Засновник: Національний авіаційний університет
Зареєстровано Міністерством юстиції України
Свідоцтво про державну реєстрацію друкованого засобу масової інформації
Серія КВ № 17079-5849 ПР від 14 жовтня 2010 р.

Постановою президії ВАК України від 10 листопада 2010 р. № 1-05/7 журнал включено ***до Переліку наукових фахових видань України,***
в яких можуть публікуватися результати дисертаційних робіт на здобуття наукових ступенів доктора та кандидата наук в галузі технічних наук

ЗАХИСТ ІНФОРМАЦІЇ
№ 2(51) 2011 р.

Журнал
Засновано у 1999 році
Виходить чотири рази на рік

Рекомендовано до друку Вченою радою Національного авіаційного університету (протокол № 6 від 21 червня 2011 р.)

Адреса редакційної колегії: 03680, м. Київ, проспект Космонавта Комарова, 1, НАУ, корпус 11, кім. 424, тел. 406-76-42.

© «Захист інформації». Наклад 300 прим. Підписано до друку 30.06.2011 р.

Демчишин

НАУКОВО-ТЕХНІЧНИЙ ЖУРНАЛ «ЗАХИСТ ІНФОРМАЦІЇ» №2, 2011

ЗМІСТ

$$P_{над} = \frac{n^2(n^{-1} + w^{-1})}{(\nu + n)},$$

де n^{-1} - середній час напрацювання програмно-технічних засобів на відмову; w^{-1} - середній час відновлення програмно-технічних засобів; ν^{-1} - середній час виконання відповідного функціонального завданню.

Таким образом, проведено аналіз математичних моделей оцінки надійності та функціонування інформаційних систем у реальному часі, з урахуванням впливу найбільш вірогідних зовнішніх та внутрішніх чинників, що знижують ефективність застосування автоматизованих систем управління цілому.

Запропоновано застосування трьохрівневого алгоритму опису моделі надання інформації в умовах ненадійності програмно-апаратних засобів.

Література

1. Євтушок В.П. Організація інформаційного забезпечення збору, аналізу та оцінки оперативних відомостей / В.П. Євтушок // Шляхи вдосконалення ОРД правоохоронних органів. – Додаток №1 до вісника ЛІВС, 2003. - №3. – С. 17-29.

2. Бойченко О.В. Організаційно-правові та програмно-технічні проблеми захисту інформації в автоматизованих системах ОВС України / О.В. Бойченко, К.С. Герасименко // Збірник наукових праць «Проблеми правознавства та правоохоронної діяльності». – Донецьк: Донецький юридичний інститут Луганського державного університету внутрішніх справ ім. Є.О. Дідоренка, 2010. – №2. – С. 68-73.

3. Кормен Т. Алгоритмы: построение и анализ: монография / Т. Кормен, Ч. Лейзерсон, Р. Ривест // М.: МЦНТО, 1999 – 206 с.

4. Портнягин Л.С. Математическая теория оптимальных процессов: монография / Л.С. Портнягии, В.Г. Болтянский, В.Г. Гамкелидзе, Е.Ф. Мищенко. - М.: Физмаггиз, 1961. – 238 с.

Надійшла: 20.05.2011 р.

Рецензент: д.т.н., проф. Щербак Л.М.

УДК 621.391

Гопиенко А.В., Куц Ю.В., Моиченко Е.В. (НАУ)

МЕТОД СКРЫТОЙ ПЕРЕДАЧИ ДАННЫХ В КОМПЬЮТЕРИЗИРОВАННЫХ ИНФОРМАЦИОННО-ИЗМЕРИТЕЛЬНЫХ СИСТЕМАХ

Вступление. Информация, циркулирующая в каналах передачи данных информационно-измерительных систем (ИИС), во многих случаях носит конфиденциальный характер и требует принятия специальных мер для сохранения ее целостности, защиты от несанкционированного доступа или сокрытии самого факта ее передачи. Одним из эффективных методов решения этой задачи является метод стеганографии [1].Этот метод защиты информации предполагает «встраивание» сообщения в поток цифровых данных, как правило имеющих аналоговую природу – речь, аудиозаписи, изображения, видео и т.п. Известны также предложения по встраиванию информации в исполняемые и текстовые файлы программ [1].

