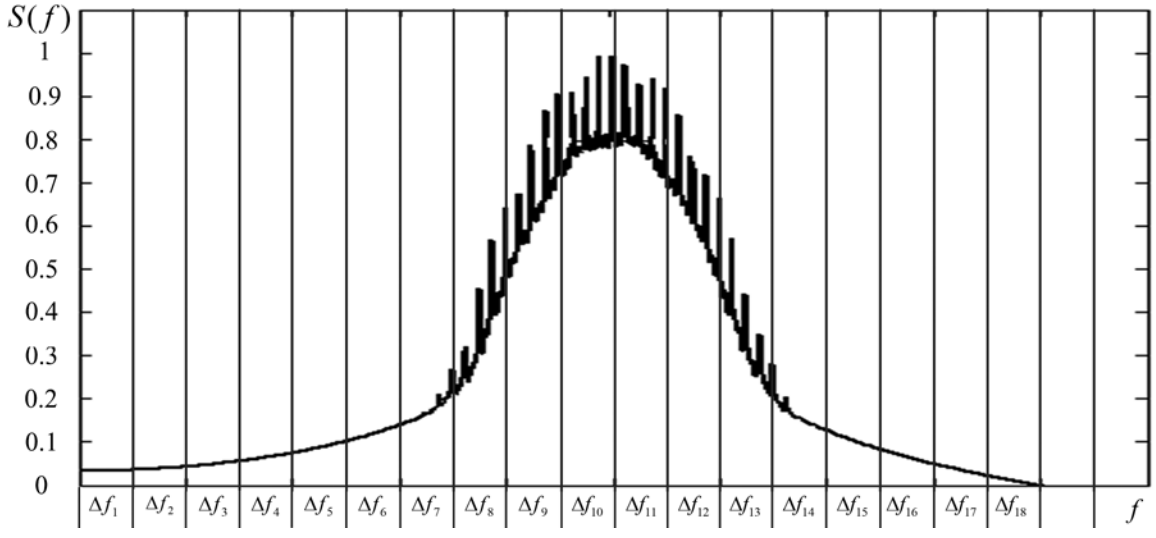

Рис. 2. Спектр короткого радиоимпульса

	1	7	8	9	10	11	12	13	14	…
1	–		…	…	…	…	…	…	…	…
7	…	–	0.968	0.97	0.972	0.982	0.947	0.898	0.939	…
8	…	0.968	–	0.979	0.984	0.986	0.93	0.873	0.922	…
9	…	0.97	0.979	–	0.986	0.994	0.952	0.905	0.929	…
10	…	0.972	0.984	0.986	–	0.994	0.98	0.946	0.976	…
11	…	0.982	0.986	0.994	0.994	–	0.996	0.976	0.993	…
12	…	0.947	0.93	0.952	0.98	0.996	–	0.991	0.9	…
13	…	0.898	0.873	0.905	0.946	0.976	0.991	–	0.982	…
14	…	0.939	0.922	0.929	0.976	0.993	0.9	0.982	–	…
…	…	…	…	…	…	…	…	…	…	…

Рис. 3. Фрагмент матрицы значений коэффициента корреляции

Из рисунке 3 видно, что в столбце (строке) 11 наблюдается наибольшее значение коэффициента корреляции R_s, что соответствует максимальному значению огибающей спектра сигнала $S(f)$ (рис. 2). Таким образом, благодаря выполнению данной последовательности действий становится возможным определение канала фильтрации, в котором будет сосредоточена основная энергетическая мощность сигнала.

Варьируя шириной канала фильтрации, можно повысить точность определения основной частоты работы источника сигнала.

Представленный способ разработан для обнаружения СШП-сигнала в условиях полной неопределенности сведений о параметрах сигнала.

В целях снижения степени неопределенности обнаружение СШП-сигнала может осуществляться либо ШП-сканирующим радиоприемным устройством с независимой параллельной обработкой каналов [12–14], позволяющим сформировать спектрограмму в широкой полосе частот, либо узкополосным сканирующим радиоприемным устройством с высокой скоростью переключения (последовательной обработкой каналов). Для обнаружения сигналов с псевдослучайной перестройкой частоты (ППРЧ) скорость переключения таких радиоприемных устройств должна быть выше, чем скорость переключения поднесущих сигнала. В этом случае ячейки корреляционной матрицы могут заполняться только для каналов, в которых обнаружен сигнал, что позволит сократить время его обработки. Кроме того, в случае предварительного формирования и обработки n-мерной корреляционной матрицы, позволяющей учитывать время и порядок смены частот, может быть не только обнаружен сигнал ППРЧ, но и определен закон его перестройки.

