отримання кількісних та якісних оцінок ефективності СЗІ дозволяє оперативно вживати ефективні механізми захисту інформації як на етапі експлуатації системи, так і на етапі її проектування, при цьому гарантувати захищеність інформації в рамках визначених обмежень. Перевагою розробленого методу є відсутність обмежень на походження частинних критеріїв та їх кількість. Диференціально-ігровий аспект в оцінюванні ефективності СЗІ проявляється на першому та другому кроках розробленого методу, саме при формалізації задачі оцінювання ефективності та при виборі частинних критеріїв ефективності гравцем захисту. Перспективним напрямом подальших досліджень є проведення процедури оцінювання діючих та перспективних СЗІ за розробленим методом.

Література

1. *Ленков С. В. Методы и средства защиты информации : монография [в 2-х т.] Т. 2. Информационная безопасность / С. В. Ленков, Д. А. Перегудов, В. А. Хорошко. – К. : Арий, 2008. – 344 с.*
2. *Кобозева А. А. Анализ информационной безопасности : монография / А. А. Кобозева, В. О. Хорошко. – К. : ДУІКТ, 2009. – 251 с.*
3. *Шматок С. О. Методика оцінки ефективності пакету заходів для захисту інформації / С. О. Шматок, В. Б. Міщенко, Т. А. Вещицька [та ін.] // Збірник наукових праць ЦНДІ ЗС України. – К. : ЦНДІ ЗС України, 2007. – № 4. – С. 173–188.*
4. *Biskup J. Security in computing systems: challenges, approaches and solutions : monograph / J. Biskup. – Berlin : Springer, 2009. – 694 p.*
5. *Шаньгин В. Ф. Защита компьютерной информации. Эффективные методы и средства / В. Ф. Шаньгин. – М. : ДМК Пресс, 2008. – 544 с.*
6. *Маслова Н. А. Методы оценки эффективности систем защиты информационных систем / Н. А. Маслова // Штучний інтелект. – Донецьк : ІШІ, 2008. – № 4. – С. 253–264.*
7. *Гарасимчук О. І. Оцінка ефективності систем захисту інформації / О. І. Гарасимчук, Ю. М. Костів // Вісник КНУ ім. М. Остроградського. – Кременчук : КНУ ім. М. Остроградського, 2011. – № 1 (66). – С. 16–20.*
8. *Harrison M. Protection in operations systems / M. Harrison, W. Ruzzo, J. Ullman // Communication of the ACM, 1976. – № 19 (8). – P. 461–471.*
9. *Грищук Р. В. Теоретичні основи моделювання процесів нападу на інформацію методами теорій диференціальних ігор та диференціальних перетворень : монографія / Р. В. Грищук. – Житомир : РУТА, 2010. – 280 с.*
10. *Воронин А. Н. Вложенные скалярные свертки векторного критерия / А. Н. Воронин // Проблемы управления и информатики. – 2003. – № 5. – С. 10–21.*
11. *Пухов Г. Е. Дифференциальные преобразования и математическое моделирование физических процессов : монография / Г. Е. Пухов. – К. : Наук. думка, 1986. – 160 с.*
12. *Воронин А. Н. Нелинейная схема компромиссов в многокритериальных задачах / А. Н. Воронин, Ю. К. Зиатдинов // Information Science and Computing. – 2003. – P. 79–85.*

Рецензент: Баранов Г.Л.
Надійшла 10.11.2011

УДК 004.68/.3:68/.32

Шатило Я. Л.
ГУНКТ

Цифровые методы обработки информационных сигналов при радиомониторинге

Введение

Развитие системы передачи, приема и обработки информации (СППОИ) как в нашей стране, так и за рубежом, свидетельствует о том, что основой научно-технического

прогресса в этой области является переход к цифровым методам передачи, приема и обработки информации. В соответствии с этой тенденцией СППОИ легко рассматривать, как проблемно-ориентировочную цифровую систему, ядром которой являются средства вычислительной техники (СВТ), которые реализуются на микропроцессорных наборах, однокристальных и микро ЭВМ. Из всего множества функций, выполняемых СВТ в СППОИ, выделим три основные направления: управление, обработка данных и обработка сигналов.

Так как при радиомониторинге эфира важнейшей функцией является обработка сигналов, при этом операции обработки по смыслу отличаются от операций, необходимых при решении задач управления и обработки данных. Для алгоритмов обработки сигналов типичным является переход от последовательной независимой переменной, которой является время, к некоторому образу (спектральной последовательности), независимой переменной которого является частота [1].

Радиомониторинг эфира заключается в обнаружении ,идентификации опасных сигналов, которые излучаются с объекта. При этом, как правило, используются энергетический и корреляционный методы обработки сигналов.

В основе энергетического метода лежит превышение энергии некоторой случайной реализации над спектральной плотностью шумов энергетического приемника. Энергетический метод реализован в аппаратуре последовательного частотного анализа: анализаторах спектра и приемника, а также программно-аппаратных комплексах радиоконтроля и радиомониторинга.

В настоящее время, идентификация опасных сигналов осуществляется в программно-аппаратных комплексах радиомониторинга различных типов методом корреляции в активном или пассивном режиме.

Основная часть

Рассмотрим модель цифровой системы мониторинга эфира (системы передачи, приема и обработки информации), которая представлена на рис. 1.

При кодировании, передаче и приеме опасного сигнала происходит его искажение за счет добавления к нему шума. Процесс цифровой обработки сигнала (ЦОС) *включает* как получение дисперсных представлений сигнала на основе некоторой модели, так и применение специальных алгоритмов для преобразования полученных дискретных представлений. Цель этого процесса – получение оптимального и наилучшего восстановления опасного сигнала на фоне шума, или в некоторых случаях выявление и определение наличия сигнала. При этом будем иметь в виду, что сигнал на входе СВТ представлен числовыми последовательностями, т.е. дискретен по времени и состоянию.

Преимущества ЦОС известны [1, 2], но самыми главными из них являются следующие:

– принципиальные: многофункциональность, возможность мультиплексирования, реализация практически любых видов преобразования, отсутствие принципиальных ограничений и сложности;

– реализационные: высокая стабильность характеристик, уникальные возможности их перестройки, высокая точность воспроизведения оператора обработки, реализация устройств при помощи БИС и СБИС;

– технико-эксплуатационные: высокая надежность и живучесть, малые вес и габаритные размеры, возможности диагностирования, возможности перепрограммирования, а так же возможности унификации.

Однако следует учитывать и то, что ЦОС присущи определенные недостатки [3]:

– относительно низкая скорость обработки сигнала из-за ограничений быстродействия СВТ;

– шумы округления, нелинейные эффекты переполнения;

– зависимость скорости от точности.

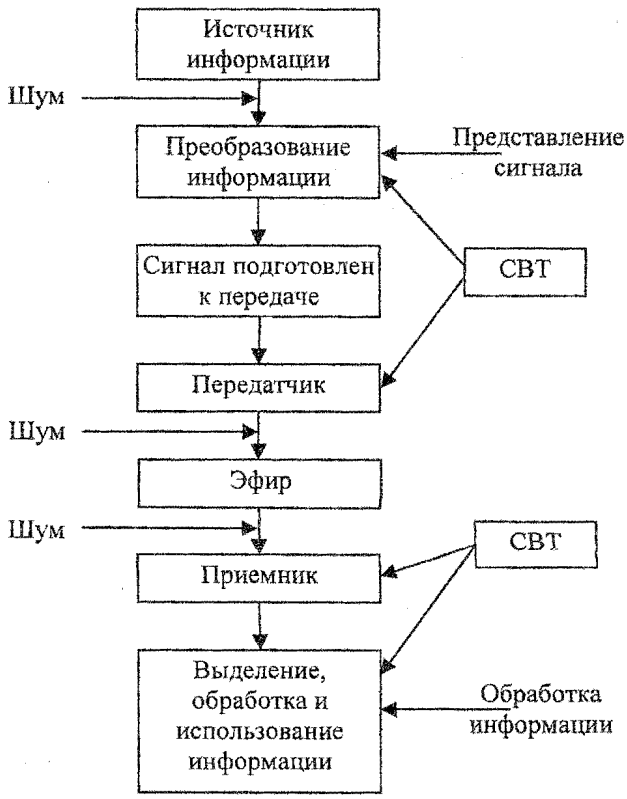

Рис. 1 Модель цифровой системы мониторинга эфира.

К классу задач, которые решаются ЦОС, относятся, прежде всего, фундаментальные задачи спектрального анализа и цифровой фильтрации. Методы ЦОС также применяются и для выполнения многих других задач техники связи и мониторинга эфира, так же, поле оценивания параметров и классификация сигналов, сжатие информации, мультиплексирование и разуплотнение.

Несмотря на растущее многообразие задач ЦОС, алгоритмы их решения могут быть сведены к сочетанию базовых форм, которые постоянно встречаются во многих приложениях и в первую очередь при проведении радиомониторинга.

В первом приближении проведем классификацию ЦОС по времени, которое требуется для их реализации при помощи СВТ [3, 4]. Их можно условно разделить на три группы:

Первая группа – это цифровые фильтры с конечно-импульснойа и бесконечно-импульсной характеристиками. Конечно-импульсная характеристика обычно представляет собой линию задержки с последовательными выводами. При этом входной сигнал X_n проходит через каскад элементов единичной задержки и на каждом этапе умножается на коэффициент фильтра. Затем произведения, полученные на всех элементах, суммируются для получения выходного сигнала. Не редко количество выводов достигает нескольких сотен. Основной операцией здесь является вычисление суммы

произведения. Время, затраченное на реализацию алгоритмов этой группы пропорционально количеству отсчетов сигнала N.

Вторая группа вмещает процедуры вычисления свертки и корреляционных функций, а также дисперсного преобразования Фурье, в частности алгоритмы быстрого преобразования Фурье. Для выполнения N-точечного быстрого преобразования Фурье требуется вычислить $(N/2)\log N$ операцией «бабочка», а каждая «бабочка» содержит четыре вещественных умножения и два комплексных сложения. Для данной группы затраты времени пропорциональны N и $N\log N$.

Третья группа. Для алгоритмов этой группы характерны сложные преобразования спектров. В число базовых процедур помимо наиболее популярных ранее алгоритмов свертки и преобразования Фурье вошли также операции умножения матрицы на матрицу и матрицы на вектор, решение систем линейных уравнений, аппроксимации по методу наименьших квадратов. Время выполнения упомянутых процедур пропорционально N.

В целом алгоритмы ЦОС характеризуются: высокой степенью параллелизма; регулярностью; большим объемом вычислительных операций; обработкой в реальном масштабе времени.

Поэтому попытка реализовывать алгоритмы ЦОС в реальном масштабе времени на основе универсальных микропроцессорных наборах, мини и микро ЭВМ, в которых распараллеливание используется очень мало и, как правило, умножение с накоплением выполняется программой, ограничивает возможности алгоритмов ЦОС [4].

Существенно улучшить характеристики СВТ для ЦОС позволяет их реализация на СВТ. Архитектура таких СВТ, названных сигнальными, позволяет осуществлять обработку сигналов любого вида. В настоящее время наметилось несколько подходов к использованию СВТ такого типа [2].

Первый подход заключается в использовании СВТ с поточной или параллельной организацией. Каждые такие СВТ обладают высокими показателями по быстродействию и являются блоком одно- или многоплатных средств обработки сигналов.

Второй подход предполагает использование специализированных сигнальных СВТ для узкого класса алгоритмов ЦОС. Такие специализированные СВТ характеризуются большой производительностью на конкретном классе задач ЦОС за счет аппаратной реализации, работают они под программным управлением универсальных ЭВМ.

Третий подход предполагает применение однокристальных микро ЭВМ, обеспечивающих программную реализацию комплекса алгоритмов ЦОС. Этот тип СВТ может осуществлять не только большой объем вычислений при обработке сигналов, что характерно и для первых двух подходов, но и на основе анализа информационного потока данных решать задачи управления.

Важной чертой этого направления является, то, что, несмотря на значительное различие в структурных схемах и системах команд микро ЭВМ, для пользователя все они выглядят как последовательный микропроцессор со стандартной архитектурой. Хотя на самом деле для увеличения производительности в архитектуре сигнальных микро ЭВМ реализованы многие виды распараллеливания вычислений, в том числе конвейерная обработка, и т.д..

Наиболее перспективным направлением являются применение векторной и метрической обработки данных. Что касается применения параллельных матричных процессов (сиболических, волновых и т.д.) на СБИС, то здесь необходимо учитывать, что программирование на любой параллельной системе труднее, чем на однопроцессорной, поскольку необходимо учитывать синхронизацию между ветвями программы.

Наибольший эффект от применения транспьютера достигается в тех случаях, когда он применяется для выполнения матичных вычислений: умножение матрицы на матрицу, аппроксимация по методу наименьших квадратов и т.д., т.е для тех операций, которые характерны для задач мониторинга, обработки сложных сигналов и формирования диаграммы направленности антенны.

Таким образом, можно предложить следующую классификацию сигнальных СВТ для ЦОС радиомониторинга:

– стандартные, на основе стандартных наборов БИС;

– специализированные, преимущественно с аппаратным способом реализации алгоритмов ЦОС на микросхемах и возможностью программного управления от универсальных ЭВМ;

– универсальные на основе СБИС, осуществляющие программную реализацию алгоритмов ЦОС;

– векторные, реализующие программную обработку векторов сигналов;

– сетевые вычислительные программные структуры с локальными связями на основе систолических, волновых или транспортных СБИС.

Даная классификация позволяет, хотя и приблизительно, определить возможности СВТ в области радиомониторинга.

Выводы

Предложенная классификация СВТ для ЦОС дает возможность определить предпочтительные области их использования в технике мониторинга. Так как основной объем передачи информации и вытекание опасных сигналов лежит в широком диапазоне частот, то ориентация на использование цифровых систем в аппаратуре передачи информации и системах радиомониторинга в ближайшие годы будет сделана на универсальные СБИС, однокристальные и микро ЭВМ.

Во-первых, универсальные специальные сигнальные микропроцессоры предназначены для решения класса задач, в основе которых лежат, прежде всего, фильтрация, сверка, быстрое преобразование Фурье, полиномиальные и логические преобразования, т.е. базовые операции ЦОС.

Во-вторых, на данном этапе развития технологии, архитектурных принципов построения СВТ и теории ЦОС применение специализированных средств ВТ в СППОИ нашло широкое распространение и весьма эффективно.

При этом практически решаются более сложные задачи ЦОС, что позволяет повысить эффективность радиомониторинга, качества вылавливания опасных сигналов и некоторые проблемы специальной СППОИ.

Литература

1. *Сергиенко А. Б. Цифровая обработка сигналов / Сергиенко А. Б. – СПб.: Изд. Питер, 2002. – 608 с.*

2. *Скорик В. Н. Мультимикропроцессорные системы / Скорик В. Н., Степанов А. Е., Хорошко В. А. – К.: Техніка, 1989. – 192 с.*

3. *Бегма Т. В. Математичні моделі функціонування складних систем / Бегма Т. В., Капустяк М. В., Хорошко В. О. // Вісник СНУ ім. В. Даля, № 7 (161), 2.1, 2011. – с. 252–263.*

4. *Рембовский А. М. Построение многофункциональных систем радиомониторинга на основе семейства малогабаритных цифровых радиоприемных устройств и модулей / Рембовский А. М., Ашихмин А. В., Сергиенко А. Р. // Специальная техника, № 4, 2005. – с. 32–41.*

5. Егоров Ф. И. Вычислительные модули для системы защиты информации / Егорова Ф. И., Орленко В. С., Хорошко В. А. // Зб. наук. праць ВІКНУ ім. Т. Шевченко, Вип. № 11, 2008. – с. 117–124.

Рецензент: Дудивекич В.Б.
Поступила 20.12.2011

УДК 681.14:004.681.3

Хорошко В.О., Чернишев О.М.
ДУІКТ

АЛГОРИТМ ВИЯВЛЕННЯ АТАК ДЛЯ ЗАСОБІВ МОНІТОРИНГУ ІНФОРМАЦІЇ

Вступ

Високий рівень інформації, що характеризує сучасне суспільство, обумовлює залежність його безпеки від захищенності інформаційних технологій які використовуються. Широке застосування систем обробки інформації (СОІ), дозволяє вірішувати задачі автоматизації процесів обробки постійно зростаючих об'ємів інформації, зробило ці процеси особливо вразливими по відношенню до атакуючих впливів, що породило нову проблему- інформаційну безпеку.

Досвід експлуатації СОІ показує, що проблема інформаційної безпеки ще повністю не вирішена, з огляду на те, що засоби і методи захисту не в змозі запобігти атакам, кількість яких постійно зростає. Необхідна розробка нових підходів до створення засобів захисту інформації, здатних забезпечити адекватну протидію загрозам і задовольнити постійно зростаючим вимогам до безпеки СОІ і мереж.

Одним з ключових механізмів захисту інформації в СОІ і мережах є засоби моніторингу безпеки, які реалізують нагляд, аналіз і прогнозування станів безпеки СОІ і мережі. Вони виконують попередній аналіз, оперативний контроль і реалізацію механізмів реакції на вторгнення в СОІ і мережі, що забезпечує виявлення атак і попереджуюче формування комплексу заходів по локалізації можливих несанкціонованих дій в системі.

Ефективність системи моніторингу безпеки СОІ (СМБ СОІ) багато в чому визначається коректністю реалізації. Одним з найважливіших її елементів є алгоритм оцінювання стану об'єкту, що контролюється, для формування реакції засобів моніторингу безпеки на потенційно небезпечні дії в системі [1,2].

Таким чином, всебічний аналіз сучасних СМБ потребує оцінки властивостей алгоритмів формування імовірності вторгнень в СОІ, що використовуються при реалізації засобів моніторингу безпеки [3].

В теперішній час існує декілька основних підходів до реалізації засобів моніторингу безпеки [4], які використовують: статистичний аналіз, експертні системи і штучні нейронні мережі.

В цілому, для всіх відомих підходів до побудови СМБ СОІ характерні наступні недоліки:

- Існуючі СМБ не здатні точно ідентифікувати зловмисника, визначити його кінцеву ціль і мотив вчинків. В загальному випадку вони лише блокують дії зловмисника, що в майбутньому може призвести до повторних атак [5].
- Алгоритми формування імовірності вторгнення в СМБ СОІ і мережі оперують скороченним вектором небезпечних дій, що сформовані лише на основі данних самої системи.