Методы стеганографии могут быть эффективно использованы и для передачи ответственной измерительной информации в каналах ИИС в различных областях – навигации, медицине, авиации и т.п. Их применение предполагает внесение незначительных модификаций, соответствующих информационному сообщению, в несущий сигнал-контейнер. Такие модификации должны быть несущественны для интегрального восприятия сигналов значительной длительности и должны восприниматься как естественные искажения и помехи, сопутствующие процессу передачи.

В ИИС в качестве контейнера могут использоваться сигналы вспомогательных служебных сообщений или информационные сигналы других, менее значимых по важности источников информации. В частности, одним из возможных вариантов реализации метода

стеганографии в каналах передачи данных ИИС может быть использование в качестве контейнера отрезков гармонических сигналов. Скрытность передачи достигается сокращением длительности информационных сигналов и уменьшением индекса модуляции их параметров и характеристик. Локальные модификации параметров сигнала-контейнера, вызванные информационным сообщением, не могут быть определены обычными амплитудными или фазовыми детекторами вследствие их инерционности [2].

Целью статьи является разработка метода скрытой передачи данных в компьютеризованных системах ИИС на основе использования информационных сигналов с локальными незначительными модификациями их фазовых характеристик.

Постановка задачи. Сигналом-контейнером для передачи информационного сообщения служит отрезок гармонического сигнала вида:

$$u_0(t) = U\sin(2\pi ft),\ t \in [0, T_H],\ T_H > 2T, \tag{1}$$

где U, f, T – соответственно амплитуда, частота и период сигнала, t – текущее время, T_H – интервал времени, на котором наблюдается сигнал-контейнер.

На интервале времени равном Tс началом в момент $t_H \in [0, T_H]$, фаза сигнала-контейнера модулируется информационным сообщением

$$\varphi(t) = \begin{cases} m\sin 2\pi ft,\ m < 1,\ t \in [t_H, t_H + T), \\ 0,\ t \in [t_H, t_H + T), \end{cases} \tag{2}$$

где m – индекс угловой модуляции, $m<1$.

Необходимо реализовать процесс демодуляции сигнала вида

$$u(t) = U\cos(2\pi ft + \varphi(t)),\ t \in [0, T_H], \tag{3}$$

найти оценку $\tilde{\varphi}(t)$ информационного сообщения и определить ее погрешность.

Решение. Идея предложенного метода скрытой передачи данных в каналах ИИС изложена в [3], [4]. Она основывается на определении фазовых характеристик сигнала, полученных с помощью преобразования Гильберта (ПГ) [5].Поскольку найти аналитическое решение поставленной задачи затруднительно, предложенное решение обосновывается путем компьютерного моделирования. Методика решения поставленной задачи предполагает выполнение следующих операций:

1. Формирование сигнала-контейнера (3), содержащего информационное сообщение $\varphi(t)$ (2).
2. Определение гильберт-образа сигнала-контейнера:

$$\hat{u}(t) = H[u(t)], \tag{4}$$

где **H** – оператор ПГ.

3. Определение дробной части фазовой характеристики сигнала-контейнера

$$\tilde{\varphi}(t) = arctg\frac{\hat{u}(t)}{u(t)} + \frac{\pi}{2}[2 - sign\,\hat{u}(t)(1 + sign\,u(t))],\ t \in [0, T_H] \tag{5}$$

4. Развертывание фазовой характеристики сигнала $u(t)$ на интервале его наблюдения с целью получения оценки развернутой фазовой характеристики $\tilde{O}(t) = \hat{\phi}(t) + 2\pi(\hat{n}(t))$, где $\tilde{n}(t)$ – ступенчатая функция, определяемая по скачкам $\tilde{\phi}(t)$.