Временные интервалы оценки матрицы зависят от тактико-технических характеристик радиоприемных устройств и могут быть вычислены при помощи аналитического или имитационного моделирования. Применение моделирования позволит также решить ряд задач:

1. Определить оптимальные параметры узкополосных радиоприемных устройств (ширину полосы пропускания, скорость переключения).

2. Определить оптимальное соотношение ширины полосы пропускания и времени корреляционной обработки ШП-радиоприемных устройств.

Заключение

Таким образом, даже при неизвестных параметрах сигнала при реализации данного способа будут обнаружены источники СШП-сигналов и определена их основная частота работы. На предлагаемый способ получен Патент РФ № 2606634 от 10.01.2017 г. [7].

СПИСОК ЛИТЕРАТУРЫ

1. Лобашев А.К. Защита информации от утечек по техническим каналам. – URL: http://mascom-uc.ru/library/354/ (дата обращения: 06.12.2016).

2. Пат. 2568784 Российская Федерация, МПК G01SL 3/02. Способ определения местоположения несанкционированно установленных на объекте электронных устройств / Закалкин П.В., Стародубцев Ю.И., Сухорукова Е.В. и др. ; заявитель СПбГТЭУ ; заявл. 31.03.2014 ; опубл. 27.07.2015, Бюл. № 21.

3. Бузов Г.А., Калинин С.В., Кондратьев А.В. Защита от утечки информации по техническим каналам : учеб. пособие. – М. : Горячая линия-Телеком, 2005.

4. Иммореев И., Судаков А. Сверхширокополосная система связи с высокой скоростью передачи информации. – URL: http://www.sanechka.nightmail.ru/my_articles/2002_3_r.pdf (дата обращения: 19.02.2016).

5. Лазоренко.О, Черногор Л. Сверхширокополосные сигналы и физические процессы. Основные понятия, модели и методы описания. – URL: http://www.twirpx.com/file/472895/?rand=7383906 (дата обращения: 19.02.2016).

6. Судаков А. Сигналы, используемые в СШП радиосистемах. – URL: http://www.sanechka.nightmail.ru/my_articles/2005_1.pdf (дата обращения: 19.02.2016).

7. Пат. 2606634 Российская Федерация, МПК G01S 7/28. Способ обнаружения сверхширокополосного сигнала / Алисевич Е.А., Закалкин П.В., Стародубцев Ю.И., Сухорукова Е.В.; заявитель СПбГТЭУ ; заявл. 12.02.2015 ; опубл. 10.01.2017, Бюл. № 1.

8. Радзиевский В.Г., Трифонов П.А. Обработка сверхширокополосных сигналов и помех. – М. : Радиотехника, 2009. – С. 28–40.

9. Сосулин Ю.Г. Теоретические основы радиолокации и радионавигации. – М. : Радио и связь, 1992, – С. 43–48.

10. Урядников Ю.Ф., Аджемов С.С. Сверхширокополосная связь. Теория и применение – М. : СОЛОН-Пресс, 2009. – С. 176–177.

11. Айфичер Эммануил С., Джервис Барри У. Цифровая обработка сигналов: практический подход. – 2-е изд. : пер. с англ. – М. : Издательский дом «Вильямс», 2004. – 992 с.

12. Повышение эффективности функционирования декаметровых радиолиний / Ю.В. Николашин, П.А. Будко, Е.С. Жолдасов, Г.А. Жуков // Т-comm: Телекоммуникации и транспорт. – 2015. – № 2. – С. 4–10.

13. SDR радиоустройства и когнитивная радиосвязь в декаметровом диапазоне частот / Ю.В. Николашин, П.А. Будко, Е.С. Жолдасов, Г.А. Жуков // Наукоемкие технологии в космических исследованиях земли. – 2015. – № 1. – С. 26–31.

REFERENCES

1. Lobashev A.K. *Zashchita informatsii ot utechek po tekhnicheskim kanalam* [Protection of Information Leakage Through Technical Channels]. Available at: http://mascom-uc.ru/library/354/ (accessed: 06.12.2016).

