УДК 004.056.53 + 621.395:004.056.53 Вестник УрФО № 1(31) / 2019, с. 5–10

**Михайлова У. В., Быкова Т. В., Афанасьева М. В.**

DOI: 10.14529/secur190101

# *СПОСОБЫ ОБНАРУЖЕНИЯ УТЕЧКИ ИНФОРМАЦИИ ПО РАДИОКАНАЛАМ СВЯЗИ*

*В данной статье рассмотрены актуальные проблемы, способы и инструменты для обнаружения утечки информации по радиоканалам связи с использованием специальных технических средств. В частности, рассматривается математическая модель функционирования комплексов радиомониторинга и ее реализация на примере комплекса радиомониторинга «Кассандра». Описан способ вычищения спектра от шума с помощью спектрального вычитания. Продемонстрирована возможность использования адаптивного и динамического порога для обнаружения закладных устройств.*

***Ключевые слова:*** *информация, безопасность, инженерно-техническая защита информации, защита информации, радиомониторинг, закладное устройство, специальное техническое средство.*

**Mikhailova U. V., Bykova T. V., Afanasyeva M. V.**

# *METHODS OF DETECTING INFORMATION LEAKAGE BY RADIO CANNELS*

*This article discusses the current problems, methods and tools for detecting information leaks through radio channels using special technical means. In particular, a mathematical model of the functioning of radio monitoring complexes and its implementation are considered on the example of the Kassandra radio-monitoring complex. A method for cleaning the spectrum from noise using spectral subtraction is described. The possibility of using an adaptive and dynamic threshold for detecting embedded devices has been demonstrated.*

***Keywords:*** *information, security, engineering and technical protection of information, information protection, radio monitoring, mortgage device, special technical tool.*

В настоящее время существует огромное разнообразие современных специальных технических средств (СТС), использующихся для несанкционированного доступа к информации (радиозакладки). Радиозакладки используют сложные типы сигналов, затрудняющие их обнаружение, а передача перехваченной информации производится по легальным ка-

налам связи. Для их обнаружения используются комплексы радиомониторинга. [1]

Комплексы радиомониторинга – это мощные компьютеризированные системы, предназначенные для мониторинга и анализа электромагнитной среды. Такие системы предназначены для постоянного автоматизированного мониторинга в одной или нескольких выбранных областях и используются для обнаружения сигналов, представляющих угрозу.

Большинство современных комплексов радиомониторинга обычно представляет собой множество деталей и подсистем, составляющих интегрированный функциональный блок. Элементы комплекса радиомониторинга состоят из аппаратного и программного обеспечения ПК, а также специфического компьютеризированного оборудования, такого как приемники, антенны, пеленгаторы и анализирующее оборудование. Как правило, в комплексах радиомониторинга они представляют собой конкретные автоматизированные системы с функциями визуализации, мониторинга и анализа. Они содержат распределенные подсистемы для измерения положения электромагнитных излучений. [2]

Следует иметь в виду, что разнообразие современных систем радиомониторинга имеет разные характеристики в зависимости от назначения системы. Например, применение оригинального цифрового приемника значительно повышает скорость работы и эффективность комплекса радиомониторинга. Уменьшенные характеристики массы и размера приводят к увеличению удобства использования комплекса. Чувствительность приемника, высокое разрешение и высокая скорость сканирования гарантируют высокую вероятность обнаружения подозрительных источников электромагнитного излучения в различных диапазонах частот в зависимости от предъявляемых требований. [3]

Основной алгоритм обнаружения радиосигнала в проблемной зоне основан на использовании разделенных антенн, которые производят измерения интенсивности поля сигнала. При осмотре рассматриваемых территорий данный метод позволяет осуществлять точное обнаружение подслушивающих устройств в процессе эксплуатации, в пределах заданной области и в случае, если работают различные типы кодирования данных (различные сложные виды модуляции, шифрования и т.д.).

Еще одним преимуществом комплексов радиомониторинга является возможность классификации обнаруженных сигналов по заданной схеме, что дает возможность выбирать только те сигналы из базы данных, которые были записаны во время предыдущих сеансов мониторинга.