5. Оценка информационного сообщения как разности фазовой характеристики сигнала $\tilde{O}(t)$ и фазы сигнала-контейнера без информационного сообщения:

$$\tilde{\varphi}(t) = \Phi(t) - 2\pi ft\,,\ t \in [0, T_H] \tag{6}$$

6. Определение погрешности оценки $\tilde{\varphi}(t)$:

$$\Delta\varphi(t) = \tilde{\varphi}(t) - \varphi(t). \tag{7}$$

Структура устройства, выполняющего формирование сигнала-контейнера и получение оценки информационного сообщения по предложенной методике, представлена на рис.1.

На рисунке обозначено: **ФС** – формирователь сигнала-контейнера, **ФФС** – формирователь фазы гармонического сигнала, ПГ – преобразователь Гильберта, ВДЧ ФХС – вычислитель дробной части фазовой характеристики сигнала, БР ФХС – блок развертки фазовой характеристики сигнала. Вычитатели Σ, приведенные в структуре, служат для определения оценки информационного сообщения $\tilde{\varphi}(t)$ и ее погрешности $\Delta\varphi(t)$ в соответствии с выражениями (6) и (7).

Рассмотрим моделирование задачи восстановления информационного сообщения вида (1) на следующем примере.

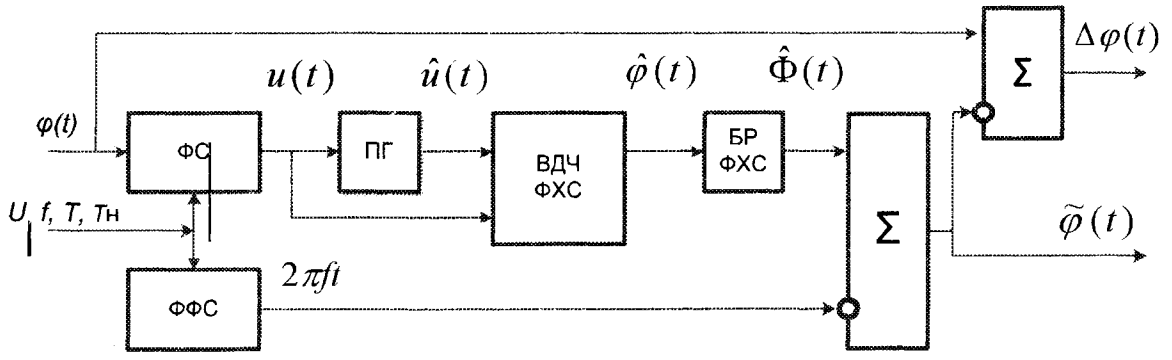

Рис. 1. Структура устройства, реализующего операции формирования сигнала-контейнера и восстановления информационного сообщения

Пример 1. Информационное сообщение (2) и сигнал-контейнер (3) представлены выборочными значениями $\varphi[j]$ и $u[j]$, $j = \overline{1, J}$, $j = [T_H / T_Д]$, полученными в результате равномерной дискретизации непрерывных сигналов (2) и (3) с периодом $T_Д = 10^{-4} c$. Были выбраны следующие параметры сигналов: $T = 10^{-2} c$, $T_H = 9T$, m=0,5рад, J=900, $t_H = 3T$.

Информационное сообщение (2) и сигнал-контейнер (3)изображены соответственно на рис.2 а, б (на рис. 2, б) кривыми 1 и 2 обозначены сигнал-контейнер соответственно до и после его модификации).

На рис. 3 изображены информационное сообщение $\varphi(t)$ (кривая 1) и восстановленное сообщение $\tilde{\varphi}(t)$ (кривая 2).

Из рис. 3 видно, что получение информационного сообщения для рассмотренных условий моделирования сопровождается погрешностью, относительное значение которой достигает 60%. В ходе проведенных исследований было установлено, что погрешность $\Delta\varphi(t)$ зависит как от соотношения частот модулирующего сообщения и несущего сигнала, так и от выбора момента времени t_H.