2. Russian Federation Patent 2568784, Int.Cl.: G01SL 3/02. *Sposob opredeleniia mestopolozheniia nesanktsionirovanno ustanovlennykh na obekte elektronnykh ustroistv* [The Method for Determining the Location of Electronic Devices Installed Without Authorization at the Facility]. Inventor: Zakalkin P.V., Starodubtsev Iu.I., Sukhorukova E.V. et al. Applicant and Proprietor: St. Petersburg State Trade and Economic University. Date of filing: March 31, 2014. Date of publication: July 27, 2015. Bull. No. 21.

3. Buzov G.A., Kalinin S.V., Kondratiev A.V. *Zashchita ot utechki informatsii po tekhnicheskim kanalam: ucheb. posobie* [Protection Against Leakage of Information Through Technical Channels. Manual]. Moscow, Goriachaia liniia-Telekom Publ., 2005.

4. Immoreev I., Sudakov A. *Sverkhshirokopolosnaia sistema sviazi s vysokoi skorostiu peredachi informatsii* [UWB Communication System with a High Data Transfer Rate]. Available at: http://www.sanechka.nightmail.ru/my_articles/2002_3_r.pdf (accessed: 19.02.2016).

5. Lazorenko O., Chernogor L. *Sverkhshirokopolosnye signaly i fizicheskie protsessy. Osnovnye poniatiia, modeli i metody opisaniia* [Ultrawideband Signals and Physical Processes. Concepts, Models and Description Techniques]. Available at: http://www.twirpx.com/file/472895/?rand=7383906 (accessed: 19.02.2016).

6. Sudakov A. *Signaly, ispolzuemye v SShP radiosistemakh* [Signals Used in UWB Radio Systems]. Available at: http://www.sanechka.nightmail.ru/my_articles/2005_1.pdf (accessed: 19.02.2016).

7. Russian Federation Patent 2606634, Int.Cl.: G01S 7/28. *Sposob obnaruzheniia sverkhshirokopolosnogo signala* [Method for Detecting an Ultra-Wideband Signal]. Inventors: Alisevich E.A., Zakalkin P.V., Starodubtsev Iu.I., Sukhorukova E.V. Applicant and Proprietor: St. Petersburg State Trade and Economic University. Date of filing: February 12, 2015. Date of publication: January 10, 2017. Bull. No. 1.

8. Radzievskii V.G., Trifonov P.A. *Obrabotka sverkhshirokopolosnykh signalov i pomekh* [The Processing of Ultra-Wideband Signals and Interference]. Moscow, Radiotekhnika Publ., 2009. pp. 28–40.

9. Sosulin Iu.G. *Teoreticheskie osnovy radiolokatsii i radionavigatsii* [Theoretical Foundations of Radar and Navigation]. Moscow, Radio i sviaz Publ., 1992. 304 p.

10. Uriadnikov Iu.F., Adzhemov S.S. *Sverkhshirokopolosnaia sviaz. Teoriia i primenenie* [UWB Communications. Theory and Application]. Moscow, Solon-Press Publ., 2009. pp. 176–177.

11. Emmanual S. Ifeachor, Barry W. Jervis. *Tsifrovaia obrabotka signalov: prakticheskii podkhod*. 2-e izd., per. s angl. [Digital Signal Processing. 2nd Edition, translated from Engl.]. Moscow, Izdatelskii dom Williams Publ., 2004. 992 p.

12. Nikolashin Iu.V., Budko P.A., Zholdasov E.S., Zhukov G.A. Povyshenie effektivnosti funktsionirovaniia dekametrovykh radiolinii [Increase of Efficiency of Decameter Radio Links Functioning]. T-Comm: *Telekommunikatsii i transport* [Telecommunications and Transport], 2015, no. 2, pp. 4–10.

13. Nikolashin Iu.V., Budko P.A., Zholdasov E.S., Zhukov G.A. SDR radioustroistva i kognitivnaia radiosviaz v dekametrovom diapazone chastot [SDR of a Radio Device and Cognitive Radiocommunication Within the Decameter Frequency Range]. *Naukoemkie tekhnologii v kosmicheskikh issledovaniiakh Zemli* [H&ES Research], 2015, no. 1, pp. 26–31.