Правильное программное обеспечение радиомониторинговой аппаратуры позволяет выполнять любой тип задач в процессе мониторинга. Все вышеперечисленные характеристики улучшают процесс радиомониторинга, повышают надежность, скорость обработки и стабильность системы, работающей на круглосуточной основе. Для удобства оборудование для радиомониторинга может быть использовано стационарно или в целях мобильного радиомониторинга. [4]

В зависимости от предпочтений или конкретных задач мониторинга, аппаратные средства радиомониторинга могут быть изменены в дальнейшем.

В *M* общем виде математическая модель функционирования комплекса радиомониторинга может быть представлена совокупностью основных систем S, отражающих основные принципы и понятия исследуемой предметной области:

$$M = \langle S_{PC}, S_{АСУЗ}, S_{РМ} \rangle,$$

где $S_{PC}$ – система, характеризующая некоторую структуру регулярной конфигурации радиосистемы $K_{PC}$ и множество радиоустройств $G_{pv}$ как совокупность функциональных элементов радиосистемы;

$S_{АСУЗ}$ – система, характеризующая принципы построения и функционирования автоматизированной системы управления защищенностью (АСУЗ);

$S_{РМ}$ - система, характеризующая процесс радиомониторинга за функционированием радиосистемы.

Конфигурация радиосистемы $K_{PC}$ определяется составом радиоустройств и ее структурой. Состав конфигурации радиосистемы может быть представлен множеством радиоустройств:

$$G_{pv} = \{g_1, g_2, \ldots, g_m\},$$

Структура конфигурации $B_{pc}$ представляет собой множество соединений между всеми радиоустройствами, входящими в состав радиосистемы:

$$B_{pc} = \{b_1, b_2, \ldots, b_n\},$$

Каждое радиоустройство по отношению к АСУЗ является управляемым и вне зависимости от функционального назначения может быть представлено вектором информационных параметров $R_{pv}$, координатами которого являются амплитудно-частотные параметры *r(t)* радиосигналов радиоустройств, индекс класса радиоустройств *a(g)*, а также показатели входных $b_{вх}$, и выходных $b_{вых}$, связей

$$R_{pv}=[r(t), a(g), b_{вх}, b_{вых}]. \text{ [5]}$$

Актуальным вопросом в задачах поискового радиоконтроля считается анализ не только широковещательных пакетов, но и пакетов мобильных устройств, получение из которых в разрешенных рамках максимума полезной информации, позволяет идентифицировать каждое такое устройство и локализовать его местоположение. В настоящее время, как показывает практика, радиомониторинг должен быть круглосуточным, так как это единственный способ проследить за тем, как ведет себя сигнал и как он соотносится с различными важными событиями на охраняемом объекте. Так же это позволяет обнаруживать закономерности во времени появления в эфире, и сравнить текущие спектры сигналов с ранее полученными.

Не зная алгоритма входа радиозакладки в эфир, крайне сложно обнаружить ее сигнал. Поэтому очень важно следить за отображением спектра сигналов в виде «водопада», позволяющего наблюдать за изменениями радиочастотного спектра с привязкой ко времени. Появляется возможность вести базу данных непрерывно и круглосуточно, не теряя ни одного сигнала. Иногда закладное устройство (ЗУ) можно обнаружить с помощью анализа такого отображения спектра. [6]

Так же при поиске СТС необходимо смотреть весь спектр, так как в небольших диапазонах они могут быть не обнаружены. Помимо полезных сигналов в спектре есть и шум. Для обнаружения ЗУ необходимо вычистить спектр от шума с помощью спектрального вычитания (СВ).

Для описания фонового шума часто используется модель аддитивного стационарного гауссовского процесса *η(t)*, некоррелированного с речевым сигналом *x(t)*. Входная запись смеси речевого сигнала и фонового шума будет равна:

$$y(t) = x(t) + \eta(t). \quad (1)$$

При компенсации шума очень важно соблюдать принцип минимального искажения сигнала, при котором все параметры алгоритма фильтрации должны наименьшим образом реагировать на подавление самого шума. Одним из более эффективных алгоритмов подавления фонового шума в речевых сигналах является метод спектрального вычитания (СВ), который основан на том, что амплитудно-частотная характеристика, рассчитываемая посредством процедуры кратковременного Фурье преобразования, несет большую информацию по сравнению с фазочастотной характеристикой. При этом статистические характеристики спектра предполагаются либо известными, либо доступными для оценки по той же кратковременной обработке в реальном времени. Таким образом, для заданной модели (1), в предположении нормального распределения плотности мощности смеси, оценка плотности мощности полезного сигнала (ПМС) $S_x(\omega)$ получается, как результат вычитания из плотности мощности смеси $S_y(\omega)$ плотности мощности фонового шума $S_n(\omega)$ , по следующему правилу:

$$S_x(\omega) = \left[|S_y(\omega)|^\beta - \alpha|S_n(\omega)|^\beta\right]^{1/\beta} \exp j\varphi_y(\omega), \quad (2)$$

где $\alpha$ - масштабный фактор, взвешивающий оценку шума, $\beta$ - фактор который настраивается с целью получения оптимального решения компенсатора шума (часто используется $\beta=2$). Для получения полной оценки ПМС комплексной записи представлена в (2) дополняется со значением фазы $exp^{j\varphi}\, y(\omega)$ входного сигнала, записанного в (1). Наконец, путем обратного преобразования Фурье образуется оценка полезного сигнала $x^t$ во времени. [7]

Поскольку большинство систем обработки речи используют спектральные представления, то метод СВ не нуждается в дополнительном комплексном преобразовании, что является одним из его достоинств. Однако, самое жесткое требование к использованию СВ состоит в наличии представительных выборок для оценки с необходимой точностью статистических параметров шума. Одним из решений этой проблемы является оценка в тех интервалах времени, при которых речь отсутствует и, следовательно, y(t)= η(t). В общем случае, метод СВ может быть осуществлен как по одноканальной схеме, так и по двухканальной схеме. [8]

Одним из основных критериев обнаружения сигнала является линия порога. Рассмо-

трим их практическое применение на примере работы комплекса радиомониторинга «Кассандра». В зависимости от порогового шума программа комплекса радиомониторинга принимает решение — идентифицировать эфирный всплеск как шум или как сигнал. Из сигналов, превысивших порог, формируется список обнаруженных сигналов. Список обнаруженных сигналов используется при поиске новых и контроле известных сигналов, а также для статистической обработки сигнальных измерений.

зволяет значительно ускорить поиск новых сигналов. Созданная таким образом линия до мелочей повторяет имеющийся спектр, и любой новый сигнал в процессе сканирования сразу же будет обнаружен и занесен в список для обработки и анализа. Добавка 3дБ к уровню уменьшает вероятность ложного срабатывания из-за приема слабых сигналов удаленных станций. Для уменьшения влияния случайных всплесков во всей полосе частот применяется программная фильтрация.

При включении динамического порога

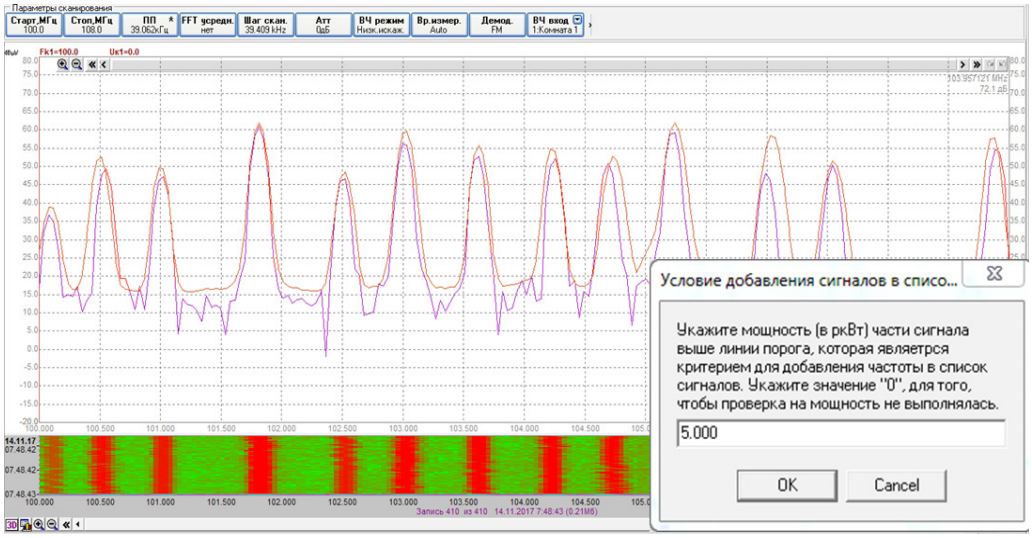


Рис.1. Линия порога в виде усредненных значений

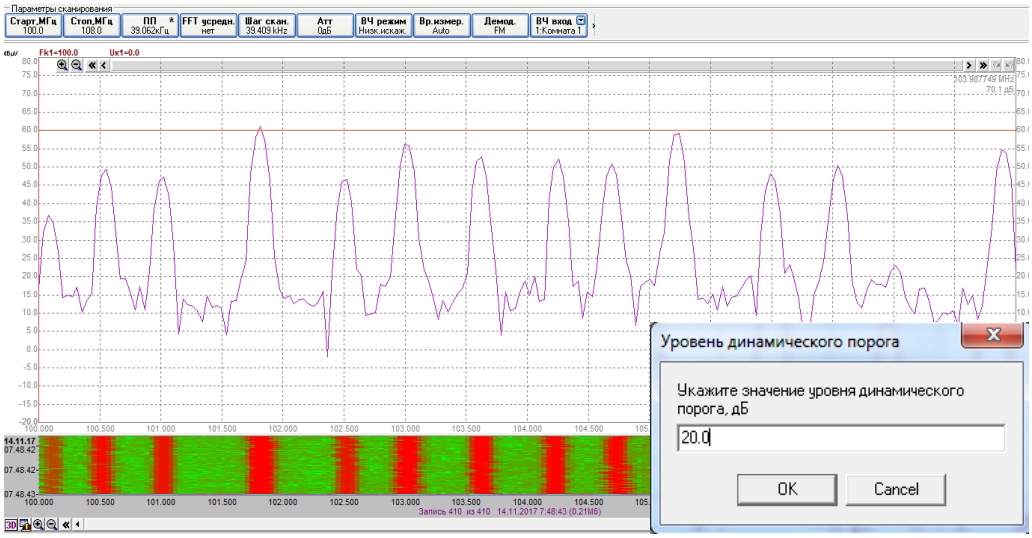


Рис. 2. Динамическая линия порога

В «Кассандре» реализовано два способа формирования линий порога: динамический и адаптивный. В особых случаях предусмотрено произвольное формирование линий в качестве линий порога.

Создание адаптивного порога (рис.1) по-

(рис.2) программа просчитывает средний суммарный уровень сигналов шума в полосе 10 МГц и отбирает сигналы, превышающие этот средний уровень на заданную величину. Отобранные сигналы попадают в список для обработки.

Проблема утечки информации через легальные каналы связи требует к себе все больше пристального и постоянного внимания, поэтому комплексы радиомониторинга непрерывно совершенствуются и дополняются списками стандартов связи, по которым операторы смогут получать исчерпывающую информацию.


**Литература**

1. Михайлова У.В., Быкова Т.В. Защита информации по радиоканалу // Новые информационные технологии в науке: сборник статей по итогам Международной научно-практической конференции — Челябинск, 2017. С. 70-75.

2. Баранкова И.И., Михайлова У.В., Лукьянов Г.И. Поиск радиозакладок с применением комплекса радиомониторинга: методические указания — Магнитогорск, 2016.

3. Баранкова И.И., Михайлова У.В., Лукьянов Г.И. Использование комплекса радиомониторинга для построения графиков текущих значений сканируемых частот: методические указания — Магнитогорск, 2016.

4. Баранкова И.И., Михайлова У.В., Лукьянов Г.И. Применение комплекса радиомониторинга для постобработки спектрограмм: методические указания — Магнитогорск, 2016.

5. Широв С.А., Разработка методического аппарата построения и функционирования адаптивных комплексов радиомониторинга радиоэлектронных средств с применением геоинформационных технологий Широв С.А.: дис. канд. техн. наук. — Владимир, 2007.

6. Михайлова У.В., Тихомиров С.Э., Быкова Т.В. Оценка эффективности защиты радиоканала // Актуальные проблемы современной науки, техники и образования: Тезисы докладов 76-ой международной научно-технической конференции — Магнитогорск, 2018. С. 298.