Возникновение этой погрешности можно пояснить следующими соображениями. Представим сигнал (3) в виде суммы синфазной и квадратурной компонент:

$$u(t) = U_0 \sin(2\pi ft + \varphi(t)) = U_0 \sin\varphi(t)\cos(2\pi ft) + U_0 \cos\varphi(t)\sin(2\pi ft) \qquad (8)$$

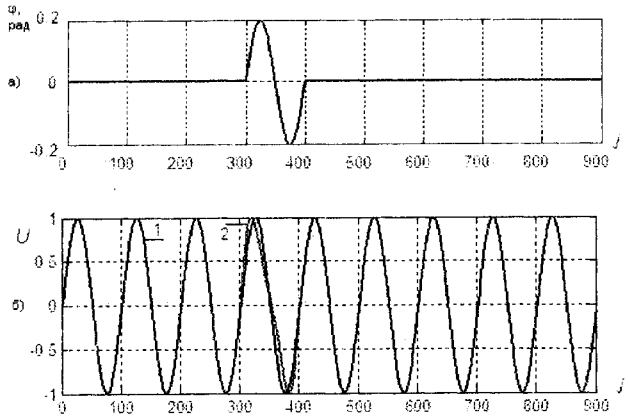

Рис.2. Графики функций $\varphi[j]$ и $u[j]$

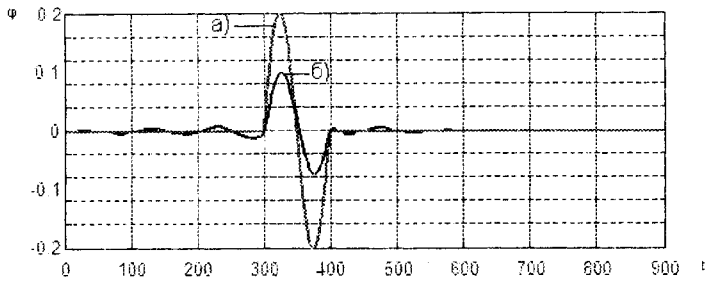

Рис. 3. Графики переданного (кривая 1) и принятого (кривая 2) информационных сообщений

Для входящих в (8) перемножаемых функций $\sin\varphi(t)$ и $\cos 2\pi ft$ не выполняется теорема Бедросиана, которая утверждает, что ПГ произведения двух функций $f(t)$ и $g(t)$ можно представить как:

$$H[f(t)g(t)] = f(t)H[g(t)]$$

только в том случае, если спектры Фурье $F(\omega)$ и $G(\omega)$ этих функций не перекрываются в частотной области, и $F(\omega) < G(\omega)$. Невыполнение условий этой теоремы, по видимому, и приводит к значительным методическим погрешностями определения фазовых и амплитудных характеристик сигнала-контейнера.

Так как амплитудная $u(t)$ и фазовая $\Phi(t)$ характеристики сигнала связаны между собой, то представляется целесообразным попытаться уменьшить погрешность оценки $\tilde{\varphi}(t)$ за счет внесения предискажений в $u(t)$, т.е. определить оценку $\tilde{\varphi}(t)$ не для исходного, а для взвешенного сигнала-контейнера $u(t)y(t)$, где $y(t)$ – некоторая весовая функция, $t \in [0, T_H]$

В качестве такой весовой функции было предложено использовать огибающую сигнала-контейнера вида

$$y(t) = \sqrt{u^2(t) + \tilde{u}^2(t)}\,.$$

В этом случае процесс определения информационного сообщения осуществляется в два этапа. На первом этапе выполняется ПГ и вычисляется оценка амплитудной характеристики

сигнала-контейнера $y(t)$. На втором этапе определяются оценки фазовой характеристики взвешенного сигнала $u(t)y(t)$ и переданного сообщения.

На рис. 4 показана структура, реализующая последовательность операций при восстановлении сообщения с использованием предложенного метода.

