

или полностью. Временные отказы микропроцессорных устройств являются следствием проблем электромагнитной помехозащищенности как по линиям питания, так и по средам распространения полезных сигналов (провода, радиоэфир).

Источники электромагнитных помех могут быть как внешними, так и внутренними. Внутренними источниками помех являются влияющие друг на друга электронные компоненты и элементы конструкции электронного устройства. Внешние источники электромагнитных помех являются одним из видов воздействия окружающей среды и могут быть естественными (атмосферный разряды, разряды статического электричества) или искусственными (электромагнитные процессы в технических системах, работа промышленных установок) [1]. Электромагнитные помехи от внешних источников в микропроцессорное устройство могут поступать в виде наводок на линии связи и дорожки печатной платы, выступающие в роли паразитных антенн. Влияние внутренних источников учитывается производителем и считается приемлемым для устройств, прошедших соответствующую сертификацию и технический контроль в условиях производства.

Основное влияние на вероятность временного отказа микропроцессорного устройства оказывает среда. Актуальным является вопрос об оценке возможности возникновения временного отказа микропроцессорного устройства в реальной ситуации. Для оценки вероятности временного отказа предлагается вначале выполнить анализ среды и оценить вероятность появления источника воздействия, а интересующую вероятность временного отказа далее получать, используя статистические данные о влиянии источников воздействий на возникновение временных отказов микропроцессорных устройств.

Список литературы

1. Хабигер Э. Электромагнитная совместимость. Основы ее обеспечения в технике. М.: Энергоатомиздат, 1995. 304 с.

ИССЛЕДОВАНИЕ КОМПЛЕКСНЫХ СПЕКТРОВ СЛОЖНЫХ СИГНАЛОВ В БАЗИСЕ ПРЕОБРАЗОВАНИЯ МЕЛЛИНА

А.М. Макаров, Е.А. Писаренко

Классическая теория обнаружения сигналов на фоне шумов хорошо разработана целым рядом российских и зарубежных ученых [1–10]. В их работах, в основном, рассматриваются сигналы, имеющие базу порядка единиц. Для сигналов с большой базой разработаны теоретические основы обнаружителей сигналов, носящих название сложных. Теория обнаружения сложных сигналов на фоне помех развита в работах В. Б. Пестрякова, Я. Д. Ширмана, Ю. С. Лезина, Д. Б. Вакмана, Г. Ван-Триса.

Все методы обнаружения сигналов на фоне шумов объединяет единая методология обнаружения – нахождение путем синтеза и анализа информативных признаков контраста, отличающих сигналы от шума. В качестве контраста может служить максимум отношения сигнал/шум или различия в автокорреляционных функциях сигналов [2, 4, 5, 6].

Наиболее широкое применение на практике нашли спектральные методы основанные на интегральном преобразовании Фурье (ПФ) анализируемых сигналов. Если структура сложного сигнала неизвестна, то ПФ малоэффективно для измерения таких излучений, но можно использовать другие базисы, например, базис интегрального преобразования Меллина (ПМ) [11, 12].

Целью работы явилось исследование свойств амплитудных спектров широкополосных сигналов (фазоманипулированных) в базисе ПМ для нахождения информативных признаков, позволяющих обнаружить фазоманипулированный сигнала на фоне шума. Доказана теорема об узкополосности амплитудного спектра фазоманипулированных сигналов в базисе ПМ. Предложена структурная схема двухбазисного обнаружения фазоманипулированных сигналов.

Список литературы

1. Обнаружение радиосигналов / П.С. Акимов [и др.]. М.: Радио и связь, 1989. 288 с.

2. Левин Б.Р. Теоретические основы статистической радиотехники. М.: Советское радио, 1974. 752 с.
3. Ван Трис Г. Теория обнаружения, оценок и модуляции. Т. 1. М.: Советское радио, 1972. 744 с.
4. Котельников В.А. Теория потенциальной помехоустойчивости. М.: Советское радио, 1956. 152 с.
5. Макаров А.М., Ермаков А.С. Оптимальный согласованный фильтр для обнаружения сигнала на фоне шума с неизвестной корреляционной функцией // Известия ЮФУ. Технические науки. 2015. № 11 (172). С. 42–54.
6. Мидлтон В. Введение в статистическую теорию связи. Т. 2. М.: Советское радио, 1962. 832 с.
7. Репин В.Г., Тартаковский Г.П. Статистический синтез при априорной неопределенности и адаптации информационных систем. М.: Советское радио, 1977. 432 с.
8. Сосулин Ю.Г. Теория обнаружения и оценивание статистических сигналов. М.: Советское радио, 1978. 447 с.
9. Френкс Л. Теория сигналов. М.: Советское радио, 1974. 344 с.
10. Bertrand J., Bertrand P., Ovarlez J. The Mellin Transform. The Transforms and Applications Handbook. Boca Raton: CRC Press LLC, 2000.
11. Ovarlez J., Bertrand P., Bertrand P. Computation of offline time – frequency distributions using the Fast Mellin transform // Proc IEEE – ICASSP. 1992.
12. Philippe Flajolet, Xavier Gourdon, Philippe Dullas. Mellin transforms and asymptotics: Harmonic sums // Theoretical Computer Science 1995. Vol. 144. P. 3–38.

ВОПРОСЫ ЗАЩИТЫ ИНФОРМАЦИИ НА ОБЪЕКТАХ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

А.В. Макатерчик

В настоящее время общественные и бизнес-процессы в той или иной мере осуществляются с использованием различных объектов специального назначения, выполняющих функции, характерные для какой-то одной или нескольких конкретных задач. Широкое применение в современном оборудовании различных компьютеризированных систем формирует новый, динамически изменяющийся перечень угроз. Так, в телекоммуникационном оборудовании, распространенном на рынке страны 60 % используют в качестве серверной ОС Windows, у 75 % – управляющее и клиентское ПО разработано под Windows, web-интерфейс у 65% оборудования разработан на Java.

Исследования показывают, что в отличие от объектов критически важной инфраструктуры, защита объектов специального назначения находится на значительно более низком уровне:

- на 74 % объектов не применяют эффективных мер для контроля доступа;
- 67 % респондентов не осуществляют должным образом мониторинг информационной безопасности;
- исполнительное руководство 65 % объектов не осознает важности угроз информационной безопасности в полной мере;
- 55 % объектов не проводят на достаточном уровне аудит безопасности;
- 61% объектов применяют недостаточные меры по защите конечных точек.

Анализ состояния указанной проблемы в мире показывает, что уровень ее научно-теоретической, практической реализации не соответствует современному уровню угроз [1, 2].

Список литературы

1. Макаренко Д.И., Хрусталева Е.Ю. Концептуальное моделирование военной безопасности государства. М.: Наука, 2008. 303 с.
2. Kim D., Solomon M.G. Fundamentals of information systems security. Jones & Bartlett Publishers, 2013. 258 p.