7. Хорев А.А. Техническая защита информации: учебное пособие для студентов вузов. Технические каналы утечки информации. - М: «НПЦ Аналитика», 2008.

8. Баранкова И.И., Михайлова У.В., Лукьянов Г.И., Калугина О.Б. Обеспечение защиты информации от утечки по техническим каналам: учебное пособие — Магнитогорск, 2018.

**References**

1. Mikhaylova U.V., Bykova T.V. Zashchita informatsii po radiokanalu // Novyye informatsionnyye tekhnologii v nauke: sbornik statey po itogam Mezhdunarodnoy nauchno-prakticheskoy konferentsii — Chelyabinsk, 2017. S. 70-75.

2. Barankova I.I., Mikhaylova U.V., Luk'yanov G.I. Poisk radiozakladok s primeneniyem kompleksa radiomonitoringa: metodicheskiye ukazaniya — Magnitogorsk, 2016.

3. Barankova I.I., Mikhaylova U.V., Luk'yanov G.I. Ispol'zovaniye kompleksa radiomonitoringa dlya postroyeniya grafikov tekushchikh znacheniy skaniruyemykh chastot: metodicheskiye ukazaniya — Magnitogorsk, 2016.

4. Barankova I.I., Mikhaylova U.V., Luk'yanov G.I. Primeneniye kompleksa radiomonitoringa dlya postobrabotki spektrogramm: metodicheskiye ukazaniya — Magnitogorsk, 2016.

5. Shirov S.A., Razrabotka metodicheskogo apparata postroyeniya i funktsionirovaniya adaptivnykh kompleksov radiomonitoringa radioelektronnykh sredstv s primeneniyem geoinformatsionnykh tekhnologiy Shirov S.A.: dis. kand. tekhn. nauk. — Vladimir, 2007.

6. Mikhaylova U.V., Tikhomirov S.E., Bykova T.V. Otsenka effektivnosti zashchity radiokanala // Aktual'nyye problemy sovremennoy nauki, tekhniki i obrazovaniya: Tezisy dokladov 76-oy mezhdunarodnoy nauchno-tekhnicheskoy konferentsii — Magnitogorsk, 2018. S. 298.

7. Khorev A.A. Tekhnicheskaya zashchita informatsii: uchebnoye posobiye dlya studentov vuzov. Tekhnicheskiye kanaly utechki informatsii. - M: «NPTS Analitika», 2008.

8. Barankova I.I., Mikhaylova U.V., Luk'yanov G.I., Kalugina O.B. Obespecheniye zashchity informatsii ot utechki po tekhnicheskim kanalam: uchebnoye posobiye — Magnitogorsk, 2018.



**МИХАЙЛОВА Ульяна Владимировна**, кандидат технических наук, доцент кафедры ИиИБ, Магнитогорский государственный технический университет им. Г. И. Носова. 455000, г. Магнитогорск, пр. Ленина 38. E-mail: ylianapost@gmail.com

**АФАНАСЬЕВА Маргарита Владимировна,** ассистент кафедры ИиИБ Магнитогорский государственный технический университет им. Г.И. Носова 455000, г. Магнитогорск, пр. Ленина 38. E-mail: nansy_stokli@mail.ru

**БЫКОВА Татьяна Викторовна**, студент кафедры ИиИБ Магнитогорский государственный технический университет им. Г.И. Носова 455000, г. Магнитогорск, пр. Ленина 38. E-mail: bykova.tatiana.mg@gmail.com

**MIKHAILOVA Uliana,** Department, Nosov Magnitogorsk State Technical University (NMSTU), Ph.D.,Associate Professor of CSISE Department, Bld. 38, Lenina Ave, Magnitogorsk, Russia, 455000, E-mail: ylianapost@gmail.com

**AFANASYEVA Margarita,** NMSTU, Teaching Assistant of CSISE Department, Bld. 38, Lenina Ave, Magnitogorsk, Russia, 455000, E-mail: nansy_stokli@mail.ru

**BYKOVA Tatyana,** NMSTU, Student of CSISE Department, Bld. 38, Lenina Ave, Magnitogorsk, Russia, 455000, E-mail: bykova.tatiana.mg@gmail.com