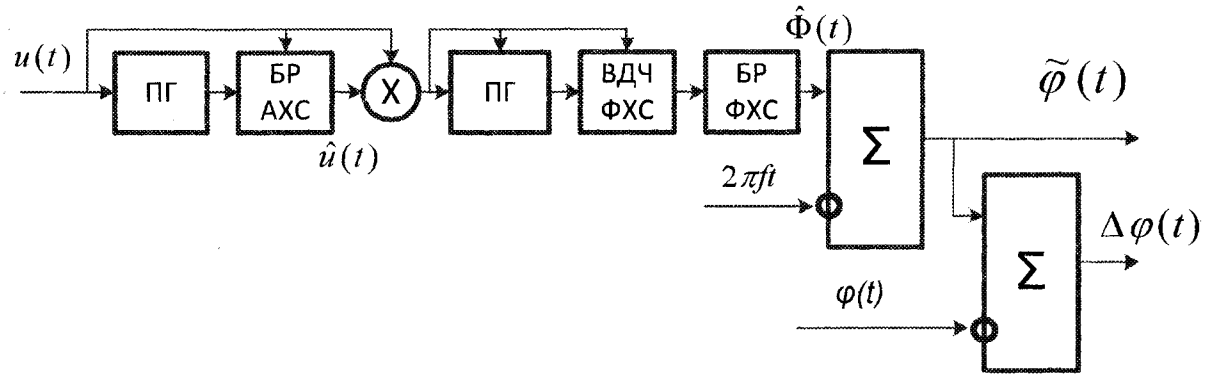

Рис.4. Структура устройства, реализующего операции восстановления информационного сообщения с использованием предварительной коррекции

На рисунке обозначено: ПГ– преобразователь Гильберта, БР АХС – блок развертки амплитудной характеристики сигнала, ВДЧ ФХС – вычислитель дробной части фазовой характеристики сигнала, БР – блок развертки фазовой характеристики сигнала.

Следующий пример подтверждает эффективность такого приема.

Пример 2.Используя исходные данные примера 1, выполним обработку сигнала по схеме, приведенной на рис. 4.

Результат восстановления информационного сообщения представлен на рис. 5.

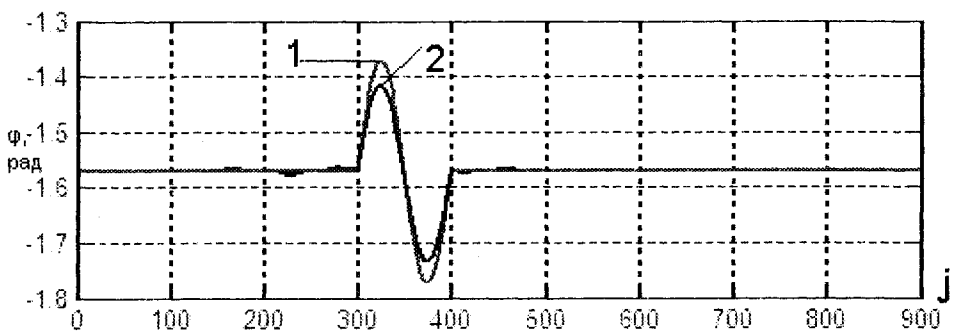

Рис. 5. Графики функций $\varphi[j]$ (кривая 1) и $\tilde{\varphi}[j]$ (кривая 2)

Из анализа кривых на рис. 5 следует, что погрешность восстановления информационного сообщения составляет менее 20%. Проведенные дополнительные исследования показали, что эта погрешность может быть еще уменьшена в несколько раз за счет корректировки весовой функции $y(t)$.

Повышение точности восстановления переданного сообщения расширяет возможности по применению различных способов кодирования передаваемой информации, таких как амплитудная модуляция и манипуляция, относительная и абсолютная фазовая модуляция, частотная модуляция. Дальнейшие исследования данного метода целесообразно провести в направлении повышения его помехоустойчивости.

Выводы. Предложенный метод скрытой передачи информации основан на использовании фазовых характеристик сигналов. Повышение скрытности достигается за счет модуляции параметров сигнала-контейнера на небольших временных интервалах, сравнимых с его периодом. Повышение точности измерения фазовых характеристик достигается путем

дополнительной весовой обработки сигнала-контейнера. В качестве сигнала-контейнера могут быть использованы сигналы вспомогательных служебных сообщений или информационные сигналы второстепенных источников информации. Метод может быть использован для защиты информации в каналах ИИС специального назначения.

Литература

1. Основи комп'ютерної стеганографії/ В.О.Хорошко, О.Д. Азаров, Ю.Є. Шелест та ін. –Вінниця: ВДТУ, 2003. – 143 с.

2. Куц Ю.В., Щербак Л.М. Задачімодуляціїсигналів у системах захистуінформації з використанням дискретного перетворення Гільберта / Защита информации: Сборник научных трудов. – К.: НАУ, 2004. – С.135–144.

3. Патент Украины на корисну модель №51344 спосіб прихованного передавання інформації. Куц Ю.В., Гопієнко А.В., Монченко О.В. – Опубл. 12.07.2010 бюл. №13, 2010.

4. Куц Ю.В., Щербак А.В., Статистична фазометрія. - Тернопіль: видавництво Тернопільського державного технічного університету імені Івана Пулюя, 2009.-383с.

5. Бендат Дж., Пирсол А. Прикладной анализ случайных данных: Пер. с англ. - М.: Мир,1989.-540 с.

Надійшла: 19.05.2011 р.

Рецензент: д.т.н., проф. Щербак Л.М.

УДК 004.056

Бабенко Т.В., Третяк О.М., Мещеряков Л.І., Кручінін О.В. (НГУ)

ОБРОБКА ПЕРСОНАЛЬНИХ ДАНИХ В УМОВАХ ДІЯЛЬНОСТІ ВИЩИХ НАВЧАЛЬНИХ ЗАКЛАДІВ

У статті розглянуто процес обробки персональних даних у вищих навчальних закладах, виконано аналіз законодавчих актів у сфері захисту інформації та висунуто ряд пропозицій щодо створення необхідних умов для реалізації вимог, зазначених у Законі України «Про захист персональних даних».

Прагнення інтеграції України до Євросоюзу та загальна інформатизація усіх сфер життя нашого суспільства сприяють реформуванню законодавчої бази України та її гармонізації з міжнародними стандартами. Останнім часом в Україні ратифіковано конвенцію Ради Європи «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних» [1], прийнято створений на її основі Закон України «Про захист персональних даних» [2], внесено зміни та доповнення до Закону «Про інформацію» [3]. Під впливом нововведень змінюються і технології обробки інформації в освітній сфері, так, зокрема, в 2011 році Міністерство освіти і науки, молоді та спорту України запровадило експеримент «Електронний вступ» [4]. Його сутність полягає в тому, що абітурієнт зможе заповнювати свої вихідні (анкетні) дані в он-лайн режимі на інтернет-порталі «Єдине освітнє інформаційне вікно України», а вищі навчальні заклади – отримувати електронні заяви та контактувати з вступником засобами електронного зв'язку. З точки зору інформаційної безпеки перехід до електронної реєстрації ставить перед учасниками цього процесу багато питань як організаційного так і програмно-технічного характеру. Зокрема, це стосується обов'язкового впровадження і сертифікації комплексної системи захисту інформації, організації захищеного зберігання, обробки та знищення персональних даних абітурієнтів.

Метою даної статті є аналіз стану та заходів щодо забезпечення захищеності інформації в інформаційно-комунікаційних системах державних вищих навчальних закладів за умови набуття чинності закону «Про захист персональних даних».

Інформаційно-комунікаційна система вищого навчального закладу, як правило, представляє собою складну сукупність підсистем, призначених для автоматизації діяльності окремих адміністративних структур, бази даних яких можуть містити персональні дані.

Певні непорозуміння виникають вже на етапі визначення поняття «персональні дані». Згідно Закону України «Про захист персональних даних» це «відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована»