

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ,
МОЛОДЕЖИ И СПОРТА УКРАИНЫ
ХАРЬКОВСКИЙ НАЦИОНАЛЬНЫЙ
УНИВЕРСИТЕТ РАДИОЭЛЕКТРОНИКИ

РАДИОТЕХНИКА

**Всеукраинский межведомственный
научно-технический сборник**

ТЕМАТИЧЕСКИЙ ВЫПУСК

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Основан в 1965 г.

ВЫПУСК 166

ХНУРЕ Radyotekhnika



819242

Харків
Харківський національний
університет радіоелектроніки
2011

Сборник включен в список специальных изданий ВАК Украины по физико-математическим и техническим наукам.

Регистрационное свидетельство КВ № 12098-969 ПР от 14. 12. 2006.

Ответственность за содержание статей несут авторы.

Редакционная коллегия:

главный редактор *В.М. Шокало*, д-р техн. наук, проф.; зам. главного редактора *А.И. Лучанинов*, д-р физ.-мат. наук, проф.; ответственный секретарь *А.Г. Пащенко*, канд. физ.-мат. наук, доц.; *Ю.Б. Гимтлевич*, д-р техн. наук, проф.; *И.Д. Горбенко*, д-р техн. наук, проф.; *Ю.Е. Гордиенко*, д-р физ.-мат. наук, проф.; *А.И. Довбня*, д-р физ.-мат. наук, проф.; *А.Г. Карабанов*, д-р философии (США); *В.М. Картшиов*, д-р техн. наук, проф.; *В.В. Конин*, д-р техн. наук, проф.; *А. А. Коноваленко*, академик НАН Украины; *Н.И. Кравченко*, д-р техн. наук, проф.; *В.М. Кузмичев*, д-р физ.-мат. наук, проф.; *Л.Н. Литвиненко*, академик НАН Украины; *И.М. Неклюдов*, академик НАН Украины; *В.В. Поповский*, д-р техн. наук, проф.; *Э.Д. Прохоров*, д-р физ.-мат., проф.; *С.-Э. Сандстрём*, проф. (Швеция); *А.И. Стрелков*, д-р техн. наук, проф.; *К.С. Сундучков*, д-р техн. наук, проф.; *П.Л. Токарский*, д-р физ.-мат. наук, проф.; *А.И. Фисун*, д-р физ.-мат. наук, проф.; *Я.С. Шифрин*, д-р техн. наук, проф.

Ответственный за выпуск д-р техн. наук, проф. И. Д. Горбенко

Технический секретарь Е.С. Полякова

Рекомендовано Ученым советом Харьковского национального университета радиоэлектроники, протокол №2 от 27. 05. 2011.

Адрес редакционной коллегии: Харьковский национальный университет радиоэлектроники (ХНУРЭ), просп. Ленина, 14, Харьков, 61166, тел. (0572) 7021-397.

Сборник «Радиотехника» включен в Каталог подписных изданий Украины, подписной индекс 08391

СОДЕРЖАНИЕ

СИНТЕЗ И АНАЛИЗ КРИПТОГРАФИЧЕСКИХ СИСТЕМ

<i>И.Д. Горбенко, И.В. Лисицкая</i> Стандартизация алгоритмов шифрования. Требования к проекту национального стандарта блочного симметричного шифрования на современном этапе развития криптографии	5
<i>Р.В. Олейников, А.В. Казимиров</i> Влияние свойств булевых функций S-блока на стойкость современных симметричных блочных шифров	11
<i>И.В. Лисицкая, В.В. Ковтун</i> Об участии S-блоков в формировании максимальных значений линейных вероятностей блочных симметричных шифров	17
<i>Г.З. Халимов</i> Каскадное универсальное хеширование по рациональным функциям алгебраических кривых	26
<i>К.А. Погребняк, Ю.М. Ленишина</i> Схема хамелеон-подписи на основе ДСТУ 4145-2002	32
<i>О.А. Мельникова, О.Н. Товма</i> Анализ возможностей уменьшения вычислительной сложности ЭЦП ДСТУ 4145-2002 при использовании нормального базиса	40
<i>А.Г. Корченко, Е.В. Котух, А.А. Бойко</i> Многокаскадное универсальное хеширование по рациональным функциям максимальной кривой третьего рода	44
<i>И.В. Лисицкая, А.А. Настенко</i> Большие шифры – случайные подстановки	50
<i>І.Д. Горбенко, П.О. Кравченко, Л.В. Макутоніна</i> Обґрунтування та вибір критеріїв та показників оцінки комбінованих ІВК	56
<i>В.І. Бондаренко, Ю.І. Горбенко, Д.Е. Хряпін</i> Аналіз вимог до генераторів випадкових і псевдовипадкових послідовностей встановлених в стандартах AIS 20 та AIS 31	64
<i>О.А. Шевчук</i> Актуальність атаки на зв'язаних ключах для апаратних реалізацій засобів КЗІ	70

МЕТОДЫ, МЕХАНИЗМЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

<i>М.Ф. Бондаренко, Н.С. Лесна, О.О. Ткач, В.М. Караваев, О.І. Шумов</i> Положення про обробку та захист персональних даних ХНУРЕ	76
<i>П.О. Філоненко, О.А. Вінокурова</i> Аналіз біометричних систем автентифікації та ідентифікації з використанням гібридних інтелектуальних методів для захисту від несанкціонованого доступу	84
<i>Д.А. Семченко, А. А. Замула</i> Методы анализа процессов контроля качества программного обеспечения используемые при проектировании и разработке систем обработки криптографической информации	94
<i>С.Г. Семенов</i> Структурно-информационные портреты информационной системы в условиях неопределенности на примере Dos-атаки	99
<i>Е.Е. Малафеев, Е.Е. Малафеев</i> Оценка эффективности динамических алгоритмических преобразователей	107
<i>В.І. Заболотний, А.А. Абузова, Б.В. Волобуєв</i> Обґрунтування плану захисту об'єктів про об'єкти, процеси та явища	112
<i>С. А. Мороз, В.А. Краснобаев, А.А. Замула</i> Методы контроля и диагностики данных в классе вычетов	117

СИНТЕЗ И АНАЛИЗ СИГНАЛОВ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

<i>И.Д. Горбенко, А.А. Замула, Р. И. Киянчук</i> Методы построения и исследования свойств производных нелинейных рекуррентных последовательностей	125
<i>А.А. Кузнецов, А.А. Смирнов</i> Встраивание данных в контейнеры-изображения с использованием сложных дискретных сигналов	134
<i>А.А. Кузнецов, А.А. Смирнов, В.Н. Сай</i> Дискретные сигналы с многоуровневой функцией корреляции	142
<i>П.А. Филоненко</i> Анализ информационных признаков отпечатков пальцев и сканирующих устройств	153

<i>В.В. Ратин</i> Исследование синхронизированного автогенератора с нелинейной обратной связью	159
<i>А.И. Литвин-Попович</i> Обработка радиолокационных сигналов в параллельных вычислительных системах	165
<i>Р.М. Дідковський, С.С. Гузнін</i> Методи багатопозиційної модуляції шумових сигналів	173
<i>В.М. Кичак, Є.С. Ленков, В.М. Лоза</i> Вибір технологічно обґрунтованого методу оцінки складу групової зосередженої цілі	180
<i>Е.В. Харченко</i> Метод расчета областей наиболее вероятного появления метеорных следов, имеющих точку зеркального отражения	186
<i>О.В. Зубков, Г.И. Сидоров</i> Адаптация рабочей частоты содара в условиях изменяющейся помеховой обстановки	193
<i>А. В. Артюх, В. А. Дорошенко</i> Возбуждение конуса с продольной щелью во временной области магнитным радиальным диполем	200
<i>Н.И. Слипченко, В.А. Письменецкий, Н.В. Герасименко</i> Исследование и моделирование электронных свойств аморфных пленок α -Si:H	205
<i>В.А. Петров, А.Н. Ключева, О.Л. Павлова</i> Оценка текущих условий загоризонтного распространения УКВ по заданному пространственному распределению коэффициента преломления воздуха	214
<i>В.А. Дорошенко, Ю.Д. Шимук</i> Моделирования рассеивания поля электрического радиального диполя одиночным полупрозрачным конусом с продольными щелями	223
<i>Н. И. Слипченко, Лю Чан, А.Ю. Панченко</i> О постановке дифракционной задачи для бистатической зоны систем радиоакустического зондирования атмосферы	228
<i>Б.В. Жуков, К.В. Нетребенко, А.В. Одновол</i> Контроль уровня высокотемпературных объектов методом акустической локации	233
<i>И.В. Шинкаренко, А.А. Дудка, А.И. Цопа</i> Анализ структурной скрытности многоуровневых линейных сигналов цифровых систем передачи информации на основе широкополосных xDSL технологий	239
<i>И. Б. Широков, И. В. Сердюк</i> Исследование влияния шумов в радиоканале на работу системы синхронизации опорных генераторов	245
<i>О.И. Харченко</i> Исследование спектра выходного сигнала нелинейной системы в режиме стохастического резонанса	254
<i>В.Г. Копух, М.А. Мирошник, С.Н. Селевко</i> Методы повышения отказоустойчивости телекоммуникационных систем	259
РЕФЕРАТЫ	269

CONTENTS

SYNTHESIS AND ANALYSIS OF CRYPTOGRAPHIC SYSTEMS

<i>I.D. Gorbenko, I.V. Lisitska</i> Standardization of cryptographic algorithms. Requirements for the project of a national standard block of a symmetric encryption at the present stage of development of cryptography	5
<i>R.V. Oliynykov, O.V. Kazymyrov</i> Impact of S-box Boolean function properties on the modern symmetric block ciphers strength	11
<i>I.V. Lisitskaya, V.V. Kovtun</i> About participation of S-blocks in formation of the maximum values of linear probabilities of block symmetric code numbers	17
<i>G.Z. Khalimov</i> Cascade universal hashing of rational functions algebraic curves	26
<i>K.A. Pogrebnyyak, I.M. Lyenshyna</i> Chameleon-signature scheme based on DSTU 4145-2002 standard	32
<i>O.A. Melnikova, O.N. Tovma</i> Analysis of the possibilities to decrease the computational complexity of electronic signature DSTU 4145-2002 when using a normal basis	40
<i>A.G. Korchenko, E.V. Kotukh, A.A. Boiko</i> Multistage universal hashing of rational functions maximal curve of the third genus	44
<i>I.V. Lisitskaya, A.A. Nastencko</i> Great ciphers – casual substitution	50
<i>I.D. Gorbenko, P.O. Kravchenko, L.V. Makutonina</i> Justification and selection of criteria and indicators for estimating the combined PKI	56
<i>V.I. Bondarenko, U.I. Gorbenko, D.E. Khriapin</i> Analysis of requirements on random and pseudorandom number generators in the AIS 20 and AIS 31 standards	64
<i>A.A. Shevchuk</i> Urgency of attack on the related keys for hardware realizations of DSS	70

METHODS, MECHANISMS AND MEANS OF INFORMATION PROTECTION

<i>M.F. Bondarenko, N.S. Lesna, O.O. Tkach, V.M. Karavaev, O.I. Shumov</i> Regulations of the KNURE personal data processing and protection	76
<i>P.A. Filonenko, E.A. Vynokurova</i> Analysis of biometric systems for authentication and identification using hybrid intellectual methods to protect unauthorized access	84
<i>D.A. Semchenko, A. A. Zamula</i> Methods for analysis of quality control processes used in software design and development of systems for handling cryptographic information	94
<i>S. Semenov</i> Structurally-informative portraits of the informative system in the conditions of vagueness on the example of Dos-attack	99
<i>Ye.Ye. Malafeev, Ye.Ye. Malafeev</i> Estimation of dynamic algorithmic converters efficiency	107
<i>V.I. Zabolotnyi, A.A. Abuzova, B.V. Volobuiev</i> Justification of the plan of objects protection about objects, processes and phenomena	112
<i>S. Moroz, V. Krasnobaev, A. Zamula</i> Methods of data monitoring and diagnosis in residue classes	117

SYNTHESIS AND ANALYSIS OF SEQUENCES SIGNALS

<i>I.D. Gorbenko Ph.D., A.A. Zamula Cand., R.I. Kiyanchuk</i> Methods for constructing and studying properties of the derivatives of nonlinear recurrence sequences	125
<i>A.A. Kuznetsov, A.A. Smirnov</i> Building of information in containers-images with the use of complex discrete signals	134
<i>A.A. Kuznetsov, A.A. Smirnov, V.N. Say</i> Discrete signals with a multilevel correlation function	142
<i>P.A. Filonenko</i> Analysis of information features and fingerprint scanners	153

<i>V. Rapin</i> Investigation of the synchronized oscillator with nonlinear feedback	151
<i>A. I. Litvin-Popovich</i> Radar signal processing in parallel computing systems	165
<i>R. M. Didkowsky, S. S. Huznin</i> Multiple-bits noise signals modulation scheme	173
<i>V. M. Kichak, E. S. Lenkov, V. M. Loza</i> Technologically justified method for estimation of the multiple grouped target content	180
<i>O. V. Kharchenko</i> Methods for calculation of areas of the most likely emergence of the meteor trails having the mirror reflection point	186
<i>O. V. Zubkov, G. I. Sidorov</i> Sodar operation frequency adaptation under the conditions of changing noise situations	193
<i>A. V. Atryukh, V. A. Doroshenko</i> Excitation of the cone with a longitudinal slot by a magnetic radial dipole in the time domain	200
<i>N. I. Slipchenko, V. A. Pismenetsky, N. V. Guerasimenko</i> Investigation and simulation of electronic properties of α -Si:H amorphous films	205
<i>V. A. Petrov, A. N. Klyueva, O. L. Pavlova</i> Estimation of current conditions transhorizon UHF propagation for a given spatial distribution of the refractive index of air	214
<i>V. A. Doroshenko, Y. D. Shimuk</i> Mathematical modeling of a resistive cone with a longitudinal slot excitation by a monochromatic source	223
<i>N. I. Slipchenko, Liu Chang, A. Yu. Panchenko</i> About statement of the diffraction problem for bistatic zone of radio acoustic atmospheric sounding	228
<i>B. V. Zhukov, K. V. Netrebenko, A. V. Odnovol</i> Control of level of high temperature objects with the acoustic location method	233
<i>I. Shynkarenko, O. Dudka, O. Tsopa</i> Structural analysis of the multi-level linear signals secrecy of digital information transmission systems based on broadband xDSL technologies	239
<i>I. B. Shirokov, I. V. Serdyuk</i> The research of noises influence in a radio channel to the reference oscillators' synchronization system operation	245
<i>O. I. Kharchenko</i> Investigation of output signal spectrum of nonlinear system in stochastic resonance regime	254
<i>V. G. Kotuh, M. A. Miroshnik, S. N. Selevko</i> Methods to improve the resiliency of telecommunications systems	259
ABSTRACTS	269

УДК 621.391:519.2:519.7

И.Д. ГОРБЕНКО, д-р техн. наук, И.В. ЛИСИЦКАЯ, канд. техн. наук

СТАНДАРТИЗАЦИЯ АЛГОРИТМОВ ШИФРОВАНИЯ. ТРЕБОВАНИЯ К ПРОЕКТУ НАЦИОНАЛЬНОГО СТАНДАРТА БЛОЧНОГО СИММЕТРИЧНОГО ШИФРОВАНИЯ НА СОВРЕМЕННОМ ЭТАПЕ РАЗВИТИЯ КРИПТОГРАФИИ

О стандартах шифрования

Значительная роль алгоритмов шифрования при защите электронной информации в массовом масштабе обусловила необходимость принятия стандартов шифрования, из которых наиболее известным и широко используемым является американский федеральный стандарт DES, принятый в середине 1970-х годов и послуживший аналогом для российского стандарта ГОСТ 28147-89. В настоящее время эти стандарты уже устарели и не соответствуют, как минимум, современным требованиям по скорости шифрования данных [1]. Так, в DES используется 56-битный секретный ключ, который в настоящее время не может обеспечить достаточной стойкости к атаке, основанной на переборе всех возможных значений ключа. Кроме того, для этого стандарта были найдены криптоаналитические атаки, сложность которых оказалась меньше прямого перебора ключей. В [2] отмечается ряд недостатков российского стандарта ГОСТ 28147-89. Так, одним из его недостатков считается сложность его аппаратной реализации. Еще одним существенным недостатком шифра ГОСТ 28147-89 является то, что в нем используются секретные долговременные ключевые данные, которые поставляются "в установленном порядке". В то же время по общепринятым требованиям стойкость алгоритма должна основываться только на секретности легко сменяемого элемента – ключа. К тому же оба шифра обладают низкой стойкостью к атакам на основе случайных аппаратных ошибок. Такая атака является опасной для шифров, применяемых в интеллектуальных электронных карточках. При осуществлении такой атаки предполагается, что нарушитель имеет возможность оказать на шифратор при выполнении процедуры шифрования внешнее физическое воздействие и вызвать одиночные случайные ошибки в регистрах, содержащих данные.

Надо отдать должное тому факту, отмечается в [2], что первый в мире официальный стандарт шифрования был принят в США. Он сыграл важную роль в закреплении мирового лидерства американских производителей криптографических средств защиты информации. Влияние американского стандарта DES на тенденции развития открытой криптографии во всем мире оказалось настолько большим, что в течение первых двадцати лет его применения разработчики блочных алгоритмов шифрования оказались "загипнотизированными" подходами, использованными при разработке DES. Общая схема построения криптосистемы DES стала образцом для подражания. Последнее привело к определенному сдерживанию новых подходов к построению блочных криптосистем, которое отчетливо проявилось в начале 1990-х годов, когда возникла потребность в скоростных методах шифрования, ориентированных на программную реализацию.

В 1998 – 2000 гг., когда стало окончательно ясно, что алгоритм DES уже исчерпал свои возможности, США, сохраняя первенство в этом направлении, провели международный открытый конкурс на стандарт 21-го столетия (продвинутый) – Advanced Encryption Standard (AES). Конкурс успешно завершился. Победителем стал шифр Rijndael бельгийских разработчиков. Сильную конкуренцию победителю составили шифры RC-6 и Tofish. Вслед за этим конкурсом был объявлен аналогичный европейский конкурс (NESSI). Еще раз важно отметить, что в процессе открытого обсуждения проектов предлагаемых шифров и примитивов, их всестороннего анализа и сравнения был осуществлен существенный прорыв не только в

теории криптографии, но и в развитии новых подходов к разработке и построению шифров, а также в развитии практических методов криптоанализа.

Конечно, через распространение своих алгоритмов шифрования и средствЗИ ведущие страны закрепляют позиции на рынке продуктов и услуг в области информационной безопасности, а также усиливают влияние и приобретают в определенной степени возможность контроля защищенности информационного ресурса других стран.

Поэтому архиважной задачей для Украины является быстрое освоение современных технологий криптографической защиты информации, выход на уровень создания и принятия собственных или гармонизированных международных стандартов, что, несомненно, способствовало бы укреплению ее суверенитета и независимости. Проблема разработки скоростных шифров, соответствующих современным мировым требованиям и тенденциям, уже декларирована и в Украине [2], и работы в этом направлении уже развернуты.

Первые уроки

Начнем с того, что 30 июня 2006 г. на сайте ДСТЗІ Украины появилось официальное объявление о проведении конкурса по выдвижению кандидатов на национальный стандарт шифрования [3]. В процессе проведения конкурса было рассмотрено пять предложений, из которых на окончательное рассмотрение было представлено четыре (шифры ADE, Калина, Мухомор и Лабиринт). В отборе и анализе представленных решений приняли участие ученые и разработчики коллектива ЗАО "ИИТ", которые представили на конкурс два своих предложения (Калина, Мухомор). Конечно, работа над экспертизой проектов потребовала освоить и уже имеющийся международный опыт и форсировать разработку собственных подходов и методик, позволяющих ускорить процесс анализа и принятия решений. Анализ представленных на украинский конкурс решений показал, что шифры Калина и Мухомор [4, 5] (можно здесь отметить и другие предложения – ADE и Лабиринт [6, 7]) не уступают практически по всем показателям, в том числе и по стойкости к атакам линейного и дифференциального криптоанализа победителю конкурса AES – шифру Rijndael. Тем не менее, по результатам конкурса принято решение остановиться на общепризнанном мировом стандарте Fips-197 (AES). Национальные предложения оказались либо слишком близкими по конструкции к мировому лидеру, либо недостаточно прозрачными с точки зрения ожидаемых показателей стойкости по сравнению с мировым авторитетом.

Действительно, при принятии решений по конструкции БСШ разработчики находились под сильным влиянием конструкции уже признанной мировым сообществом

Шифр Калина по существу явился подражанием мировому лидеру. При его построении пошли по простому пути – не меняя принципиальных решений внести изменения, позволяющие перекрыть к тому времени уже обнаруженные потенциальные слабости шифра Rijndael, заключающиеся в его заметной алгебраичности (его прозрачная сбалансированная конструкция допускала алгебраическое описание [8]). Поэтому было принято решение заменить S-блоки, поддающиеся алгебраическому описанию, случайными и дополнительно ввести сложение с цикловыми подключами по еще одному модулю (наряду с операцией XOR, как это сделано в оригинале, ввести и операцию сложения по $\text{mod } 2^{32}$). Позже стало известно, что близкие решения были приняты и в шифре Anubis, представленном на конкурс NESSIE [9].

При построении шифра Мухомор использованы решения, близкие к другой уже достаточно хорошо известной конструкции шифра FOX [10]. Скелет цикловой функции строился на основе использования схемы Лея – Массэя, а внутренние преобразования цикловой функции, как и в шифре FOX, строились с применением матричного умножения выходов линейки S-блоков (SL-преобразование).

Оказались невостребованными и другие украинские предложения (шифры ADE и Лабиринт).

Отметим, что все указанные четыре шифра оказались близкими по показателям стойкости и быстродействию шифру Rijndael (Лабиринт медленнее Rijndael-я). По крайней мере.

два из предложений считались не уступающими ничем Rijndael-ю. Тем не менее, окончательное решение, как уже было отмечено выше, оказалось в пользу мирового лидера (стандарта FIPS-197).

Какие уроки можно вынести из прошедших событий:

1. Решения, представленные на украинский конкурс, не имели заметных преимуществ по сравнению с шифром Rijndael, или научно методический аппарат, которым владели разработчики, не позволил им обосновать преимущества своих решений;

2. Стратегия подражания, когда разработки в значительной степени повторяют известные решения, себя не оправдывает, т.е. необходимо искать конструкции, обладающие большей оригинальностью и ощутимыми преимуществами (испытание временем тоже очень серьезный критерий при анализе альтернатив);

3. Конкурировать с предложениями, прошедшими экспертизу специалистов мирового класса, очень трудная задача. Необходимо выходить со своими разработками на более высокие уровни экспертизы и их анализа, в частности нельзя игнорировать участие в международных конкурсах и проектах.

4. Быстро хорошего решения не найдешь. Должен идти непрерывный процесс накопления и совершенствования перспективных разработок и решений.

Но это все уроки на будущее. А пока остается работа по углубленному изучению опыта и достижений современной криптографии и поиска своего вклада в теорию и практику блочного симметричного шифрования, дальнейшее осмысление обширного набора требований к национальному стандарту и поиска путей эффективного их выполнения.

Требования к современным блочным симметричным шифрам (БСШ)

В этом разделе мы хотим привести требования к перспективным БСШ, которые в концентрированной форме изложены в положении прошедшего украинского конкурса [2]. Конечно, эти требования стали результатом изучения и обобщения мирового опыта в этом направлении, в частности прошедших конкурсов AES, NESSIE, CRYPTREC, и поэтому нет необходимости возвращаться к анализу известных документов.

Следуя [2], представим основное его содержание. Можно отметить, что изложенные требования можно свести к следующим основным:

1. Параметры криптоалгоритма:

- криптоалгоритм должен быть симметричным блоковым;
- размер блока данных – 128, 256, 512 бит;
- размер разового (сеансового) ключа – 128, 256, 512 бит.

2. Принципы построения:

– способность противостоять известным методам криптографического анализа и иметь запас стойкости с учетом тенденций развития средств электронной вычислительной техники и криптологической науки;

- применяемые криптографические преобразования должны базироваться на надежной и прозрачной математической базе и не иметь встроенных лазеек;

- скорость криптоалгоритма должна быть не меньше, чем скорость существующего государственного стандарта шифрования (а еще лучше быть того же порядка, что и у FIPS-197).

3. Реализация алгоритма:

– криптоалгоритм должен быть ориентирован на возможности реализации на 32- или 64-разрядных процессорах;

– определенные в криптоалгоритме операции должны допускать эффективную программную и аппаратную реализации;

– необходимый для работы объем памяти должен учитывать возможности реализации алгоритма в микроустройствах;

– должна быть предусмотрена возможность распараллеливания основных операций (алгоритмов шифрования, расшифрования и разворачивания ключей).

Ключевая система:

- криптоалгоритм может предусматривать наличие долговременного ключа;
- длина синхропосылки – не меньше 64 битов.

Режимы шифрования:

В криптоалгоритме должны быть предусмотрены следующие режимы шифрования:

- простая замена;
- сцепление блоков шифрованного текста;
- обратная связь по входу;
- обратная связь по выходу;
- режим выработки гаммы ("длинного цикла").

Как видно из представленного списка требований, в них учтены материалы и результаты прошедших международных конкурсов и имеющийся собственный опыт эксплуатации существующего стандарта. Сегодня уже можно отметить работу по уточнению и доработке этих требований.

В частности, просматривается возрастание технологических требований к алгоритмам шифрования [3]. Ставится задача – при сохранении требования обеспечения гарантированной стойкости реализовать высокую скорость шифрования как при программной (более 100 Мбит/с), так и при аппаратной (более 1000 Мбит/с) реализациях. При этом ставится условие, чтобы устройства шифрования по своей стоимости были доступными массовому пользователю. Дополнительно актуализируется необходимость обеспечения стойкости алгоритмов к ряду нетрадиционных атак, например к атаке на основе случайных аппаратных ошибок.

Некоторые полезные результаты пройденного пути

Решение задач, связанных с разработкой современных стандартов шифрования, очевидно, выдвигает на первый план владение современными методами оценки эффективности разрабатываемых и предлагаемых решений, важнейшей компонентой которых является владение методами криптоанализа

Конечно, основная (определяющая) компонента требований к блочным симметричным шифрам состоит в обеспечении высоких показателей криптостойкости. Здесь мы хотим отдельно остановиться на обеспечении стойкости к атакам дифференциального и линейного криптоанализа, считающимся наиболее мощными и наиболее опасными.

Следует отметить, что работа над представленными на украинский конкурс проектами не прошла даром. Получен опыт не только в разработке современных шифров, но и в освоении всего научно-методического аппарата, применяемого для оценки и сравнения между собой различных алгоритмов шифрования, выполнения проверки свойств и показателей стойкости алгоритмов шифрования за короткий период их анализа.

Сегодня уже можно сказать, что итогом прошедшего времени является предложенная и проверенная в действии новая ускоренная методика криптоанализа современных шифров, основанная на разработке и изучении свойств уменьшенных версий (моделей) шифров [11].

Выявлены недостатки существующей методики оценки стойкости блочных шифров к атакам дифференциального и линейного криптоанализа [12].

Разработана новая идеология (система взглядов) к оценке стойкости блочных симметричных шифров к атакам дифференциального и линейного криптоанализа, обладающая более высокой объективностью и точностью оценок [13].

Установлено, что показатели стойкости блочных шифров (максимальные значения полных дифференциалов и линейных корпусов) определяются не свойствами нелинейных преобразований (S-блоков), применяемых в современных шифрах, как это пропагандируется во многих зарубежных работах, а свойствами случайных подстановок, к которым приходят со-

временные шифры в процессе выполнения многоцикловых процедур шифрования [13]. Для каждого шифра существует свой переходный процесс прихода к случайной подстановке.

В результате появляется возможность выполнить сравнительную оценку шифрующих преобразований (шифров) по числу циклов шифрования, необходимых для "прихода" шифра к показателям случайной подстановки. Например, шифр семейства IDEA NXT требует для "прихода" к асимптотическому (установившемуся) значению полного дифференциала на два цикла преобразований больше, чем это требуется для шифра Rijndael. Поэтому (при прочих равных условиях) шифр Rijndael следует считать более совершенной конструкцией.

Этот критерий предлагается ввести для оценки эффективности конструкций цикловых преобразований. Возможно, что из всех вариантов построения цикловых конструкций та будет перспективнее, которая обеспечит переход к асимптотическому значению максимума полного дифференциала и асимптотическому значению максимума линейного корпуса за меньшее число циклов шифрования. Естественно, такое сравнение полноразмерных шифров неосуществимо. Однако его можно выполнить на малых (масштабированных) версиях шифров в рамках уже отмеченной выше ускоренной методики криптоанализа [11].

Заключение

Действительно, разработка и принятие нового стандарта блочного симметричного шифрования является для Украины одной из центральных задач в области криптографии. При ее решении необходимо исходить из двух альтернатив: создание оригинальной конструкции или гармонизация на основе лучших международных стандартов.

Мировой опыт разработки и принятия новых стандартов и результаты проведенных международных конкурсов позволили сформировать систему критериев (требований), которым должен удовлетворять современный блочный симметричный шифр.

Уже имеется опыт построения шифров, претендующих стать национальными стандартами, однако пока не удалось (а может, и не удастся) предложить конструкции, обладающие существенными преимуществами по сравнению с имеющимися решениями (алгоритмами шифрования), хотя следует отметить, что уже имеются прогрессивные решения в плане повышения быстродействия.

Одним из перспективных направлений поисков прогрессивных решений может стать разработка более эффективной конструкции циклового преобразования, позволяющего за меньшее число циклов шифрования реализовать переход к состоянию, обладающему показателями случайной подстановки.

Список литературы: 1. *NESSIE security report* // [http:// www. Cryptonessie. Org / NES/DOC/ENS/WPS/D20/2](http://www.Cryptonessie.Org/NES/DOC/ENS/WPS/D20/2), 2003. 2. *Молдавян А.А. и др Криптография: скоростные шифры.* – СПб. : БХВ-Петербург, 2002. – 496 с. 3. *Положення про проведення відкритого конкурсу криптографічних алгоритмів.* <http://dstszi.gov.ua/dstszi/control/uk/publish/>, 2006. 4. *Горбенко І.Д.* Перспективний блоковий симетричний шифр "Калина" – основні положення та специфікації / Горбенко І.Д., Долгов В.І., Олейников Р.В., Руженцев В.І., Михайленко М.С., Горбенко Ю.І., Тоцький О.С., Казьміна С.В. // *Прикладна радіоелектроніка.* – 2007. – Т.6. – № 2. – С. 195-208. 5. *Горбенко І.Д.* Перспективний блоковий симетричний шифр «Мухомор» – основні положення та специфікація / Горбенко І.Д., Бондаренко М.Ф., Долгов В.І., Олійников Р.В., Руженцев В.І., Михайленко М.С., Горбенко Ю.І., Олешко О.І., Кузьміна С.В // *Прикладна радіоелектроніка.* – Харьков : ХТУРЭ. – 2007. – Т. 6, №2. – С. 147-157. 6. *Головашич С.А.* Спецификация алгоритма блочного симметричного шифрования «Лабиринт» // *Прикладна радіоелектроніка.* – Харьков: ХТУРЭ. – 2007. – Т. 6, №2. – С. 230-240. 7. *Кузнецов А.А.* Симметричный криптографический алгоритм ADE (Algorithm of Dynamic Encryption) / Кузнецов А.А., Сергиенко Р.В., Наумко А.А. // *Прикладна радіоелектроніка.* – Харьков : ХТУРЭ. – 2007. – Т. 6, №2. – С. 241–249. 8. *Nicolas Courtois.* General Principles of Algebraic Attacks and New Design Criteria for Components of Symmetric Ciphers. In H. Dobbertin, V. Rijmen. and A. Sowa, editors, Fourth Conference on the Advanced Encryption Standard – AES4, volume 3373 of Lecture Notes in Computer Science, pages 67–83. Springer-Verlag, 2004. 9. *P. Barreto, V. Rijmen.* The Anubis Block Cipher. Submission to the NESSIE Project, 2000. 10. *P. Junod and S. Vaudenay.* FOX: a new family of block ciphers. In H. Handschuh

and A. Hasan, editors, Selected Areas in Cryptography: 11th International Workshop. SAC 2004. Waterloo, Canada, August 9-10, 2004. Revised Selected Papers, volume 3357 of Lecture Notes in Computer Science, pages 114–129. Springer-Verlag, 2004. 11. Долгов В.И. Подход к криптоанализу современных шифров / Долгов В.И., Лисицкая И.В., Олейников Р.В. // Материалы второй международной конференции "Современные информационные системы. Проблемы и тенденции развития". -- Харьков-Туапсе, Украина, 2–5 октября. – 2007. – С. 435-436. 12. Лисицкая И.В. Об участии S-блоков в формировании максимальных значений дифференциальных вероятностей блочных симметричных шифров / Лисицкая И.В., Казимиров А.В. // Proceedings International Conference SAIT 2011. – Kyiv, Ukraine, May 23-28, 2011. – С. 459. 13. Горбенко І.Д. Новая идеология оценки стойкости блочных симметричных шифров к атакам дифференциального и линейного криптоанализа / Горбенко І.Д., Долгов В.И., Лисицкая И.В., Олейников Р.В. // Прикладная радиоэлектроника. – 2010. – Т. 9. № 3. – С. 212-320.

*Харьковский национальный
университет радиоэлектроники*

Поступила в редколлегию 11.07.2011

AN IMPACT OF S-BOX BOOLEAN FUNCTION PROPERTIES TO STRENGTH OF MODERN SYMMETRIC BLOCK CIPHERS

Introduction

Modern symmetric block ciphers use an idea of interleaving of linear and non-linear layers. For most of ciphers, S-boxes are the only one non-linear component determined the cryptographic strength to various analytical attacks. Up to date an important question of generation of substitutions with optimal characteristics to prevent all known cryptanalytical attacks remains open. There exist several approaches to generation of S-boxes with good cryptographic properties, and methods based on the analysis of Boolean function properties are among widespread ones. Another method for generation of S-boxes with perfect differential and linear properties based on the power function in the finite field was proposed in [1]. Such type of S-boxes was used in many ciphers, including AES/Rijndael. However, further analysis has shown that this approach leads to existence of overdefined system of equations with low degree for S-boxes, and potential vulnerability of the cipher to XSL attack [2]. Further analysis of Boolean function properties have shown that such type of S-boxes uses the single non-linear Boolean function with different linear transformation of its arguments [3]. In this article there are identified most important properties of S-boxes Boolean function properties with respect to strength of symmetric block ciphers to known cryptanalytical attacks, and correlation of such properties with other known S-box characteristics.

Cryptographic properties of Boolean functions

Let $V_2^n = GF(2)^n$ be the N -dimensional vector space of binary N -tuples. An N -variable Boolean function $f(x)$ is a mapping from $f(x) : V_2^N \rightarrow V_2$ where $x = (x_{n-1}, x_{n-2}, \dots, x_0)$.

Let $f(x)$ be N -variable Boolean function. Then Hadamard weight is calculated as follows:

$$hw(f) = \sum_{x=0}^{2^n-1} f(x) \quad (1)$$

Let $f(x)$ and $g(x)$ are N -variable Boolean functions. Then hamming distance between this functions can be calculated as follows:

$$hd(f, g) = \sum_{x=0}^{2^n-1} f(x) \oplus g(x) \quad (2)$$

The algebraic normal form (ANF) of an N -variable Boolean function $f(x)$ is written as follows:

$$f(x) = a \oplus a_0x_0 \oplus a_1x_1 \oplus \dots \oplus a_{n-1}x_{n-1} \oplus a_{01}x_0x_1 \oplus a_{02}x_0x_2 \oplus \dots \oplus a_{(n-2)(n-1)}x_{n-2}x_{n-1} \oplus \dots \oplus a_{012\dots n-1}x_0x_1x_2\dots x_{n-1} \quad (3)$$

The algebraic degree of a Boolean function $f(x)$, denoted by $deg(f)$, is defined to be the number of variables in the largest product term of the function's ANF having a non-zero coefficient.

The Walsh Hadamard transform (WHT) of the truth table of a Boolean function $f(x)$, denoted by $W(\omega)$, is a measure of the correlation between a function and the set of all linear functions. It is defined by

$$W(x) = \sum_{x=0}^{2^n-1} (-1)^{f(x) \oplus l_\omega(x)}, \quad (4)$$

where Boolean function of the form $l_\omega(x) = \omega \cdot x = \omega_0x_0 \oplus \omega_1x_1 \oplus \dots \oplus \omega_{n-1}x_{n-1}$ is a linear function of N variables.

Function $f(x)$ of N -variable is called balanced if

$$hw(f) = 2^{n-1} \quad (5)$$

The nonlinearity of an N -variable Boolean function $f(x)$, denoted by $NL(f)$, is the minimum distance to the set of all N -variable affine functions. Following equation describes relationship between the nonlinearity of Boolean function $f(x)$ and the Walsh Hadamard transform:

$$NL(f) = \frac{1}{2} (2^n - W_{\max}) \quad (6)$$

The autocorrelation function of the truth table of a Boolean function $f(x)$, denoted by $r_f(\alpha)$, is a measure of the directional derivative of a function for an input shift in the direction of α overall $x \in V_2^n$. It is defined by

$$r_f(\alpha) = \sum_{x=0}^{2^n-1} (-1)^{f(x) \oplus f(x \oplus \alpha)} \quad (7)$$

Let $|AC|_{\max}$ denote the maximum absolute autocorrelation value derived from the autocorrelation function $r_f(\alpha)$, then:

$$|AC|_{\max} = \max_{\alpha} |r_f(\alpha)| \quad (8)$$

Let σ denote the sum-of-square indicator, also derived from the autocorrelation function $r_f(\alpha)$, then:

$$\sigma = \sum_{\alpha=0}^{2^n-1} r_f^2(\alpha) \quad (9)$$

An N -variable Boolean function $f(x)$ is said to satisfy strict avalanche criterion (SAC) if for every s is true that:

$$\begin{cases} hw(s) = 1; \\ \sum_{x=0}^{2^n-1} f(x) \oplus f(x \oplus s) = 2^{n-1}. \end{cases} \quad (10)$$

An N -variable Boolean function $f(x)$ is said to satisfy the propagation criteria of degree k , $PC(k)$, accounting a non-zero vector $\alpha \in V_2^n$ if

$$\begin{cases} 1 \leq hw(\alpha) \leq k; \\ \sum_{x=0}^{2^n-1} f(x) \oplus f(x \oplus \alpha) = 2^{n-1}. \end{cases} \quad (11)$$

An N -variable Boolean function $f(x)$ is m^{th} -order correlation immunity, denoted by $CI(m)$, if for every ω is true that

$$\begin{cases} 1 \leq hw(\omega) \leq m; \\ W(\omega) = 0. \end{cases} \quad (12)$$

An N -variable Boolean function, $f(x)$, which is both balanced and has m^{th} -order correlation immunity, is known as an m -resilient Boolean function.

Cryptographic properties of substitutions

Let $S = (f_M, f_{M-1}, \dots, f_1)$ be an $N \times M$ substitution (S-box) where f_i ($i = M, M-1, \dots, 1$) are N -variable Boolean functions. Let g_j be the set of linear combinations of f_i ($i = M, M-1, \dots, 1$) (which includes the functions f_i). Then:

- the nonlinearity of S , denoted by $N(S_{N,M})$ can be expressed as follows:

$$N(S_{N,M}) = \min_g \{NL(g_j)\} \quad (j=1,2,\dots,2^{M-1}) \quad (13)$$

- the algebraic degree of S , denoted by $\deg(S_{N,M})$, is defined as:

$$\deg(S_{N,M}) = \min_g \{\deg(g_j)\} \quad (j=1,2,\dots,2^{M-1}) \quad (14)$$

- the maximum absolute autocorrelation value of S , denoted by $|AC(S_{N,M})|_{\max}$, is defined as:

$$|AC(S_{N,M})|_{\max} = \max_g \{r_{g_j}(\alpha)\} \quad (15)$$

where $\alpha \in \{1,2,\dots,2^{N-1}\}$ and $(j=1,2,\dots,2^{M-1})$.

- S is said to satisfy strict avalanche criterion if every g_j ($j=1,2,\dots,2^{M-1}$) satisfies SAC.
- S is said to satisfy propagation criteria of order k , if every g_j ($j=1,2,\dots,2^{M-1}$) satisfies $PC(k)$.
- S is t^{th} -order correlation immunity if all g_j ($j=1,2,\dots,2^{M-1}$) are t^{th} -order correlation immunity Boolean functions.
- S is a t -resilient s-box, if all g_j ($j=1,2,\dots,2^{M-1}$) are t -resilient Boolean functions.
- S is balanced if every g_j ($j=1,2,\dots,2^{M-1}$) is balanced.

Let S be an $N \times M$ S-box. Let δ be the largest value in the differential distribution table of the S-box (not taking into account first row and column). Then

$$\delta = \max_{\alpha \in V_2^N, \alpha \neq 0, \beta \in V_2^M} \max \# \{x \mid S(x) \oplus S(x \oplus \alpha) = \beta\} \quad (16)$$

Let S be an $N \times M$ S-box. Let λ be the largest value in the linear distribution table of the S-box (not taking into account first row and column). Then

$$\lambda = \max_{\alpha \in V_2^N, \alpha \neq 0, \beta \in V_2^M} \left| \# \left\{ x \mid \bigoplus_{s=0}^N (x[s] \cdot \alpha[s]) = \bigoplus_{t=0}^N (S(x)[t] \cdot \beta[t]) \right\} \right|, \quad (17)$$

where $\zeta[s]$ is a s^{th} bit of ζ .

Let r be the number of equations of a system, which described an $N \times M$ S-box. Then:

$$r = \sum_{x=0}^d \binom{N+M}{d} - \text{Rank}(A), \quad (18)$$

where A is a matrix, which contains all input and output bits, and all combinations up to degree d .

We said that S-box is good, if $\text{Rank}(A) = 2^N$. It is easy to see, that if $\text{Rank}(A) = 2^N$ then d has a maximum value [4]. Increasing of d up to the maximum value increases the system dimension and consequently more memory is required for processing the system of equations.

Next three properties were given in works [5, 6]. Let S be an $N \times N$ S-box. Let η be a number of inversions in substitution. Then

$$\left| \eta - \frac{N(N-1)}{4} \right| \leq a \frac{\sqrt{N^3}}{6}, \quad (19)$$

where $a=1$ in general case.

Let S be an $N \times N$ S-box. Let ς be a number of cycles in substitution. Then

$$|\varsigma - \ln(N)| \leq a\sqrt{\ln(N)}, \quad (20)$$

where $a=1$ in general case.

Let S be an $N \times N$ S-box. Let θ be a number of increases in substitution. Then

$$\left| \theta - \frac{N}{2} \right| \leq a\sqrt{\frac{n}{12}}, \quad (21)$$

where $a=1$ in general case.

Analysis of criteria for generation of substitutions

After publishing papers on differential [7] and linear [8] cryptanalysis there were suggested criteria for S-box selection for protection of such types of attacks. In [1] there were proposed a method for generation of perfect non-linear S-boxes with the minimal achievable probability of non-trivial difference transformation and linear approximation. The algebraic attack is based on possibility to describe all cipher by a system of equations. In contrast to differential and linear cryptanalysis, attacker needs several pairs of plaintext and corresponding ciphertext [9, 10, 11, 12].

The relationship between difference distribution table and table of Boolean functions' autocorrelation is showed in [13]. In paper only the boundary between autocorrelation and maximum of differential table is described

$$\delta > 2^{N-M} + 2^{-M} AC(S_{N,M})_{\max}. \quad (22)$$

This relationship suggests that the rate of the autocorrelation is important for choosing a S-box, but now there is no method for determining direct correspondence between the autocorrelation of Boolean functions and a the maximum of differential table.

Nonlinearity of Boolean functions is directly related with maximum value of approximating table as $NL(S_{N,M} = 2^{N-1} - \lambda)$. Clearly, these two criteria are commutative. Thus, if we know the nonlinearity of Boolean functions, we can uniquely determine the maximum of approximating table and vice versa.

The avalanche effect is an important property of S-boxes. It shows how many of output bits of S-box change with changing of a subset of the input bits. This property is necessary to prevent statistical attacks and connected with differential properties of S-box. If a substitution satisfies the strict avalanche criterion then changing of a single input bit changes exactly half of output bits. Propagation criterion includes strict avalanche criterion. From equation (11) is easily seen that when $k=1$ PC becomes SAC. Thus, we should choose only propagation criterion while generating substitution.

The correlation immunity criteria of Boolean functions are used in primary to protect stream ciphers against the correlation attacks. In [14] χ^2 -attack on ciphers RC-5 and RC-6 is shown. But till now there are no papers showed application of such type of attacks to block ciphers.

In addition, in recent papers there was showed that the value of the differential does not depend on non-linear S-box properties after sufficient number of rounds [15]. However, it is noted that the S-box influence on dynamic indicators, i.e. how quickly the cipher comes to the theoretical average maximum of differential table. This means that S-box with good properties is much more effective than randomly generated.

The table below contains results of calculating the number of equations describing substitution, properties of Boolean functions, the maximum of differential and linear table. Values were calculated for substitutions that are used in ciphers AES, Camellia, Labyrinth and Kalina [16, 17].

Results given in the table 1 show that S-boxes of modern symmetric block ciphers does not satisfy to many well-known requirements for Boolean functions. Substitutions from current standards of encryption (such as AES, Camellia) do not satisfy propagation criterion (including the SAC).

correlation immunity, but have the minimal value of non-trivial transformation in differential and linear approximating tables.

According to strength to known cryptanalytical attacks, there can be selected the following criteria for S-boxes of symmetric block ciphers:

- nonlinearity of Boolean functions (or maximum of approximating table);
- maximum of differential table;
- maximum degree of the system representing the S-box.
- propagation criterion.

It also should be mentioned that it is necessary to research the relationships between these criteria.

S-boxes Char.	AES	Cam.	Lab.	K0	K1	K2	K3	K7
Balance of BF	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
NL	112	112	112	96	98	96	96	96
AC	32	32	32	88	88	88	104	96
SSI	133120	133120	133120	244480	252928	259456	291712	251392
PC	0	0	0	0	0	0	0	0
CI	0	0	0	0	0	0	0	0
Resilient	0	0	0	0	0	0	0	0
Degree	7	7	7	7	7	6	7	7
Number of eq.	39	39	39	441	441	441	441	441
Degree of eq.	2	2	2	3	3	3	3	3
Inversions	Yes	No	Yes	No	No	No	No	Yes
Cycles	Yes	No	Yes	Yes	Yes	No	Yes	Yes
Increases	Yes	No	Yes	No	No	Yes	Yes	Yes
MDT	4	4	4	8	8	8	8	8
MLT	16	16	16	32	30	32	32	32
Bijjective	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Conclusions

There exist several different approaches to generation of cryptographically strength S-boxes for symmetric block ciphers. An approach based on analysis of Boolean function properties takes into consideration requirements of non-linear components of stream ciphers for construction of S-boxes for block ciphers. It is shown, that S-boxes of widely used modern symmetric block ciphers does not satisfy to several well-known requirements to Boolean functions, like propagation criterion and correlation immunity. But other properties of S-box Boolean functions, like nonlinearity and autocorrelation, connected to strength of the cipher to differential and linear attacks.

References: 1. Kaisa Nyberg, "Perfect nonlinear S-boxes". Advances in Cryptology, EUROCRYPT, 1991, 378-386. 2. Nicolas T. Courtois, Gregory V. Bard, "Algebraic Cryptanalysis of the Data Encryption Standard". Lecture Notes in Computer Science, Volume 4887/2007, 2007, 152-169. 3. J.Fuller, W. Millan, "Linear Redundancy in S-Boxes". Lecture Notes in Computer Science, Volume 2887/2003, 2003, 74-86. 4. R. Oliynykov, O. Kazymyrov, "The choice of S-boxes for symmetric cryptographic algorithms based on the analysis of algebraic properties". Journal of Kharkov National University. Mathematical simulation. Information Technology. Control Systems., 2010, 177-179. 5. I.V. Lysytska, A.S. Koriak, et al. "The selection criteria of random substitution tables for symmetric enciphering algorithms" / Abstracts of XXVIth General Assembly. Toronto, Ontario Canada 1999, 204. 6. Dolgov V.I., Lysytsky K.E. "Random substitutions in cryptography" / Radioelectronic and computer systems, №5 2010, 79-85. 7. E. Biham, . Shamir, "Differential Cryptanalysis of DES-like Cryptosystems" Advances in Cryptology, Springer-Verlag 1990, 2-21. 8. Mitsuru Matsui, "Linear cryptanalysis method for DES cipher". In Workshop on the theory and application of

cryptographic techniques on Advances in cryptology (EUROCRYPT '93), Tor Helleseeth (Ed.). Springer-Verlag New York, Inc., Secaucus, NJ, USA 1993, 386-397. 9. *R.V. Oliynykov, O.V. Kazymyrov*, "Algebraic properties of the key schedule of block symmetric cipher "Kalina"". Radioelectronic and computer systems, №5, 2010, 61-66. 10. *R.V. Oliynykov, O.V. Kazymyrov*, "Construction of the overdefined system of equations to describe symmetric block cipher "Labyrinth"". Applied electronics, Volume 8, №3, 2009, 247-251. 11. *N. Courtis, J. Pieprzyk*, "Cryptanalysis of Block Cipher with Overdefined System of Equations". Lecture Notes in Computer Science, Volume 2501/2002 2002, 267-287. 12. *N. Courtois, A. Klimov, J. Patarin, A. Shamir*, "Efficient Algorithms for solving Overdefined System of Multivariate Polynomial Equations". Lecture Notes in Computer Science, Volume 1807/2000 2000, 392-407. 13. *X. Zhang, Y. Zheng, H. Imai*, "Relating Differential Distribution Tables to Other Properties of of Substitution Boxes". Designs, Codes and Cryptography, Volume 19, Number 1, 1998, 45-63. 14. *T. Shimoyama, K. Takeuchi, J. Hayakawa*, "Correlation Attack to the Block Cipher RC5 and the Simplified Variants of RC6". In Proceedings of the 3rd AES Conference (AES3), 2000. 15. *V.I. Dolgov, I.V. Lysytska, O.V. Kazymyrov*, "Variations on a theme cipher Rijndael". Applied electronics, Volume 9, №3, 2010, 321-325. 16. *I.D. Gorbenko, V.I. Dolgov, R.V. Oliynykov et al.*, "Advanced symmetric block cipher "Kalina"- the basic main aspects and specifications". Applied electronics, Volume 6, №2, 2007, 195-208. 17. *S. Golovashich*, "Specification of block symmetric encryption algorithm "Labyrinth"". Information processing systems. Volume 4, 2007, 230-240.

Kharkov National University of Radioelectronics

Received 25.08.2011

ОБ УЧАСТИИ S-БЛОКОВ В ФОРМИРОВАНИИ МАКСИМАЛЬНЫХ ЗНАЧЕНИЙ ЛИНЕЙНЫХ ВЕРОЯТНОСТЕЙ БЛОЧНЫХ СИММЕТРИЧНЫХ ШИФРОВ

Введение

Мы хотим возвратиться к работе [1], в которой приведен краткий обзор ряда публикаций последних лет по вопросам оценки доказуемой стойкости блочных симметричных шифров (БСШ) к атакам дифференциального и линейного криптоанализа.

В этой работе отмечается, что в затронутых публикациях и во многих других работах на эту тематику развивается концепция, в соответствии с которой показатели доказуемой стойкости БСШ к атакам дифференциального и линейного криптоанализа непосредственно связываются с дифференциальными и линейными показателями входящих в шифры S-блоковых конструкций, и излагается новая точка зрения к оценке соответствующих показателей. Эта точка зрения появилась на основе развития нового подхода в теории и методах криптоанализа, родившегося на кафедре БИТ ХНУРЭ [3], о котором уже говорилось в работе [4]. Он ориентирован, как было отмечено, с одной стороны, на использование при определении ожидаемых показателей стойкости больших шифров результатов анализа уменьшенных их версий, а с другой, — сформированной в последнее время новой идеологии определения показателей стойкости БСШ к атакам дифференциального и линейного криптоанализа [1], основывающейся на подтвержденном многочисленными экспериментами с уменьшенными версиями современных шифров (DES, ГОСТ, Rijndael, Лабиринт, Мухомор, Калина, ADE, Камелия, FOX и многих других) положении (факте), состоящем в том, что все эти шифры (и большие и малые их версии) через определенное число циклов (для рассмотренных уменьшенных моделей от трех циклов до семи) независимо от используемых в шифрах S-блоков приобретают свойства случайной подстановки по комбинаторным показателям (числу инверсий, возрастаний и циклов), а также по законам распределения переходов XOR таблиц дифференциальных разностей (полных дифференциалов) и законам распределения смещений таблиц линейных аппроксимаций (линейных корпусов) они повторяют соответствующие показатели случайной подстановки [5 – 7]). Здесь и далее под случайной подстановкой понимается подстановка, удовлетворяющая установленным критериям близости законов распределения циклов, возрастания и инверсий, а также законов распределения переходов их XOR таблиц и смещений таблиц линейных аппроксимаций соответствующим теоретическим (асимптотическим) законам распределения вероятностей [8]. Этот факт зафиксирован в работе [1] в виде утверждения.

Утверждение. *Для каждого блочного симметричного шифра (из числа известных итеративных БСШ) существует вполне определенное число циклов, после которого шифр приобретает свойства случайной подстановки. Дальнейшее наращивание числа циклов не влияет на итоговые дифференциальные и линейные свойства шифра. Это значение является одним и тем же для всех шифрующих преобразований с одинаковым битовым размером входа.*

Конечно, аккуратнее было бы говорить только об уже проверенных шифрах, но, на взгляд авторов работы [1], это свойство должно быть присуще любому сколько-нибудь внушающему доверие шифру.

А это значит, что концепция, разрабатываемая в представленных выше и многих других работах, является неверной. Для подтверждения выдвинутых в работе [1] положений были проведены многочисленные исследования дифференциальных и линейных свойств уменьшенных моделей ряда современных шифров [2, 9 – 12 и др.], а теперь уже и их больших прототипов [13, 14], и экспериментами показано, что и малые и большие конструкции современ-

ных шифров действительно при полном наборе шифрующих операций приобретают свойства случайных подстановок соответствующей степени.

Здесь мы хотим отдельно отметить работу [2], одну из большого числа отмеченных публикаций, посвященную непосредственно исследованию влияния на показатели стойкости шифров характеристик, используемых при их построении S-блоков. В ней были представлены результаты оценки такого влияния на полные дифференциалы уменьшенных моделей ряда современных шифров. В этой работе мы продолжаем излагать результаты исследований в отмеченном направлении и приводим результаты оценки влияния на значения теперь уже максимумов линейных корпусов (оболочек) шифров линейных показателей применяемых при их построении S-блоков.

Понятийный аппарат линейного криптоанализа

Кратко напомним подходы к определению линейных показателей подстановочных преобразований (S-блоков и шифров в целом).

Для характеристики линейных показателей S-блоков воспользуемся определениями работы [15] и ряда других работ. Далее S-блоки рассматриваются как булевы векторные функции.

Определение 1 [16]. Векторной булевой функцией $y = f(x)$, $f = (f_1, f_2, \dots, f_n)$ называется функция (последовательность функций), отображающая булевой вектор (вектор с битовыми координатами) в другой булевой вектор (здесь и далее такой же размерности, как и исходный вектор):

$$f : GF(2^n) \rightarrow GF(2^n), x \mapsto y = f(x).$$

Очевидно, что одной из математических реализаций булевой векторной функции выступает подстановка.

Аффинность и нелинейность. При использовании математического аппарата булевой алгебры для описания свойств подстановочных преобразований рассматриваются свойства компонентных булевых функций.

Определение 2 [17]. Аффинной называется функция $f(x) : GF(2^n) \rightarrow GF(2)$ (здесь рассматривается одна функция из полного их набора f) над $GF(2^n)$ вида

$$f = a_1 x_1 \oplus \dots \oplus a_n x_n \oplus c,$$

где $a_j, c \in GF(2)$, $j = 1, 2, \dots, n$.

В обозначениях работы [18]:

$$f = w \bullet x \oplus c.$$

Здесь $w \bullet x$ обозначает скалярное произведение двух векторов $w, x \in GF(2^n)$. Если $c = 0$, то функция f называется линейной.

Определение 3 [17]. Хэмминговым весом вектора $x \in GF(2^n)$ ((0,1)-последовательности), обозначаемым как $W(x)$, называется число единиц в этом векторе.

Определение 4 [18]. Расстоянием Хэмминга $d_H(f, g)$ между двумя функциями f и g является количество позиций, в которых последовательности этих функций различаются.

Определение 5 [18,19]. Нелинейность функции N_f – это минимальное расстояние Хэмминга между функцией f и всеми аффинными функциями линейного пространства $GF(2^n)$:

$$N_f = \min_{i=1, 2, \dots, 2^{n+1}} \{d_H(f, \varphi_i)\},$$

где $\varphi_1, \varphi_2, \dots, \varphi_{2^{n+1}}$ – аффинные функции n мерного линейного пространства над полем $GF(2)$.

В [18] представлено определение нелинейности N_f в виде

$$N_f = \min_{w, c} d_H(f(x), w \bullet x \oplus c).$$

Установлено [17], что для произвольной булевой функции f нелинейность N_f над $GF(2^n)$ может достигать значения

$$N_f \leq 2^{n-1} - 2^{\frac{n-1}{2}}.$$

Для сбалансированной функции f над $GF(2^n)$ ($n \geq 3$) нелинейность N_f может достигать значений [17]:

$$N_f \leq \begin{cases} 2^{n-1} - 2^{n/2-1} - 2, & n = 2k, \\ \left\lfloor \left\lfloor 2^{n-1} - 2^{n/2-1} \right\rfloor \right\rfloor, & n = 2k + 1, \end{cases}$$

где $\lfloor x \rfloor$ – максимальное четное целое, меньшее либо равное x .

Определение 6 (Линейная аппроксимационная таблица – LAT для S-блоков) [20].

Для данного S-блока $S(x): GF(2^n) \rightarrow GF(2^n)$ (векторной булевой функции) *линейная аппроксимационная таблица*, имеющая вход в w -ю строку и c -ю колонку (в этой работе для обозначения векторов используются прописные символы, которые не выделяются полужирным шрифтом), определяется как

$$\begin{aligned} LAT(w, c) &= |x / c \bullet S(x) = w \bullet x| - 2^{n-1} = |x / f(x) = w \bullet x| - 2^{n-1} \\ &= |x| f(x) = l_w(x) | - 2^{n-1} \\ &= 2^n - d_H(f, l_w) - 2^{n-1} \\ &= 2^{n-1} - d_H(f, l_w). \end{aligned} \quad (1)$$

В качестве значения ячейки таблицы выступает смещение истинного значения числа выполнения равенств $c \bullet S(x) = w \bullet x$ для заданного значения пары входов в w -ю строку и c -ю колонку таблицы от значения 2^{n-1} (по предложению автора линейного криптоанализа М. Мацуи).

В этих же обозначениях

Определение 7 (Критерий нелинейности для S-блоков) [18]. *Нелинейность N_S S-блока определяется как худший случай нелинейности:*

$$N_S = \min_f N_f = \min_f \{N_f / f(x) = c \bullet S(x), c \neq 0\}, \quad (2)$$

где минимизация ведется по всем возможным выходным битовым комбинациям $f(x) = \bigoplus_{i=1}^n c_i f(x_i) = c \bullet S(x)$, соответствующим всем ненулевым значениям маскового вектора $c = (c_1, \dots, c_n) \big|_{1 \times n}$ (по всем компонентным булевым функциям).

Полезно будет также напомнить лемму из работы [18].

Лемма (Соотношение между нелинейностью S-блока и максимальным значением элемента LAT). *Нелинейность S-блока, определяемая из (2), может быть представлена в терминах максимального значения элемента LAT как*

$$N_s = \min_f N_f = 2^{n-1} - \max_{w, c \in F_2^n} |LAT(w, c)|, \quad (3)$$

где $f(x) = c \bullet S(x)$, $c \neq 0$ является любой из выходных линейных комбинаций.

Далее приведены два определения, относящиеся уже к подстановочному преобразованию в виде ключезависимой функции $f = f[k](x)$ (шифра), заимствованные из работы [15].

Определение 8 (Линейная вероятность): *Линейная вероятность LP^f для ключезависимой функции f с n -битным входом x и n -битным выходом y ($x, y \in GF(2)^n$) есть*

$$LP^f = (Gx \rightarrow Gy) = \left(\frac{\#\{x \in GF(2)^n / x \cdot Gx = f(x) \cdot Gy\}}{2^{n-1}} - 1 \right)^2.$$

где Gx и Gy являются входной и выходной масками ключезависимой функции f ; $x \cdot Gx$ обозначает результат скалярного произведения x и Gx (это практически повторение определения (1) в других обозначениях). Мы несколько модифицируем обозначения работы [15], вводя в них зависимость от ключа зашифрования. В работе [16] при рассмотрении случайных блочных шифров вводится понятие фиксировано-ключевой корреляции $LP[k]$ (в нашем случае мы воспользуемся обозначением $LP^{f[k]}$). Нам оно кажется более уместным.

Определение 9 ($LP_{\max}^{f[k]}$). *Максимальное значение линейной вероятности для ключезависимой функции f определяется как*

$$LP_{\max}^{f[k]} = \max_{Gx, Gx \neq 0} LP^{f[k]}(Gx \rightarrow Gy). \quad (2)$$

В общем случае ключезависимая функция f является сильной, если значение $LP_{\max}^{f[k]}$ функции f является достаточно малым [15].

Приведем еще одно определение, являющееся нашей модификацией выражения, введенного в работе [15] для *MALHP*.

Определение 10 (*ALHMP*). *Среднее (по ключам) значение максимальной вероятности линейных корпусов функций $f[k](x)$ есть*

$$ALHMP = \text{ave}_k LP_{\max}^{f[k]}(Gx \rightarrow Gy) = \frac{1}{2^h} \sum_{i=1}^{2^h} LP_{\max}^{f[k]}(Gx \rightarrow Gy).$$

где 2^h – мощность использованного множества ключей зашифрования.

Результаты вычислительных экспериментов

В этой разделе продемонстрированы результаты исследований по оценке влияния на линейные показатели современных шифров (их малых версий) линейных показателей используемых в шифрах блоков нелинейных замен (S-блоков).

Первая часть экспериментов была связана с генерацией и отбором S-блоков с различными показателями нелинейности. Конкретные примеры подстановок, отобранных в ходе экспериментов этого этапа, иллюстрирует табл. 1.

Представленные в таблице подстановки были использованы в качестве S-блоков во всех исследуемых малых моделях шифров (в каждом шифре использовались S-блоки с одинаковыми показателями нелинейности).

Таблица 1

Полубайтовые подстановки (S-блоки) с различными показателями нелинейности

Нелинейность	S-блок
0	$S_1 = \{12, 13, 5, 1, 10, 11, 6, 2, 14, 3, 7, 15, 4, 0, 8, 9\}$
0	$S_2 = \{5, 0, 13, 6, 4, 8, 2, 3, 9, 1, 15, 10, 12, 14, 7, 11\}$
2	$S_3 = \{10, 4, 5, 8, 2, 15, 7, 0, 14, 9, 11, 12, 6, 13, 1, 3\}$
2	$S_4 = \{2, 5, 0, 9, 3, 14, 4, 1, 10, 11, 8, 15, 7, 12, 6, 13\}$
4	$S_5 = \{10, 4, 3, 11, 8, 14, 2, 12, 5, 7, 6, 15, 0, 1, 9, 13\}$

Вторая (основная) часть исследований и вычислительных экспериментов была посвящена вычислению поцикловых средних значений максимумов смещений линейных корпусов (ALHMP) уменьшенных моделей трех шифров из представленных на украинский конкурс (шифры Лабиринт, Мухомор и Калина) и уменьшенной модели шифра Rijndael. Сами конструкции уменьшенных моделей шифров были заимствованы из работ, выполненных на кафедре.

Для каждого шифра с фиксированным числом циклов шифрования выполнялось построение линейных корпусов (таблиц линейных аппроксимаций) для 30 различных ключей зашифрования, сгенерированных случайным образом, определялись максимальные значения смещения для каждой из таблиц, а затем результаты усреднялись. Мы интересовались зависимостью средних значений максимумов смещений линейных корпусов от числа циклов зашифрования.

В табл. 2 – 5 представлены поцикловые значения средних значений максимумов смещений таблиц линейных аппроксимаций (линейных корпусов) для рассмотренных в работе шифров.

Таблица 2

Математическое ожидание максимальных смещений линейных корпусов шифра мини-Лабиринт со значениями среднеквадратического отклонения

Число циклов шифрования r	Показатели нелинейности S-блоков, использованных в шифре				
	0	2	0	2	4
1	10751,6±1934	4385,6±1166	3200±494	4300±1774	3178±777
2	1910,8±460	1182,2±162	1219,6±312	1043,60±252	980±193
3	1032,8±190	839,2±34	864,4±55	831,6±27	825,4±14
4	810±15	813,6±13	822,4±17	811,4±11	825,6±23
5	816,2±17	827,8±16	833,4±25	809±15	817,2±11
6	826,4±24	832±32	814,8±24	828,2±35	824±21
7	817,8±18	812±13	811±17	837,4±22	823,4±30
8	835,4±16	813,6±19	822,6±23	815,4±20	833,6±35
9	819,4±23	812,6±14	815,8±26	820,4±15	824,8±24
10	820,6±20	815,4±22	814,4±20	808±21	819±17

Как следует из представленных результатов, во всех случаях, независимо от значения показателя нелинейности S-блоков, все шифры приходят к одному и тому же среднему значению максимума смещения линейного корпуса, характерному (весьма близкому) случайной подстановке соответствующей степени [6, 7]. По всем рассмотренным шифрам видно, что для перехода к асимптотическому значению смещения требуется 4 – 5 циклов. Видно, что использование S-блоков с высокими показателями нелинейности дает выигрыш в динамике выхода к асимптотическому значению в пределах одного цикла.

Таблица 3

Математическое ожидание максимальных смещений линейных корпусов шифра мини-Калина со значениями среднеквадратического отклонения для соответствующих S-блоков

Число циклов шифрования r	Показатели нелинейности S-блоков, использованных в шифре				
	0	2	0	2	4
1	21845,3±5565	18090,6±1043	16497,7±2222	11491,5±1825	9671,1±867
2	9557,33±1231	7288,8±758	5432,88±693	3968±307	3370,6±301
3	2823,55±436	1661,22±168	1394,66±219	862,66±50	836,8±15
4	1307,77±216	822,55±30	815,33±17	826,44±23	832,2±21
5	818,88±21	796±20	818,66±11	811,77±12	838,6±21
6	824,22±15	808,66±29	840,44±28	816,88±13	835,5±33
7	810±18	811±30	820,88±32	824,44±23	821,5±22
8	819,77±21	808,88±29	834,66±43	829,33±16	827,3±18
9	808±20	810,66±11	811,33±15	827,77±22	813,3±21
10	836,44±39	821,55±26	816±11	817,33±16	834±28

Таблица 4

Математическое ожидание максимальных смещений линейных корпусов шифра мини-Мухомор со значениями среднеквадратического отклонения для соответствующих S-блоков

Число циклов шифрования r	Показатели нелинейности S-блоков, использованных в шифре				
	0	2	0	2	4
1	32768±0	32768±0	32768±0	32768±0	32768±0
2	16896±2101	15616±1511	14364,4±1372	10951,1±1112	12839,3±1031
3	7082,6±1020	6553,3±663	6599,1±678	6200,8±841	6400±697
4	2190,4±364	2022,6±381	2052,4±395	1663,1±222	1797,6±347
5	1035,7±33	828,8±48	857,5±40	866±47	837,8±47
6	828,6±25	823,1±24	820±34	818,6±15	815,6±24
7	837,5±26	821,7±22	824,4±24	821,7±20	817,2±20
8	849,5±33	810,2±12	830,8±21	834±19	815,8±15
9	810,2±13	815,7±25	825,7±19	806,6±13	815,5±15
10	808,6±8	819,3±21	836,6±27	813,5±18	810±17

В то же время из представленных результатов следует, что значение показателя нелинейности S-блоков не является определяющим. Для S-блоков с одной и той же нелинейностью результаты перехода к асимптотическому значению отличаются на один-два цикла.

В работе [16] рассматриваются корреляции случайных блочных шифров $\mathcal{A}$ (блочных шифров с битовой длиной n и ключевой длиной h , являющихся массивом из 2^h векторных булевых подстановок, оперирующих с n битными векторами). Каждое ключевое значение k определяет векторную булеву подстановку, обозначенную как $\mathcal{A}[k]$. Такой шифр рассматривается как *фиксированно-ключевой (блочный) шифр*. Случайный блочный шифр с блочной длиной n и ключевой длиной h является массивом из 2^h n -битных случайных подстановок: одна случайная n -битная подстановка для каждого ключевого значения.

Таблица 5

Математическое ожидание максимальных смещений линейных корпусов шифра мини-Rijndael со значениями среднеквадратического отклонения для S-блоков с различными показателями нелинейности.

Число циклов шифрования r	Показатели нелинейности S-блоков, использованных в шифре				
	0	2	0	2	4
1	32768±0	24576±0	32768±0	24576±0	16384±0
2	24576±0	7808±0	10368±0	3584±0	2048±0
3	12288±0	2527,1±54	2304±0	1128±107	851,5±48
4	5233,1±58	891,7±58	905,7±29	829,3±22	814,2±14
5	2040,2±103	822,6±24	831,3±29	817,7±11	828,6±20
6	1077,7±35	825,3±19	832,2±21	820,8±23	827,7±31
7	839,7±34	815,7±16	826,4±21	822,6±27	822,2±28
8	821,7±11	810,8±21	822,8±20	819,3±26	803,7±12
9	830±26	811,1±15	821,7±34	830,4±27	810,4±18
10	811,3±18	834,4±29	806,6±11	808,4±14	823,1±27

Эквивалентно, случайный блочный шифр с блочной длиной n и ключевой длиной h является блочным шифром, выбранным случайно из множества $(2^n!)^{2^h}$ возможных блочных шифров той же размерности, где каждый блочный шифр имеет равную вероятность быть выбранным.

Интересно отметить, что в этой работе доказывается теорема о том, что распределение среднего значения LP линейного корпуса над случайным блочным шифром очень близко к нормальному распределению со средним значением 2^{-n} и стандартным отклонением $2^{-n} 2^{(1-h)/2}$. В табл. 6 приведены данные (и оценки), характеризующие временные затраты на проведение вычислительных экспериментов по определению линейных показателей уменьшенных моделей шифров при использовании базового и ускоренного алгоритмов.

Таблица 6

Время построения ЛАТ

Алгоритм	T_1 строки	T_1 таблицы	T_{10} циклов	T_{30} ключей
Базовый	2,5 мин (2^{32} операций)	272 ч (2^{48} операций)	113 д (2^{51} операций)	3390 дней (2^{56} операций)
Ускоренный	—	2,5 мин (2^{32} операций)	25 мин (2^{35} операций)	12,5 ч (2^{40} операций)

Приведенные результаты свидетельствуют, что концепция оценки доказуемой стойкости, развиваемая в приведенных во введении и многих других работах, ошибочна! Во всех рассмотренных примерах показатели стойкости шифров не зависят от подстановок, использованных при их построении, а зависят только от битового размера входа в шифр. Подстановки влияют лишь на динамику перехода к асимптотическому значению. Этот результат, следующий из большого числа экспериментов со случайными подстановками и малыми моделями шифров, будет сохраняться и для больших версий шифров (и не только для шифров с SPN структурой!).

Заключение

Общий вывод состоит в том, что итоговые асимптотические показатели стойкости шифров к атакам линейного криптоанализа определяются свойствами случайной подстановки соответствующей степени и от свойств S-блоков, используемых в шифре, не зависят. А раз так, то интересующие нас показатели доказуемой стойкости шифров к атакам теперь уже и линейного криптоанализа могут быть определены расчетным путем из соответствующих формул для теоретических законов распределения переходов XOR таблиц и смещений таблиц линейных аппроксимаций случайных подстановок соответствующей степени, полученных в работах [10, 11].

Среднее значение максимального смещения таблицы линейных аппроксимаций (линейных каркасов (оболочек)) для шифров с n -битным значением размера входного блока данных аппроксимируется соотношением $\left(\frac{3}{2}\right)^n$. Для среднего значения максимума вероятности ли-

нейного корпуса ($ALHMP$) 128-битного шифра приходим к результату $ALHMP^R$

$$= \left(\frac{\left(\frac{3}{2}\right)^{128}}{2^{127}} \right)^2 = 2^{-104}. \text{ Реальное значение может отличаться от приведенного, по нашим пред-}$$

положениям, менее чем в два раза.

Исследованиями установлено, что все рассмотренные шифры после 4 – 5 циклов шифрования становятся случайными подстановками.

Полученными результатами подтверждается концепция оценки стойкости БСШ, развиваемая на кафедре БИТ ХНУРЭ, в соответствии с которой показатели стойкости БСШ к атакам линейного и дифференциального криптоанализа могут быть получены расчетным путем с использованием значений максимумов XOR таблиц и смещений таблиц линейных аппроксимаций случайных подстановок соответствующей степени.

В отношении сохранения в большом шифре свойств уменьшенной модели можно лишь отметить, что мы говорим о сохранении свойств и показателей случайной подстановки. Представляется, что при увеличении битового размера входа в шифр (с увеличением степени подстановки) ее соответствие асимптотическим законам распределения вероятностей (по инверсиям, возрастаниям и циклам), а также законам распределения вероятностей переходов таблиц полных дифференциалов и таблиц линейных корпусов будет только повышаться, что подтверждается и вычислительными экспериментами с большими версиями шифров.

Список литературы: 1. Горбенко И.Д. Новая идеология оценки стойкости блочных симметричных шифров к атакам дифференциального и линейного криптоанализа / Горбенко И.Д., Долгов В.И., Лисицкая И.В., Олейников Р.В. // Прикладная радиоэлектроника. – 2010. – Т. 9, № 3. – С. 212-320. 2. Лисицкая И.В. Об участии S-блоков в формировании максимальных значений дифференциальных вероятностей блочных симметричных шифров / Лисицкая И.В., Казимиров А.В. // System Research and Information Technologies. – 2011 (в печати). 3. Долгов В.И. Подход к криптоанализу современных шифров / Долгов В.И., Лисицкая И.В., Олейников Р.В. // Материалы второй междунар. конф. "Современные информационные системы. Проблемы и тенденции развития". – Харьков-Туапсе, Украина, 2–5 октября. – 2007. – С. 435-436. 4. Долгов В.И. Дифференциальные свойства блочных симметричных шифров, представленных на украинский конкурс / Долгов В.И., Кузнецов А.А., Исаев С.А. // Представлена к опубликованию. 5. Lysytska I.V. The selection criteria of random substitution tables for symmetric enciphering algorithms / Lysytska I.V., Koriak A.S., Golovashich S.A., Olesheko O.I., Oleinik R.V // Abstracts of XXVIth General Assembly. Toronto, Ontario Canada, August 13-21. 1999. – P. 204. 6. Олейников Р.В. Дифференциальные свойства подстановок / Олейников Р.В., Олешко О.И., Лисицкий К.Е.,

Тевяшев А.Д. // Прикладная радиоэлектроника. – 2010. – Т.9. – № 3. – С. 326–333. 7. Долгов В.И. Свойства таблиц линейных аппроксимаций случайных подстановок / Долгов В.И., Лисицкая И.В., Олешко О.И. // Прикладная радиоэлектроника. – 2010. – Т.9. – № 3. – С. 334–340. 8. Долгов В.И. Случайные подстановки в криптографии / Долгов В.И., Лисицкая И.В., Лисицкий К.Е. // Радіоелектронні та комп'ютерні системи. – 2010. – № 5 (46). – С. 79–84. 9. Долгов В.И. Исследование дифференциальных свойств мини-шифров Baby-ADE и Baby-AES / Долгов В.И., Кузнецов А.А., Сергиенко Р.В., Олешко О.И. // Прикладная радиоэлектроника. – 2009. – Т.8, № 3 – С. 252–257. 10. Долгов В.И. Мини-версия блочного симметричного алгоритма криптографического преобразования информации с динамически управляемыми криптопримитивами (Baby-ADE) / Долгов В.И., Кузнецов А.А., Сергиенко Р.В., Белоковаленко А.Л. // Прикладная радиоэлектроника. – 2008. – Т.7 – № 3. – С. 215–224. 11. Долгов В.И. Криптографические свойства уменьшенной версии шифра "Калина" / Долгов В.И., Олейников Р.В., Большаков А.Ю., Григорьев А.В., Дробатько Е.В. // Прикладная радиоэлектроника. – 2010. – Т.9. – № 3. – С. 349–354. 12. Долгов В.И. Исследование циклических и дифференциальных свойств уменьшенной модели шифра Лабиринт / Долгов В.И., Лисицкая И.В., Григорьев А.В., Широков А.В. // Прикладная радиоэлектроника. – Харьков : ХТУРЭ. – 2009. – Т. 8 – № 3. – С. 283–295. 13. Лисицкая И.В. Большие шифры – случайные подстановки. / Лисицкая И.В., Настенко А. // Прикладная радиоэлектроника. – 2011. (в печати). 14. Лисицкая И.В. Дифференциальные свойства шифра FOX / Лисицкая И.В., Кайдалов Д. // Прикладная радиоэлектроника. – 2011. (в печати). 15. F. Sano, K. Ohkuma, H. Shimizu, S. Kawamura. On the Security of Nested SPN Cipher against the Differential and Linear Cryptanalysis/ IEICE Trans. Fundamentals, vol. E86-a, NO.1 January 2003, pp. 37–46. 16. Joan Daemen, Vincent Rijmen Probability distributions of Correlation and Differentials in Block Ciphers./ Joan Daemen, Vincent Rijmen // April 13, 2006. 17. J. Seberry, X. S. Zhang and Y. Zheng. Relationships among nonlinearity criteria. Presented at EUROCRYPT-94. 1994. 18. M.D. Yücel IAM501-Introduction to Cryptography. Institute of Applied Mathematics METU, Ankara, Turkey (9700501). 2002, p. 1–28. 19. W. Saier, O. Staffelbach. Nonlinearity criteria for cryptographic functions. In Advances in Cryptology – EUROCRYPT'89, vol.434. Lecture Notes in Computer Science. Springer-Verlag, pp.549–562, 1990. 20. M. Matsui, "The First Experimental Cryptanalysis of the Data Encryption Standard", Advances in Cryptology – CRYPTO' 94. Lectures in Computer Science no.839, Springer-Verlag, pp. 1–11, 1994.

Харьковский национальный
университет радиоэлектроники

Поступила в редколлегию 05.08.2011

КАСКАДНОЕ УНИВЕРСАЛЬНОЕ ХЕШИРОВАНИЕ ПО РАЦИОНАЛЬНЫМ ФУНКЦИЯМ АЛГЕБРАИЧЕСКИХ КРИВЫХ

Универсальные семейства хеш-функций являются объектами полевых структур, характеризуются прозрачными комбинаторными свойствами и имеют доказуемую секретность. Применение для аутентификации каскадного хеширования позволяет получить наименьшую вероятность коллизии, сложность вычислений хешей для фиксированного объема хешируемых данных и размерности конечного поля. Основные результаты представлены в работах [1 – 5]. В работе [1] показано, что вероятность коллизии можно эффективно уменьшить путем хеширования сообщений по нескольким независимо выбранным хеш-функциям. Стинсон рассмотрел композиционное хеширование со снятием ограничения на размер ключевых данных для строго универсального хеширования [2]. Букетное хеширование, допускающее параллельные алгоритмы вычислений и снимающее ограничение на сложность, предложено Рогавеем [3]. Оценки вероятности коллизии для каскадного универсального хеширования со связкой хеша предыдущего каскада с текстом последующего каскада получены в [4]. Свойства многократного универсального хеширования по проективной прямой и кривой Эрмита представлены в [5].

В данной работе предлагается метод каскадного универсального хеширования по рациональным функциям алгебраических кривых на основе произведения функциональных полей. С этой целью в разд. 1 рассмотрено каскадное универсальное хеширование по рациональным функциям алгебраических кривых со связкой хеша предыдущего каскада с текстом последующего. В разд. 2 представлено многократное универсальное хеширование на основе произведения функциональных полей алгебраических кривых.

1. Каскадное универсальное хеширование со связкой хеша с текстом

Для универсального хеширования по рациональным функциям алгебраических кривых определение каскадного хеширования со связкой по хешу и тексту имеет следующее определение.

Определение 1 [4]. Пусть F_q – конечное поле, M – сообщение и $M = M_1 \parallel M_2$. Каскадное универсальное хеширование по рациональным функциям алгебраических кривых определяется выражением

$$Ch(M) = AGh_2(AGh_1(M_1) \parallel M_2), \quad (1)$$

где AGh_1 , AGh_2 – универсальные схемы хеширования по рациональным функциям алгебраических кривых, $Ch(M)$ определяет универсальное семейство хеш функций $\varepsilon - AU$, где $\varepsilon = \max(\varepsilon_1, \varepsilon_2) + 1/|H^2|$, $\varepsilon_1, \varepsilon_2$ – соответственно вероятности коллизий для AGh_1 и AGh_2 хеширования.

Коллизионные свойства каскадной конструкции определяются утверждениями 1.2.

Утверждение 1 [4]. Если H_1 есть $\varepsilon_1 - U$ универсальный класс и H_2 есть $\varepsilon_2 - U$, тогда $H = H_1 H_2$ есть $\varepsilon - U$, где $\varepsilon = \max(\varepsilon_1, \varepsilon_2) + 1/|H^2|$.

Утверждение 2 [4]. Пусть H_1 и H_2 соответственно $\varepsilon_1 - U$ и $\varepsilon_2 - U$ универсальные классы хеш функций. Каскадная конструкция $H_1 H_2$ имеет наименьшую вероятность коллизии, если $\varepsilon_1 = \varepsilon_2$.

Замечание 1.

1. Каскадное хеширование определяется тем, что хеш предыдущего каскада связывается с текстом следующего каскада через конкатенацию.

2. Каскадное хеширование $Ch(M)$ при фиксированном поле вычислений предполагает разбиение данных на блоки приблизительно равной длины. Для двух каскадного универсального хеширования по проективной прямой вероятность коллизии уменьшится только в два раза, так как вероятность коллизии зависит пропорционально от значения длины данных. Для хеширования по максимальным кривым эта зависимость определяется как корень квадратный от длины сообщения и вероятность коллизии уменьшится только в $\sqrt{2}$ раз.

3. Вероятность коллизии каскадного хеширования имеет ограничение по наименьшему полю вычисления хеша одного из каскадов.

4. Размер ключевых данных увеличивается пропорционально числу каскадов, с учетом поля вычисления и универсального хеширования каскада.

5. Каскадное хеширование позволяет эффективно увеличить общую длину хешируемых данных и зафиксировать вероятность коллизии на уровне хеша первого каскада, если на втором и последующих каскадах увеличить поле вычислений. Примером является алгоритм хеширования UMAC(2000), каскадная схема применяется с подъёмом поля вычисления, сначала 32 бита, затем 64 бита и 128 бит.

Рассмотрим свойства каскадного хеширования без увеличения размера поля вычисления на примере двух каскадного хеширования по функциональному полю кривой Эрмита и проективной прямой.

Определение 2 [4]. Пусть F_q , $q = p^2$ – расширенное конечное поле, M – сообщение и $M = M_1 \parallel M_2$. Алгоритм вычисления хеша кода в каскадной конструкции определяется выражением

$$Ch(M) = Hh_q(PSh_q(M_1) \parallel M_2),$$

где Hh_q, PSh_q – универсальные схемы хеширования по кривой Эрмита и проективной прямой.

Свойства двух каскадного хеширования по кривой Эрмита и проективной прямой рассмотрены в [4].

Утверждение 3 [4]. Пусть F_q , $q = p^2$ – расширенное конечное поле, $M = M_1 \parallel M_2$, $|M_1| \leq \sqrt{q} + 1$, $|M_2| \leq q\sqrt{q}$, $0 < k \leq q\sqrt{q} + \sqrt{q}$. Тогда $Ch_q(M)$ определяет универсальное семейство хеш функций $\varepsilon - U(q^2\sqrt{q}, q^k, q)$, $\varepsilon = \max(\varepsilon_{PS}, \varepsilon_H) + 1/|q\sqrt{q}|$, $\varepsilon_{PS}, \varepsilon_H$ – соответственно, вероятности коллизий для PSh_q и Hh_q хеширования.

Замечание 2.

1. Для $Ch_q(M) = Hh_q(PSh_q(M_1) \parallel M_2)$ хеширования является справедливым утверждение 2. Вероятность коллизии будет минимальной, если $\varepsilon_H = \varepsilon_{PS}$.

2. Применение во внутреннем каскаде PSh_q хеширования дает преимущество в скорости вычислений, так как PSh_q хеширование определено над простым полем. Практический алгоритм вычислений может учитывать эту особенность. Для малых длин данных используется только PSh_q хеширование и при превышении длины подключается Hh_q хеширование.

3. Ключевое пространство увеличивается в q раз, вероятность коллизии фиксируется на уровне $\varepsilon_H = \varepsilon_{PS} = \sqrt{2k'}/q$, где k' определяется уравнением $k'^2 + k' = k$, k – число слов сообщения.

4. Каскадирование $Hh_q(PSh_q(M_1) \parallel M_2)$ приводит к небольшому увеличению размера хешируемых данных $k + \sqrt{k}$. Наибольшее увеличение хешируемых данных в два раза достигается, если на первом и втором каскадах используется одинаковая функция хеширования.

2. Каскадное хеширование на основе произведения функциональных полей

Дальнейшим развитием каскадного хеширования является хеширование на основе произведения функциональных полей.

Определение 3. Пусть F_q – конечное поле, M – сообщение и $M = M_1 \parallel M_2 \parallel \dots \parallel M_t$. Алгоритм вычисления хеш кода в каскадной конструкции определяется выражением

$$Ch_t(M) = AGh_2(AGh_1(M_1) \parallel AGh_1(M_2) \parallel \dots \parallel AGh_1(M_t)), \quad (2)$$

где AGh_1, AGh_2 – универсальные схемы хеширования по алгебраическим кривым, $Ch_t(M)$ определяет универсальное семейство хеш функций $\varepsilon - AU$, где $\varepsilon = \max(\varepsilon_1, \varepsilon_2) + 1/\lceil H^2 \rceil$, $\varepsilon_1, \varepsilon_2$ – соответственно, вероятности коллизий для AGh_1 и AGh_2 хеширования.

Замечание 3.

1. Коллизионные свойства каскадного хеширования следуют из утверждения 1.

2. Каскадное хеширование $Ch_t(M)$ при фиксированном поле вычислений предполагает разбиение данных на t блоков равной длины. Для первого каскада вероятность коллизии определяется размером блока данных, для второго – значением t .

3. Вероятность коллизии каскадного хеширования имеет ограничение по наименьшему полю вычисления хеша одного из каскадов.

4. Размер ключевых данных определяется произведением пространства ключей первого и второго каскадов, с учетом поля вычисления и универсального хеширования каскада.

5. Каскадное хеширование $Ch_t(M)$ позволяет эффективно увеличить общую длину хешируемых данных и зафиксировать вероятность коллизии на уровне хеша одного из каскадов.

6. Двух каскадная конструкция $Ch_t(M)$ легко распространяется на многокаскадную $l - Ch_t(M)$, где l – число вложенных каскадов универсальных схем хеширования по алгебраическим кривым $AGh_1, AGh_2, \dots, AGh_l$.

Рассмотрим свойства каскадного хеширования $Ch_t(M)$ на примере двух каскадного хеширования по функциональному полю кривой Эрмита и проективной прямой.

Определение 4. Пусть $F_q, q = p^2$ – расширенное конечное поле, M – сообщение и $M = M_1 \parallel M_2 \parallel \dots \parallel M_t$. Алгоритм вычисления хеш кода в каскадной конструкции определяется выражением

$$Ch_t(M) = Hh_q(PSh_q(M_1) \parallel PSh_q(M_2) \parallel \dots \parallel PSh_q(M_t)). \quad (3)$$

где Hh_q, PSh_q – универсальные схемы хеширования по кривой Эрмита и проективной прямой.

Утверждение 4. Пусть $F_q, q = p^2$ – расширенное конечное поле, M – сообщение и $M = M_1 \parallel M_2 \parallel \dots \parallel M_t$. $Ch_t(M)$ – хеширование (3). Тогда $Ch_t(M)$ определяет универсальное семейство хеш функций $\varepsilon - U(q^2\sqrt{q}, q^k, q)$, $\varepsilon = (2k)^{1/3}/q, 0 < k \leq q\sqrt{q}/2$.

Доказательство. Хеширование на каждом каскаде является универсальным и каскадная хеш функция также является универсальной. Пространство ключей определяется произведе-

нием числа ключей первого и второго каскадов и равно $q^2\sqrt{q}$. Пусть k число слов данных и k' – размер блока данных, $t = k/k'$. Наименьшая вероятность коллизии в силу утверждения 2 реализуется в случае $\varepsilon_H = \varepsilon_{PS}$. Подставим в выражения для ε_H и ε_{PS} значения k' и $t = k/k'$, получим $k' = (2k)^{1/3}$ и оценку для вероятности $\varepsilon = (2k)^{1/3}/q$. Так как ε имеет оценку сверху $\varepsilon \leq 1/\sqrt{q}$, для $k' \leq g$ получим $k \leq q\sqrt{q}/2$, где g – род кривой Эрмита.

Замечание 4.

1. Каскадное хеширование по кривой Эрмита и проективной прямой $PSh_q - Hh_q$ имеет вероятность коллизии $\varepsilon = (2k)^{1/3}/q$, что совпадает с хешированием по кривой Сузуки $\varepsilon = 3k^{1/3}/q$ (см. [6]). Затраты по ключу несколько больше – $q^2\sqrt{q}$, в отличие от q^2 – для кривой Сузуки.

2. Вычисления в каскадном хешировании существенно проще. Вычисления по PSh_q каскаду выполняются на одной рациональной функции со сложностью $\sim k'$ и по Hh_q каскаду на двух рациональных функциях – со сложностью $\sim t + \sqrt{t}$. С учетом $t = k/k'$ и $k' = (2k)^{1/3}$ получим оценку для числа вычислений $k + t + \sqrt{t} = k + k^{2/3}/2^{1/3} + k^{1/3}/2^{1/6}$, что меньше почти в два раза числа вычислений по кривой Сузуки на четырёх рациональных функциях – $2k + 1.04k^{2/3} + 2\sqrt[3]{3}k^{1/3}$.

Возможны комбинации других универсальных хеш функций в двух каскадной схеме хеширования. Свойства каскадирования с кривой Ферма представлены утверждением 5.

Утверждение 5. Пусть F_q – конечное поле, M – сообщение и $M = M_1 \# M_2 \# \dots \# M_l$, $Ch_t(M)$ – хеширование вида (1), где $AGh_1 = PSh_q$, $AGh_2 = Fh_q$ – универсальные схемы хеширования по проективной прямой и кривой Ферма $x^{(q-1)/3} + y^{(q-1)/3} + 1 = 0$ соответственно. Тогда $Ch_t(M)$ определяет универсальное семейство хеш функций $\varepsilon = U(q^3, q^k, q)$, $\varepsilon = (9k/2)^{1/3}/q$, $0 < k \leq q\sqrt{q}$.

Замечание 5. Доказательство подобно доказательству утверждения 4. Результаты каскадного хеширования $PSh_q - Fh_q$ совпадают по вероятности коллизии с хешированием $PSh_q - Hh_q$, но требуют больший размер ключа, соответственно q^3 и $q^2\sqrt{q}$.

Оценки многокаскадного универсального хеширования $l - Ch_t(M)$ по рациональным функциям алгебраических кривых представлены утверждениями 6-8.

Утверждение 6. Пусть F_q – конечное поле, $M = M_1 \# M_2 \# \dots \# M_l$ и $l - Ch_t(M)$ – l -каскадное универсальное хеширование по проективной прямой. Тогда $l - Ch_t(M)$ определяет универсальное семейство хеш функций $\varepsilon = U(q^l, q^k, q)$, $\varepsilon = k^{1/l}/q$, $0 < k \leq q^l$, со сложностью вычислений $k + k^{l-1/l} + k^{l-2/l} + \dots + k^{1/l}$.

Доказательство. Хеширование на каждом каскаде является универсальным и каскадная хеш функция, также является универсальной. Пространство ключей определяется произведением числа ключей всех каскадов и равно q^l . Наименьшая вероятность коллизии в силу утверждения 2 реализуется, если на каждом каскаде значение вероятности коллизии является наименьшим. Это достигается, если размер данных хеширования k' на каждом каскаде является наименьшим $k' = k^{1/l}$. Подставим в выражения для ε_{PS} значения k' получим

$\varepsilon = k^{1/l} / q$ и оценку для $0 < k \leq q^l$. Оценка сложности вычислений определяется тем, что на каждом каскаде число вычислений уменьшается в $k' = k^{1/l}$. Суммирование по всем каскадам дает результирующее выражение $k + k^{l-1/l} + k^{l-2/l} + \dots + k^{1/l}$.

Утверждение 7. Пусть $F_q, q = p^2$ – расширенное конечное поле, M – сообщение и $M = M_1 \parallel M_2 \parallel \dots \parallel M_l, l - Ch_l(M)$ – l -каскадное универсальное хеширование по кривой Эрмита. Тогда $l - Ch_l(M)$ определяет универсальное семейство хеш функций $\varepsilon - U(q^{l+1/2}, q^k, q), \varepsilon = \sqrt{2k^{1/l}} / q, 0 < k \leq q^l$, со сложностью вычислений $k + k^{(2l-1)/2l} + k^{l-1/l} + k^{(2l-3)/2l} + \dots + k^{1/l} + k^{1/2l}$.

Доказательство аналогично утверждению 6.

Утверждение 8. Пусть $F_q, q = p^2$ – расширенное конечное поле, M – сообщение и $M = M_1 \parallel M_2 \parallel \dots \parallel M_l, l - Ch_l(M)$ – l -каскадное универсальное хеширование по кривой Ферма $x^{(q-1)/3} + y^{(q-1)/3} + 1 = 0$ с большим числом точек. Тогда $l - Ch_l(M)$ определяет универсальное семейство хеш функций $\varepsilon - U(q^{2l}, q^k, q), \varepsilon = 3\sqrt{k^{1/l}} / (\sqrt{2}q), 0 < k \leq q^l$, со сложностью вычислений $k + k^{(2l-1)/2l} + k^{l-1/l} + k^{(2l-3)/2l} + \dots + k^{1/l} + k^{1/2l}$.

Доказательство аналогично утверждению 6.

Параметры многокаскадного универсального хеширования по алгебраическим кривым: представлены в таблице.

Схемы каскадного хеширования	Параметры универсального хеширования	Оценки сложности вычислений
$Ch_l(M),$ $PSh_q - PSh_q$	$\varepsilon - U(q^2, q^k, q), \varepsilon = k^{1/2} / q,$ $0 < k \leq q^2$	$k + k^{1/2}$
$Ch_l(M),$ $PSh_q - Hh_q$	$\varepsilon - U(q^2 \sqrt{q}, q^k, q),$ $\varepsilon = (2k)^{1/3} / q, 0 < k \leq q\sqrt{q} / 2$	$k + k^{2/3} / 2^{1/3} + k^{1/3} / 2^{1/6}$
$Ch_l(M),$ $PSh_q - Fh_q$	$\varepsilon - U(q^3, q^k, q),$ $\varepsilon = (9k/2)^{1/3} / q, 0 < k \leq q\sqrt{q}$	$k + k^{2/3} / 2^{1/3} + k^{1/3} / 2^{1/6}$
$l - Ch_l(M),$ $PSh_q - PSh_q - \dots$	$\varepsilon - U(q^l, q^k, q), \varepsilon = k^{1/l} / q,$ $0 < k \leq q^l$	$k + k^{l-1/l} + k^{l-2/l} + \dots + k^{1/l}$
$l - Ch_l(M),$ $Hh_q - Hh_q - \dots$	$\varepsilon - U(q^{l+1/2}, q^k, q),$ $\varepsilon = \sqrt{2k^{1/l}} / q, 0 < k \leq q^l$	$k + k^{(2l-1)/2l} + k^{l-1/l} + k^{(2l-3)/2l} + \dots$ $+ k^{1/l} + k^{1/2l}$
$l - Ch_l(M),$ $Fh_q - Fh_q - \dots$	$\varepsilon - U(q^{2l}, q^k, q),$ $\varepsilon = 3\sqrt{k^{1/l}} / (\sqrt{2}q), 0 < k \leq q^l$	$k + k^{(2l-1)/2l} + k^{l-1/l} + k^{(2l-3)/2l} + \dots$ $+ k^{1/l} + k^{1/2l}$

Выводы

1. Каскадное хеширование эффективно увеличивает размер хешируемых данных и выравнивает вероятность коллизии с изменением длины данных.

2. Применение многокаскадного универсального хеширование $l - Ch_l(M)$ с одной и той же функцией хеширования на всех каскадах в $\sqrt[l]{k}$ раз уменьшает вероятность коллизии.

Наименьшая вероятность коллизии реализуется в схеме $Hh_q - Hh_q$. Вычисления в поле ~ 64 бит обеспечивает доказуемую стойкость $P_{\text{кол}} < 2^{-57}$ для данных длиной до нескольких Гбт. Затраты по ключам в схеме $Hh_q - Hh_q$ являются наименьшими 124 бит.

3. Каскадное хеширование $PSh_q - PSh_q$ по вероятности коллизии совпадает с однокаскадным хешированием по максимальным плоским кривым и кривой Ферма или Гурвица с большим числом точек и несколько проигрывает $Hh_q - Hh_q$ хешированию. По числу вычислений $PSh_q - PSh_q$ хеширование совпадает с хешированием Hh_q и Fh_q . Преимуществом по сравнению с хешированием по кривой Эрмита являются вычисления в простом поле, в отличие от вычислений в квадратичном поле для Hh_q . Затраты по ключам совпадают с затратами на Fh_q хешированием и определяются значением квадрата поля вычисления.

4. Двухкаскадные схемы хеширования $PSh_q - Hh_q$, $PSh_q - Fh_q$, по вероятности, коллизии являются эквивалентными. Чуть проигрывает хеширование $PSh_q - Fh_q$ и с увеличением размерности поля отличие от $PSh_q - Hh_q$ хеширования становится меньше. Хеширование $PSh_q - Hh_q$ имеет наименьшие затраты по ключам и наименьшую сложность вычислений, для первого каскада в простом поле по одной рациональной функции и по второму каскаду в квадратичном поле по двум рациональным функциям. Затраты по ключам в корень квадратный от размерности поля вычислений больше по сравнению с однокаскадным Fh_q хешированием по кривой Ферма.

Список литературы: 1. Wegman M. N. New hash functions and their use in authentication and set equality // Wegman M. N., Carter J. L. // J. Computer and System Science. – 1981. – V. 22. – P. 265-279. 2. Stinson D. Universal hashing and authentication codes / Stinson D. // Design, Codes and Cryptography. – 1994. – V. 4. – P.369-380. 3. Rogaway P. Bucket hashing and its application to fast message authentication / Rogaway P. // rogaway.cs.ucdavis.edu. 4. Халимов Г.З. Каскадное универсальное хеширование с использованием АГК кодов / Халимов Г.З., Нохов А.Ю. // Восточно-европейский журнал передовых технологий. – Х., 2005. – Вып. 2/2(14). – С. 111–119. 5. Халимов Г.З. Багатократне універсальне хешування // Халимов Г.З. // Спеціальні телекомунікаційні системи та захист інформації : Зб. наук. праць. – Київ : ДССЗ та ЗІ. – 2010. – Вип. 2(18). – С.43-49. 6. Халимов Г.З. Универсальное хеширование по кривой Сузуки / Г.З. Халимов, Е.В. Котух // Прикладная радиоэлектроника. – Харьков : ХНУРЭ. – 2011. – Т.10, № 2. – С.80-86.

Харьковский национальный
университет радиозлектроники

Поступила в редколлегию 15.08.2011

СХЕМА ХАМЕЛЕОН-ПІДПISУ НА ОСНОВІ ДСТУ 4145-2002**Вступ**

Стрімкий розвиток систем, що пов'язані з електронною комерцією (наприклад, інтернет-аукціони або системи закритого електронного голосування), призвів до необхідності додаткових послуг безпеки. Окрім традиційних послуг цілісності та неспростовності, які забезпечує звичайний механізм електронного цифрового підпису (ЕЦП), виникла необхідність забезпечення послуг приватності. За приватністю у даному контексті слід розуміти непередаваність ЕЦП та прихованість підписаного повідомлення. Непередаваність ЕЦП – неможливість доведення валідності ЕЦП будь-якій третій стороні без участі підписувача. Прихованість повідомлення – відсутність необхідності розкриття підписувачем змісту підписаного повідомлення у ході виникнення можливих протиріч. Ці послуги забезпечує механізм хамелеон-підпису, який представляє собою довільний базовий алгоритм ЕЦП із застосуванням геш-функції спеціального виду – функції геш-хамелеону.

Як відомо, у якості легітимної системи ЕЦП в Україні працює інфраструктура відкритих ключів, що використовує у якості стандарту ЕЦП – ДСТУ 4145-2002. Метою наших досліджень є розробка алгоритму ЕЦП, що, з однієї сторони, зміг би забезпечити необхідні послуги, а з іншої – не суперечив би діючим нормативним документам і мав би використовуватися в існуючій інфраструктурі відкритих ключів. У статті пропонується механізм хамелеон-підпису на основі ДСТУ 4145-2002, що задовольняє висунутим вимогам.

1. Історичний аналіз розвитку хамелеон-підписів

Механізм хамелеон-підпису, що вперше був представлений у роботі Кравчука та Рабіна [1], базується на звичній парадигмі геш-та-підпис, де функція геш-хамелеону використовується для обчислення криптографічного дайджесту повідомлення. Функція геш-хамелеону представляє собою односторонню геш-функцію, яка не дозволяє нікому, окрім власника інформації про лазівку, обчислити колізію для випадково обраних вхідних даних. Хамелеон-підпис є неінтерактивним, тобто підписувач може згенерувати хамелеон-підпис без попереднього зв'язку з визначеним одержувачем, і одержувач, в свою чергу, може перевірити валідність підпису без взаємодії з підписувачем. З іншої сторони, якщо створено підроблений підпис, підписувач може заперечувати його дійсність шляхом відкриття деяких значень, але не змісту повідомлення (прихованість повідомлення). Протокол спростування підробленого підпису також є неінтерактивним. Суттєвим обмеженням оригінального алгоритму хамелеон-підпису є те, що результатом підробки підпису є знаходження підписувачем інформації про лазівку, якою володіє одержувач, тобто його секретного ключа [2]. Підписувач може використати цю інформацію з метою заперечення валідності інших підписів, які він раніше підписував для цього одержувача. У гіршому випадку підписувач має можливість зв'язатися із зловмисною метою з іншими учасниками інформаційного обміну для заперечення валідності інших підписів, що перевіряються однаковим відкритим ключем. Хоча це стримує одержувача від підробки ЕЦП, у багатьох застосуваннях таке обмеження є неприпустимим. Пізніше ця проблема отримала назву проблеми витоку ключа. Атеніс та Медейрос [2] вперше запропонували вирішення проблеми витоку ключа шляхом застосування криптографії, що базується на ідентифікаторах. Тепер підписувач зміг підписувати повідомлення визначеному одержувачу без попереднього запиту його сертифіката відкритого ключа (СВК). Більш того, підписувач використовує різні відкриті ключі (пов'язані з різними секретними ключами) для кожної транзакції з одержувачем. Таким чином, результатом створення підробленого підпису може бути лише відкрита підписувачем інформація про лазівку, пов'язана з конкретною транзакцією. Але ця схема не отримала широкого застосування, адже разом з вирішенням проблеми витоку ключа виникла проблема розповсюдження дуже великої кількості ключів (для кожної транзакції свій відкритий, а отже і секретний ключ), вирішення якої, як відомо, є складною задачею.

У роботі Чена [3] вперше з'явилася ідея створення геш-хамелеона, вільного від проблеми витoku ключа, що заснована на використанні гап-груп Діффі-Гелмана (GDH groups – Gap Diffi-Helman groups) з білінійними спарюваннями. Потім Атеніс і Медейрос [4] представили три схеми хамелеон-підписів, вільні від проблеми витoku ключа, дві з яких засновані на припущеннях RSA (вперше схеми не застосовували спарювання), а третя – на спарюваннях. Пізніше Гао [5] представив схему хамелеон-підпису, вільну від проблеми витoku ключа, що базувалася на схемі підпису Шнора. Однак вона потребувала інтерактивного зв'язку між підписувачем і одержувачем, що підривало концепцію неінтерактивності хамелеон-підпису.

Усі існуючі схеми геш-хамелеонів, що базувалися на складності вирішення задачі дискретного логарифму, могли бути реалізовані лише у GDH групах. У роботах Чена [3, 7] вперше було представлено схему хамелеон-підпису, вільну від проблеми витoku ключа, без використання GDH груп. Нами обрана саме ця схема для створення хамелеон-підпису на основі ДСТУ 4145-2002, вільного від проблеми витoku ключа.

2. Аналіз властивостей хамелеон-підпису на основі ДСТУ 4145-2002

2.1. Опис схеми хамелеон-підпису на основі ДСТУ 4145-2002

Схема формування хамелеон-підпису (рис.1) на основі ДСТУ 4145-2002 [6] складається з таких етапів:

- обчислення загальних параметрів хамелеон-підпису;
- обчислення одержувачем відкритого та секретного ключів функції геш-хамелеону, після чого відкритий ключ геш-хамелеону передається підписувачу для обчислення функції геш-хамелеону;
- ДСТУ 4145-2002, після чого відкритий ключ підпису передається одержувачу підписаного повідомлення;
- обчислення цифрового передпідпису згідно ДСТУ 4145-2002;
- обчислення базової функції гешування згідно ГОСТ 34.311-95;
- обчислення функції геш-хамелеону;
- формування хамелеон-підпису.

Розглянемо докладніше деякі з вищезазначених етапів.

На етапі «Обчислення загальних параметрів хамелеон-підпису» обирається еліптична крива над полем $E(F_2)$, $|E(F_2)| = n \times cof$, $\{P\} \subset E(F_2)$, $|\{P\}| = n$, де n – просте число.

На етапі «Обчислення загальних параметрів функції геш-хамелеону» обирається G – мультиплікативна група з генератором групи g простого порядку q . Визначається криптографічна функція гешування: $H_2: B \rightarrow G^*$, де $B = \{H_1(T): T \in \{0,1\}^*\}$, враховуючи, що $H_1: \{0,1\}^* \rightarrow \{0,1\}^*$ – базова функція гешування (згідно ГОСТ 34.311). Загальними параметрами функції геш-хамелеону будуть: $\{G, g, q, H_1, H_2\}$.

На етапі «Обчислення відкритого та секретного ключів функції геш-хамелеону» спочатку виконується алгоритм обчислення секретного ключа функції геш-хамелеону наступним чином: одержувач випадково генерує ціле число $x \in Z_q^*$.

Даті виконується алгоритм обчислення відкритого ключа функції геш-хамелеону наступним чином: відкритий ключ обчислюється як $y = g^x$, його дійсність засвідчується включенням його до складу сертифікату відкритого ключа одержувача.

Етап «Обчислення відкритого та особистого ключів хамелеон-підпису» виконується згідно з ДСТУ 4145-2002 без будь-яких змін. Особистим та відкритим ключем відповідно будуть випадкове ціле d та точка еліптичної кривої виду $Q = -dP$, де P – базова точка еліптичної кривої, а $d \in [1, n-1]$. Даті виконується етап «Обчислення цифрового передпідпису» (згідно з ДСТУ 4145-2002 без будь-яких змін). Цифровий передпідпис позначається як (e, F_e) , де e – випадкове число, а $F_e = x_e$ та $R = eP = (x_R, y_R)$.

Вихідні дані алгоритму «Обчислення хамелеон-підпису»:

- загальні параметри хамелеон-підпису;
- особистий ключ хамелеон-підпису d ;
- відкритий ключ геш-хамелеону y .

Результат виконання алгоритму: хамелеон-підпис D повідомлення T .

Розглянемо докладніше алгоритм обчислення хамелеон-підпису (відмітимо, що етапи, пов'язані з перевіркою коректності загальних параметрів, оцінкою правильності особистого та відкритого ключів, і таке інше, здійснюються згідно з ДСТУ 4145-2002 без будь-яких змін):

1. Від повідомлення T обчислюється результат базової функції гешування H_1 .
2. Обирається випадкове число $a \in Z_q^*$.
3. Обчислюється g^a .
4. Обчислюється $h = H_2(y \| I)$, де $I = ID_S \| ID_R \| ID_T$ – загальний ідентифікатор, ID_S – ідентифікатор підписувача, ID_R – ідентифікатор одержувача, ID_T – ідентифікатор транзакції.
5. За результатом обчислення базової функції гешування H_1 обчислюється значення функції геш-хамелеону $h_{ch} = H_{ch}(H_1(T), g^a, h) = g^a h^{H_1(T)}$, де $H_{ch} : B \times Z_q^* \times Z_q^* \rightarrow Z_q^*$.
6. Результат обчислення функції геш-хамелеону h_{ch} перетворюється в елемент базового поля $\bar{h}_{ch}$.
7. Обчислюється передпідпис (e, F_e) .
8. Обчислюється елемент базового поля $t = \bar{h}_{ch} + F_e$.
9. Елемент базового поля t перетворюється на ціле число r .
10. Обчислюється ціле число $s = (e + dr) \bmod n$.
11. Значення хамелеон-підпису визначається як $D = (T, g^a, y^e, r, s)$.

Відмітимо, що етапи 6-10 виконуються згідно з ДСТУ 4145-2002 без будь-яких змін.

Запропонований алгоритм хамелеон-підпису на основі ДСТУ 4145-2002 забезпечує властивості, що представлені у табл. 1.

Таблиця 1

Властивість	Опис властивості
Неінтерактивність	Відсутність необхідності зі сторони як підписувача так і одержувача зв'язуватися між собою перед початком формування або перевірки підпису
Неможливість підробки	Неможливість створення валідного ЕЦП будь-ким та одержувачем до генерації його підписувачем
Неспростовність	Неможливість підписувачем у подальшому відмовитись від факту вироблення ЕЦП. Формально це означає, що підписувач не здатен сформувати колізію відносно функції геш-хамелеону
Реверсивність (відновлення повідомлення)	Можливість використання хамелеон-підпису у якості стандартного ЕЦП із додатком (при необхідності). Під стандартним ЕЦП із додатком вважається ЕЦП ДСТУ 4145-2002
Непередаваність ЕЦП	Неможливість доведення одержувачем справжності ЕЦП будь-якій третій стороні без участі підписувача
Прихованість повідомлення	Відсутність необхідності розкриття підписувачем змісту повідомлення будь-якій третій стороні при вирішенні можливих протиріч
Відсутність витоку особистого ключа геш-хамелеону	Неможливість отримання або обчислення підписувачем особистого ключа геш-хамелеону одержувача у разі виникнення протиріччя та, як наслідок, спростування у подальшому повідомлень, що були підписані

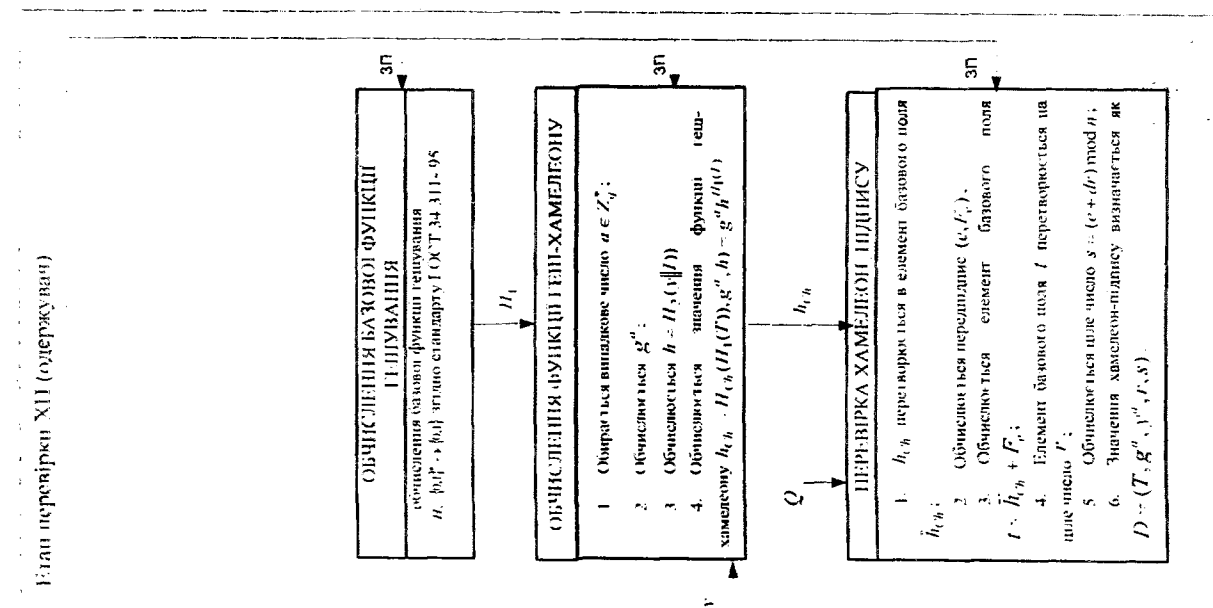
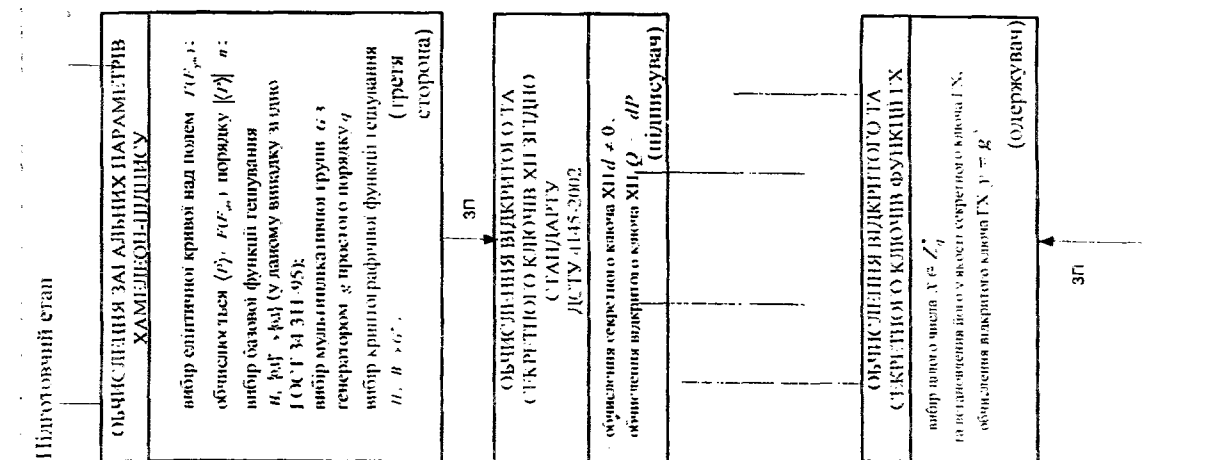
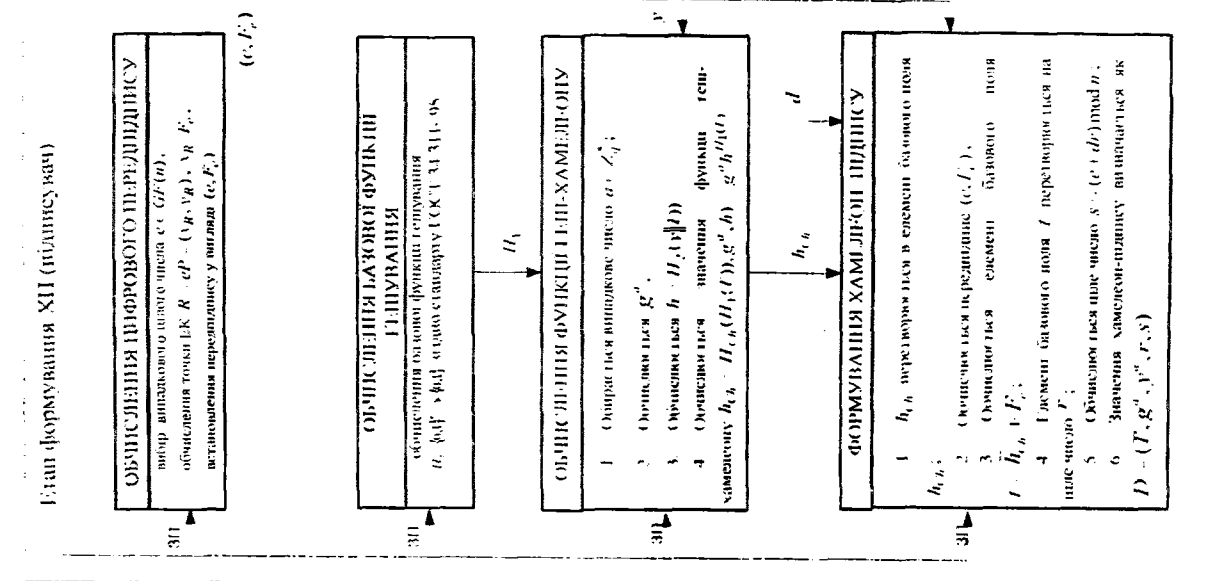


Рис. 1

2.2. Алгоритм взаємодії учасників у разі виникнення протиріч

Розглянемо протокол спростування підробленого підпису. У подальшому під протиріччям розуміється або відмова підписувача від факту формування ЕЦП, або твердження одержувача про факт підписання хибного повідомлення.

У разі виникнення протиріччя одержувач надає третій довірчій стороні (ТДС) підпис $D = (T^*, g^{a^*}, y^{a^*}, r, s)$ та неінтерактивне доведення знання Π_1^* рівності двох дискретних логарифмів $x = \log_g y = \log_{g^{a^*}} y^{a^*}$. Якщо D або Π_1^* є недійсними, ТДС відхиляє запит одержувача. Якщо перевірка пройшла успішно, ТДС відправляє підпис підписувачу. Якщо підписувач вважає отриманий підпис дійсним, він підтверджує ТДС цей факт. У протилежному випадку він формує колізію функції геш-хамелеону наступним чином:

1. Якщо підписувач хоче забезпечити властивість «відновлення повідомлення» [7], він надає ТДС набір (T, g^a, y^a, Π_1) у якості колізії, де Π_1 – неінтерактивне доведення знання рівності двох дискретних логарифмів $\log_g g^a = \log_y y^a$. Тільки якщо $T^* \neq T$, $h_{Ch} = g^a h^{H_1(T)}$ та Π_1 є дійсним, ТДС може бути впевнена у тому, що одержувач сформував підробку підпису повідомлення T . Розгорнутий протокол спростування підробленого підпису у разі необхідності забезпечення властивості «відновлення повідомлення» представлена на рис. 2.

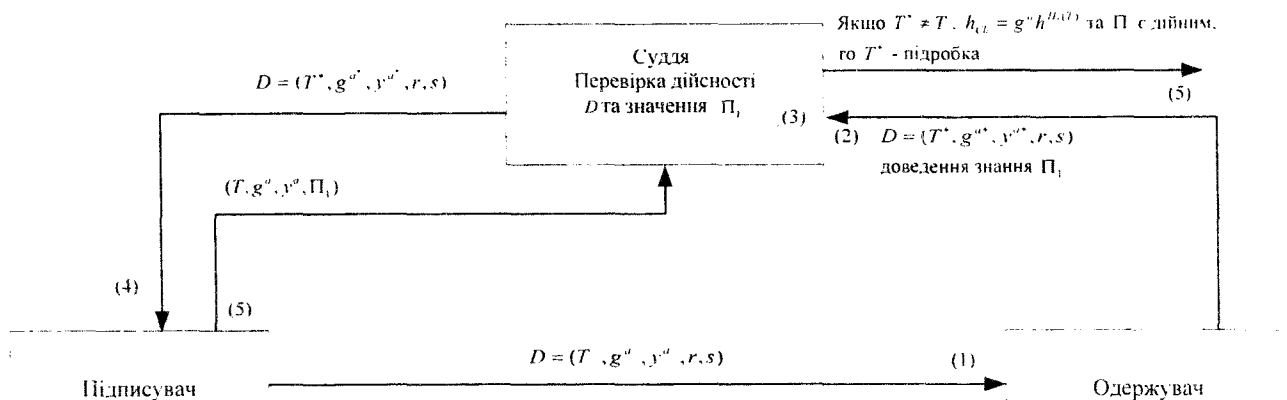


Рис. 2

2. Якщо підписувач хоче забезпечити властивість «прихованість повідомлення» [7], він надає ТДС набір (g^a, y^a, Π_1, Π_2) у якості колізії, де Π_2 – неінтерактивне доведення знання дискретного логарифму $T = \log_h h_{Ch} / g^a$ та Π_1 – неінтерактивне доведення знання рівності двох дискретних логарифмів $\log_g g^a = \log_y y^a$. Тільки якщо, $g^{a^*} \neq g^a$, та Π_1, Π_2 є дійсними, ТДС може бути впевненим у тому, що одержувач сформував підробку підпису повідомлення T^* , і водночас, повідомлення T залишилося конфіденційним.

Розгорнутий протокол спростування підробленого підпису у разі необхідності забезпечення властивості «прихованість повідомлення» представлено на рис. 3.

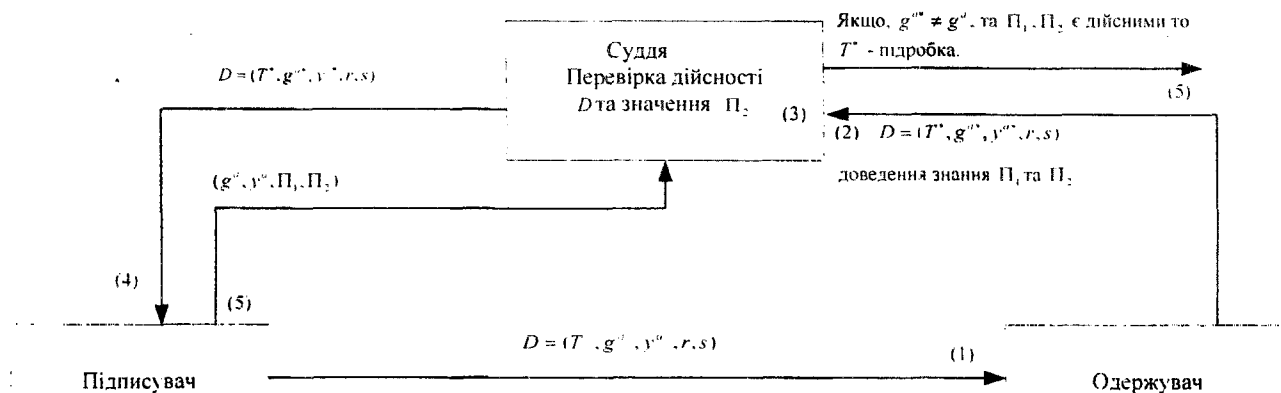


Рис. 3

3. Аналіз складності хамелеон-підпису на основі ДСТУ 4145-2002

Наділення алгоритму ЕЦП додатковими властивостями зазвичай супроводжується зростанням складності обчислень. Тому важливим питанням є вимірювання зростання складності отриманого алгоритму.

У табл. 2 наведено результати порівняльного аналізу складності алгоритму ЕЦП згідно з ДСТУ 4145-2002 та алгоритму хамелеон-підпису на основі ДСТУ 4145-2002. У таблиці використовуються наступні позначення: H – складність обчислення базової функції гешування, M_E – множення на скаляр у групі точок ЕК, M_F – множення у скінченному полі, M_G – множення у скінченній групі, A_E – бінарна операція у групі точок ЕК, E_G – зведення до ступеня у скінченній групі.

Таблиця 2

Процес	ДСТУ 4145-2002	Хамелеон-підпис згідно з ДСТУ 4145-2002
Формування підпису	$1H + 1M_E + 2M_F$	$2H + 1M_E + 2M_F + 3E_G + 1M_G$
Перевірка підпису	$1H + 2M_E + 1M_F + 1A_E$	$2H + 2M_E + 1M_F + 1A_E + 2E_G + 1M_G$

За результатами табл. 2 відмітимо, що складність хамелеон-підпису відносно складності алгоритму ЕЦП ДСТУ 4145-2002 визначається тільки схемою геш-хамелеону, а саме – наскільки її швидкісні показники відрізняються від базової функції гешування, що використовується у схемі ЕЦП.

У табл. 3 наведено результати порівняльного аналізу складності обчислень геш-хамелеону та геш-функції згідно з ГОСТ 34.311-95. Слід зазначити, що складність алгоритму геш-хамелеону залежить від структури скінченної групи та базової функції гешування. У якості скінченної групи використовується мультиплікативна група поля Галуа, тобто складність функції геш-хамелеону визначатиметься характеристикою поля.

Порівняльний аналіз будемо проводити у залежності від зростання бітової довжини характеристики поля та розміру даних, що будуть гешуватися.

Реалізація алгоритмів гешування виконана мовою програмування Java та тестовий стенд має наступні характеристики: ОС Windows XP SP 3, AMD Athlon 64 X2 Dual Core Processor 3800+ 2.01Ghz, 3.00 Gb of RAM.

Виходячи з отриманих результатів, відмітимо, що при збільшенні характеристики поля та використанні даних розміром до 1 Кб швидкість виконання геш-хамелеону уповільнюється відносно базової функції гешування у сотні разів. Але при використанні даних розміром від 1 Мб та більше, складність обчислень майже однакова. Це пов'язано з тим, що при обчисленні результату геш-хамелеону спочатку виконується базова функція гешування, а після виконуються 3 операції зведення до ступеня та 1 множення у групі незалежно від об'єму вхідних даних.

дних даних. Таким чином, при зростанні об'єму вхідних даних до базової функції гешування зростання бітової довжини характеристики поля не вносить суттєвого вклад у складність обчислення функції геш-хамелеону.

Таблиця 3

	1 Кб	1 Мб	10 Мб
ГОСТ 34-311	0.002 с	2.552 с	25.542 с
Геш-хамелеон – 512	0.006 с	2.592 с	25.657 с
Геш-хамелеон – 1024	0.014 с	2.535 с	25.579 с
Геш-хамелеон – 2048	0.040 с	2.576 с	26.003 с
Геш-хамелеон – 3072	0.084 с	2.618 с	25.434 с
Геш-хамелеон – 4096	0.146 с	2.671 с	25.750 с
Геш-хамелеон – 6144	0.328 с	2.867с	26.682 с
Геш-хамелеон – 8192	0.571 с	3.090 с	28.010 с

При застосуванні функції геш-хамелеону у протоколах, що передбачають використання даних невеликої довжини (менш ніж 1 Кб) зазначимо, що збільшення складності обчислення приблизно у 300 разів є відносним, оскільки таке збільшення є максимальним на довжині характеристики поля у 8192 біта та абсолютний час виконання геш-хамелеону складає приблизно 0,5 с.

У табл. 4 наведено приклад обчислення функції геш-хамелеону із бітовою довжиною характеристики поля 512 біт та демонструється формування колізії.

Таблиця 4

Формування функції геш-хамелеону	
Опис	Значення
Рівень стійкості (біт)	512
Характеристика поля	0xEA0D54F24469F1D9C9A850B0AF7346FEF9A09F30BB6AC6C9966D700849133E0ECF57D4F9F7199842B8D2EDC6F5823E9644C10A5881343C96B5A41B9BE081F9D3
Генератор групи	0x71C4F7F7BD0F18E8605DADBF0E6674938B4A768D7290427D7D2793A9CB63FBC968388D7B7059FE6D7A191FA5AA6329B253A6623555BC411CE3FB3D5273521DAE
Порядок групи	0x856E6BA94E3169D3D7EA71764ADF11971703A0F1
Особистий ключ хамелеон-підпису	0x399E744F7E09EAC152B161989616A2C7D4EE6DB4
Відкритий ключ геш-хамелеону	0xE5099FE4EE5AEFBC40C6CE5047ED9943083BB0427D46FB0D9A45CEBE5606A482032C83DA9E0035CE36D60186E67F8150A1F29440FA4F09FD72D63927749F0FB3
Ідентифікатор підписувача	Підписувач
Ідентифікатор одержувача	Одержувач
Ідентифікатор транзакції	1324564
Повідомлення T	abcdefghijkl
Значення функції геш-хамелеону	0x3505A80A448902937CE404CF226E349B99B6E02FBF0E684198303C61CE498713
Формування колізії	
Повідомлення T^*	123456789
Значення функції геш-хамелеону	0x3505A80A448902937CE404CF226E349B99B6E02FBF0E684198303C61CE498713

Висновки

Сучасні вимоги бізнесу у сфері електронної комерції потребують забезпечення додаткових послуг безпеки. Аналіз доступних джерел дозволяє зробити висновок, що забезпечення цих властивостей потребує застосування нових концепцій та вдосконалення існуючих меха-

нізмів захисту інформації, проте вдосконалення існуючих схем не повинно призводити до суттєвого погіршення характеристик (наприклад, складність обчислень, стійкість, пропускна здатність тощо), що ними забезпечувались. У роботі викладаються результати досліджень, що дозволяють запропонувати нове застосування національного стандарту ЕЦП ДСТУ 4145-2002 у сферах закритих інтернет-аукціонів та системах закритого електронного голосування [8,9]. Таке вдосконалення стало можливим за рахунок інтеграції до ЕЦП ДСТУ 4145-2002 геш-функції спеціального виду (геш-хамелеон). Запропонована схема забезпечує ряд властивостей, серед яких основними є непередаваність ЕЦП та прихованість повідомлення. Наділення базової схеми ЕЦП новими властивостями не зменшує її рівень стійкості, що визначається специфікою інтеграції функції геш-хамелеону у зазначену схему ЕЦП.

На основі теоретичних досліджень схеми хамелеон-підпису було отримано аналітичний вираз для складності обчислень. Збіг теоретично очікуваних результатів та результатів практичної реалізації доводять їх достовірність. Аналіз часової складності схеми хамелеон-підпису проводився без врахування протоколів спростування підробленого підпису як і з забезпеченням властивості «відновлення повідомлення», так і властивості «прихованість повідомлення», оскільки вони виконуються лише у випадку виникнення протиріччя.

Відмітимо, що запропонована схема хамелеон-підпису у порівнянні за схемою ДСТУ 4145-2002 має близькі за значенням швидкісні характеристики. Відхилення від показників швидкодії при зростанні рівня стійкості геш-хамелеону спостерігається лише на малих довжинах повідомлень, але таке відхилення є відносним та не заважає його практичному застосуванню, зокрема у системах закритих інтернет-аукціонів та закритого електронного голосування.

У межах подальших досліджень планується створення функції геш-хамелеону в групі точок ЕК з метою вдосконалення схеми хамелеон-підпису на основі ДСТУ 4145-2002 на етапі генерування загальносистемних параметрів, а також детальний аналіз стійкості запланованої схеми.

Список літератури: 1. *H. Krawczyk and T. Rabin, Chameleon hashing and signatures Proc. of NDSS. – 2000. – P.143-154, 2000.* 2. *G. Ateniese and B. de Medeiros. Identity-based chameleon hash and applications. FC 2004, LNCS 3110, Springer-Verlag, 2004, pp.164-180.* 3. *X. Chen, F. Zhang, and K. Kim, Chameleon hashing without key exposure, ISC 2004, LNCS 3225, Springer-Verlag, 2004, pp.87-98.* 4. *G. Ateniese and B. de Medeiros, On the key exposure problem in chameleon hashes. SCN 2004, LNCS 3352, Springer-Verlag, 2005, pp.165-179.* 5. *W. Gao, F. Li, and X. Wang, Chameleon hash without key exposure based on Schnorr signature, Computer Standards and Interfaces 31, 2009, pp. 282-285.* 6. *ДСТУ 4145-2002 "Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння".* 7. *X. Chen, F. Zhang, Key-Exposure Free Chameleon Hashing and Signatures Based on Discrete Logarithm Systems, Cryptology ePrint Archive: Report 2009/035, 2009.* 8. *А.В. Лєншин, Ю.М. Іценко, Додаткові властивості безпеки електронних транзакцій у системах, що використовують сервіси комбінованої ІВК // Вісник Харк. нац. ун-ту ім. В.Н. Каразіна. – №890. Сер. Математичне моделювання. Інформаційні технології. Автоматизовані системи управління". – Х., 2010. – Вип. 13. – С. 109-114.* 9. *Ю.М. Лєншина, Д.С. Беяк, Реалізація послуги приватності у схемі інтернет-аукціону з використанням хамелеон-підпису // Системи обробки інформації. Інформаційні технології та комп'ютерна інженерія. – Х., 2011. – Вип. 3(93). – С. 126-129.*

*Харківський національний
університет радіоелектроніки*

Надійшла до редколегії 15.08.2011

АНАЛИЗ ВОЗМОЖНОСТЕЙ УМЕНЬШЕНИЯ ВЫЧИСЛИТЕЛЬНОЙ СЛОЖНОСТИ ЭЦП ДСТУ 4145-2002 ПРИ ИСПОЛЬЗОВАНИИ НОРМАЛЬНОГО БАЗИСА

Нормальный и полиномиальный базисы рекомендуются к использованию во многих стандартах, связанных с криптографией на эллиптических кривых, например ДСТУ 4145-2002 [1], IEEE P1363 [2]. Аппаратная реализация арифметики нормального базиса даёт большие преимущества в сравнении с аппаратной реализацией полиномиального базиса и программной реализацией нормального базиса. Но, так как аппаратная реализация является материально затратной и часто возникает необходимость совместимости реализации стандартов различных стран, поэтому применяется программная эмуляция. Поэтому появляются задачи более эффективной программной реализации преобразований в нормальном базисе.

Представление в нормальном базисе имеет вычислительное преимущество при возведении в квадрат элемента. Данная операция представляет собой циклический сдвиг. Одним из наиболее актуальных вопросов арифметики конечных полей остается уменьшение вычислительной сложности таких операций, как умножение и инверсия. Но так как инверсия является более трудоемкой операцией, то вопрос оптимизации инверсии стоит более остро.

Чаще всего применяется класс нормальных базисов, называемый Гауссовскими нормальными базисами (ГНБ), поскольку он обладает меньшей вычислительной сложностью за счет оптимизации правил умножения. Тип 1 и 2 ГНБ имеют самые эффективные правила умножения среди всех нормальных базисов.

Проведенный анализ научных работ показал, что в настоящее время чаще всего рекомендуются следующие алгоритмы (по именам их авторов):

- 1) Wang [3];
- 2) Itoh, Tsujii [4];
- 3) Feng [5];
- 4) Chang [6];
- 5) Takagi, Yoshiki [7].

В ДСТУ 4145-2002 и IEEE P1363 рекомендуется использовать алгоритм [4], однако появились более эффективные варианты. Для перечисленных алгоритмов был проведен теоретический и экспериментальный анализ их характеристик.

Алгоритм [3], как и последующие, использует следствие из малой теоремы Ферма.

Из малой теоремы Ферма следует, что $\forall a \neq 0, a \in \text{GF}(2^m) \exists a^{-1} = a^{2^m-2}$, где m – степень расширения поля. Как известно, стандартом [1] рекомендуются нечетные, более того, простые m : 173, 179, 191, 233, 431.

Поскольку $2^m - 2 = 2^1 + 2^2 + \dots + 2^{m-1}$, a^{-1} представляется как $a^{-1} = a^{2^m-2} = a^{2^1} \times a^{2^2} \times \dots \times a^{2^{m-1}}$.

Алгоритм [3] требует $m-2$ умножений.

Itoh и Tsujii [4] предложили модернизацию алгоритма [3], а именно – разложение степени 2^m-2 следующим образом: $a^{-1} = a^{2^m-2} = \left(a^{2^{m-1}-1} \right)^2$.

Далее степень $2^{m-1}-1$ раскладывается:

- 1) при нечетном m

$$a^{2^{m-1}-1} = 2^{(2^{(m-1)/2}-1)(2^{(m-1)/2}+1)},$$

- 2) при четном m

$$a^{2^{m-1}-1} = 2(2^{(m-2)/2} - 1)(2^{(m-2)/2} + 1) + 1.$$

Алгоритм требует $q(m-1) + w(m-1) - 1$ умножений, где $w(m)$ – вес Хемминга и $q(m-1) = \lfloor \log_2(m-1) \rfloor$.

Алгоритм, предложенный Feng [5], по вычислительной сложности практически эквивалентен алгоритму [4].

Алгоритм [5] отличается лишь тем, что он вычисляет квадратные корни каждую итерацию, а потом возводит в квадрат 2^{m-m_0} , в то время как алгоритм [4] выполняет возведение в квадрат каждую итерацию. И оценка вычислительной сложности алгоритма [5] составляет $(q(m) + w(m))$ умножений, где $q(m) = \lfloor \log_2(m) \rfloor$.

Алгоритм [6] основывается на следующем разложении: $m-1 = s \times t$. При этом элемент a^{-1} может быть выражен следующим образом:

$$a^{-1} = (a^{(2^{s-1}-2)})((2^s)^{t-1} + (2^s)^{t-2} - \dots - (2^s)^1 + (2^s)^0).$$

$a^{(2^{s-1}-2)}$ может быть вычислено с помощью алгоритма [4] с заменой $m-1$ на s .

Он требует $(q(s) + w(s) - 2) + (q(t) + w(t) - 2)$ умножений, где $m-1 = s \times t$. Данный алгоритм эффективен, однако область его применения ограничена (он не может быть использован, когда $m-1$ является простым числом). Однако это ограничение не является критичным для реализации отечественного стандарта [1] (рекомендовано использовать простые m , т.е. $m-1$ гарантированно непростое число).

Количество умножений уменьшается по сравнению с алгоритмом [4]. Например, для $m = 233$ [1], количество умножений для алгоритма [6] равно 8, а для алгоритма [4] количество умножений равно 10. Необходимо отметить, что количество умножений зависит от способа разложения числа $m-1$ на сомножители (когда возможны различные варианты) $m-1$ может быть разложено на несколько комбинаций чисел. Кроме того, при некоторых значениях m , количество умножений в оценке вычислительной сложности алгоритма не всегда меньше, чем для алгоритмов [4, 5] (зависит от веса сомножителей s, t). Однако это не относится к вариантам из [1].

Takagi и др. [7] предложили усовершенствование алгоритма [6], которое основывается на следующем типе разложения: $m-1 = s \times t + h$. Так как

$$2^m - 2 = 2^{m-1} + 2^{m-1} - 2 = 2^{m-1} + 2^{m-2} + \dots + 2^{m-h} - 2, \text{ то}$$

$$a^{-1} = a^{2^m-2} = a^{2^{m-1}} \times a^{2^{m-2}} \times \dots \times a^{2^{m-h}-2}.$$

где $a^{2^{m-i}}$ вычисляется при помощи i -битового циклического сдвига влево. Таким образом, a^{-1} получают из $a^{2^{m-h}-2}$ при помощи h умножений, а значение $a^{2^{m-h}-2}$ вычисляется при помощи алгоритмов [4] или [6] (при замене m на $m-h$). Далее $s \times t$ можно разложить на более мелкие сомножители, и для них использовать описанный выше подход повторно.

В общем случае, при представлении $m-1 = \prod_{j=1}^k s_j + h$ и вычислительная сложность оценивается как $\sum_{j=1}^k (q(s_j) + w(s_j) - 2) + h$.

Очевидно, что количество умножений зависит от способа разложения. Может существовать несколько разложений, которые уменьшают количество умножений. В таком случае, лучше всего адаптировать наипростейшее разложение, то есть разложение с наименьшим количеством компонентов, с целью сделать контроль вычисления a^{-1} проще. Далее разложение, минимизирующее количество требуемых умножений и состоящее из минимально возможного количества компонентов, называется «оптимальным разложением». Оптимальных разложений для одного и того же числа может быть несколько.

При нахождении оптимального разложения руководствуются следующими утверждениями:

1) При $m-1 = 2^n$ оптимальным разложением является само значение $m-1$ и количество умножений в оценке вычислительной сложности равно n .

2) При $m-1 = 2^n + 2^{n'}$ ($n > n'$) вес $w(m-1) = 2$, оптимальным разложением является само значение $m-1$ и количество требуемых умножений $n + 1$.

3) При $m-1 = 2^{n'}s + h$, где s – нечетное, наименьшее количество требуемых умножений по разложению $m-1$ как $\prod_{j=1}^k s_j + h$ равно $n' + h$ плюс количество требуемых умножений для оптимального разложения s .

При представлении $m-1 = \prod_{j=1}^k s_j + h$, если s_1 далее не раскладывается, то количество умножений в оценке вычислительной сложности не менее $\sum_{j=1}^k q(s_j) + h \geq q(m-1) + h$, т.к. $w(s_j) \geq 2$. При дальнейшем использовании оптимального разложения s_1 требуется не менее $q(s_1)$ умножений, т. е. количество умножений при оптимальном разложении $m-1$ не менее $q(m-1) + h$.

4) В оптимальном разложении $m-1$, выбирают остаток $h < w(m-1)-2$.

В табл. 1 обобщены теоретические оценки вычислительной сложности рассмотренных алгоритмов в количестве умножений элементов поля.

Таблица 1

Алгоритм	Сложность, кол. умножений
Wang [3]	$m-2$
Itoh, Tsujii [4]	$q(m-1) + w(m-1) - 1$
Feng [5]	$q(m) + w(m)$
Chang [6]	$q(s) + w(s) + q(t) + w(t) - 4$
Takagi, Yoshiki [7]	$\sum_{j=1}^k (q(s_j) + w(s_j) - 2) + h$

При заданном m мы можем найти все варианты оптимальных разложений $m-1$. При этом стоит заметить, что можно использовать предложения для нахождения оптимального разложения первого сомножителя s_1 . Проблема нахождения оптимального разложения не является критичной, потому как мы должны решать её, только когда мы выбираем m .

В табл. 2 приведены результаты предварительного просчета количества умножений при использовании всех возможных разложений для значений m , рекомендованных в [1].

Таблица 2

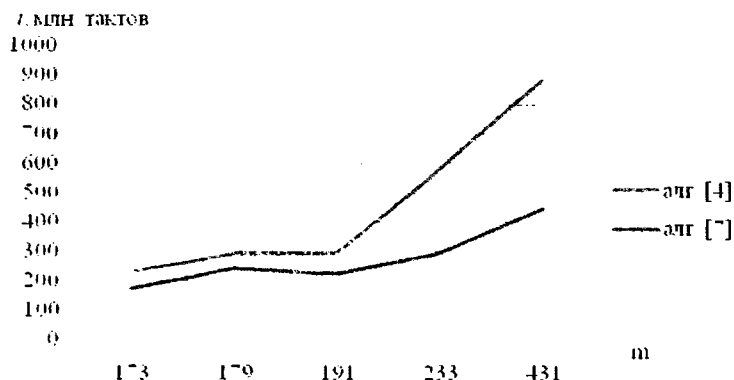
m	Факт.-ция $m-1$ (для алг. [7])	Варианты разложений $m-1$ (для алг. [6])			Количество умножений					
					[4]	[5]	[6]			[7]
173	$2 \times 2 \times 43$	4×43	2×86	-	10	11	7	5	-	6
179	2×89	2×89	-	-	10	11	9	-	-	9
191	$2 \times 5 \times 19$	10×19	38×5	95×2	12	13	8	8	10	7
233	$2 \times 2 \times 2 \times 29$	4×58	8×29	2×116	10	11	8	8	8	8
431	$2 \times 5 \times 43$	10×43	2×215	5×86	13	13	9	11	10	9

Очевидно, что при любых вариантах разложения наименьшей вычислительной сложностью обладают алгоритмы [6, 7], причём для большинства рекомендованных [1] полей оптимален алгоритм [7], однако желательно иметь возможность использовать оба варианта (например, алгоритм [6] для поля с расширением $m = 173$).

При проведении экспериментальных исследований рассматривались алгоритмы [4, 7], так как алгоритм [4] является рекомендованным ДСТУ 4145-2002 и IEEE P1363, а алго-

ритм [7] характеризуется наилучшими теоретическими оценками вычислительной сложности.

На рисунке приведены соответствующие результаты экспериментальных исследований, а именно оценки среднего количества тактов процессора t при рекомендованных [1] значениях степени m .



Анализ существующих алгоритмов инверсии в нормальном базисе выявил, что алгоритмы [6, 7] показывают лучшие вычислительные характеристики по сравнению с рекомендованным стандартами алгоритмом [4]. Для значений m , рекомендованных [1], теоретические оценки средней вычислительной сложности алгоритмов [6, 7] меньше соответствующей оценки алгоритма [4] приблизительно на 29%.

Экспериментальные исследования показали, что вычислительная сложность алгоритма [7] меньше, чем у алгоритма [4], в среднем на 37,5%. Таким образом, именно алгоритм [7] может быть рекомендован к использованию при реализации операции инверсии в нормальном базисе. Однако желательно иметь возможность программного выбора между реализациями вариантов алгоритмов [6, 7] в зависимости от текущего используемого поля. А также необходимы более детальные экспериментальные исследования возможных наиболее эффективных рекурсивных версий реализации данных методов.

Список литературы: 1. ДСТУ 4145 – 2002. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння: Введ. 1.07.2003. – К. : Державний комітет України з питань технічного регулювання та споживчої політики. 2003 р. – 36 с. 2. IEEE P1363 / D9 (Draft Version 9). Standard specifications for public key cryptography. Annex A (informative). Number – theoretic background, 1999. – 170 p. 3. C.C.Wang, T.K.Truong, H.M.Shao, L.J.Deutsch, J.K.Omura, I.S.Reed. VLSI architecture for computing multiplications and inverses in $GF(2^m)$. IEEE Trans. Computers, vol. 34, no. 8, pp. 709-716, 1985. 4. T.Itoh, S.Tsujii. A fast algorithm for computing multiplicative inverses in $GF(2^m)$ using normal basis. Information and Computing, vol. 78, pp. 171-177, 1988. 5. G.L.Feng. A VLSI architecture for fast inversion in $GF(2^m)$. IEEE Trans. Computers, vol. 38, pp.1383-1386, 1989. 6. T.Chang, E.Lu, Y.Lee, Y.Leu, H.Shyu. Two algorithms for computing multiplicative inverses in $GF(2^m)$ using normal basis, accepted by Information Processing Letters. 7. N.Takagi, Y.Yoshiki, K.Takagi. A fast algorithm for multiplicative inversion in $GF(2^m)$ using normal basis // IEEE Transactions on Computers, vol. 50, no. 5, pp. 394-398, 2001.

Харьковский национальный
университет радиоэлектроники

Поступила в редколлегию 15.08.2011

МНОГОКАСКАДНОЕ УНИВЕРСАЛЬНОЕ ХЕШИРОВАНИЕ ПО РАЦИОНАЛЬНЫМ ФУНКЦИЯМ КРИВОЙ СУЗУКИ

Введение

Применение для аутентификации каскадного хеширования позволяет получить наименьшую вероятность коллизии, сложность вычислений хешей для фиксированного объема данных и размерности конечного поля. Основные результаты представлены в работах [1, 2]. Наилучший результат универсального хеширования достигается на максимальных кривых, число точек которых лежит на границе Хассе–Вейля. Свойства каскадного универсального хеширования по проективной прямой и кривой Эрмита представлены в [1]. Оценки вероятности коллизии для многократного универсального хеширования получены в [2]. Максимальные кривые ассоциированные с группой Сузуки и группой Ри имеют максимально возможное значение рода и соответственно число точек [3]. Актуальным является построение многокаскадного универсального хеширования по рациональным функциям кривой Сузуки.

В данной работе предлагается метод каскадного универсального хеширования по рациональным функциям кривой Сузуки. С этой целью в разд. 1 рассмотрено каскадное универсальное хеширование по рациональным функциям алгебраических кривых. В разд. 2 представлено многокаскадное универсальное хеширование на основе произведения функциональных полей кривой Сузуки и хеширования по проективной прямой и кривой Эрмита.

1. Каскадное универсальное хеширование по алгебраическим кривым

Каскадное универсальное хеширование по алгебраическим кривым рассмотрено в [1] и представляется двумя основными схемами: каскадное хеширование со связкой хеша и текста и каскадное хеширование на основе произведения функциональных полей.

Определение каскадной схемы универсального хеширования со связкой хеша и текста имеет следующее представление.

Определение 1. [1]. Пусть F_q – конечное поле, M – сообщение и $M = M_1 \parallel M_2$. Каскадное универсальное хеширование по рациональным функциям алгебраических кривых определяется выражением $Ch(M) = AGh_2(AGh_1(M_1) \parallel M_2)$, где AGh_1 , AGh_2 есть универсальные схемы хеширования по рациональным функциям алгебраических кривых, $Ch(M)$ определяет универсальное семейство хеш функций $\varepsilon - AU$, где $\varepsilon = \max(\varepsilon_1, \varepsilon_2) + 1/\lceil H^2 \rceil$, $\varepsilon_1, \varepsilon_2$ – соответственно, вероятности коллизий для AGh_1 и AGh_2 хеширования.

Утверждение 1. [1] Пусть AGh_1 , AGh_2 соответственно $\varepsilon_1 - U$ и $\varepsilon_2 - U$ универсальные классы хеш функций. Каскадная конструкция $Ch(M)$ имеет наименьшую вероятность коллизии, если $\varepsilon_1 = \varepsilon_2$.

Замечание 1.

1. Каскадное хеширование $Ch(M)$ при фиксированном поле вычислений предполагает разбиение данных на блоки приблизительно равной длины. Вероятность коллизии каскадного хеширования имеет ограничение по наименьшему полю вычисления хеша одного из каскадов.

2. Размер ключевых данных увеличивается пропорционально числу каскадов, с учетом поля вычисления и универсального хеширования каскада.

3. Каскадное хеширование позволяет эффективно увеличить общую длину хешируемых данных и зафиксировать вероятность коллизии на уровне хеша первого каскада, если на втором и последующих каскадах увеличить поле вычислений. Примером является алгоритм хе-

ширования UMAC(2000), каскадная схема применяется с подъёмом поля вычисления, сначала 32, затем 64 и 128 бит.

Свойства каскадного хеширования по алгебраическим кривым на основе произведения функциональных полей имеют следующее определение.

Определение 2. Пусть F_q – конечное поле, M – сообщение и $M = M_1 \parallel M_2 \parallel \dots \parallel M_t$. Алгоритм вычисления хеша кода в каскадной конструкции определяется выражением

где AGh_1, AGh_2 – универсальные схемы хеширования по алгебраическим кривым, $Ch_t(M)$ определяет универсальное семейство хеш функций $\varepsilon - AU$, где $\varepsilon = \max(\varepsilon_1, \varepsilon_2) + 1/\lceil H^2 \rceil$, $\varepsilon_1, \varepsilon_2$ – соответственно вероятности коллизий для AGh_1 и AGh_2 хеширования.

Замечание 2.

1. Коллизионные свойства каскадного хеширования следуют из утверждения 1.

2. Каскадное хеширование $Ch_t(M)$ при фиксированном поле вычислений предполагает разбиение данных на t блоков равной длины. Для первого каскада вероятность коллизии определяется размером блока данных, для второго – значением t – числа блоков данных.

3. Вероятность коллизии каскадного хеширования имеет ограничение по наименьшему полю вычисления хеша одного из каскадов.

4. Размер ключевых данных определяется произведением пространства ключей первого и второго каскадов, с учетом поля вычисления и универсального хеширования каскада.

5. Каскадное хеширование позволяет эффективно увеличить общую длину хешируемых данных и зафиксировать вероятность коллизии на уровне хеша одного из каскадов.

6. Двух каскадная конструкция $Ch_t(M)$ легко распространяется на многокаскадную $l - Ch_t(M)$, где l – число вложенных каскадов универсальных схем хеширования по алгебраическим кривым $AGh_1, AGh_2, \dots, AGh_l$.

2. Многокаскадное универсальное хеширование по рациональным функциям кривой Сузуки

Основные результаты по кривой Сузуки. Кривые Сузуки S являются F_q изоморфными плоской кривой $y^q - y = x^q(x^q - x)$, где $q = 2q_0^2$ и $q_0 = 2^s$. Род кривой $g = q_0(q - 1)$, число F_q рациональных точек равно $q^2 + 1$.

Точками кривой являются особая точка на бесконечности $P_0 = (0:1:0)$ кратности q_0 и рациональные точки $P_{a,b} = (a:b:1)$, где $a, b \in F_q$, и $b^q - b = a^{q_0}(a^q - a)$.

Подгруппа Вейерштрасса функционального поля кривой содержит подгруппу $H(P_0) = \langle q, q + q_0, q + 2q_0, q + 2q_0 + 1 \rangle$. Кривая Сузуки определяется полной линейной серией $D = [(q + 2q_0 + 1)P_0]$ размерности $\dim = 4$. Базис пространства $L(P_0)$ задается функциями вида $\{w^i \cdot v^j \cdot x^r : i(q + 2q_0) + j(q + 2q_0 + 1) + r(q + q_0) \leq \rho\}$, что следует из подгруппы Вейерштрасса $H(P_0)$, представленной порядками полюсов функций $x = X/Z$, $y = Y/Z$, $v = x^{2q_0+1} + y^{2q_0}$, $w = xy^{2q_0} + x^{2q+2q_0} + y^{2q}$. Порядки полюсов $\text{div}_x(x) = qP_0$, $\text{div}_x(y) = (q + q_0)P_0$, $\text{div}_x(v) = (q + 2q_0)P_0$, $\text{div}_x(w) = (q + 2q_0 + 1)P_0$.

Универсальный класс хеш функций, построенный по рациональным функциям кривой Сузуки, представлен в [4, 5]. Основные результаты следующие.

Определение 3. [4] Хеш функция $h_{x,v}(m) \in F_q$, $q = 2q_0^2$, $q_0 = 2^s$ для сообщения m по рациональным функциям кривой $Y^q Z^{q_0} - YZ^{q+q_0-1} = X^{q+q_0} - X^{q_0+1}Z^{q-q_0-1}$ в точке x, y определяется выражением $h_{x,v}(m) = \sum m_{i,j,t,r} \cdot w^i \cdot v^j \cdot y^t \cdot x^r$, где ρ_k – полюс подгруппы Вейерштрасса $H(P_\infty)$, $m_{i,j,t,r} \in F_q$ – слова сообщения m , $i \geq 0$, $0 \leq j \leq 2q_0 - 1$, $0 \leq t \leq 1$, $0 \leq r \leq q_0$, $i(q + 2q_0) + j(q + 2q_0 + 1) + t(q + q_0) + rq \leq \rho_k$, $x = X/Z$, $y = Y/Z$, $v = x^{2q_0+1} + y^{2q_0}$, $w := xy^{2q_0} + x^{2q+2q_0} + y^{2q}$.

Утверждение 2. [4] Хеширование по рациональным функциям кривой $y^q - y = x^{q_0}(x^q - x)$, где $q = 2q_0^2$ и $q_0 = 2^s$ над полем F_q , определяет универсальный хеш класс $\varepsilon - U(q^2, q^k, q)$, где q^2 – число хеш функций (объем ключевого пространства), q^k – объем пространства сообщений, q – объем пространства хеш кодов. Вероятность коллизии ε определяется соотношениями

$$\varepsilon = (i(q + 2q_0) + j(q + 2q_0 + 1) + t(q + q_0) + rq) / q^2, \text{ если } k < q_0(q - 1), \quad (2)$$

$$\varepsilon = (k + q_0(q - 1)) / q^2, \text{ если } k \geq q_0(q - 1), \quad (3)$$

где i, j, t, r определяются леммой.

Лемма [4]. Пусть $k < q_0(q - 1)$. Для кривой Сузуки имеет место $i = p - j$, $j = \Delta - t \cdot q_0 - 1$, $r = s - s_2 + d \cdot q_0$, $t = t_1 \bmod 2$, где $s' = \lfloor (3k)^{1/3} \rfloor$, $\Sigma = s'(s'+1)(2s'+1)/6$, $s = s' + \lfloor k/\Sigma \rfloor$, $s_1 = s - q_0 - 1$, $\Sigma_{s-1} = s(s-1)(2s-1)/6 - s_1(s_1-1)(2s_1-1)/3 - s_1(s_1-1)$, $k' = k - \Sigma_{s-1}$, $k_1 = \lceil k'/2 \rceil$, $d = \lfloor s_2/(s-t) \rfloor$, $k_2 = k_1 + s_1(s_1+1)/2$, $s_2 = \lfloor (2k_2+1/4)^{1/2} - 1/2 \rfloor$, $s_3 = s_2 - q_0 - 1$, $\Delta = k' - 2k_3$, $t_1 = \lfloor \Delta/q_0 \rfloor$, $k_3 = (s_2-1)s_2/2 - (s_1-1)(s_1+1)/2 - s_3(s_3+1)/2$, $p = s_2 - (s_2-t)d$, $\lceil \cdot \rceil$ – округление к большему целому числу, $\lfloor \cdot \rfloor$ – округление к меньшему целому числу, $\lceil \cdot \rceil$ – округление к ближайшему целому числу.

Предложение [5]. Сложность универсального хеширования по кривым $y^q - y = x^{q_0}(x^q - x)$, где $q = 2q_0^2$ и $q_0 = 2^s$ над полем F_q определяется выражением

$$N_{\text{опер}} = k + s^3/3 + s^2/2 + 2s - 1, \text{ если } s \leq q_0. \quad (4)$$

$$N_{\text{опер}} = k + q_0^3/3 + q_0^2/2 + (s - q_0)(2q_0 - 1) + 2s - 1, \text{ если } s > q_0, \quad (5)$$

где $s = (3k)^{1/3}$.

Замечание 1. Асимптотическая оценка для вероятности коллизии (2) имеет значение $\varepsilon = (3k)^{1/3}/q$ для $k < q_0(q - 1)$.

Каскадное хеширование $Ch_i(M)$ по функциональному полю кривой Сузуки имеет следующее представление.

Определение 4. Пусть F_q , $q = p^2$ – расширенное конечное поле, M – сообщение и $M = M_1 \parallel M_2 \parallel \dots \parallel M_t$. Алгоритм вычисления хеш кода в каскадной конструкции определяется выражением $Ch_i(M) = Sh_q(PLh_q(M_1) \parallel PLh_q(M_2) \parallel \dots \parallel PLh_q(M_t))$, где Sh_q , PLh_q – универсальные схемы хеширования по кривой Сузуки и проективной прямой.

Утверждение 3. Пусть F_q – конечное поле, M – сообщение и $M = M_1 \parallel M_2 \parallel \dots \parallel M_t$. $Ch_i(M)$ – хеширование вида (1), где $AGh_1 = PLh_q$, $AGh_2 = Sh_q$ есть универсальные схемы.

хеширования по проективной прямой $\varepsilon_{PL} = U(q, q^{k_1}, q)$, $\varepsilon_{PL} = k_1/q$ и кривой Сузуки $\varepsilon_S = U(q^2, q', q)$, $\varepsilon_S = (3t)^{1/3}/q$ соответственно. Тогда $Ch_i(M)$ определяет универсальное семейство хеш функций $\varepsilon = U(q^3, q^k, q)$, $\varepsilon = (3k)^{1/4}/q$, $k = k_1 t$ – число слов данных, $0 < k \leq gq$, $g = q_0(q-1)$ – род кривой Сузуки.

Доказательство. Хеширование на каждом каскаде является универсальным, и каскадная хеш функция также является универсальной. Пространство ключей определяется произведением числа ключей первого и второго каскадов и равно $q^2 \cdot q = q^3$. Пусть k число слов данных и k' – размер блока данных, $t = k/k'$. Наименьшая вероятность коллизии в силу утверждения 1 реализуется в случае $\varepsilon_S = \varepsilon_{PL}$. Подставим в выражения для ε_S и ε_{PL} значения k' и $t = k/k'$, получим $(3t)^{1/3} = k'$, $k' = (3k)^{1/4}$ и оценку для вероятности $\varepsilon = (3k)^{1/4}/q$. Так как ε_{PL} имеет оценку сверху $\varepsilon_{PL} < 1$ для $k' \leq q$, а $\varepsilon_S \leq (3k)^{1/3}/q$ для $k \leq g$, получим $0 < k \leq gq$, где g – род кривой Сузуки.

Замечание 4.

1. Результаты каскадного хеширования $PLh_q - Sh_q$ являются наилучшими среди схем, где на первом каскаде используется PLh_q хеширование, и обеспечивают хеширование наибольшей длины данных.

2. Недостатком каскадного хеширования $PLh_q - Sh_q$ является повышенная сложность хеширования. Вычисления по PLh_q каскаду выполняются на одной рациональной функции со сложностью $\sim k'$ и по Sh_q каскаду на четырёх рациональных функциях – со сложностью $\sim 2t + 1.04t^{2/3} + 2\sqrt[3]{3t^{1/3}}$ (4). С учетом $t = k/k'$ и $k' = (3k)^{1/4}$ получим оценку для числа вычислений $k + 2t + 1.04t^{2/3} + 2\sqrt[3]{3t^{1/3}} = k + 1.52k^{3/4} + 0.87k^{1/2} + 2.63k^{1/4}$. Относительное увеличение сложности по сравнению с PLh_q хешированием составляет $\sim 1 + 1.52k^{-1/4}$.

Возможны комбинации других универсальных хеш функций в двух каскадной схеме хеширования, свойства представлены утверждением 4.

Утверждение 4. Пусть F_q – конечное поле, M – сообщение и $M = M_1 \parallel M_2 \parallel \dots \parallel M_r$, $Ch_i(M)$ – хеширование вида (1), где $AGh_1 = Hh_q$, $AGh_2 = Sh_q$ – универсальные схемы хеширования по кривой Эрмита и кривой Сузуки соответственно. Тогда $Ch_i(M)$ определяет универсальное семейство хеш функций $\varepsilon = U(q^3 \sqrt{q}, q^k, q)$, $\varepsilon = 1.43k^{1/5}/q$, $0 < k \leq q^2 \sqrt{q}$.

Замечание 5.

1. Доказательство подобно доказательству утверждения 3. Результаты каскадного хеширования $Hh_q - Sh_q$ являются абсолютно наилучшими среди двух каскадных схем и обеспечивают хеширование наибольшей длины данных.

2. Недостатком каскадного хеширования $Hh_q - Sh_q$ является увеличенная сложность хеширования. Вычисления по Hh_q каскаду выполняются на двух рациональных функциях со сложностью $\sim t(k' + \sqrt{k'})$ и по Sh_q каскаду на четырёх рациональных функциях – со сложностью $\sim 2t + 1.04t^{2/3} + 2\sqrt[3]{3t^{1/3}}$ (4). С учетом $t = k/k'$ и $k' = 1.02k^{2/5}$ получим оценку для числа вычислений $t(k' + \sqrt{k'}) + 2t + 1.04t^{2/3} + 2\sqrt[3]{3t^{1/3}} = k + k^{4/5} + 2k^{3/5} + k^{2/5} + 2.88k^{1/5}$. Относительное увеличение сложности по сравнению с PLh_q хешированием составляет $\sim 1 + k^{-1/5}$.

Оценки многокаскадного универсального хеширования $l - Ch_l(M)$ представлены утверждением 5.

Утверждение 5. Пусть F_q , $q = 2^{2^{l+1}}$ – расширенное конечное поле, M – сообщение и $M = M_1 \parallel M_2 \parallel \dots \parallel M_l$, $l - Ch_l(M)$ – l -каскадное универсальное хеширование по кривой Сузуки. Тогда $l - Ch_l(M)$ определяет универсальное семейство хеш функций $\varepsilon = U(q^{2^l}, q^k, q)$.
 $\varepsilon = \sqrt[3]{3}k^{1/3l} / q$, $0 < k \leq q^{l+1/2}$, со сложностью вычислений:
 $2k + 1.04k^{(3l-1)/3l} + 2.88t^{(3l-2)/3l} + 2k^{(l-1)/l} + 1.04k^{(3l-4)/3l} + 2.88t^{(3l-5)/3l} + \dots$

Доказательство. Хеширование на каждом каскаде является универсальным и каскадная хеш функция также является универсальной. Пространство ключей определяется произведением числа ключей всех каскадов и равно q^{2l} . Наименьшая вероятность коллизии в силу утверждения 1 реализуется, если на каждом каскаде значение вероятности коллизии является наименьшим. Это достигается, если размер данных хеширования k' на каждом каскаде является наименьшим $k' = k^{1/l}$. Подставим в выражения для ε_s значения k' , получим: $\varepsilon_s = \sqrt[3]{3}k^{1/3l} / q$ и оценку для $0 < k \leq q^{l+1/2}$. Оценка сложности вычислений определяется тем, что на каждом каскаде число вычислений уменьшается в $k' = k^{1/l}$.

Суммирование по всем каскадам дает результирующее выражение

$$2k + 1.04k^{(3l-1)/3l} + 2.88t^{(3l-2)/3l} + 2k^{(l-1)/l} + 1.04k^{(3l-4)/3l} + 2.88t^{(3l-5)/3l} + \dots$$

Параметры многокаскадного универсального хеширования по кривой Сузуки представлены в табл. 1.

Таблица 1

Параметры многокаскадного универсального хеширования по кривой Сузуки

Схемы каскадного включения	Параметры универсального хеширования	Оценки сложности вычислений
$Ch_l(M)$, $PSh_q - Sh_q$	$\varepsilon = U(q^3, q^k, q)$, $\varepsilon = (3k)^{1/4} / q$, $0 < k \leq q^2$	$k + 1.52k^{3/4} + 0.87k^{1/2} + 2.63k^{1/4}$
$Ch_l(M)$, $Hh_q - Sh_q$	$\varepsilon = U(q^3 \sqrt{q}, q^k, q)$, $\varepsilon = 1.43k^{1/5} / q$, $0 < k \leq q^2 \sqrt{q}$	$k + k^{4/5} + 2k^{3/5} + k^{2/5} + 2.88k^{1/5}$
$l - Ch_l(M)$, $Sh_q - Sh_q - \dots$	$\varepsilon = U(q^{2l}, q^k, q)$, $\varepsilon = \sqrt[3]{3}k^{1/3l} / q$, $0 < k \leq q^{l+1/2}$	$2k + 1.04k^{(3l-1)/3l} + 2.88t^{(3l-2)/3l} +$ $2k^{(l-1)/l} + 1.04k^{(3l-4)/3l} +$ $2.88t^{(3l-5)/3l} + \dots$

Оценки вероятности коллизии и сложности вычислений для многокаскадного хеширования в конечном поле представлены в табл. 2.

Выводы

1. Каскадное хеширование эффективно увеличивает размер хешируемых данных и выравнивает вероятность коллизии с изменением длины данных.

2. Применение многокаскадного универсального хеширования $l - Ch_l(M)$ с одной и той же функцией хеширования на всех каскадах в $\sqrt[l]{k}$ раз уменьшает вероятность коллизии. Наименьшая вероятность коллизии реализуется в схеме $Sh_q - Sh_q$. Вычисления в поле ~64 бит обеспечивает доказуемую стойкость $P_{coll} < 2^{-57}$ для данных длиной до нескольких Гбт.

3. Двухкаскадные схемы хеширования $PLh_q - Sh_q$ и $Hh_q - Sh_q$ по вероятности коллизии являются эквивалентными. С увеличением размерности поля отличие от $PLh_q - Sh_q$ и $Hh_q - Sh_q$ хеширования становится меньше.

Таблица 2

Оценки вероятности коллизии и сложности вычислений
для многокаскадного хеширования по кривой Сузуки над полем F_q

Схемы каскадов	F_q	Вероятность коллизии для данных размером L /сложность вычислений			Размер ключей, бит	Размер хеш кода, бит
		1 Кбт	1 Мбт	1 Гбт		
$Ch_q(M),$ $PSh_q - Sh_q$	$q = 2^{31}$	$2^{-28,7}/2^8 + 2^6$	$2^{-26,2}/2^{18} + 2^{16}$	$2^{-3,7}/2^{28} + 2^{20}$	93	31
	$q = 2^{63}$	$2^{-61}/2^7 + 2^5$	$2^{-58,5}/2^{17} + 2^{10}$	$2^{-56}/2^{27} + 2^{20}$	189	63
$Ch_q(M),$ $Hh_q - Sh_q$	$q = 2^{31}$	$2^{-29}/2^8 + 2^7$	$2^{-27}/2^{18} + 2^{15}$	$2^{-25}/2^{28} + 2^{23}$	109	31
	$q = 2^{63}$	$2^{-61}/2^7 + 2^6$	$2^{-59}/2^{17} + 2^{14}$	$2^{-57}/2^{27} + 2^{22}$	221	63
$Ch_q(M)$ $Sh_q - Sh_q$	$q = 2^{31}$	$2^{-29}/2^9 + 2^7$	$2^{-27,5}/2^{19} + 2^{14}$	$2^{-26}/2^{29} + 2^{24}$	124	31
	$q = 2^{63}$	$2^{-61}/2^8 + 2^6$	$2^{-59,5}/2^{18} + 2^{13}$	$2^{-58}/2^{28} + 2^{23}$	148	62

Список литературы: 1. Халимов Г.З. Каскадное универсальное хеширование с использованием АГК кодов / Халимов Г.З., Нохов А.Ю. // Восточно-европейский журнал передовых технологий. – Х., 2005. – Вып. 2/2(14). – С. 111–119. 2. Халимов Г.З. Багатократне універсальне хешування // Халимов Г.З. // Спеціальні телекомунікаційні системи та захист інформації : Зб. наук. праць. – Київ : ДССЗ та ЗІ, 2010. – Вип. 2(18). – С.43-49. 3. Torres F. The Deligne-Lusztig curve associated to the Suzuki group / F. Torres // arXiv:alg-geom/9706012v1 26Jun. – 1997. 4. Халимов Г.З. Универсальное хеширование по кривой Сузуки / Г.З. Халимов, Е.В. Котух // Прикладная радиоэлектроника. – Харьков : ХНУРЭ. – 2011. – Т.10, № 2. – С.80-86. 5. Халимов Г.З. Универсальное хеширование по кривой Сузуки / Г.З. Халимов, Е.В. Котух // Восточно-европейский журнал передовых технологий. – Х., 2011. – Вып. 3/9(51). – С. 10–15.

Харьковский национальный
университет радиоэлектроники

Поступила в редколлегию 25.08.2011

БОЛЬШИЕ ШИФРЫ – СЛУЧАЙНЫЕ ПОДСТАНОВКИ**Введение**

В этой работе речь идет об обосновании новой точки зрения по оценке безопасности блочных шифров к атакам дифференциального и линейного криптоанализа, пропагандируемой в работе [1].

Эта точка зрения появилась на основе развития нового подхода в теории и методах криптоанализа, родившегося на кафедре БИТ ХНУРЭ [2]. Он ориентирован, как уже было отмечено в [1], с одной стороны, на использование при определении ожидаемых показателей стойкости больших шифров результатов анализа уменьшенных их версий, а с другой, – уточненной в последнее время на основе изучения свойств и показателей случайных подстановок и уменьшенных моделей шифров, рассматриваемых как подстановочные преобразования, новой идеологии определения показателей стойкости БСШ к атакам дифференциального и линейного криптоанализа. Предлагаемая идеология основывается на подтвержденном многочисленными экспериментами с уменьшенными версиями современных шифров (DES, ГОСТ, Rijndael, Лабиринт, Мухомор, Калина, ADE, Камелия, FOX и многих других) положении, состоящем в том, что все эти шифры (и большие, и малые их версии) через определенное число циклов (для рассмотренных уменьшенных моделей – от трех циклов до девяти) независимо от используемых в шифрах S-блоков (речь идет не о вырожденных их конструкциях) приобретают свойства случайной подстановки (по комбинаторным показателям (числу инверсий, возрастаний и циклов), а также по законам распределения переходов XOR таблиц дифференциальных разностей (полных дифференциалов) и законам распределения смещений таблиц линейных аппроксимаций (линейных корпусов) они повторяют соответствующие показатели случайной подстановки [3 – 5]). Соответствующее свойство (переходный период к некоторому установившемуся значению полных дифференциалов и линейных корпусов отмечается в ряде публикаций и для больших шифров (например, в [6] для шифра Rijndael).

В отношении сохранения в малом шифре свойств большой модели следует отметить, что мы говорим лишь о сохранении свойств и показателей случайной подстановки. Можно считать, что при увеличении битового размера входа в шифр (с увеличением степени подстановки) ее соответствие асимптотическим законам распределения вероятностей (по инверсиям, возрастаниям и циклам), а также законам распределения вероятностей переходов таблиц полных дифференциалов и смещений таблиц линейных корпусов будет только повышаться. Тем не менее, находится немало скептиков, которые полагают, что то, что свойственно малым моделям шифров, совсем не обязательно присуще их большим прототипам.

В этой работе мы поставили задачу убедить сомневающихся, в том, что и большие шифры являются случайными подстановками. В дальнейшем речь будет идти только о дифференциальных показателях шифров, хотя соответствующие оценки можно получить и для линейных характеристик.

1. Стратегия анализа показателей случайности больших шифров

Очевидно, что построение закона распределения переходов таблицы полных дифференциалов для большого шифра является вычислительно нереализуемой задачей.

В этих условиях стратегия решения задач оценки показателей случайности больших шифров может быть только одна – суметь найти подтверждение желаемого результата на основе использования выборки ограниченного (приемлемого) объема. Изучить подходы к продвижению вперед в этом направлении и станет нашей ближайшей целью.

Вся таблица XOR разностей (ее A_{π} -я часть [3, 4]) для шифра с n -битным входом содержит $2^{n-1} \times 2^{n-1}$ ячеек, которые заполнены соответствующими значениями переходов входных

разностей ΔX в выходные разности ΔY . Для полного набора пар входов (пар открытых текстов) с заданной разностью ΔX , которая может принимать значения от 0 до 2^{n-1} , выходные значения – разности зашифрованных текстов ΔY для случайной подстановки при накоплении результатов счета могут принимать значения от 0 до $k^* \leq n + 4$ [3].

Заметим, что максимальное значение для каждой ячейки таблицы свое и может быть получено из полностью построенной таблицы разностей (при выполнении полного набора $2^n - 1 \times 2^n - 1$ экспериментов по вычислению отдельных переходов).

Если считать, события, состоящие в выборе пар со случайными значениями входов в таблицу $(\Delta X, \Delta Y)$, независимыми и равновероятными, можно убедиться, что для случайной подстановки порядка 2^n уже при $n = 64$ (например, если в качестве случайной подстановки рассматривать шифр ГОСТ 28147-89) уменьшение выборки до поддающегося вычислениям объема, равного $\sqrt{2^n} = \sqrt{2^{64}} = 2^{32}$, не позволяет получить какое либо нетривиальное значение перехода, превышающее единицу. Тем более, не осуществим анализ такого типа для шифров с большим битовым размером входа.

Таким образом, рассмотренная стратегия, ориентированная на построение выборки из случайного набора дифференциальных переходов для больших шифров, не перспективна.

Существует, однако, еще одна возможность формирования случайной выборки из дифференциальных переходов большого шифра. Можно анализировать значения переходов разностей не для всей дифференциальной таблицы шифра, а только для ее "пропорционально уменьшенной" части. Предполагается рассматривать, например, дифференциальную таблицу, получающуюся при использовании шифра для шифрования не n -битных блоков данных, а блоков, уменьшенных по размеру в 2 – 4 раза.

Большой шифр используется по типу малого для шифрования блоков данных уменьшенной длины (зашифрованные блоки данных тоже усекаются до необходимого размера), при этом сохраняются все преобразования и внутренние связи большого шифра. Примечательно при таком подходе то, что появляется возможность применить весь наработанный аппарат изучения показателей случайности малых версий шифров для изучения показателей случайности больших шифров.

Предлагаемый подход позволяет получить, по крайней мере, два полезных результата.

В первом случае можно использовать 16-битные блоки открытых и соответствующих им зашифрованных текстов. Здесь мы приходим к условиям, в которых исследовались малые модели шифров [7 – 9 и др.]. Вычислительных ресурсов здесь хватает для построения всей дифференциальной таблицы (большой шифр работает, как его уменьшенная 16-битная версия).

Очевидно, что при рассматриваемом подходе можно построить и строку смещений таблицы линейных аппроксимаций. Этого мало, но уже можно проверить совпадение теоретического и экспериментального законов распределения вероятностей переходов в строке (или нескольких строках) шифра и случайной подстановки соответствующей степени.

Во втором случае можно строить строки дифференциальной таблицы при использовании большого шифра для шифрования 32-битных блоков данных. Для таблиц линейных аппроксимаций удастся вычислить отдельные значения ячеек. Здесь открываются, на наш взгляд, перспективы для решения исследовательских задач и поиска ответов на вопрос, можно ли считать большие шифры случайными подстановками.

Дальнейший материал посвящен изложению результатов применения этой методики для исследования дифференциальных и линейных свойств шифров Rijndael (AES) и ГОСТ 28147.

2. Анализ показателей случайности больших шифров

Первый эксперимент был выполнен с использованием шифра Rijndael в режиме шифрования 16-битных блоков данных. Результаты этого эксперимента иллюстрирует табл.1.

Таблица 1
Поцикловые значения максимумов полных
дифференциалов при шифровании
16-битными блоками

Число циклов r	Значение максимума полного дифференциала	Средне-квадратическое отклонение
1	65536	0
2	3652,26	$\pm 630,312$
3	19,0666	$\pm 1,436$
4	19,0666	$\pm 0,99777$
5	18,8666	$\pm 1,23108$
6	19,1332	$\pm 0,99106$
7	19,2666	$\pm 1,0934$
8	19,1332	$\pm 1,431394$
9	19,0666	$\pm 1,23648$
10	19,3333	$\pm 1,2995$
11	19,4	$\pm 1,474222$
12	18,8666	$\pm 0,991072$
13	18,8666	$\pm 0,991072$
14	18,9332	$\pm 1,123486$

В процессе экспериментов осуществлялось зашифрование 16-битных блоков данных на 30 случайно выбранных ключах. Полученные результаты были усреднены по этому множеству ключей.

Из представленных результатов видно, что большой шифр Rijndael уже с третьего цикла шифрования приходит к установившемуся значению максимума полного дифференциала, повторяющему соответствующее значение (равное 19), свойственное случайной подстановке степени 2^{16} [4]. Видно, что это асимптотическое значение практически не зависит от используемых ключей зашифрования (среднеквадратическое отклонение не превышает 1,5). Отметим, что для уменьшенной до 16-битного входа модели шифра Rijndael асимптотическое значение (19) наступает после трех-четырех циклов (в зависимости от конструкции линейного преобразования).

В табл. 2 представлены результаты аналогичных экспериментов, выполненных с шифром ГОСТ.

Видно, что и в этом случае шифр становится случайной подстановкой, но теперь для этого ему необходимо девять циклов зашифрования. Обратим внимание, что девять циклов для большого шифра ГОСТ – эта для него глубина лавинного эффекта, – уже давно установленный параметр [10], свидетельствующий о наступлении момента, с которого изменение каждого бита входа начинает влиять на все выходные биты (при изменении любого бита входа начинает изменяться в среднем половина битов выходного текста). Заметим, что этот эффект выявлен и в уменьшенной модели этого шифра [11], что свидетельствует о том, что уменьшенная модель шифра повторяет свойства прототипа.

Следующим экспериментом стало вычисление закона распределения переходов для отдельной строки дифференциальной таблицы для 32-битного варианта использования рассматриваемых шифров. В табл. 3 приведен закон распределения вероятностей переходов строки дифференциальной таблицы для шифра ГОСТ с полным числом циклов (32). В этой таблице в левой колонке приведены результаты экспериментов, а в правой – результаты, полученные для случайной подстановки степени 2^{32} расчетным путем. Видно и без привлечения методов оценки близости распределений хорошее совпадение результатов.

В табл. 4 представлены аналогичные результаты для шифра Rijndael (при 14-цикловом шифровании). И в этом случае можно констатировать, что шифр Rijndael действительно можно считать случайной подстановкой.

В табл. 5 приводятся модульные значения максимальных смещений для шифра ГОСТ вместе со среднеквадратическими отклонениями.

Аналогичные результаты для шифра Rijndael иллюстрирует табл. 6.

Интересно отметить, что закон распределения переходов для строки случайной подстановки степени 2^n (в нашем случае 2^{32}) полностью повторяет закон распределения всей дифференциальной таблицы подстановки степени 2^{n-1} (в нашем случае 2^{16}).

Видно, что и 128-битный Rijndael тоже хорошо повторяет свойства случайных подстановок. В табл. 5, 6 представлены результаты экспериментов с определением линейных свойств наших шифров.

Таблица 2
Поцикловые значения максимумов полных дифференциалов при шифровании 16-битными блоками

Число циклов r	Значение максимума полного дифференциала	Средне-квадратическое отклонение
1	65536	0
2	65536	$\pm 12,934$
3	61952	$\pm 1278,614$
4	56008.6	$\pm 5181,74$
5	31358	$\pm 857,546$
6	2046.7	$\pm 637,692$
7	973.4	$\pm 29,7630$
8	52.2	$\pm 6,80882$
9	19.1	$\pm 0,97978$
10	19.5	$\pm 2,32664$
11	18.7	$\pm 0,86602$
12	18.9	$\pm 0,99498$
13	19.1	$\pm 1,16618$
14	19.4	$\pm 0,97978$
15	19.4	$\pm 1,337908$
16	19.3	$\pm 0,979796$
17	19.3	$\pm 1,07338$
18	19.4	$\pm 0,994988$
19	19.4	$\pm 0,95394$
20	19.9	$\pm 1,193216$
21	19.9	$\pm 1,176190$
22	19.10	$\pm 0,95394$
23	18.90	$\pm 1,083216$
24	19.30	$\pm 1,044552$
25	18.6	$\pm 0,979796$
26	19.2	$\pm 1,307670$
27	19.0	$\pm 1,179982$
28	19.9	$\pm 0,979796$
29	19.6	$\pm 1,729162$
30	19.1	$\pm 1,176190$
31	19.3	$\pm 1,356466$
32	19.1	$\pm 1,144552$

Таблица 3
Закон распределения переходов в строке таблицы дифференциальных разностей шифра ГОСТ в режиме шифрования 32-битных блоков данных

Значение перехода $2k$	Количество переходов (эксперимент)	Количество переходов (расчет)
0	2604902589	$2,6049 \times 10^9$
2	1302505752	$1,30245 \times 10^9$
4	325630272	$3,25612 \times 10^8$
6	54278054	$5,42687 \times 10^7$
8	6779658	$6,78359 \times 10^6$
10	679466	678359
12	56094	56529.9
14	4077	4037.85
16	253	252.366
18	10	14,0203
20	1	0,701016

Таблица 4
Закон распределения переходов в строке таблицы дифференциальных разностей шифра Rijndael в режиме шифрования 32-битных блоков данных

Значение перехода $2k$	Количество переходов (эксперимент)	Количество переходов (расчет)
0	2605041617	$2,6049 \times 10^9$
2	1302473402	$1,30245 \times 10^9$
4	325669098	$3,25612 \times 10^8$
6	54262758	$5,42687 \times 10^7$
8	6783634	$6,78359 \times 10^6$
10	676065	678359
12	56376	56529.9
14	4089	4037.85
16	232	252.366
18	16	14,0203
20	0	0,701016

Таблица 5

Цикловые значения максимумов смещений
линейных корпусов при шифровании
16-битными блоками для шифра ГОСТ 28147

Число Циклов r	Значение макси- мума смещения линейного кор- пуса	Средне- квадратиче- ское откло- нение
1	0	0
2	32768	0
3	17162	$\pm 1425,35$
4	31181,7	$\pm 2676,77$
5	16150,1	$\pm 1228,27$
6	16669,5	$\pm 3530,38$
7	2144,77	$\pm 374,142$
8	2380,93	$\pm 632,23$
9	826,833	$\pm 21,1157$
10	828,1	$\pm 22,4148$
11	823,767	$\pm 18,9573$
12	821,433	$\pm 28,5723$
13	826,067	$\pm 18,3556$
14	830,567	$\pm 27,4817$
15	818,833	$\pm 23,3539$
16	823,767	$\pm 23,8868$
17	821,7	$\pm 20,2075$
18	823,933	$\pm 21,9286$
19	819,3	$\pm 22,3967$
20	816,467	$\pm 17,5798$
21	815,567	$\pm 19,0817$
22	817,967	$\pm 20,9467$
23	820,067	$\pm 22,2844$
24	822,067	$\pm 16,7729$
25	823,333	$\pm 21,9109$
26	817,833	$\pm 17,6467$
27	823,967	$\pm 27,0549$
28	820,9	$\pm 24,6405$
29	824,467	$\pm 25,6239$
30	840,067	$\pm 35,3553$
31	823,333	$\pm 17,8612$
32	820,733	$\pm 18,6582$

Таблица 6

Поцикловые значения максимумов смещений
линейных корпусов при шифровании
16-битными блоками для шифра Rijndael

Число Циклов r	Значение мак- симула смеше- ния линейного корпуса	Средне- квадратиче- ское откло- нение
1	0	0
2	9284.27	$\pm 657,454$
3	818.467	$\pm 26,8809$
4	815	$\pm 28,204$
5	818.5	$\pm 18,536$
6	815.967	$\pm 20,18$
7	832.1	$\pm 33,1887$
8	823.133	$\pm 23,5722$
9	829.9	$\pm 33,5741$
10	827.4	$\pm 25,2885$
11	815.6	$\pm 22,3138$
12	819	$\pm 27,0025$
13	824.9	$\pm 23,7716$
14	821.2	$\pm 22,653$

Заключение

Представленные результаты свидетельствуют о том, что шифры Rijndael и ГОСТ28147-89 по своим дифференциальным и линейным показателям полностью укладываются в рамки случайных подстановок. Экспериментальные результаты хорошо согласуются с теоретическими, т.е. полностью подтверждается гипотеза о том, что большие шифры, как и малые их версии, после определенного числа циклов шифрования приобретают свойства случайных подстановок соответствующей степени.

Общий вывод, который напрашивается из представленных материалов, состоит в том, что не только Rijndael и ГОСТ, но и все другие известные итеративные шифры на полной цикловой длине обладают свойствами случайных подстановок. Мы тем самым подтвердили в известной степени общепринятую и естественную точку зрения о том, что всякий хороший шифр должен быть случайной подстановкой.

Список литературы: 1. Горбенко И.Д. Новая идеология оценки стойкости блочных симметричных шифров к атакам дифференциального и линейного криптоанализа / Горбенко И.Д., Долгов В.И., Лисицкая И.В., Олейников Р.В. // Прикладная радиоэлектроника. – 2010. – Т. 9, № 3. – С. 212-320. 2. Долгов В.И. Подход к криптоанализу современных шифров / Долгов В.И., Лисицкая И.В., Олейников Р.В. // Материалы второй междунар. конф. "Современные информационные системы. Проблемы и тенденции развития". – Харьков-Туапсе, Украина, 2–5 октября, 2007. – С. 435-436. 3. Олейников

Р.В. Дифференциальные свойства подстановок / Олейников Р.В., Олешко О.И., Лисицкий К.Е., Тевяшев А.Д. // Прикладная радиоэлектроника. – 2010. – Т.9. – № 3. – С. 326–333. 4. L. J. O'Connor. On the Distribution of Characteristics in Bijective Mappings. Advances in Cryptology. EUROCRYPT 93, Lecture Notes in Computer Science, vol. 795, T. Hellesehed., Springer-Verlag, pages 360–370, 1994. 5. Долгов В.И. Свойства таблиц линейных аппроксимаций случайных подстановок / Долгов В.И., Лисицкая И.В., Олешко О.И // Прикладная радиоэлектроника. – 2010. – Т.9. – № 3. – С. 334–340. 6. К. Ohkuma Security Assessment of Hierocrypt and Rijndael against the Differential and Linear Cryptanalysis/ К. Ohkuma, H. Shimizu, F. Sano, S. Kawamura // In Proceedings of the 2nd NESSIE workshop (2001). 7. Лисицкая И.В. Криптографические свойства уменьшенной версии шифра "Мухомор" / Лисицкая И.В., Олешко О.И., Руденко С. Н, Дроботько Е. В., Григорьев А. В. // Спеціальні телекомунікаційні системи та захист інформації : Зб. наук. праць. – Київ, 2010. – С. 31-42. 8. Долгов В.И. Исследование циклических и дифференциальных свойств уменьшенной модели шифра Лабиринт / Долгов В.И., Лисицкая И.В., Григорьев А.В. Широков А.В. // Прикладная радиоэлектроника. – 2009. – Т.8. №3 – С. 283-289. 9. Долгов В.И. Криптографические свойства уменьшенной версии шифра "Калина"/ Долгов В.И. Олейников Р.В. Большаков А.Ю, Григорьев А.В., Дроботько Е.В. // Прикладная радиоэлектроника. – 2010. – Т.9. – № 3. – С. 349–354. 10. Б. Шнаер. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М. : ТРИУМФ, 2002. – 816 с. 11. Лисицкая И.В. Исследование криптографических показателей уменьшенных моделей шифров ГОСТ и DES / Лисицкая И.В., Макаручук Я.В. // Прикладная радиоэлектроника. – 2011. – (в печати).

*Харьковский национальный
университет радиоэлектроники*

Поступила в редколлегию 15.08.2011

ОБГРУНТУВАННЯ ТА ВИБІР КРИТЕРІЇВ ТА ПОКАЗНИКІВ ОЦІНКИ КОМБІНОВАНИХ ІВК

Вступ

Як показали дослідження, побудову та розгортання інфраструктури відкритих ключів супроводжує ряд проблем. Аналіз зарубіжних публікацій показує, що деякі з недоліків можуть бути усунені за допомогою схем на ідентифікаторах, однак переваги, що надають ІВЕ схеми, теж не дозволяють уникнути ряду суттєвих недоліків.

Перспективним напрямком вдосконалення інфраструктури відкритих ключів є об'єднання ІВК і ІВЕ, що дозволяє створити нову схему, яка збереже переваги обох систем. Це об'єднання дозволить забезпечити захищений обмін повідомленнями між користувачами, як за допомогою сертифікатів відкритих ключів, так і без них.

Без ІВЕ, системи РКІ вимагають попереднього одержання сертифікатів перед початком захищеного інформаційного обміну. З ІВЕ користувач може зареєструватися в системі вже після отримання повідомлення, так як ідентифікатор користувача використовується в якості ключа шифрування. Іншим проблемним питанням є проблема довіри до уповноваженого на генерацію таємних ключів. Цю проблему можна вирішувати за допомогою розподілення уповноваженого на декілька центрів генерації ключів. Дослідження у цьому напрямку вже велися, але кожне рішення мало свої обмеження [1]. Також не існує методу, що дозволяє визначити необхідну кількість центрів генерації ключів.

Практичне впровадження цих альтернативних систем в Україні передбачає розв'язання наступних завдань:

1. Розробка критеріїв порівняння систем.
2. Розробка показників оцінки стійкості і складності протоколів, що лежать в їх основі.
3. Розробка методичних рекомендацій щодо інтеграції розглянутих схем в існуючу ІВК України.

Серед переваг ІВЕ можна виділити такі:

- в якості відкритого ключа користувача виступає відкритий ідентифікатор. Це дозволяє відмовитись від використання сертифікатів;
- не потребує реєстрації користувача до початку інформаційного обміну;
- дозволяє спростити процедуру відновлення секретного ключа;
- підтримує офф-лайн обмін (відправнику не треба перевіряти бази відкликаних сертифікатів);
- можливість інтеграції додаткових сервісів (анті-спам, перевірка на віруси, архівація);
- може використовуватися поряд з РКІ.

Тобто, можна говорити, що інфраструктура ІВЕ є більш простою та психологічно прийнятною для кінцевого користувача.

До основних недоліків ІВЕ можна віднести:

- необхідність довіри до уповноваженого на генерацію ключів;
- необхідність використання конфіденційного каналу для передачі таємних ключів користувачу;
- недостатньо досліджений математичний апарат та стійкість криптографічних перетворень, на яких ґрунтується ІВЕ;
- складна політика безпеки;
- складність впровадження та використання у великих (реальних) системах.

В цілому у новій архітектури досить багато недоліків, що стримує її широке використання.

Але завдяки своїй простоті (відкритий ключ є одночасно ідентифікатором користувача) ІВЕ системи гарно підходять для використання у невеликих компаніях, де:

- потрібний захищений документообіг;
- немає коштів і потреби у використанні сертифікатів;
- є необхідність у підключенні додаткових сервісів (антиспам, антивірус тощо);
- є необхідність у контролі документообігу з боку керівництва або є довіра до уповноваженого на генерацію ключів;
- кожен співробітник має унікальний ідентифікатор.

Для такої ситуації з вищезазначених проблем жодна не буде впливати на ефективність захисту.

1. Аналіз основних робіт

Очевидно, що з того моменту, як криптографічне співтовариство усідомило недоліки і переваги традиційних схем та схем на ідентифікаторах, були зроблені спроби створити якісно нові системи, які б володіли перевагами обох схем.

Однією з перших таких спроб була робота Girault [2], який запропонував схему, в якій відкриті ключі були б само сертифіковані. Таємний ключ користувач виробляє собі сам, а відкритий ключ обчислюється уповноваженим та користувачем. Але, як показала робота Saeednia [7], ця система має недоліки, які дозволяють уповноваженому обчислити таємний ключ користувача.

В схемі Girault довірений орган обчислює відкриті ключі користувачів, зв'язані з їх ідентифікаторами, не володіючи при цьому інформацією про їх секретні ключі.

Схема складається з трьох етапів:

- встановлення параметрів – виконується довіреним органом;
- генерація ключової пари – виконується відправником;
- етап ідентифікації – на цьому етапі одержувач ідентифікує відправника, затверджуючи його відкритий ключ.

1. Етап встановлення параметрів

На етапі встановлення параметрів довірений орган обирає набір параметрів:

- ціле число n , добуток двох простих чисел p і q , таких, що $p = 2fp' + 1$, $q = 2fq' + 1$, де f, p', q' – прості числа;

- ціле число b порядку f по модулю p і q ($b^f \pmod n = 1$);

- ціле число e , взаємно просте з $p-1$ і $q-1$.

Далі він обчислює $h = b^e \pmod n$ та $d, e \cdot d \equiv 1 \pmod{\lambda(n)}$.

Останнім кроком довірений орган параметри n, f, b, e, h оголошує відкритими, параметр d – секретним, а p і q – відкидаються.

2. Етап генерації ключової пари

Відправник генерує секретний ключ s , обчислює $v = b^{-s} \pmod n$ та відправляє v до уповноваженого на генерацію (УГ). УГ формує ціле l , на підставі ідентифікатора відправника, та обчислює його відкритий ключ, як: $P = \Gamma^d v \pmod n$.

3. Етап ідентифікації

- відправник генерує випадкове число $r \in \{0, \dots, f-1\}$, обчислює $x = h^r \pmod n$, та відсилає x та (P, l) до одержувача:

- одержувач перевіряє, чи відповідає l ідентифікатору відправника, генерує випадкове число $c \in \{0, \dots, e-1\}$ та відсилає c до відправника:

- відправник обчислює $y = r - sc \pmod f$ та відсилає y до одержувача:

- одержувач перевіряє рівняння $h^y (P^e \Gamma^c \pmod n) = x$, якщо воно виконується, тоді відкритий ключ відправника вважається дійсним.

Таким чином, можна виділити основні кроки схеми Girault:

- 1) УГК формує набір відкритих параметрів n, f, b, e, h , та передає їх до А; параметр d – зберігає в секреті.

- 2) А генерує секретний ключ s , за допомогою якого обчислює v , відправляє v до УГК.
- 3) УГК, використовуючи отримане v та ціле I (по суті ідентифікатор), обчислює відкритий ключ P та відправляє його до А.
- 4) Потім йде автентифікація відкритого ключа користувача А користувачем В:
 - А формує x , відправляє x свій ідентифікатор I та відкритий ключ P до В;
 - В перевіряє дійсність ідентифікатора I , формує випадкове c та відправляє c до А;
 - А за допомогою отриманого c обчислює y та відправляє його до В;
 - В перевіряє рівняння $h'(P^e I)^c \pmod n = x$, якщо воно виконується, тоді відкритий ключ А вважає дійсним.

Можна зробити висновок, що для виконання цієї схеми необхідна інтерактивна взаємодія користувачів між собою, але завдяки цьому забезпечується явна автентифікація відкритого ключа користувача А.

Shahrokh Saeednia та Rei Safavi-Naini [7] запропонували дві атаки на схему Girault, що дозволяють зловмиснику сформуванати ідентифікатор, та відповідний йому відкритий ключ, без знання секретного значення довіреного органу. Перша атака можлива завдяки властивості $I^{2f} = 1 \pmod n$ ідентифікатора I . Тобто, ця атака працює для всіх ідентифікаторів I , що мають порядок 2, f і $2f$. Якщо даний ідентифікатор I має один із цих порядків, тоді можна обчислити відкритий ключ, пов'язаний з ним, не маючи секретного значення довіреного органу. Друга атака можлива, якщо можна знайти ідентифікатори I_1, I_2 , такі, що $I_3 = I_1 I_2$, які відповідають дійсним ідентифікаторам. Атака може бути реалізована будь-якою підмножиною користувачів, які дійсно мають відкритий і закритий ключі пов'язані з їх ідентифікаторами.

В 2003 році С. Gentry [3] запропонував комбіновану схему на базі білінійних спарювань з використанням СВК.

Схема складається з чотирьох етапів:

- 1) setup – встановлення системних параметрів, виконується довіреним органом;
- 2) certification – сертифікація відкритого ключа користувача, виконується довіреним органом під час інтерактивної взаємодії з користувачем;
- 3) encrypt – зашифрування, виконується відправником;
- 4) decrypt – розшифрування, виконується одержувачем.

1. Етап встановлення системних параметрів:

На етапі встановлення параметрів довірений орган обирає набір параметрів:

- генерується груп G_1, G_2 , простого порядку q , та $\hat{e}: \langle G_1, G_1 \rangle \rightarrow G_2$ – оператор спарювання в групі точок еліптичної кривої;
- генерується базова точка $P \in G_1$;
- випадково обирається секретне значення $s_C \in \mathbb{Z}/q\mathbb{Z}$ та розраховується $Q = s_C P$;
- обираються дві геш-функції: $H_1: \{0,1\}^* \rightarrow G_1$, $H_2: G_2 \rightarrow \{0,1\}^n$, де n – довжина повідомлення.

Системними параметрами є: $params = \langle G_1, G_2, \hat{e}, n, P, Q, H_1, H_2 \rangle$, $s_C \in \mathbb{Z}/q\mathbb{Z}$ – секретне значення довіреного органу.

2. Етап сертифікації

- отримувач відправляє довіреному органу свої ідентифікаційні дані I , в тому числі свій відкритий ключ $s_{omp} P$;
- довірений орган перевіряє інформацію отримувача, якщо перевірка пройдена успішно, обчислює $P_{omp} = H_1(s_C P, i, I) \in G_1$ за час i ;
- довірений орган формує сертифікат $Cert_{omp} = s_C P_{omp}$ і відправляє його одержувачу.

Перед початком розшифрування, отримувач повинен здійснити процедуру підписання I , на виході якої буде $s_{omp} P'_{omp}$, де $P'_{omp} = H_1(I)$, де $S_{omp} = s_C P_B + s_{omp} P'_{omp}$ – це комбі-

нований підпис для двох осіб. Відправник буде використовувати цей комбінований підпис у якості ключа розшифрування.

3. Етап зашифрування

Відправник виконує наступні дії:

- 1) обчислює $P'_{omp} = H_1(I) \in G_1$;
- 2) обчислює $P_{omp} = H_1(s_C P, i, I) \in G_1$.
- 3) випадково обирає $r \in Z/qZ$.
- 4) виробляє зашифрований текст:

$$C = [rP, M \oplus H_2(g^r)], \text{ де } g = \hat{e}(s_C P, P_{omp}) \hat{e}(s_{omp} P, P'_{omp}) \in G_2.$$

4. Етап розшифрування

- 1) одержувач виробляє підпис для даних I , на виході якого буде $s_{omp} P'_{omp}$, де $P'_{omp} = H_1(I)$. де $S_{omp} = s_C P_B + s_{omp} P'_{omp}$ – це комбінований підпис для двох осіб;
- 2) одержувач розшифровує повідомлення: $M = V \oplus H_2(\hat{e}(U, S_{omp}))$, $C = \langle U, V \rangle \in C$ – зашифрований текст.

Особливість цієї схеми полягає в використанні комбінованого підпису у якості ключа розшифрування, та у використанні сертифікату, який виробляється довіреним органом, у якості відкритого ключа. При цьому користувач власноруч генерує собі секретний ключ. Серед недоліків цієї схеми можна зазначити невизначеність механізму відновлення ключів та складність вироблення спільного підпису (необхідність попереднього з'єднання між користувачами).

Al-Riyami та Paterson [4] запропонували схему шифрування без сертифікатів (CLE – Certificateless Encryption Scheme), що реалізовується за сім етапів:

1. Встановлення системних параметрів (Setup)

Результатом цього кроку є наступні системні параметри:

$$params = \langle G_1, G_2, e, n, P, P_0, H_1, H_2, H_3, H_4 \rangle.$$

Простір зашифрованого тексту визначається як $C = G_1 \times \{0,1\}^{2n}$.

2. Розрахунок часткового секретного ключа (Partial-Private-Key-Extract)

- 1) $Q_A = H_1(ID_A) \in G_1^*$, де $ID_A = \{0,1\}^*$ – ідентифікатор отримувача;
- 2) частковий секретний ключ: $D_A = sQ_A \in G_1^*$.

Отримувач може перевірити правильність виробленого часткового секретного ключа, перевіривши рівняння: $e(D_A, P) = e(Q_A, P_0)$.

3. Встановлення секретного значення (Set-Secret-Value)

На вхід алгоритму надходять системні параметри $params$ та ідентифікатор отримувача ID_A . Алгоритм випадково обирає $x_A \in Z_q^*$, та встановлює його як секретне значення отримувача.

4. Встановлення секретного ключа (Set-Private-Key)

На вхід алгоритму надходять $params$, частковий секретний ключ отримувача D_A та секретне значення отримувача $x_A \in Z_q^*$. Алгоритм перетворює частковий секретний ключ D_A у повний секретний ключ S_A шляхом обчислення: $S_A = x_A D_A = x_A s Q_A \in G_1^*$.

5. Встановлення відкритого ключа (Set-Public-Key)

На вхід алгоритму подаються $params$, $x_A \in Z_q^*$, на виході – сформований відкритий ключ, як: $P_A = \langle X_A, Y_A \rangle$, де $X_A = x_A P$ та $Y_A = x_A P_0 = x_A s P$.

6. Зашифрування (Encrypt)

Для того, щоб зашифрувати повідомлення M , відправнику потрібно мати $ID_A = \{0,1\}^*$.
 $P_A = \langle X_A, Y_A \rangle$, результатом цього кроку є вироблення криптограми
 $C = \langle r, P \cdot \sigma \oplus H_2(e(Q_A, Y_A)^r), M \oplus H_4(\sigma) \rangle$.

7. Розшифрування (Decrypt)

Використовуючи секретний ключ відправника S_A одержувач розшифровує повідомлення та в результаті отримує відкритий текст.

Основна ідея схем CLE полягає в особливостях формування секретного ключа користувача. Генерація секретного ключа користувача здійснюється шляхом використання двох компонент:

- перша компонента секретного ключа, або частковий секретний ключ (PPK – partial private key), генерується Ω на основі майстер-ключа;
- друга компонента – секретне значення користувача.

Користувач публікує також відкритий ключ, отриманий з секретного значення. Відправник, який хоче зашифрувати повідомлення, повинен мати лише відкритий ключ і ID одержувача, а також відкриті параметри центру генерації ключів.

Схема CLE дозволяє будь-якому користувачеві зашифрувати повідомлення для окремого одержувача, використовуючи відкриту інформацію (подібно PKI і IBE) без використання сертифікатів.

Існують і інші погляди на проблемні питання криптографії на ідентифікаторах. Наприклад, J. Callas [5] зазначає, що, по-перше, проблема анулювання сертифікатів у сучасному світі вже не стоїть гостро, і в подальшому, можливо, зовсім зникне. Це пов'язано з тим, що сьогодні можливості комп'ютерів зросли, а необмежений доступ до глобальної мережі вже не виняток, а реальність. Це зауваження деякою мірою ставить під сумнів один з найважливіших переваг IBE – відсутність сертифікатів (і відповідно off-line роботу). По-друге, використання унікальних та простих для запам'ятовування ідентифікаторів теж породжує деякі проблеми. Це, з одного боку, дає можливість зломиснику (чи соціальному інженеру) досліджувати структуру організації, де використовують таку IBK, і отримувати інформацію про її службовців. Друга проблема полягає в тому, що отримати ідентифікатор користувача системи набагато легше (тому що він загальновідомий) і, відповідно, обчислити відкритий ключ теж дуже легко. А це вже дозволить спамерам направлено шифрувати повідомлення, будучи впевненими, що воно дійде до адресату.

J. Callas запропонував рішення, яке, на його погляд, вирішувало зазначені ним недоліки та було найбільш ефективним. Він відмовився від використання сертифікату як такого, замінивши його відповіддю (скоріш за все, підписаною) сервера.

Наведемо його схему:

1. УГК обирає таємний ключ.
 2. УГК генерує IDT (цифровий відбиток ідентифікатора), використовуючи свій таємний ключ в якості простого секрету.
 3. УГК обирає детермінований псевдовипадковий генератор, який ініціалізується за допомогою IDT. Цей генератор повинен видавати ключову пару (відкритий ключ, таємний ключ). Він також може бути будь-яким асиметричним криптографічним перетворенням.
- Схема дійсно ставить у відповідність будь-якому ідентифікатору відповідну ключову пару та може використовувати відомі та перевірені криптопримітиви.

Процедура видачі ключів, згідно цієї схеми, буде наступна:

- 1) УГК виробляє IDT для кожного ID.
- 2) УГК ініціалізує рандомізований генератор (RNG) початковим значенням, рівним IDT.
- 3) УГК генерує ключову пару за допомогою RNG.
- 4) Якщо УГК отримує неавтентифікований запит для будь-якого ID, він повертає відкритий ключ Аліси. Це трапляється, коли Боб хоче дізнатися відкритий ключ Аліси.

5) Якщо УГК отримує автентифікований запит для будь-якого ID, він повертає таємний ключ. Це трапляється, коли Аліса хоче отримати свій таємний ключ.

Механізми автентифікації та захисту каналу зв'язку не уточнюються. По суті, від стандартної IBK на ідентифікаторах відрізняється лише тим, що:

- користувачі виробляють відкриті ключі не самостійно, а роблять запит до уповноваженої сторони;
- можливо використовувати будь-які відомі криптопримітиви.

Проведемо аналіз переваг такої схеми. Тепер зломисник не має можливості самостійно генерувати або визначати відкриті ключі користувачів, йому прийдеться відправляти запит на сервер. Крім того, для такої схеми можна використовувати відомі криптопримітиви, які вже пройшли перевірку часом.

Серед недоліків можна відзначити:

1) Необхідність чітко визначати та застосовувати механізми перевірки цілісності та справжності переданої інформації. Це пов'язано з тим, що відповідь УГК, навіть на запит зовнішнього користувача, повинна бути підписана (для забезпечення цілісності переданого відкритого ключа).

2) Так і не вирішена проблема відповідності єдиного відкритого ключа різним ідентифікаторам, тому що, згідно з запропонованою схемою, різним ідентифікаторам відповідають різні *IDT*, а тому і різні відкриті ключі.

3) Значно більше навантаження на УГК (порівняно з IBE), якщо він буде генерувати ключі навіть на неавтентифікований запит.

4) Крім того, зломисники все рівно зможуть отримувати доступ до відкритих ключів користувачів, тому що вони мають можливість зробити неавтентифікований запит на сервер (якщо це дозволяють правила мережевого екрану).

Ця схема нагадує скоріше не IBK на ідентифікаторах, а традиційну IBK, де користувачі здійснюють пошук сертифіката по ключовому полю (яким, по суті, є ідентифікатор). Для великих систем цю систему недоречно використовувати, тому що вона має основний недолік PKI – необхідністю довіри до УГК.

Компанія Voltage [6] запропонувала комбінацію IBE та PKI, яка має наступну архітектуру та особливості (див. рисунок):

1. Користувач володіє сертифікатом PKI та ключами IBE (або чимось одним).

2. Сертифікати використовуються для автентифікації користувача та накладання цифрового підпису

3. Ключі IBE використовуються для шифрування.

Відповідно, змінюються етапи при зашифруванні повідомлення:

1. Користувач А отримує сертифікат відкритого ключа PKI.

2. Маючи в якості вхідних даних загальносистемні параметри та ідентифікатор одержувача В, А направлено шифрує повідомлення та підписує його на своєму таємному ключі IBE.

3. В надсилає запит до УГК на генерацію таємного ключа.

4. УГК перевіряє автентичність В, перевіряючи його сертифікат.

5. УГК генерує та надсилає В його таємний ключ.

6. В перевіряє цифровий підпис А, перевіряючи сертифікат А.

7. В розшифровує повідомлення.

Сильними сторонами такої системи, на думку компанії Voltage, буде:

1. Відмова від перевіряння відправником сертифікату одержувача (тепер це входить до обов'язків УГК).

2. Можливість взаємодії користувачів з сертифікатами та без них.

3. Можливість підключення додаткових сервісів.

4. Спрощення процедури анулювання сертифікату.

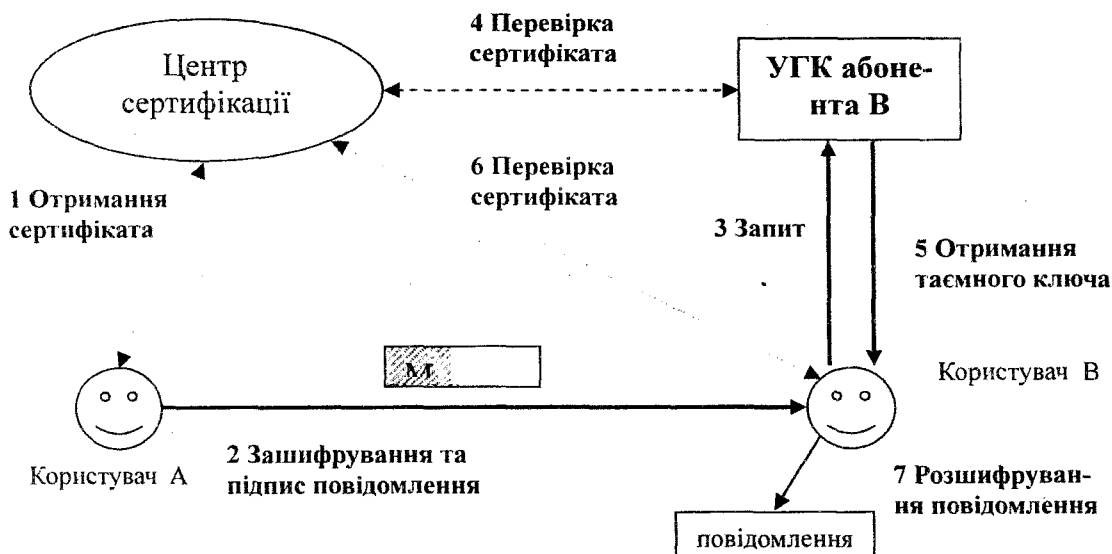


Схема взаємодії користувачів IBE+PKI Voltage

Необхідно зауважити, що:

1. Ця система може використовуватися, як надбудова над PKI.
2. Для повноцінної взаємодії користувачі повинні мати сертифікати.
3. Якщо користувачі обслуговуються різними УГК, вони мають отримувати цілісні загальні параметри цих УГК.
4. Одержувач інформації усе рівно повинен перевірити сертифікат відправника для верифікації його підпису.
5. Користувач, який не має сертифікату, може приймати повідомлення від інших користувачів, але він не має можливості підписувати повідомлення (або тільки на ключах IBE) та повинен деяким чином проходити автентифікацію на УГК. Крім того, він повинен власноруч отримувати відкриті параметри УГК одержувача.

6. УГК повинні довіряти усім користувачам, тому що він має доступ до таємних ключів.

Чим краща, ніж звичайна PKI:

- 1) Відправнику не потрібно перевіряти сертифікат одержувача.
- 2) Можна налагодити взаємодію між користувачами з сертифікатами та без.

Чим гірше:

- 1) УГК кожного користувача може розшифровувати повідомлення.
- 2) Користувачі повинні бути зареєстровані в УГК (або пройти автентифікацію, кожен раз, коли отримують ключі).

Тобто виходить, що навіть ті користувачі, які мають сертифікат, повинні довіряти УГК. Це значний недолік, що не дозволить цій системі розвиватися. Тому ця система не відповідає висунутим вимогам, що дозволяє говорити про недоречність її використання у реальному середовищі.

2. Обґрунтування та вибір критеріїв та показників оцінки комбінованих ІВК

Спочатку сформулюємо безумовні критерії оцінки комбінованої інфраструктури відкритих ключів.

- 1) Повинна бути реалізована модель взаємної недовіри та взаємного захисту.
- 2) Для захисту інформації у відкритих каналах зв'язку повинні використовуватися криптопримітиви зі складністю розкриття не менше експоненційної (а для внутрішніх мереж – не менше субекспоненційної).

3) Захищеність протоколів генерації та видачі ключа, що лежить в основі комбінованої ІВК, від аналітичних атак (тобто атак, що мають за мету порушити нормальний хід протоколу і скривдити цілі безпеки).

Також, для більш детального аналізу наведених схем, пропонуються наступні умовні критерії:

1. Рівень довіри до ІВК (згідно Girault).
2. Необхідність використання сертифікатів.
3. Порядок генерації відкритого ключа.
4. Порядок генерації таємного ключа.
5. Необхідність взаємодії між користувачами у реальному часі.
6. Необхідність взаємодії з сервером у реальному часі.
7. Кількість проходів / взаємодій між користувачами та сервером.
8. Автентифікація відкритого ключа.

Згідно з наведеними критеріями було проведено порівняльний аналіз наведених гібридних схем, результати якого увійшли у таблицю.

Схема Критерій	Girault	Gentry	Al-Riyami, Paterson	J. Callas	Voltage
1	2	3	3	1	1
2	-	+	-	- (підпис)	+/-
3	УГК	УГК	користувач	УГК	УГК
4	користувач	відправник одержувач	спільно з УГК	УГК	УГК / користу- вач
5	+	+	-	-	+
6	+	+	-	+	+
7	5	5	3	1	7
8	відправника	+	-	-	+

Висновки

Перспективним напрямком вдосконалення інфраструктури відкритих ключів є об'єднання ІВК і ІВЕ, що дозволяє створити нові схеми, які збережуть переваги обох систем.

Пропонується порівняння комбінованих інфраструктур здійснювати на основі використання інтегрального безумовного та інтегрального умовного критеріїв. При цьому інтегральні критерії можна обчислювати на основі часткових критеріїв.

Запропоновані безумовні критерії забезпечують вибір інфраструктури, яка буде безпечною з точки зору криптографічної стійкості, формальної стійкості криптографічних протоколів, та буде реалізовувати модель взаємної недовіри та взаємного захисту. За наведеними умовними критеріями можна провести порівняння та вибрати схему, що буде найбільш підходити до конкретного випадку.

Список літератури: 1. Бондаренко М.Ф., Горбенко І.Д., Мелецький О.П., Кравченко П.О. Аналіз та перспективи сучасних протоколів видання та генерації ключів для інфраструктури на базі ідентифікаторів // Прикладная радиоэлектроника. – 2007. – Т. 6, №3. – С. 356-362. 2. M. Girault: Self-Certified Public Keys // Eurocrypt. – 1991: 490-497 3. S. Al-Riyami. K. Paterson. Certificateless public key cryptography. – 2003. 3. C. Gentry. Certificate-based encryption and the certificate revocation problem. 2003. 4. K. Paterson. Cryptography from pairings: a snapshot of current research. 2002. 5. J. Callas Identity-Based Encryption with Conventional Public-Key Infrastructure. PGP Corporation Palo Alto, California, USA, 2005. 6. Voltage Security. Identity-Based Encryption and PKI Making Security Work. 2005. 7. S Saeednia. R. Safavi-Naini. On the security of Girault's identification scheme // 1998 International Workshop on Practice and Theory in Public Key Cryptography (PKC'98). – 1998. – P 114-118.

АНАЛІЗ ВИМОГ ДО ГЕНЕРАТОРІВ ВИПАДКОВИХ І ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ, ВСТАНОВЛЕНИХ В СТАНДАРТАХ AIS 20 ТА AIS 31

Вступ

У зв'язку з розвитком інформаційно-телекомунікаційних систем усе більше актуальними стають задачі побудови надійних систем обробки інформації з функціями криптографічного захисту інформації. Один з найважливіших елементів цих систем, з точки зору забезпечення високого рівня захищеності, є засоби генерації ключів та параметрів. На сучасному етапі засоби генерації ключів будуються на основі генераторів випадкових послідовностей (ГВП) (недетермінованих) та псевдовипадкових (детермінованих) послідовностей (ПВП). Вони майже завжди входять до складу криптографічних засобів, прикладом їх використання є генерація ключів, загальносистемних параметрів, випадкових чисел, які використовуються для забезпечення захисту від повторної передачі повідомлень, при виконанні різноманітних протоколів, тощо. Саме тому аналіз та розробка засобів оцінки властивостей генераторів випадкових послідовностей є дуже актуальним та важливим напрямком досліджень.

Задача оцінки ГВП виникла у зв'язку з необхідністю використання при розробці технічних рішень спеціальних методів оцінки, які базуються на ряді керівних принципів. Аналіз показав, що для вирішення цих задач у Німеччині прийняті нормативні документи відповідно для оцінки ПВП застосовується AIS 20 [1], а для ГВП AIS 31 [2]. При їх розробці були враховані основні положення й досвід застосування федеральних стандартів США FIPS 140-1 [3] і FIPS 140-2 [4]. Обидва ці документи містять критерії для оцінки детермінованих генераторів випадкових послідовностей (ДГВП). Основна ідея полягає в тому, що придатність ДГВП повинна бути оцінена з урахуванням криптографічних засобів, у яких вони використовуються.

Метою даної статті є аналіз основних положень AIS 20 і AIS 31 та визначення можливостей їх застосування в Україні при розробці ДГВП.

1. Аналіз загальних положень AIS 20

В AIS 20 визначені вимоги до ДГВП. Такий генератор генерує псевдо випадкові числа, які залежать виключно від ініціюючого внутрішнього стану. Логічна структура генератора й процес вибору початкового числа визначаються п'ятьма параметрами (S, R, φ, ψ, p_A). Ці параметри мають такі визначення (табл.1):

Таблиця 1

Параметри	Визначення параметрів
S	кінцева множина можливих внутрішніх станів ГВП
R	множина можливих вихідних значень (випадкові числа)
φ	функція стану
ψ	функція виходу
p_A	імовірнісна міра, що описує розподіл випадкової величини, яка використовується як початкове значення

На кроці $n > 1$ внутрішній стан спочатку модифікується за допомогою використання виразу $s_n := \varphi(s_{n-1}) \in S$, після цього випадкове число $r_n := \psi(s_n)$ розраховується та подається на вхід перетворення.

Оскільки різні криптографічні системи висувають різні вимоги до випадкових чисел, то необхідно оцінювати відповідність конкретної системи до вимог, які встановлені для систем цього класу. Саме такий підхід було реалізовано в AIS 20. В цьому нормативному документі представлено чотири ієрархічних функціональних класи. Кожен наступний клас містить

більш високий рівень вимог до вихідних послідовностей, а саме він включає в себе усі вимоги попереднього класу і додає нові вимоги до ДГВП. Ці класи також впорядковані в залежності від вимог до криптосистем, в яких ДГВП буде використовуватися.

1.1. Вимоги до ДГВП класу K1

K1 (i) вимагає щоб ймовірність того, що вектори $(r_1, \dots, r_c), (r_{c+1}, \dots, r_{2c}), \dots, (r_{M-c+1}, \dots, r_M)$ парно різні, повинна бути, принаймні, $1 - \varepsilon$

Якщо $\varepsilon = 0$, то стійкість механізму визначається як "висока".

В інших випадках застосовуються наступні умови:

- $M^2/c^2 \varepsilon > 2^{52}$ та $\varepsilon < 2^{-16}$: стійкість механізму "висока";
- $M^2/c^2 \varepsilon > 2^{32}$ та $\varepsilon < 2^{-12}$: стійкість механізму "середня";
- $M^2/c^2 \varepsilon > 2^{20}$: стійкість механізму "низька".

Вибір параметрів c , ε та M залежить від призначення криптографічної системи. Прикладом систем, в яких застосовується ДГВП такого класу, можуть бути будь які інтерактивні протоколи.

1.2. Вимоги до ДГВП класу K2

ДГВП повинен задовольняти вимозі K1 (i). А також K2 (ii), яка вимагає, щоб випадкові числа, які генеровані ДГВП, мали статистичні властивості такі, як і випадкові числа, які генеровані ідеальним ГВП.

K2 (ii) – послідовності випадкових чисел $r_1, r_2, \dots$ та їх бітові представлення повинні задовольняти статистичним тестам T1 – T5, які наведені в додатках до AIS 20. Якщо ДГВП проходить всі індивідуальні тести, тоді підтверджується, що ДГВП задовольняє вимозі K2 (ii). Якщо більш ніж один індивідуальний тест не пройдений, то вважають, що ДГВП не задовольняє вимозі K2 (ii).

Якщо тільки один тест не пройдений, то весь порядок тестування повинен бути повторений, і якщо на цей раз ДГВП проходить всі тести, то підтверджується, що він задовольняє вимозі K2 (ii). Друге повторення тестування не дозволяється.

Метою застосування класу K2 є виключення кореляційних атак на криптографічні алгоритми, що засновані на використанні статистично слабких випадкових чисел (випадкових ключів).

Прикладом криптографічних систем з ДГВП класу K2 є потокові шифри.

1.3. Вимоги до ДГВП класу K3

ДГВП повинен задовольняти вимогам K1 (i) та K2 (ii). Крім того висуваються нові вимоги K3 (iii) та K3 (iv), які полягають в тому, що:

K3 (iii) Якщо стійкість механізму "висока", то $H(p) \geq 80$; для "середньої" стійкості механізму – $H(p) \geq 48$. Ентропія p_A обчислюється як: $H(p) = -\sum_{s \in S} p_A(s) \log_2(p_A(s))$.

K3 (iv) Повинне бути фактично неможливо обчислити або вгадати попереднє r_{i-1} або наступне r_{i+j+1} з відомої підпослідовності $r_i, r_{i+1}, \dots, r_{i+j}$, ($i + j \leq M$), а також обчислити або вгадати внутрішній стан. Потенціал передбачуваних атак супротивника залежить від стійкості механізму. Навіть при використанні сучасних передових знань імовірність атаки (реалізована прийнятним частковим методом перебору) може бути незначно більше чим, якби підпослідовність була би невідомою. Передбачається, що супротивник знає параметри (S, R, ϕ, ψ, p_A) , однак він не знає ніяких внутрішніх станів $s_0, s_1, \dots, s_M$.

Метою K3 є захист проти відновлення попередніх випадкових чисел і вгадування наступних з відомої підпослідовності.

Можливі криптографічні системи, в яких можуть використовуватися ДГВП K3:

1. генерація ключів;
2. генерація підпису DSS (секретний ключ x або випадкове число k);
3. генерація паролів.

1.4. Вимоги до ДГВП класу K4

ДГВП повинен задовольняти вимогам K1 (i), K2 (ii), K3 (iii), K3 (iv), та висувається нова вимога K4 (v), яка полягає в тому, що має бути фактично неможливо виробити попереднє випадкове число r_{i-1} знаючи внутрішній стан s_i . Потенціал передбачуваних атак супротивника залежить тут від стійкості механізму. Навіть використовуючи сучасні передові знання, імовірність атаки (реалізована прийнятним частковим методом перебору) може бути незначно більше чим, якби s_i було б не відомо. Передбачається, що супротивник знає параметри (S, R, ϕ , ψ , p_A).

Метою K4 є захист проти відновлення попередніх випадкових чисел з відомого внутрішнього стану.

ДГВП класу K4, можуть використовуватися в наступних криптографічних системах:

4. генерація ключів;
5. генерація підпису DSS (секретний ключ x або випадкове число k);
6. генерація сеансових ключів для симетричних криптографічних механізмів;
7. генерація паролів.

1.5. Аналіз класів K1 – K4 та вимог що вони встановлюють

Аналізуючи класи ДГВП можна зробити висновок, що класи є ієрархічно залежними, тобто кожен наступний повністю включає в себе попередній та доповнює своїми новими вимогами (табл. 2).

Таблиця 2

Функціональний клас	Вимоги до ДГВП	Криптографічні системи в яких застосовуються ДГВП такого класу
K1	K1(i)	Інтерактивні протоколи
K2	K1(i) + K2(ii)	Потокові шифри
K3	K1(i) + K2(ii) + K3(iii) + K3(iv)	Генерація ключів, генерація цифрового підпису DSS (секретний ключ x або випадкове число k), генерація паролів.
K4	K1(i) + K2(ii) + K3(iii) + K3(iv) + K4(v)	Генерація ключів, генерація цифрового підпису DSS (секретний ключ x або випадкове число k), генерація сеансових ключів для симетричних криптографічних механізмів, генерація паролів.

Вказані вимоги встановлюють всі рівні захищеності, як від найменшого (використання ДГВП як лічильника), так і найвищого (аналітик, навіть при знанні певних внутрішніх станів генератора, не може скомпрометувати усю послідовність). Методика тестування, що викладена в AIS 20, може застосовуватись як в реальному часі, так і в процесі досліджень, а також для технологічного тестування.

2. Аналіз загальних положень AIS 31

В AIS 31 представлені критерії оцінки криптографічних властивостей генераторів випадкових чисел. Оцінка фізичних генераторів випадкових послідовностей (ФГВП) ґрунтується в основному на статистичних тестах. На основі різних можливих сценаріїв атак можна розробити вимоги до властивостей зовнішніх і відповідно внутрішніх випадкових чисел. Беручи до уваги ці обставини в AIS 31 уведено 2 класи функціональності (P1, P2).

В AIS 31 враховані вимоги якісного перевіряння на випадковість та можливості оперативного тестування. Перевірка здійснюється на відповідність функціональним класам P1 та P2.

При перевірці на відповідність P1 використовуються тести, що були взяті в FIPS 140-1, але додатково введено авто кореляційний тест, що дозволяє перевірити кореляції між послідовністю та зсувом цієї ж послідовності.

При перевірці на відповідність до P2 додатково використовуються три тести: тест перевірки рівномірного закону розподілу, порівняльний тест для поліноміальних розподілів та ентропійного тестування.

2.1. Вимоги до ДГВП класу P1

Для відповідності класу P1 повинні виконуватися вимоги P.1 (i) – P.1 (vi) в відповідності до механізмів та функцій стійкості.

P.1 (i) вимагає, щоб послідовність випадкових векторів, створена з внутрішніх випадкових чисел (ВЧ) $r_1, r_2, \dots$ з великою ймовірністю являються попарно різними.

Для верифікації вимоги P.1 (ii) внутрішня послідовність ВЧ $r_1, r_2, \dots$ та їх проекції на окремі біти повинні задовольняти статичним тестам T1-T5.

Для P.1 (iii), якщо при увімкненні ДГВП відбувається загальна зупинка джерела шуму, то ця зупинка повинна бути автоматично розпізнана та після зупинки не можуть бути подані зовнішні ВЧ.

Для P.1 (iv), якщо під час роботи ДГВП виникає загальна зупинка джерела шуму, то після зупинки припиняється виробка випадкових значень, що вироблюються внутрішньою випадковою послідовністю. В якості заміни достатньо, щоб після загальної зупинки джерела шуму ДГВП вів себе для кожної постійної послідовності сигналів шуму як K2-ДГВП AIS 20, вихідні послідовності якого відповідають передбаченій меті застосування.

P.1 (v) вимоги в P.1 (i) і P.1 (ii) повинні бути перевірені при наперед визначених зовнішніх впливах, так як вони можуть впливати на функціонування джерела шуму.

Для P.1 (vi) ДГВП повинен містити *online*-тест, котрий по зовнішньому виклику перевіряє якість внутрішніх ВЧ.

Після запуску апаратний генератор шуму починає виготовляти блоки необроблених випадкових байтів. Для негайного виявлення несправностей фізичного джерела шуму на старті повинні застосовуватися повні статичні випробування (*online*-тест). Тільки в випадку успіху ФГВП доходить до стандартного режиму роботи і стає доступним елементом криптографічної системи. В стандартному режимі *online*-тест застосовується до кожного генерованого блоку випадкових байтів. Якщо тестування пройдене, ФГВП повернеться до робочого режиму. Інакше ФГВП буде заблоковано, і, відповідно, усі запити, що використовують ФГВП, будуть повернені з відповідним кодом помилки. Під час роботи кінцевого об'єкту оцінки повинне виконуватися неперервне тестування ФГВП для перевірки коректності його роботи.

Можливі застосування ФГВП P1:

- відкриті, змінні вектори ініціалізації (сінхро послідовності);
- генерація начального стану для ДГВП класів K1 та K2 AIS 20.

2.2. Вимоги до ДГВП класу P2

ДГВП повинен належати класу P1 як мінімум з такими ж механізмами та функціями стійкості.

P.2 (i) Перевірка властивостей P1.

P.2 (vii) Дискретизовані послідовності шумових сигналів (ДПШС), задовольняють певним критеріям, повинні проходити статичні тести, котрі крім усього іншого повинні виключати багатокрокові залежності. Крім того, повинне бути пройдене ентропійне тестування T8.

P.2 (viii) Додаткова математична обробка не повинна зменшувати ентропію на біт.

P.2 (ix) При кожному включенні ФГВП повинен бути достовірні мінімальні статистичні властивості ДПШС. До тих пір, доки не закінчиться статичне тестування, ВЧ не можуть бути видані.

P.2 (x) Якщо під час роботи ФГВП відбувається загальна зупинка джерела шуму, повинна виключатися видача випадкових чисел, так як відповідні внутрішні випадкові послідовності були сгенеровані після зупинки.

P.2 (xi) В роботу ФГВП повинен бути імплементован *online*-тест, з допомогою якого може бути перевірено статистичну якість дискретизованої послідовності шумового сигналу. *Online*-тест повинен бути викликаний ззовні або ФГВП повинен сам викликати його. Після

повинне здійснюватися постійно або принаймні через регулярні проміжки. *Online*-тест повинен розрізняти в узгоджений час незначні статистичні дефекти або погіршення статичних властивостей дискретизованої шумової послідовності.

P.2 (xii) Вимоги P.2 (vii) повинні бути перевірені для передбачених зовнішніх умов використання, так як вони можуть впливати на функціонування джерела шуму.

P.2 (xiii) ФГВП повинен сам викликати *online*-тест.

Можливі застосування ФГВП класу P2:

- ключі та параметри шифрування;
- випадкове заповнення;
- паролі.

2.3. Порівняння AIS 31 з іншими стандартами

Попередні дослідження та тестування підтвердили, що AIS 31 є надійною методикою тестування і по своїй ефективності забезпечує результати, що і NIST STS. Перевагою AIS 31 є те, що він забезпечує тестування в реальному часі. Методика, що визначена в AIS 31, може застосовуватися як в реальному часі, так і в процесі досліджень, та для технологічного тестування. В AIS 31 враховані вимоги якісного перевіряння на випадковість та можливості оперативного тестування.

Аналіз показав, що AIS 31 базується на математично-технічній основі AIS 20. Що стосується застосування, то класи P1 і P2 відповідають класам K1-K2 і K3-K4 AIS 20.

3. Оцінка ДГВП заснованого на спарюванні точок еліптичної кривої та ґешуванні згідно AIS 20

Відповідно до аналізу, що наведений в [5], указаний генератор задовольняє вимогам K1(i), K3(iii) та K3(iv). Вимога K2 (ii), яка полягає в тому, що послідовності $r_1, r_2, \dots$ та їх бітові представлення повинні задовольняти статистичним тестам T1 – T5, які наведені в додатках до AIS 20, буде виконуватися якщо в якості фінального перетворення використовувати ґеш функцію із ISO/IEC 10118-2. По суті, вказана вимога забезпечує властивість непередбачуваності. Вимога K4(v) полягає в тому, що аналітик, навіть маючи дані про внутрішній стан генератора, не може обчислити наступне або попереднє вихідне значення. Використовуючи модель випадкового оракулу можна довести, що якщо аналітик може визначити сусіднє вихідне значення генератору, то оракул, який він для цього застосовує, можна використати в якості засобу ефективного криптографічного аналізу при вирішенні задачі дискретного логарифму в групі точок еліптичної кривої.

Тому генератор, що заснований на спарювання точок еліптичної кривої, можна віднести до функціонального класу K4. Для порівняння, запропонований в стандарті США X9.98 [6] генератор також належить до класу K4, але оскільки він заснований лише на багаторазовому використанні алгоритмів ґешування, то складність пошуку сусідніх вихідних значень генератора має лише поліноміальний характер, тобто цей генератор може застосовуватися лише в умовах використання досить великих (тому безпечних) загально системних параметрів.

Висновки

Прийняті в Німеччині нормативні документи AIS 20 та AIS 31 [2] враховують основні положення й досвід застосування федеральних стандартів США FIPS 140-1 [3] і FIPS 140-2 [4]. Нормативний документ AIS 20 містить критерії, що ефективно можуть застосовуватись для оцінки ДГВП.

Наведені в статті дані дозволяють зробити висновок про те, що усі чотири класи K1 – K4 є ієрархічно залежними, коли кожен наступний повністю включає в себе попередній та доповнює своїми новими вимогами.

В AIS 31 представлені критерії оцінки криптографічних властивостей генераторів випадкових чисел. Причому, оцінка фізичних генераторів випадкових послідовностей (ФГВП) ґрунтується в основному на статистичних тестах.

ДГВП, що заснований на спарювання точок еліптичної кривої, можна віднести до функціонального класу К4, тому він має перспективу застосування, в тому числі в Україні.

ДГВП, що запропонований в стандарті США Х9.98 [6], теж належить до класу К4, але оскільки він заснований лише на багаторазовому використанні алгоритмів гешування, то складність пошуку сусідніх вихідних значень генератора має лише поліноміальний характер.

Список літератури: 1. *Application Notes and Interpretation of the Scheme (AIS) 20. Functionality classes and evaluation methodology for physical random number generators. Certification body of the BSI in context of certification scheme. BSI, 1999, 23 p.* 2. *Application Notes and Interpretation of the Scheme (AIS) 31. Functionality classes and evaluation methodology for physical random number generators. Certification body of the BSI in context of certification scheme. BSI, 2001, 38 pages.* 3. *Federal Information Processing Standards Publication (FIPS PUB) 140-1. Security requirements for cryptographic modules. NIST, 1994, 48 pages.* 4. *Federal Information Processing Standards Publication (FIPS PUB) 140-2. Security requirements for cryptographic modules. NIST, 1999, 58 pages.* 5. *Гриненко Т.А., Горбенко Ю.И., Орлова С.Ю. Метод формирования и свойства ПВП на эллиптических кривых // Радиотехника. – 2001. – Вып.119. – С. 119-123.* 6. *Стандарт США Х9.98-2010*

*Харківський національний
університет радіоелектроніки*

Надійшла до редколегії 12.08.2011

АКТУАЛЬНІСТЬ АТАКИ НА ЗВ'ЯЗАНИХ КЛЮЧАХ ДЛЯ АПАРАТНИХ РЕАЛІЗАЦІЙ ЗАСОБІВ КЗІ

Вступ

З поширенням та впровадженням у щоденне життя засобів КЗІ зростає кількість виробників цих рішень, поширюється та поповнюється новими сторонами сітка дистрибуції. За таких умов кількість сторін, яким довіряє користувач засобів КЗІ, значно зростає. Постає питання – чи може користувач бути впевненим у тому, що на всіх етапах, від виробництва до впровадження рішень, не було допущено грубих помилок, або навмисно внесено лазівок? Загалом проблема довіри може бути частково вирішена незалежним аудитом та сертифікацією засобів, що зводить кількість зовнішніх сторін, яким треба довіряти, до однієї. Але чи можна бути впевненим, що продукти, які проходили сертифікацію, та продукти, що впроваджуються, – це ті самі продукти? У випадках з програмними засобами КЗІ можливо користуватись контрольною сумою, що наведено у матеріалах результатів сертифікації. Для апаратних та програмно-апаратних рішень неможливо обчислити геш значення. Нemoжливо дослідити, що чіпи та контроллери, що впроваджуються, – це саме ті контролери та чіпи, що було досліджено.

Така ситуація могла б не становити значної загрози, якщо б компрометація могла бути здійснена тільки за рахунок використання лазівок. Більш важлива можливість компрометації за результатами роботи засобів КЗІ, що здійснюються за рахунок невиконання важливих умов, на які розраховує алгоритм.

В статті на прикладі ЕЦП показана схема компрометації приватного ключа, що може бути використана у програмно-апаратних засобах.

Модель загроз

Визначимо положення моделі загроз, у якій зловмисником виступає розробник.

- Розробник виконує програмно-апаратну реалізацію схеми ЕЦП, передає засоби користувачеві.
- Розробник та користувач не можуть змінювати логіку роботи засобів після впровадження засобу.
- Розробник не має можливості взаємодіяти з засобом після впровадження.
- Вхідні дані та результат її обробки не є секретними, та можуть бути отримані зацікавленими сторонами.
- Вихідні дані можуть бути протестовані сторонніми засобами (наприклад – NIST STS). Користувач не довіряє розробнику.

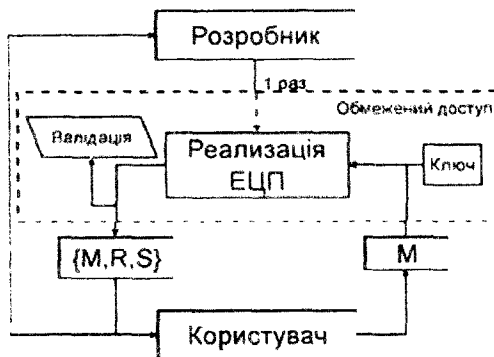


Рис. 1. Загальна модель загроз

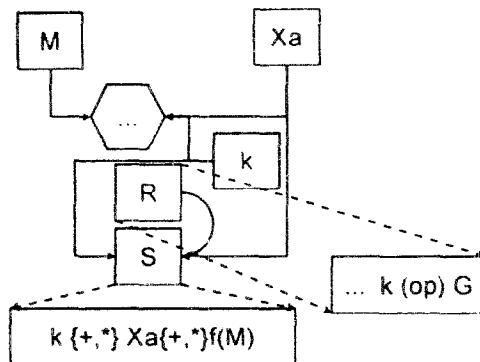


Рис. 2. Загальний вигляд

Задачі зловмисника та користувача такі:

- зловмисник – виробити засіб КЗІ таким чином, щоб сторонній засіб тестування не виявив наявності закладки. З наявних у публічному доступі пар даних та ЕЦП даних відновити приватний ключ користувача;
- користувач – виробити засіб та методику тестування вихідних значень засобу КЗІ таким чином, щоб мати можливість виявити наявність закладки або порушень у роботі пристрою, що можуть призвести до компрометації приватного ключа.

Для досягнення мети зловмисник має обрати такий елемент підпису, що використовується завжди, на який користувач не має ніякого впливу, та який отримано за допомогою функції отримання випадкового числа. Наприклад, доменні параметри ЕЦП дуже вразливі до невиконання вимог. Але, як правило, доменні параметри ЕЦП можуть бути визначені довіреною стороною.

Приватний ключ користувача – більш вдалий параметр для нав'язування. Його генерує пристрій, звичайно його неможливо отримати та дослідити. Але деякі пристрої мають можливість імпортувати приватний ключ до пристрою.

Найбільш придатним до модифікації є другий приватний ключ користувача. Подивимося, яку роль грає інший приватний ключ, так званий ключ сесії, на прикладі деяких ЕЦП у г.т. ЕК з відновленням та доповненням повідомлення.

Ключові данні у ЕЦП з доповненням та відновленням повідомлення

Для підписів ECDSA/ДСТУ/ГОСТ/ECNR/ECPV та інших [1 – 4] існує пара ключів, що формуються випадковим чином. Визначимо їх як $X_a = RNG()$ та $k = RNG()$. X_a формується один раз та називається секретним ключем, k формується для кожного підпису окремо та називається сесійним ключем. Але треба відзначити, що хоча k і називається сесійним ключем, він не має очікуваних властивостей сесійних ключів, подібних до тих, що мають схеми шифрування. Компрометація ключа k негайно призводить до компрометації X_a .

Подивимося докладніше. У всіх схемах ЕЦП k обчислюється і використовується двічі: як рандомізуючий компонент чи ключ KDF $k = RNG()$, $P = \pi(kG)$; та як другий ключ у S компоненті [1. 2. 3. 4]

$\{R, S\}$:

- ECDSA: $\{r = P; s = k^{-1}(f(M) + X_a r); \text{mod } N\}$
- ДСТУ: $\{r = f(M)P; s = (k + X_a r); \text{mod } N\}$
- ECNR: $\{r = f(M) + P; s = (k - X_a r); \text{mod } N\}$
- ECMR: $\{r = f(M) \oplus P; s = (r * k - r - 1)/(X_a + 1); \text{mod } N\}$
- ...

Для підписів з доповненням $f(M) = \text{Hash}(M)$. Для підписів з відновленням $f(M)$ обчислюється відповідно до схеми.

Стандарти схем ЕЦП висувають k та $RNG()$ жорсткі вимоги щодо випадковості значення. Стандарт DSA, наприклад, визначає k як непередбачуваний секретний параметр, що ніколи не повторюється. На практиці ця вимога іноді не виконується, а у деяких джерелах вимоги скорочуються до k як «випадкового» числа.

Проблема є актуальною. За останні декілька років трапилось два досить відомих випадки, коли невиконання вимог щодо випадковості k призвело до створення масових загроз безпеки та зашкодило репутації корпорації.

У 2008 р. група, що виконує обов'язки з аудиту програмного забезпечення дистрибутиву Debian (Debian Security Team), виявила значні недоліки у пакеті з реалізацією ЕЦП – openssl. Проблема полягала у тому, що генератор псевдовипадкових послідовностей ініціалізувався ідентифікатором потоку користувача, що міститься у множині значень $s \in (0; 32768)$. Помилка мала місце у функціонуючих системах два роки. В результаті було масово відкликано не

тільки ті сертифікати, які було сформовані за час функціонування версій ПЗ, що мали недоліки, але й ті, що використовувалися у той проміжок часу[5].

У 2010 р. на 27-й конференції Chaos Communication Congress було зроблено доповідь про значний успіх у роботі над завантаженням до Sony PlayStation 3 довільного ПЗ. Корпорація Sony реалізує у продаж мільйони пристроїв PlayStation 3 нижче собівартості пристрою, розраховуючи на прибутки від продажу програмного забезпечення. Ігровий засіб не виконує не підписане корпорацією ПЗ. Дослідники змогли відновити закритий ключ корпорації завдяки невиконанню вимог до випадкової компоненти k у реалізації ЕЦП ECDSA. Відновлений ключ відкриває шлях до завантаження та виконання довільного ПЗ на пристрої. Можна констатувати, що корпорація понесе значні збитки [6].

Модель атаки на реалізацію з використанням Г(П)СЧ

Визначимо суть та мету атаки: для функції RNG необхідно виробити таку функцію відображення $a()$ ($a(): (k = RNG()) \rightarrow k'$), вектор результатів виконання $[k_n, k_1, \dots, k_n]$ якої буде задовольняти наступним умовам:

- $\exists \{k_i, k_j\} \in [k_n, k_1, \dots, k_n]: k_i - k_j = \varepsilon = const, n = const$
- $\forall \{k_i, k_j\} \in [k_n, k_1, \dots, k_n]: k_i - k_j \neq 0, n = const$
- $K = a(RNG(N)); \forall K: STS([k_n, k_1, \dots, k_n], nN) = 0, n = const$, де $STS(K, N)$ – функція статистичного тестування бітової послідовності довжиною N біт, що вертає 0, якщо послідовність відповідає критеріям випадковості, та 1 – якщо не відповідає; $RNG(N)$ – вертає випадковий бітовий рядок довжиною N біт.

Наведемо приклад алгоритму функції $a()$, що задовольняє двом умовам з трьох:

$$\forall \{k_n, k_n\} \in a(): k_n - k_n = 0 \quad (1)$$

Дійсно, якщо $n = const$, тоді $i - j = 0 - n = const$. Тестування подібної послідовності з використанням комплекту NIST STS 2.1 для функції $STS()$ показує, що для $L_n(k_i) = 160$ та $n = 1000$ та вказаних до NIST STS рекомендаціях послідовність, що отримана за рахунок відображення функцією $a()$ вважається випадковою.

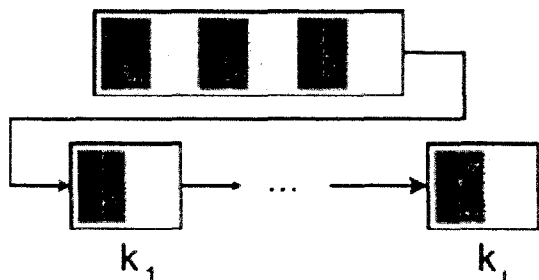


Рис. 3. Повторювання послідовності

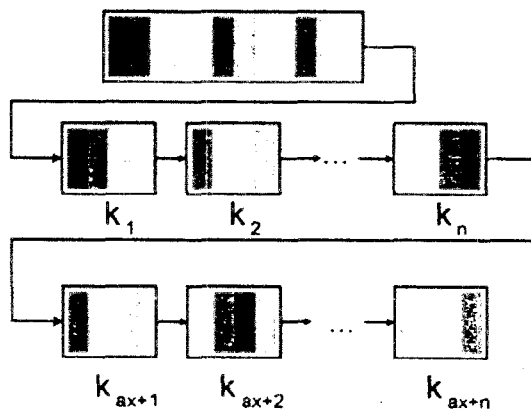


Рис. 4. Невипадкова послідовність

Для функції (1) відновлення ключа x буде мати такий вигляд:

- ECDSA:

$$k = \frac{d_2 - d_1}{s_1 - s_2}; x = \frac{sk - d}{r} \mod N.$$

- ДСТУ:

$$x = \frac{(s_1 - s_2)}{(r_1 - r_2)} \mod N.$$

- ECNR, ECPV, ECAO, ECKNR:

$$x = \frac{s_1 - s_2}{r_2 - r_1} \bmod N$$

- ECMR:

$$x = \frac{r_2 - r_1}{r_1 s_2 - r_2 s_1} \bmod N$$

Модифікуємо (1) таким чином, щоб нове рівняння задовольняло усім умовам:

$$\forall \{k_n, k_n\} \in a() : k_n - k_n = \varepsilon = \text{const.} \quad (2)$$

Для послідовностей, де $\varepsilon = 2^{\log_2 n - 1} - 1$ та $n > 900$, функція відображення $a()$ значно не змінює статистичну картину, що отримано за допомогою NIST STS 2.1, та зовсім не змінює кількість тестів на випадковість що не пройдено.

Для функції (2) відновлення ключа x буде мати такий вигляд.

- ECNR, ECPV, ECAO, ECKNR:

$$x = \frac{s_1 - s_2 + \varepsilon}{r_2 - r_1} \bmod N.$$

- ECMR:

$$x = \frac{r_2 - r_1 + r_1 r_2 \varepsilon}{r_1 s_2 - r_2 s_1} \bmod N.$$

Можна зробити висновок, що k становить для зломисника оптимальний вектор атаки: користувач не впливає на процес формування цього параметру, він випадковий. Його неможливо відновити та складно проаналізувати.

Виявлення небезпечних ключових послідовностей

Визначимо небезпечну ключову послідовність як бітовий рядок B , який відповідає умові

$$\exists \{i, j\} : f(k_i, \varepsilon) = k_j \quad (3)$$

де $k_0 \parallel k_1 \parallel \dots \parallel k_n \parallel \text{pad} = B$, $f(x, y) = x'$ – деяка відома лінійна функція, що може бути виражена груповими операціями від змінної та константи, та є дистрибутивною операцією щодо групової операції в групі точок еліптичної кривої; ε – деяке відоме значення.

Для $\{k_0, k_1, \dots, k_n\}$ згідно до (2) відновлення секретного параметру можливе.

Визначимо можливу методику використання послідовності B . По-перше, сформулюємо у загальному вигляді процес використання пов'язаних значень. Зломисник для відновлення секретного параметру x використовує відомі параметри двох підписів $\{r_1, s_1, d_1\}, \{r_2, s_2, d_2\}$ та відомий параметр ε , та вирішує рівняння

$$S(r_1, d_1, k_i, x) = S(r_2, d_2, f(k_i, \varepsilon), x). \quad (4)$$

відновлюючи секретний параметр x , де $S(\dots)$ – функція формування s компоненти підпису. Якщо вимоги до функції $f()$ виконані, тоді (4) має тривіальне вирішення для існуючих схем ЕЦП. Випадок нелінійності функції $f()$ не було досліджено.

Розглянемо можливі способи виявлення таких послідовностей. k -компонента підпису використовується в обох частинах ЕЦП: $\{r, s\}$. В загальному вигляді r може бути представлене як $r = \text{OS2IP}(\text{EC2OSP}(kG))$, де група функцій $\text{OS2IP}(\text{EC2OSP}())$ відіграє роль функції відображення точки еліптичної кривої до скінченного поля, яка в більшості випадків не є ізоморфною. Таким чином, у загальному вигляді r компонента підпису не має джерел для аналізу, за випадком деяких тривіальних відображень (ДСТУ 4145, ECDSA), де r представлена як $r = x, (x, y) = kG$. Завжди доступна можливість дослідження kG у час

перевірки ЕЦП. В усіх схемах ЕЦП з k компонентою у групі точок еліптичної кривої на останніх етапах проводиться відновлення передпідпису.

Визначимо методику дослідження передпідпису. Для дослідження точки kG як елемента групи точок еліптичної кривої ми можемо використовувати операції $\{=, +\}$. З (4) зрозуміло, що об'єктом дослідження є можливість визначення для деяких пар $\{k, j\}$ такого ε , що $k_j = f(k, \varepsilon)$. Єдиний спосіб аналізувати зв'язок k компонент за допомогою відновленого передпідпису – перевіряти

$$k_j G = f(k_j G, \varepsilon' G) \quad (5)$$

де ε' – обране для перевірки випадкове (чи визначене) число. Якщо (5) дійсне, тоді для k_j та k_j існує зв'язок, що визначено функцією $f()$ з параметром ε' . Треба зауважити, що складність пошуку ε' за допомогою оракула дорівнює складності пошуку k . Модель пошуку за (5) з використанням оракулу накладає додаткові обмеження на функцію $f()$. Легко побачити, що функція $f()$ має бути виражена тільки за допомогою операції '+’.

Використання зв'язку для рівномірної вибірки даних

Визначимо ознаку рівномірності. Нехай $y = RNG_n(x)$ – функція, що вертає деяке $y \in [0, x-1]$ з джерела D . Тоді рівномірною вибіркою даних назовемо такий кортеж $\{(x_0, y_0), (x_1, y_1), \dots, (x_n, y_n)\}$, для яких

$$\forall x \in \{x_0, x_1, \dots, x_n\} : \log_2 x = C = const \quad (6)$$

Нехай джерело D постачає кожні 163 біти, з проміжком 163000 бітів, як $y_i = 2^{163} - 1 - y_{i-163000-163}$. У разі, коли $f(\xi) = \xi + \varepsilon$, та $y = RNG_n(x) = d \bmod x$, $d \in D$, $\lfloor \log_2 d \rfloor = \lfloor \log_2 x \rfloor$, $D = \{d_0, d_1, \dots, d_n\}$ можливі наступні варіанти. Якщо $d < x$, тоді $k = y$, та $k' = f(k) = k + \varepsilon = y + \varepsilon$. Коли $d > x$, тоді $k = x - d$, та $k' = f(k) = k + \varepsilon - x = y - x + \varepsilon$.

Таким чином, в загальному випадку для перевірки гіпотези щодо значення ε' необхідно перевірити рівняння (2) з параметрами $\varepsilon = \varepsilon'$ та $\varepsilon = \varepsilon' - x$.

У разі, коли джерело D є постачальником скомпроментованих значень k , постає питання – що буде, коли в (6) $x \neq const$?

По-перше, виникає проблема визначення того факту, що використане значення k містить частину невідповідного d . Встановити це можливо, якщо результати використання усіх k наявні.

По-друге, необхідно переформатувати d таким чином, щоб рівняння (6) було дійсним. Нехай $D = \{\dots, d_{i+1}, d_i, d_{i-1}, \dots\}$, де $\delta = (d_{i+1} \parallel d_i \parallel d_{i-1})$, для якого є відоме значення ε , $y = d_i$, та $f(), \varepsilon'$ пов'язують між собою d . Така нерівномірність з обох боків призводить до ускладнення загальної схеми.

Висновки

Визначена проблема можливості створення функції відображення є загальною, та не має відношення тільки до конкретних схем ЕЦП. Суть проблеми становить композиція характеристик схеми, що поєднана з фізичною реалізацією. Визначимо важливі тези.

- Наявність компонент у криптографічних схемах, які приймають значення з деякою вірогідністю, унеможливають створення пакету тестування, що буде функціонувати за методикою чорної скриньки.

- Пов'язаність безпеки приватних даних, а не безпеки однієї транзакції. У разі компрометації сесійного ключа компроментується секретний компонент схеми.

- Можливість визначення приватної компоненти за можливості визначення такої функції $f(k_i) = k_j$, що робить можливим обчислення одного сесійного ключа з іншого, та яка визначена для усіх можливих k .

- Діючі вимоги до апаратних засобів та діючі вимоги до сесійної компоненти k (випадковий ключ сесії k має бути знищений одразу після виконання криптографічної операції) унеможливають ані отримання, ані аналіз.

- Принципова неможливість валідації існуючого засобу КЗІ, що функціонує як чорна скринька. Можна казати, що існує так звана «проблема чорного лебідя». Повний аналіз пристрою виведе його з робочого стану та не буде гарантувати того, що інші пристрої є безпечними. Необхідно внести вимоги щодо можливості фізичної декомпозиції засобу КЗІ.

Проблемні питання з цього напрямку включають наступні пункти:

- вирішення рівняння пов'язаних ключів для нерівномірних вибірок даних;
- отримання диференційної моделі джерела випадкових послідовностей;
- внесення змін вимог до реалізації апаратних засобів КЗІ;
- пошук оптимального співвідношення $\{\epsilon, i-j\}$ для рівняння (3).

Список літератури: 1. ДСТУ 4145-2002 Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевірка". – К. : Держстандарт України, 2003. 2. ГОСТ Р 34.10-2001. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. Госстандарт России, 2001. 3. Iso/iec 9796-3: Discrete logarithm based mechanisms / ISO/IEC. URL:<http://www.iso.org/>. 2006. вересень. 4. American National Standards Institute, 1120 Connecticut Ave., N.W.Washington, DC 20036. Public Key Cryptography For The Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA), 1998, вересень. 5. US-CERT/NIST. Cve-2008-0166. 6. fail0verlow. Console hacking 2010. URL: http://events.ccc.de/congress/2010/Fahrplan-/attachments/-1780_27c3_-console_-hacking_2010.pdf.

Харківський національний
університет радіоелектроніки

Надійшла до редколегії 12.08.2011

ПОЛОЖЕННЯ ПРО ОБРОБКУ ТА ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ ХНУРЕ

Вступ

Національною доктриною розвитку освіти, затвердженою Указом Президента України від 17.04.2002 р. №347/2002, державною програмою "Інформаційні та комунікаційні технології в освіті і науці на 2006–2010 рр.", затвердженою постановою Кабінету Міністрів України від 07.12.2005р. № 1153, законом України "Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 рр." від 09.01.2007 р. та рядом інших нормативних актів, визначено пріоритетні напрями державної політики у галузі інформатизації освіти.

Відповідно до визначених напрямів інформатизації в Харківському національному університеті радіоелектроніки (далі – Університет) впровадженні автоматизовані інформаційні (інформаційно-телекомунікаційні) системи та технології, які забезпечують вирішення завдань обробки та ефективного використання інформації в електронній формі в більшості основних процесів інформаційної діяльності: навчання, наукових досліджень, методичної й адміністративно-господарської роботи, управління вищим навчальним закладом. Разом із тим, у зв'язку з особливостями використання та розповсюдження інформації, окремі процеси інформаційної діяльності реалізуються не автоматизованими інформаційними технологіями (обробка та використання інформації у формі картотек, архівів, особистих справ, довідників, адресних книг та інших паперових документів без використання комплексів засобів автоматизації).

Суттєвою особливістю певної частини впроваджених в Університеті інформаційних процесів навчання, наукових досліджень, методичної й адміністративно-господарської роботи, управління вищим навчальним закладом та відповідних інформаційних технологій є використання відомостей про фізичну особу (персональних даних) під час обробки інформації навчального, соціального, фінансового, науково-технічного, адміністративного та іншого характеру.

Враховуючи необхідність застосування сучасних технологій при автоматизованій обробці інформації про особу, а також виникнення загрози для конкретної людини стосовно витоку та несанкціонованого використання персональних даних, багато європейських країн підписали Конвенцію № 108 Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних [1] та Додатковий протокол до Конвенції № 108 про захист осіб у зв'язку з автоматизованою обробкою персональних даних щодо органів нагляду та трансграничних потоків даних [2].

Принципи, що містяться у Конвенції, уточнюються і розширюються в Директиві 95/46/ЕС Європейського парламенту і Ради Європи від 24.10.95 р. "Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних" [3], в Директиві 2002/58/ЕС Європейського парламенту й Ради Європи від 12.07.2002 р. "Про обробку персональних даних та захист таємниці сектора електронних комунікацій (директива про секретність та електронні комунікації) [4], Директиві 2006/24/ЕС Європейського парламенту та Ради Європи від 15.03.2006 р. "Про збереження даних, створених або оброблених при наданні загальнодоступних послуг електронних повідомлень або громадських мереж зв'язку та внесення поправок в Директиву 2002/58/ЕС" [5].

У зв'язку з набуттям чинності закону України "Про захист персональних даних" [6] виникла необхідність запровадження єдиного підходу щодо визначення і формування завдань, функцій, підрозділів та окремих посадових осіб, їх повноважень та відповідальності, а також

організації робіт із захисту персональних даних впродовж всіх етапів життєвого циклу інформаційних систем Університету.

З метою вирішення цих питань в Університеті, як передбачено ст. 6. Закону [6], було зроблено "Положення про обробку та захист персональних даних" (далі – Положення), яке регулює діяльність Університету з питань обробки та захисту персональних даних в інформаційних (автоматизованих) системах та в картотеках персональних даних (далі – залежно від контексту викладення використовується узагальнюючий термін – інформаційні системи персональних даних (ІСПДн)).

Положення є офіційним керівним документом Університету, який призначений для керівного складу, фахівців підрозділів захисту інформації та працівників структурних підрозділів, які організують і здійснюють роботи з обробки інформації про фізичну особу (персональних даних) в процесі інформаційної діяльності з навчання, наукових досліджень, методичної й адміністративно-господарської роботи, управління вищим навчальним закладом.

Положення складається з наступних основних розділів, короткий зміст яких наведений далі.

1. Розділ "Загальні положення"

В розділі визначені мета і призначення документу, галузь застосування, порядок затвердження "Положення ..." і змін до нього, обов'язок уповноважених працівників Університету забезпечити кожному суб'єктові персональних даних можливість ознайомлення з документами й матеріалами, що безпосередньо зачіпають його права й свободи, якщо інше не передбачено законом.

2. Розділ "Суб'єкти відносин, пов'язаних із персональними даними"

В розділі відповідно до ст. 2 і 4 Закону [6] наводиться перелік юридичних та фізичних осіб, які пов'язані із обробкою персональних даних в ІСПДн Університету, а саме:

1) МОН України – власник баз персональних даних відомчих інформаційних систем, компоненти яких впроваджені в Університеті за наказами Міністерства (системи "Освіта", "Конкурс", "Реєстр докторів наук та професорів" та ін.). МОНУ затверджує мету обробки персональних даних у базах даних цих систем, встановлює склад цих даних та процедури їх обробки;

2) Органи державної влади та органи місцевого самоврядування (Податкова адміністрація, Пенсійний фонд та ін.) – власники баз персональних даних державних інформаційних систем, компоненти яких впроваджені в Університеті, до повноважень яких відповідно до закону належить здійснення обробки та захисту персональних даних, затвердження мети обробки персональних даних у базах даних цих систем, встановлення складу цих даних та процедур їх обробки;

3) Харківській національний університет радіоелектроніки, якій є:

– власником баз персональних даних власних інформаційних підсистем, що впроваджені в Університеті за наказами ректора, який затверджує мету обробки персональних даних у базах даних цих підсистем, встановлює склад цих даних та процедури їх обробки (підсистеми "Університет", "Приймальна комісія", "Відділ кадрів професорсько-викладацького складу", "Профком студентів" та ін.);

– розпорядником баз персональних даних інформаційних підсистем, компоненти яких впроваджені в Університеті за наказами МОН України, законів та нормативно-розпорядчих документів органів державної влади та органів місцевого самоврядування (податкові органи, пенсійні фонди, органи соціального страхування, органи статистики та ін.);

4) Уповноважені працівники Університету – посадові особи (проректори, керівники структурних підрозділів) й працівники структурних підрозділів Університету, яким наказом ректора надано право здійснювати обробку персональних даних в інформаційних системах персональних даних Університету;

5) Суб'єкти персональних даних в Університеті – фізичні особи (носії персональних даних), які передали на обробку, як на добровільній основі, так й у рамках виконання вимог законів та нормативно-правових актів, свої персональні дані Університету, у тому числі: наукові й науково-педагогічні працівники, студенти, здобувачі вчених ступенів, аспіранти й докторанти, абітурієнти, слухачі курсів й окремих освітніх програм, інші особи, що надають персональні дані Університету;

6) Уповноважений державний орган з питань захисту персональних даних – Державна служба з питань захисту персональних даних – центральний орган виконавчої влади, до повноважень якого належить захист персональних даних, що утворюється відповідно до законодавства;

7) Третя особа – будь-яка особа, за винятком суб'єкта персональних даних, власника чи розпорядника бази персональних даних та уповноваженого державного органу з питань захисту персональних даних, якій власником чи розпорядником бази персональних даних здійснюється передача персональних даних відповідно до закону (юридичні й фізичні особи, які звертаються до Університету за одержанням необхідних відомостей про фізичну особу – суб'єкта персональних даних і користуються ними без права передачі й розголошення).

В розділі також визначаються функції та повноваження окремих посадових осіб і підрозділів щодо організації, планування, координації робіт з обробки та забезпечення захисту персональних даних в ІСПДн Університету.

3. Розділ "Поняття й склад персональних даних"

В розділі наведений семантичний аналіз правових аспектів визначення терміну "персональні дані" ст. 2 Закону "Про захист персональних даних" [6].

Зазначено, що суб'єктом персональних даних фізична особа стає з моменту, коли з'являється можливість її ідентифікації, тобто встановлення тотожності або можливість відокремлення від інших на підставі збігу характеристик. Ідентифікація може бути проведена за однією унікальною особистою характеристикою індивідуальності або за комбінацією кількох загальних і особистих характеристик особи. Ідентифікація особи можлива безпосередньо (пряма) або опосередковано (непряма). Наводяться приклади прямої та непрямої (опосередкованої) ідентифікації.

Наведено, що для визначення того, чи можна особу конкретно ідентифікувати (встановити), повинні враховуватися всі засоби, використання яких власником бази персональних даних чи якою-небудь іншою особою імовірно очікувати для ідентифікації цієї особи. Таким чином, визначення вичерпного переліку характеристик індивідуальності, які однозначно кваліфікують відомості як персональні дані, залежить від кількості можливих засобів ідентифікації фізичної особи в конкретній інформаційній системі персональних даних.

Зазначено, що конкретний склад та зміст персональних даних в кожній ІСПДн Університету визначається її функціональним призначенням, складом і змістом даних її інформаційного забезпечення, категоріями суб'єктів персональних даних і затверджується ректором Університету відповідно до положень законів, нормативно-правових актів в галузі трудових цивільно-правових відносин і освіти України, міжнародних угод та нормативно-розпорядчих документів МОН України.

З метою визначення методів і способів захисту інформації, необхідних для забезпечення безпеки персональних даних проводиться категоріювання персональних даних, що обробляються, та класифікація інформаційних систем на етапі їх створення або в ході експлуатації (для раніше введених в експлуатацію і (або) модернізованих інформаційних систем). Порядок проведення класифікації інформаційних систем персональних даних визначається нормативними документами Державної служби з питань захисту персональних даних.

У відповідності із визначенням терміну "персональні дані", особливих вимог до їх обробки, що визначені в законі [6], та ступенем можливих негативних наслідків для фізичної осо-

би у випадку порушення заданої характеристики їх безпеки в інформаційних системах Університету, запропоновані чотири категорії персональних даних.

В розділі наведені узагальнені переліки персональних даних (в т.ч. по категоріям), що сформовані на підставі складу та змісту персональних даних, що визначені у законах та інших нормативно-правових актах України в області трудових відносин й освіти, нормативних й розпорядничих документах МОН України, наказах ректору Університету.

Також в розділі для кожної категорії суб'єктів персональних даних Університету наведений базовий склад документів, у яких містяться персональні дані.

Далі в розділі зазначено, що відповідно до законів [6, 9] персональні дані, крім знеособлених персональних даних, за режимом доступу є інформацією з обмеженим доступом (далі – ІЗОД), якій за своїм правовим режимом надано статус конфіденційної.

4. Розділ "Принципи обробки персональних даних"

Відповідно до вимог закону [6] в розділі визначені наступні принципи, яких слід дотримуватися при обробці персональних даних в ІСПДн Університету:

- законності (легітимності) цілей і способів обробки;
- відповідності цілей обробки персональних даних;
- законності персональних даних (дані повинні бути отримані на законних підставах й оброблені сумлінним і законним способом);
- адекватності й релевантності персональних даних (склад та зміст даних мають бути відповідними та ненадмірними стосовно визначеної мети їх обробки);
- якості даних (дані мають бути точними, достовірними, у разі необхідності вчасно оновлюватися);
- анонімності (дані обробляються у формі, що допускає ідентифікацію фізичної особи, якої вони стосуються);
- строкowości обробки даних (дані обробляються у строк, не більший ніж це необхідно відповідно до їх законного призначення за винятком випадків, установлених законами України);
- гарантії безпеки (дані повинні бути захищені від випадкового або несанкціонованого знищення або випадкової втрати, а також несанкціонованого доступу, зміни або поширення);
- приватності суб'єкта персональних даних (обробка даних ґрунтується на основі дотримання особистих прав суб'єктів персональних даних);
- правоздатності суб'єкта персональних даних (суб'єкт персональних даних Університету, якому належать відповідні персональні дані, є їх власником, який у повному об'ємі реалізує немайнові права володіння, користування, розпорядження цими даними);
- правоможності власника бази персональних даних (Університет як власник та розпорядник баз персональних даних виконує функцію володіння цими даними й має повноваження розпорядження ними в межах, установлених законодавством України).

5. Розділ "Загальні правила обробки персональних даних"

В підрозділах цього розділу відповідно до вимог закону [6] визначені цілі, основні положення і умови обробки персональних даних. Наведені правила використання, збирання, накопичення та зберігання в інформаційних (автоматизованих) системах (підсистемах) Університету і в картотеках персональних даних, зміни і доповнення, знищення, поширення персональних даних.

6. Розділ "Права та обов'язки суб'єктів персональних даних та Університету"

В розділі відповідно до вимог Конституції [7] та законів [6, 9] визначені права та обов'язки фізичних осіб, які є суб'єктами персональних даних, та юридичної особи – Університету, як власника баз персональних даних.

7. Розділ "Порядок доступу до персональних даних"

В розділі відповідно до вимог закону [6] наведено порядок:

- доступу працівників Університету до персональних даних суб'єктів;
- доступу до персональних даних інших суб'єктів відносин, пов'язаних із персональними даними;
- відстрочення або відмова у доступі до персональних даних;
- оскарження рішення про відстрочення або відмову в доступі до персональних даних
- оплати доступу до персональних даних.

8. Розділ "Захист персональних даних"

Персональні дані належать до окремих видів інформації, необхідність захисту якої визначено законодавством [6].

Розділ включає такі підрозділи: цілі захисту персональних даних, об'єкти захисту, принципи забезпечення безпеки персональних даних, загальний порядок організації захисту персональних даних в Університеті, захист персональних даних у інформаційних (автоматизованих) системах (підсистемах) Університету, захист персональних даних в картотеках персональних даних

В підрозділі *"Цілі захисту персональних даних"* відповідно до Конституції [7] та чинного законодавства [6, 8, 9] визначені головна мета та основні цілі захисту персональних даних суб'єктів захисту.

В підрозділі *"Об'єкти захисту"* відповідно до законів України [6, 9, 10] та постанови КМ України [11] наведені об'єкти захисту в ІСПДн Університету:

В підрозділі *"Принципи забезпечення безпеки персональних даних"* наведені наступні принципи системно-концептуального підходу забезпечення безпеки персональних даних в ІСПДн Університету:

1) Законності. Уповноважені працівники Університету повинні бути освідомлені про відповідальність за правопорушення в області захисту інформації в ІСПДн (ст. 330, 363, 363-1 та інші статті Кримінального Кодексу України) [12];

2) Відповідальності Університету перед зовнішніми сторонами. Згідно з Законом України "Про захист інформації в інформаційно-телекомунікаційних системах" [10] Університет повинен забезпечити адекватний захист цієї інформації і несе відповідальність за порушення конфіденційності, цілісності та доступності персональних даних під час їх обробки засобами системи;

3) Системності та комплексності. Захист повинен здійснюватися ешелоновано на основі комплексного застосування методів та засобів захисту інформації, взаємодії всіх елементів та служб Університету;

4) Своєчасність. Розробка системи захисту повинна вестися паралельно з розробкою й модернізацією самої ІСПДн. Це дозволить урахувати вимоги безпеки при проектуванні архітектури й, в остаточному підсумку, створити більш ефективну (як по витратах ресурсів, так і по стійкості) захищену систему;

5) Безперервність захисту;

6) Економічна доцільність (порівнянність можливого збитку й витрат);

7) Обов'язковість й ефективність контролю;

8) Науково-технічна обґрунтованість і реалізуємість;

9) Спадкоємність і безперервність удосконалення;

10) Спеціалізація й професіоналізм. Експлуатація цих заходів і засобів повинна здійснюватися професійно підготовленими посадовими особами Університету;

11) Взаємодія й координація – при забезпеченні безпеки персональних даних взаємодія із Держслужбою з питань захисту персональних даних, Держспецзв'язком України, МОН України й іншими зацікавленими органами виконавчої влади, а також з підприємствами й

організаціями, що залучаються для виконання робіт із забезпечення безпеки персональних даних.

Підрозділ "Загальний порядок організації захисту персональних даних в Університеті" встановлює єдині загальні правила і вимоги до порядку організації захисту персональних даних в інформаційних (автоматизованих) системах та в картотеках персональних даних, основні з яких наведено нижче.

Захист персональних даних в Університеті від незаконної обробки, а також від незаконного доступу до них здійснюється відповідно до вимог Конституції України [7], закону України "Про захист персональних даних" [6], інших законів та нормативно-правових актів, міжнародних договорів України, згода на обов'язковість яких надана Верховною Радою України, приписів Державної служби з питань захисту персональних даних, нормативно-розпорядчих документів Держспецзв'язку, МОН України та інших органів державних влади, уповноважених в області захисту інформації, а також затверджених положень й інструкцій Університету.

Захист персональних даних є однією із складових частин управлінської, наукової та навчальної діяльності щодо забезпечення безпеки інформації і являє собою сукупність організаційних і технічних заходів, які ґрунтуються на вищевикладених принципах.

Згідно закону [6] державна політика з питань захисту персональних даних реалізується Державною службою з питань захисту персональних даних у взаємодії з іншими центральними та місцевими органами державної виконавчої влади. Забезпечення захисту персональних даних у базах персональних даних в електронній формі та у формі картотек покладається на власника цих баз.

Враховуючи наявність у складі ІСПДн Університету як компонентів відомчих та державних інформаційних систем, так і власних інформаційних підсистем, забезпечення захисту персональних даних відповідно до закону [6] покладається:

- на МОН України як власника баз персональних даних відомчих інформаційних систем, компоненти яких впроваджені в Університеті за наказами Міністерства (системи "Освіта", "Конкурс", "Реєстр докторів наук та професорів" та ін.);
- органи державної влади та органи місцевого самоврядування (Податкова адміністрація, Пенсійний фонд та ін.), як власників баз персональних даних державних інформаційних систем, компоненти яких впроваджені в Університеті;
- Університет, що є власником баз персональних даних власних інформаційних підсистем, які впроваджені в Університеті за наказами ректора.

Безпека персональних даних при її обробці в ІСПДн Університету досягається шляхом виключення несанкціонованого, в тому числі випадкового, доступу до персональних даних, результатом якого може стати знищення, зміна, блокування, копіювання, поширення персональних даних, а також інших несанкціонованих дій.

При обробці персональних даних в інформаційних (автоматизованих) системах та картотеках персональних даних Університету має бути забезпечено:

- а) проведення заходів, спрямованих на запобігання несанкціонованого доступу до персональних даних і (або) передачі їх особам, які не мають права доступу до такої інформації;
- б) своєчасне виявлення фактів несанкціонованого доступу до персональних даних;
- в) недопущення впливу на технічні засоби автоматизованої обробки персональних даних, в результаті якого може бути порушено їх функціонування;
- г) можливість негайного відновлення персональних даних, модифікованих або знищених внаслідок несанкціонованого доступу до них;
- д) постійний контроль за забезпеченням рівня захищеності персональних даних.

Безпека персональних даних при їх обробці в інформаційних системах Університету забезпечується за допомогою систем захисту персональних даних, що включають організаційні заходи та засоби захисту інформації (у тому числі криптографічні засоби, засоби запобігання несанкціонованому доступу, програмно-технічним впливам на технічні засоби обробки пер-

сональних даних), а також інформаційні технології, що використовуються в інформаційній системі.

Роботи з забезпечення безпеки персональних даних при їх обробці в інформаційних системах Університету є невід'ємною частиною робіт щодо створення інформаційних систем. Витрати, пов'язані із здійсненням заходів щодо захисту персональних даних, включаються до загального кошторису на створення ІСПДн.

Під організацією захисту персональних даних при їх обробці в ІСПДн Університету розуміється формування сукупності заходів, що здійснюються на всіх стадіях життєвого циклу систем, узгоджених за метою, завданням, місцем і часом, спрямованих на запобігання (нейтралізацію) і протидії загроз безпеки персональних даних, на відновлення нормального функціонування ІСПДн після нейтралізації загроз, з метою мінімізації як безпосереднього, так і опосередкованого збитку від можливої реалізації таких загроз.

Заходи щодо організації робіт із захисту персональних даних є складовою частиною комплексу робіт із захисту конфіденційної інформації в Університеті і мають деякі особливості при організації та проведенні заходів, які зумовлені чинним законодавством у сфері захисту персональних даних.

Також в підрозділі наведений загальний порядок організації робіт із захисту персональних даних в ІСПДн Університету та вимоги до розміщення і фізичному захисту приміщень та обладнання ІСПДн.

Підрозділ *"Захист персональних даних у інформаційних (автоматизованих) системах (підсистемах) Університету"* у доповненні до загального порядку організації захисту персональних даних в Університеті встановлює єдині загальні правила і вимоги до порядку організації захисту персональних даних в інформаційних (автоматизованих) системах (далі – автоматизовані ІСПДн), основні із яких наведені нижче.

Забезпечення захисту персональних даних в автоматизованих ІСПДн Університету повинне здійснюватися відповідно до загальних вимог та організаційних засад, що визначені міжвідомчими *"Правилами забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах"* [11], нормативними документами Державної служби з питань захисту персональних даних та відомчими нормативно-розпорядчими документами МОН України.

Обробка конфіденційних персональних даних в автоматизованих ІСПДн Університету повинна здійснюватися з використанням захищеної технології, яка спрямована на забезпечення режиму безпеки.

Під режимом безпеки розуміється установлений відповідно до вимог законодавства єдиний порядок забезпечення захисту конфіденційної інформації, який визначає сукупність правових, організаційних (адміністративних), інженерно-технічних заходів, заходів контролю за дотриманням цього порядку тощо, а також правила застосування програмно-апаратних засобів захисту інформації.

В підрозділі наведено вимоги щодо забезпечення захисту персональних даних в автоматизованих ІСПДн Університету відповідно до постанови КМ України [11].

Організація та порядок проведення робіт із створення комплексної системи захисту інформації в автоматизованих ІСПДн Університету повинні здійснюватися відповідно до вимог НД ТЗІ 3.7-003-05 [13].

Порядок створення КСЗІ в автоматизованих ІСПДн є єдиним незалежно від того, створюється КСЗІ в системі, яка проектується, чи в діючій ІТС, якщо виникла необхідність забезпечення захисту персональних даних або модернізації вже створеної КСЗІ.

Обробка персональних даних в автоматизованих ІСПДн дозволяється тільки після завершення робіт з створення КСЗІ, проведення випробувань та оцінки рівня захищеності інформації на відповідність вимогам нормативних документів системи ТЗІ, за результатами якої Держспецв'язком або уповноважені ним органи надають атестат відповідності.

Дозвіл на експлуатацію автоматизованої ІСПДн надається наказом ректора Університету на підставі атестату відповідності та отримання документу про реєстрацію баз персональних даних у державному реєстрі Державної служби з питань захисту персональних даних.

Вибір і реалізація методів і способів захисту інформації в автоматизованих ІСПДн здійснюються на основі визначених загроз безпеки персональних даних (моделі загроз) і в залежності від категорії персональних даних, класу інформаційної системи, визначених відповідно до порядку, встановленого нормативними документами Державної служби з питань захисту персональних даних і Держспецзв'язку України.

В КСЗІ автоматизованої ІСПДн в залежності від класу системи та виходячи із загроз безпеки персональним даним, структури системи, наявності міжмережевої взаємодії і режимів обробки персональних даних з використанням відповідних методів і способів захисту інформації від несанкціонованого доступу повинні реалізовуватися функції управління доступом, реєстрації та обліку, забезпечення цілісності, аналізу захищеності, забезпечення безпечної міжмережевої взаємодії і виявлення вторгнень.

Також в підрозділі наведено основні методи і способи захисту персональних даних від несанкціонованого доступу в локальних автоматизованих ІСПДн та систем, які мають підключення до телекомунікаційних мереж загального користування, відомчих або інформаційних систем загального доступу (в т.ч. Internet).

Підрозділ "*Захист персональних даних в картотеках персональних даних*" встановлює єдині загальні правила і вимоги до порядку організації захисту персональних даних в картотеках персональних даних.

В інших розділах Положення визначені:

- організація контролю за додержанням законодавства у сфері захисту персональних даних;
- порядок взаємодії з Державною службою з питань захисту персональних даних;
- відповідальність за порушення законодавства про захист персональних даних;
- порядок та джерела фінансування робіт із захисту персональних даних;
- положення та вимоги при міжнародному співробітництві відповідно до закону [6].

Список літератури: 1. Конвенція №108 Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних. – Страсбург, 28.01.2001 р. Офіційний переклад. (ратифікована Законом України №2438-VI від 06.07.2010 р.). 2. Додатковий протокол до Конвенції № 108 про захист осіб у зв'язку з автоматизованою обробкою персональних даних щодо органів нагляду та транскордонних потоків даних. – Страсбург, 08.11.2001 р. Офіційний переклад. (протокол ратифіковано Законом України № 2438-VI від 06.07.2010 р.). 3. Директива 95/46/ЕС Європейського Парламенту та Ради Європи від 24.10.1995р. "Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних". 4. Директива 2002/58/ЄС Європейського парламенту та Ради від 12.07.2002 р. "Про обробку персональних даних та захист таємниці сектора електронних комунікацій (директива про секретність та електронні комунікації). Офіційний переклад Мін'юсту України. 5. Директива 2006/24/ЄС Європейського парламенту та Ради Європи від 15.03.2006 р. "Про збереження даних, створених або оброблених при наданні загальнодоступних послуг електронних повідомлень або громадських мереж зв'язку та внесення поправок в Директиву 2002/58/ЄС". 6. Закон України "Про захист персональних даних". 7. Конституція України (із змінами). 8. Цивільний кодекс України (із змінами). 9. Закон України "Про інформацію" (із змінами). 10. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" (із змінами). 11. Постанова Кабінету Міністрів України "Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах" від 29.03.2006 р. №373. 12. Кримінальний кодекс України (із змінами). 13. НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.

АНАЛІЗ БІОМЕТРИЧНИХ СИСТЕМ АВТЕНТИФІКАЦІЇ ТА ІДЕНТИФІКАЦІЇ З ВИКОРИСТАННЯМ ГІБРИДНИХ ІНТЕЛЕКТУАЛЬНИХ МЕТОДІВ ДЛЯ ЗАХИСТУ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

Вступ

На сьогодні у розвинених країнах світу, таких як США, Російська Федерація та країни ЄС, існує актуальний напрямок – впровадження біометрії в криптографію. На сучасному етапі виникло два основних методи застосування біометрики: автентифікація особи та криптографія. Традиційним напрямом є використання біометрики для автентифікації, який має велику історію вивчення та застосування (наприклад, в системах контролю та доступу до приміщень та джерел інформації з розмежуванням рівня гарантії).

Застосування біометричних методів (наприклад, для забезпечення секретності та автентифікації інформації) в криптографії має свої особливості. Стійкість методів базується на припущенні, що секретний ключ відомий тільки власнику, і задача збереження секретності ключа є основною задачею в криптосистемі.

Біометричні методи автентифікації особи мають деяку перевагу по відношенню до традиційних:

біометричні шаблони дуже важко фальсифікувати;

в силу унікальності біометричних характеристик достовірність автентифікації за біометричними даними дуже висока;

біометричні ідентифікатори не можна забути або загубити, як пароль чи картку;

біометрична автентифікація потребує наявності власника біометричних характеристик.

Суттєвий поштовх розвитку біометричних технологій дала програма створення паспортно-візових документів нового покоління. На даний момент у міжнародній організації з стандартизації ISO/IEC, комітету JTC1 (Information Technology), підкомітету SC37 (Biometrics) налічується за цією програмою 108 міжнародних біометричних стандартів і проектів, з яких 55 прийнятих та 53 стандарти перебувають у стадії обговорення і розробки [1]. Що дає можливість вивчати цей напрямок та впроваджувати в системи захисту інформації.

Огляд схем процедур біометричної ідентифікації

При дослідженні стандартів підкомітету SC37 було виявлено що для проходження автентифікації особи використовуються класичні схеми перетворення. Одну з таких схем наведено на рис. 1, а.

Для реалізації подібних технологій необхідно мати біометричний шаблон (блок 3. рис. 1, а), що відображає інформаційну частину біометричного образу.

З приведеної схеми випливає, що вона є вкрай вразливою. Для реалізації успішної атаки на біометричний захист достатньо:

- підміняти біометричний шаблон;
- скомпрометувати біометричний шаблон для виготовлення електронного або фізичного муляжу біометричного образу «Свій».

Також потребує створення захищеної бази зберігання біометричних шаблонів що призводить до додаткових витрат на ресурси.

Одним із шляхів вирішення завдання захисту біометричного шаблону є деяке змінення класичної схеми, а саме заміни зберігання біометричних шаблонів для порівняння на систему з використанням гібридних інтелектуальних систем (рис. 1, б).

Як видно з рис. 1, б, біометричний шаблон при ідентифікації з використанням інтелектуальних систем відсутній як такий. Замість цього використовуються у порівнянні зв'язки та

вагові коефіцієнти. Таким чином, при використанні схеми, представленої на рис. 1, б, виключається атака зломисникам на підміну чи компрометацію біометричного шаблону.

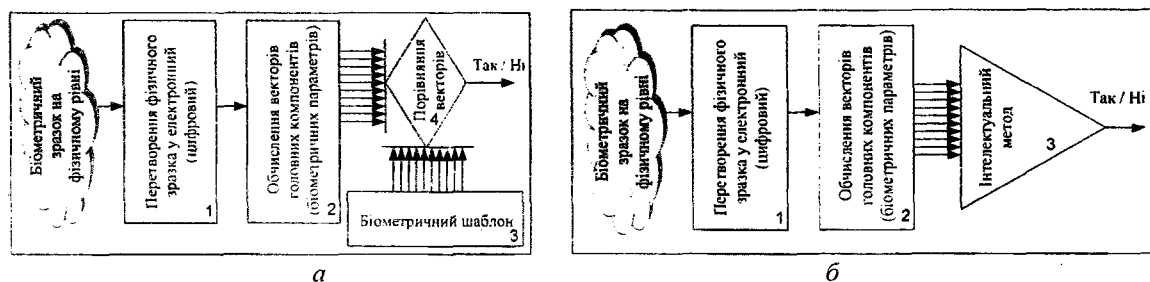


Рис. 1

При створенні інтелектуальної системи США та Російська Федерація намагаються вирішувати цю задачу з різних боків, пропонуючи два різних технічних підходи, які направлені на вирішення складностей використання біометричних даних.

Перший оснований на використанні багатошарових штучних нейронних мереж, що автоматично навчаються модифікувати біометричний образ особи в його секретний ключ [2]. При використанні нейромережових технологій основною проблемою є навчання багатошарових штучних нейронних мереж. Коли багатошарова нейронна мережа має небагато параметрів, що повинні настроюватися, то можуть бути використані відомі алгоритми навчання, але зі збільшенням параметрів розмірності нейронних мереж зростає і складність задачі навчання. Вирішення проблеми алгоритмів навчання дозволило б вирішити складності використання біометричних даних: нерівномірність інформаційного розподілу, шляхом збагачування даних за допомогою нейромережевого перетворювача.

Друга технологія при генерації ключа з біометричних параметрів використовується метод «нечітких екстракторів» [3]. Відкритий та відповідний йому секретний ключі створюються за допомогою ключа з біометричних параметрів.

Підходи істотно відрізняються. Перша технологія дозволяє отримувати сильні ключі від спеціальних генераторів випадкових чисел. Fuzzy-технологія близька до нейромережевої, але вона не припускає навчання. Fuzzy-логіка проектується однократно, та далі Fuzzy-правила не змінюються.

Біометрична характеристика людини та системи перетворення фізичного образу в цифровий

На даний момент з основних приведених біометричних характеристик людини (райдужна оболонка ока, дактилоскопія, геометрія обличчя та інші) системи розпізнавання по відбитках пальців займає більш половини біометричного ринку. Безліч російських і закордонних компаній займаються виробництвом систем управління доступом, заснованих на методі дактилоскопічної ідентифікації. Внаслідок того, що цей напрям є одним з найдавніших, він набув найбільшого поширення.

У даному розділі розглядаються порівняльні характеристики статичного біометричного методу. Як порівняльні характеристики, використані наступні показники: FRR при фіксованому значенні FAR [4]. Основними характеристиками будь-якої біометричної охоронної системи є два числа – FAR (False Acceptance Rate) і FRR (False Rejection Rate). Перше число характеризує ймовірність помилкового збігу біометричних характеристик двох людей. Друге – ймовірність відмови доступу людині, що має допуск. Система тим краще, чим менше значення FRR при однакових значеннях FAR.

Як джерело даних по FAR і FRR використовувалися статистичні дані Verifinger SDK, отримані за допомогою сканера відбитків пальців DP U.are.U (табл. 1).

Характерне значення FAR для методу розпізнавання відбитків пальців – 0,001%.

Таблиця 1

False Acceptance Rate	False Rejection Rate
0,1%	0,3%
0,01%	0,4%
0,001%	0,6%
0,0001%	0,9%

Вірогідність помилкового збігу отриманого сканером відбитку пальця для бази даних з N відбитків дорівнює $FAR \cdot N$. Щодня через пункт контролю доступу проходить теж порядку N чоловік. Тоді вірогідність помилки за робочий день $FAR \cdot N2$. Звичайно, залежно від цілей системи ідентифікації вірогідність помилки за одиницю часу може сильно варіюватися, але якщо прийняти допустимим одну помилку протягом робочого дня, то:

$$FAR \cdot N2 \approx 1 \quad (1)$$

$$N \approx \frac{1}{FAR} \quad (2)$$

Тоді отримаємо, що стабільна робота системи ідентифікації при $FAR = 0,001\%$ можлива при чисельності персоналу N , що приблизно рівний 300.

Переваги:

- висока достовірність,
- низька вартість пристроїв сканування,
- достатня простота процедури сканування відбитку.

Недоліки:

- папілярний узор відбитку пальця дуже легко ушкоджується дрібними подряпинами, порізами,
- недостатня захищеність від підробки зображення відбитку, частково викликана широким розповсюдженням методу.

Для перетворення фізичного образу в цифровий використовуються сканери. На сьогоднішній день їх існує дуже багато. Вони відрізняються по ймовірності несанкціонованого доступу, часу ідентифікації (пропускна здатність) та ймовірності помилкової тривоги (див. табл. 2).

Таблиця 2

Модель (фірма)	Ймовірність несанкціонованого доступу, %	Ймовірність помилкової тривоги, %	Час ідентифікації (пропускна здатність), с
FingerScan (Identix)	0,0001	1,0	0,5
TouchSafe (Identix)	0,001	2,0	1
TouchNet (Identix)	0,001	1,0	3
Startek	0,0001	1,0	1
U.are.U (Digital Persona)	0,01	3,0	1
FIU(Sony, I/O Software)	0,1	1,0	0,3
BioMause (ABC)	0,2	-	1
Кордон (Росія)	0,0001	1,0	1
DS-100 (Росія)	0,001	-	1...3
Veriprint 2100 (Biometric ID)	0,001	0,01	1

Сучасні системи сканування оснащені різними датчиками (температури, сили натиснення і т. п.), які підвищують ступінь захисту від підробок. З кожним днем системи стають все

більш зручними і компактними. Більшість компаній виробляють готові системи, які оснащені усім необхідним, включаючи програмне забезпечення. Інтеграторам в цій області просто немає необхідності збирати систему самостійно, оскільки це не вигідно і займе більше часу і сил, чим купити готову і вже недорогої при цьому систему, тим більш вибір буде дійсно широким.

Алгоритми обчислення біометричного образу

Після створення цифрового біометричного образу за допомогою сканерів, зберігання їх у базі суттєво зменшує стійкість від атаки злоумисника. Отже образ зберігається в системі до того часу поки не будуть зроблені наступні дії, а саме обчислення біометричних параметрів з пред'явленого образу.

Для обчислення біометричного образу було проаналізовано два існуючих алгоритми: алгоритм Precise BioMatch та алгоритм, запропонований Російсько-Вірменським (Слов'янським) державним університетом.

Алгоритм Precise BioMatch [5] використовує як переваги традиційних методів виділення ключових точок, так і передові алгоритми порівнювання візерунків. Такий подвійний підхід дозволяє отримати максимальну кількість інформації з відбитку для подальшого якісного аналізу та гарантування вірної автентифікації. Precise BioMatch створена не тільки для алгоритмів автентифікації особистості у великій базі даних (як, наприклад, алгоритм AFIS – автоматизовані системи ідентифікації відбитків пальців), але і для найкращого підтвердження особи в логічному і фізичному доступі.

Алгоритм Precise BioMatch не прив'язаний до конкретного типу датчика (сканера відбитків). Значить, користувач може зареєструвати відбитки на одному типі датчика, а проходити перевірку на іншому. Це надзвичайно важливо у випадках, коли біометричне розпізнавання використовується на великому, неконтрольованому просторі.

Метод виявлення ключових точок.

Відбиток пальця складається з певної кількості борозен і смужок. Смуги – це підняті частини шкірного покриву, борозни – запалі частини. Смуги складають так звані ключові точки: краї смуг (там, де смуги закінчуються) і роздвоєння – там, де вони розгалужуються [6].

Під час реєстрації ключові точки розташовуються у визначеному місці (рис. 2), а їх розташування один до одного та їх напрям – реєструються. На основі цих даних створюється зразок (шаблон) – інформація, яка згодом буде використана для посвідчення особи користувача.

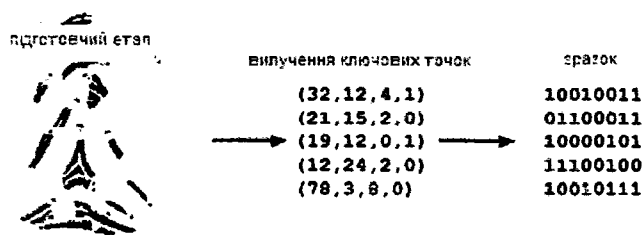


Рис. 2

На етапі зіставлення (рис. 3) лічене зображення відбитка пальця піддається попередній обробці, в ході якої витягуються ключові точки. Вони зіставляються із зареєстрованим зразком, необхідно розташувати в певному місці як можна більшу кількість схожих точок у межах заданих меж. Результатом співставлення, як правило, є набір ключових точок. Потім використовується поріг, що визначає, наскільки великим повинне бути це число, щоб було можливо зіставити відбиток пальця зі зразком.

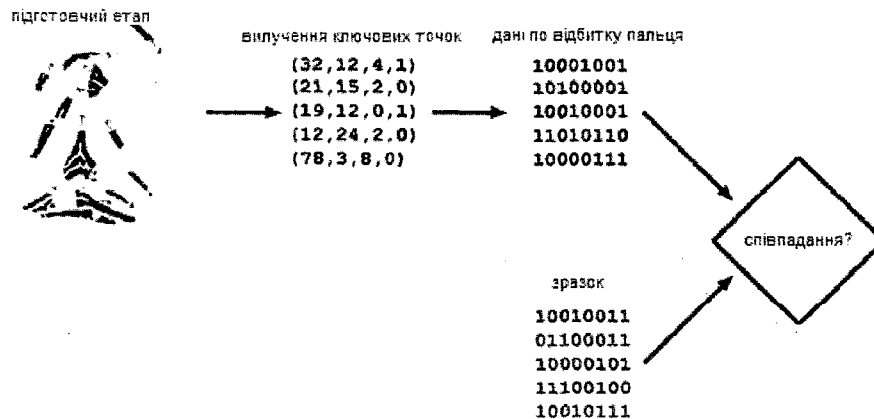


Рис. 3

Переваги:

- використовується в застосуваннях AFIS (Automated Fingerprint Identification System);
- широко відомий, добре досліджений метод;
- алгоритм підходить для множинного зіставлення.

Недоліки:

- так як метод висуває великі вимоги до дозволу і розмірів чутливого датчика, він може бути використаний не у всіх технологіях, що зчитують відбитки пальців. При використанні сканерів, менш досконалих, ніж апаратура AFIS-класу, дає низькі результати;
- люди, які не мають зовсім або мають невелику кількість ключових точок (особливий стан шкірного покриву), не можуть користуватися цією системою. Кількість ключових точок може бути обмежуючим фактором для безпеки алгоритму;
- можливі збої в системі через хибні ключових точок (ділянка, що містить помилку, що виникла із-за низької якості реєстрації, відтворення зображення або нечіткого відбитку смуг).

Метод зіставлення візерунків.

Важливою властивістю алгоритму зіставлення візерунків є те, що до уваги беруться не лише окремо взяті крапки, але і більш охоплюючі характеристики відбитка пальця. Ці характеристики можуть також включати певний відсоток додаткових даних, включаючи товщину смуг, їх кривизну або щільність. У зв'язку з цим збільшенням кількості даних, алгоритм, заснований на зіставленні візерунків, менше залежить від величини сканера і абсолютно не залежить від кількості ключових точок у відбитку пальця. Заснований на зіставленні візерунків, алгоритм, на відміну від методу виділення ключових точок, не зустрічає труднощів при розпізнаванні пальця з відбитком гіршої якості [7].

Алгоритм зіставлення візерунків Precise Biometrics під час реєстрації відбитка визначає наявність вищезазначених додаткових характеристик. Невеликі ділянки відбитка і відстань між ними беруться з загальної картини (рис. 4) з метою максимально збільшити кількість унікальної інформації. Найбільш значимі ділянки навколо ключових точок і ділянки з невеликим радіусом згину. Основна структура та унікальні комбінації смуг також є цінними даними.

Процес підтвердження (рис. 5) починається з попередньої обробки зчитаного зображення відбитка. Зареєстровані візерунки, що зберігаються у зразку, зіставляються з зображенням відбитка, що перевіряється, щоб визначити, наскільки зразок збігається із зображенням. Поріг, що описує найменше припустиме відхилення згодом використовується при визначенні ступеня відповідності відбитка наявному зразку.

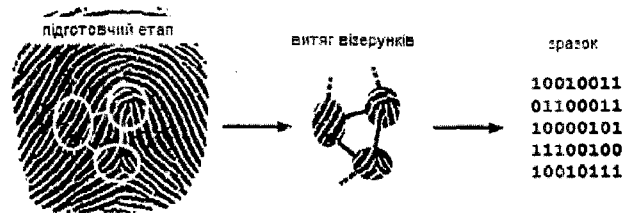


Рис. 4

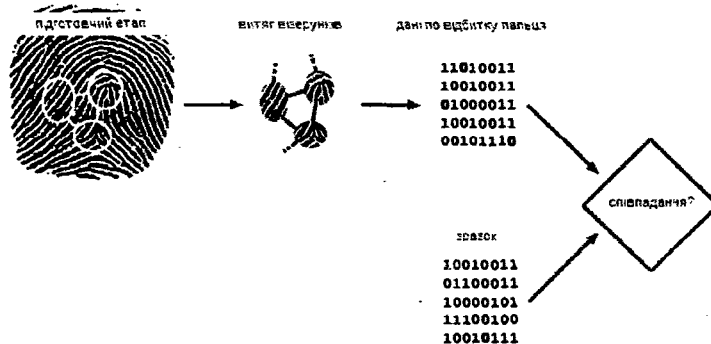


Рис. 5

Переваги:

- прекрасно працює з усіма відомими типами сканерів відбитків пальців;
- будь-який відбиток, який можна записати, може бути зареєстрований, навіть якщо він не має або має невелику кількість ключових точок;
- чудово підходить для здійснення роботи з недостатньою кількістю обчислювальних ресурсів, наприклад смарт-картою.

Недоліки:

- не може використовувати базу даних AFIS (проте, може використовувати необроблені зображення);
- не оптимізований для ідентифікації (тобто для встановлення конкретної особистості, для схеми «один до багатьох»).

Чисті алгоритми зіставлення візерунків і алгоритми, що покладаються тільки на зіставлення ключових точок, не можуть задовольнити всім вимогам. Наприклад, чистий алгоритм виділення ключових точок пред'являє дуже великі вимоги до розмірів пристрою, що зчитує, а, отже, дає погані результати при невеликому розмірі сканера або наявності у користувача невеликої кількості ключових точок. З іншого боку, чистий метод зіставлення візерунків не може працювати зі стандартизованими ключовими точками. Об'єднуючи сильні сторони обох методів, рішення Precise BioMatch пропонує розробникам і кінцевим користувачам кращі технології з обох методик і забезпечує високофункціональні і гнучкі рішення, які враховують найрізноманітніші вимоги до захисту.

Алгоритм Російсько-Вірменського державного університету дещо відрізняється від Precise BioMatch. Він складається з трьох етапів для класичної схеми процедур біометричної ідентифікації та достатньо двох для використання у схемі процедур біометричної ідентифікації з використанням інтелектуальних систем.

Опис методу

Задача ідентифікації особи по відбитку пальця вирішується шляхом зіставлення ідентифікованого відбитка з еталонними. Коефіцієнт (відсоток) відповідності обчислюється за формулою

$$K = S / \min(p, q) \cdot 100\% \quad (3)$$

де S – кількість мінуцій, що співпали, p – кількість мінуцій в еталонном відбитку, q – кількість мінуцій в ідентифікованому відбитку. Відбитки вважаються ідентичними, якщо коефіцієнт відповідності становить 65 % і вище (цей поріг можна змінити).

Метод вирішення даної задачі складається з трьох основних етапів: обробка вихідного зображення, виділення мінуцій і зіставлення мінуцій відбитків пальців.

Для докладного опису методу введемо такі позначення: I – матриця вихідного зображення. Розмірність матриці визначається розміром зображення в пікселях. Елементи матриці – натуральні числа від 0 до 255 (колір пікселя).

Множина $W(u,v,n)=\{(i,j) \mid |i-u|<n, |j-v|<n\}$ матриці є свого роду віном точки (i,j) розміром n . Вектори $P(i,j)=((i-u),(j-v))$ і $d(i,j)=P(i,j)/|P(i,j)|$ визначаються для будь-якої точки кожного вікна.

Обробка вихідного зображення.

Як правило, вихідне зображення відбитка (якщо воно не отримано електронним способом [8], має погану якість (пошкоджені лінії, мають різні спотворення і т.д.

Для достовірного визначення мінуцій необхідно обробити зображення і привести до особливого виду (формату). Процес обробки зображення здійснюється наступним чином:

- обчислення орієнтації ліній,
- поліпшення якості ліній,
- бінаризація зображення,
- потоншення ліній зображення.

Обчислення орієнтації ліній.

Для обчислення орієнтації ліній вибираються точки $(u,v) \in I$, розглядаються вікна $W(u,v,n)$, де n залежить від розмірності матриці, визначається вектор, перпендикулярний до прямої, якій належить вибрана точка, і визначаються суми:

$$S_1 = \sum_{(i,j) \in W} g_1(u,v,i,j) \quad (4)$$

$$S_2 = \sum_{(i,j) \in W} g_2(u,v,i,j) \quad (5)$$

$$g_1(u,v,i,j) = \begin{cases} 0, & |I(u,v) - I(i,j)| < T, \\ d(i,j), & |I(u,v) - I(i,j)|, d_y(i,j) \geq 0, \\ -d(i,j), & |I(u,v) - I(i,j)|, d_y(i,j) < 0, \end{cases} \quad (6)$$

$$g_2(u,v,i,j) = \begin{cases} 0, & |I(u,v) - I(i,j)| < T, \\ d(i,j), & |I(u,v) - I(i,j)|, d_x(i,j) \geq 0, \\ -d(i,j), & |I(u,v) - I(i,j)|, d_x(i,j) < 0, \end{cases} \quad (7)$$

де T – постійна величина (наприкладі $T = 60$), а вектор $d(i,j)$ було визначено вище.

Використовуючи ці формули, для всіх точок $(u,v) \in I$ визначається вектор $D(u,v)$:

$$D(u,v) = \begin{cases} \frac{S_1}{|S_1|}, & |S_1| > |S_2|, \\ \frac{S_2}{|S_2|}, & |S_2| > |S_1|. \end{cases} \quad (8)$$

Цей процес повторюється 5 разів (число 5 вибрано за результатами експериментів). Після першого застосування алгоритму деякі вектори виходять нульовими. При наступних застосуваннях алгоритму якість зображення поліпшується і, отже, кількість нульових векторів зменшується.

Для уточнення напрямків отриманих векторів розглядаються вікна $W(u,v,n)$ для всіх точок $(u,v) \in I$. Використовуючи нульовий вектор $D(i,r)$, для усіх векторів $D(i,j)$ визначають

кут між векторами $D(i,r)$ і $D(i,j)$. Якщо цей кут тупий, то $D(i,r) = D(i,r) - D(i,j)$, у противному випадку $D(i,r) = D(i,r) + D(i,j)$. Обчислюється вектор $D(u,v) = D(i,r) / |D(i,r)|$ для всіх точок вікна $W(u,v,n)$. Цей процес також повторюється 5 разів.

Поліпшення якості ліній.

Використовуючи вектори $D(u,v)$, отримані вище, і середню вагу вікон $W(u,v,n)$, можна поліпшити якість ліній, замінюючи значення всіх елементів матриці на середню вагу їх вікон. У якості ваги береться модуль $\sin \alpha$, де α – кут між векторами $D(u,v)$ і $D(i,j)$, $(i,j) \in W$. Середня вага вікна обчислюється за формулою

$$I(u,v) = \frac{S(u,v)}{Q(u,v)}, \quad (9)$$

де

$$S(u,v) = \sum_{(i,j) \in W} I(i,j) |\sin \alpha|, \quad (10)$$

$$Q(u,v) = \sum_{(i,j) \in W} I(i,j) |\sin \alpha|, \quad (11)$$

На етапі виділення мінуцій є зображення відбитків кращої якості з тонкими лініями. Для знаходження мінуцій розглядаються вікна $W(u,v,n)$ для всіх точок (u,v) матриці I (на прикладі $n = 2$ число n вибирається достатнім – але маленьким, таким, щоб у вікні не виявилися точки чорного кольору з сусідніх ліній).

Вибирається центральна точка вікна і підраховується кількість чорних (ненульових) пікселів, що знаходяться навколо вікна. Піксель в центрі вважається мінуцією, якщо він сам ненульовий, і кількість ненульових пікселів навколо вікна – одне (мінуція типу «закінчення») або три (мінуція типу «роздвоєння»). Координати виявлених мінуцій і їх кути орієнтації записуються у вектор $M(p)$, p – кількість мінуцій. Даний підхід дозволяє отримати всі можливі потенційні мінуції. Реальні мінуції визначаються шляхом видалення з множини $M(p)$ сусідніх і крайових точок зображення.

Для видалення сусідніх точок розглядається пара елементів множини $M(p)$. Обчислюється відстань між елементами даної пари. Елементи, відстань між якими менше, ніж задана величина T (на прикладі $T = 2$), видаляються з безлічі, а в безліч додається середня точка цих елементів. Цей процес виконується для всіх можливих пар елементів множини $M(p)$. У підсумку виходить безліч мінуцій $M(r)$, де $r \leq p$.

На наступному етапі виявляються і видаляються мінуції тих ділянок, які у вихідному зображенні мали погану якість та при поліпшенні якості не відновилися. Видалення цих точок виконується наступним чином: з безлічі $M(r)$ видаляються ті точки (u,v) , яким відповідає нульовий вектор $D(u,v)$. Отриману безліч мінуцій позначимо через $M(q)$, де $q \leq r$. Остаточна безліч реальних мінуцій визначається шляхом видалення крайових точок зображення. З безлічі $M(q)$ видаляються ті точки, відстань яких від краю зображення менше, ніж заздалегідь задана величина $T1$ (на прикладі $T1 = 8$). Після завершення цього етапу виходить безліч реальних мінуцій, яка на наступному етапі буде використовуватися для порівняння відбитків пальців.

Алгоритм роботи методу рециркуляційних нейронних мереж

Рециркуляційні нейронні мережі (PHM) (recirculation neural network) [9] представляють собою багатосарові нейронні мережі, що є аналогом так званих нейронних мереж «bottleneck» [10], які дозволяють вирішувати клас задач по стисненню інформації. Архітектура такої мережі представлено на рис. 6

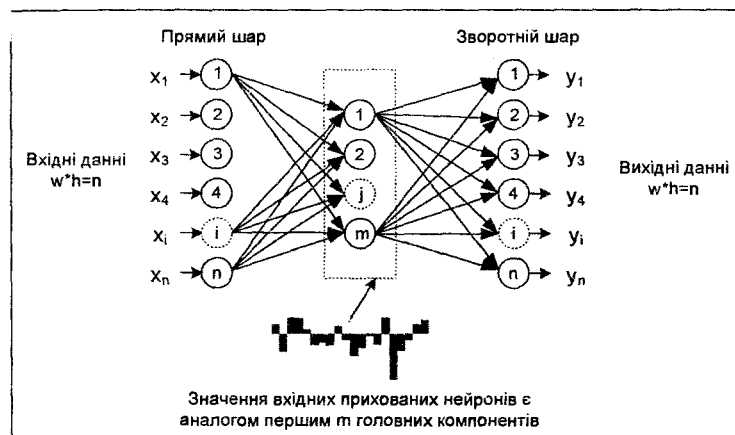


Рис. 6

Обчислення виходів нейронної мережі: $y_{ki} = x_i, k = 0$;

$$y_{ki} = \tanh \left(\sum_{j=1}^p y_{k-1,j} w_{kij} \right), k = 1..L, \quad (12)$$

де $\tanh(\cdot)$ – функція гіперболічного тангенса; k – поточний шар, зростає від 0 до L ; p – кількість нейронів у попередньому ($k-1$) шарі; i – індекс нейрона у поточному шарі; j – індекс нейрона в попередньому шарі; x_i – піксель вхідного зображення; y_{ki} – значення виходів шару k (і вхідні значення наступного шару); w_{kij} – синаптична вага, що з'єднує нейрон j_{k-1} і нейрон i_k ; L – індекс останнього шару.

Оскільки мережа ініціалізується випадковими значеннями, відповідності між номерами компонент і нейронами немає. Для реконструкції зображення на вихід нейронів прихованого шару подають обчислені вектори головних компонентів і розраховують значення вихідного шару.

Для навчання мережі застосовується алгоритм корекції синаптичних ваг (зворотне поширення похибки). Для останнього шару обчислюється похибка (різниця між вихідними y_{ki} і еталонними t_i значеннями) і поширюється назад по мережі крізь ваги прихованих нейронів. Величина корекції помилки δ_{ki} :

$$\delta_{ki} = (y_{ki} - t_i)(1 - y_{ki}^2), k = L; \quad (13)$$

$$\delta_{ki} = \left(\sum_{j=1}^q \delta_{k+1,j} w_{k+1,ji} \right) (1 - y_{ki}^2), k = (L-1)..1, \quad (14)$$

де k зменшується від L до 1; q – число нейронів у шарі $k+1$, для РНМ еталоном є вхідні вектори головних компонентів: $t_i = y_{0,i}$.

Подальше коригуються ваги:

$$w_{kij}(t+1) = w_{kij}(t) - \alpha(t) \delta_{ki} y_{k-1,j}, k = 1..L, \quad (15)$$

де $\alpha(t)$ – крок навчання; t – дискретний час. Для класичного зворотного поширення швидкість фіксована. Існують евристичні підходи, в яких швидкість змінюється від більшої спочатку до меншої в кінці навчання.

Головна перевага підходу – адаптивний крок, який розраховується індивідуально для кожного шару на кожній ітерації, щоб зробити кращий крок у напрямі мінімізації середньоквадратичної похибки мережі:

$$\alpha(t) = \frac{\sum_{i=1}^r \frac{\delta_{ki}^2}{1 - y_{ki}^2}}{\left(1 + \sum_{j=1}^p y_{k-1,j}^2\right) \left(\sum_{i=1}^r \delta_{ki}^2\right)}, \quad (16)$$

де r – число нейронів у шарі k . Слід приймати $\frac{\delta_{ki}^2}{1 - y_{ki}^2} = 0$ при $1 - y_{ki}^2 = 0$ і $\alpha(t) = 0$ при $\sum_{i=1}^r \delta_{ki}^2 = 0$.

Адаптивний крок позбавляє від необхідності вибирати крок вручну, що зменшує вплив людського фактору. Процес навчання сходиться порівняно швидко і стабільно. Для простоти не використовувалося роздільне навчання.

Перед навчанням синаптичні ваги мережі ініціалізуються невеликими випадковими значеннями $[-0.01; +0.01]$.

Навчальний процес складається з послідовності навчальних епох і завершується, коли їх кількість перевищує допустиме значення або помилка нейронної мережі стає менше заданої.

Висновки

У результаті аналізу проблемних питань систем автентифікації осіб були розглянуті можливі моделі біометричної автентифікації у класичному вигляді, які використовуються в біометричних стандартах США, Російської Федерації та країн ЄС щодо підвищення стійкості від загроз в сфері інформаційної безпеки, та з використанням гібридних інтелектуальних методів. Було визначено перспективну модель біометричної автентифікації та ідентифікації особи для впровадження та застосування в Україні.

Список літератури: 1. *Standards and projects under the direct responsibility of JTC 1/SC 37 Secretariat.* Точка доступу: http://www.iso.org/iso/iso_catalogue/-catalogue_tc/catalogue_tc_browse.htm?commid=-313770&published=on 2. *ГОСТ Р 52633-2006 «Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации».* 3. *Dodis Y. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data / Dodis Y., Reyzin L., Smith A. // Advances in Cryptology – EUROCRYPT 2004. Christian Cachin and Jan Camenisch, ed. Vol. 3027 of Lecture Notes in Computer Science. Springer – Verlag. – 2004. – P. 79-100.* 4. *Characteristics of biometric systems.* Точка доступу: <http://www.ccert.edu.cn/education/cissp/hism/039-041.html> 5. *ISO/IEC 7816-11. Personal Verification Through Biometric Methods.* 6. *ISO/IEC 19794-2. Finger Minutiae Data.* 7. *ISO/IEC 19794-4. Finger Image Data.* 8. *Задорожний В. Идентификация по отпечаткам пальцев. // PC Magazine, № 1, 2, 2004.* 9. *Bryliuk D., Starovoitov V. Application of recirculation neural network and principal component analysis for face recognition // The 2nd International Conference on Neural Networks and Artificial Intelligence, October 2-5, 2001, Minsk, Belarus, pp. 136-142.* 10. *Haykin S. Neural Networks: A Comprehensive Foundation. – Pearson Education, Inc., 2005. – 823 p.*

Харківський національний
університет радіоелектроніки

Надійшла до редколегії 11.08.2011

МЕТОДЫ АНАЛИЗА ПРОЦЕССОВ КОНТРОЛЯ КАЧЕСТВА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, ИСПОЛЬЗУЕМЫЕ ПРИ ПРОЕКТИРОВАНИИ И РАЗРАБОТКЕ СИСТЕМ ОБРАБОТКИ КРИПТОГРАФИЧЕСКОЙ ИНФОРМАЦИИ

Технические термины в области программного обеспечения (ПО) определены в стандартах ISO/IEC 9126-1, IEEE/IEC 12207, IEEE 1028 [1 – 3], что позволяет однозначно сформулировать используемую терминологию. В стандарте ISO/IEC 9126-1[4] определены соответствующие характеристики качества, при которых фундаментальный процесс тестирования состоит: из планирования и контроля, анализа и проектирования, внедрения и сопровождения оценки критериев для завершения тестирования и создания отчетной документации. Процесс тестирования базируется на сопоставлении ожидаемого (описанного в технической документации) и фактического (полученного в ходе испытаний) результата. В случае, когда результаты процессов совпадают, тест считается пройденным успешно.

Для достижения структурированной и управляемой разработки программного обеспечения используются модели разработки ПО. На данный момент известны и активно используются фундаментальные модели (модель «водопада» и V-модель) [5] и пошаговые модели (RAD, RUP, XP, SCRUM, DSDM) [6]. Важную роль в процессе разработки и тестирования ПО играет психологический аспект. Человек не склонен замечать свои собственные ошибки. Этот факт относится к аспектам организации и проведения процесса тестирования[7]. Поэтому процессы разработки и тестирования должны быть организованы независимо друг от друга.

Для получения объективной оценки о качестве ПО, с точки зрения функциональности, надежности, удобства использования, эффективности и гибкости к модификациям, необходимо использовать различные методы, которые можно разделить на две большие группы: статического и динамического анализа.

Под статическим анализом понимают анализ программного обеспечения, производимый без реального выполнения исследуемых программ. Как правило, важность методов статического анализа недооценивается, однако полученные результаты позволяют оптимизировать процесс разработки и обнаружить ошибки и отклонения от технической документации, стандартов и плана проекта. Кроме того, статический анализ может быть использован в целях выявления проблем безопасности (например, отсутствие защиты от переполнения буфера или отсутствие проверки входных данных на допустимые значения).

Ключевыми понятиями статического анализа являются экспертная оценка и инспекция (обзор). Существует четыре основных типа обзора: анализ со стороны руководства, технический анализ, информационный анализ, пошаговый анализ [8].

Количественные характеристики качества при статическом анализе могут быть получены путем использования метрик [9]. Метрики сложности программ принято разделять на три основные группы.

Метрики первой группы базируются на определении количественных характеристик, связанных с размером программы, и отличаются относительной простотой. К наиболее известным метрикам данной группы относится набор метрик Холстеда [9].

Основу метрики Холстеда составляют четыре измеряемые характеристики программы:

- NU_{Optr} (Number of Unique Operators) – число уникальных операторов программы, включая символы-разделители, имена процедур и знаки операций;
- NU_{Oprnd} (Number of Unique Operands) – число уникальных операндов программы;
- N_{Optr} (Number of Operators) – общее число операторов в программе;
- N_{Oprnd} (Number of Operands) – общее число операндов в программе.

На основании этих характеристик рассчитываются оценки длины программы, объема программы, сложности программы:

- длина программы (Halstead Program Length, HP_{Len}): $HP_{Len} = N_{Oprtr} + N_{Oprnd}$;
- объем программы (Halstead Program Volume, HP_{Vol}): $HP_{Vol} = HP_{Len} \log_2 HP_{Voc}$;
- сложность программы (Halstead Difficulty, H_{Diff}): $H_{Diff} = (NU_{Cprtr}/2) \times (N_{Oprnd} / NU_{Oprnd})$.

Метрики второй группы ориентированы на анализ исходного кода программы. Представителем данной группы является метрика цикломатической сложности по Мак-Кейбу, которая базируется на основе графа управляющей логики, в котором вычислительные операторы или выражения представляются в виде узлов, а передача управления между узлами – в виде дуг (см. рис. 1)

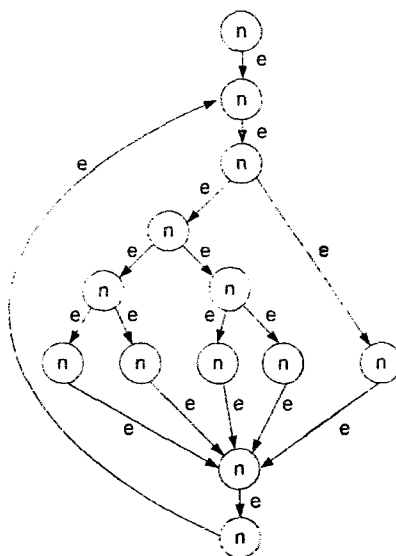


Рис. 1. Вид графа управляющей логики

Показатель цикломатической сложности позволяет оценить трудоемкость реализации отдельных элементов программы и скорректировать общие показатели оценки длительности и стоимости проекта. Упрощенная формула вычисления цикломатической сложности представляется следующим образом:

$$C = e - n + 2.$$

где e – число ребер. n – число узлов на графе управляющей логики.

Показатель цикломатической сложности по Мак-Кейбу показывает требуемое количество проходов для покрытия всех связей в графе или количество тестовых прогонов программы, необходимых для наиболее полного тестирования.

Метрики третьей группы базируются на оценке использования, конфигурации и размещения данных в программе. К данной группе относятся метрика Чепина [9].

Суть метрики состоит в оценке информационной стойкости отдельно взятого программного модуля с помощью анализа характера использования переменных из списка входных и выходных переменных (список ввода-вывода). Все множество переменных, составляющих список ввода-вывода, разбивается на четыре функциональные группы:

- множество «Р» – вводимые переменные для расчетов и для обеспечения вывода;
- множество «М» – модифицируемые или создаваемые внутри программы переменные;
- множество «С» – переменные, участвующие в управлении работой программного модуля;
- множество «Т» – не используемые в программе переменные.

Значение метрики Чепина рассчитывается по формуле

$$Q = a_1P + a_2M + a_3C + a_4T.$$

где a_1, a_2, a_3, a_4 – весовые коэффициенты, которые используются для отражения различного влияния на сложность программы каждой функциональной группы.

Использование статических методов анализа дает возможность уменьшить затраты на проведение тестирования за счет использования метрик. Результаты использования метрик должны быть получены до начала обзора и должны служить входными данными для экспертной оценки.

Динамический анализ представляет собой процесс оценки поведения системы или компонента системы (тест-объекта) во время выполнения (например, производительности памяти, использования процессора).

Существует несколько подходов для проведения тестирования тест-объекта, которые можно разделить на две группы: тестирование черного ящика и тестирование белого ящика.

При тестировании черного ящика, компонент системы рассматривается как объект внутреннее устройство которого неизвестно [10]. Тестовые данные берутся из спецификации тестового объекта. Эффективно применять такие техники тестирования черного ящика: анализ эквивалентных классов, анализ граничных значений, построение причинно-следственных связей, построение диаграмм прецедентов.

Основу техники анализа эквивалентных классов составляют два положения:

- исходные данные необходимо разбить на конечное число классов эквивалентности. Классом эквивалентности $C(a)$ элемента a называется подмножество элементов, эквивалентных a . Из приведенного определения следует, что, если $b \in C(a)$, то $C(a) = C(b)$. В одном классе эквивалентности содержатся такие тесты, что, если один тест из класса эквивалентности обнаруживает некоторую ошибку, то и любой другой тест из этого класса эквивалентности должен обнаруживать эту же ошибку;

- каждый тест должен включать, по возможности, максимальное количество классов эквивалентности, чтобы минимизировать общее число тестов.

Разработка тестов данной техникой осуществляется в два этапа: выделение классов эквивалентности и построение теста. Классы эквивалентности выделяются путём выбора каждого входного условия, которые берутся из технического задания или спецификации.

Техника анализа граничных значений представляет собой определение максимальных и минимальных значений на границах классов эквивалентности. Разработка тестов этой техникой осуществляется путем составления позитивных (используются значения, принадлежащие классу эквивалентности) и негативных тестов (используются значения, не принадлежащие рассматриваемому классу эквивалентности).

Данная техника отображает взаимосвязь между причинами возникновения ошибки и их влиянием на компоненты системы (см. рис. 2).

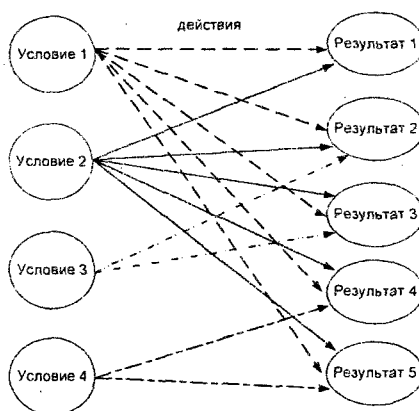


Рис. 2. Отображение причинно-следственных связей на графе

Разработка тестов этой техникой осуществляется путем разбиения спецификации на части, для каждой из которых определяется множество причин и следствий. Под причиной понимается отдельное входное условие или класс эквивалентности. Следствие представляет собой выходное условие или преобразование системы. На основе анализа семантического (смыслового) содержания спецификации строится граф, в котором последовательно перебираются всевозможные комбинации причин и следствия для них. После построения графа делаются выводы о том, какие условия должны быть объединены в отдельные тесты.

Техника построения диаграммы прецедентов используется для отображения внешнего вида системы с точки зрения пользователя и для моделирования взаимосвязей между различными подсистемами.

Основой для тестирования белого ящика служит исходный код тестового объекта. Поэтому, техники тестирования белого ящика также называют структурным тестированием. Основная идея тестирования заключается в выполнении каждой части кода тестового объекта хотя бы один раз. Операторы и условия которые используются в тестируемой части кода представляются в виде блок-схем (см. рис. 3).

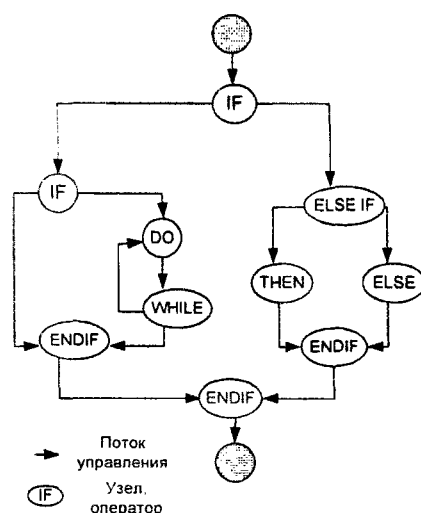


Рис. 3. Фрагмент кода программы

Использование блок-схем упрощает задачу создания тестов за счет наглядного представления механизма функционирования программного кода, позволяя наиболее полно найти существующие недостатки за минимальное время.

Для достижения высоких показателей качества ПО необходимо исчерпывающее тестирование, то есть тестирование над всеми возможными наборами данных. В большинстве случаев это невозможно из-за недостатка времени на проведение тестирования. Решением данной проблемы служит совокупное использование рассмотренных методов, выбор наиболее приоритетных тестов (по результатам каждого метода составляется набор тестов) в соответствии с функциональными требованиями, выдвигаемыми к системе.

Методы и техники тестирования необходимо выбирать в зависимости от сложности структуры системы, требований, которые выдвинуты к системе, и временных рамок, в пределах которых система должна быть введена в эксплуатацию.

При планировании и проведении тестирования необходимо учитывать требования: соответствие стандартам, результаты проведенного анализа рисков системы, опыт персонала; наличие инструментария для проведения автоматического тестирования и технической документации по ней.

При управлении процессом тестирования необходимо осуществлять планирование, мониторинг и контроль на различных циклах испытаний. Проведение тестирования осуществляется согласно документации – плану тестирования. В плане тестирования должна быть

описана стратегия (цели, меры, средства) тестирования и приоритетность проведения испытаний, основанная на анализе рисков. Анализ рисков представляет собой анализ вероятности появления ошибок после проведения испытания. Количество и интенсивность испытаний должны быть адаптированы с конкретными потребностями проекта.

Список литературы: 1. *ISO/IEC 9126-1:2001, Software Engineering. – Product quality – Part 1: Quality model, Quality characteristics and sub-characteristics.* 2. *IEEE/EIA Std 12207-1996: Information Technology – Software life cycle processes.* 3. *IEEE Std 1028-1996: IEEE.* 4. *ISO/IEC 9126-1:2001, Software Engineering. – Product quality – Part 1: Quality model, Quality characteristics and sub-characteristics.* 5. *Boehm, B. W: "A Spiral Model of Software Development and Enhancement", ACM SIGSOFT, August 1986, pp. 14-24.* 6. *Spillner, A. From V-model to W-model – Establishing the Whole Test Process / Proceedings.* 7. *IEEE Std 829-1998, IEEE Standard for Software Test Documentation (under revision, new edition probably in 2006).* 8. *Beizer, B. Software Testing Techniques, Van Nostrand Reinhold, 1990.* 9. *Fenton, N. E.: Software Metrics, Chapman&Hall, 1991.* 10. *Beizer, B. Black-Box Testing, John Wiley & Sons, 1995.* 11. *Fenton, N. E.: Software Metrics, Chapman&Hall, 1991.* Conquest 2000 – Workshop on "Testing Non-Functional Software Requirements", Sept. 2000. Nuremberg, pp. 221-231.

*Харьковский национальный
университет радиоэлектроники*

Поступила в редколлегию 12.07.2011.

СТРУКТУРНО-ИНФОРМАЦИОННЫЕ ПОРТРЕТЫ ИНФОРМАЦИОННОЙ СИСТЕМЫ В УСЛОВИЯХ НЕОПРЕДЕЛЕННОСТИ НА ПРИМЕРЕ DOS-АТАКИ

Постановка проблемы

В настоящее время в Украине практически нет отраслей, где бы ни использовались информационные системы, выполняющие телекоммуникационные, информационные и расчетные функции (обработка и обмен данными, хранение информационных ресурсов, формирование сигналов управления критическими системами, построение графиков, отчетов и др.). При этом их управление осуществляется по отдельным, заранее известным алгоритмам. Однако проведенные исследования показали наличие в большинстве информационных систем различного рода структурных и функциональных априорных неопределенностей, что предполагает использование средств моделирования нечетких данных и знаний, нечеткого логического выделения, методов теории адаптивных систем [1 – 4, 7].

Анализ литературы [2 – 5, 7, 8] показал, что существующие подходы к идентификации и моделированию информационных систем оперируют априорными данными или результатами компьютерного моделирования. Однако в условиях априорной неопределенности до настоящего времени каких-либо методов или формализованных процедур выбора структуры модели не предложено.

В работе [7] был предложен подход к построению модели информационной системы на основе структурно-информационных портретов и предложен комплексный показатель эффективности функционирования системы. Однако вопросам оценки влияния внешних факторов воздействия на состояние информационной системы и изменение характеристик структурно-информационных портретов в данной работе внимания не было уделено.

Поэтому актуальной научной задачей представляется построение и исследование наблюдаемых структурно-информационных портретов информационных систем с оценкой и выбором информативных переменных в условиях воздействия различного рода внешних факторов (в том числе и негативных).

Моделирование информационных систем в условиях априорной неопределенности

В [2] представлена динамическая модель информационной системы на основе наблюдаемого структурно-информационного портрета, учитывающая апостериорные данные о ее структурных изменениях в условиях внешних воздействий. Причинно-следственные связи в структурно-функциональном пространстве R исследуемого объекта на множестве апостериорных данных $I_{an} = \{Y(t), U(t), \chi(t), \xi(t), t \in R^t\}$ описываются с помощью выражений

$$S(t) = F_I(S, A_1, U, \chi, \xi, t, \tau), \quad (1)$$

$$Y(t) = F(S, A, U, \chi, \xi, t), \quad (2)$$

а множество динамических процессов в объектах управления задается с помощью дифференциального уравнения с одним входом и выходом [2]

$$a_0 y^{(m)} + a_1 y^{(m-1)} + \dots + a_m y = b_0 u^{(k)} + b_1 u^{(k-1)} + \dots + b_k u + \xi + \chi, \quad (3)$$

где $S(t) \in R^s$ – вектор внутреннего состояния объекта управления, $\tau \in \mathcal{T}$ – некоторый интервал времени (временная задержка). F_I, F – внутренние нелинейные операторы, структура которых известна с точностью до векторов искомых параметров $A_1(t), A(t)$, принадлежащих ограниченной, но априори неизвестной области $G_A \subseteq R^v$. $Y(t)$ – вектор выходных параметров системы.

Исследования [1 – 4, 7] показали, что для линейного стационарного объекта управления уравнение в пространстве состояний имеет вид [2, 7]:

$$\dot{X} = AX + BU + \xi + \chi, \quad (4)$$

$$Y = CX + DU + \zeta, \quad (5)$$

где $X \in R^m$ – вектор состояния, $A \in R^{m \times m}$ – матрица состояния, $U \in R^k$ – вектор входа, $Y \in R^n$ – вектор выхода, $B \in R^{m \times k}$, $C \in R^{n \times m}$, $D \in R^{n \times k}$, $\zeta \in R^n$ – ненаблюдаемый вектор ошибок измерения, $\xi \in R^m$, $\chi \in R^m$ – вектора помех (ξ – контролируемые возмущения, χ – неконтролируемые шумы).

В [3] показано, что реализация моделей в пространстве состояний связана с необходимостью оценки ненаблюдаемых компонентов вектора $X(t)$ на множестве I_{an} . Однако, как показали исследования, в условиях априорной неопределенности данная задача не всегда выполнима с заданной точностью. В то же время решение о структуре модели исследуемой системы должно приниматься исходя из принципа информационной полноты анализируемых (используемых при моделировании) данных (множества $I = \{I_a, I_{an}\}$, где I_a, I_{an} – соответственно априорная и апостериорная информация об объекте исследования). Особенно это важно в условиях априорной неопределенности, характерной для функционирования информационных систем.

Используем приведенные выше предложения при моделировании информационной системы. Для этого рассмотрим систему уравнений [3]:

$$\dot{X} = F(X, U, A, t), \quad (6)$$

$$Y = F_Y(X, U, A_1, t),$$

где $U \in \Omega_U \subset \hat{U} \subseteq R^m$ – входной вектор системы, $Y \in \hat{Y} \subseteq R^n$ – выход системы, $X \in \hat{X} \subseteq R^q$ – вектор состояния, $\hat{U}, \hat{Y}, \hat{X}$ – множества входных и выходных сигналов, а также состояний системы соответственно, $\hat{Y} \subseteq \hat{X} \subseteq R^n$, $A \in R^{q \times p}$, $A_1 \in R^{n \times q}$ – матрицы параметров, $F : R^q \times R^m \times J \rightarrow R^q$ – гладкая непрерывно дифференцируемая по $\hat{X}$ и по A вектор-функция, $t \in J$, $F_Y : R^q \times R^m \times J \rightarrow R^n$ – функция, задающая способ формирования выходного вектора системы.

В состав множества I_{an} входят не сами векторы U и Y , а их наблюдаемые и вычисляемые аналоги (векторы $\tilde{U}(t)$, $\tilde{Y}(t)$, $\tilde{K}(t)$), которые получаются в результате мониторинга информационной системы и применения операторов f_U, f_Y, f_K в пространствах $\aleph, \mathfrak{N}, \mathfrak{Z}$ входных и выходных векторов соответственно, а так же временном пространстве J :

$$f_U : \aleph \times J \rightarrow R^m, f_Y : \mathfrak{N} \times J \rightarrow R^n, f_K : \mathfrak{Z} \times J \rightarrow R^k. \quad (7)$$

Следует заметить, что указанные в (6) операторы отражают также ошибки измерения.

Операторы $f_U \in N_U$, $f_Y \in N_Y$ определены на множествах N_U, N_Y , характеризующих неопределенность процесса измерения. В зависимости от доступности процесса наблюдения множества N_U и N_Y могут иметь как нечеткую природу, так и статистическую [2, 3].

Как показали исследования [2, 3, 7], при идентификации динамических систем целесообразно использовать множество I_{an} . Используя операторы (7), получим множество наблюдений (наблюдаемое структурно-информационное множество)

$$I_{an} = I(\tilde{U}, \tilde{Y}) = \left\{ \tilde{U} \in R^m, \tilde{Y} \in R^n \mid \tilde{U}(t) = f_U(U, t), \tilde{Y}(t) = f_Y(Y, t) \forall (t \in J) \right\}. \quad (8)$$

Представим множество (8) в виде: $I_{an} = I(\tilde{U}, \tilde{Y}) = I(\tilde{U}) \cup I(\tilde{Y}) \quad \forall t \in J$.

Определим бинарное отношение Z между множествами $\tilde{U}$ и $\tilde{Y}$ системы (6): $Z \subset \tilde{U} \times \tilde{Y}$. Назовем это множество портретом системы (6) в пространстве $\mathbb{N} \times \mathbb{R}$. Соответствующий фазовый портрет системы (6) представим в виде

$$Z_\phi \subset \hat{X} \setminus \hat{U} \times \hat{Y} \quad \forall U(\cdot) \in \Omega_U. \quad (9)$$

Расширенным фазовым портретом системы будем называть отображение $Z_\phi \subset \hat{X} \times \hat{U} \quad (\forall U(\cdot) \in \Omega_U) \& (\forall t \in J)$.

Для любого наблюдаемого структурно-информационного множества $I(\tilde{U}, \tilde{Y})$ (8) системы (6) определенного в пространстве $\mathbb{N} \times \mathbb{R}$, наблюдаемые структурно-информационными портретами, называются бинарные отношения:

$$Z_i = Z_i(I_{an}) \subset I(\tilde{U}) \times I(\tilde{Y}), \quad (10)$$

$$Z_i = Z_i(I_{an}) \subset I(\tilde{U} / \tilde{Y}) \times I(\tilde{Y}). \quad (11)$$

Из (10) следует, что $Z \subseteq Z_i$ и $dom(Z_\phi) = rng(Z)$, т. е. между ними существует структурное соответствие.

Исследование информационной системы в условиях воздействия DOS-атаки

Проведем сравнительное исследование расширенного фазового и наблюдаемых структурно-информационных портретов подсистемы информационного обеспечения [7] информационной системы на примере входного трафика данных в условиях воздействия на нее Dos-атаки.

На рис. 1. представлен расширенный фазовый портрет подсистемы информационного обеспечения в условиях воздействия на подсистему информационного обеспечения Dos-атаки, при этом в качестве показателя системы выступает характеристика интенсивности входного (рис. 1, а) и выходного (рис. 1, б) трафика данных. Для наглядности графика количество отсчетов показателя интенсивности входного и выходного трафика ограничено числом 150.

Сравнивая рис. 1, а и 1, б, следует отметить изменения, характерные для исследуемого вида внешнего воздействия на информационную систему (Dos-атаку). Прежде всего, это появление второго «уровня» показателя интенсивности трафика данных (см. рис. 1), связанного с увеличением интенсивности входного потока данных. На практике именно это увеличение чаще всего приводит к деструктивным изменениям в исследуемой системе.

Использование расширенного фазового портрета в определенной степени дает картину структурных изменений в системе при воздействии внешних факторов, однако информации о внутренних свойствах системы с помощью фазовых портретов получить чаще всего невозможно. Поэтому при моделировании информационной системы целесообразно использовать и структурно-информационные портреты системы.

На рис. 2. представлены наблюдаемые структурно-информационные портреты подсистемы информационного обеспечения в условиях воздействия на нее Dos-атаки, при этом в качестве измеряемых векторов наблюдаемого структурно-информационного множества $I(\tilde{U}, \tilde{Y})$ выступают интенсивность входного ($\tilde{U}$) и выходного ($\tilde{Y}$) трафика данных (рис. 2, а),

коэффициент структурности $K(t) = \frac{\tilde{Y}(t)}{\tilde{U}(t)}$ (рис. 2, б), и коэффициент пачечности

$K_n(t) = \frac{\tilde{V}_{\max}(t)}{\tilde{V}_{cp}(t)}$ (рис 2, в), где $\tilde{V}_{\max}$ – максимальная скорость передаваемых данных, $\tilde{V}_{cp}$ – средняя скорость передаваемых данных.

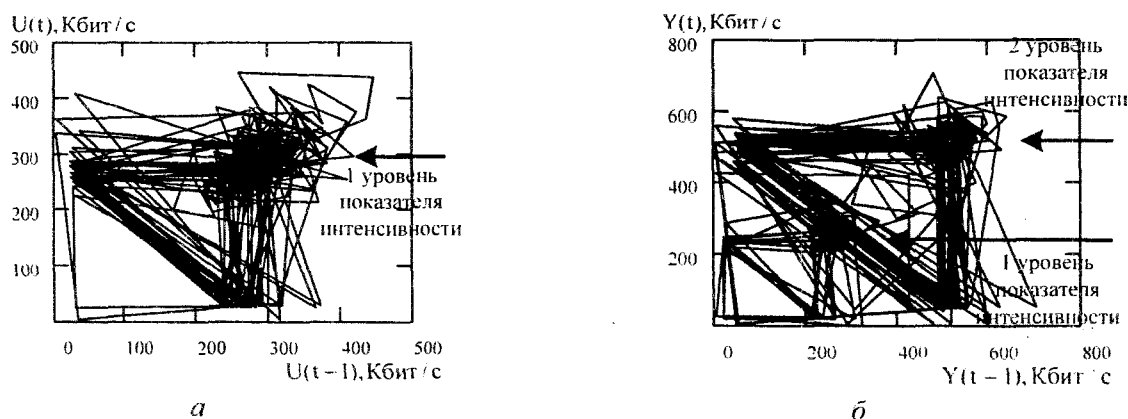


Рис. 1

Анализ графиков на рис. 1 и 2 позволяет сделать вывод о разнородности траекторий наблюдаемых структурно-информационных портретов и траекторий на фазовой плоскости подсистемы информационного обеспечения. Это подтверждает гипотезу о том, что множества Z_ϕ и Z_i имеют различные структуры. Данная закономерность объясняется, прежде всего внутренними свойствами подсистемы информационного обеспечения и структурной сложностью информационного трафика.

Рассмотренные на рис. 2 примеры построения наблюдаемых структурно-информационных портретов иллюстрируют структуру системы в пространствах $\mathbb{N} \times \mathbb{R}$ (рис. 2, а), $\mathbb{Z} \times \mathbb{R}$ (рис. 2, б, в) и могут быть использованы при решении задачи структурной идентификации.

Однако, как показали исследования, на основе качественной (визуальной) информации состоянии исследуемых объектов можно сделать вывод только о стационарности (или нестационарности) системы. При этом остается нерешенным вопрос выбора информативных переменных наиболее полно описывающих состояние системы. Поэтому следующей важной научной задачей представляется задача исследования наблюдаемых структурно-информационных портретов на предмет выбора кортежа информативных векторов, наиболее полно описывающих структурные особенности системы.

Проведенные исследования [8] показали, что в теории идентификации для решения данной задачи чаще всего используются методы корреляционного анализа [2, 3, 6, 8], при этом в качестве показателя отбора применяется коэффициент взаимной корреляции.

Пусть исследуемый объект, описывается уравнением:

$$y(t) = f(t, U), \quad \{y(t) = f(t, K), y(t) = f(t, Kn)\}, \quad (12)$$

где $f(\cdot)$ – функция заданного класса.

Рассмотрим проекцию наблюдаемых структурно-информационных портретов Z_i на плоскости $\{y, u_i\}$, $\{y, k_i\}$, $\{y, kn_i\}$, где $u_i \in \mathbb{N}$, $k_i \in \mathbb{Z}$, $kn_i \in \mathbb{Z}$ – точки входных данных мониторинга в пространствах $\mathbb{N}$, $\mathbb{R}$, $\mathbb{Z}$ (см рис. 3, а, б, в соответственно). Получим сужение отображений $Z_i: Z_i^{u_i} \subset Z_i|_{u_i \in U}$, $Z_i: Z_i^{k_i} \subset Z_i|_{k_i \in K}$, $Z_i: Z_i^{kn_i} \subset Z_i|_{kn_i \in U}$ и траектории движения системы, заданные графиками $\varphi_{u_i}: I(y) \rightarrow I(u_i \in U)$, $\varphi_{k_i}: I(y) \rightarrow I(k_i \in K)$, $\varphi_{kn_i}: I(y) \rightarrow I(kn_i \in Kn)$.

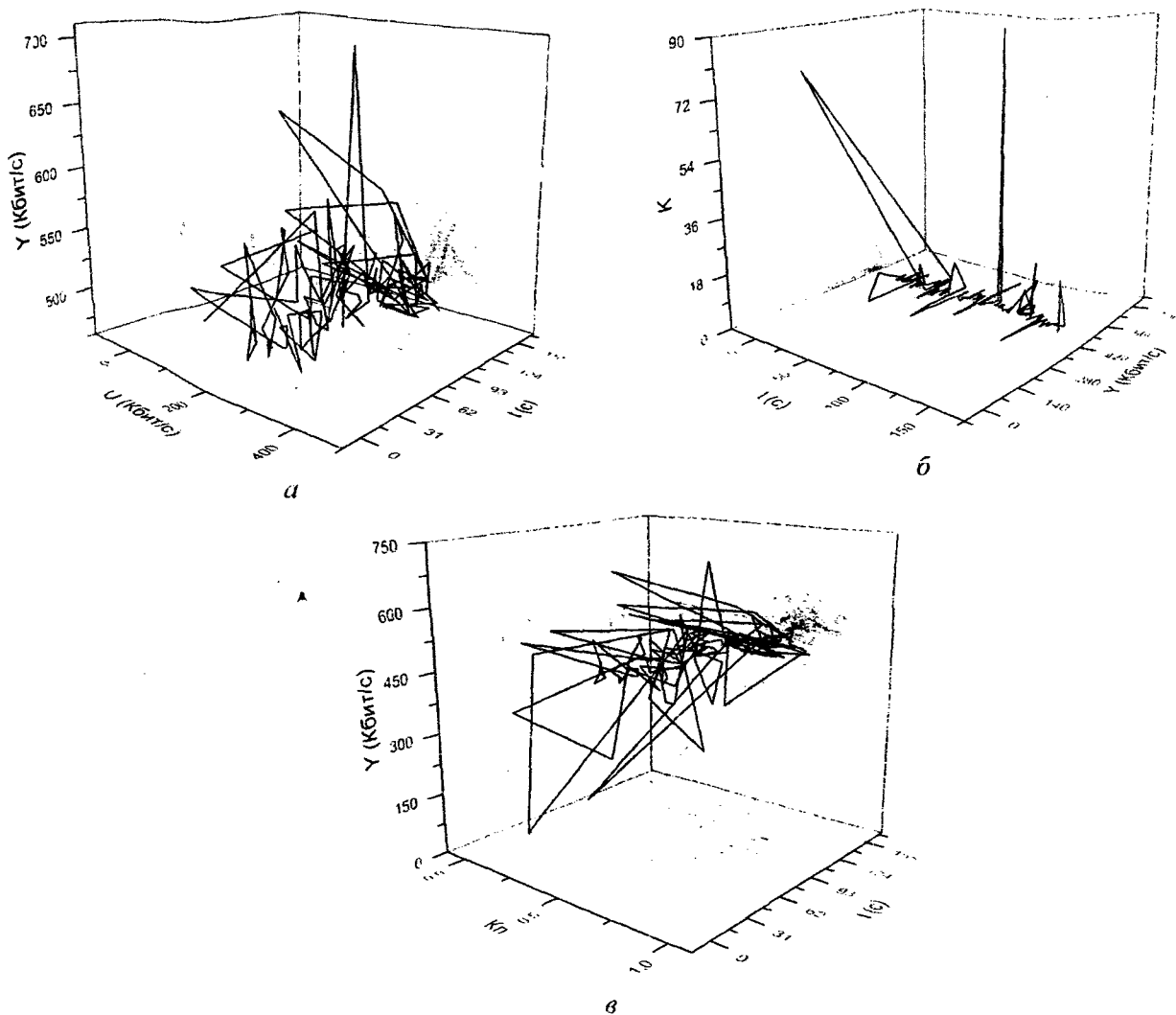


Рис. 2

Рассмотрим зависимости $u_i = u_i(y)$, $k_i = k_i(y)$ и $kn_i = kn_i(y)$, где $u_i(y)$, $k_i(y)$, $kn_i(y)$ – проекция точек u_i , k_i , kn_i на плоскости $\{y, u_i\}$, $\{y, k_i\}$, $\{y, kn_i\}$ соответственно и аппроксимируем их линейными моделями $\overline{\varphi}_{u_i}$, $\overline{\varphi}_{k_i}$, $\overline{\varphi}_{kn_i}$ (на основе полученных данных добавим линии тренда), то есть получим оценку изменений переменных $u_i(y)$, $k_i(y)$, $kn_i(y)$ в среднем:

$$\overline{\varphi}_{u_i} : u_i = u_i(y) = a_{0,i} + a_{1,i}y, \quad (13)$$

$$\overline{\varphi}_{k_i} : k_i = k_i(y) = b_{0,i} + b_{1,i}y, \quad (14)$$

$$\overline{\varphi}_{kn_i} : kn_i = kn_i(y) = c_{0,i} + c_{1,i}y, \quad (15)$$

где $a_{0,i}$, $a_{1,i}$, $b_{0,i}$, $b_{1,i}$, $c_{0,i}$, $c_{1,i}$ – некоторые числа.

Найдем среднеквадратическое отклонение для переменных u_i , k_i , kn_i :

$$\sigma_{u_i, \{ \sigma_{k_i}, \sigma_{kn_i} \}} = \sqrt{\frac{1}{n} \sum_{j=1}^n \left[u_i(t_j) \{ k_i(t_j), kn_i(t_j) \} - M \{ u_i, k_i, kn_i \} \right]^2}. \quad (16)$$

$$\sigma_{u_i(y)} \{ \sigma_{k_i(y)}, \sigma_{kn_i(y)} \} = \sqrt{\frac{1}{n} \sum_{j=1}^n \left[u_i(t_j) \{ k_i(t_j), kn_i(t_j) \} - u_i(y_j) \{ k_i(y_j), kn_i(y_j) \} \right]^2} \quad (17)$$

где $t_j \in J$ – дискретный момент получения данных эксперимента ($j = \overline{1, n}$); $M\{u_i, k_i, kn_i\}$ – математическое ожидание случайных величин u_i, k_i, kn_i ; $u_i(y_j)$ – оценка математического ожидания, полученная с помощью модели (13) – (15).

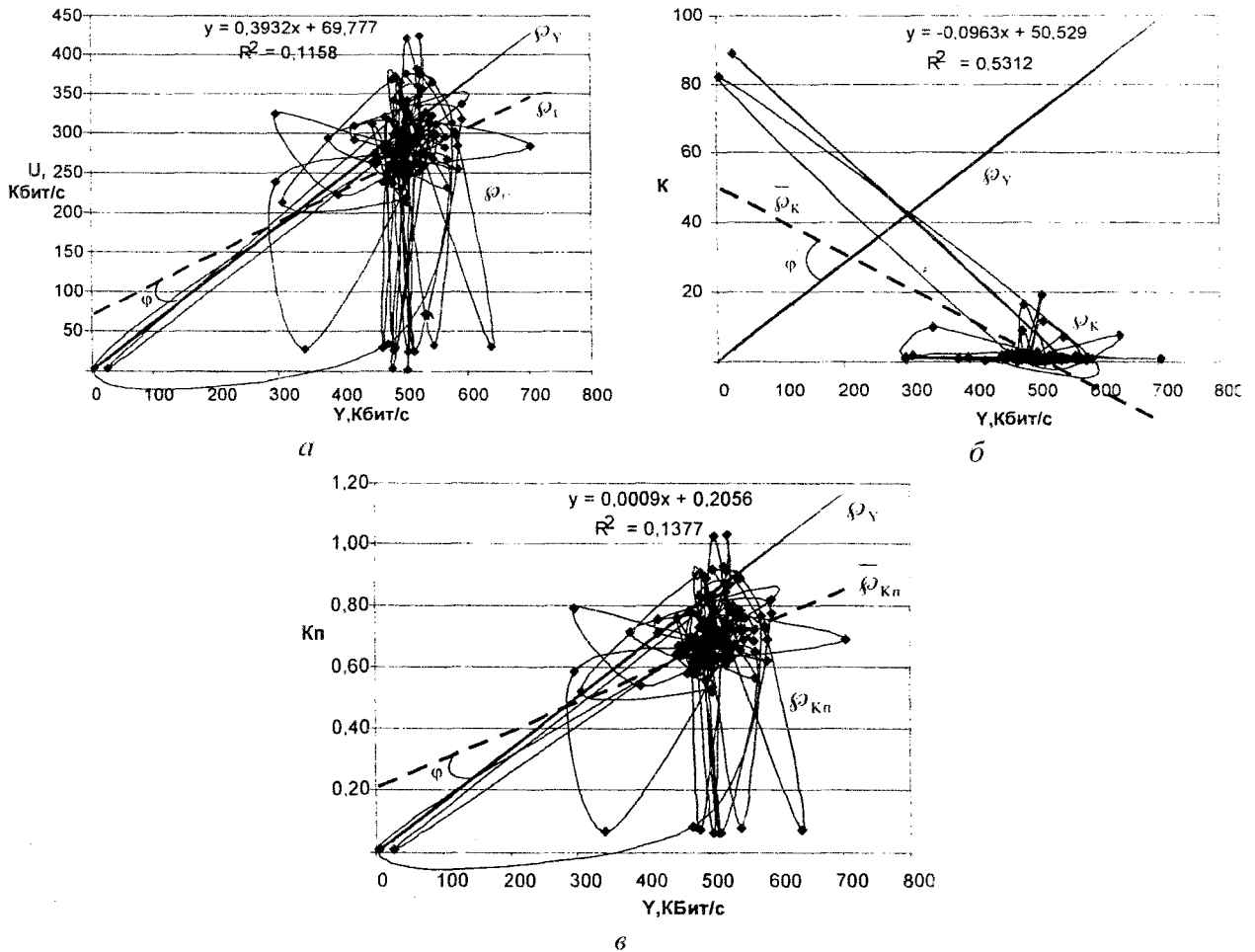


Рис. 3

Для оценки степени связности переменных $u_i \{k_i, kn_i\}$ и y определим характеристики:

$$\varpi_{u_i \{k_i, kn_i\}} = \frac{a_{1,i} \{b_{1,i}, c_{1,i}\} - 1}{1 + a_{1,i} \{b_{1,i}, c_{1,i}\}} \quad (18)$$

$$\kappa_{\gamma_{u_i}} = \frac{\sigma_{u_i} \{ \sigma_{k_i}, \sigma_{kn_i} \}}{\sigma_{u_i(y)} \{ \sigma_{k_i(y)}, \sigma_{kn_i(y)} \}} \quad (19)$$

где $\varpi_{u_i \{k_i, kn_i\}} = \text{tg} \varphi$ – угол между прямыми γ_y и $\gamma_{u_i \{k_i, kn_i\}}$.

Характеристика ϖ отражает влияние переменных u_i, k_i, kn_i на переменную y в (12). Величина $\kappa_{\gamma_{u_i}}$ характеризует степень взаимосвязи переменных u_i, k_i, kn_i и y .

Пусть $\hbar_{y,u_i}$, $\hbar_{y,k_i}$, $\hbar_{y,kn_i}$ – коэффициенты связности переменных y с u_i , k_i , kn_i соответственно:

$$\hbar_{y,u_i\{k_i,kn_i\}} = \text{sgn}(\varpi_{u_i\{k_i,kn_i\}}) \kappa_{y u_i\{k_i,kn_i\}},$$

где $\text{sgn}(\varpi_{u_i\{k_i,kn_i\}})$ – функция направления:

$$\text{sgn}(\varpi_{u_i\{k_i,kn_i\}}) = \begin{cases} 1, \varpi > 0 \\ -1, \varpi < 0 \end{cases}.$$

Проведенные исследования [2, 3, 7] показали, что для любого $\hbar_{y,u_i\{k_i,kn_i\}}$ справедливо

$$\hbar_{y,u_i\{k_i,kn_i\}} = g_{y,u_i\{k_i,kn_i\}}, \quad (20)$$

где $g_{y,u_i\{k_i,kn_i\}}$ – коэффициент взаимной корреляции между y и u_i , k_i , kn_i .

В таблице представлены значения коэффициентов $\hbar_{y,u_i\{k_i,kn_i\}}$, $g_{y,u_i\{k_i,kn_i\}}$ и $\varpi_{u_i\{k_i,kn_i\}}$ для случаев использования наблюдаемых структурно-информационных портретов подсистемы информационного обеспечения в условиях воздействия на нее Dos-атаки (см. рис. 3).

	$\hbar_{y,u_i\{k_i,kn_i\}}$	$g_{y,u_i\{k_i,kn_i\}}$	$\varpi_{u_i\{k_i,kn_i\}}$
u_i	0.319	0.319	0.972
k_i	0.02	0.02	0.961
kn_i	-0.004	-0.004	-0.659

Из результатов эксперимента, приведенных в таблице, видно, что g_{y,u_i} имеет наибольшее значение, и, следовательно, переменную u_i целесообразно использовать в качестве информативной переменной при структурной идентификации и моделировании информационной системы.

Выводы

Таким образом, в результате проведенных исследований предложен подход к моделированию информационной системы в условиях априорной неопределенности. Такой подход позволит повысить точность структурной идентификации системы в условиях воздействия на нее различного рода помех.

Построены и исследованы расширенный фазовый и наблюдаемые структурно-информационные портреты информационной системы в условиях воздействия на нее Dos-атаки. На их примерах показано возникновение структурных изменений (характерных для подсистемы информационного обеспечения в целом).

Проведена оценка характеристик наблюдаемых структурно-информационных портретов информационной системы в условиях воздействия Dos-атаки. Выявлено, что при структурной идентификации и моделировании информационной системы в качестве информативной переменной целесообразно использовать переменную u_i .

Список литературы: 1. Городецкий А.Я. Информационные системы. Вероятностные модели и статистические решения : Учеб. пособие / А.Я.Городецкий. – СПб : Изд-во СПбГПУ, 2003. – 326 с. 2. Карабутов Н.Н. Адаптивная идентификация систем: Информационный синтез / Н.Н.Карабутов. – М. : КомКнига, 2006. – 384 с. 3. Карабутов Н.Н. Структурная идентификация систем: анализ динамических структур / Н.Н.Карабутов. – М. : МГИУ, 2008. – 160 с. 4. Киричков В.Н. Построение адаптивных моделей динамических объектов по данным эксперимента / В.Н. Киричков, А.Н. Сильвестров. – К. : Вища шк., 1985. – 68 с. 5. Кузнецов А.А. Метод структурной идентификации информационных пото-

ков в телекоммуникационных сетях на основе BDS-тестирования / А.А.Кузнецов, С.Г.Семенов, С.Н.Симоненко, Е.В.Мелешко // Наука і техніка Повітряних Сил Збройних Сил України. – 2010. Вип. 2 (4). – Х. : ХУПС. – С. 131 – 137. 6. Кузнецов Д.Ф. Численное моделирование стохастических дифференциальных уравнений и стохастических интегралов / Д.Ф. Кузнецов. – СПб. : Наука, 1999. 463 с. 7. Семенов С.Г. Структурно-функциональный анализ современных информационных систем: разработка комплексного показателя эффективности их функционирования / С.Г. Семенов // Зб. наук. праць. Системи обробки інформації. – Х. : ХУПС, 2011. – Вип. 2(92). – С.145-150. 8. Семенов С. Сравнительные исследования методов идентификации трафика в телекоммуникационной сети для повышения оперативности передачи данных / С.Г.Семенов, Е.В.Мелешко // Прикладная радиоэлектроника. – 2010. – Т. 9, №3. – С.444-448.

*Харьковский национальный
университет радиоэлектроники*

Поступила в редколлегию 05.09.2011

ОЦЕНКА ЭФФЕКТИВНОСТИ ДИНАМИЧЕСКИХ АЛГОРИТМИЧЕСКИХ ПРЕОБРАЗОВАТЕЛЕЙ

Введение

Глобальное проникновение информационных технологий в нашу жизнь, постепенный переход к электронным способам ведения бизнеса ставят перед участниками рынка новые задачи по обеспечению информационной безопасности. Всеобщая информатизация сопровождается ростом числа компьютерных преступлений и, как следствие, материальных потерь. Быстрое развитие Интернет технологий и появление новых видов угроз требует обеспечения адекватных мер информационной безопасности [1].

Защита программных продуктов от несанкционированного использования является первостепенной задачей для их разработчиков в связи с ростом видов атак на современное программное обеспечение (ПО): нелегальное использование; обратное проектирование, когда из ПО извлекаются наиболее ценные модули; и модификация исходного кода, приводящая к существенным потерям разработчиков ПО вплоть до потери ими авторских прав [2]. В последнее время появились новые проблемы обеспечения безопасности, связанные с информационными технологиями, которые, по мнению ряда зарубежных и отечественных экспертов в области их создания и применения, в значительной степени определяют эффективность создаваемых компьютерных систем. На первый план выдвигается безопасность технологий создания программного обеспечения компьютерных систем [3].

Анализ исследований и публикаций

Одним из новых и перспективных методов защиты программного обеспечения является метод обфускации или запутывания программ. Впервые идея обфускации была высказана в работе Диффи и Хеллмана [4] и впоследствии развита группой, возглавляемой Х. Колбергом и К. Томборсоном [5]. Теоретические основы этого метода заложены такими учеными, как Захаров С.С. [6], Гайсарян С.С. [7], Чернов А.В. [8].

В соответствии с принятыми в литературе определениями [5, 6] запутанной (obfuscated) называется программа, которая на всех допустимых для исходной программы входных данных выдаёт тот же самый результат, что и оригинальная программа, но более трудна для анализа, понимания и модификации. Запутанная программа получается в результате применения к исходной незапутанной программе запутывающих преобразований (obfuscating transformations).

Задача обфускации программ заключается в разработке таких преобразований, которые сохраняют функциональные характеристики программ, но при этом делают невозможным или чрезвычайно трудоемким извлечение из открытого текста программы полезной информации об устройстве алгоритмов и структур данных, содержащихся в исходной программе [7, 8]. В работе [9] были исследованы способы обфускации и была доказана невозможность построения универсальных обфускаторов, которые позволяли бы скрыть от противника все сведения о произвольной защищаемой программе.

Теория запутывания программ – молодое направление, и сейчас разрабатываются новые методы запутывания. В работе [10] предложено проводить обфускацию на этапе разработки алгоритмов, а алгоритмы реализовать в виде динамических алгоритмических преобразователей (ДАП). При этом необходимо оценивать эффективность запутанных алгоритмов.

Вопрос оценки эффективности запутывающих преобразований является довольно сложным. Это связано с тем, что в результате преобразований получается запутанная программа «более сложная для понимания и восстановления». Как отмечено в работах [5, 8], качественная оценка этого параметра затруднена, т.к. частично основывается на субъективных

знавательных способностях. Поэтому в большинстве работ по данному вопросу предлагается использовать отдельные характеристики программ (метрики) [7, 8]. К сожалению, известные методы оценки – эвристические и не учитывают специфики ДАП.

В связи с изложенным была поставлена следующая цель работы: разработать способ оценки эффективности динамических алгоритмических преобразователей.

Изложение основного материала исследования

Динамические алгоритмические преобразователи предназначены для реализации заданного алгоритма при различных преобразованиях, что затрудняет динамический анализ алгоритма.

Обобщенная структура динамического алгоритмического преобразователя приведена на рис. 1.

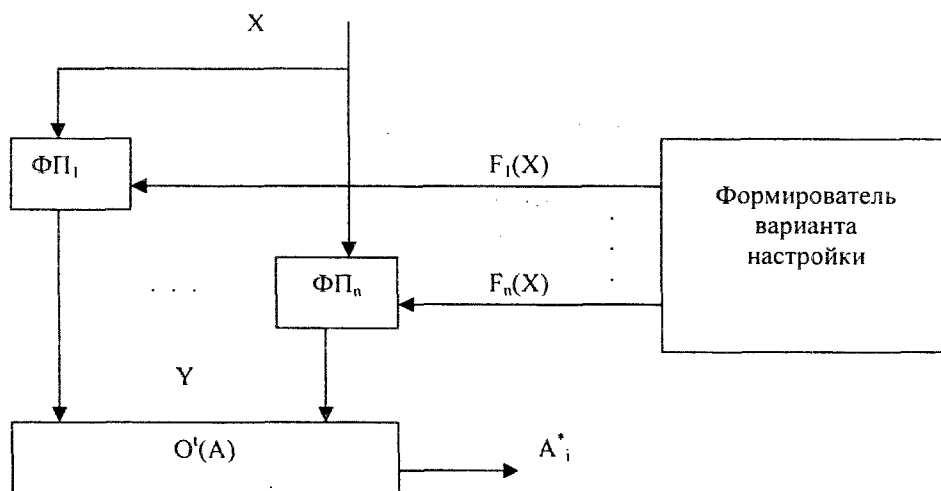


Рис. 1

При описании ДАП использованы следующие обозначения:

A – заданный алгоритм;

k – количество условных переменных алгоритма A ;

A^*_i – i -я модификация алгоритма A ;

t – количество модификаций алгоритма A .

$O^l(A)$ – запутанный алгоритм, реализующий при соответствующих преобразованиях модификаций алгоритма A ;

n – количество условных переменных алгоритма $O^l(A)$;

$H = \{h_1, h_2, \dots, h_q\}$ – множество преобразований (настроек) алгоритма $O^l(A)$;

$O^l(A)/h_i$ – производный алгоритм, реализуемый при настройке h_i .

Функциональные преобразователи (ФП), на основании заданного варианта настройки $h_i \in H$, преобразуют множество входных сигналов X в соответствующие логические функции $F_1(X), F_2(X), \dots, F_n(X)$, значения которых поступают на входы $O^l(A)$. При этом на выходе ДАП реализуется алгоритм $A^*_i = O^l(A)/h_i$, который называется i -й модификацией алгоритма A . Алгоритмы A^*_i и A являются слабоэквивалентными. Они имеют одну и ту же область определения и результаты переработки одинаковых слов из этой области совпадают, но сам процесс их переработки отличается. В результате при каждом обращении к ДАП реализуется новая модификация алгоритма A . При этом активизируются различные ветви алгоритма $O^l(A)$, что затрудняет динамический анализ его работы.

Описание настроек представляется в виде таблицы истинности (табл. 1). Десятичные эквивалент двоичных значений на выходах функциональных преобразователей, соответствующих i -му набору обозначим α_i .

Таблица 1

№	X_1	...	X_i	...	X_k	$F_1(X)$	...	$F_j(X)$	...	$F_n(X)$	α
0	0	0	0	0	0	$f_{1,0}$	...	$f_{j,0}$	...	$f_{n,0}$	α_0
...	...	...	...	...	...						
2^k-1	1	1	1	1	1	$f_{1,2^k-1}$	...	$f_{j,2^k-1}$	...	$f_{n,2^k-1}$	α_{2^k-1}

Множество $\alpha = \{\alpha_0, \dots, \alpha_{2^k-1}\}$ однозначно описывает вид настройки, т.к. i -е значение элемента массива α_i соответствует i -му набору входных переменных, а после преобразования его значения в двоичный код $F_{1,i}, \dots, F_{n,i}$ можно восстановить вид функций, входящих в настройку.

Заданный алгоритм A и запутанный алгоритм $O^t(A)$, реализующие множество операторов $P = \{P_1, \dots, P_d\}$, могут быть представлены в виде совершенной дизъюнктивной нормальной формы:

$$A(X) = P_1^{U_1} \vee \dots \vee P_i^{U_i} \vee \dots \vee P_d^{U_d}, \\ O^t(A) = P_1^{W_1} \vee \dots \vee P_i^{W_i} \vee \dots \vee P_d^{W_d},$$

где U_i – множество наборов значений условий X , при которых алгоритм A выполняет оператор P_i , W_i – множество наборов значений условий Y , при которых алгоритм $O^t(A)$ выполняет оператор P_i .

Количество наборов переменных, при которых реализуются соответствующие операторы, обозначим через $T = \{T_1, \dots, T_d\}$ для алгоритма A и $V = \{V_1, \dots, V_d\}$ для запутанного алгоритма $O^t(A)$.

Поскольку оба алгоритма полностью определены, то имеют место следующие соотношения между элементами множеств T и V :

$$\sum_{i=1}^d T_i = 2^k, \quad \sum_{i=1}^d V_i = 2^n.$$

Для того чтобы можно было по-разному реализовать операторы при разных настройках, необходимо, чтобы была возможность выбора, т.е. необходимо, чтобы $V_i > T_i, i = 1, \dots, d$. При этом для i -го оператора количество вариантов его реализации определяется количеством размещений T_i элементов среди V_i объектов. Следовательно, количество модификаций t алгоритма A , реализуемых алгоритмом $O^t(A)$, определяется следующим образом:

$$t = \prod_{i=1}^d \left(C_{V_i}^{T_i} \times T_i! \right).$$

В качестве примера рассмотрим алгоритмы A и $O^t(A)$, характеристики которых приведены в табл. 2.

Поскольку количество вхождений каждого оператора в алгоритм $O^t(A)$ больше, чем в алгоритм A , то существуют различные варианты выбора операторов при настройках. В табл. 3 приведены примеры значений множества α для некоторых настроек, реализующих различные модификации алгоритма.

Таблица 2

i	Оператор	Алгоритм A		Алгоритм $O^t(A)$	
		T_i	U_i	V_i	W_i
1	P_1	4	3, 7, 8, 12	6	0, 2, 9, 15, 21, 25
2	P_2	3	5, 6, 13	6	1, 12, 13, 14, 16, 28
3	P_3	3	1, 4, 11	7	3, 4, 5, 17, 22, 29, 30
4	P_4	4	0, 2, 10, 15	7	6, 7, 19, 20, 23, 24, 27
5	P_5	2	9, 14	6	8, 10, 11, 18, 26, 31

Вопрос выбора количества операторов каждого вида в алгоритме $O^t(A)$ связан с оценкой количества модификаций алгоритма. Если распределение операторов по численности определено, то для определения множеств наборов, при которых они реализуются, можно использовать метод структурно-функциональных преобразований, описанный в работе [11].

Таблица 3

№	α_0	α_1	α_2	α_3	α_4	α_5	α_6	α_7	α_8	α_9	α_{10}	α_{11}	α_{12}	α_{13}	α_{14}	α_{15}
1	7	3	19	0	4	1	12	2	9	8	20	5	15	13	10	23
2	19	17	20	9	22	14	16	15	21	11	7	30	25	28	18	6
3	20	29	7	15	4	13	1	0	25	26	23	3	9	16	31	24
4	6	5	27	2	22	12	14	9	21	10	19	17	25	28	18	7
5	27	4	23	21	29	28	16	25	0	31	24	3	9	1	10	20

Алгоритм $O^l(A)$, характеристики которого приведены в табл. 2, реализует 3×10^{11} модификаций алгоритма А, в то время как при изменении состава множества V возможны и более эффективные варианты построения запутанного алгоритма. В табл. 4 приведены некоторые возможные варианты множеств V для данного алгоритма А.

Таблица 4

№	V_1	V_2	V_3	V_4	V_5	t	№	V_1	V_2	V_3	V_4	V_5	t
1	16	4	4	5	3	1.8×10^{10}	6	10	6	5	8	3	3.7×10^{11}
2	15	4	4	6	3	4.1×10^{10}	7	9	6	5	7	5	3.7×10^{11}
3	14	5	5	5	3	6.2×10^{10}	8	8	8	5	8	3	3.4×10^{11}
4	13	5	5	6	3	1.3×10^{11}	9	8	8	8	6	4	4.9×10^{11}
5	11	4	4	9	4	1.7×10^{11}	10	7	7	6	7	5	3.6×10^{11}

Анализ приведенных результатов показывает, что при виде множества $V = \{8, 8, 6, 6, 4\}$ реализуется 4.9×10^{11} , т.е. в 1,6 раза больше.

Максимальное количество реализуемых модификаций существенно зависит от значений n, k, и вида множества T. Были исследованы все варианты построения множества T для $k=3$ и для каждого из них определены значения максимального и минимального количества реализуемых модификаций заданного алгоритма (табл. 5). Приведенные результаты показывают, что выбор состава операторов алгоритма $O^l(A)$ и вид исходного алгоритма А существенно влияет на количество реализуемых модификаций алгоритма А.

Таблица 5

№	T	$t_{\max}$	$t_{\min}$	$t_{\max}/t_{\min}$
1	7, 1	3.5×10^7	3.2×10^5	110
2	6, 2	8.0×10^6	1.1×10^6	7.1
3	6, 1, 1	2.7×10^6	7.1×10^4	38
4	5, 3	3.6×10^6	2.3×10^6	1.6
5	5, 2, 1	7.3×10^5	7.2×10^4	10
6	5, 1, 1, 1	2.4×10^5	1.7×10^4	14
7	4, 4	2.8×10^6	9.5×10^5	3
8	4, 3, 1	4.0×10^5	1.1×10^5	3.7
9	4, 2, 2	2.4×10^5	1.3×10^5	1.9
10	4, 2, 1, 1	8.1×10^4	1.7×10^4	4.7
11	4, 1, 1, 1, 1	2.7×10^4	4.8×10^3	5.6
12	3, 3, 2	1.7×10^5	7.3×10^4	2.4
13	3, 3, 1, 1	5.8×10^4	9.2×10^3	6.3
14	3, 2, 2, 1	3.5×10^4	1.4×10^4	2.5
15	3, 2, 1, 1, 1	1.2×10^4	3.9×10^3	3
16	3, 1, 1, 1, 1, 1	3.8×10^3	1.5×10^3	2.5
17	2, 2, 2, 2	2.1×10^4	9.1×10^3	2.4
18	2, 2, 2, 1, 1	6.9×10^3	3.9×10^3	1.8
19	2, 2, 1, 1, 1, 1	2.3×10^3	1.3×10^3	1.8
20	2, 1, 1, 1, 1, 1, 1	7.7×10^2	5.8×10^2	1.3
21	1, 1, 1, 1, 1, 1, 1, 1	2.6×10^2	2.6×10^2	1

Процедура поиска операторного состава алгоритма $O^i(A)$, реализующего максимальное количество модификаций, состоит из следующих этапов:

1. Для заданного операторного состава $T = \{T_1, \dots, T_d\}$ исходного алгоритма A формируются варианты построения операторного состава $V = \{V_1, \dots, V_d\}$ запутанного алгоритма $O^i(A)$, удовлетворяющие условию $V_i > T_i, i = 1, \dots, d$.

2. Оценивается количество модификаций для каждого варианта и выбирается вариант операторного состава $V = \{V_1, \dots, V_d\}$, реализующий наибольшее количество модификаций.

Пример выбора наилучшего варианта для $n = 4, k = 3, d = 5$ и $T = \{3, 2, 1, 1, 1\}$ приведен в табл. 6.

Таблица 6

№	V_1	V_2	V_3	V_4	V_5	t	№	V_1	V_2	V_3	V_4	V_5	t
1	7	3	2	2	2	1.0×10^4	6	5	3	3	3	2	6.5×10^3
2	6	4	2	2	2	1.2×10^4	7	4	4	4	2	2	4.6×10^3
3	6	3	3	2	2	8.6×10^3	8	4	4	3	3	2	5.2×10^3
4	5	5	2	2	2	9.6×10^3	9	4	3	3	3	3	3.9×10^3
5	5	4	3	2	2	8.6×10^3							

Наибольшее количество модификаций ($t = 1.2 \times 10^4$) алгоритма A реализует алгоритм $O^i(A)$, имеющий операторный состав $V = \{6, 4, 2, 2, 2\}$.

С ростом количества модификаций заданного алгоритма, реализуемых запутанным алгоритмом, усложняется сложность динамического анализа запутанного алгоритма, поэтому целесообразно использовать этот показатель при оценке эффективности ДАП.

Выводы

Предложенный подход к оценке эффективности ДАП и выбору его операторного состава позволяет создавать ДАП с наибольшим количеством реализуемых модификаций исходного алгоритма.

Следующий этап при исследовании ДАП – выбор способа формирования функциональных преобразователей.

Список литературы: 1. Горбенко И.Д., Гриненко Т.О. Захист інформації в інформаційно-телекомунікаційних системах. Ч. 1: Криптографічний захист інформації. – Х. : ХНУРЕ, 2004. – 368 с. 2. Казарин О.В. Безопасность программного обеспечения компьютерных систем. – М. : МГУЛ, 2003. – 212 с. 3. Ефимов А.И., Пальчун Б.П. О технологической безопасности компьютерной инфосферы // Вопросы защиты информации. – 1995. – №3(30). – С. 86–88. 4. Diffie W., Hellman M. New direction in cryptography // IEEE Transaction in Information Theory. – 1976. – V. 22. – P. 644–654. 5. Collberg, Thomborson C., Low D. A Taxonomy of Obfuscating Transformations // Technical Report #148. Department of Computer Science. – The University of Auckland, New Zealand. 1997. 36 p. 6. Варновский Н.П., Захаров В.А., Кузюрин Н.Н., Шокуров А.В. Современные методы обфускации программ: классификация и сравнительный анализ // Известия ЮФУ. – 2007. – N 1. – С. 93–98. 7. Аветисян А.И., Иванников В.П., Гайсарян С.С. Анализ и трансформация программ // Всерос. конкурсный отбор обзорно-аналитических статей по приоритетному направлению “Информационно-телекоммуникационные системы”. – 2008. – 78 с. 8. Чернов А. В. Анализ запутывающих преобразований программ // Труды Ин-та Системного программирования РАН. – 2002. – № 2. – С. 7–38. 9. Varnovsky N.P., Zakharov V.A. On the possibility of provably secure obfuscating programs // Lecture Notes in Computer Science. – 2003. – V. 2890. – P. 91–102. 10. Малафеев Е.Е., Малафеев Е.Е. Динамические алгоритмические преобразователи // Системы обработки информации : 36. наук. праць. – 2010. – Вып. 6(87). – С. 133–135. 11. Малафеев Е.Е., Малафеев Е.Е., Павлик А.В. Структурно-функциональный метод преобразования алгоритмических структур // 36. наук. праць Харк. ун-ту повітряних сил. – 2010. – Вып. 2 (24). – С. 76–78.

Публичное акционерное общество
“АО Научно-исследовательский
институт радиотехнических измерений”

Поступила в редколлегию 03.08.2011

**ОБҐРУНТУВАННЯ ПЛАНУ ЗАХИСТУ ОБ'ЄКТІВ ІНФОРМАЦІЇ
ПРО ОБ'ЄКТИ, ПРОЦЕСИ ТА ЯВИЩА****Вступ**

Розвиток України в економічному плані інтенсифікує процес збільшення матеріального виробництва конкурентоздатної наукоємної продукції. Отримати суттєвий прибуток від своєї продукції власник може тільки у тому випадку, коли забезпечить раптовість її появи на відповідному ринку [1]. У сфері матеріального виробництва раптовість стосується: параметрів, споживчих характеристик виробів, терміну початку, обсягів, місця виробництва, застосованих новітніх технологій. Вказані дані конкуренти спроможні одержати за допомогою методів та засобів, у тому числі і за рахунок використання відповідних технічних засобів.

Відомі два шляхи добування даних за допомогою засобів технічних розвідок [1].

По-перше, є шлях добування інформації, яка існує у знаковій формі. Знакова форма представляє сукупність символів, літер, цифр, звуків, які відображають предмети та явища реального світу у віртуальному світі. Носіями інформації з обмеженим доступом (ІзОД) є інформаційні сигнали [3] у формі фізичних полів (електромагнітних, оптичних, акустичних, електричних сигналів, вібраційних коливань у твердих предметах). Шлях захисту від таких розвідок – технічний захист інформації (ТЗІ). Національні стандарти та інші документи щодо його реалізації широко відомі [3 – 5].

По-друге, конкуренти можуть спостерігати власне за самими матеріальними об'єктами у тому числі за допомогою засобів технічних розвідок. Форма проявлення матеріальних об'єктів реального світу у процесі виробництва й застосування продукції різного призначення – електромагнітні, оптичні, гравітаційні, акустичні та інші поля й випромінювання, хімічні речовини [3]. Мова про такий шлях добування даних йдеться у ряді джерел [2, 3, 5]. Тому для забезпечення принципу раптовості з'явлення на ринку продукції необхідне забезпечення прихованості розробки, виготовлення дослідних зразків та їх повномасштабних випробувань [1]. Надалі характеристики реальних об'єктів, що проявляються ними через фізичні поля та хімічні речовини, будуть називатися відомостями з обмеженим доступом (ВзОД) для відрізнєння від інформації з обмеженим доступом (ІзОД) яка підлягає технічному захисту.

На даний час з'являються роботи про заходи захисту ВзОД як захист від конкурентної розвідки у бізнесі [6]. Планування таких заходів потребує певної формалізації процесів розвідки-захисту для прийняття рішень у цій сфері.

Одним із способів формалізації процесів розвідки-захисту є застосування математичного апарату логічних систем розпізнавання об'єктів та явищ [7]. Причому там наведено підходи впливу маскування та протидії розвідці на якість розпізнавання.

Недоліками запропонованих підходів є, по-перше, визначені фіксовані образи об'єктів, що підлягають захисту і об'єкти, під які здійснюється маскування. Цим самим обмежується можливість захисту технічних характеристик нової продукції від конкурентної розвідки, що у ряді випадків є визначальним. По-друге, логічні системи розпізнавання орієнтовані більше на якісний опис образів об'єктів, чим на кількісний, що затрудняє їх використання.

Подоланню цих недоліків і призначена стаття.

Постановка задачі

Нехай підприємство (розробник) підійшло до виготовлення експериментального зразка і випробування нового виробу. Новий виріб відноситься до певного типу групи виробів, де K – кількість типів виробів даної групи. Вироби випускають на різних підприємствах, які можуть знаходитися у конкурентних відносинах.

Перелік типових характеристик виробів групи відомий. Їх кількість M . Окремі або усі характеристики нового виробу представляють собою ВЗОД (табл. 1). Обмеження доступу до ВЗОД – до часу вільного продажу нового виробу.

Таблиця 1

Характеристики виробів	Вироби					
	Існуючі K типів					Новий
	B_1	...	B_K	...	B_K	B_H
P_1	P_{11}	...	P_{1K}	...	P_{1K}	P_{1H}
P_2	P_{21}	...	P_{2K}	...	P_{2K}	P_{2H}
...	...	...	...	...	...	...
P_M	P_{M1}	...	P_{MK}	...	P_{MK}	P_{MH}
...	...	...	...	...	...	...
P_M	P_{M1}	...	P_{MK}	...	P_{MK}	P_{MH}

Задача – спланувати діяльність по захисту ВЗОД від конкурентів щодо основних характеристик виробів до часу зняття обмежень на ВЗОД.

Способи захисту [3 – 8] ВЗОД: дезінформація та (або) приховування.

Дезінформація, виходячи із задуму, може спрямовуватися до нав'язування конкурентам відомостей про споживчі характеристики виробів:

- 1) погіршених;
- 2) завищених.

Приховування спрямоване на забезпечення невизначеності конкретних характеристик конкурентами за результатами ведення розвідки.

За результатами розвідки конкуренти можуть приймати певні рішення (табл. 2).

Таблиця 2

Спосіб захисту ВЗОД	Реакція конкурента на одержані відомості	Дії конкурента на подальшу розвідку
Дезінформація на погіршення характеристик	Довіра	Відмова
	Недовіра	Посилення
Дезінформація на завищення характеристик	Довіра	Відмова
	Недовіра	Посилення
Приховування	Продовжувати розвідку	Посилення

Довіра конкурентів до результатів розвідки може базуватися на невеликому відхиленні одержаних ВЗОД від очікуваних, типових для даної групи виробів. Відсутність даних про споживчі характеристики виробу буде вести до посилення розвідки.

Посилення розвідки є негативним результатом заходів захисту. Це може привести до додаткових витрат на заходи захисту і обмежень у ході виготовлення та випробувань виробу.

З викладеного витікає необхідність зваженості обґрунтування та проведення заходів дезінформації при припустимих заходах приховування.

Зваженість обґрунтування повинна витікати з кількісних показників, які будуть наведені далі.

Пропозиція щодо рішення задачі

Суть пропозиції заключається у оцінці припустимого значення кожної характеристики нового виробу, що підлягає захисту способом дезінформації, як випадкової величини на тлі відомих подібних характеристик даної групи виробів. Випадковість характеристики для розвідки ґрунтується на її апріорній невідомості для конкурента. У ході розвідки набираються розвіддані і по них поступово можуть уточнюватися конкретні значення характеристик.

Хибні розвіддані або їх недостатність, створені заходами дезінформації і приховування, приведуть до хибних оцінок.

Таким чином, апіорний розподіл кожної із характеристик може бути визначений типовими, відомими значеннями $P_m \{P_{m1}, \dots, P_{mk}, \dots, P_{mK}\}$. Відомі величини P_{mk} можна представити як багатокутник частот з нерівномірним поділом по вісі абсцис. Значення окремих характеристик P_{mk} можуть бути як дискретними, так і безперервними у певному діапазоні.

Апіорні ймовірності схожості характеристик нового виробу під старі $p(B_k)$ можна узяти рівними, якщо інших даних про це немає. У такому випадку, з точки зору теорії інформації, невизначеність розподілу характеристик в інтервалі області визначення буде найбільша.

З початку розвідки апостеріорні характеристики розвідуваного параметру будуть стягуватися до такого значення, до якого будуть приводити розвіддані.

Ще раз слід зазначити, що науково-технічний прогрес, за своїм змістом, спрямований на поліпшення споживчих характеристик виробів. Поліпшення не обов'язкове для усіх характеристик, деякі другорядні характеристики можуть і погіршуватися. Тому при розробці заходів захисту можна використовувати дане положення і дезінформувати відносно визначеного набору характеристик як у погіршення, так і поліпшення характеристик. Процес обрання згаданих характеристик у роботі не розглядається. Він може бути встановлений експертною групою розробника, виходячи із конкретної природи характеристики виробу.

Для кожної характеристики слід встановити ранг, за яким визначається пріоритет важливості захисту.

Деякі характеристики функціонально пов'язані між собою і між ними існує зв'язок. Такий зв'язок може встановлюватися методами регресійного аналізу. Окремими випадками регресійного аналізу може бути кореляційний аналіз. Кількість парних регресій, що потрібні визначити, буде $M!/(2 \times (M - 2)!)^2$ співвідношень, що при застосуванні комп'ютерної техніки нескладно виконати.

Для залежних пар характеристик ранг може складатися як сума рангів відповідних вихідних рангів характеристик.

Експертна група, також повинна встановити напрям зміни величини характеристики по вісі шкали у сторону їх погіршення та завищення.

Оцінку якості заходів захисту по кожній характеристиці для нового виробу можна проводити шляхом співставлення очікуваного результату захисту із густиною розподілу значення відповідної характеристики для множини типів виробів. Недоліком використання співставлення розподілів випадкових величин є складність визначення законів їх розподілу із-за невеликої вибірки типів виробів – K . Зазначений недолік можна подолати за рахунок використання моментів випадкових величин: 1) математичного очікування, 2) середньоквадратичного відхилення; нормованих центральних моментів 3) третього порядку (асиметрія) та 4) четвертого порядку (експес).

Співставлення значення характеристики нового виробу з 1) та 2) параметрами дає уяву про величину її споживчої якості на відповідній шкалі.

Асиметрія та експес свідчать про тенденції групування значень характеристик виробів. Для від'ємної асиметрії – переважає велика густина характеристик із великим значеннями, над малою густиною менших величин і навпаки. Позитивний експес свідчить про гостровершинну скупченість значень характеристик, а від'ємний – про плоску вершинну. Означені моменти 3) та 4) можуть обґрунтовувати доцільність вибору для дезінформації конкретних значень характеристик на тлі відомих.

Розробка плану захисту – вибору значень характеристик для дезінформації конкурента повинна відповідати певним принципам [5].

Комплексності захисту – у перекритті усіх нетехнічних і технічних каналів витоку інформації по фізичним полям. Всі заходи щодо захисту повинні бути узгоджені за місцем, метою і часом.

Активності захисту – у наполегливому нав'язуванні конкуренту невірної інформації про приховуваний виріб.

Переконливості захисту – у правдоподібності, відповідати обстановці в цілому.

Безперервності захисту – у постійному проведенню, у будь-яких умовах, за будь-яких обставин у процесі заданого терміну часу (до рекламної кампанії, продажу).

Різноманітності прийомів захисту – виключення будь-якого шаблону і формальності при проведенні захисту.

Заходи захисту також повинні бути економічно обгрунтованими.

Алгоритм рішення задачі

1. Складається опис відомих виробів у формі табл. 1. Додається стовпчик із конкретними характеристиками для нового виробу, які можуть складати як ВЗОД, так і відкриті дані.

2. Експертна група проводить ранжування конкретних характеристик нового виробу по ступеню важливості по їх захисту від конкурентів.

3. Обчислюють математичне очікування, середньоквадратичне відхилення, асиметрію та ексцес усіх технічних характеристик виробів.

4. Методом найменших квадратів оцінюються коефіцієнти парної регресії для усіх можливих пар характеристик Π_i, Π_m . Встановлюються ранги для пар характеристик.

5. Згідно одержаного рангу для одиночних характеристик, починаючи з найвищого, експертами пропонуються заходи захисту щодо споживчих характеристик виробів:

- із погіршенням характеристик високих рангів (дезінформація);
- приховуванням та погіршенням характеристик середніх рангів;
- покращенням характеристик низьких рангів (дезінформація).

6. Провести перевірку на узгодженість заходів захисту характеристик низьких рангів заходам захисту характеристик високих рангів по коефіцієнтам парної регресії (п.4) і відповідним чином їх відкоригувати (п.5).

7. Скласти сукупний опис відомих виробів і нового виробу з характеристиками, що пропонується показувати конкурентам, у формі табл. 1 (змінений останній стовпчик ВЗОД на характеристики які потрібно пред'являти конкурентам).

8. Визначити ознаки ВЗОД, які треба захищати способами дезінформації і приховування. Перевірити можливість реалізації запропонованих заходів при виготовленні та випробуваннях нових виробів. При неможливості – повторити дослідження, починаючи з п. 5. І так до досягнення бажаного результату.

9. Скласти план заходів дезінформації і приховування від конкурентної розвідки за розділами:

- заходи дезінформації у відкритих джерелах інформації, Інтернеті тощо;
- заходи забезпечення контрольованої зони навколо об'єктів з виготовлення та випробування нових виробів;
- заходи захисту від безпосереднього спостереження та технічної розвідки за виготовленням і випробуванням виробів із-за меж контрольованої зони способами технічної дезінформації та приховування.

Даний алгоритм дає основу для обгрунтованої розробки комплексу захисту нових виробів від конкурентної розвідки.

Рішення даної задачі доцільно проводити на ПОЕМ із використанням програмного забезпечення обробки статистичних даних.

Висновки

Формалізація задач захисту дозволяє розробляти їх варіанти, порівнювати між собою та обирати кращі з них по визначеним критеріям.

Застосування обчислювальної техніки з програмним забезпеченням із статистичних розрахунків полегшує та прискорює дослідження варіантів захисту.

Список літератури: 1. *Заболотний В.І.* Класифікація технічних каналів витоку інформації // Радіотехніка. – 2003. – Вип. 134. 2. *Юцук Е.А.* Конкурентная разведка: маркетинг рисков и возможностей. – Казань : Экспресс-формат, 2010. – 241 с. 3. *ДСТУ3396.2-97* Захист інформації. Технічний захист інформації. Терміни та визначення. 4. *ДСТУ3396.0-96* Захист інформації. Технічний захист інформації. Основні положення. 5. *Положення про технічний захист інформації в Україні.* Затверджено постановою КМУ 9 вересня 1994 р. №632 // Збірка нормативних документів системи технічного захисту інформації, 1997. 6. *Кузин А.А., Нежданов И.В., Юцук Е.А.* Дезинформация и активные средства в бизнесе. – Казань : Яналиф, 2009. – 134с. 7. *Горелик А.Л., Скрипкин В.А.* Методы распознавания. – М. : Высш. шк., 1984. – 208 с. 8. *Брусницын Н.А.* Информационная война и безопасность. – М. : Вита-Пресс, 2001. – 280 с.

*Харківський національний
університет радіоелектроніки*

Надійшла до редколегії 17.07.2011

МЕТОДЫ КОНТРОЛЯ И ДИАГНОСТИКИ ДАННЫХ В КЛАССЕ ВЫЧЕТОВ

Введение

Основу современных телекоммуникационных систем составляют встроенные компьютерные средства передачи и обработки цифровой информации (данных) (КСПОЦИ). В этом случае одним из основных путей достижения высокой эффективности функционирования телекоммуникационных систем является повышение, в первую очередь, таких характеристик КСПОЦИ, как производительность обработки информации, отказоустойчивость функционирования и достоверность вычислений при обработке данных в реальном времени.

Известно, что непозиционная система счисления в классе вычетов (КВ) обеспечивает высокую пользовательскую производительность обработки данных, представленных в целочисленном виде. Однако обеспечение высокой достоверности результата вычислений КСПОЦИ, функционирующих в КВ, требует разработки и методов и средств контроля, диагностики и коррекции данных, участвующих в процессе передачи и обработки информации.

Таким образом, важны и актуальны исследования методов контроля и диагностики ошибок данных, представленных в КВ.

Анализ результатов исследований

Рассмотрим ряд научных утверждений, результаты доказательств которых можно положить в основу методов контроля и диагностики ошибок данных, представленных в непозиционной системе счисления класса вычетов [1, 2]. Отметим, что в дальнейшем предполагается только однократная (в одном остатке a_i , ($i = \overline{1, n+1}$), числа $A = (a_1, a_2, \dots, a_n, a_{n+1})$, представленного в КВ) ошибка.

Утверждение 1. Пусть задана упорядоченная ($m_i < m_{i-1}$, $i = \overline{1, n}$) система оснований (модулей) КВ с n информационными и одним $m_k = m_{n+1}$ контрольным основаниями, и пусть число $A = (a_1, a_2, \dots, a_{i-1}, a_i, a_{i+1}, \dots, a_n, a_{n+1})$ неискаженное (правильное), т.е. $A < M_0 / m_{n+1}$, где $M_0 = M \cdot m_{n+1}$ и $M = \prod_{i=1}^n m_i$. Тогда величина A не изменится, если это число будем представлять в КВ, из которого изъято основание m_i , т.е. если в представлении числа A убрать остаток a_i .

Полученное таким образом число будем называть проекцией $A_i = (a_1, a_2, \dots, a_{i-1}, a_{i+1}, \dots, a_n, a_{n+1})$ числа A по модулю m_i .

Утверждение 2. Если в упорядоченной системе оснований КВ задано правильное число A , то проекции A_i ($i = \overline{1, 1+n}$) этого числа равны между собой, т.е. $A = A_1 = A_2 = \dots = A_i = \dots = A_n = A_{n+1} < M_0 / m_{n+1}$. Действительно, для правильного числа A имеет место соотношение $A < M_0 / m_{n+1} < M_0 / m_k < \dots < M_0 / m_i < \dots < M_0 / m_1$. В соответствии с результатами утверждения 1 имеем $A = A_i$.

Утверждение 3. Пусть для упорядоченной системы оснований КВ все возможные проекции A_i ($i = \overline{1, n+1}$) числа A совпадают. В этом случае число $A = (a_1, a_2, \dots, a_n, a_{n+1})$ является правильным.

Покажем это. Предположим, что число A будет неправильным за счет искажения остатка a_i по модулю m_i . Заменим в числе A искаженный остаток a_i на правильный $\tilde{a}_i$. В этом случае получили правильное число $\tilde{A} = (a_1, a_2, \dots, \tilde{a}_i, \dots, a_n, a_{n+1})$. Тогда в соответствии с результатом утверждения 2 имеем $\tilde{A}_1 = \tilde{A}_2 = \dots = \tilde{A}_i = \dots = \tilde{A}_n = \tilde{A}_{n+1}$. С другой стороны, $A_i = (a_1, a_2, \dots, a_{i-1}, a_{i+1}, \dots, a_n, a_{n+1})$ и одновременно $\tilde{A}_i = (a_1, a_2, \dots, a_{i-1}, a_{i-1}, \dots, a_n, a_{n+1})$, т.е. $A_i = \tilde{A}_i$. В этом случае должно выполняться следующее соотношение $A = A_1 = \tilde{A}_1 = A_2 = \tilde{A}_2 = \dots = A_n = \tilde{A}_n = A_{n+1} = \tilde{A}_{n+1}$. Однако по условию утвер-

ждения 3 проекции $A_j (j \neq i)$ числа A отличается от проекции A_i остатком a_i по основанию m_i . Вследствие этого $A_i \neq A_j$, что противоречит условию неправильности числа A .

Утверждение 4. Если в упорядоченной системе оснований КВ проекция $A_i = (a_1, a_2, \dots, a_{i-1}, a_{i+1}, \dots, a_n, a_{n+1})$ числа $A = (a_1, a_2, \dots, a_{i-1}, a_i, a_{i+1}, \dots, a_n, a_{n+1})$ удовлетворяет условию $A \geq M_0 / m_{n+1}$, то этом случае считается, что остаток a_i числа A по модулю m_i не искажен. Отметим еще раз, что предполагается только однократная ошибка.

Действительно, если остаток a_i числа A по модулю m_i искажен, то проекция A_i , составленная из неискаженных $a_j (j = \overline{1, n+1} \text{ и } i \neq j)$ остатков, должна быть правильным числом. Однако по условию $A_i \geq M_0 / m_{n+1}$ - неправильное число, что противоречит условию утверждения 4. Кроме этого, отметим, что если $A_i \geq M_0 / m_{n+1} (i = \overline{1, n})$, то искажен остаток a_{n+1} .

Основная часть

На основании результатов изложенных выше научных утверждений рассмотрим метод контроля и метод диагностики данных, представленных в КВ.

Пусть задано проверяемое число $A = (a_1, a_2, \dots, a_i, \dots, a_n, a_{n+1})$ в КВ с информационными $m_i (i = \overline{1, n})$ и одним контрольным $m_k = m_{n+1}$ основаниями. Необходимо, во-первых, провести контроль (определить правильность) числа A , и, во-вторых, провести диагностику остатков $a_i (i = \overline{1, n+1})$ числа A , т.е. этого числа, и определить искаженные (или неискаженные) остатки.

Контроль и диагностика данных проводятся последовательно в два этапа.

1. *Первый этап.* Метод контроля данных A .

1.1. Определить значения $B_i (i = \overline{1, n+1})$ ортогональных базисов для полной системы оснований $\{m_i\}$ КВ.

1.2. Используя систему ортогональных базисов B_i , исходное A число в КВ перевести в позиционную систему счисления (ПСС) по формуле $A_{ПСС} = (\sum_{i=1}^{n+1} a_i \cdot B_i) \bmod M_0 \quad (1)$.

1.3. Провести операции позиционного сравнения значений $A_{ПСС}$ и M . Если результат сравнения показал, что $A_{ПСС} < M$, то число A правильное. Если $A_{ПСС} \geq M$, то считается, что число A неправильное, в случае если искажен только один из остатков a_i числа A .

2. *Второй этап.* Метод диагностики остатков $a_i (i = \overline{1, n+1})$ кодовой структуры $\tilde{A}$ данных.

2.1. Определить значения ортогональных базисов B_j для каждого частного набора из оснований полного КВ. Частные наборы оснований образуются путем последовательного удаления из полного $m_1 \div m_{n+1}$ КВ одного из модулей $m_j (j = \overline{1, n+1})$. В этом случае значение ортогонального базиса для j -го частного набора $\{m_i\} (i = \overline{1, n+1} \text{ и } i \neq j)$ модулей КВ обозначается как B_j . Кодовые числа в j -м частном наборе оснований КВ принадлежат множеству $\{A_j\}$ возможных проекций числа A . Мощность такого множества равна значению M_0 / m_j .

2.2. Последовательно определяется правильность каждого остатка $a_i (i = \overline{1, n+1})$ числа A . Для этого вычислим все проекции $\tilde{A}_j$ числа $\tilde{A}$. После этого по формуле (1) определяются значения $\tilde{A}_{jПСС}$ в ПСС, где $M_j = M_0 / m_j = \prod_{\substack{K=1 \\ K \neq j}}^{n+1} m_K (M_{n+1} = M)$.

Далее проводим $(n+1)$ -о сравнение чисел $\tilde{A}_{jПСС}$ и числа $M = M_0 / m_{n+1}$. Если среди проекций $\tilde{A}_j$ есть числа, не находящиеся внутри информационного $[0, M)$ числового интервала (т.е. $\tilde{A}_K \geq M$), содержащего k правильных чисел, то делается вывод о том, что эти k остатков числа A не искажены. Ошибочными могут быть только остатки, находящиеся среди остальных $[(n+1) - k]$ остатков числа $\tilde{A}$. Определение истинно искаженных остатков требует отдельных дополнительных исследований.

Рассмотрим пример применения метода контроля и диагностики в КВ для однобайтового ($l = 1$) машинного слова (8 двоичных разрядов) КСПОЦИ. При этом полный КВ (для упорядоченной системы оснований) с одним контрольным основанием может быть задан следующими информационными $m_1 = 3, m_2 = 4, m_3 = 5, m_4 = 7$ и контрольным $m_K = m_{n+1} = 11$ основаниями.

При этом обеспечиваются все требования к основаниям КВ ($\text{НОД}(m_i, m_j) = 1, i, j = \overline{1, n+1}, i \neq j$), а также требования однозначности представления кодовых слов в данном информационном числовом $[0, M)$ диапазоне. Для данного КВ имеем: $M_0 = \prod_{i=1}^{n+1} m_i = 4620$ – общее количество кодовых слов в данном КВ; $M = \prod_{i=1}^n m_i = 420$ – количество информационных кодовых слов.

В этом случае полный $[0, M_0)$ и информационный $[0, M)$ числовые диапазоны чисел определяются, соответственно, как $[0, 4620)$ и $[0, 420)$. Все возможные частные наборы оснований КВ представлены в табл. 1, где $M_j = M_0 / m_j$. В табл. 2 представлены все возможные числовые диапазоны $[j \cdot M_1, (j + 1) \cdot M)$ попадания неправильного $\tilde{A}$ числа для $l = 1$, а в табл. 3 – значения рангов r M_0 числа A .

Таблица 1. Набор оснований КВ ($l = 1$)

j	m_1	m_2	m_3	m_4	M_j
1	4	5	7	11	1540
2	3	5	7	11	1155
3	3	4	7	11	924
4	3	4	5	11	660
5	3	4	5	7	420

Таблица 3. Значения рангов числа A для диапазона $[0, 4620)$

r	$r \cdot M_0 = r \cdot 4620$
1	4620
2	9240
3	13860
4	18480
5	23100
6	27720
7	32340
8	36960
9	41580
10	46200

Таблица 2. Числовые диапазоны попадания неправильного $\tilde{A}$ числа

j	$[jM, (j+1) \cdot M)$	$\gamma_{\tilde{A}}^{(j)} = \gamma_s^{(j)}$
0	$[0, 420)$	$\gamma_s^{(0)} = 0$
1	$[420, 840)$	$\gamma_s^{(1)} = 2$
2	$[840, 1260)$	$\gamma_s^{(2)} = 4$
3	$[1260, 1680)$	$\gamma_s^{(3)} = 6$
4	$[1680, 2100)$	$\gamma_s^{(4)} = 8$
5	$[2100, 2520)$	$\gamma_s^{(5)} = 10$
6	$[2520, 2940)$	$\gamma_s^{(6)} = 1$
7	$[2940, 3360)$	$\gamma_s^{(7)} = 3$
8	$[3360, 3780)$	$\gamma_s^{(8)} = 5$
9	$[3780, 4200)$	$\gamma_s^{(9)} = 7$
10	$[4200, 4620)$	$\gamma_s^{(10)} = 9$

Пусть в процессе передачи или обработки данных вместо правильного $A_{100} = (1, 0, 0, 2, 1)$ результата операции ($100 < M = 420$) получено число вида $\tilde{A}_{2760} = (0, 0, 0, 2, 1)$. Необходимо провести контроль правильности числа $\tilde{A}$ и диагностику его остатков $a_i (i = \overline{1, 5})$.

В табл. 4 даны значения ортогональных B_i базисов для данного КВ.

Таблица 4. Ортогональные базисы $B_i (i = \overline{1, 5})$

$B_1 = (1, 0, 0, 0, 0) = 1540$	$\bar{m}_1 = 1$
$B_2 = (0, 1, 0, 0, 0) = 3465$	$\bar{m}_2 = 3$
$B_3 = (0, 0, 1, 0, 0) = 3696$	$\bar{m}_3 = 4$
$B_4 = (0, 0, 0, 1, 0) = 2640$	$\bar{m}_4 = 4$
$B_5 = (0, 0, 0, 0, 1) = 2520$	$\bar{m}_5 = 6$

$$\begin{cases} 1 \cdot 140 \equiv 8 \pmod{11}, \\ 2 \cdot 140 \equiv 5 \pmod{11}, \\ 3 \cdot 140 \equiv 2 \pmod{11}, \\ 4 \cdot 140 \equiv 10 \pmod{11}, \\ 5 \cdot 140 \equiv 7 \pmod{11}, \end{cases} \quad \begin{cases} 6 \cdot 140 \equiv 4 \pmod{11}, \\ 7 \cdot 140 \equiv 1 \pmod{11}, \\ 8 \cdot 140 \equiv 9 \pmod{11}, \\ 9 \cdot 140 \equiv 6 \pmod{11}, \\ 10 \cdot 140 \equiv 3 \pmod{11}. \end{cases}$$

В этом случае $B_{41} = 7 \cdot 140 = 980$.

2.1.2. Определяем значения B_{i2} для второго ($j = 2$) набора оснований $m_1 = 3, m_2 = 5, m_3 = 7$ и $m_4 = 11$ КВ (табл. 1). В этом случае $M_2 = \prod_{i=1}^4 m_i = 1155$ ($M = 420$).

Определяем значение B_{12} . В этом случае $m_1 = 3, M_2 / m_1 = 1155 / 3 = 385, \overline{m}_{12} = \overline{1, m_1 - 1} = \overline{1, 2}$.

$$\begin{cases} 1 \cdot 385 \equiv 1 \pmod{3}, \\ 2 \cdot 385 \equiv 2 \pmod{3}. \end{cases}$$

В этом случае $B_{12} = 1 \cdot 385 = 385$.

Определим B_{22} . Имеем $m_2 = 5, M_2 / m_2 = 1155 / 5 = 231, \overline{m}_{22} = \overline{1, m_2 - 1} = \overline{1, 4}$.

$$\begin{cases} 1 \cdot 231 \equiv 1 \pmod{5}, \\ 2 \cdot 231 \equiv 2 \pmod{5}, \end{cases} \quad \begin{cases} 3 \cdot 231 \equiv 3 \pmod{5}, \\ 4 \cdot 231 \equiv 4 \pmod{5}. \end{cases}$$

Тогда $B_{22} = 1 \cdot 231 = 231$.

Определим B_{32} . Имеем $m_3 = 7, M_2 / m_3 = 1155 / 7 = 165, \overline{m}_{32} = \overline{1, m_3 - 1} = \overline{1, 6}$.

$$\begin{cases} 1 \cdot 165 \equiv 4 \pmod{7}, \\ 2 \cdot 165 \equiv 1 \pmod{7}, \\ 3 \cdot 165 \equiv 5 \pmod{7}, \end{cases} \quad \begin{cases} 4 \cdot 165 \equiv 2 \pmod{7}, \\ 5 \cdot 165 \equiv 6 \pmod{7}, \\ 6 \cdot 165 \equiv 3 \pmod{7}. \end{cases}$$

Тогда $B_{32} = 2 \cdot 165 = 330$.

Определим B_{42} . Имеем $m_4 = 11, M_2 / m_4 = 1155 / 11 = 105, \overline{m}_{42} = \overline{1, m_4 - 1} = \overline{1, 10}$.

$$\begin{cases} 1 \cdot 105 \equiv 6 \pmod{11}, \\ 2 \cdot 105 \equiv 1 \pmod{11}, \\ 3 \cdot 105 \equiv 7 \pmod{11}, \\ 4 \cdot 105 \equiv 2 \pmod{11}, \\ 5 \cdot 105 \equiv 8 \pmod{11}, \end{cases} \quad \begin{cases} 6 \cdot 105 \equiv 3 \pmod{11}, \\ 7 \cdot 105 \equiv 9 \pmod{11}, \\ 8 \cdot 105 \equiv 4 \pmod{11}, \\ 9 \cdot 105 \equiv 10 \pmod{11}, \\ 10 \cdot 105 \equiv 5 \pmod{11}. \end{cases}$$

Тогда $B_{42} = 2 \cdot 105 = 210$.

2.1.3. Определим значения B_{i3} для третьего ($j = 3$) набора оснований $m_1 = 3, m_2 = 4, m_3 = 7, m_4 = 11$ КВ (табл. 1). В этом случае $M_3 = \prod_{i=1}^4 m_i = 924$ ($M = 420$).

Определим B_{13} . Имеем $m_1 = 3, M_3 / m_1 = 924 / 3 = 308, \overline{m}_{13} = \overline{1, m_1 - 1} = \overline{1, 2}$.

$$\begin{cases} 1 \cdot 308 \equiv 2 \pmod{3}, \\ 2 \cdot 308 \equiv 1 \pmod{3}. \end{cases}$$

Тогда $B_{13} = 2 \cdot 308 = 616$.

Определим B_{23} . Имеем $m_2 = 4, M_3 / m_2 = 924 / 4 = 231, \overline{m}_{23} = \overline{1, m_2 - 1} = \overline{1, 3}$.

$$\begin{cases} 1 \cdot 231 \equiv 3 \pmod{4}, \\ 2 \cdot 231 \equiv 2 \pmod{4}, \\ 3 \cdot 231 \equiv 1 \pmod{4}. \end{cases}$$

В этом случае $B_{23} = 3 \cdot 231 = 693$.

1. Первый этап.

1.1 Определяем все значения $B_i (i = \overline{1, 5})$ ортогональных базисов для полной системы оснований $m_1 = 3, m_2 = 4, m_3 = 5, m_4 = 7$ и $m_5 = 11$ КВ (см. табл. 4).

1.2. Используя данные табл. 4 по формуле (1), определяем значение $\tilde{A}_{ПСС}$

$$\tilde{A}_{ПСС} = (0 \cdot 1540 + 0 \cdot 3465 + 0 \cdot 3696 + 2 \cdot 2640 + 1 \cdot 2520) \bmod 4620 = 3180 \pmod{4620}.$$

1.3. Проводим сравнение полученного числа $A_{ПСС}$ и значения $M = 420$. Так, как $\tilde{A}_{ПСС} > M = 420$, то делается вывод, что полученный $\tilde{A}$ результат искажен по какому-то одному из остатков a_i числа $A_{100} = (1, 0, 0, 2, 1)$.

2. Второй этап.

2.1. Определим значения B_{ij} ортогональных базисов для каждого из 5 наборов (табл. 1) оснований КВ. Так, для $i = 4$ и $j = 5$ имеем:

$$\begin{cases} B_{1j} = (1, 0, 0, 0), \\ B_{2j} = (0, 1, 0, 0), \\ B_{3j} = (0, 0, 1, 0), \\ B_{4j} = (0, 0, 0, 1). \end{cases}$$

В общем случае значения B_{ij} ортогональных базисов определяется исходя из следующего сравнения $B_{ij} = \frac{M_i \cdot \bar{m}_{ij}}{m_i} \equiv 1 \pmod{m_i}$ (2), где $\bar{m}_{ij} \equiv \overline{1, m_i - 1}$ - вес ортогонального базиса B_{ij} .

2.1.1. Определим значения B_{i1} для первого ($j = 1$) набора оснований $m_1 = 4, m_2 = 5, m_3 = 7$ и $m_4 = 11$ (табл. 1). В этом случае $M_1 = \prod_{i=1}^4 m_i = 1540$ ($M = 420$). Определяем значения базисов B_{i1} исходя из соотношения (2) – $B_{i1} = \frac{M_1 \cdot \bar{m}_{i1}}{m_i} \equiv 1 \pmod{m_i}$.

Определяем значение B_{11} . В данном случае используем $m_1 = 4$. При этом $M_1 / m_1 = 1540 / 4 = 385$; $\bar{m}_{11} \equiv \overline{1, m_1 - 1} = \overline{1, 3}$. Составляем возможные значения вида (2) для $i = 1$, т.е. $\bar{m}_{11} \cdot M / m_1$:

$$\begin{cases} 1 \cdot 385 \equiv 1 \pmod{4}, \\ 2 \cdot 385 \equiv 2 \pmod{4}, \\ 3 \cdot 385 \equiv 3 \pmod{4}. \end{cases}$$

В этом случае $B_{11} = 1 \cdot 385 = 385$.

Определим значение B_{21} . В данном случае $m_2 = 5, M_1 / m_2 = 1540 / 5 = 308$. $\bar{m}_{21} \equiv \overline{1, m_2 - 1} = \overline{1, 4}$.

Составляем совокупность сравнений:

$$\begin{cases} 1 \cdot 308 \equiv 3 \pmod{5}, \\ 2 \cdot 308 \equiv 1 \pmod{5}, \end{cases} \quad \begin{cases} 3 \cdot 308 \equiv 4 \pmod{5}, \\ 4 \cdot 308 \equiv 2 \pmod{5}. \end{cases}$$

Имеем, что $B_{21} = 2 \cdot 308 = 616$.

Определим значение B_{31} . Имеем $m_3 = 7, M_1 / m_3 = 1540 / 7 = 220, \bar{m}_{31} \equiv \overline{1, m_3 - 1} = \overline{1, 6}$. Тогда

$$\begin{cases} 1 \cdot 220 \equiv 3 \pmod{7}, \\ 2 \cdot 220 \equiv 6 \pmod{7}, \\ 3 \cdot 220 \equiv 2 \pmod{7}, \end{cases} \quad \begin{cases} 4 \cdot 220 \equiv 5 \pmod{7}, \\ 5 \cdot 220 \equiv 1 \pmod{7}, \\ 6 \cdot 220 \equiv 4 \pmod{7}. \end{cases}$$

В этом случае $B_{31} = 5 \cdot 220 = 1100$.

Определяем значение B_{41} . В этом случае $m_4 = 11, M_1 / m_4 = 1540 / 11 = 140$. $\bar{m}_{41} \equiv \overline{1, m_4 - 1} = \overline{1, 10}$. Имеем

Определим B_{33} . Имеем $m_3 = 7$, $M_3 / m_3 = 924 / 7 = 132$, $\overline{m_{33}} \equiv \overline{1, m_3 - 1} = \overline{1, 6}$.

$$\begin{cases} 1 \cdot 132 \equiv 6 \pmod{7}, \\ 2 \cdot 132 \equiv 5 \pmod{7}, \\ 3 \cdot 132 \equiv 4 \pmod{7}, \end{cases} \quad \begin{cases} 4 \cdot 132 \equiv 3 \pmod{7}, \\ 5 \cdot 132 \equiv 2 \pmod{7}, \\ 6 \cdot 132 \equiv 1 \pmod{7}. \end{cases}$$

В этом случае $B_{33} = 6 \cdot 132 = 792$.

Определим B_{43} .

Имеем $m_4 = 11$, $M_3 / m_4 = 924 / 7 = 84$, $\overline{m_{43}} \equiv \overline{1, m_4 - 1} = \overline{1, 10}$.

$$\begin{cases} 1 \cdot 84 \equiv 7 \pmod{11}, \\ 2 \cdot 84 \equiv 3 \pmod{11}, \\ 3 \cdot 84 \equiv 10 \pmod{11}, \\ 4 \cdot 84 \equiv 6 \pmod{11}, \\ 5 \cdot 84 \equiv 3 \pmod{11}, \end{cases} \quad \begin{cases} 6 \cdot 84 \equiv 9 \pmod{11}, \\ 7 \cdot 84 \equiv 5 \pmod{11}, \\ 8 \cdot 84 \equiv 1 \pmod{11}, \\ 9 \cdot 84 \equiv 8 \pmod{11}, \\ 10 \cdot 84 \equiv 4 \pmod{11}. \end{cases}$$

В этом случае $B_{43} = 8 \cdot 84 = 672$.

2.1.4. Определим значения B_{i4} для четвертого ($j = 4$) набора оснований $m_1 = 3$, $m_2 = 4$, $m_3 = 5$, $m_4 = 11$ КВ (табл. 1). В этом случае $M_4 = \prod_{i=1}^4 m_i = 660$ ($M = 420$).

Определим B_{14} . Имеем $m_1 = 3$, $M_4 / m_1 = 660 / 3 = 220$, $\overline{m_{14}} \equiv \overline{1, m_1 - 1} = \overline{1, 2}$.

$$\begin{cases} 1 \cdot 220 \equiv 1 \pmod{3}, \\ 2 \cdot 220 \equiv 2 \pmod{3}. \end{cases}$$

В этом случае $B_{14} = 1 \cdot 220 = 220$.

Определим B_{24} . Имеем $m_2 = 4$, $M_4 / m_2 = 660 / 4 = 165$, $\overline{m_{24}} \equiv \overline{1, m_2 - 1} = \overline{1, 3}$.

$$\begin{cases} 1 \cdot 165 \equiv 1 \pmod{4}, \\ 2 \cdot 165 \equiv 2 \pmod{4}, \\ 3 \cdot 165 \equiv 3 \pmod{4}. \end{cases}$$

В этом случае $B_{24} = 1 \cdot 165 = 165$.

Определим B_{34} . Имеем $m_3 = 5$, $M_4 / m_3 = 660 / 5 = 132$, $\overline{m_{34}} \equiv \overline{1, m_3 - 1} = \overline{1, 4}$.

$$\begin{cases} 1 \cdot 132 \equiv 2 \pmod{5}, \\ 2 \cdot 132 \equiv 4 \pmod{5}, \end{cases} \quad \begin{cases} 3 \cdot 132 \equiv 1 \pmod{5}, \\ 4 \cdot 132 \equiv 3 \pmod{5}. \end{cases}$$

В этом случае $B_{34} = 3 \cdot 132 = 396$.

Определим B_{44} . Имеем $m_4 = 11$, $M_4 / m_4 = 660 / 11 = 60$, $\overline{m_{44}} \equiv \overline{1, m_4 - 1} = \overline{1, 10}$.

$$\begin{cases} 1 \cdot 60 \equiv 5 \pmod{11}, \\ 2 \cdot 60 \equiv 10 \pmod{11}, \\ 3 \cdot 60 \equiv 4 \pmod{11}, \\ 4 \cdot 60 \equiv 9 \pmod{11}, \\ 5 \cdot 60 \equiv 3 \pmod{11}, \end{cases} \quad \begin{cases} 6 \cdot 60 \equiv 8 \pmod{11}, \\ 7 \cdot 60 \equiv 2 \pmod{11}, \\ 8 \cdot 60 \equiv 7 \pmod{11}, \\ 9 \cdot 60 \equiv 1 \pmod{11}, \\ 10 \cdot 60 \equiv 6 \pmod{11}. \end{cases}$$

В этом случае $B_{44} = 9 \cdot 60 = 540$.

2.1.5. Определим значения B_{i5} для пятого ($j = 5$) набора оснований $m_1 = 3$, $m_2 = 4$, $m_3 = 5$, $m_4 = 7$ КВ (табл. 1). В этом случае $M_5 = \prod_{i=1}^4 m_i = 420$ ($M = 420$).

Определим B_{15} . Имеем $m_1 = 3$, $M_5 / m_1 = 420 / 3 = 140$, $\overline{m_{15}} \equiv \overline{1, m_1 - 1} = \overline{1, 2}$.

$$\begin{cases} 1 \cdot 140 \equiv 2 \pmod{3}, \\ 2 \cdot 140 \equiv 1 \pmod{3}. \end{cases}$$

В этом случае $B_{15} = 2 \cdot 140 = 280$.

Определим B_{25} . Имеем $m_2 = 4$, $M_5 / m_2 = 420 / 4 = 105$, $\overline{m_{25}} \equiv \overline{1, m_2 - 1} = \overline{1, 3}$.

$$\begin{cases} 1 \cdot 105 \equiv 1 \pmod{4}, \\ 2 \cdot 105 \equiv 2 \pmod{4}, \\ 3 \cdot 105 \equiv 3 \pmod{4}. \end{cases}$$

В этом случае $B_{25} = 1 \cdot 105 = 105$.

Определим B_{35} . Имеем $m_3 = 5$, $M_5 / m_3 = 420 / 5 = 84$, $\overline{m_{35}} \equiv \overline{1, m_3 - 1} = \overline{1, 4}$.

$$\begin{cases} 1 \cdot 84 \equiv 4 \pmod{5}, & \begin{cases} 3 \cdot 84 \equiv 2 \pmod{5}, \\ 4 \cdot 84 \equiv 1 \pmod{5}. \end{cases} \\ 2 \cdot 84 \equiv 3 \pmod{5}, \end{cases}$$

В этом случае $B_{35} = 4 \cdot 84 = 336$.

Определим B_{45} . Имеем $m_4 = 7$, $M_5 / m_4 = 420 / 7 = 60$, $\overline{m_{45}} \equiv \overline{1, m_4 - 1} = \overline{1, 6}$.

$$\begin{cases} 1 \cdot 60 \equiv 4 \pmod{7}, & \begin{cases} 4 \cdot 60 \equiv 2 \pmod{7}, \\ 5 \cdot 60 \equiv 6 \pmod{7}, \\ 6 \cdot 60 \equiv 3 \pmod{7}. \end{cases} \\ 2 \cdot 60 \equiv 1 \pmod{7}, \\ 3 \cdot 60 \equiv 5 \pmod{7}. \end{cases}$$

В этом случае $B_{45} = 2 \cdot 60 = 120$.

Совокупность рассчитанных ортогональных базисов B_j приведена в табл. 5.

Таблица 5. Ортогональные базисы B_{ji} для $i = 1$

$\begin{smallmatrix} j \\ i \end{smallmatrix}$	1	2	3	4
1	385	616	1100	980
2	385	231	330	210
3	616	693	792	672
4	220	165	396	540
5	280	105	336	120

2.2. Определим правильность остатков числа $\tilde{A}$. Вначале составим все проекции $\tilde{A}_j$ числа $\tilde{A} = (0, 0, 0, 2, 1)$

$$\begin{cases} \tilde{A}_1 = (0, 0, 2, 1), \\ \tilde{A}_2 = (0, 0, 2, 1), \\ \tilde{A}_3 = (0, 0, 2, 1), \end{cases} \quad \begin{cases} \tilde{A}_4 = (0, 0, 0, 1), \\ \tilde{A}_5 = (0, 0, 0, 2). \end{cases}$$

По формуле (1) представим значения проекций $\tilde{A}_j$ $j = \overline{1, 5}$ в ПСС, и используя данные (табл. 5):

$$\tilde{A}_1 = (a_1 \cdot B_{11} + a_2 \cdot B_{21} + a_3 \cdot B_{31} + a_4 \cdot B_{41}) \bmod M_1 = (0 \cdot 385 + 0 \cdot 616 + 2 \cdot 1100 + 1 \cdot 980) \bmod 1540 = 100$$

$$\tilde{A}_2 = (a_1 \cdot B_{12} + a_2 \cdot B_{22} + a_3 \cdot B_{32} + a_4 \cdot B_{42}) \bmod M_2 = (0 \cdot 385 + 0 \cdot 231 + 2 \cdot 330 + 1 \cdot 210) \bmod 1155 = 870$$

$$\tilde{A}_3 = (a_1 \cdot B_{13} + a_2 \cdot B_{23} + a_3 \cdot B_{33} + a_4 \cdot B_{43}) \bmod M_3 = (0 \cdot 616 + 0 \cdot 693 + 2 \cdot 792 + 1 \cdot 672) \bmod 924 = 418$$

$$\tilde{A}_4 = (a_1 \cdot B_{14} + a_2 \cdot B_{24} + a_3 \cdot B_{34} + a_4 \cdot B_{44}) \bmod M_4 = (0 \cdot 220 + 0 \cdot 165 + 2 \cdot 396 + 1 \cdot 540) \bmod 660 = 540$$

$$\tilde{A}_5 = (a_1 \cdot B_{15} + a_2 \cdot B_{25} + a_3 \cdot B_{35} + a_4 \cdot B_{45}) \bmod M_5 = (0 \cdot 280 + 0 \cdot 105 + 2 \cdot 336 + 1 \cdot 120) \bmod 420 = 240$$

Таким образом, среди всех проекций $\tilde{A}_i$ числа $\tilde{A}$ есть также проекции такие, как $\tilde{A}_1$, $\tilde{A}_2$ и $\tilde{A}_5$, которые меньше $M = 420$. Проекция A_2 и $\tilde{A}_4$ больше $M = 420$ и такие проекции. Проекция $\tilde{A}_2$ и A_4 больше значения M . Следовательно остатки a_1 , a_3 и a_5 могут быть ошибочными, а остатки a_2 и a_4 точно не искажены.

Выводы

В статье предложены метод контроля и метод диагностики информации, представленной в КВ. Данные методы основаны на использовании ортогональных базисов для полной системы оснований $\{m_i\}$ КВ, а также совокупности проекций $A_i = (a_1, a_2, \dots, a_{i-1}, a_{i+1}, \dots, a_n, a_{n+1})$ числа A по модулю m_i . Приведен конкретный пример контроля и диагностики данных в КВ для КСПОЦИ с однобайтовой разрядной сеткой. Предложенные методы позволяют упростить техническую процедуру контроля и диагностики данных, представленных в КВ, а также повысить оперативность проведения этой процедуры.

Список литературы: 1. Акулиский И.Я., Юдицкий Д.И. Машинная арифметика в остаточных классах. – М. : Радио и связь, 1968. – 440с. 2. Барсов В.И., Сорока Л.С., Краснобаев В.А. Методология параллельной обработки информации в модулярной системе счисления. – Х. : ХУПС, 2009. – 268с.

*Харьковский национальный
технический университет сельского хозяйства
имени Петра Василенка,
Харьковский национальный
университет радиозлектроники*

Поступила в редколлегию 07.06.2011.

МЕТОДЫ ПОСТРОЕНИЯ И ИССЛЕДОВАНИЯ СВОЙСТВ ПРОИЗВОДНЫХ НЕЛИНЕЙНЫХ РЕКУРРЕНТНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Системы нелинейных рекуррентных последовательностей (НРП) являются плотноупакованными по периодической функции корреляции (ПФАК), существуют для большого спектра длительностей L , однако размерность ансамбля НРП ограничена, например для НРП характеристического типа – функцией Эйлера. Проведенные исследования показали, что дальнейшее увеличение размерности ансамбля и улучшение структурных свойств может быть достигнуто на основе использования L -позиционных НРП, построение которых осуществляется посредством образования последовательного произведения $Z_i, i = \overline{1, k}$, символов W_i^j НРП с одно- или двухуровневой ПФАК.

Правило построения символов W_i^p производных нелинейных рекуррентных последовательностей (ПНРП) сформулируем в виде

$$W_i^p = \prod_{j=1}^k W_{i(\bmod L_1), j} \quad (1)$$

ПФАК, построенную по (1) ПНРП, найдем, используя соотношение $r_j(l) = \sum_{i=1}^{L-m} W_i^j (W_{i+l}^j)^*$:

$$R_w^p(l) = \sum_{i=0}^{L-1} \prod_{j=1}^{K_1} W_{i(\bmod L_1), j} \prod_{j=1}^{K_2} W_{i+l(\bmod L_1), j} \quad (2)$$

где $K_1 \neq K_2$.

Анализ корреляционных свойств с использованием (2) в общем виде затруднен, поэтому рассмотрим ряд частных случаев, важных с теоретической и практической точек зрения.

1. Пусть $K_1 = K_2$, а $L_1 \neq L_2$, тогда (2) имеет вид

$$R_w(l) = \sum_{i=0}^{L-1} W_{i(\bmod L_1), 1} \cdot W_{i+l(\bmod L_1), 1} \cdot W_{i(\bmod L_1), 2} \cdot W_{i+l(\bmod L_2), 2} \quad (3)$$

Для преобразования (3) представим индекс суммирования i в L_2 -ричной системе исчисления

$$i = \nu L_2 + \varepsilon, \quad 0 \leq \varepsilon \leq L_2, \quad 0 \leq \nu \leq L_1 \quad (4)$$

$$R_w(l) = \sum_{\nu=0}^{L_1-1} \sum_{\varepsilon=0}^{L_2-1} W_{\nu L_2 + \varepsilon(\bmod L_1), 1} \cdot W_{\nu L_2 + \varepsilon(\bmod L_2), 2} \cdot W_{\nu L_2 + \varepsilon + l(\bmod L_1), 2} \cdot W_{\nu L_2 + \varepsilon + l(\bmod L_2), 2} = \sum_{\varepsilon=0}^{L_2-1} W_{\varepsilon(\bmod L_1), 1} \cdot W_{\varepsilon + l(\bmod L_1), 1} \cdot W_{\varepsilon(\bmod L_2), 2} \cdot W_{\varepsilon + l(\bmod L_2), 2} = R_{W_2}(l) \quad (5)$$

С учетом того, что $r_j(l) = \sum_{i=1}^{L-m} W_i^j (W_{i+l}^j)^*$

$$\sum_{\varepsilon=0}^{L_2-1} W_{\varepsilon(\bmod L_2), 2} \cdot W_{\varepsilon+l(\bmod L_2), 2} = R_{W_2}(l) \quad (6)$$

Кроме того, если ν принимает значение из множества вычетов по $\text{mod } L_1$, то $\nu L_2 + \varepsilon$ пробегает значения по модулю L_1 , поэтому

$$\sum_{\varepsilon=0}^{L_1-1} W_{\nu L_2 + \varepsilon (\text{mod } L_1), 1} \cdot W_{\nu L_2 + \varepsilon + l (\text{mod } L_1), 1} = \sum_{q=0}^{L_1-1} W_{q (\text{mod } L_1), 1} \cdot W_{q + \varepsilon (\text{mod } L_1), 1} = R_{W_1}(l) \quad (7)$$

и ПФАК ПНРП может быть вычислена с использованием выражения

$$R_{W''}(l) = R_{W_1}(l) \cdot R_{W_2}(l). \quad (8)$$

Но так как $R_{W_1}(l)$ и $R_{W_2}(l)$ могут принимать соответственно значения L_1 и L_2 при $l = 0$, $R_{W_1}(l)$ и $R_{W_2}(l)$ при $l = \overline{1, L-1}$, то

$$R_{W''}(l) = \begin{cases} L, & \text{при } l \equiv 0 (\text{mod } L); \\ L_2 R_{W_1}(l), & \text{при } l \equiv 0 (\text{mod } L_2), L \neq 0 (\text{mod } L_1); \\ L_1 R_{W_2}(l), & \text{при } l \equiv 0 (\text{mod } L_1), l \neq 0 (\text{mod } L_2); \\ R_{W_1}(l) \cdot R_{W_2}(l), & \text{при } l \neq 0 (\text{mod } L_1, \text{mod } L_2). \end{cases} \quad (9)$$

Анализ (9) показывает, что минимальные боковые лепестки ПНРП достигаются в случае, если L_2 , $R_{W_1}(l)$, L_1 , $R_{W_2}(l)$ принимают минимальные значения. Кроме того, как следует из [1], ПНРП имеет максимальный период, если L_1 и L_2 взаимно простые числа.

2. Пусть $K = 3$, а $L_1 \neq L_2 \neq L_3$. В этом случае по аналогии с (9) выражение (2) можно представить в виде

$$R_{W''}(l) = R_{W_1}(l) \cdot R_{W_2}(l) \cdot R_{W_3}(l). \quad (10)$$

Или

$$R_{W''}(l) = \begin{cases} L, & \text{при } l \equiv 0 (\text{mod } L); \\ R_{W_1}(l) \cdot R_{W_2}(l) \cdot R_{W_3}(l), & \text{при } l \neq 0 (\text{mod } L_1, L_2, L_3); \\ L_1 \cdot R_{W_2}(l) \cdot R_{W_3}(l), & \text{при } l \equiv 0 (\text{mod } L_1), l \neq 0 (\text{mod } L_2, L_3); \\ L_2 \cdot R_{W_1}(l) \cdot R_{W_3}(l), & \text{при } l \equiv 0 (\text{mod } L_2), l \neq 0 (\text{mod } L_1, L_3); \\ L_3 \cdot R_{W_1}(l) \cdot R_{W_2}(l), & \text{при } l \equiv 0 (\text{mod } L_3), l \neq 0 (\text{mod } L_1, L_2); \\ L_1 \cdot R_{W_2}(l) \cdot L_3, & \text{при } l \equiv 0 (\text{mod } L_1, L_3), l \neq 0 (\text{mod } L_2); \\ L_1 \cdot L_2 \cdot R_{W_3}(l), & \text{при } l \equiv 0 (\text{mod } L_1, L_2), l \neq 0 (\text{mod } L_3); \\ R_{W_1}(l) \cdot L_2 \cdot L_3, & \text{при } l \equiv 0 (\text{mod } L_2, L_3), l \neq 0 (\text{mod } L_1). \end{cases} \quad (11)$$

Рассмотрение (11) показывает, что для минимизации $R_{W''}(l)$ необходимо и достаточно, чтобы $R_{W_1}(l)$, $R_{W_2}(l)$ и $R_{W_3}(l)$ были минимальными, а L_1 , L_2 и L_3 – минимальными и взаимно простыми. Минимальное значение R_{W_i} , $i = \overline{1, 3}$, равно 0 и достигается только при использовании в качестве W_i последовательности [2] вида $\{1 \ 1 \ 1 \ -1\}$. В этом случае выражение (11) принимает вид

$$R_{W''}(l) = \begin{cases} L, & \text{при } l \equiv 0 (\text{mod } L); & a) \\ L_1 \cdot R_{W_2}(l) \cdot R_{W_3}(l), & \text{при } l \equiv 0 (\text{mod } L_1), l \neq 0 (\text{mod } L_2, L_3); & б) \\ L_1 \cdot R_{W_3}(l) \cdot L_2, & \text{при } l \equiv 0 (\text{mod } L_1, L_2), l \neq 0 (\text{mod } L_3); & в) \\ L_1 \cdot R_{W_2}(l) \cdot L_3, & \text{при } l \equiv 0 (\text{mod } L_1, L_3), l \neq 0 (\text{mod } L_2). & г) \end{cases} \quad (12)$$

Исследование выражений (12, а, б, в) показывает, что для их минимизации необходимо, чтобы как принимаемые значения ПФАК $R_{w_1}(l)$, $R_{w_2}(l)$ и $R_{w_3}(l)$, так и значения их длительностей были бы минимальными. С учетом того, что $L_1 = 4$, максимальные значения ПФАК $R_w(l)$ дают слагаемые в) и в). Если L_2 и L_3 – взаимно простые, то минимальные значения $R_{w_2}(l)$ и $R_{w_3}(l)$ могут быть соответственно равны $\{\pm 1\}$ и $\{-4, 0\}$ или $\{0, 4\}$, или $\{2, -2\}$, поэтому

$$R_{w''}(l) = \begin{cases} L, & \text{при } l \equiv 0(\text{mod } L); \\ \pm 4, & \text{при } l \equiv 0(\text{mod } L_1), l \neq 0(\text{mod } L_2, L_3); \\ \pm 4L_1L_2, & \text{при } l \equiv 0(\text{mod } L_1, L_2), l \neq 0(\text{mod } L_3); \\ \pm L_1L_3, & \text{при } l \equiv 0(\text{mod } L_1, L_3), l \neq 0(\text{mod } L_2). \end{cases} \quad \begin{matrix} \text{а)} \\ \text{б)} \\ \text{в)} \\ \text{г)} \end{matrix} \quad (13)$$

Если L_1 и L_2 – взаимно простые, то выражение $\pm 4L_1L_2$ принимает значение либо $\pm 4L_1R_{w_2}(l)$, либо $\pm 4R_{w_1}(l)L_2$, поэтому максимальный боковой лепесток дает составляющая $\pm L_1L_3$.

Из рассмотренного следует, что для минимизации боковых лепестков необходимо, чтобы L_1 , L_2 и L_3 были взаимно простыми. Этого можно достичь, если L_1 и L_2 – простые, а $L_3 \equiv 0(\text{mod } 2)$. При этих условиях составляющие (11) принимают значения

$$R_{w''}(l) = \begin{cases} L, & \text{при } l \equiv 0(\text{mod } L); \\ R_{w_1}(l) \cdot R_{w_2}(l) \cdot R_{w_3}(l), & \text{при } l \neq 0(\text{mod } L_1, L_2, L_3); \\ L_1 \cdot R_{w_2}(l) \cdot R_{w_3}(l), & \text{при } l \equiv 0(\text{mod } L_1), l \neq 0(\text{mod } L_2, L_3); \\ L_2 \cdot R_{w_1}(l) \cdot R_{w_3}(l), & \text{при } l \equiv 0(\text{mod } L_2), l \neq 0(\text{mod } L_1, L_3); \\ L_3 \cdot R_{w_1}(l) \cdot R_{w_2}(l), & \text{при } l \equiv 0(\text{mod } L_3), l \neq 0(\text{mod } L_1, L_2). \end{cases} \quad (14)$$

3. Пусть $L_1 = L_2 = L_K = L$, а $K_1 = K_2 = K$. Для этих условий с учетом (2) выражение для ПФАК ПНРП можно представить в виде

$$R_{w''}(l) = \sum_{i=0}^{L-1} \prod_{j=1}^K W_{i,j}^q \prod_{j=1}^K W_{i-L,j}, \quad (15)$$

причем (15) позволяет вычислить ПФАК, если положить, что $q = r$.

Проведенные исследования показали, что для (15) можно получить оценки, если воспользоваться теорией двухзначных характеров, в частности тем, что для любого нетривиального характера справедливо [3]

$$\sum_{y \in GF(P)} \Psi(ay + b) = \sum_{\substack{y \in GF(P^n) \\ y \equiv 0(\text{mod } P)}} \Psi(ay + b) + \Psi(b) = 0$$

и фиксированными правилами кодирования. Например, для наиболее мощного класса двухуровневых последовательностей – последовательностей характеристического типа с числом символов $L = 2x = P^n - 1$, $x = 1, 2, 3, \dots, z, \dots$

$$W^q = \{W_i^q, \quad i = \overline{0, P^n - 1}\};$$

$$W_i^q = \begin{cases} \Psi(\Theta_q^i + 1), & \text{если } \Theta_q^i + 1 \not\equiv 0 \pmod{f(x), P}; \\ 1, & \text{если } \Theta_q^i + 1 \equiv 0 \pmod{f(x), P}; \end{cases} \quad a) \quad (16)$$

либо

$$W_i^q = \begin{cases} \Psi(\Theta_q^i + 1), & \text{если } \Theta_q^i + 1 \not\equiv 0 \pmod{f_m(x), P}; \\ -1, & \text{если } \Theta_q^i + 1 \equiv 0 \pmod{f_m(x), P}; \end{cases} \quad б) \quad (16)$$

где Θ_q – q -й первообразный элемент поля $GF(P)$, а $f_m(x)$ – m -й первообразный примитивный полином степени n .

Приведем вывод аналитического выражения для ПФАК ПНРП.

Используя (15) и полагая, что $q \neq r$, имеем

$$R_{W_n}(l) = \sum_{i=0}^{L-1} \Psi(\Theta_q^i + 1) \cdot \Psi(\Theta_q^{i+l} + 1) \cdot \Psi(\Theta_r^{i+l} + 1). \quad (17)$$

С учетом того, что $\Psi(0) = 0$, [4], при $l \neq 0 \pmod{L}$

$$R_{W_n}(l) = \sum_{i=0}^{P^n-2} \Psi(\Theta_q^i + 1) \cdot \Psi(\Theta_q^{i+l} + 1) \cdot \Psi(\Theta_r^{i+l} + 1) \pm Z \quad (18)$$

где Z – учитывает сумму слагаемых, входящих в (17), для которых

$$(\Theta_q^i + 1) \equiv 0 \vee (\Theta_q^{i+l} + 1) \equiv 0 \vee (\Theta_r^{i+l} + 1) \equiv 0 \pmod{f_m(x), P} \quad (19)$$

Более точно структуру (19) определяют сформулированные ниже утверждения.

Утверждение 1. Пусть $\Theta_v^i + 1$ и $\Theta_v^{i+l} + 1$ есть элементы поля $GF(P^n)$ а Θ_v^v – v -й первообразный элемент, тогда при $l \neq 0 \pmod{L}$ $\Theta_v^i + 1$ и $\Theta_v^{i+l} + 1$ никогда не сравнимы с $0 \pmod{f_m(x), P}$. Доказательство утверждения следует из цикличности поля $GF(P^n)$ [4].

Утверждение 2. Пусть $\Theta_v^r + 1$ и $\Theta_k^m + 1$ – элементы поля $GF(P^n)$, а Θ_v и Θ_k – первообразные. Существуют T^{s1} и T^{s2} автоморфные преобразования, при которых $\Theta_v^r + 1 \equiv \Theta_k^m + 1 \equiv 0 \pmod{L}$.

Доказательство утверждения следует из авто- и изоморфных свойств поля $GF(P^n)$ [4].

С учетом утверждения (17) и (18) выражение (19) распадается на следующие логические высказывания:

$$\begin{aligned} \Theta_q^i + 1 \equiv 0 \wedge \Theta_q^{i+l} + 1 \equiv 0 \wedge \Theta_r^{i+l} \not\equiv 0 \pmod{L}; & a) \\ \Theta_q^i + 1 \equiv 0 \wedge \Theta_q^{i+l} + 1 \not\equiv 0 \wedge \Theta_r^i + 1 \equiv 0 \wedge \Theta_r^{i+l} + 1 \not\equiv 0 \pmod{L}; & б) \\ \Theta_q^i + 1 \equiv 0 \wedge \Theta_q^{i+l} + 1 \not\equiv 0 \wedge \Theta_r^i + 1 \not\equiv 0 \wedge \Theta_r^{i+l} + 1 \equiv 0 \pmod{L}; & в) \\ \Theta_q^i + 1 \not\equiv 0 \wedge \Theta_q^{i+l} + 1 \equiv 0 \wedge \Theta_r^i + 1 \not\equiv 0 \wedge \Theta_r^{i+l} + 1 \not\equiv 0 \pmod{L}; & г) \\ \Theta_q^i + 1 \not\equiv 0 \wedge \Theta_q^{i+l} + 1 \equiv 0 \wedge \Theta_r^i + 1 \equiv 0 \wedge \Theta_r^{i+l} + 1 \not\equiv 0 \pmod{L}; & д) \\ \Theta_q^i + 1 \not\equiv 0 \wedge \Theta_q^{i+l} + 1 \equiv 0 \wedge \Theta_r^i + 1 \not\equiv 0 \wedge \Theta_r^{i+l} + 1 \equiv 0 \pmod{L}; & е) \\ \Theta_q^i + 1 \not\equiv 0 \wedge \Theta_q^{i+l} + 1 \not\equiv 0 \wedge \Theta_r^i + 1 \equiv 0 \wedge \Theta_r^{i+l} + 1 \not\equiv 0 \pmod{L}; & ж) \\ \Theta_q^i + 1 \not\equiv 0 \wedge \Theta_q^{i+l} + 1 \not\equiv 0 \wedge \Theta_r^i + 1 \not\equiv 0 \wedge \Theta_r^{i+l} + 1 \equiv 0 \pmod{L}. & з) \end{aligned} \quad (20)$$

Анализ (20) показывает, что исключаящими являются высказывания а), г), ж), з), поэтому

$$Z = \Psi(-\Theta_q^{i+l} + 1) \cdot \Psi(-\Theta_r^i + 1) \cdot \Psi(-\Theta_r^{i+l} + 1) + \Psi(-\Theta_q^{-l} + 1) \cdot \Psi(\Theta_r^i + 1),$$

$$\Psi = (\Theta_r^{i+l} + 1) + \Psi(-\Theta_r^i + 1) \cdot \Psi(\Theta_q^i + 1) \Psi(\Theta_q^{i+l} + 1) + \Psi(-\Theta_r^{-l} + 1) \Psi(\Theta_q^i + 1) \Psi(\Theta_q^{i+l} + 1). \quad (21)$$

Если истинно высказывание (20, а), то $\Psi(\Theta_q^i + 1) = 0$, так как $\Theta_q^i + 1 \equiv 0 \pmod{L}$ [4], поэтому $\Psi(\Theta_q^{i+l} + 1) = \Psi[\Theta_q^i (\Theta_q^i + \Theta_q^{-l})] = \Psi[\Theta_q^i (\Theta_q^{-l} - 1)] = \Psi(\Theta_q^i \cdot \Theta_q^{-l} - \Theta_q^i) = \Psi(1 - \Theta_q^i) = \Psi(-\Theta_q^i + 1)$.

В случае, если $\Theta_q^{i+l} + 1 \equiv 0 \pmod{L}$, то

$$\Psi(\Theta_q^i + 1) = -\Psi(\Theta_q^i \cdot \Theta_q^i \cdot \Theta_q^{-l} + 1) = \Psi[\Theta_q^{-l} (\Theta_q^{i+l} + \Theta_q^{-l})] = \Psi[\Theta_q^{-l} (\Theta_q^{-l} - 1)] = \Psi(-\Theta_q^{-l} + 1).$$

Преобразуем выражение (18), используя свойство характера Ψ [Альберт], не рассматривая Z сумму, определяемую (П. 7.5), обозначив его переменной X :

$$\begin{aligned} X &= \sum_{i=0}^{P^n-2} \Psi(\Theta_q^i + 1) \cdot \Psi(\Theta_q^{i+l} + 1) \cdot \Psi(\Theta_r^i + 1) \cdot \Psi(\Theta_r^{i+l} + 1) = \\ &= \Psi(\Theta_q^i) \cdot \Psi(\Theta_r^i) \sum_{i=0}^{P^n-2} \Psi(\Theta_q^i + 1) \cdot \Psi(\Theta_q^i + \Theta_q^{-l}) \cdot \Psi(\Theta_r^i + 1) \cdot \Psi(\Theta_r^i + \Theta_r^{-l}) = \Psi(\Theta_q^i) \cdot \Psi(\Theta_r^i) \cdot Q \end{aligned} \quad (22)$$

Проанализируем выражение

$$Q = \sum_{i=0}^{P^n-2} \Psi(\Theta_q^i + 1) \cdot \Psi(\Theta_q^i + \Theta_q^{-l}) \cdot \Psi(\Theta_r^i + 1) \cdot \Psi(\Theta_r^i + \Theta_r^{-l}),$$

учитывая, что если i принимает значения индексов суммирования, то степени первообразных элементов Θ_q и Θ_r принимают значения всех ненулевых элементов поля $GF(P^n)$. Обозначая ненулевые элементы поля через a_i и b_i соответственно для первообразных Θ_q и Θ_r , при $i = \overline{0, P^n - 2}$, перейдем к сумме произведения характеров ненулевых элементов

$$Q = \sum_{a_i, b_i \in GF(P^n)} \Psi(a_i + 1) \cdot \Psi(a_i + \Theta_q^{-l}) \cdot \Psi(b_i + 1) \cdot \Psi(b_i + \Theta_r^{-l}). \quad (23)$$

Полагая в (23) $c_i = a_i + 1$ и $d_i = b_i + 1$, проанализируем все c_i и d_i , если a_i и b_i пробегают при изменении все ненулевые элементы поля $GF(P^n)$, то c_i и d_i также пробегают все ненулевые поля $GF(P^n)$, исключая 1, поэтому

$$Q = \sum_{\substack{c, d_i \in GF(P^n) \\ c, d_i \neq 1 \pmod{P}}} \Psi(c_i) \cdot \Psi(c_i + \Theta_q^{-l} + 1) \cdot \Psi(d_i) \cdot \Psi(d_i + \Theta_r^{-l} - 1) \quad (24)$$

Если же

$$\begin{aligned} c_i = 1, \quad \text{то } Q_1 &= \Psi(\Theta_q^{-l}) \Psi(d_i) \Psi(d_i + \Theta_r^{-l} - 1), & a) \\ d_i = 1, \quad \text{то } Q_2 &= \Psi(c_i) \Psi(c_i + \Theta_q^{-l} - 1) \Psi(\Theta_r^{-l}), & б) \\ c_i = 1, d_i = 1, \quad \text{то } Q_3 &= \Psi(\Theta_q^{-l}) \Psi(\Theta_q^{-l}) \Psi(\Theta_r^{-l}), & в) \end{aligned} \quad (25)$$

Исключим в (25) условие $c_i, d_i \neq 1 \pmod{P}$, для этого добавим в него и вычтем Q_1 , Q_2 и Q_3 . В результате получим

$$\begin{aligned}
Q &= \sum \Psi(c_i) \Psi(c_i + \Theta_q^{-l} - 1) \Psi(d_i) \Psi(d_i + \Theta_r^{-l}) - \Psi(\Theta_q^{-l}) \Psi(d_i) \Psi(d_i + \Theta_r^{-l} - 1) - \\
&- \Psi(c_i) \Psi(c_i + \Theta_q^{-l} - 1) \Psi(\Theta_r^{-l}) - \Psi(\Theta_q^{-l}) \Psi(\Theta_r^{-l}) = \\
&= \sum_{\substack{c_i, d_i \in GF(P^n) \\ c_i, d_i \neq 0 \pmod{P}}} \Psi(c_i^2) \Psi(1 + (\Theta_q^{-l} - 1)c_i^{-1}) \Psi(d_i^2) \Psi[1 + (\Theta_r^{-l} - 1)d_i^{-1}] - Q_1 - Q_2 - Q_3.
\end{aligned} \tag{26}$$

Даже принимая во внимание, что $\Theta_q^{-l} - 1$ и $\Theta_r^{-l} - 1 \in GF(P^n)$ являются постоянными, обозначив их как $q_1 = \Theta_q^{-l} - 1$ и $q_2 = \Theta_r^{-l} - 1$, $q_1, q_2 \neq 0 \pmod{P}$, а также обозначив $x_i = c_i^{-1}$ и $y_i = d_i^{-1}$, которые пробегают так же все элементы поля $GF(P^n)$, получим

$$Q = \sum_{\substack{x_i, y_i \in GF(P^n) \\ x_i, y_i \neq 0 \pmod{P}}} \Psi(1 + q_1 x_i) \Psi(1 + q_2 y_i) - Q_1 - Q_2 - Q_3.$$

С учетом (21), (23), (25), выражение (18) есть:

$$\begin{aligned}
R_{W^n}(l) &= \Psi(\Theta_q^l) \Psi(\Theta_r^l) \left\{ \sum_{\substack{x_i, y_i \in GF(P^n) \\ x_i, y_i \neq 0 \pmod{P}}} \Psi(1 + q_1 x_i) \Psi(1 + q_2 y_i) - [\Psi(\Theta_q^{-l}) \cdot \Psi(d_i) \Psi(d_i - \Theta_r^{-l} - 1) + \right. \\
&+ \Psi(c_i) \Psi(c_i + \Theta_q^{-l} - 1) \Psi(\Theta_r^{-l}) + \Psi(\Theta_q^{-l}) \Psi(\Theta_r^{-l})] \} + \{ \Psi(-\Theta_q^l + 1) \Psi(\Theta_q^l + 1) \Psi(\Theta_r^{i+l} + 1) + \\
&+ \Psi(-\Theta_q^{-l} + 1) \Psi(\Theta_r^l + 1) \Psi(\Theta_r^{i+l} + 1) + \Psi(-\Theta_r^l + 1) \Psi(\Theta_q^l + 1) \Psi(\Theta_q^{i+l} + 1) + \\
&+ \Psi(-\Theta_r^{-l} + 1) \Psi(\Theta_r^{-l} + 1) \Psi(\Theta_r^{i+l} + 1) + \Psi(-\Theta_r^l + 1) \Psi(\Theta_q^l + 1) \Psi(\Theta_q^{i+l} + 1) + \\
&+ \Psi(-\Theta_r^{-l} + 1) \Psi(\Theta_q^{i+l} + 1) \Psi(\Theta_q^{i+l} + 1) \},
\end{aligned} \tag{27}$$

где запись $\{y\}$ означает, что слагаемые в скобках необходимо брать со знаками $+$ ($-$) во всех возможных сочетаниях, то есть 2^k – сочетаний, если k – число слагаемых.

Упростим (27) учитывая, что все слагаемые

$$\begin{aligned}
&\Psi(\Theta_q^l), \Psi(\Theta_r^l), \Psi(\Theta_q^{-l}), \Psi(d_i), \Psi(d_i - \Theta_r^{-l} - 1), \dots, \\
&\Psi(-\Theta_r^{-l} + 1) \Psi(\Theta_q^l + 1) \Psi(\Theta_q^{i+l} + 1) \in \{1, -1\}.
\end{aligned} \tag{28}$$

Из (28) непосредственно следует, что

$$\begin{aligned}
Z &= \pm \{ \Psi(-\Theta_q^l + 1) \Psi(\Theta_q^l + 1) \Psi(\Theta_r^{i+l} + 1) + \Psi(-\Theta_q^{-l} + 1) \Psi(\Theta_r^l + 1) \Psi(\Theta_r^{i+l} + 1) + \\
&+ \Psi(-\Theta_r^l + 1) \Psi(\Theta_q^l + 1) \Psi(\Theta_q^{i+l} + 1) + \Psi(-\Theta_r^{-l} + 1) \Psi(\Theta_q^l + 1) \Psi(\Theta_q^{i+l} + 1) \}
\end{aligned}$$

принимает значение на множестве чисел $Z' = \{-4, -3, -2, -1, 0, 1, 2, 3, 4\}$. Поэтому, используя (28), выражение (27) можно представить

$$R_{W^n}(l) = \{ \pm \sum_{\substack{x_i, y_i \in GF(P^n) \\ x_i, y_i \neq 0 \pmod{P}}} \Psi(1 + q_1 x_i) \Psi(1 + q_2 y_i) \pm [3] \} \pm [4], \tag{29}$$

где запись [3] и [4] означает, что вместо [3] при анализе необходимо подставлять числа $(-3, -2, -1, 0, 1, 2, 3)$, а вместо [4] – числа $(-4, -3, -2, -1, 0, 1, 2, 3, 4)$.

Рассмотрим вывод аналитического выражения для ПФВК ПНРП. Используя выражение для расчета функции взаимной корреляции

$$R_{j,m}^v(l) = \sum_{i=1}^{L-k} W_i^v (W_{i+1}^j)^* + \sum_{i=L-k+1}^L W_i^v (W_{i-L+k}^m)^*,$$

получим ($j = m$)

$$R_{W^n}^B(l) = \sum_{i=0}^{L-1} \Psi(\Theta_{r_1}^i + 1) \Psi(\Theta_{r_2}^i + 1) \Psi(\Theta_{r_3}^{i+l}) \Psi(\Theta_{r_4}^{i+l} + 1). \quad (30)$$

Приведем вывод выражения для оценки выбросов ПФВК

$$R_{W^n}^B(l) = \sum_{i=0}^{L-1} \Psi(\Theta_{r_1}^i + 1) \Psi(\Theta_{r_2}^i + 1) \Psi(\Theta_{r_3}^{i+l} + 1) \Psi(\Theta_{r_4}^{i+l} + 1) \quad (30)$$

Далее, аналогично выражению (19)

$$R_{W_n}(l) = \sum_{i=0}^{P^n-1} \Psi(\Theta_{r_1}^i + 1) \cdot \Psi(\Theta_{r_2}^i + 1) \cdot \Psi(\Theta_{r_3}^{i+l} - 1) \cdot \Psi(\Theta_{r_4}^{i+l} - 1) \pm Z, \quad (31)$$

где Z представляет собой сумму слагаемых, входящих в (30), для которых $\Theta_{r_1}^i + 1 \equiv 0 \vee (\Theta_{r_2}^i + 1) \equiv 0 \vee (\Theta_{r_3}^{i+l} + 1) \equiv 0 \vee (\Theta_{r_4}^{i+l} + 1) \equiv 0$, что эквивалентно:

$$\begin{aligned} \Theta_{r_1}^i + 1 &\equiv 0 \vee \Theta_q^{i+l} + 1 \neq 0 \wedge \Theta_{r_2}^{i+l} + 1 \neq 0 \wedge \Theta_{r_3}^{i+l} + 1 \neq 0 \pmod{L}; & a) \\ \Theta_{r_1}^i + 1 &\neq 0 \vee \Theta_q^{i+l} + 1 \equiv 0 \wedge \Theta_{r_2}^{i+l} + 1 \neq 0 \wedge \Theta_{r_3}^{i+l} + 1 \neq 0 \pmod{L}; & б) \\ \Theta_{r_1}^i + 1 &\neq 0 \vee \Theta_q^{i+l} + 1 \neq 0 \wedge \Theta_{r_2}^{i+l} + 1 \equiv 0 \wedge \Theta_{r_3}^{i+l} + 1 \neq 0 \pmod{L}; & в) \\ \Theta_{r_1}^i + 1 &\neq 0 \vee \Theta_q^{i+l} + 1 \neq 0 \wedge \Theta_{r_2}^{i+l} + 1 \neq 0 \wedge \Theta_{r_3}^{i+l} + 1 \equiv 0 \pmod{L}; & г) \end{aligned}$$

поэтому:

$$\begin{aligned} Z = & \pm \{ \Psi(\Theta_{r_2}^i + 1) \Psi(\Theta_{r_3}^{i+l} + 1) \Psi(\Theta_{r_4}^{i+l} + 1) + \Psi(\Theta_{r_1}^i + 1) \Psi(\Theta_{r_3}^{i+l} + 1) \Psi(\Theta_{r_4}^{i+l} + 1) + \\ & + \Psi(\Theta_{r_1}^i + 1) \Psi(\Theta_{r_2}^i + 1) \Psi(\Theta_{r_3}^{i+l} + 1) + \Psi(\Theta_{r_1}^i + 1) \Psi(\Theta_{r_2}^i + 1) \Psi(\Theta_{r_4}^{i+l} + 1) \}, \end{aligned} \quad (32)$$

может принимать значения на множестве $Z' = \{-4, -3, -2, -1, 0, 1, 2, 3, 4\}$, следовательно (29) есть

$$R_{W_n}(l) = \sum_{i=0}^{P^n-1} \Psi(\Theta_{r_1}^i + 1) \cdot \Psi(\Theta_{r_2}^i + 1) \cdot \Psi(\Theta_{r_3}^{i+l} + 1) \cdot \Psi(\Theta_{r_4}^{i+l} + 1) \pm [4] = x \pm [4]. \quad (33)$$

Преобразуем выражение для x следующим образом:

$$\begin{aligned} x &= \Psi(\Theta_{r_3}^i) \Psi(\Theta_{r_4}^i) \sum_{i=0}^{P^n-1} \Psi(\Theta_{r_1}^i + 1) \Psi(\Theta_{r_2}^i + 1) \Psi(\Theta_{r_3}^i + \Theta_{r_3}^{-l}) \Psi(\Theta_{r_4}^i + \Theta_{r_4}^{-l}) = \\ &= \Psi(\Theta_{r_3}^i) \Psi(\Theta_{r_4}^i) \cdot Q. \end{aligned} \quad (34)$$

Далее, выражение для Q (обозначив $\Theta_{r_1}^i + 1 = a_i$ и $\Theta_{r_2}^i + 1 = b_i$), представим в виде:

$$Q = \sum_{\substack{a, b_i \in GF(P^n) \\ a, b_i \neq 1 \pmod{P}}} \Psi(a_i) \Psi(b_i) \Psi(\Theta_{r_3}^i + \Theta_{r_3}^{-l}) \Psi(\Theta_{r_4}^i + \Theta_{r_4}^{-l})$$

С учетом (24) – (26), а также того, что $\Theta_{r_3}^{-l}$ и $\Theta_{r_4}^{-l}$ могут принимать все значения из $GF(P^n)$, обозначив $c_i = \Theta_{r_3}^i + \Theta_{r_3}^{-l}$ и $d_i = \Theta_{r_4}^i + \Theta_{r_4}^{-l}$, причем, так как, во-первых,

$\Theta_{r_3}^i \neq 0(\text{mod } P)$ и $\Theta_{r_3}^{-i} \neq 1(\text{mod } P)$, $\Theta_{r_3}^i + \Theta_{r_3}^{-i} \neq 1(\text{mod } P)$, а во-вторых, при $\Theta_{r_4}^i \neq 0(\text{mod } P)$ и $\Theta_{r_4}^{-i} \neq 1(\text{mod } P)$, $\Theta_{r_4}^i + \Theta_{r_4}^{-i} \neq 1(\text{mod } P)$, (34), можно представить в виде:

$$\begin{aligned} R_{W''}^B(I) &= \sum_{\substack{a_i, b_i, c_i, d_i \in GF(P^n) \\ a_i, b_i, c_i, d_i \neq 0(\text{mod } P)}} \Psi(a_i) \Psi(b_i) \Psi(c_i) \Psi(d_i) = \\ &= \sum_{\substack{a_i, b_i, c_i, d_i \in GF(P^n) \\ a_i, b_i, c_i, d_i \neq 0(\text{mod } P)}} \Psi(a_i) \Psi(b_i) \Psi(c_i) \Psi(d_i) \pm [4] \pm [15] = \sum_{\substack{a_i, b_i, c_i, d_i \in GF(P^n) \\ a_i, b_i, c_i, d_i \neq 0(\text{mod } P)}} \Psi(a_i) \Psi(b_i) \Psi(c_i) \Psi(d_i) \pm [19]. \end{aligned} \quad (35)$$

Анализ (35) показывает, что элементы полей c_i, d_i представляют собой автоморфизмы полей $\Theta_{r_3}^i$ и $\Theta_{r_4}^i$ при $i = \overline{0, P^n - 2}$. Сумма в нем берется по всевозможным произведениям характеров над $a_i, b_i, c_i, d_i \in GF(P^n)$ и дает оценку для максимально достигаемого выброса $R_{W''}^B(I)_{\max}$. С учетом того, что элементы a_i, b_i, c_i и d_i строятся по различным первообразным: и пары условий

$$\begin{aligned} \Psi(a_i) &= \Psi(1) \wedge \Psi(b_i) = \Psi(1), \\ \Psi(c_i) &= \Psi(1) \wedge \Psi(d_i) = \Psi(1) \end{aligned}$$

не истинны, (35) имеет вид

$$\begin{aligned} R_{W''}^B(I) &= \sum_{\substack{a_i, b_i, c_i, d_i \in GF(P^n) \\ a_i, b_i, c_i, d_i \neq 0(\text{mod } P)}} \Psi(a_i) \Psi(b_i) \Psi(c_i) \Psi(d_i) \pm [8] \pm [4] = \\ &= \sum_{\substack{a_i, b_i, c_i, d_i \in GF(P^n) \\ a_i, b_i, c_i, d_i \neq 0(\text{mod } P)}} \Psi(a_i) \Psi(b_i) \Psi(c_i) \Psi(d_i) \pm [4] \pm [12]. \end{aligned} \quad (36)$$

Важной задачей является несбалансированность ПНРП по число символов (+1) и (-1).

Если $\Theta_1, \Theta_2, \dots, \Theta_k$ — первообразные элементы поля $GF(P^n)$, то несбалансированность в числе символов есть

$$R_{W''}(0) = \sum_{i=0}^{L-1} \prod_{j=1}^k \Psi(\Theta_j^i + 1)$$

При $k = 2$ аналогично (32)

$$R_{W''}(0) = \sum_{i=0}^{P^n-2} \Psi(\Theta_{r_1}^i + 1) \Psi(\Theta_{r_2}^i + 1) = \sum_{i=0}^{P^n-2} \Psi(\Theta_{r_1}^i + 1) \Psi(\Theta_{r_2}^i + 1) \pm Z,$$

где Z представляет собой сумму слагаемых, для которых

$$\Theta_{r_1}^i + 1 = 0 \vee \Theta_{r_2}^i + 1 \equiv 0(\text{mod } P), \quad (37)$$

то есть

$$Z = \pm \Psi(\Theta_{r_1}^i + 1) + \Psi(\Theta_{r_2}^i + 1) \rightarrow \pm 2 \quad (38)$$

Далее обозначив $a_i = \Theta_{r_1}^i$ и $b_i = \Theta_{r_2}^i$, а затем $c_i = a_i + 1$ и $d_i = b_i + 1$ аналогично (21) — (25) имеем

$$\begin{aligned}
x = \sum_{\substack{a_i, b_i \in GF(P^n) \\ a_i, b_i \neq 0 \pmod{P}}} \Psi(a_i + 1) \Psi(b_i + 1) &= \sum_{\substack{c_i, d_i \in GF(P^n) \\ c_i, d_i \neq 1 \pmod{P}}} \Psi(c_i) \Psi(d_i) = \\
\sum_{\substack{c_i, d_i \in GF(P^n) \\ c_i, d_i \neq 0 \pmod{P}}} \Psi(c_i) \Psi(d_i) - \Psi(c_i) - \Psi(d_i) &= \sum_{\substack{c_i, d_i \in GF(P^n) \\ c_i, d_i \neq 0 \pmod{P}}} \Psi(c_i) \Psi(d_i) \pm [2]
\end{aligned} \quad (39)$$

С учетом (39)

$$R_{W''}^B(0) = \sum_{\substack{c_i, d_i \in GF(P^n) \\ c_i, d_i \neq 0 \pmod{P}}} \Psi(c_i) \Psi(d_i) \pm [4]. \quad (40)$$

Заметим, что для случая $k = 4$, $R_{W''}(0)$ можно оценить, используя соотношения (36):

$$R_{W''}^B(0) = \sum_{\substack{a_i, b_i, c_i, d_i \in GF(P^n) \\ a_i, b_i, c_i, d_i \neq 0 \pmod{P}}} \Psi(a_i) \Psi(b_i) \Psi(c_i) \Psi(d_i) \pm [12]. \quad (41)$$

Анализ (41) показывает, что несбалансированность, а следовательно, и шумы неортогональности с увеличением k увеличиваются и уже при $k = 4$ достигают значительной величины, даже без учета результатов сумм в (40) и (41).

Особенности вычисления выражений (29), (36), (41) и оценки их значений рассмотрим на примере выражения (41).

Воспользовавшись свойством функции характеров, имеем

$$R_{W''}^B(0) = \sum_{\substack{a_i, b_i, c_i, d_i \in GF(P^n) \\ a_i, b_i, c_i, d_i \neq 0 \pmod{P}}} \Psi(a_i, b_i, c_i, d_i) \pm 12. \quad (42)$$

Для случая двухзначного характера, используя (15) имеем

$$R_{W''}^B(0) = \sum_{u_i^* \in GF(P^n)} \exp(-j\pi u_i^*) \pm 12. \quad (43)$$

Непосредственный анализ (43) показывает, что оценка максимальных боковых лепестков ПФАК, ПФВК и несбалансированности (тоже максимальной) в числе символов (1) и (-1) может быть сведена к изучению несбалансированности по четности и нечетности индексов производного поля, элементами которого являются числа (полиномы) вида

$$x_i = a_i \cdot b_i \cdot c_i \cdot d_i \pmod{f(x), P}.$$

Сопоставительное рассмотрение (43) показывает, что для анализа НРП (ПНРП) по критерию минимума максимальных выбросов $R_W^B(l)(R_{W''}^B(l))$ с точки зрения вычислительной сложности, предпочтительнее использовать алгоритм (42), а при вычислении основных статистических характеристик алгоритм (43).

Список литературы: 1. Виноградов И.М. Основы теории чисел. – М. : Наука, 1965. 2. Свердлик М.Б. Оптимальные дискретные сигналы. – М. : Сов. радио, 1975. – 200 с. 3. Холл М. Комбинаторика. – М. : Мир, 1970. – 421 с. 4. Альберт А. А. Константные поля // Киберн. сб. ВМП. 3. – М. : Мир, 1966. – 242 с.

Харьковский национальный
университет радиоэлектроники

Поступила в редколлегию 25.08.2011

ВСТРАИВАНИЕ ДАННЫХ В КОНТЕЙНЕРЫ-ИЗОБРАЖЕНИЯ С ИСПОЛЬЗОВАНИЕМ СЛОЖНЫХ ДИСКРЕТНЫХ СИГНАЛОВ

Введение

Одним из перспективных направлений в развитии методов стеганографической защиты информации является использование технологии прямого расширения спектра для встраивания информационных данных в контейнеры-изображения [1 – 4]. Реализация таких стеганографических систем предполагает использование больших ансамблей дискретных сигналов с улучшенными корреляционными и ансамблевыми свойствами [2 – 4]. В то же время, как показали исследования [3, 4], число ошибок в извлекаемых данных в стеганографических системах с прямым расширением спектра неприемлемо высоко, а вероятность правильного извлечения встроенных данных непосредственно зависит от статистических свойств используемого контейнера-изображения. Другими словами, применение технологии прямого расширения спектра в стеганографических целях выдвигает дополнительные требования к используемым дискретным сигналам: их коррелированность с отдельными фрагментами контейнера-изображения должна быть минимизирована.

В данной работе проводятся исследования эффективности стеганографических методов встраивания информации в неподвижные контейнеры-изображения с использованием технологии прямого расширения спектра, исследуются зависимости величины вносимых искажений и вероятности возникающих ошибок при извлечении информационных данных от пропускной способности стеганоканала. Предлагается использование адаптивно формируемых ансамблей слабокоррелированных (квазиортогональных) дискретных сигналов для встраивания информационных данных. Показано, что за счет минимизации коэффициента корреляции формируемых дискретных сигналов и используемых контейнеров удастся существенно снизить вероятность ошибочного извлечения встроенных данных.

Прямое расширение спектра в стеганографии

Технология прямого расширения спектра традиционно используется для построения широкополосных помехозащищенных систем скрытной радиосвязи, реализации множественного доступа с кодовым разделением каналов (CDMA – Code Division Multiple Access), обеспечения высокой имитостойкости на уровне применяемых ансамблей дискретных сигналов [5 – 7]. В стеганографических целях прямое расширение спектра частот используется для скрытного встраивания информационных данных в цифровые контейнеры, например неподвижные изображения [1 – 4]. При этом стеганографическая система наследует все преимущества широкополосных систем связи: устойчивость к несанкционированному извлечению встроенных сообщений (аналог скрытности в системе связи), устойчивость к разрушению или модификации встроенных сообщений (аналог помехозащищенности), устойчивость к навязыванию ложных сообщений (аналог имитостойкости в системе связи) [3, 4].

Введем следующие обозначения. Пусть $\Phi = \{\Phi_0, \Phi_1, \dots, \Phi_{M-1}\}$ будет множеством (ансамблем) из $M = |\Phi|$ дискретных сигналов $\Phi_i = (\varphi_{i0}, \varphi_{i1}, \dots, \varphi_{in-1})$ длины n . Каждый дискретный сигнал представляет собой двоичную псевдослучайную последовательность (ПСП), т.е. его элементы принимают одно из значений: $\varphi_{iz} = \begin{cases} +1 \\ -1 \end{cases}, z = 0, \dots, n-1$.

Важной характеристикой ансамбля Φ является коррелированность (похожесть) его элементов, для оценки которой используют коэффициент корреляции [5 – 7]:

$$\rho(\Phi_i, \Phi_j) = \frac{1}{n} \sum_{z=0}^{n-1} \Phi_{iz} \Phi_{jz} \quad (1)$$

Величина $\rho(\Phi_i, \Phi_j)$ характеризует статистическую взаимосвязь ПСП из ансамбля Φ . Для ортогональных сигналов $\rho(\Phi_i, \Phi_j) = 0$, для квазиортогональных $\rho(\Phi_i, \Phi_j) \approx 0$.

Основной задачей теории дискретных сигналов является разработка вычислительно эффективных методов синтеза больших ансамблей слабокоррелированных дискретных сигналов, т.е. при заданных ограничениях на максимальное значение $\rho(\Phi_i, \Phi_j)$ требуется максимизировать мощность ансамбля $M = |\Phi|$ (либо при фиксированном $M = |\Phi|$ минимизировать максимальное значение $\rho(\Phi_i, \Phi_j)$).

Для передачи данных в широкополосной системе связи с прямым расширением спектра информационный сигнал $x(t) = \begin{cases} +1 \\ -1 \end{cases}$ модулируется посредством его умножения на расширяющий кодовый сигнал $g(t) = \Phi_i \in \Phi$:

$$y(t) = x(t)g(t) \quad (2)$$

Предположим, что временная длительность немодулированного сигнала $x(t)$ равна T , а его частота соответственно $F(x(t)) = \frac{1}{T}$. Передача модулированного сигнала $y(t)$ при той же временной длительности T приведет к расширению частотного спектра передаваемого сигнала, пропорционально числу элементов псевдослучайной последовательности, т.е. пропорционально длине n : $F(y(t)) = n \frac{1}{T} = nF(x(t))$. Поскольку кодовый сигнал по своим статистическим свойствам подобен шуму, то полученный расширенный (широкополосный) сигнал $y(t)$ слабо отличим от шумов в канале связи, что и позволяет осуществить скрытую передачу. Таким образом, передаваемые сообщения приобретают вид шумоподобных последовательностей, а за счет большой мощности ансамбля Φ и прямого расширения частотного спектра обеспечивается высокая имитостойкость, помехозащищенность и скрытность цифровых каналов связи [5 – 7].

При приеме в демодуляторе полученный сигнал $y'(t) = y(t) + e(t)$ как смесь переданной последовательности $y(t)$ и произошедших в канале связи ошибок $e(t)$ умножается на синхронизированную копию расширяющего сигнала $g(t)$. Другими словами, на приемной стороне осуществляется вычисление коэффициента корреляции (1), значение которого определяет правило принятия решения:

$$\rho(y'(t), g(t)) = \frac{1}{n} \sum_{z=0}^{n-1} x(t) \Phi_{iz} \Phi_{iz} + \frac{1}{n} \sum_{z=0}^{n-1} e(t) \Phi_{iz}$$

Учитывая псевдослучайность Φ_i , используемых в качестве $g(t)$, вторым слагаемым в правой части равенства можно пренебречь (количество «+1» примерно равно количеству «-1»), т.е.

$$\rho(y'(t), g(t)) \approx \rho(y(t), g(t)) = x(t) \frac{1}{n} \sum_{z=0}^{n-1} (\Phi_{iz})^2 = x(t), \quad (3)$$

т.е. значение информационного сигнала на приемной стороне определяется из выражения

$$x(t) = \begin{cases} +1, \text{ при } \rho(y'(t), g(t)) \approx +1; \\ -1, \text{ при } \rho(y'(t), g(t)) \approx -1; \end{cases} \quad (4)$$

где знак « $\approx$ » предполагает наличие ошибок $e(t)$, вызванных естественными или преднамеренными помехами в канале связи.

Использование прямого расширения спектра передаваемого сигнала обеспечивает одновременную передачу многих других информационных сигналов в той же полосе частот. Это следует из слабой взаимной коррелированности ПСП из применяемых ансамблей дискретных сигналов. Действительно, если на приемной стороне принята аддитивная смесь $\sum_l y_l(t)$

нескольких модулированных сигналов, тогда вычисление коэффициента корреляции даст следующее:

$$\rho\left(\sum_l y_l(t), g(t)\right) = \frac{1}{n} \sum_l \sum_{z=0}^{n-1} x_l(t) \Phi_{l_z} \Phi_{i_z}. \quad (5)$$

Но все последовательности из множества Φ имеют низкое значение взаимной корреляции, т.е. при $l \neq i$ имеем $\rho(\Phi_l, \Phi_i) \approx 0$ (для ортогональных сигналов имеем равенство $\rho(\Phi_l, \Phi_i) = 0$). Следовательно, всеми слагаемыми при $l \neq i$ в правой части равенства (5) можно пренебречь. Отсюда, при наличии в аддитивной смеси $\sum_l y_l(t)$ дискретного сигнала

$\Phi_{l=i}$, имеем выражение (3) и соответствующее правило принятия решения (4).

Рассмотренный подход к организации цифровых помехозащищенных каналов связи нашел применение и при построении стеганографических методов защиты информации. Так, в работе [2] расширение спектра прямой последовательностью использовано для создания стеганографического метода встраивания данных в неподвижные изображения.

Целью стеганографического преобразования информации является встраивание каждого отдельного блока сообщения m_i , $i = 0, \dots, N-1$ в соответствующий блок контейнера-изображения. Встраивание информационного сообщения осуществляется следующим образом. Каждый блок информационного сообщения сопоставляется с отдельным блоком контейнера-изображения. Каждый информационный бит блока m_{ij} , $j = 0, \dots, n-1$ представляется

в виде информационного сигнала $m_{ij}(t) = \begin{cases} +1, m_{ij} = 1; \\ -1, m_{ij} = 0; \end{cases}$ и по аналогии с (2) модулируется расширяющим кодовым сигналом, т.е. ПСП $\Phi_j \in \Phi$.

В результате, для каждого информационного блока m_i формируется модулированный информационный сигнал

$$E_i(t) = \sum_{j=0}^{n-1} \sum_{z=0}^{n-1} m_{ij}(t) \Phi_{j_z}.$$

Полученный информационный сигнал $E_i(t)$ попиксельно суммируется с подблоком контейнера C_i : $S_i = C_i + E_i \cdot G$, где $G > 0$ – коэффициент усиления расширяющего сигнала, задающий «энергию» встраиваемых бит m_{ij} , $j = 0, \dots, n-1$ информационной последовательно-

сти. Стеганограмма (заполненный контейнер) S формируется посредством объединения массивов данных S_i , $i = 0, \dots, N-1$.

При извлечении информационных данных первичный контейнер C не требуется. Операция декодирования заключается в восстановлении скрытого сообщения путем проецирования каждого блока S_i полученной стеганограммы S на все $\Phi_j \in \Phi$, $i = 0, \dots, N-1$. Для этого каждый блок S_i представляется в форме вектора $S_i = (S_{i_0}, S_{i_1}, \dots, S_{i_{n-1}})$, $i = 0, \dots, N-1$

Чтобы извлечь j -й бит сообщения из i -го блока стеганоизображения, необходимо вычислить коэффициент корреляции между Φ_j и принятым блоком S_i (представленного в виде вектора):

$$\rho(S_i, \Phi_j) = \frac{1}{n} \sum_{z=0}^{n-1} S_{i_z} \Phi_{j_z} = G \cdot \frac{1}{n} \sum_{z=0}^{n-1} E_{i_z} \Phi_{j_z} + \frac{1}{n} \sum_{z=0}^{n-1} C_{i_z} \Phi_{j_z}, \quad (6)$$

где под C_i понимается одномерный массив, т.е. соответствующий блок контейнера, представленный в форме вектора.

Предположим, что массив C_i имеет случайную статистическую структуру, т.е. положим, что второе слагаемое в правой части выражения (6) близко к нулю и им можно пренебречь. Тогда имеем:

$$\rho(S_i, \Phi_j) \approx G \cdot E_i \cdot \Phi_j = G \cdot \sum_{l=0}^{n-1} \sum_{z=0}^{n-1} m_{i_x}(t) \cdot \Phi_{l_z} \Phi_{j_z}. \quad (7)$$

По аналогии с (5) отметим, что все последовательности из множества Φ слабокоррелированы, т.е. при $l \neq j$ имеем $\rho(\Phi_l, \Phi_j) \approx 0$. Следовательно, всеми слагаемыми в правой части равенства (7) при $l \neq j$ можно пренебречь. Отсюда имеем:

$$\rho(S_i, \Phi_j) \approx G \cdot m_{i_j}(t) \cdot \frac{1}{n} \sum_{z=0}^{n-1} (\Phi_{j_z})^2 = G \cdot m_{i_j}(t).$$

Тогда, по аналогии с (5) значения $m_{i_j}(t)$ могут быть легко восстановлены с помощью выражения:

$$m_{i_j}(t) = \begin{cases} +1, \text{ при } \rho(S_i, \Phi_j) \approx G \\ -1, \text{ при } \rho(S_i, \Phi_j) \approx -G; \end{cases}$$

где знак « $\approx$ » предполагает наличие незначительной статистической взаимосвязи отдельных элементов множества Φ и C_i .

Таким образом, процесс встраивания информационных сообщений для скрытной передачи очень схож с технологией расширения спектра дискретных сигналов в системах связи. Поэлементное сложение модулированного сообщения $E(t)$ с контейнером-изображением $C(t)$ следует интерпретировать как наложение ошибок $e(t)$ на полезный сигнал $y(t)$ в канале связи. Задача извлечения сообщения $m(t)$ из $S(t)$ на приемной стороне стеганосистемы эквивалентна задаче детектирования $x(t)$ из смеси полезного сигнала и помехи $y'(t) = y(t) + e(t)$ в широкополосной системе связи. Другими словами, рассмотренная стеганосистема фактически является некоторой интерпретацией широкополосных систем связи:

устойчивость к несанкционированному извлечению встроенных сообщений соответствует скрытности в системе связи, устойчивость к разрушению или модификации встроенных сообщений – помехозащищенности, устойчивость к навязыванию ложных сообщений – имитостойкости в системе связи.

Таким образом, использование развитого математического аппарата теории дискретных сигналов и технологии прямого расширения спектра в стеганографических целях позволяет осуществить встраивание информационных данных в неподвижные изображения для скрытной передачи и реализовать, таким образом, стеганографическую защиту информации.

Исследование эффективности стеганосистем с прямым расширением спектра

Для оценки эффективности стеганосистем в [3, 4] введены следующие показатели:

- пропускная способность Q ограничиваемого стеганоканала – отношение объема V встраиваемой в контейнер информации к общему объему D контейнера $Q = V / D$;
- величина вносимых искажений I как процентное отношение среднеарифметического всех абсолютных значений данных контейнера к максимально возможному значению;
- вероятность ошибочного извлечения $P_{ош}$ информационных данных сообщения.

Для проведения экспериментальных исследований эффективности встраивания сообщений в неподвижные изображения с использованием прямого расширения спектра разработана программная реализация, с помощью которой получены следующие эмпирические оценки: зависимости $I(V)$ и $P_{ош}^*(V)$ при фиксированном $D = 256$; зависимости $I(G)$ и $P_{ош}^*(G)$, где $P_{ош}^* \approx P_{ош}$ – частота ошибок извлечения, G – коэффициент усиления из (6).

Исследования проводились при встраивании информационных данных в растровые данные изображения (цветовая модель R,G,B) с 8-битным кодированием каждого цвета. Эмпирические зависимости для случая использования ансамблей ортогональных сигналов Уолша–Адамара приведены на рис. 1 – 4.

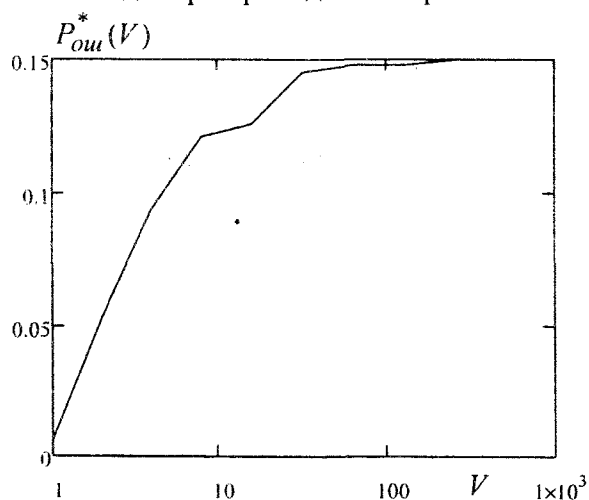


Рис. 1. Зависимость $P_{ош}^*(V)$, $D = 256$, $G = 1$

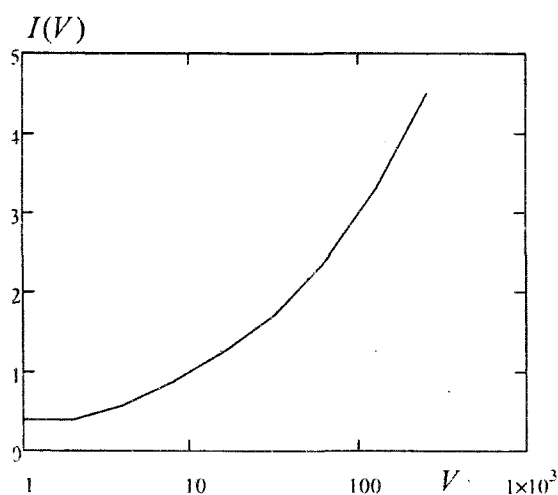


Рис. 2. Зависимость $I(V)$, $D = 256$, $G = 1$

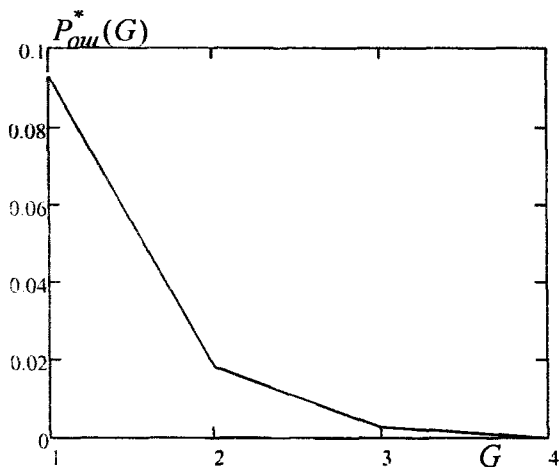


Рис. 3. Зависимость $P_{ош}^*(G)$, $D = 256$, $V = 4$

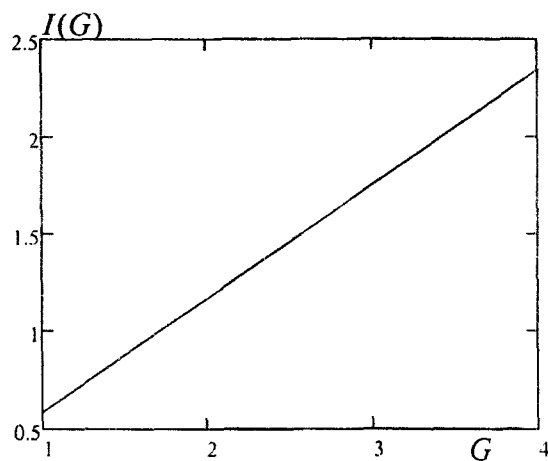


Рис. 4. Зависимость $I(G)$, $D = 256$, $V = 4$

Приведенные графики показывают, что повышение объема встраиваемых данных приводит к увеличению как вероятности ошибочного извлечения, так и к повышению доли вносимых искажений в контейнер-изображение. Приведенные зависимости также свидетельствуют, что увеличение коэффициента усиления G приводит к резкому снижению вероятности ошибочного извлечения и одновременному повышению величины вносимых искажений.

Следует отметить, что рассчитанное значение I является усредненной величиной, характеризующей долю внесенных искажений в среднем, по всем пикселям контейнера-изображения. Отдельные пиксели или группа пикселей могут быть значительно искажены, доля вносимых искажений для этих фрагментов изображения может существенно превышать рассчитанное усредненное значение V . Для примера на рис. 5, 6 приведены: контейнер S , заполненный с показателями: $V = 128$, $G = 1$ (рис. 5); исходный контейнер (рис. 6).



Рис. 5. Пример заполненного контейнера



Рис. 6. Пример пустого контейнера

Как следует из приведенных выше графиков, встраивание с такими параметрами дает усредненное значение доли вносимых искажений в пределах порога зрительной чувствительности человека. Однако, как видно из приведенных изображений (рис. 5, 6), для некоторых фрагментов искажения очень существенны. Таким образом, применение ортогональных дискретных сигналов оправдано только для стеганографических систем с малым объемом встраиваемых данных. Для повышения пропускной способности стеганоканалов при прочих равных условиях целесообразно использовать квазиортогональные дискретные сигналы.

На рис. 7, 8 приведены результаты исследования эффективности стеганосистем с использованием квазиортогональных дискретных сигналов, которые сформированы:

- 1) без адаптации к статистическим свойствам контейнера-изображения;
- 2) с адаптивным формированием последовательностей.

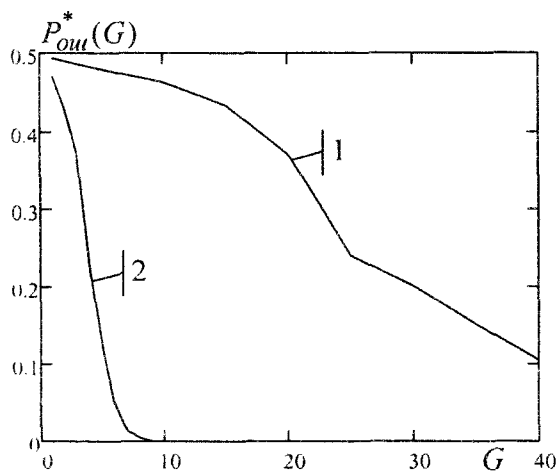


Рис. 7. Зависимость $P_{om}^*(G)$, $D = 256$, $V = 10$

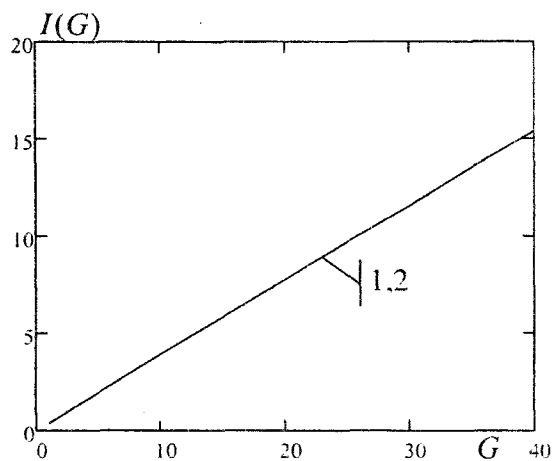


Рис. 8. Зависимость $I(G)$, $D = 256$, $V = 10$

Полученные эмпирические зависимости показывают, что повышение коэффициента усиления приводит к резкому снижению вероятности ошибочного извлечения информационных бит сообщения (см. рис.7). Однако это также ведет к увеличению вносимых искажений в контейнер-изображение (рис. 8). В то же время, как показывают проведенные исследования, по сравнению с использованием ортогональных дискретных сигналов применение квазиортогональных последовательностей приводит к меньшему искажению контейнера-изображения. Так, например, при $V = 4$ с использованием ортогональных дискретных сигналов при коэффициенте усиления $G = 4$ величина вносимых искажений составляет более 2.33 % (см. рис. 4). При большем числе вносимых бит данных ($V = 10$), а следовательно, и при большей пропускной способности стеганографического канала передачи данных применение квазиортогональных дискретных сигналов даже с большим значением коэффициента усиления ($G = 5$) приводит к меньшим искажениям контейнера, величина вносимых искажений не превосходит 2 % (см. рис. 8). Однако, как следует из представленных на рис. 7 зависимостей, использование квазиортогональных дискретных сигналов без адаптации к статистическим свойствам контейнера-изображения приводит к существенному повышению вероятности ошибочного извлечения бит сообщения (за счет сильной коррелированности ПСП с отдельными фрагментами контейнера-изображения). Так, например, для значений $G < 10$ величина ошибочно извлекаемых бит данных составляет почти 50 % (см. зависимость 1, рис. 7). Избавиться от этого негативного фактора можно за счет адаптивного формирования квазиортогональных дискретных сигналов с учетом особенностей используемого контейнера-изображения.

В качестве примера на рис. 7, 8 цифрой 2 отмечена эмпирическая зависимость, полученная для случая использования адаптивно формируемых ансамблей квазиортогональных дискретных сигналов. Очевидно, что без увеличения величины вносимых искажений удастся существенно снизить вероятность ошибочного извлечения информационных бит сообщений. Уже для значений $G = 7..10$ удастся реализовать практически безошибочное извлечение информационных сообщений.

Таким образом, как следует из полученных результатов, применение адаптивно формируемых квазиортогональных дискретных сигналов позволяет существенно повысить пропускную способность организовываемых стеганографических каналов при сравнимых искажениях, вносимых в контейнер-изображение.

Выводы

Применение технологии прямого расширения спектра для встраивания данных в контейнеры-изображения позволяет строить эффективные стеганографические системы для

скрытной передачи информационных сообщений. Наиболее целесообразным является использование больших ансамблей квазиортогональных дискретных сигналов с адаптивным формированием (выбором) ПСП по критерию минимизации коэффициента корреляции с контейнером-изображением. Это позволяет существенно повысить пропускную способность организуемого стеганоканала и снизить вероятность ошибочного извлечения встраиваемых данных.

Список литературы: 1. *Конахович Г. Ф., Пузыренко А. Ю.* Компьютерная стеганография. Теория и практика. – К. : МК-Пресс, 2006. – 288 с. 2. *J. Smith, B. Comiskey.* Modulation and Information hiding in Image // Information hiding: First Int. Workshop "InfoHiding'96", Springer as Lecture Notes in Computing Science, vol 1174. – 1996. – Р. 207-227. 3. *Кузнецов А. А.* Встраивание информационных данных в неподвижные изображения с использованием прямого расширения спектра / А. А. Кузнецов, А. М. Ботнов, П. А. Лаптий // Прикладная радиоэлектроника. – Т.9, N 3. – С.470-478. 4. *Kuznetsov A., Serhiienko R., Kovtun V., Botnov A.* Use of Complex Discrete Signals for Steganographic Information Security // Statistical Methods of Signal and Data Processing (SMSDP-2010): Proceedings. – Kiev : National Aviation University "NAU-Druk" Publishing House, 2010. – Р. 143 – 146. 5. *Цифровые методы в космической связи* / Под ред. С. Голомба. – М. : Связь, 1969. – 272 с. 6. *Скляр Б.* Цифровая связь. Теоретические основы и практическое применение. – М. : Вильямс, 2003. – 1104 с. 7. *Горбенко И.Д., Стасев Ю.В.* Анализ производных ортогональных систем сигналов // Радиотехника. – 1989. – № 9. – С. 16 – 18.

*Харьковский национальный
университет радиоэлектроники*

Поступила в редколлегию 10.07.2011

ДИСКРЕТНЫЕ СИГНАЛЫ С МНОГОУРОВНЕВОЙ ФУНКЦИЕЙ КОРРЕЛЯЦИИ

Введение

Эффективное функционирование современных систем управления сопряжено с обеспечением требуемых показателей помехозащищенности, имитостойкости и скрытности радиоканалов связи, внедрением новейших информационных технологий кодирования и цифровой обработки сигналов [1, 2]. Актуальной задачей в этом смысле является разработка методов синтеза больших ансамблей слабокоррелированных дискретных сигналов с улучшенными ансамблевыми, корреляционными и структурными свойствами [1 – 4].

Линейные групповые коды

Перспективным направлением в развитии методов формирования дискретных сигналов является подход, который основан на использовании алгебраических и структурных свойств групповых кодов, что позволяет синтезировать новые классы дискретных сигналов с многоуровневой функцией корреляции. [3, 4].

Зафиксируем конечное поле $GF(q)$. Рассмотрим векторное пространство $GF^n(q)$ как множество n -последовательностей элементов из $GF(q)$ с покомпонентным сложением и умножением на скаляр. *Линейный (n, k, d) код V* есть подпространство $GF^k(q)$ в пространстве $GF^n(q)$, т.е. непустое множество n -последовательностей (кодированных слов) над $GF(q)$. k – размерность линейного подпространства, d – минимальное кодовое расстояние (минимальный вес ненулевого кодового слова).

Циклический код является частным случаем подпространства, обладающего дополнительным свойством цикличности. Каждый вектор из $GF^n(q)$ можно представить многочленом от формальной переменной x степени не выше $n - 1$. Компоненты вектора отождествляются с коэффициентами многочлена. Множество многочленов обладает структурой векторного пространства, идентичной структуре пространства $GF^n(q)$, а также структурой кольца многочленов $GF(q)[x]/(x^n - 1)$. В кольце многочленов определено умножение над многочленами: $p_1(x) \cdot p_2(x) = R_{x^n - 1}[p_1(x) \cdot p_2(x)]$, где $R_b[a]$ – остаток от деления многочлена a на многочлен b . Циклический сдвиг на $\tau \in \{0, \dots, n - 1\}$ элементов в терминах алгебры многочленов запишется в виде

$$x^\tau \cdot p(x) = R_{x^n - 1}[x^\tau \cdot p(x)]. \quad (1)$$

Если кодовые слова (n, k, d) кода над $GF(q)$ задаются в виде многочленов, то код V является подмножеством кольца $GF(q)[x]/(x^n - 1)$. Код V является циклическим, если вместе с кодовым словом $C(x)$ он содержит также многочлен $x \cdot C(x)$.

Единственный приведенный ненулевой многочлен $g(x)$ наименьшей степени $r = n - k$ однозначно задает (n, k, d) циклический код над $GF(q)$ и обозначается порождающим многочленом, причем $g(x) = \prod_i (x - \beta^i)$, где $\beta^i \in GF(q^m)$. Он связан с проверочным многочленом $h(x)$ соотношением $g(x) \cdot h(x) = x^n - 1$, или $R_{x^n - 1}[g(x) \cdot h(x)] = 0$.

Рассмотрим структуру конечного поля $GF(q^m)$ как множество многочленов степени $\leq m$ с коэффициентами из $GF(q)$, т.е. структуру кольца многочленов $GF(q)[x]/(x^m - 1)$. В соответствии с общими положениями теории полей Галуа кольцо многочленов $GF(q)[x]/(x^m - 1)$ с операциями по модулю неприводимого многочлена является расширенным полем Галуа $GF(q^m)$. Такое поле состоит из совокупности циклотомических классов $\alpha^{i(q^s)}$, $s = 0, 1, \dots, m_i - 1$, где m_i – наименьшее положительное целое, такое, при котором выполняется равенство [5]: $i q^{m_i} = (i) \bmod (q^m - 1)$.

Каждый циклотомический класс элементов задает (через корни) минимальный многочлен $f_i(x)$. Произведение всех минимальных многочленов $f_i(x)$ конечного поля $GF(q^m)$ задает многочлен $(x^{q^m - 1} - 1)$, т.е. имеем:

$$(x^{q^m - 1} - 1) = \prod_{\forall i \in \{0, \dots, q^m - 1\}} f_i(x) = \prod_{\forall i \in \{0, \dots, q^m - 1\}} (x - \alpha^i),$$

где α – примитивный элемент поля $GF(q^m)$, откуда следует

$$g(x) = H.O.K. \left(\prod_j f_j(x) \right) = H.O.K. \left(\prod_j \prod_{s=0}^{m_j} (x - \alpha^{j(q^s)}) \right),$$

$$h(x) = \frac{x^n - 1}{g(x)} = H.O.K. \left(\prod_{i \neq j} f_i(x) \right) = H.O.K. \left(\prod_{i \neq j} \prod_{s=0}^{m_i} (x - \alpha^{i(q^s)}) \right).$$

Рассмотрим структуру группового (n, k, d) кода V над $GF(q)$ с точки зрения циклических свойств образующих его последовательностей. Будем использовать при этом понятие *циклической орбиты* V_ξ – множество последовательностей с элементами из $GF(q)$, эквивалентных друг другу относительно операции циклического сдвига, т.е. множество таких

$$C_i = (c_0^i, c_1^i, \dots, c_{n-1}^i), c_v^i \in GF(q) \text{ и } C_j = (c_0^j, c_1^j, \dots, c_{n-1}^j), c_v^j \in GF(q),$$

что выполняется равенство

$$(c_0^i, c_1^i, \dots, c_{n-1}^i) = (c_{(\tau) \bmod(n)}^j, c_{(\tau+1) \bmod(n)}^j, \dots, c_{(\tau+n-1) \bmod(n)}^j) \quad (2)$$

для какого-либо $\tau \in \{0, \dots, n-1\}$.

Выражение (2) с использованием (1) выразим в терминах алгебры многочленов:

$$p_i(x) = x^\tau \cdot p_j(x) = R_{x^n - 1} [x^\tau \cdot p_j(x)],$$

где

$$p_i(x) = c_0^i + c_1^i x + \dots + c_{n-1}^i x^{n-1}, p_j(x) = c_0^j + c_1^j x + \dots + c_{n-1}^j x^{n-1}.$$

Рассмотрим множество W всех n -последовательностей с элементами из $GF(q)$, которые образуют так называемый «полный код». Структура множества эквивалентна векторному пространству $GF^n(q)$ с покомпонентным сложением и умножением на скаляр. Разобьем все множество W на подмножества орбит $V_0, V_1, \dots, V_L$, каждая из которых содержит совокупность последовательностей, эквивалентных друг другу относительно операции циклического сдвига (2).

Циклический код по определению содержит все циклические сдвиги собственных последовательностей (кодовых слов). В терминах орбит это означает, что циклический код яв-

ляется объединением конечного числа орбит: $V = V_0 \cup V_1 \cup \dots \cup V_M$, т.е. объединением конечного числа подмножеств, элементы которых удовлетворяют свойству (2).

Веса w последовательностей орбит (число ненулевых элементов последовательностей C_i) определяются весовым спектром кода V . Нулевая орбита V_0 содержит одну (нулевую) последовательность. Каждая ненулевая орбита содержит не более n последовательностей, эквивалентных друг другу относительно операции циклического сдвига (2). Последовательности из разных орбит не могут быть циклически сдвинутыми копиями друг друга.

Таким образом, групповой код однозначно задается лидерами (представителями) составляющих его циклических орбит. Это свойство положим в основу синтеза ансамбля дискретных сигналов: на основе сечения ненулевых циклических орбит (выбора лидера, представителя каждой орбиты) сформируем множество дискретных последовательностей с дистанционными свойствами исходного группового (n, k, d) кода V и не эквивалентных друг другу относительно циклического сдвига (2), т.е. не принадлежащих одной орбите.

Схема сечения ненулевых циклических орбит группового кода представлена на рис. 1.

На рис. 1 показано разложение векторного пространства $GF^n(q)$ на множества непересекающихся орбит V_ξ , $\xi = 0, \dots, L$, представление группового кода V через объединение конечного числа орбит и схема выбора лидеров орбит – по одному произвольному представителю из каждого циклического подмножества V_ξ , $\xi = 0, \dots, M$ (для удобства обозначения кодовые слова $C_{v,u} = (c_0^{v,u}, c_1^{v,u}, \dots, c_{n-1}^{v,u})$ обозначены двумя индексами: v – номер орбиты V_v кода V , $v = 1, \dots, M$; u – номер кодового слова в орбите, $u = 1, \dots, z_v$, где z_v – число кодовых слов в орбите V_v , $z_v \leq n-1$).

Из отобранных представителей орбит сформируем множество $S = (S_1, S_2, \dots, S_M)$, где $S_v = C_{v,u}$, $v = 1, \dots, M$, а выбор индекса u при соответствующем $C_{v,u}$ определяется правилом сечения v -й циклической орбиты группового кода.

Рассмотрим двоичный случай, т.е. ограничимся исследованием свойств множества $S = (S_1, S_2, \dots, S_M)$, образованного посредством сечения циклических орбит двоичного группового кода. Элементы формируемых дискретных последовательностей (дискретных сигналов) $S_v = (s_0^v, s_1^v, \dots, s_{n-1}^v)$ зададим по элементам отобранных кодовых слов (лидеров орбит

$C_{v,u} = (c_0^{v,u}, c_1^{v,u}, \dots, c_{n-1}^{v,u})$ следующим образом: $s_i^v = \begin{cases} 1, & c_i^{v,u} = 1; \\ -1, & c_i^{v,u} = 0. \end{cases}$

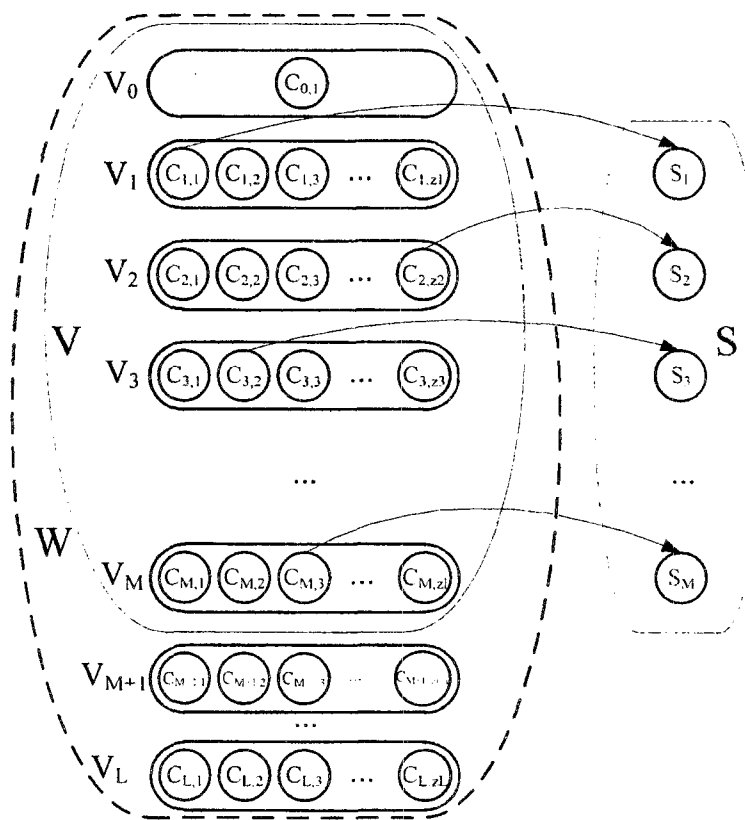


Рис. 1. Схема сечения ненулевых циклических орбит группового кода

Предположим, что рассматриваемый код V имеет весовой спектр вида: $A(w)$, $w = 0, \dots, n$, где $A(w)$ – число кодовых слов кода V с весом w .

Тогда образованное сечением циклических орбит кода V множество двоичных дискретных сигналов $S = (S_1, S_2, \dots, S_M)$ обладает корреляционными и ансамблевыми свойствами, определяемыми следующим утверждением [3, 6].

Утверждение.

1. Боковые лепестки периодической функции авто- (ПФАК) и взаимной (ПФВК) корреляции ансамбля сигналов $S = (S_1, S_2, \dots, S_M)$ принимают следующие значения:

$$\text{ПФВК}, \text{ПФАК} = \frac{n-2w}{n}, \text{ для таких } w = d, d+1, \dots, n, \text{ что } A(w) \neq 0. \quad (3)$$

2. Для всех таких $w = d, d+1, \dots, n$, что $A(w) = 0$ боковые лепестки ПФАК и ПФВК никогда не принимают значения $\frac{n-2w}{n}$.

3. Мощность M ансамбля $S = (S_1, S_2, \dots, S_M)$ определяется числом ненулевых орбит кода V и ограничена снизу выражением $M \geq \frac{2^k - 1}{n}$. Равенство выполняется в случае максимального периода последовательностей всех орбит, образующих код, т.е. если код V состоит из набора орбит, образованных последовательностями максимальной длины (m -последовательностями).

Таким образом, алгебраическое сечение циклических орбит группового кода позволяет сформировать множество последовательностей $S = (S_1, S_2, \dots, S_M)$, которые не являются циклически сдвинутыми копиями друг друга и обладают заранее заданными дистанционными свойствами группового кода. Это позволяет алгебраически строить большие ансамбли дискретных сигналов с многоуровневой функцией авто- и взаимной корреляции.

Формирование дискретных сигналов

Ключевым этапом в формировании дискретных сигналов является синтез линейного группового кода с требуемыми дистанционными и структурными свойствами. Групповой (n, k, d) код над $GF(q)$ по определению задается своими проверочным $h(x)$ и/или порождающим $g(x)$ многочленами через произведение конечного числа минимальных многочленов $f_i(x)$ конечного поля $GF(q^m)$ (здесь и далее будем рассматривать групповые коды примитивной длины $n = q^m - 1$). В свою очередь, каждый минимальный многочлен задается через свои корни, сгруппированные в соответствующие классы сопряженных элементов, т.е. запишем

$$h(x) = H.O.K. \left(\prod_{i \neq j} f_i(x) \right) = H.O.K. \left(\prod_{i \neq j} \prod_{s=0}^{m_i} (x - \alpha^{i(q^s)}) \right).$$

Добавление минимальных многочленов в качестве сомножителей в разложении проверочного многочлена приводит к повышению мощности кода (увеличению количества кодовых слов) и соответствующему снижению дистанционных свойств. Напротив, уменьшение количества минимальных многочленов в качестве сомножителей в разложении $h(x)$ приводит к снижению мощности кода (уменьшению количества кодовых слов) и соответствующему улучшению дистанционных свойств. Это схематично отражено на рис. 2., из которого следует, что поочередное добавление (удаление) минимальных многочленов в качестве сомножителей порождающего/проверочного многочлена приводит к изменению параметров (n, k, d) кода V над $GF(q)$.

Проведем оценку свойства двоичных дискретных сигналов для различных правил формирования группового (n, k, d) кода V над $GF(2)$, т.е. для различного числа сомножителей в $h(x)$ и $g(x)$.

Рассмотрим первый, наиболее простой случай, когда двоичный групповой (n, k, d) код V над $GF(2)$ задан через проверочный многочлен вида $h(x) = f_i(x) = \prod_{s=0}^{m-1} (x - \alpha^{i(2^s)})$.

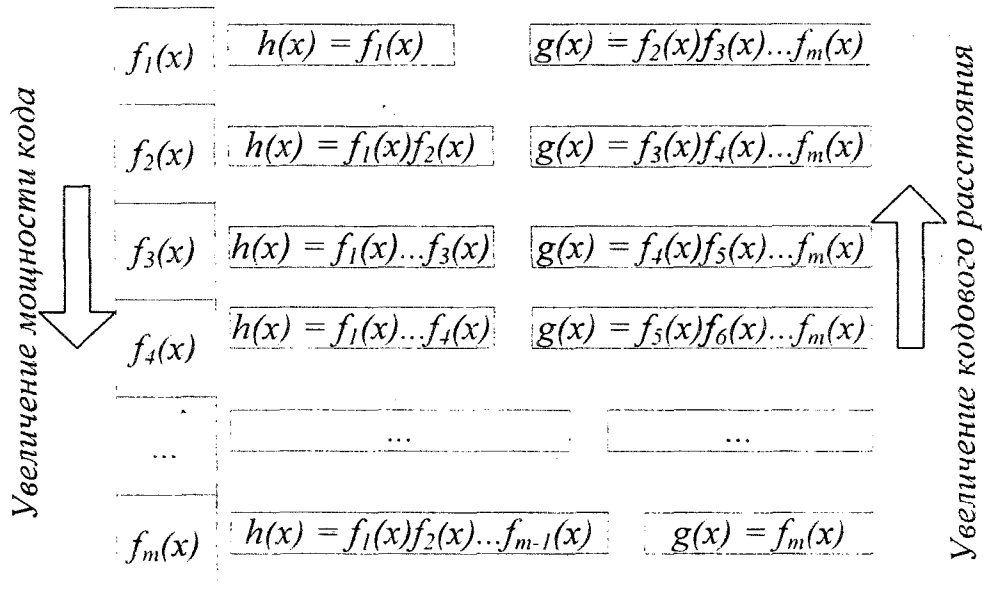


Рис. 2. Схема формирования ансамблей дискретных сигналов с многоуровневой функцией корреляции

Схема формирования проверочного $h(x)$ и порождающего $g(x)$ многочленов группового кода через элементы циклотомических классов представлена на рис. 3. Такой код содержит одну ненулевую циклическую орбиту, его весовой спектр имеет вид:

$$A(w) = \begin{cases} 1, w = 0; \\ 0, w = 1, \dots, 2^{m-1} - 1; \\ \neq 0, w = 2^{m-1}; \\ 0, w = 2^{m-1} + 1, \dots, 2^m - 1, \end{cases}$$

что с учетом (3) дает следующую оценку значений боковых лепестков:

$$ПФВК, ПФАК = \frac{-1}{2^m - 1}. \quad (4)$$

Пример нормированной ПФАК субортогональных сигналов для $n = 127$ приведен на рис. 4.

Оценим мощность M ансамбля формируемых сигналов. Всего имеем $2^k - 1 = 2^m - 1$ ненулевых кодовых слов группового кода.

Период каждой последовательности максимальный (что следует из примитивности элемента α). Откуда имеем

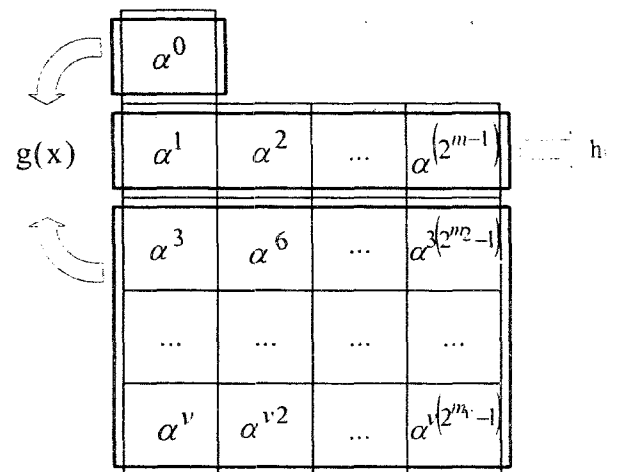


Рис. 3. Схема формирования многочленов $h(x)$ и $g(x)$ при синтезе субортогональных сигналов

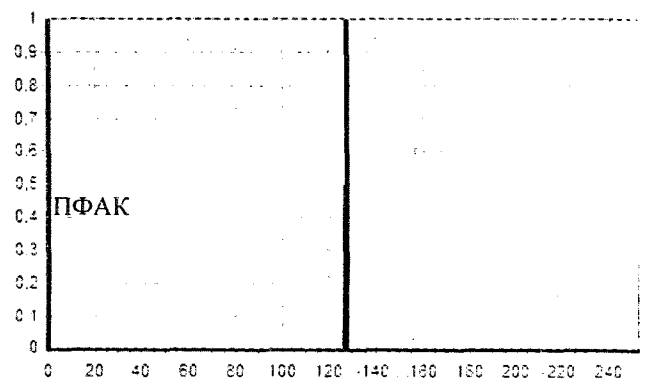


Рис. 4. ПФАК субортогональных сигналов для $n = 127$

$M = \frac{2^m - 1}{2^m - 1} = 1$, т.е. код содержит всего одну ненулевую орбиту, каждый представитель которой является субортогональным сигналом ($ПФВК, ПФАК = \frac{-1}{2^m - 1}$). Другими словами, через сечение циклической орбиты группового кода нами синтезирован простейший и наиболее изученный класс сигналов: m -последовательность.

Для построения более сложных классов сигналов рассмотрим случай, когда двоичный групповой (n, k, d) код V над $GF(2)$ задан через проверочный многочлен вида $h(x) = \prod_{s=0}^{m-1} (x - \alpha^{i_1(2^s)}) (x - \alpha^{i_2(2^s)})$, где порядок элементов α^{i_1} и α^{i_2} равен порядку мультипликативной группы конечного поля $GF(2^m)$. Схема формирования проверочного $h(x)$ и порождающего $g(x)$ многочленов через элементы циклотомических классов представлена на рис. 5. Очевидно, что по сравнению со случаем формирования субортогональных дискретных сигналов в качестве корней проверочного многочлена используются элементы двух циклотомических классов.

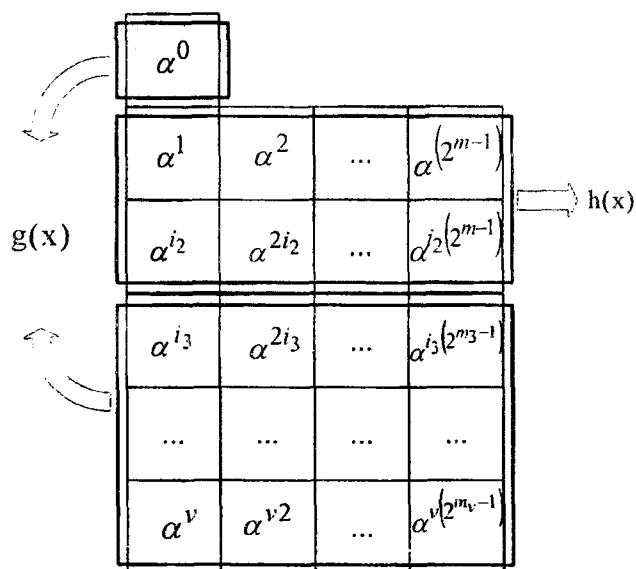


Рис. 5. Схема формирования многочленов $h(x)$ и $g(x)$ при синтезе сигналов Голда

Весовой спектр рассматриваемого кода имеет следующий вид:

$$A(w) = \begin{cases} 1, w = 0; \\ 0, w = 1, \dots, 2^{m-1} - 2^{\frac{m+1}{2}-1} - 1; \\ \neq 0, w = 2^{m-1} - 2^{\frac{m+1}{2}-1}; \\ 0, w = 2^{m-1} - 2^{\frac{m+1}{2}-1} + 1, \dots, 2^{m-1} - 1; \\ \neq 0, w = 2^{m-1}; \\ 0, w = 2^{m-1} + 1, \dots, 2^{m-1} + 2^{\frac{m+1}{2}-1} - 1; \\ \neq 0, w = 2^{m-1} + 2^{\frac{m+1}{2}-1}; \\ 0, w = 2^{m-1} + 2^{\frac{m+1}{2}-1} + 1, \dots, 2^m - 1. \end{cases}$$

Используя выражение (3) получим:

$$ПФВК, ПФАК = \begin{cases} \frac{-1 + 2^{\frac{m+1}{2}}}{2^m - 1}, w = 2^{m-1} - 2^{\frac{m+1}{2}-1}; \\ \frac{-1}{2^m - 1}, w = 2^{m-1}; \\ \frac{-1 - 2^{\frac{m+1}{2}}}{2^m - 1}, w = 2^{m-1} + 2^{\frac{m+1}{2}-1}. \end{cases} \quad (5)$$

Мощность ансамбля формируемых таким образом сигналов определяется выражением

$$M = \frac{2^{2m} - 1}{2^m - 1} = 2^m + 1. \quad (6)$$

Полученные оценки соответствуют дискретным последовательностям Голда [7, 8]. Таким образом, предлагаемый подход позволяет синтезировать известные классы дискретных сигналов (субортогональные последовательности и коды Голда) новым способом – через сечение циклических орбит группового кода.

Примеры нормированных ПФАК и ПФВК сигналов с трехуровневой функцией корреляции для $n = 127$ приведены на рис. 6, 7.

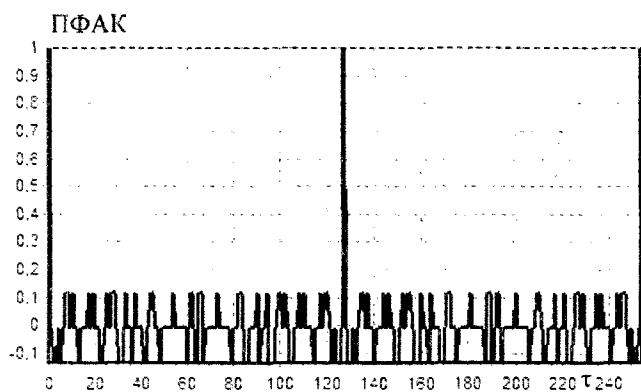


Рис. 6. ПФАК

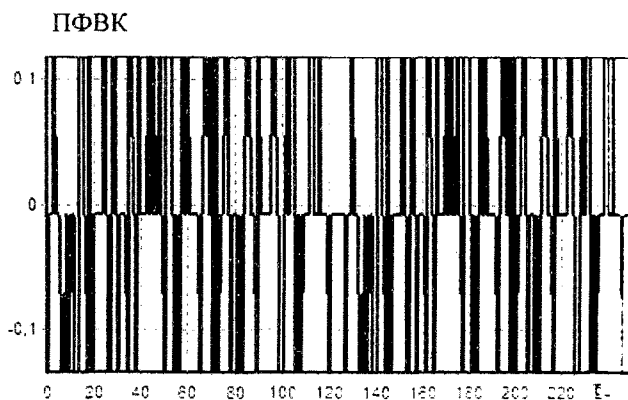


Рис. 7. ПФВК

Для построения новых классов дискретных сигналов рассмотрим случай, когда двоичный групповой (n, k, d) код V над $GF(2)$ задан через проверочный многочлен вида

$$h(x) = \prod_{s=0}^{m-1} \left(x - \alpha^{i_1(2^s)} \right) \left(x - \alpha^{i_2(2^s)} \right) \left(x - \alpha^{i_3(2^s)} \right),$$

где порядок элементов α^{i_1} , α^{i_2} и α^{i_3} равен порядку мультипликативной группы конечного поля $GF(2^m)$.

Схема формирования $h(x)$ и $g(x)$ через элементы циклотомических классов представлена на рис. 8.

В данном случае в качестве корней проверочного многочлена используются элементы трех циклотомических классов:

$$\left\{ \alpha^{i_1(2^0)}, \alpha^{i_1(2^1)}, \dots, \alpha^{i_1(2^{m-1})} \right\},$$

$$\left\{ \alpha^{i_2(2^0)}, \alpha^{i_2(2^1)}, \dots, \alpha^{i_2(2^{m-1})} \right\}$$

и

$$\left\{ \alpha^{i_3(2^0)}, \alpha^{i_3(2^1)}, \dots, \alpha^{i_3(2^{m-1})} \right\},$$

где $s = 0, 1, \dots, m-1$.

Весовой спектр заданного таким образом кода имеет вид:

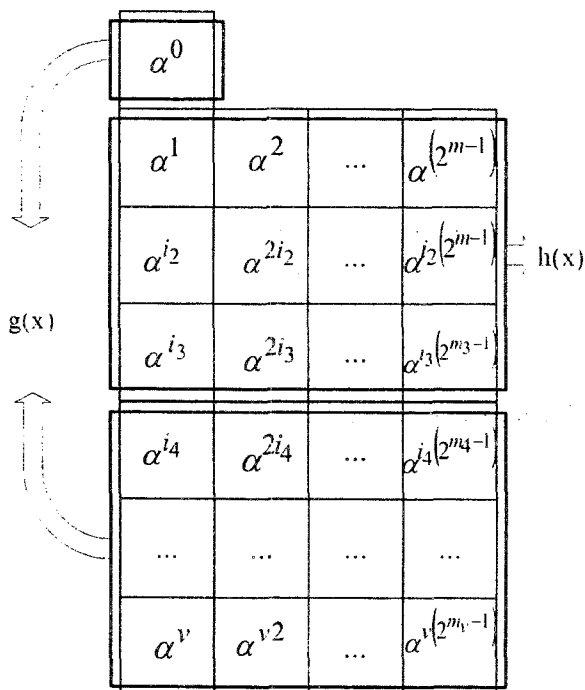


Рис. 8. Схема формирования многочленов $h(x)$ и $g(x)$ при синтезе сигналов с пятиуровневой функцией корреляции

$$A(w) = \begin{cases} 1, w = 0; \\ 0, w = 1, \dots, 2^{m-1} - 2^{\frac{m+1}{2}} - 1; \\ \neq 0, w = 2^{m-1} - 2^{\frac{m+1}{2}}; \\ 0, w = 2^{m-1} - 2^{\frac{m+1}{2}} + 1, \dots, 2^{m-1} - 2^{\frac{m+1}{2}-1} - 1; \\ \neq 0, w = 2^{m-1} - 2^{\frac{m+1}{2}-1}; \\ 0, w = 2^{m-1} - 2^{\frac{m+1}{2}-1} + 1, \dots, 2^{m-1} - 1; \\ \neq 0, w = 2^{m-1}; \\ 0, w = 2^{m-1} + 1, \dots, 2^{m-1} + 2^{\frac{m+1}{2}-1} - 1; \\ \neq 0, w = 2^{m-1} + 2^{\frac{m+1}{2}-1}; \\ 0, w = 2^{m-1} + 2^{\frac{m+1}{2}-1} + 1, \dots, 2^{m-1} + 2^{\frac{m-1}{2}} - 1; \\ \neq 0, w = 2^{m-1} + 2^{\frac{m+1}{2}}; \\ 0, w = 2^{m-1} + 2^{\frac{m+1}{2}} + 1, \dots, 2^m - 1. \end{cases}$$

После подстановки в (3) получим оценку уровней боковых лепестков ПФВК, ПФАК:

$$\text{ПФВК, ПФАК} = \begin{cases} \frac{-1 - 2^{\frac{m+1}{2}+1}}{2^m - 1}, w = 2^{m-1} - 2^{\frac{m+1}{2}}; \\ \frac{-1 - 2^{\frac{m+1}{2}}}{2^m - 1}, w = 2^{m-1} - 2^{\frac{m+1}{2}-1}; \\ \frac{-1}{2^m - 1}, w = 2^{m-1}; \\ \frac{-1 + 2^{\frac{m+1}{2}}}{2^m - 1}, w = 2^{m-1} + 2^{\frac{m+1}{2}-1}; \\ \frac{-1 + 2^{\frac{m+1}{2}+1}}{2^m - 1}, w = 2^{m-1} + 2^{\frac{m+1}{2}}. \end{cases} \quad (7)$$

Таким образом, нами получен новый класс сигналов с пятиуровневой функцией корреляции и значительно улучшенными ансамблевыми свойствами. При этом три уровня боковых лепестков соответствуют рассмотренным выше трехуровневым дискретным сигналам (кодам Голда), два дополнительных уровня соответствуют ненулевым компонентам весового

спектра использованного группового кода. Мощность ансамбля сигналов

$$M = \frac{2^{3m} - 1}{2^m - 1} = 2^{2m} + 2^m + 1. \tag{8}$$

Примеры нормированных ПФАК и ПФВК пятиуровневых сигналов приведены на рис. 9, 10.

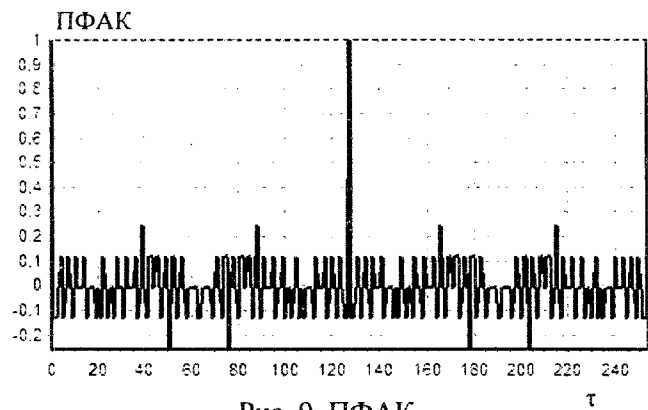


Рис. 9. ПФАК

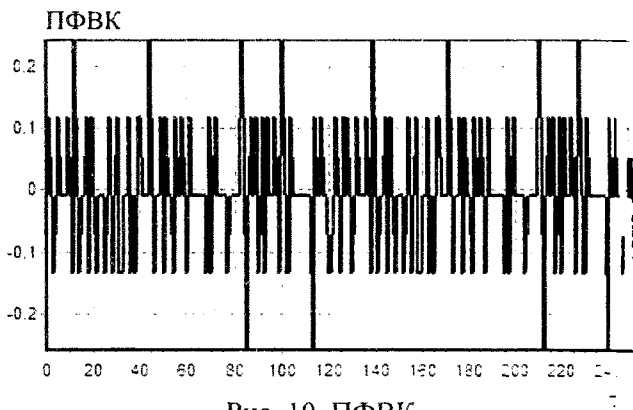


Рис. 10. ПФВК

Таким образом, использование групповых кодов позволяет сформировать новый класс дискретных сигналов с пятиуровневой ПФВК.

Обобщим полученные выше результаты на случай построения двоичных дискретных сигналов с многоуровневой функцией корреляции. Для этого рассмотрим случай, когда (n,k,d) код V над $GF(2)$ задан через проверочный многочлен вида

$$h(x) = \prod_{s=1}^{m-1} \left(x - \alpha^{i_1(2^s)} \right) \left(x - \alpha^{i_2(2^s)} \right) \dots \left(x - \alpha^{i_u(2^s)} \right),$$

где порядок элементов $\alpha^{i_1}, \alpha^{i_2}, \dots, \alpha^{i_u}$ равен порядку мультипликативной группы поля $GF(2^m)$.

Схема формирования $h(x)$ и $g(x)$ через элементы произвольного числа циклотомических классов представлена на рис. 11.

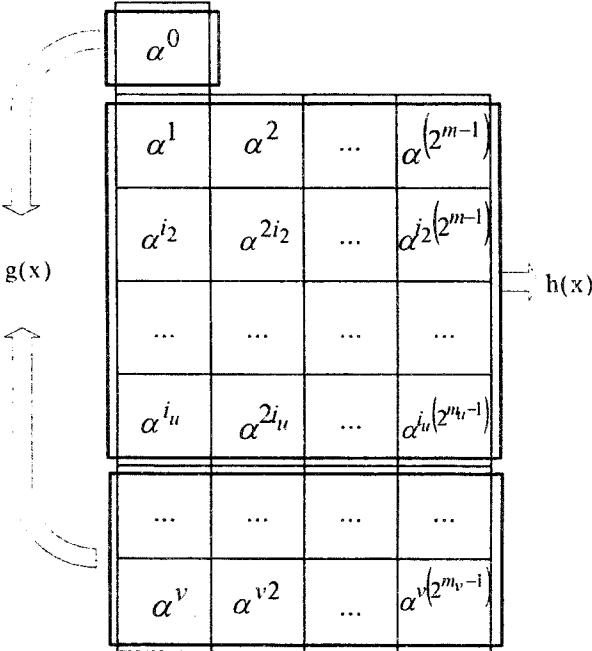


Рис. 11. Схема формирования многочленов $h(x)$ и $g(x)$ при синтезе сигналов с многоуровневой функцией корреляции

Оценим мощность ансамбля формируемых дискретных сигналов. Мощность используемого кода $2^k = 2^{um}$, всего имеется $2^k - 1 = 2^{um} - 1$ ненулевых кодовых слов. Положим, что каждое кодовое слово обладает максимальным периодом, тогда

$$M = \frac{2^{um} - 1}{2^m - 1} = 2^{(u-1)m} + 2^{(u-2)m} + \dots + 2^m + 1. \quad (9)$$

Оценим весовой спектр кода. Многочлен $h(x)$ содержит в качестве сомножителя проверочные многочлены всех кодов, с проверочными многочленами

$$h_y(x) = f_{i_1}(x)f_{i_2}(x)\dots f_{i_y}(x), y \leq u.$$

Отсюда следует, что ненулевые компоненты весового спектра образуются поочередным добавлением (в порядке добавления сомножителей в многочлен $h(x)$) соответствующей пары (для всех $y = 2, 3, \dots, u$):

$$A(z_y) \neq 0, A(2^m - z_y) \neq 0,$$

где

$$z_y = \max_{s=0, \dots, m-1} \{ \{2^s\} \bmod (2^m - 1), \{i_2 2^s\} \bmod (2^m - 1), \dots, \{i_y 2^s\} \bmod (2^m - 1) \}.$$

Общее выражение для оценки весового спектра запишем в виде:

$$A(w) = \begin{cases} 1, w = 0; \\ 0, w = 1, \dots, z_u - 1; \\ \neq 0, w = z_u; \\ \dots \\ \neq 0, w = z_3 = 2^{m-1} - 2^{\frac{m+1}{2}}; \\ 0, w = z_3 + 1, \dots, z_2 - 1; \\ \neq 0, w = z_2 = 2^{m-1} - 2^{\frac{m+1}{2}-1}; \\ 0, w = z_2 + 1, \dots, z_1 - 1; \\ \neq 0, w = z_1 = 2^{m-1}; \\ 0, w = z_1 + 1, \dots, 2^m - z_2 - 1; \\ \neq 0, w = 2^m - z_2 = 2^{m-1} + 2^{\frac{m+1}{2}-1}; \\ 0, w = 2^m - z_2 + 1, \dots, 2^m - z_3 - 1; \\ \neq 0, w = 2^m - z_3 = 2^{m-1} + 2^{\frac{m+1}{2}}; \\ \dots \\ \neq 0, w = 2^m - z_u; \\ 0, w = w = 2^m - z_u + 1, \dots, 2^m - 1. \end{cases}$$

С учетом (3) соответствующее выражение по оценке уровней боковых лепестков ПФВК примет вид:

$$\begin{aligned}
 & \frac{2^m - 2z_u - 1}{2^m - 1}, w = z_u; \\
 & \dots \\
 & \frac{2^m - 2z_3 - 1}{2^m - 1} = \frac{-1 - 2^{\frac{m+1}{2} + 1}}{2^m - 1}, w = z_3; \\
 & \frac{2^m - 2z_2 - 1}{2^m - 1} = \frac{-1 - 2^{\frac{m+1}{2}}}{2^m - 1}, w = z_2; \\
 & \frac{2^m - 2z_1 - 1}{2^m - 1} = \frac{-1}{2^m - 1}, w = z_1; \\
 & \frac{2^m - 2(2^m - z_2) - 1}{2^m - 1} = \frac{-1 + 2^{\frac{m+1}{2}}}{2^m - 1}, w = 2^m - z_2; \\
 & \frac{2^m - 2(2^m - z_3) - 1}{2^m - 1} = \frac{-1 + 2^{\frac{m+1}{2} + 1}}{2^m - 1}, w = 2^m - z_3; \\
 & \dots \\
 & \frac{2^m - 2(2^m - z_u) - 1}{2^m - 1}, w = 2^m - z_u.
 \end{aligned}
 \tag{10}$$

Анализ полученных выражений (4) – (10) показывает, что формируемые предлагаемым методом дискретные сигналы обладают многоуровневыми функциями авто- и взаимной корреляции. Величины боковых выбросов принимают конечное число значений, задаваемых весовыми свойствами используемого группового кода. Мощность ансамбля сигналов определяется кодовыми соотношениями группового кода.

Выводы

Проведенные исследования показали, что предлагаемый метод синтеза дискретных сигналов позволяет формировать большие ансамбли слабокоррелированных двоичных последовательностей. Мощность ансамбля формируемых дискретных сигналов и их корреляционные свойства аналитически зависят от кодовых соотношений используемых групповых кодов. Установлено, что предлагаемый метод синтеза дискретных сигналов обобщает известные подходы, в том числе, процедуры формирования субортогональных последовательностей и кодов Голда. Кроме того, синтезированы новые классы дискретных последовательностей с многоуровневыми функциями корреляции.

Список литературы: 1. Скляр Б. Цифровая связь. Теоретические основы и практическое применение / Б. Скляр. – М. : Вильямс, 2003. – 1104 с. 2. Гряник М.В., Фролов В.И. Технология CDMA – будущее сотовых систем в Украине / М.В. Гряник, В.И. Фролов // Мир связи. – 1998. – № 3. – С. 40-43. 3. Кузнецов А.А. Метод синтеза псевдослучайных последовательностей с пятиуровневой функцией корреляции / А.А. Кузнецов, В.И. Грабчак, А.Н. Коваленко, В.Н. Сай // Матеріали четвертої наукової конференції Харківського університету Повітряних Сил ім. Івана Кожедуба. – Х. : ХУ ПС, 2008. – С. 135. 4. Стасев Ю.В. Способ построения ансамблей дискретных сигналов с заданными значениями боковых выбросов корреляции / Ю.В. Стасев, А.А. Кузнецов, А.Н. Коваленко // Матеріали першої науково-технічної конференції «Науково-методичні основи оцінювання та управління техногенною безпекою у разі виникнення надзвичайної ситуації». – Х. : НДІ макрографії, 2007. – С. 7-8. 5. Блейхут Р. Теория и практика кодов, контролирующих ошибки : пер. с англ. – М. : Мир. – 1986. – 576с. 6. Stasev Y., Discrete Signals with Multi-Level Correlation Function / Stasev Y., Kuznetsov A., Sai V., Karpenko O. Statistical Methods of Signal and Data Processing (SMSDP-2010): Proceedings. – Kiev : National Aviation University "NAU-Druk" Publishing House – 2010. – P. 176 – 179. 7. Gold R. Optimal Binary Sequences for Spread Spectrum Multiplexing // IEEE Trans., Inf. Th., 1967, v. IT-13, N 4. – P. 619-621. 8. Диксон Р.К. Широкополосные системы : пер. с англ. – М. : Связь, 1979. – 304с.

Харьковский национальный
университет радиоэлектроники

Поступила в редколлегию 12.09.2011

АНАЛИЗ ИНФОРМАЦИОННЫХ ПРИЗНАКОВ ОТПЕЧАТКОВ ПАЛЬЦЕВ И СКАНИРУЮЩИХ УСТРОЙСТВ

Введение

В наше время пароли, персональные идентификационные номера и специальные идентификационные карточки стали жизненной необходимостью. Таким образом, человек должен хранить в своей памяти огромное количество различных комбинаций цифр и букв.

Чтобы облегчить участь современного человека, компании, специализирующиеся на производстве компьютеров, начали заниматься разработкой биометрических технологий. Биометрия – эта наука, изучающая возможности использования различных характеристик человеческого тела (будь то отпечатки пальцев или уникальные свойства человеческого зрачка или голоса) для идентификации каждого конкретного человека. Пользуясь биометрическими технологиями, человек никогда не сможет забыть необходимый ему пароль или код, поскольку его большой палец, голос или зрачок глаза всегда находятся с ним [1].

Отпечаток пальца образует так называемые папиллярные линии на гребешковых выступах кожи, разделенных бороздками. Из этих линий складываются сложные узоры (дуговые, петлевые и завитковые), которые обладают свойствами индивидуальности и неповторимости, что позволяет абсолютно надежно идентифицировать личность. Хотя процент отказа в доступе уполномоченных пользователей составляет около трех процентов ошибочного доступа – меньше одного к миллиону. Преимущества доступа по отпечатку пальца – простота использования, удобство и надежность. Весь процесс идентификации занимает мало времени и не требует усилий от тех, кто использует данную систему доступа [2]. Исследования также показали, что использование отпечатка пальца для идентификации личности является наиболее удобным из всех биометрических методов. Вероятность ошибки при идентификации пользователя намного меньше в сравнении с другими биометрическими методами [3]. Кроме того, устройство идентификации по отпечатку пальца не требует много места на клавиатуре или в механизме.

В каждом отпечатке пальца можно определить два типа признаков – глобальные и локальные.

Глобальный признак отпечатка пальца

Глобальные признаки – те, которые можно увидеть невооружённым глазом (рис. 1) [4]:

- Папиллярный узор. Область образа – выделенный фрагмент отпечатка, в котором локализованы все признаки.
- Ядро – пункт, локализованный в середине отпечатка или некоторой выделенной области.
- Пункт "дельта" – начальная точка. Место, в котором происходит разделение или соединение бороздок папиллярных линий, либо очень короткая бороздка (может доходить до точки).
- Тип линии – две наибольшие линии, которые начинаются как параллельные, а затем расходятся и огибают всю область образа.
- Счётчик линий – число линий на области образа, либо между ядром и пунктом "дельта".

На рис. 1 представлены следующие типы узоров. С 1 по 4 – узоры типа «петля» (левая, правая, центральная, двойная). 5 и 6 – узоры типа «дельта» или «дуга» (простая и острая). 7 и 8 – узоры типа «спираль» (центральная и смешанная))

Метод на основе глобальных признаков.

Выполняется обнаружение глобальных признаков (ядро, дельта). Количество этих признаков и их взаимное расположение позволяет классифицировать тип узора. Окончательное

распознавание выполняется на основе локальных признаков (число сравнений получается на несколько порядков ниже для большой базы данных).



Рис. 1

Локальный признак отпечатка пальца

Другой тип признаков – локальные. Их называют минуциями – уникальные для каждого отпечатка признаки, определяющие пункты изменения структуры папиллярных линий (окончание, раздвоение, разрыв и т.д.), ориентацию папиллярных линий и координаты в этих пунктах. Каждый отпечаток содержит до 70 минуций (рис. 2).



Рис. 2

На рис. 2 представлен отпечаток пальца на котором отмечены следующие признаки: две линии – "тип линии"; то, что между ними – может выступать в качестве области образа, но обычно берётся вся площадь отпечатка; окружность слева – пункт "дельта"; окружность ниже – ядро; квадратами выделены некоторые минуции. Папиллярный узор – левая петля.

Практика показывает, что отпечатки пальцев разных людей могут иметь одинаковые глобальные признаки, но совершенно невозможно наличие одинаковых микроузоров минуций. Поэтому глобальные признаки используют для разделения базы данных на классы и на этапе аутентификации. На втором этапе распознавания используют уже локальные признаки.

Для использования локальных признаков прибегают к этапам сравнения двух отпечатков:

- Этап 1. Улучшение качества исходного изображения отпечатка. Увеличивается резкость границ папиллярных линий.

- Этап 2. Вычисление поля ориентации папиллярных линий отпечатка. Изображение разбивается на квадратные блоки, со стороной больше 4 пикселей и по градиентам яркости вычисляется угол / ориентации линий для фрагмента отпечатка.

- Этап 3. Бинаризация изображения отпечатка. Приведение к чёрно-белому изображению (1 bit) пороговой обработкой.

- Этап 4. Утончение линий изображения отпечатка. Утончение производится до тех пор, пока линии не будут шириной 1 пиксель (рис. 3).

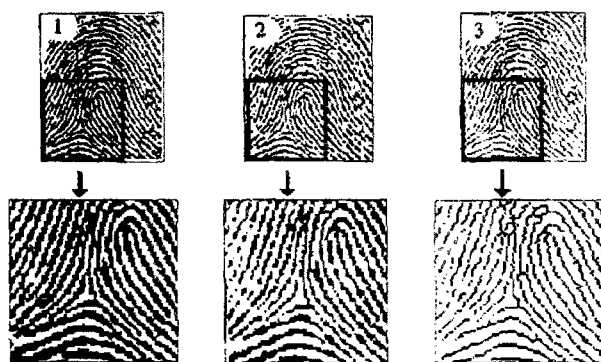


Рис. 3

- Этап 5. Выделение минучий. Изображение разбивается на блоки 9x9 пикселей. После этого подсчитывается число чёрных (ненулевых) пикселей, находящихся вокруг центра. Пиксель в центре считается минучией, если он сам ненулевой, и соседних ненулевых пикселей один (минучия "окончание") или два (минучия "раздвоение") (рисунок 4).

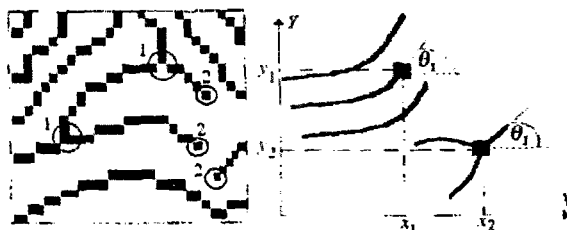


Рис. 4

Координаты обнаруженных минучий и их углы ориентации записываются в вектор:

$$W(p) = [(x_1, y_1, t_1), (x_2, y_2, t_2) \dots (x_p, y_p, t_p)].$$

где p – число минучий. При регистрации пользователей этот вектор считается эталоном и записывается в базу данных. При распознавании вектор определяет текущий отпечаток (что вполне логично).

- Этап 6. Сопоставление минучий. Два отпечатка одного пальца будут отличаться друг от друга поворотом, смещением, изменением масштаба и/или площадью соприкосновения в зависимости от того, как пользователь прикладывает палец к сканеру. Поэтому нельзя сказать, принадлежит ли отпечаток человеку или нет на основании простого их сравнения (векторы эталона и текущего отпечатка могут отличаться по длине, содержать несоответствующие минучии и т.д.). Из-за этого процесс сопоставления должен быть реализован для каждой минучии отдельно.

Этапы сравнения:

- Регистрация данных.
- Поиск пар соответствующих минучий.
- Оценка соответствия отпечатков.

При регистрации определяются параметры аффинных преобразований (угол поворота, масштаб и сдвиг), при которых некоторая минучия из одного вектора соответствует некоторой минучии из второго.

При поиске для каждой минучии нужно перебрать до 30 значений поворота (от -15 градусов до +15), 500 значений сдвига (от -250 пкс. до +250 пкс. хотя, конечно, границы выбирают и поменьше) и 10 значений масштаба (от 0.5 до 1.5 с шагом 0.1). Итого до 150 000 ша-

гов для каждой из 70 возможных минуций. (На практике, все возможные варианты не перебираются – после подбора нужных значений для одной минуции их же пытаются подставить и к другим минуциям, иначе было бы возможно сопоставить практически любые отпечатки друг другу).

Оценка соответствия отпечатков выполняется по формуле

$$K = (D * D * 100\%) / (p * q),$$

где D – количество совпавших минуций, p – количество минуций эталона, q – количество минуций идентифицируемого отпечатка). В случае, если результат превышает 65%, отпечатки считаются идентичными (порог может быть понижен выставлением другого уровня бдительности).

Если выполнялась аутентификация, то на этом всё и заканчивается. Для идентификации необходимо повторить этот процесс для всех отпечатков хранящихся в базе данных, затем выбирается пользователь, у которого наибольший уровень соответствия (разумеется, его результат должен быть выше порога 65%).

Анализ существующих сканеров отпечатка пальца

Устройства считывания отпечатков пальцев сейчас находят различные применения. Их устанавливают на ноутбуки, в мыши, клавиатуры, флеш накопителя, а также применяют в виде отдельных внешних устройств и терминалов, продающихся в комплекте с системами AFIS (Automated fingerprint identification systems – системы автоматизированной идентификации отпечатков пальцев).

Несмотря на внешние различия, все сканеры можно разделить на несколько основных видов (см. таблицу):

- оптические;
- полупроводниковые (меняют свойства в местах контакта);
- ультразвуковые (ультразвук возвращается через различные промежутки времени, отражаясь от бороздок или линий).

Сканеры отпечатков пальцев прошли действительно долгий путь к улучшению. Современные системы оснащены различными датчиками (температуры, силы нажатия и т. п.), которые повышают степень защиты от подделок. С каждым днем системы становятся все более удобными и компактными. Большинство компаний производят готовые системы, которые оснащены всем необходимым, включая программное обеспечение. Интеграторам в этой области просто нет необходимости собирать систему самостоятельно, поскольку это невыгодно и займет больше времени и сил, чем купить готовую и уже недорогую при этом систему, тем более выбор будет действительно широк.

Стандарты для использования отпечатков пальцев

Сейчас в основном используются стандарты ANSI и ФБР США. В них определены следующие требования к образу отпечатка:

- каждый образ представляется в формате несжатого TIF;
- образ должен иметь разрешение не ниже 500 dpi;
- образ должен быть полутоновым с 256 уровнями яркости;
- максимальный угол поворота отпечатка от вертикали не более 15 градусов;
- основные типы минуций – окончание и раздвоение.

Обычно в базе данных хранят более одного образа, что позволяет улучшить качество распознавания. Образы могут отличаться друг от друга сдвигом и поворотом. Масштаб не меняется, так как все отпечатки получают с одного устройства.

На сегодняшний день разработаны и приняты международные стандарты, которые облегчают решение поставленной задачи[6]:

- ISO/IEC 7816-11. Personal Verification Through Biometric Methods.
- ISO/IEC 19794-2. Finger Minutiae Data.

ISO/IEC 19794-4. Finger Image Data.

Разновидность технологии	Сущность	Достоинства	Недостатки
Оптическая (на отражение)	Для захвата оптического изображения отпечатка пальца используется CMOS или CCD матрица	-	Трудность различения живого пальца и его имитации; чувствительность к загрязнениям.
Оптическая (на просвет)	Кончик пальца освещается со стороны ногтя. Прошедший через палец свет попадает на линзу датчика и далее на оптический сенсор, анализирующий характеристики поглощения света живыми тканями. Этот способ разработан компанией Mitsubishi Electric Corp.	Высокая надежность считывания и устойчивость к обману; не требуется контакт пальца с поверхностью датчика	Сложность изготовления
Емкостная	Кончик пальца помещается напротив массива элементов, чувствительных к емкости. Различия в диэлектрике между гребнем (в основном вода) и впадиной (воздух) позволяют их идентифицировать и построить образ отпечатка.	Один из наиболее популярных методов вследствие его надежности и низкой стоимости	Уязвимость от электростатического разряда (ESD); возможность обмана искусственным кончиком пальца.
Радио	Кончик пальца возбуждается радиоволной низкой интенсивности. В этом случае он действует как передатчик, а различие расстояний между гребнями и впадинами может быть обнаружено массивом соответствующих настроенных антенн. Необходимо, чтобы кончик пальца контактировал с областью излучения датчика (по его периферии).	Поскольку анализируются физиологические свойства кожи, очень сложно обмануть такой датчик искусственным пальцем.	Неустойчивая работа при плохом контакте пальца с передающим кольцом, которое может стать некомфортно горячим
Давление	Массив чувствительных к давлению пикселей на основе пьезоэлектрических элементов преобразует давление гребней пальца в электрические импульсы.	-	Низкая чувствительность, срабатывание от имитации пальца, повреждение при чрезмерном давлении
MEMS	Кончик пальца анализируется множеством микроэлектромеханических элементов.	-	Высокая вероятность ошибки; возможность обмана имитацией;
Тепловая	Использование пирозлектрического материала для преобразования различия температуры в напряжение. Тепловой датчик на основе массива элементов из такого материала измеряет разницу температур между элементом под гребнем и элементом под впадиной кончика пальца.	Устойчивость к электростатическому разряду; отсутствие какого-либо воздействия на палец; работа в широком диапазоне температур; невозможность обмана с помощью имитации пальца.	Тепловой образ на датчике сохраняется короткое время ~0,1 с, поскольку при касании датчика быстро наступает тепловое равновесие

BioAPI является стандартом BioAPI Consortium, разработанным специально для унификации программных интерфейсов программного обеспечения разработчиков биометрических устройств. На данный момент принятым за основу стандартом является версия стандарта 1.0, которая вышла в марте 2001 года и была реализована под Windows. Пока ещё не вышла её версия под платформы Unix (Linux), но, насколько можно судить по сообщениям BioAPI Consortium, разработка ведётся давно и уже был период бета-тестирования среди членов консорциума. Согласно статистике сайта консорциума, более 90 биометрических производителей уже заявили о совместимости своих продуктов и решений со стандартом BioAPI.

CBEFF (Common Biometric Exchange File Format) – единый формат представления биометрических данных, который предлагается для замены биометрических форматов, используемых производителями различных сегментов биометрического рынка в своём оборудовании и программном обеспечении. При создании CBEFF были учтены все возможные аспекты его применения, в том числе криптография, многофакторная биометрическая идентификация и интеграция с карточными системами идентификации.

AAMVA Fingerprint Minutiae Format/National Standard for the Driver License/Identification Card DL/ID-2000, американский стандарт на формат представления, хранения и передачи отпечатков пальцев для водительских прав. Совместим со спецификациями BioAPI и стандартом CBEFF.

ANSI/NIST-ITL 1-2000 Fingerprint Standard Revision – американский стандарт, определяющий общий формат представления и передачи данных по отпечаткам пальцев, лицу, ладонным шрамам и татуировкам для использования в правоохранительных органах США.

Выводы

Анализ информационных признаков является неотъемлемой частью системы идентификации личности по отпечаткам пальцев, предназначенной для обнаружения сходства между двумя изображениями отпечатка пальца. В результате распознавания можно установить личность человека, приложившего палец, что может использоваться при входе в систему. Путём использования глобальных и локальных признаков удастся значительно понизить уровень влияния смещения и переноса отпечатка пальцев, а также шумов и искажений в изображении. Большое количество разработанных и введенных в действие стандартов дает возможность дальше изучать и применять на практике биометрическую характеристику человека, а именно – отпечатки пальцев.

Список литературы 1. *Биометрические технологии – альтернатива персональным идентификационным номерам и паролям.* Точка доступа: <http://www.k2kapital.com/archives/research/rs20000508.html> 2. *Alonso-Fernandez, F. Combining Multiple Matchers for fingerprint verification: a case study in BioSecure Network of Excellence / F. Alonso-Fernandez, J. Fierrez, J. Ortega-Garcia, H. Fronthaler, K. Kollreider, J. Bigun // Annals of Telecommunications, Multimodal Biometrics.* – Mallorca, Spain. – 2007. – P. 357-379. 3. *Завгородний В.И. Комплексная защита информации в компьютерных системах : учеб. пособие.* – М.: Логос, 2001. – 264 с. 4. *Bazen, A. Segmentation of fingerprint images / A. Bazen, S. Gerez Proc. Workshop on Circuits Systems and Signal Processing.* – Basel: T&Y. – 2001. – P. 276–280. 5. *Biometric Standards Activity.* Точка доступа: <http://www.biometrics.org/standards.php>.

Харьковский национальный
университет радиоэлектроники

Поступила в редколлегию 11.07.2011.

ИССЛЕДОВАНИЕ СИНХРОНИЗИРОВАННОГО АВТОГЕНЕРАТОРА С НЕЛИНЕЙНОЙ ОБРАТНОЙ СВЯЗЬЮ

Введение

Использование фазовой обратной связи в синхронизированных автогенераторах позволило не только существенно улучшить их уже известные характеристики, но и получить новые свойства. А большие функциональные возможности автогенераторов в режиме синхронизации обусловили их широкое применение в радиотехнике при создании синхронных радиоприемных устройств, усилении и демодуляции АМ, ЧМ и ФМ сигналов, фазовой коррекции, нелинейной фильтрации и т.д. [1 – 7]. В информационно-измерительной технике они используются в качестве основных элементов фазогенераторных преобразователей, чувствительность которых на два порядка выше чувствительности, достигаемой с помощью мостовых и резонансных методов. Однако влияние нелинейной обратной связи, каковой по существу является фазовая обратная связь, рассматривалось только в случае квазигармонических автогенераторов.

Цель статьи – исследовать влияние нелинейной обратной связи на процесс полигармонической синхронизации на основном тоне одноконтурного LC-автогенератора, используемого в качестве следящего фильтра.

1. Структурная схема автогенератора с нелинейной обратной связью

Рассмотрим синхронизированный на основном тоне одноконтурный LC-автогенератор, структурная схема которого показана на рис. 1. Принципиальная схема собственно автогенератора представлена на рис. 2.

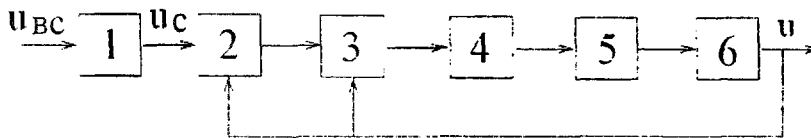


Рис. 1. Структурная схема автогенератора с нелинейной обратной связью:
1 – широкополосный фильтр; 2, 3 – блоки формирования нелинейной обратной связи; 4 – блок стабилизации амплитуды сигнала;
5 – преобразователь напряжения в ток; 6 – автогенератор;
 $u_{вс}$ – внешний сигнал; u – сигнал автогенератора.

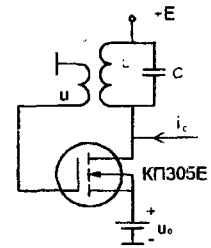


Рис. 2. Принципиальная электрическая схема автогенератора

Нелинейная обратная связь реализуется путем формирования непосредственного сигнала синхронизации i_c в соответствии с алгоритмом формирования отрицательной фазовой обратной связи второго рода [8].

Обозначим нижнюю граничную частоту следящего фильтра как ω_n а верхнюю как ω_v . Таким образом, частота первой гармонической составляющей входного сигнала меняется в диапазоне $\omega_n \leq \omega_c \leq \omega_v$.

Следящий фильтр может работать в двух режимах. Первый – это когда частота первой гармоники сигнала синхронизации, а следовательно и частота первой гармоники сигнала автогенератора, принимает такие значения, при которых через широкополосные фильтры проходят только первые гармоники сигналов. Второй режим наступает тогда, когда в полосы пропускания указанных фильтров с фиксированной полосой пропускания попадают первая и вторая гармоники сигналов внешнего и автогенератора. Диапазон изменения частоты сигнала синхронизации $0.577\omega_0 < \omega_c < 1.73\omega_0$. Частота, на которой происходит смена режимов,

$\omega_{пер} = 0.866\omega_0$, где ω_0 – резонансная частота контура.

2. Формирование сигнала нелинейной обратной связи

Допустим, что полигармонические сигналы описываются выражениями: внешний посл. прохождения фильтра 1 в виде $u_c = A_{c1} \cos(\omega_c t + \varphi_{c1}) + A_{c2} \cos(2\omega_c t + \varphi_{c2})$, а обратной связи – в виде $u = A_1 \cos(\omega_c t + \varphi_1) + A_2 \cos(2\omega_c t + \varphi_2)$. В выражении для внешнего сигнала синхронизации дополнительные фазовые сдвиги за счет фильтра 1 входят в фазы φ_{c1} и φ_{c2} , в силу произвольности фаз гармоник сигнала $u_{вн}$. Эти сигналы обрабатываются в блоках формирования нелинейной обратной связи 2, 3. Для обеспечения заданной полосы синхронизации в последующем устройстве амплитуда непосредственного сигнала синхронизации устанавливается определенной величины и поддерживается неизменной посредством блока стабилизации амплитуды 4. Тогда выходной сигнал блока 4 можно представить как

$$u_{сн} = A_{1н} \cos(\omega_c t + \varphi_{c1}) + A_{2н} \cos(2\omega_c t + \varphi_{c2}).$$

Выходной сигнал этого блока преобразуется в ток в преобразователе 5 и используется в качестве непосредственного сигнала синхронизации:

$$i_c = I_{c1} \cos(\omega_c t + \varphi_{c1}) + I_{c2} \cos(2\omega_c t + \varphi_{c2}), \quad I_{c2}/I_{c1} = 4A_2/A_1.$$

Особенность данной нелинейной обратной связи заключается в том, что первая гармоническая составляющая непосредственного сигнала синхронизации имеет фазу, такую же как и фаза первой гармоники внешнего сигнала синхронизации, а амплитуда второй гармоники непосредственного сигнала синхронизации не зависит от амплитуды второй гармоники внешнего сигнала.

Математическая модель автогенератора с нелинейной обратной связью

Особенность рассматриваемого в данной работе режима синхронизации автогенератора на основном тоне заключается в том, что периодическим полигармоническим сигналом является широкая полоса синхронизации, что приводит к изменению амплитуды колебаний в широких пределах. Такое условие исходит из практического использования данного режима синхронизации в нелинейном автогенераторном следящем фильтре. Это обстоятельство вынуждает выбрать для автогенератора режим колебаний первого рода. Тогда для аппроксимации нелинейной характеристики его усилительного элемента целесообразно использовать полином третьей степени. Считаем, что непосредственным сигналом синхронизации является ток, который подается в контур автогенератора вместе с током усилительного элемента. Уравнение, описывающее процессы в данном автогенераторе, легко получить, используя законы Кирхгофа

$$\frac{d^2 u}{d\tau^2} + u = \frac{(\omega_c^2 - \omega_0^2)}{\omega_c^2} u + \varepsilon \frac{\omega_0}{\omega_c} (1 - 2\beta u - 3\gamma u^2) \frac{du}{d\tau} + \varepsilon \frac{KR}{\alpha} \frac{\omega_0}{\omega_c} \frac{di_c}{d\tau},$$

где ε – малый параметр; $\tau = \omega_c t$ – безразмерное время; α, β, γ – коэффициенты, ω_0, R, K – резонансная частота контура автогенератора, его сопротивление и модуль коэффициента положительной обратной связи.

Поскольку интерес представляет только первая и вторая гармоники, то решение его будем искать методом разделения частот. Этот метод использует аналитический сигнал, позволяет постепенно наращивать точность и получать интересные зависимости в наиболее простом виде. Тогда укороченную комплексную моделью автогенераторного следящего фильтра можно представить в виде уравнений (1).

Первое уравнение описывает первую гармоническую составляющую с точностью до величин порядка квадрата малого параметра, второе уравнение описывает вторую гармоническую составляющую с учетом величин порядка квадрата малого параметра. Эта система допускает последовательное решение – вначале решается первое уравнение, а затем второе:

$$\begin{aligned}\frac{d^2 w_1}{d\tau^2} + \frac{\omega_0^2}{\omega_c^2} w_1 &= \varepsilon \frac{\omega_0}{\omega_c} \left\{ \frac{d}{d\tau} \left[\left(1 - \frac{3}{4} \gamma A_1^2 \right) w_1 \right] + \frac{KR}{\alpha} \frac{dw_{c1}}{d\tau} \right\}, \\ \frac{d^2 w_2}{d\tau^2} + \frac{\omega_0^2}{\omega_c^2} w_2 &= \varepsilon \frac{\omega_0}{\omega_c} \left\{ \frac{d}{d\tau} \left[\left(1 - \frac{3}{2} \gamma A_1^2 \right) w_2 - \frac{1}{2} \beta w_1^2 \right] + \frac{KR}{\alpha} \frac{dw_{c2}}{d\tau} \right\}.\end{aligned}\quad (1)$$

Первая гармоническая составляющая сигнала автогенератора

Рассмотрим первое уравнение системы (1). Подставляя выражения для аналитических сигналов $w_1 = A_1 e^{j\varphi_1} e^{j\tau}$ и $w_{c1} = I_{c1} e^{j\varphi_{c1}} e^{j\tau}$, переходим к функциям действительной переменной. Исходя из условий практического использования рассмотрим только стационарный режим. Вводим безразмерную амплитуду первой гармонической составляющей сигнала автогенератора $y = A_1 / A_{10}$. A_{10} – амплитуда первой гармоники сигнала автогенератора в автономном режиме. Тогда укороченные уравнения автогенератора для первой гармонической составляющей его сигнала записываются следующим образом:

$$\begin{aligned}y^3 - y &= \frac{B}{\alpha} \cos \theta^0, \\ \frac{\varepsilon B}{y \alpha} \frac{\omega_0}{\omega_c} \sin \theta^0 &= -\frac{\omega_c^2 - \omega_0^2}{\omega_c^2},\end{aligned}$$

где $\theta^0 = \varphi_1 - \varphi_{c1}$, $B = I_{c1} / I_0$. I_0 – амплитуда первой гармоники тока усилительного элемента автогенератора в автономном режиме.

Решение этой системы позволяет определить величину амплитуды первой гармонической составляющей сигнала синхронизированного автогенератора и сдвига фазы его относительно первой гармоники внешнего сигнала.

Вторая гармоническая составляющая сигнала автогенератора

Рассмотрим второе уравнение системы (1). Подставляя выражения для сигналов $w_{c2} = I_{c2} e^{j\psi_{c2}} e^{j2\tau}$ и $w_2 = A_2 e^{j\varphi_2} e^{j2\tau}$, переходим к функциям действительной переменной.

После несложных преобразований и разделения действительных и мнимых частей, получим систему уравнений, описывающую амплитуду и фазу второй гармоники

$$\begin{aligned}\left(\frac{\omega_0}{\omega_c} - 4 \frac{\omega_c}{\omega_0} \right) A_2 &= \varepsilon \beta A_1^2 \sin(2\varphi_1 - \varphi_2) - 2\varepsilon \frac{KR}{\alpha} I_{c2} \sin(\psi_{c2} - \varphi_2), \\ 2\chi A_2 - \beta A_1^2 \cos(2\varphi_1 - \varphi_2) &+ 2 \frac{KR}{\alpha} I_{c2} \cos(\psi_{c2} - \varphi_2) = 0.\end{aligned}\quad (2)$$

Далее следует учесть величину малого параметра. Если его значение таково, что членами второго уравнения, появившимися в результате второго приближения, можно пренебречь, то математической моделью такого фильтра является система уравнений

$$\left(\frac{\omega_0}{\omega_c} - 4\frac{\omega_c}{\omega_0}\right)A_2 = \varepsilon\beta A_1^2 \sin(2\varphi_1 - \varphi_2) - 2\varepsilon\frac{KR}{\alpha}I_{c2} \sin(\psi_{c2} - \varphi_2),$$

$$-\beta A_1^2 \cos(2\varphi_1 - \varphi_2) + 2\frac{KR}{\alpha}I_{c2} \cos(\psi_{c2} - \varphi_2) = 0.$$

Рассмотрим первый режим работы фильтра, когда $I_{c2} = 0$. Из второго уравнения видно, что $2\varphi_1 - \varphi_2 = \pi/2$. Первое уравнение позволяет определить интересующую величину

$$\frac{A_2}{A_1} = \varepsilon \frac{\beta y A_{10}}{\frac{\omega_0}{\omega_c} - 4\frac{\omega_c}{\omega_0}}.$$

В этом случае вторая гармоника непосредственного сигнала синхронизации не оказывает влияния на выходной сигнал следящего фильтра, и амплитуда второй гармоники его определяется только автогенератором.

Рассмотрим далее второй режим работы следящего фильтра. Учтем теперь вторую гармоническую составляющую непосредственного сигнала синхронизации $I_{c2} = 4I_{c1}A_2/A_1$:

$$\frac{A_2}{A_1} = \varepsilon \frac{\beta y A_{10} \sin(2\varphi_1 - \varphi_2)}{\left(\frac{\omega_0}{\omega_c} - 4\frac{\omega_c}{\omega_0}\right) + 8\varepsilon \frac{B}{\alpha y} \sin(\psi_{c2} - \varphi_2)}. \quad (3)$$

Теперь амплитуда второй гармоники выходного сигнала следящего фильтра зависит от амплитуд вторых гармоник непосредственного сигнала синхронизации и сигнала генератора, а также фазовых соотношений между ними. Однако, с практической точки зрения, интерес представляет максимальное значение этого параметра, которое не является постоянной величиной, а меняется в зависимости от сложившихся фазовых соотношений. Числитель выражения (3) максимален при $\sin(2\varphi_1 - \varphi_2) = 1$. Знаменатель должен удовлетворять неравенству

$$\left(\frac{\omega_0}{\omega_c} - 4\frac{\omega_c}{\omega_0}\right) + 8\varepsilon \frac{B}{\alpha y} \sin(\psi_{c2} - \varphi_2) < 0,$$

поскольку $\beta < 0$. Выражение $\left(\frac{\omega_0}{\omega_c} - 4\frac{\omega_c}{\omega_0}\right) < 0$ в полосе синхронизации. Аргумент тригонометрической функции включает сдвиги фаз фильтров с фиксированной полосой пропускания, входящих в блоки формирования нелинейной обратной связи. Выражение (3) может принимать большие значения из-за влияния этих фазовых сдвигов, которые должны учитываться при разработке следящего фильтра.

Отношение амплитуд второй и первой гармоник следящего фильтра может существенно возрасти при приближении частоты внешнего сигнала синхронизации к нижней границе полосы синхронизации. Это связано с тем, что при этом частота первой гармоники сигнала автогенератора удаляется от резонансной частоты контура и амплитуда ее уменьшается. Частота второй гармоники сигнала автогенератора наоборот приближается к резонансной частоте контура, и амплитуда ее возрастает. Однако в этом случае существенную роль играют фазовые соотношения. При возникновении баланса фаз для второй гармоники в петле нелинейной обратной связи ее амплитуда может резко увеличиться, поскольку относительная амплитуда второй гармоники непосредственного сигнала синхронизации больше одноименного параметра для сигнала автогенератора.

Полученные до сих пор соотношения относятся к случаю, когда математическая модель описывает синхронизированный автогенератор с точностью до величин порядка малого параметра. Если малый параметр недостаточно мал, то вторую гармоническую составляющую

следящего фильтра необходимо рассматривать с точностью до величин порядка квадрата малого параметра, т.е. необходимо исходить из системы (2). Для первого режима эти уравнения имеют вид

$$\begin{aligned} \left(\frac{\omega_0}{\omega_c} - 4\frac{\omega_c}{\omega_0}\right)A_2 &= \varepsilon\beta A_1^2 \sin(2\varphi_1 - \varphi_2), \\ 2\chi A_2 &= \beta A_1^2 \cos(2\varphi_1 - \varphi_2). \end{aligned}$$

Решая эти уравнения, приходим к выражению

$$\frac{A_2}{A_1} = -\varepsilon \frac{\beta \gamma A_{10}}{\sqrt{\left(\frac{\omega_0}{\omega_c} - 4\frac{\omega_c}{\omega_0}\right)^2 + (2\varepsilon\chi)^2}},$$

где значение квадратного корня берется со знаком “плюс”.

При рассмотрении второго режима представим уравнения (2) в виде

$$\begin{aligned} \left(\frac{\omega_0}{\omega_c} - 4\frac{\omega_c}{\omega_0}\right)A_2 + 2\varepsilon\frac{KR}{\alpha}I_{c2} \sin(\psi_{c2} - \varphi_2) &= \varepsilon\beta A_1^2 \sin(2\varphi_1 - \varphi_2), \\ 2\chi A_2 + 2\frac{KR}{\alpha}I_{c2} \cos(\psi_{c2} - \varphi_2) &= \beta A_1^2 \cos(2\varphi_1 - \varphi_2). \end{aligned}$$

Возводя в квадрат левые и правые части уравнений, складывая их и учитывая, что

$$I_{c2} = 4I_{c1} \frac{A_2}{A_1}, \text{ а } 2\frac{KR}{\alpha}I_{c2} = 8\frac{B}{\alpha\gamma}A_2,$$

после несложных преобразований получаем

$$\frac{A_2}{A_1} = -\varepsilon \frac{\beta \gamma A_{10}}{\sqrt{\left(\frac{\omega_0}{\omega_c} - 4\frac{\omega_c}{\omega_0}\right)^2 + (2\varepsilon\chi)^2 + \left(8\varepsilon\frac{B}{\alpha\gamma}\right)^2 + 16\varepsilon\frac{B}{\alpha\gamma}\left\{\left(\frac{\omega_0}{\omega_c} - 4\frac{\omega_c}{\omega_0}\right)\sin(\psi_{c2} - \varphi_2) + 2\varepsilon\chi\cos(\psi_{c2} - \varphi_2)\right\}}}$$

В этом выражении, так же как и ранее, результат вычисления квадратного корня надо брать со знаком “плюс”. Уточнение интересующего параметра не устранило зависимость его от фазовых соотношений в петле нелинейной обратной связи при работе во втором режиме.

Заключение

Использование нелинейной обратной связи позволяет в еще большей степени реализовать потенциальные возможности автоколебательных систем. Ранее проведенные исследования имели своей целью определение закономерностей влияния этой обратной связи на сдвиг фазы сигнала синхронизированного автогенератора относительно внешнего сигнала синхронизации. Влияние нелинейной обратной связи на спектр сигнала автогенератора при полигармонической синхронизации не рассматривалось.

Данное исследование позволило установить, что предложенная нелинейная обратная связь может использоваться в автогенераторных следящих фильтрах. Она дает возможность исключить влияние высших гармоник внешнего сигнала синхронизации на спектральный состав сигнала автогенератора, что увеличивает его избирательность.

Список литературы: 1. *Самойленко Ю.И.* Избирательные свойства автоколебательной системы, синхронизированной гармоническим сигналом // Радиотехника и электроника. – 1959. – №1. – С. 39-42. 2. *R.V. Khokhlov.* A Method of Analysis in the Theory of Sinusoidal Self-Oscillations // IRE Transactions on Circuit Theory. – 1960. – Vol. CT-7, № 4. – P. 398-413. 3. *C.L. Ruthroff.* Injection-Locked Oscillator FM Receiver Analysis // The Bell System Technical Journal. – 1968. – № 7. – P. 1653-1661. 4. *Toyosaku Isobe.* Power Amplification for FM and PM Signals with Synchronized IMPATT Oscillators // IEEE Trans. – 1970. – Vol. MTT-18, №11. – P. 906- 911. 5. *K. Daikoku, Y. Mizushima.* Properties of Injection Locking in the non-linear oscillator // International Journal of Electronics. – 1974. – Vol. 31, №3. – P. 279-292. 6. *Карпов В.В., Квасов М.Е.* Усилительные свойства синхронизированного автогенератора // Вестн. Моск. ун-та. – 1978. – Сер.3. Физика, астрономия. – Т. 19, № 3. – С. 116-118. 7. *M.K. Kazmierczuk, V.G. Krizhanovskii, J.V. Rassokhina, D.V. Chernov.* Injection-Locked Class-E Oscillator // IEEE Trans. – 2006. CAS- I. – Vol. 53, № 6. – P. 1214-1222. 8. *Рапин В.В.* Формирование фазовой обратной связи в неавтономных квазигармонических динамических системах // Радиотехника. – 2002. – Вып. 130. – С. 178-181.

Украинская инженерно-педагогическая академия

Поступила в редколлегию 12.07.2011

ОБРАБОТКА РАДИОЛОКАЦИОННЫХ СИГНАЛОВ В ПАРАЛЛЕЛЬНЫХ ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМАХ

Введение

Радиолокационные системы применяются для измерения координат, скоростей и ускорений различных объектов, а также для бесконтактного зондирования атмосферы, поверхности суши и воды. Для ряда применений требуется высокий темп выдачи получаемых результатов. Распространенным подходом к реализации систем цифровой обработки радиолокационных сигналов является разбиение последовательности операций на ряд относительно несложных действий, каждое из которых выполняется отдельным сигнальным процессором либо программируемой логической матрицей. Такое решение обеспечивает необходимое быстродействие, однако время разработки такой системы и ее себестоимость значительны.

Несмотря на интенсивное развитие вычислительной техники, производительности центральных процессоров (ЦП) персональных компьютеров до сих пор недостаточно для реализации всех процедур обработки радиолокационных сигналов с приемлемой скоростью. Невозможность создания существенно более производительных процессоров привела к появлению систем параллельной обработки на базе нескольких ЦП (многопроцессорные системы), ЦП с несколькими арифметико-логическими устройствами и ЦП с несколькими ядрами (многоядерные ЦП), а также специализированных сопроцессоров, рассчитанных на быстрое выполнение определенного набора действий.

Применение многопроцессорных вычислительных систем ставит дополнительную задачу при разработке алгоритмического и программного обеспечения обработки радиолокационных сигналов. Для эффективного использования имеющихся вычислительных ресурсов, необходимо разделить процедуру обработки на ряд независимых операций, которые могут проходить одновременно. В статье рассматриваются методы обработки радиолокационных сигналов на базе систем параллельной обработки. В качестве вычислительных устройств рассмотрены четырехъядерные ЦП современных персональных компьютеров, а также графические процессоры (ГП) фирмы NVIDIA, допускающие проведение математических расчетов со значительной производительностью. Применение распространенных комплектующих позволяет реализовать достаточно низкую стоимость системы обработки и при этом получить высокую производительность.

Постановка задачи

Принцип действия радиолокационных систем вертикального зондирования атмосферы (РЛС ВЗ) основан на регистрации сигналов, рассеянных неоднородностями коэффициента диэлектрической проницаемости атмосферы [1]. Измерение параметров рассеянных сигналов позволяет оценить динамические параметры атмосферы, в частности направление и скорость ветра. РЛС ВЗ обеспечивают построение профиля скорости ветра по сигналам, рассеянным неоднородностями атмосферы (в частности, неоднородностями диэлектрической проницаемости), образование которых обусловлено неоднородным нагревом подстилающей поверхности [1]. После предварительного накопления рассеянного сигнала осуществляется спектральный анализ, результатом которого является оценка спектральной плотности мощности (СПМ) сигнала. Если отношение сигнал/шум недостаточное, далее производится некогерентное накопление спектров.

При параметризации происходит оценивание информативных параметров рассеянного сигнала – доплеровского сдвига центральной частоты, а также ширины спектра и мощности рассеянного сигнала. Доплеровский сдвиг частоты обусловлен переносом турбулентности

как целого преобладающим ветром и является искомым параметром. Ширина спектра зависит от интенсивности турбулентных процессов в импульсном объеме.

Методы параметризации принято разделять на параметрические и непараметрические. К параметрическим относятся методы, основанные на априорной информации и форме и параметрах СПМ рассеянного сигнала [1]. В литературе приводятся сведения о том, что форма спектра рассеянного сигнала сходится к функции Гаусса с увеличением времени накопления [3]. На этих предпосылках основан метод наименьших квадратов (МНК) [1, 2].

Ранее проведенные исследования [4] позволяют заключить, что методы параметризации на основе метода наименьших квадратов обеспечивают наименьшую величину погрешностей среди применяемых в РЛС ВЗ методов. Кроме того, процедура параметризации по затратам вычислительных ресурсов многократно превосходит остальные процедуры обработки сигналов. В связи с этим, темп выдачи результатов системой может быть повышен за счет оптимизации этой процедуры.

Введем обозначения: g – модель спектральной плотности мощности (СПМ) рассеянного сигнала, y – СПМ рассеянного сигнала, k – число точек в СПМ. Для методов наименьших квадратов процесс параметризации сводится к минимизации невязки, записываемой как

$$e(\psi_1 \dots \psi_N) = \sum_{i=1}^k (y_i - g(i, \psi_1 \dots \psi_N))^2.$$

Поскольку, по результатам натурных экспериментов [3], форма СПМ рассеянного сигнала сходится к гауссовой с ростом времени накопления, то в качестве модели применяем функцию Гаусса:

$$g(i, \psi_1, \psi_2) = \exp\left(-\frac{(i - \psi_1)^2}{2\psi_2}\right)$$

В данном случае физический смысл параметров модели таков: ψ_1 – центр тяжести спектра (оценка доплеровского сдвига частоты рассеянного сигнала f_0), ψ_2 – оценка ширины спектра рассеянного сигнала Δf .

Таким образом, задача параметризации спектров рассеянных сигналов сводится к отысканию минимума целевой функции двух переменных при выполнении ограничений. По принципу действия методы минимизации можно разделить на две категории – прямые (используют только значения целевой функции) и косвенные (используют производные целевой функции) [5]. Косвенные методы обычно сходятся за меньшее число итераций, однако предъявляют требования к целевой функции, в частности требуют ее дифференцируемости. Кроме того, результат косвенных методов может сходиться к точкам перегиба целевой функции вместо ее глобального минимума, что приведет к промахам в результатах. Это обуславливает целесообразность применения прямых методов. Большинство прямых методов, в частности метод покоординатного спуска [5], используют процедуру отыскания минимума функции одной переменной. При этом минимизация проходит в несколько этапов, во время каждого из которых определяется минимум сечения целевой функции по одной из искомым переменных. Рассмотрим примеры регистраций спектров рассеянных сигналов и соответствующих сечений целевых функций параметризации.

В случае параметризации данных, полученных при малом интервале осреднения (рис. 2, а) получаются целевые функции с локальными минимумами (рис. 2, б) и с меньшей крутизной (рис. 2, в). Это способствует появлению промахов при оценивании параметров сигнала методами, использующими сокращенные процедуры минимизации. В условиях сложной формы целевой функции единственным методом её минимизации, обеспечивающим безусловную сходимость к глобальному минимуму, является метод прямого вычисления целевой функции во всех точках сетки. Этот метод редко применяется на практике из-за значительных вычис-

лительных затрат. Вместе с тем, в параллельных вычислительных системах он может быть реализован очень эффективно, так как вычисления функции в разных точках сетки полностью независимы друг от друга и могут проводиться одновременно. В дальнейшем в статье рассматриваются два метода параметризации – с полным вычислением целевой функции (обозначен как метод 1) и метод покоординатного спуска (метод 2).

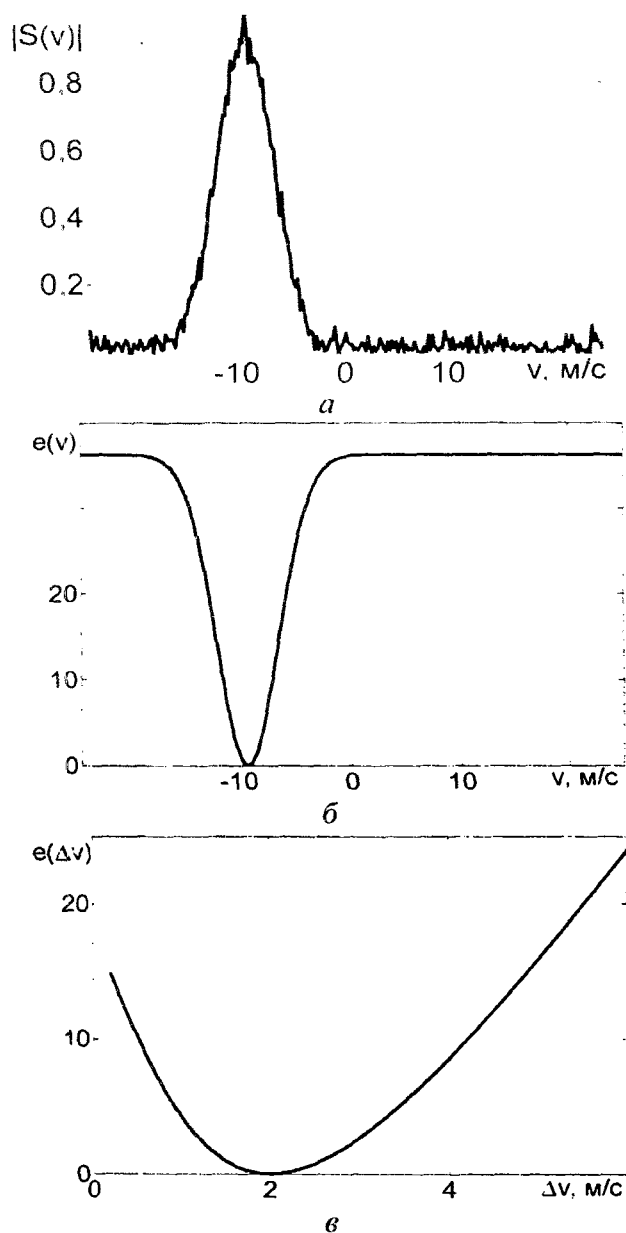


Рис. 1. Спектр рассеянного сигнала, полученный при времени осреднения 20 секунд (а), а также сечения целевой функции по v_0 (б) и Δv (в)

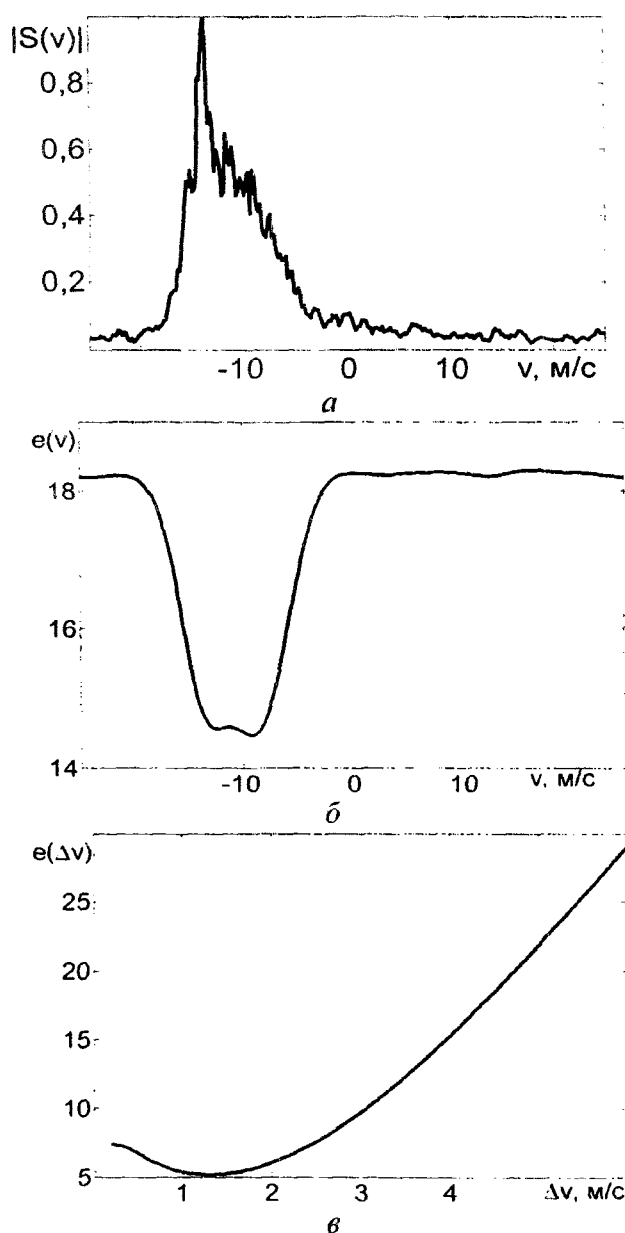


Рис. 2. Спектр рассеянного сигнала, полученный при времени осреднения 1 секунда (а), а также сечения целевой функции по v_0 (б) и Δv (в)

Точностные характеристики методов параметризации получены путем имитационного моделирования. Проводится сопоставление получаемых оценок значений параметров с заданными в модели. Постановку модельного эксперимента иллюстрирует рис. 3.

В данной статье использована две модель рассеянного сигнала, основанная на методе «блестящих точек». При этом имитируется процесс рассеяния радиоволн неоднородностями атмосферы. Рассеянный сигнал на входе приемного устройства определяется как суперпозиция сигналов, рассеянных отдельными точечными отражателями в составе импульсного объема [6]. Моделирование проводилось для следующих условий: диапазон скоростей ветра

± 25 м/с, отношение сигнал/шум $-20 \dots +30$ дБ. Отдельно рассмотрены случаи со временем накопления спектров 20 с и 1 с.

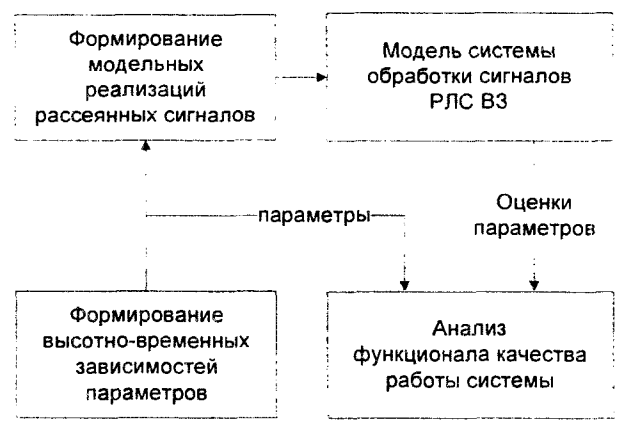


Рис. 3. К пояснению постановки модельного эксперимента

При анализе точностных характеристик методов параметризации используются две метрики погрешностей: среднеквадратическое отклонение (СКО) оценки и среднее по модулю отклонение (СМО) оценки. Обозначим через ψ истинное значение оцениваемого параметра, через ψ' – получаемую оценку, а через N – число измерений. Тогда, среднеквадратическое отклонение оценки

$$\sigma(\psi) = \sqrt{\frac{1}{N-1} \sum_{i=1}^N (\psi - \psi')^2} . \tag{3}$$

Полученные СКО оценок сопоставим с границей Рао–Крамера для измерения неэнергетических параметров [7]: $\sigma^2(\psi) = -\frac{1}{q^2 F''(\psi_0)}$, где $F''(\psi_0)$ – вторая производная автокорреляционной функции по оцениваемому параметру. Отсюда

$$\sigma_{PK}(\psi) = \sqrt{-\frac{1}{q^2 F''(\psi_0)}} . \tag{4}$$

Средний модуль отклонения: $M(\psi) = \frac{1}{N} \sum_{i=1}^N |\psi - \psi'|$. Также примем следующие обозначения: пусть ε – предельно допустимое отклонение оценки параметра ψ , то есть предполагается, что

$$M(\psi) \leq \varepsilon . \tag{5}$$

Поскольку результат оценивания параметра в присутствии шумов является случайной величиной, то (5) в общем случае выполняется не для всех результатов, а для некоторой их части:

$$D(\varepsilon) = \frac{n\{M(\psi) \leq \varepsilon\}}{N} . \tag{6}$$

Величина, обратная (6), показывает вероятность промахов при измерениях для заданного предельного отклонения оценки:

$$C(\varepsilon) = \frac{100}{D(\varepsilon)} . \tag{7}$$

Основные положения

На рис. 4 – 9 приведены результаты моделирования. Графики для ЦП и ГП отдельно не приводятся, поскольку отклонения результатов при реализации одного и того же метода на разных вычислительных устройствах отличаются в пределах погрешности машинного представления данных.

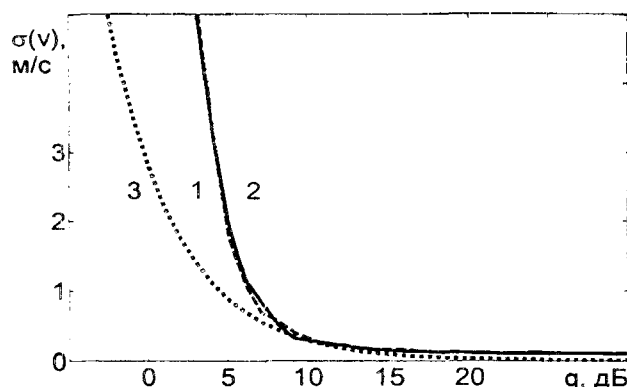


Рис. 4. Зависимость СКО оценок скорости ветра от отношения сигнал/шум

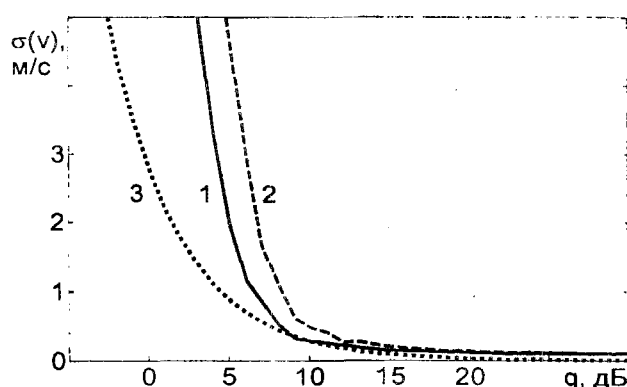


Рис. 5. Зависимость СКО оценок скорости ветра от отношения сигнал/шум

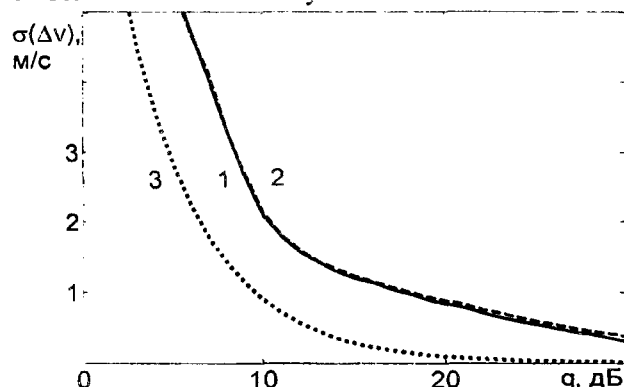


Рис. 6. Зависимость СКО оценок ширины спектра сигнала от отношения сигнал/шум

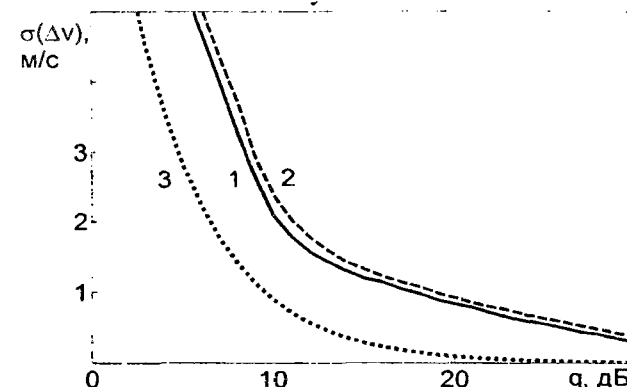


Рис. 7. Зависимость СКО оценок скорости ветра от отношения сигнал/шум

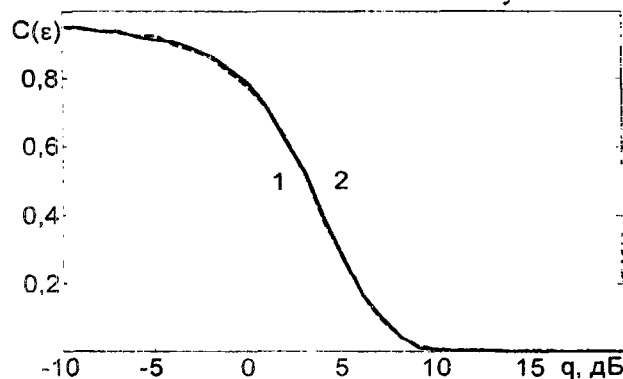


Рис. 8. Зависимость вероятности промахов оценивания скорости ветра от отношения сигнал/шум

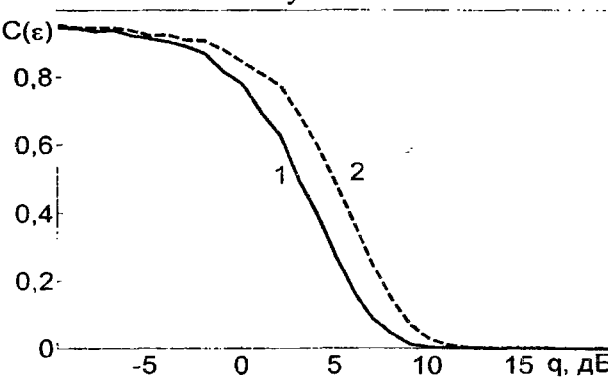


Рис. 9. Зависимость вероятности промахов оценивания скорости ветра от отношения сигнал/шум

На рис. 4, 6, 8 приведены результаты оценок для времени накопления спектров 20 с, а на рис. 5, 7, 9 – для времени накопления 1 с. Для вероятностных характеристик принято пороговое значение ошибки 1 м/с. Цифрой 1 обозначены результаты параметризации методом прямого вычисления целевой функции, 2 – методом покоординатного спуска, 3 – граница Рао – Крамера.

Для случая времени осреднения 20 с, результаты параметризации обоими методами совпадают (рис. 4, 6, 8). Таким образом, подтверждается безусловная сходимость метода покоординатного спуска к глобальному минимуму целевой функции, при отсутствии локальных минимумов.

Для случая времени осреднения 1с (рис. 5, 7, 9), результаты методов параметризации различаются. Метод прямого вычисления целевой функции оказывается более точным, в особенности при низких отношениях сигнал-шум. Это обусловлено появлением локальных минимумов целевой функции и промахами при её минимизации. Вероятность промахов при параметризации тем ниже, чем меньше отклонения формы спектра рассеянного сигнала от функции Гаусса. Таким образом, при параметризации одномодовых спектров, осредненных за десятки секунд и более, метод 2 дает приемлемые результаты. При наличии многомодовых спектров рассеянных сигналов точность оценивания параметров сигнала методом прямого вычисления целевой функции выше, чем методом покоординатного спуска. Метод прямого вычисления значений целевой функции имеет преимущество перед оптимизированными методами минимизации при зондировании атмосферы с высоким темпом выдачи результатов.

Рассмотрим вопрос аппаратурной реализации методов обработки. В табл. 1 приведены конфигурации тестовых систем. Для графических процессоров (ГП) приведен объем локальной видеопамяти.

Таблица 1

Процессор	Число ядер	Тактовая частота, МГц	Пиковая вычислительная мощность, ГФлоп/с	Объем ОЗУ	Пиковая пропускная способность ОЗУ, Гбайт/с	Тип
Intel Q9400	4	2660	42,56	4096 Мб	12,8	ЦП
G86	16	900	43,2	256 Мб	12,8	ГП
GT216	24	1100	79,2	1024 Мб	25,3	ГП
G215	96	1340	386	512 Мб	54,4	ГП
G94	64	1625	312	512 Мб	57,6	ГП
G92	128	1836	705	512 Мб	70,4	ГП
GF110	480	1464	1405	1280 Мб	152	ГП

Архитектура ГП имеет ряд особенностей, которые следует учитывать при разработке программного обеспечения [8]:

1. В составе ГП имеется набор арифметико-логических устройств (АЛУ), каждое из которых может использоваться для вычислений. Каждое из АЛУ имеет отдельную кэш-память небольшого объема и набор регистров.
2. Видеокарта имеет в своем составе значительный объем быстродействующего ОЗУ (в современных моделях – сотни мегабайт). Эту память можно использовать для хранения исходных данных, результатов расчетов и временных данных.
3. Видеокарта имеет доступ в ОЗУ системы через шину. Пропускная способность шины значительно меньше пропускной способности локальной видеопамяти.

Полностью задействовать вычислительные ресурсы ГП можно следующим образом:

1. Программа должна допускать параллельное выполнение однотипных инструкций над разными данными.
2. Исходные данные должны быть предварительно загружены в видеопамять.
3. Операции ввода-вывода должны происходить одновременно с вычислениями.

Программы, использованные для сравнительного анализа в рамках статьи, написаны на языке C++, и скомпилированы Visual Studio 2008 Express Edition с использованием ПО NVIDIA CUDA Toolkit для поддержки вычислений на базе видеопроцессоров. Для версий

программ, рассчитанных на исполнение на ЦП, использована явная многопоточность, реализованная с помощью OpenMP. При этом на разных ядрах ЦП выполняются операции с разными частями массива данных. При разработке программ для ГП дополнительно приняты меры к минимизации числа операций обмена данными между ОЗУ системы и ОЗУ видеоадаптера, поскольку такие операции проходят через относительно медленную шину соединения. Оценки времени выполнения процедур параметризации при различных размерах выборки приведены в табл. 2. Для РЛС ВЗ атмосферного приграничного слоя, требования к временному и высотному разрешению приводят к предельному времени параметризации порядка 25 мс [9]. Результаты параметризации методом покоординатного спуска для многопоточных конфигураций не приведены, поскольку тесты показали неэффективность параллельного исполнения этой процедуры.

Таблица 2

		Время вычислений, мс							
		Метод прямого вычисления весаевой функции				Метод покоординатного спуска			
		64	128	256	512	64	128	256	512
ЦП	1 поток	4.030	31.650	264.230	2240.520	0.266	0.847	3.119	12.203
	2 потока	3.020	18.520	145.650	1262.240	-	-	-	-
	3 потока	3.190	14.120	108.120	927.590	-	-	-	-
	4 потока	2.980	12.440	97.390	773.400	-	-	-	-
ГП	G86	1.625	10.875	66.797	695.844	-	-	-	-
	G94	1.030	5.763	31.584	178.087	-	-	-	-
	G92	1.641	5.594	23.562	113.922	-	-	-	-
	G215	0.966	3.535	20.194	142.613	-	-	-	-
	GT216	0.937	4.860	34.716	272.245	1.903	5.981	20.433	79.107
	GF110	0.210	0.52	2.120	14.630	-	-	-	-

На рис. 10 приведены оценки времени выполнения параметризации на ЦП, а на рис. 11 – на ГП. В табл. 3 приведены результаты оценки эффективности многопоточного исполнения программы на ЦП. Разделение цикла на несколько потоков повышает скорость обработки, однако с увеличением числа потоков эффективность снижается из-за ограничений полосы пропускания ОЗУ

Таблица 3

Число ядер ЦП	Относительная производительность
1	1
2	1.81
3	2.44
4	2.90

Характер зависимости времени выполнения от размера выборки полностью сохраняется. Для различных видеокарт наблюдается некоторое изменение эффективности использования графического процессора. Это связано с недостаточной полосой пропускания видеопамати. Для видеокарты на базе GF110 (кривая 6) производительность существенно выше за счет наличия быстрой кеш-памяти на ядре ГП.

При малых размерах выборки результаты всех ГП фактически одинаковы. Это обусловлено небольшим временем исполнения самой минимизации, и необходимостью обмена данными с ЦП системы через медленную соединительную шину.

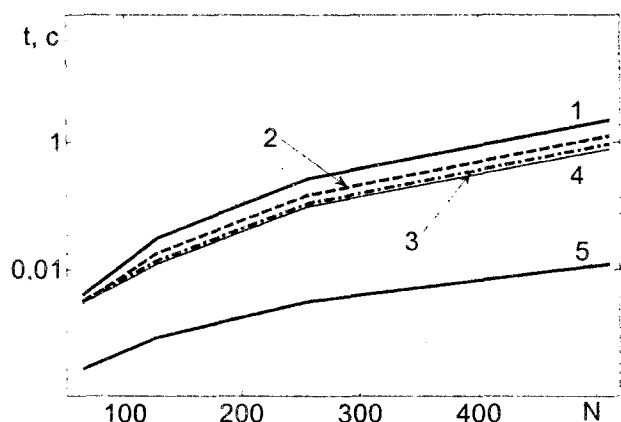


Рис. 10. Время выполнения процедуры параметризации на ЦП (1...4 – метод 1, 1...4 потока, 5 – метод 2)

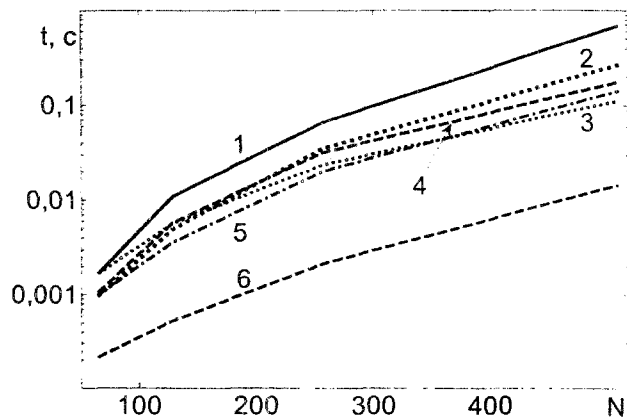


Рис. 11. Время выполнения процедуры параметризации на ГП (1 – G86, 2 – GT216, 3 – G92, 4 – G94, 5 – G215, 6 – GF110)

Выводы

Для спектров рассеянных сигналов, полученных с малым временем накопления, метод прямого вычисления целевой функции обеспечивает меньшую величину погрешностей параметризации по сравнению с методом покоординатного спуска. Реализация этого метода на базе параллельных вычислительных устройств обеспечивает получение требуемого темпа выдачи результатов в РЛС вертикального зондирования атмосферы.

Автор хотел бы выразить признательность коллегам за предоставленные результаты тестирования разработанного ПО на графических процессорах G215, G92, G94 и GF110.

Список литературы: 1. *Дистанционные методы и средства исследования процессов в атмосфере Земли* / Под общ. ред. Б. Л. Кашеева, Е. Г. Прошкина, М. Ф. Лагутина. – Харьков : Харьк. нац. ун-т радиоэлектроники; Бизнес Информ, 2002. – 426 с. 2. *Strauch R. G. Data analyses techniques: spectral processing* // Handbook for middle atmosphere program. – Urbana, Illinois. – 1983. – Vol. 9. – P. 528-531. 3. *Довиак Р.* Доплеровские локации и метеорологические наблюдения. / Р. Довиак, Д. Зрнич. – Л. Гидрометеиздат, 1988. – 503 с. 4. *Литвин-Попович А.И.* Параметризация спектров рассеянных сигналов в РЛС вертикального зондирования атмосферы / А.И. Литвин-Попович, В.Н. Олейников // Радиотехника. – 2008. – Вып. 152. – С. 49-52. 5. *Бахвалов Н.С.* Численные методы. / Н.С. Бахвалов. – М : Наука, 1975. – 630 с. 6. *Островитянов Р.В.* Статистическая теория радиолокации протяженных целей / Р. В. Островитянов, Ф. А. Басалов. – М. : Радио и связь, 1982. – 232 с. 7. *Тихонов В.И., Харисов В.Н.* Статистический анализ и синтез радиотехнических устройств и систем: учеб. пособие для вузов. – М : Радио и связь, 2004. – 608 с. 8. *Xiaoshu Si, Hong Zheng.* High Performance Remote Sensing Image Processing Using CUDA // ISECS, pp.121-125, Third International Symposium on Electronic Commerce and Security, 2010. 9. *Отчет с резолюциями и рекомендациями.* Комиссия по основным системам всемирной метеорологической ассоциации // 23 февр. – 3 марта 2005г., тринадцатая сессия. ВМО № 895.

Харьковский национальный
университет радиоэлектроники

Поступила в редколлегию 15.05.2011

МЕТОДИ БАГАТОПОЗИЦІЙНОЇ МОДУЛЯЦІЇ ШУМОВИХ СИГНАЛІВ**Вступ**

Розвиток елементної бази радіотехнічних пристроїв, а також методів і техніки цифрової обробки сигналів дозволили на новому рівні підійти до розробки систем зв'язку, що використовують хаотичні [1] та шумові [2] сигнали в якості носія інформації.

Широкополосні системи зв'язку, побудовані на базі шумових сигналів з передачею опорного сигналу, мають цілий ряд привабливих особливостей:

- 1) автокореляційний метод прийому;
- 2) високий рівень захищеності інформації на сигнальному рівні;
- 3) стійкість до багатопроменевого розповсюдження та спотворень сигналу в каналах зв'язку із змінними параметрами;
- 4) відсутність необхідності високочастотної та фазової синхронізації;
- 5) відсутність генератора опорного сигналу та системи вимірювання параметрів каналу зв'язку в приймачі системи, відповідне спрощення приймальних пристроїв;
- 6) можливість використання в якості носійної шумових сигналів отриманих від природних джерел (шумових діодів, тощо), що спрощує передавальні пристрої.

Ці особливості були відмічені в роботах [3 – 5]. За певних умов вони можуть бути підставою для надання переваги автокореляційним системам з шумовими сигналами, незважаючи на певні втрати завадостійкості (пов'язані з «зашумленням» опорного сигналу) порівняно з взаємно-кореляційними системами.

В роботі [6] запропонована та досліджена багатопозиційна система зв'язку, побудована на основі бінарної системи, що розглянута в роботах [3] та [5]. Однак в [7] показано, що бінарна система з фазовою маніпуляцією шумового сигналу (ФМШС), запропонована в роботі [2], має кращу завадостійкість порівняно з системою, запропонованою в [3]. Поліпшення завадостійкості відбувається за рахунок зменшення впливу внутрішньо системних завад шляхом змін в структурі сигналу (часового рознесення опорного та інформаційного сигналу).

Отже, для побудови багатопозиційної системи в якості базової слушно обрати бінарну систему з ФМШС, запропоновану в [2].

Постановка задачі

Розглянемо деякі методи багатопозиційної модуляції шумових сигналів, розроблених на базі бінарної ФМШС. Методами імітаційного обчислювального експерименту дослідимо завадостійкість цих методів.

Проведемо порівняльний аналіз завадостійкості та визначимо оптимальний метод модуляції.

Будова та функціонування базової бінарної системи

Символьний інтервал t_s базової бінарної системи зв'язку з ФМШС складається з двох рівновеликих часових проміжків $T = 0.5 \cdot t_s$. На першому проміжку в канал зв'язку випромінюється безпосередньо вихід генератора шуму $x(t)$, $t \in [0, T)$, тут початок відліку часу суміщено з початком символьного інтервалу. Позначимо цей фрагмент сигналу $\bar{x}$.

Тоді на другій половині символьного інтервалу $t \in [T, t_s)$ випромінюється сигнал $\alpha \bar{x}$, який називаємо інформаційним сигналом. Коефіцієнт $\alpha = 1$, якщо передають біт «1», і $\alpha = -1$, якщо передають біт «0».

Таким чином, протягом символного інтервалу випромінюється кортеж $\bar{y} = (\bar{x}, \alpha\bar{x})$.

На вході приймача спостерігається сигнал $\bar{z} = \bar{y} + \bar{n}$, де $\bar{n}$ – білий гауссовий шум (адитивна завада). Нехай $\bar{n}_1$ – фрагмент завад, що відповідає опорному сигналу, а $\bar{n}_2$ – інформаційному. Тоді можна записати $\bar{z} = \bar{y} + \bar{n} = (\bar{x}, \alpha\bar{x}) + (\bar{n}_1, \bar{n}_2) = (\bar{x} + \bar{n}_1, \alpha\bar{x} + \bar{n}_2)$.

На приймальній стороні рішення приймається виходячи із знаку величини

$$r = \langle \bar{x} + \bar{n}_1, \alpha\bar{x} + \bar{n}_2 \rangle = \alpha \langle \bar{x}, \bar{x} \rangle + \alpha \langle \bar{x}, \bar{n}_1 \rangle + \langle \bar{x}, \bar{n}_2 \rangle + \langle \bar{n}_1, \bar{n}_2 \rangle,$$

якщо $r > 0$, то прийнятий біт дорівнює «1», а якщо $r < 0$, то – «0».

Деякі методи багатопозиційної модуляції

Розглянемо п'ять методів багатопозиційної модуляції, що базуються на ФМШС. Структуру модульованого сигналу, згаданого вище, будемо описувати у вигляді кортежу векторів кожен з яких представляє фрагмент сигналу на елементарному для даного типу модуляції часовому слоті довжини T . Такий фрагмент будемо називати елементарним сигналом, а його базу будемо позначати B .

1. Перший тип модуляції базується на використанні одного слота в якості опорного сигналу. Інформаційний сигнал складається з k дублікатів опорного сигналу, кожен з яких незалежно модульований окремим інформаційним бітом. Отже, структуру сигналу передавача на одному символному інтервалі можна зобразити так:

$$(\bar{x}; \alpha_1\bar{x}, \alpha_2\bar{x}, \dots, \alpha_k\bar{x}).$$

Крапка з комою в цьому записі відокремлює опорний сигнал від інформаційного. Таким методом модуляції дозволяє протягом символного інтервалу передавати k біт інформації. Якщо база опорного сигналу $\bar{x}$ залишається незмінною, то імовірність помилки передачі кожного окремого біта в символі залишиться незмінною. Однак час, необхідний для передачі k -бітного символу, дорівнюватиме $t_s = (k+1)T$, проти $t_s = 2kT$ для бінарної системи. Отже, енергетичний виграш (за рахунок збільшення швидкості передачі), отриманий від застосування даного методу модуляції дорівнює

$$\frac{2k}{k+1}$$

і прямує до 2 (або 3.01 дБ) із зростанням k .

2. Другий метод модуляції передбачає ускладнення опорної частини символного інтервалу шляхом дублювання сигналу $\bar{x}$ із елементарного часового слота k разів. Отже, сигнал на символному інтервалі можна подати у вигляді

$$(\underbrace{\bar{x}, \bar{x}, \dots, \bar{x}}_k; \alpha_1\bar{x}, \alpha_2\bar{x}, \dots, \alpha_k\bar{x}).$$

Це дозволяє на приймальній стороні усереднити значення сигналів з різних слотів опорної частини сигналу, що еквівалентно застосуванню фільтра ковзаючого усереднення [8]. В такий спосіб при передачі сигналу на фоні білого гауссового шуму вдасться суттєво покращити відношення сигнал-завада для опорного сигналу.

Механізм цього явища наступний. На приймальній стороні опорний сигнал має вигляд

$$(\bar{x} + \bar{n}_1, \bar{x} + \bar{n}_2, \dots, \bar{x} + \bar{n}_k),$$

де $\bar{n}_1, \bar{n}_2, \dots, \bar{n}_k$ – фрагменти сигналу завад. Після усереднення отримаємо наступну оцінку опорного сигналу

$$\tilde{\bar{x}} = \frac{\bar{x} + \bar{n}_1 + \bar{x} + \bar{n}_2 + \dots + \bar{x} + \bar{n}_k}{k} = \bar{x} + \frac{\bar{n}_1 + \bar{n}_2 + \dots + \bar{n}_k}{k}.$$

Оскільки сигнали $\bar{n}_1, \bar{n}_2, \dots, \bar{n}_k$ статистично незалежні і завади вважаємо стаціонарним процесом з дисперсією σ_n^2 , то дисперсія суми $\bar{n}_1 + \bar{n}_2 + \dots + \bar{n}_k$ дорівнює $k \cdot \sigma_n^2$. Ділення суми на k зменшує дисперсію на k^2 . Таким чином, дисперсія другого доданку попередньої формули σ_n^2/k . Отже, з ростом k відношення сигнал-завада на ділянці опорного сигналу прямує до нуля.

Слід однак відмітити, що виграшу в швидкості передачі порівняно з базовою системою в даному випадку немає. Виграш досягається за рахунок зменшення імовірності помилки передачі при тому самому відношенні сигнал-завада.

Наступні три методи розроблені з метою підвищення відношення сигнал-завада в інформаційній частині сигналу.

3. Структура сигналу в даному випадку аналогічна до 1-го методу з тією особливістю, що коефіцієнти α_j замінені елементами деякого рядка матриці Адамара. Номер рядка визначається поточним інформаційним символом. Рядки матриці використовуються безпосередньо та взяті із знаком мінус. Це дозволяє збільшити об'єм інформації, що передається протягом одного символного інтервалу на 1 *bit*. Таким чином, якщо інформаційна частина сигналу містить k слотів, то символ містить $1 + \log_2 k$ біт, а структуру сигналу можна записати так:

$$(\bar{x}; h_{j1}\bar{x}, h_{j2}\bar{x}, \dots, h_{jk}\bar{x}),$$

де h_{jl} – елемент кодової послідовності, що відповідає символу номер j .

Кодові послідовності слушно будувати так, щоб символи, які мають протилежні бітові представлення, зображувалися протилежними кодовими послідовностями, наприклад для $k = 4$ алфавіт кодових послідовностей наведено в наступній таблиці:

№	Символ	Кодова послідовність	№	Символ	Кодова послідовність
0	000	+1,+1,+1,+1	4	100	-1,+1,+1,-1
1	001	+1,-1,+1,-1	5	101	-1,-1,+1,+1
2	010	+1,+1,-1,-1	6	110	-1,+1,-1,+1
3	011	+1,-1,-1,+1	7	111	-1,-1,-1,-1

При застосуванні даного методу модуляції виграш у швидкості передачі відносно бінарної системи обчислюється так:

$$\frac{2 \cdot (1 + \log_2 k)}{k + 1}.$$

У зв'язку з тим, що логарифм повільно зростаюча функція, то виграш в швидкості передачі спостерігається лише при $k = 2$ та $k = 4$.

4. Даний метод наслідує будову опорного сигналу від методу №2, а будову інформаційного від методу №3. Отже, структура символного інтервалу в цьому випадку буде наступною

$$(\underbrace{\bar{x}, \bar{x}, \dots, \bar{x}}_k; h_{j1}\bar{x}, h_{j2}\bar{x}, \dots, h_{jk}\bar{x}).$$

Як і в другому варіанті модуляції, на приймальній стороні опорний сигнал уточнюється шляхом усереднення по k часових слотах. Відносна швидкість передачі в даному випадку дорівнює

$$\frac{1 + \log_2 k}{k}.$$

Дана система програє бінарній системі в швидкості при $k > 2$.

5. П'ятий метод відрізняється від четвертого тим, що всі слоти опорного сигналу містять в собі різні реалізації шумового сигналу. Відповідно маємо наступну структуру

$$(\bar{x}_1, \bar{x}_2, \dots, \bar{x}_k; h_{j1}\bar{x}_1, h_{j2}\bar{x}_2, \dots, h_{jk}\bar{x}_k).$$

Відносна швидкість передачі обчислюється аналогічно до п. 4.

Рис. 1 дозволяє порівняти швидкість передачі даних для різних типів систем при фіксованих параметрах елементарного сигналу.

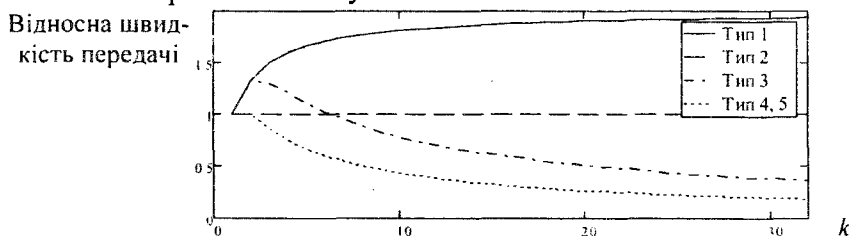


Рис. 1

Дослідження завадостійкості систем

Системи першого типу. Використовуючи результати розрахунків залежності імовірності помилки передачі інформаційного біта P_b від відношення сигнал-завада h^2 отримані для базисної системи і викладені в [7], легко отримати точні теоретичні оцінки потенційної завадостійкості для багатопозиційної системи першого типу. Для цього достатньо помножити параметр h^2 на вираз $\frac{k+1}{2k}$. Результати обчислень проілюстровані на рис. 2. а. Для всіх кривих, зображених на рисунку, база елементарного сигналу $B = 16$.

Для підтвердження адекватності отриманих залежностей на цьому ж рисунку наведені дані, одержані за допомогою серії імітаційних обчислювальних експериментів.

З рисунку видно, що збільшення довжини кортежу k до величин більших ніж 8 не є ефективним, оскільки подальше зменшення імовірності помилки дуже уповільнюється з наближенням до граничного значення $k \rightarrow \infty$. Гранична крива може бути отримана шляхом зміщення вліво на 3 дБ кривої, що відповідає $k = 1$.

Теоретична оцінка потенційної завадостійкості наступних систем шляхом простих аналітичних співвідношень не можлива. Тому в подальшому будемо спиратися лише на результати імітаційних обчислювальних експериментів.

Системи другого типу. Теоретична границя поліпшення завадостійкості систем другого типу при $k \rightarrow \infty$ може бути отримана шляхом зсуву вправо на 3 дБ кривої, яка характеризує потенційну завадостійкість когерентного взаємно-кореляційного прийому протилежних сигналів. В результаті, як видно з рис. 2.б, маємо багато ширший коридор між кривими, що відповідають $k = 1$ та $k \rightarrow \infty$. Як і в попередньому випадку, розрахунки проведено при $B = 16$.

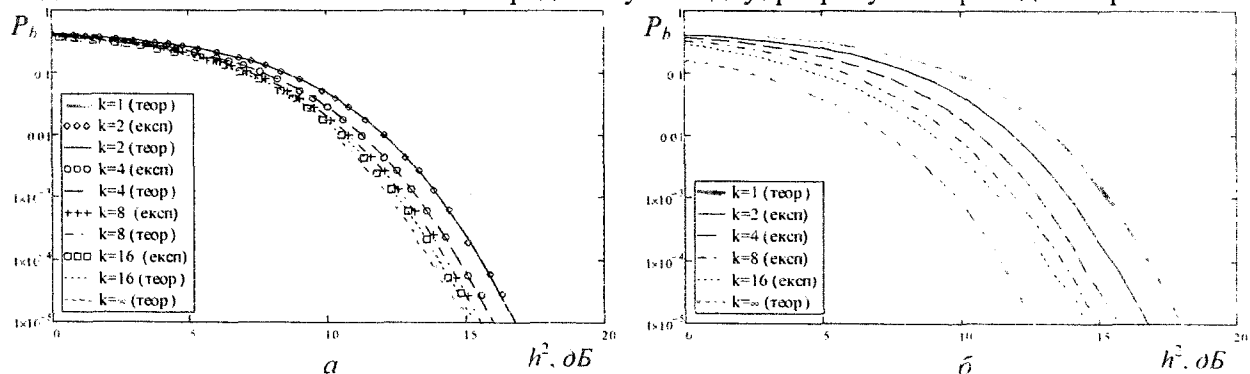


Рис. 2

Завдяки цьому, ускладнення структури сигналу із збільшенням k дає більш значний ефект для поліпшення завадостійкості системи 2-го типу, ніж для системи 1-го типу. Це досягається ціною ускладнення обробки вхідного сигналу на приймальній стороні (приймач системи 2-го типу містить додатковий блок усереднення фрагментів опорного сигналу).

Крім того, для систем другого типу зменшення імовірності помилки із збільшенням k досягається як при великих значеннях відношення h^2 , так і при малих.

Системи третього типу. Показники завадостійкості для систем 3-го типу поліпшуються із зростанням k лише для $k = 2$ та $k = 4$, див. рис. 3, а (при фіксованому $B = 16$). Тому графік функції $P_b(h^2)$ для $k = 4$ визначає межу поліпшення потенційної завадостійкості за рахунок ускладнення структури сигналу для систем даного типу.

Подальше збільшення k веде до втрат завадостійкості при порівнянні кривих на площині (P_b, h^2) , оскільки втрати швидкості передачі не компенсуються збільшенням достовірності передачі при фіксованому відношенні потужностей сигналу і завад.

Отже, системи 3-го типу не складають інтересу для подальших досліджень.

Системи четвертого типу. На рис. 3, б зображено графіки залежності імовірності помилки передачі біта інформації від відношення сигнал-завада для системи 4-го типу. Графіки отримані при $B = 16$.

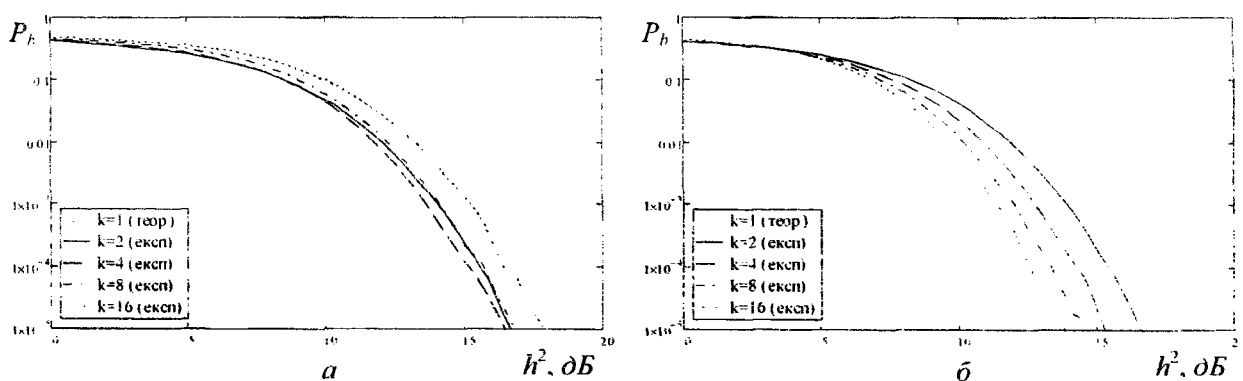


Рис. 3

З рисунку видно, що при малих значеннях h^2 ефект від збільшення k незначний, однак при $h^2 > 4$ системи з більш складною структурою сигналу (при більшому k) отримують значний виграв у завадостійкості. Цей виграв найбільший з усіх систем, що були розглянуті дотепер.

Такий результат досягається одночасним ускладненням обробки як опорної, так і інформаційної частини сигналу.

Системи п'ятого типу. Конструктивно приймач системи 5-го типу більш простий, ніж системи 4-го типу, оскільки він не містить блока усереднення фрагментів опорного сигналу.

Характер зміни функції $P_b(h^2)$ при зростанні k для систем даного типу найбільш складний (див. рис. 4, а при $B = 16$). При $k = 2$ завадостійкість системи залишається незмінною порівняно до бінарної системи. Подальше збільшення k веде до збільшення імовірності помилки для малих h^2 і стрімкого зменшення P_b для великих відношень сигнал-завада ($h^2 > 13$ дБ). Стійке поліпшення завадостійкості із збільшенням k можна отримати, якщо залишати незмінним не базу елементарного сигналу B , а добуток $B \cdot k$ (рис. 4, б).

Це означає, що підвищення завадостійкості по всіх h^2 в даному випадку спостерігається не при збільшенні тривалості сигналу на символному інтервалі (шляхом збільшення кілько-

сті слотів фіксованої довжини), а при розбитті фіксованого символного інтервалу на все дрібніші слоти.

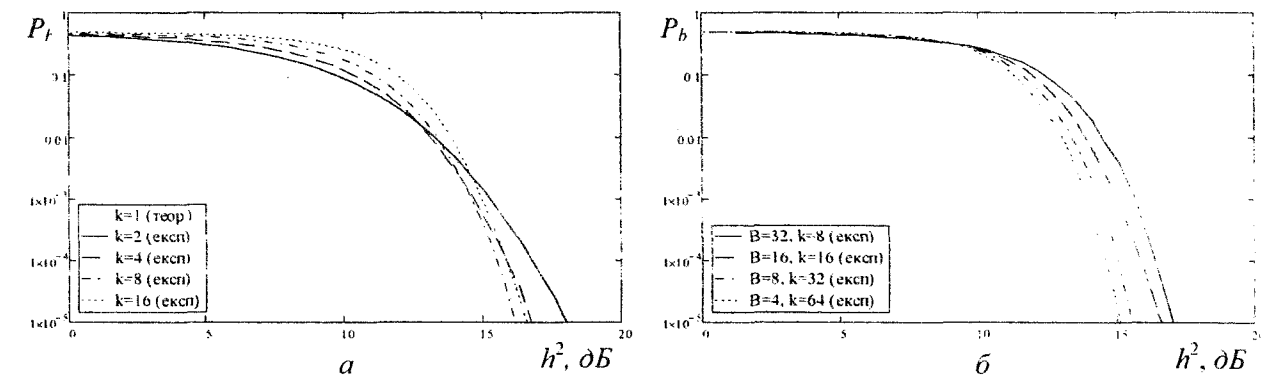


Рис. 4

Вказати однозначно, що система 5-го типу поступається в завадостійкості системі 4-го типу неможливо. Ситуація багато складніша.

Проведемо докладний порівняльний аналіз завадостійкості систем різного типу. Системи 3-го типу, як зазначалось вище, у зв'язку з їх низькою завадостійкістю до розгляду не беруться.

Вибір оптимального методу багатопозиційної модуляції

На рис. 5 подано чотири графіки залежностей P_b від h^2 . Всі графіки отримані при фіксованому значенні добутку $B \cdot k = 256$, який визначає базу інформаційної частини символного інтервалу, при чотирьох різних варіантах розбиття числа 256 на два множники.

Кожен із чотирьох графіків дозволяє порівняти завадостійкості систем різного типу при фіксованих значеннях B та k .

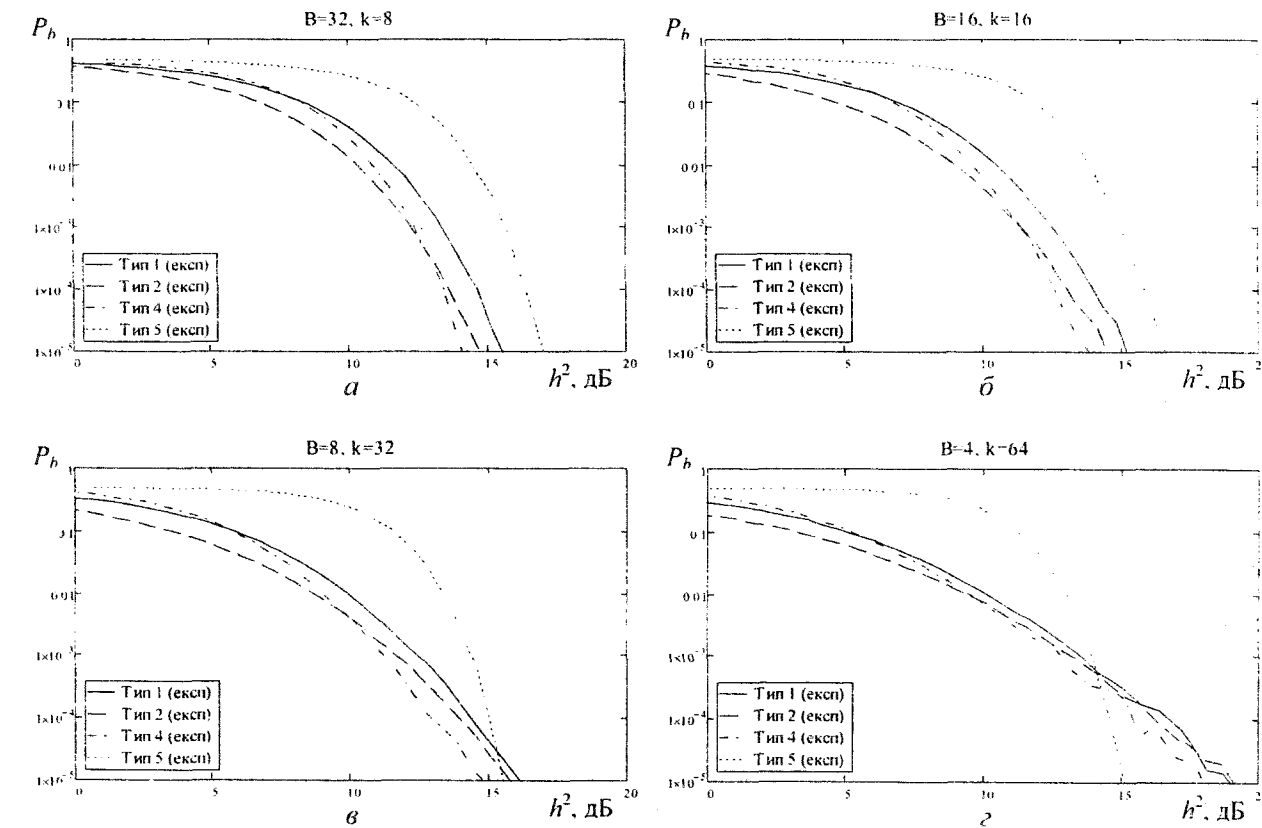


Рис. 5

Аналіз даних, проілюстрованих на рис. 5. дозволяє стверджувати, що при малих значеннях відношення сигнал-завада h^2 найкращі показники завадостійкості мають системи 2-го типу. На другому місці 1-й тип систем, на третьому – 4-й тип, і найгіршими за цих умов є системи 5-го типу. Слід відмітити, що системи 2-го типу мають кращі показники завадостійкості порівняно з системами 1-го типу при будь-яких значеннях h^2 . Причому збільшення бази елементарного сигналу B при фіксованому добутку $B \cdot k$ веде до зростання переваги системи 2-го типу для $h^2 > 5$ дБ.

При $h^2 < 5$ дБ системи 4-го типу поступаються в завадостійкості як системам 1-го, так і 2-го типу. Однак із ростом h^2 імовірність помилки систем даного типу швидко зменшується, і вже на рівні $P_b < 5 \cdot 10^{-4}$ вони отримують перевагу перед системами 1-го і 2-го типу.

Системи 5-го типу поступаються в завадостійкості всім іншим системам при $h^2 < 10$ дБ. При подальшому збільшенні відношення сигнал-завада імовірність помилки таких систем швидко зменшується. Особливо вираженим це явище є для малих значень B та великих k (див. рис. 4, ϵ). За таких умов системи 5-го типу виграють в завадостійкості у всіх інших систем.

Висновки

У роботі запропоновано п'ять методів багатопозиційної модуляції шумових сигналів, отриманих на базі фазової маніпуляції.

Методами імітаційного обчислювального експерименту отримано оцінки потенційної завадостійкості даних методів. Проведено аналіз впливу таких параметрів, як база елементарного сигналу та кількість часових слотів в інформаційній частині сигналу, на завадостійкість системи.

Виконано порівняльний аналіз завадостійкості різних методів багатопозиційної модуляції. Отримано наступні результати:

1. Якщо необхідно забезпечити якомога більшу швидкість передачі даних, то оптимальним вибором є перший тип модуляції. Цей же метод модуляції є найменш затратним з точки зору складності обробки сигналу.
2. Якщо можливо використовувати елементарні сигнали з великою базою, то найкращі результати можна отримати при використанні 4-го типу модуляції. Даний тип модуляції вимагає найбільш складного алгоритму обробки сигналу.
3. Якщо необхідно використовувати елементарні сигнали з порівняно малою базою, то оптимальним варіантом є 5-ий тип модуляції.

Список літератури: 1. Короновский А.А., Москаленко О.И., Храмов А.Е. Скрытая передача информации на основе режима обобщенной синхронизации в присутствии шумов // Журнал технической физики. – 2010. Т.80. – Вып.4. С.1-8. 2. Первунінський С.М., Дідковський Р.М., Метелат В.В., Тобілевич Ю.Є. Математичне моделювання систем зв'язку з кореляційно-часовою модуляцією // Вісник Черкаськ. ун-ту. Серія «Прикладна математика». – ЧНУ. 2006. Вип. 83. – С.112-123. 3. Семенов А.М., Сикарев А.А. Широкополосная радиосвязь. – М : Воениздат, 1970. 4. Бунин С.Г., Войтер А.П. Вычислительные сети с пакетной радиосвязью. – К. : Техника, 1989. 5. Воронин А.А. Шумоподобные сигналы – эффективный метод борьбы с замираниями // Электросвязь. – 1966. – №7. 6. Лега Ю.Г., Первунінський С.М., Гузнін С.С. Дослідження завадостійкості М-позиційного приймача шумових сигналів в каналі з адитивним білим гаусовим шумом // Вісник Нац. ун-ту «Львівська політехніка» // Радіоелектроніка та телекомунікації. – 2009. – № 645. – С.167 -176. 7. Дідковський Р.М. Порівняльний аналіз завадостійкості бінарних систем зв'язку з протилежними шумовими сигналами // Вісник ДУІКТ. – 2010. – Т.8. №4. – С.387-407. 8. Виленкин С.Я. Статистическая обработка результатов исследования случайных функций. – М. : Энергия, 1979.

**ВИБІР ТЕХНОЛОГІЧНО ОБГРУНТОВАНОГО МЕТОДУ
ОЦІНКИ СКЛАДУ ГРУПОВОЇ ЗОСЕРЕДЖЕНОЇ ЦІЛІ**

Групова зосереджена ціль (ГЗЦ) являє собою групу цілей (зазвичай 2 – 4), просторова модель якої менша за імпульсний об'єм РЛС.

Завдання оцінки складу ГЗЦ класифікується як завдання "розрізнення – виявлення" (на відміну від "повного" розрізнення з виміром координат кожної одиночної цілі) і може бути вирішена тільки методами надрелеєвського розрізнення (НРР).

До теперішнього часу розроблена серйозна теоретична база методів НРР, класифікація яких не має чіткого визначення. Тому для аналізу суб'єктивно обрано кілька груп методів, що відрізняються як за часом розробки, так і ідеологічною спрямованістю методів.

Для формулювання цільової установки роботи перед основною частиною аналізу проводиться коротке подання розглянутих методів із узагальненою оцінкою їх реалізації.

Історично першим етапом розробки методів НРР служить теорія оптимального розрізнення, що розроблена Я.Д.Ширманом в 60-х роках. Вона базується на вирішенні завдання розрізнення як оптимального виявлення цілей на фоні близько розташованих заважаючих сигналів однакової структури [1]. Процедура оптимального розрізнення дозволяє одержати оптимальну (за критерієм Крамера – Рао) оцінку координати, яка вимірюється.

Наступним етапом розвитку теорії НРР можна вважати два останні десятиліття, коли поширення отримали методи альтернативного спектрального оцінювання (методи "надрозрізнення"). Основи теорії "надрозрізнення", а також методи, способи й алгоритми обробки сигналів представлені в класичній роботі С.Л. Марпл-Мл [2]. У теорії спектральних методів термін "спектр" розуміється, як сукупність значень лінійного оператора або матриці (в основному кореляційної матриці) сигналів, які спостерігаються.

В останні 3...4 рр. з'явилося цілий ряд публікацій по теорії нових евристичних і оптимізаційних методів НРР, що не належать до класу спектрального оцінювання. Основна ідеологічна лінія нових методів викладена в монографії А.А. Чижова [3] і ряді статей (його й інших авторів).

Принципово відмінними від вище зазначених методів є процедури оцінки складу ГЗЦ на основі методів розпізнавання радіолокаційних портретів цілі. Для них одержання критичних оцінних статистик не вимагає обчислення елементів зворотної кореляційної матриці прийнятих сигналів, а технічна реалізація можлива без застосування багатоелементних антенних решіток. Однак практично реалізовані розробки систем НРР стосовно до завдання розрізнення ГЗЦ авторам не відомі.

Загальним недоліком представлених вище методів НРР є їх явно виражена теоретична спрямованість із акцентом розробок на математичний апарат обчислювальних процедур нехтуючи повною алгоритмічною завершеністю й обґрунтуванням шляхів практичної реалізації. Крім того абсолютна більшість алгоритмів обробки пов'язані з високими вимогами до обчислювальних ресурсів системи, що ставить під сумнів можливість їх реалізації в оглядових РЛС у реальному масштабі часу.

Дана стаття має на меті вибір технологічно обґрунтованих методів НРР на основі результатів моніторингу методів НРР, тобто таких для яких:

- є (або може бути розроблено в подальших дослідженнях) алгоритм технічної реалізації й практичне обґрунтування застосування (навіть до структурних схем);
- забезпечуються низькі вимоги до обчислювальних ресурсів системи, тобто доступної вартості впровадження.

Перед початком аналізу необхідно уточнити моделі ГЗЦ, для яких вирішується поставлене завдання. У більшості публікацій за тематикою НРР при математичному аналізі передбачається довільне число одиночних цілей у складі ГЗЦ із відмінними параметрами. Із практичної точки зору така постановка завдання не є виправданою, тому що можливе число цілей у межах імпульсного об'єму РЛС (з розміром: за дальністю – 250–500 м і лінійним за азимутом в центрі зони – до 2.3–2.6 км) можна очікувати не більше 2–4.

Тому в якості цільових моделей приймаються дві моделі:

- 1) парна ціль (2 літака) з однаковими дальностями,
- 2) ланка (3 цілі) із трикутною геометрією побудови. Ілюстрація обраних моделей представлена на рис. 1 і 2 відповідно.

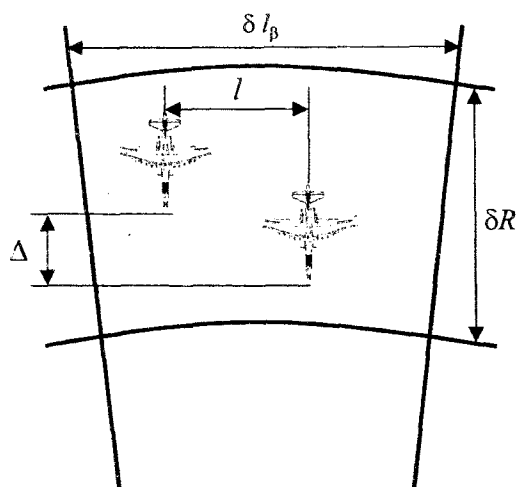


Рис. 1. Модель побудови парної цілі

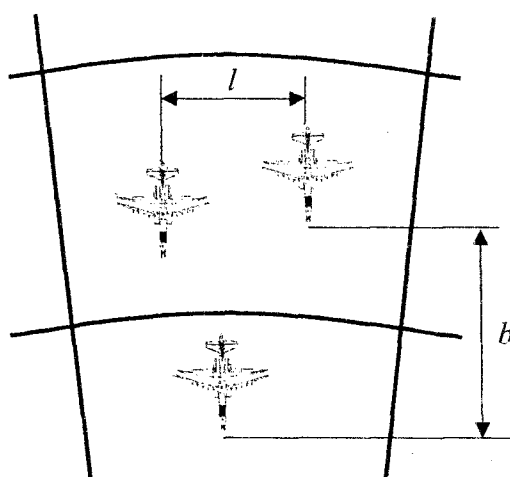


Рис. 2. Модель побудови групової зосередженої цілі за формою ланки із трикутною геометрією

Для першої моделі практично існує незначний розкид дальностей (на рис. 1 позначений Δ). Її величина є випадковою й звичайно не перевищує лінійного розміру літака. Вона не впливає на результати розрізнення цілей, але призводить до зміни параметрів відбитого сигналу за рахунок інтерференції двох луна-сигналів з випадковою початковою фазою відбитих від точкових випромінювачів. Для другої моделі ГЗЦ інтервал між ведучою і веденими цілями (на рис. 2 позначено b) перевищує розрізнення за дальністю δR (це стосується кращих зразків РЛС ППО й усіх нових РЛС із широкосмуговим сигналом). Отже, і в цьому випадку завдання, яке вирішується аналогічне попередньому. Таким чином, еквівалентна модель обраної ГЗЦ являє собою два точкових джерела випромінювання з однаковими параметрами й дальністю, які необхідно розрізнити за азимутом.

Основні висновки з аналізу зазначених вище груп методів НРР представлені нижче.

Методи спектрально-часового аналізу (аналізуються першими так як отримали найбільшу популярність), що одержали назву "методів високого розрізнення", виправдовують свою назву тільки у випадку розрізнення некорельованих сигналів. Алгоритми цих методів (Кейпона, лінійного пророкування, Писаренко, MUSIC і інші) передбачають:

- 1) перехід від вихідних сигналів приймальних каналів до функції $\varphi(A)$ від кореляційної матриці (КМ) цих сигналів (для алгоритму Кейпона – до зворотної КМ, для MUSIC – до власних векторів КМ).

- 2) обчислення проекції, тобто оцінного вектора на підпростір, однозначно пов'язане з $\varphi(A)$.

- 3) вимір параметрів оцінного вектора для пошуку максимуму функції, утвореної від $\varphi(A)$.

Очевидно, що алгоритми методів спектрального аналізу вимагають великого обсягу обчислювальних операцій. Крім того вони спрямовані на вирішення завдання "повного" розрізнення, у той час, коли на сучасному етапі основним проблемним моментом застосування методів НРР є завдання оцінки кількості компонент у спостережуваній суміші сигналів.

"Нові" методи НРР (що публіковались останні кілька років). Вони не належать до методів спектрального оцінювання. Проблема НРР розглядається із принципово інших позицій – як проблема вирішення так званого зворотнього завдання розсіювання. З фізичної точки зору це завдання оцінки портрету групової цілі за прийнятим сигналом. Математична особливість вирішення зворотнього завдання розсіювання полягає в її некоректності, так як розв'язок, що отримується не єдиний й вкрай нестійкий внаслідок впливу шумів.

Базовим напрямком "нових" методів є розробка способів і алгоритмів, що дозволяють у певній мері подолати фактор некоректності.

Найбільш ефективним з даної групи методів є *проекційний метод* вирішення завдання. Принципова особливість методу полягає у використанні проекційної схеми розв'язку операторних рівнянь. У якості математичної моделі портрету цілі використовуються не самі елементи вектора прийнятого сигналу, а їх проекції на деякий пробний простір, який вибирається на основі наявної апіорної інформації. Вибір раціонального вигляду таких просторів практично досить важкий, так як у якості апіорної інформації необхідно задавати форми портретів ГЗЦ.

Відповідь на питання про ступінь технологічної обґрунтованості методу впливає з оцінки виконаних теоретичних розробок [3], автор яких висловився в анотації: "изложение материала несколько абстрактно и кажется оторванным от "квадратиков" и "стрелочек" функциональных схем, а тем более реализации в "железе"".

Метод оптимального алгоритму розрізнення. Завдання оптимального розрізнення двох сигналів формулюється як прийняття рішення про наявність окремо кожного із сигналів у присутності іншого заважаючого сигналу, еквівалентного перешкоді.

Критична статистика розпізнавання полягає в обчисленні кореляційного інтегралу, в якому замість опорного сигналу, що представляє собою копію очікуваного, використовується вирішальна функція, яка виконує завдання придушення заважаючого сигналу, в області перекриття. Ступінь придушення залежить від коефіцієнта кореляції сигналу, що виявляється в цей момент разом з заважаючим.

$$z = y^H w, \quad (1)$$

де z – значення кореляційного інтегралу (КІ); $y = x + v$ – вектор вхідного процесу (x – корисний сигнал, v – шум); w – вирішальна функція КІ, обумовлена виразом:

$$w = x_1 - k \cdot x_2, \quad (2)$$

де $k = 1 - \rho \frac{q_2}{q_2 + 1}$ – коефіцієнт використання енергії сигналу, що виявляється; $q = \frac{E}{N_0}$ – відношення сигнал/шум (індекс опускається, тому що для розглянутої моделі ГЗЦ сигнали мають однакову амплітуду).

Приклад вигляду вирішальної функції для розрізнення нормованих до 1 сигналів прямокутної форми при довільній координаті α з коефіцієнтом перекриття більше 0.5 представлений на рис. 3.

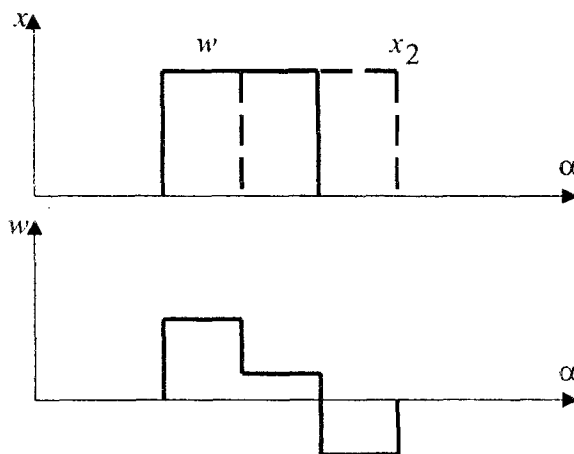


Рис.3. Приклад вигляду вирішальних сигналів прямокутної форми

Алгоритм оптимального розрізнення практично не застосовується у зв'язку з апіорі невідомим ступенем перекриття сигналів, хоча в принципі його реалізація можлива за рахунок багатоканальності побудови системи обробки. Тому не можна повністю погодитися з висновком про непрацездатність алгоритму оптимального розрізнення, що зустрічається в окремих публікаціях (наприклад, [3]).

Значно трудніше реалізувати необхідний алгоритм розрізнення цілей за просторовими координатами, коли формування вирішальної функції повинне здійснюватися антеною системою або застосуванням антенних решіток (АР) із просторовими фільтрами. Але, як стверджується в [1], принцип просторового розрізнення може бути реалізований на деякій лінійній апертурі антени. Залежно від розподілу випромінювачів на апертурі створюється певний розподіл поля. На це поле накладається поле шумів теплового випромінювання, яке можна вважати ізотропним. Інформація про наявність одного з випромінювачів у присутності заважаючого другого, може бути отримана шляхом аналізу напруженості поля як функції двох змінних: часу й координати розкриття. Даний аналіз виконується додатковим інтегруванням по апертурі за допомогою багатoelementної антени або антени з одним виходом, що формує еквівалентну ДН. Мінімум у такий ДН повинен бути спрямований на джерело заважаючого сигналу.

Проведений аналіз показує, що при використанні антени типу АР і багатоканальної цифрової обробки на базі погоджених і режекторних фільтрів можна рекомендувати процедуру обробки, що в деякому наближенні реалізує алгоритм оптимального просторового розрізнення для розробки технологічно прийнятної системи визначення складу виділених моделей ГЗЦ.

Метод розпізнавання радіолокаційних портретів відбитої пачки імпульсів.

У теорії радіолокації розроблені методи розпізнавання радіолокаційних портретів за дальністю й швидкістю. При вирішенні завдання розрізнення ГЗЦ необхідно дослідити можливості розпізнавання цілей за просторовим портретом. У відомих публікаціях авторам не відомі роботи з вирішення такого завдання. Щодо характеристики луна-сигналу ГЗЦ є тільки загальне визначення (наприклад, в [3]): як "некогерентний сигнал с когерентними неортогональними складаючими". У завданні розрізнення за азимутом необхідно дослідити характеристики не одного імпульсу, а всієї пачки відбитих імпульсів у динаміці, тобто в процесі послідовного опромінення імпульсами двох точкових рівноцінних випромінювачів, що рознесені по азимуту на деякий інтервал:

$$\Delta\beta_{12} < \beta_{0,5P}. \quad (3)$$

Аналітичний вираз комплексного вектора, що обгинає луна-пачки ГЗЦ має вигляд:

$$x_{ГЦ} = \sum_{i=1}^{M_1} x_{1i} + \sum_{i=M_1}^M (x_{1i} + x_{2_{M_1-i}}) + \sum_{i=M}^{M_{\Sigma}} x_{2_{M-i}} = y_1 + y_{12} + y_2, \quad (4)$$

де x_1 , x_2 , $x_{ГЦ}$ – вектори відбитих сигналів від першої, другої одиночних цілей і ГЗЦ.

$$x_{1i} = h_i u \cdot B_1; \quad x_{2i} = h_i u \cdot B_2 e^{j\Delta\varphi}, \quad (5)$$

h_i – вагові коефіцієнти імпульсів, обумовлені значенням пеленгаційної характеристики антени $H(\beta)$: $h_j = H(\beta)\delta(\beta - \beta_j)$; $\beta_j = j\Delta\beta_T$, δ – дельта-функція, що дорівнює: $\delta(\beta - \beta_i) = 1$ при $\beta = \beta_i$ і 0 при $\beta \neq \beta_i$, $\Delta\beta_T$ – кутовий інтервал між сусідніми імпульсами.

$$M_1 = \frac{\Delta\beta_{12}}{\Omega_{\beta}} = k \cdot M; \quad k = \frac{\Delta\beta_{12}}{\beta_{0,5P}}; \quad M_{\Sigma} = M(1+k), \quad (6)$$

де Ω_{β} – кутова швидкість обертання антени; B_1 , B_2 – комплексні множники при відбитті від цілей (у зв'язку з однотипними цілями надалі приймаються однаковими й умовно рівними 1); $\Delta\varphi = \frac{2\pi}{\lambda} \cdot \Delta r$ – різниця фаз сигналів за рахунок зсуву по дальності.

Елементи вектора, позначеного y_{12} , являють собою результат інтерференції сигналів, відбитих від одиночних випромінювачів:

$$y_{12} = (h_i + h_{M-i})u \cdot \delta, \quad (7)$$

де δ – коефіцієнт втрат за рахунок інтерференції.

Оскільки фаза є занадто "чутливим" параметром, то навіть при незначному зсуві цілей за дальністю значення $\Delta\varphi$ може приймати значення від 0 до 2π . При розрахунках можна орієнтуватися на усереднене значення множника $e^{j\Delta\varphi}$, який дорівнює характеристичній функції параметром дисперсії $\sigma_{\Delta\varphi}^2$. На рис.4 наведений приклад вигляду пачки відбитих імпульсів ГЗЦ, на якому амплітуди імпульсів, що відповідають y_{12} мають деяке середнє значення (a) – пачка зондувального сигналу, b – вигляд точкових випромінювачів одиночних цілей, c – пачка імпульсів відбитих від ГЗЦ).

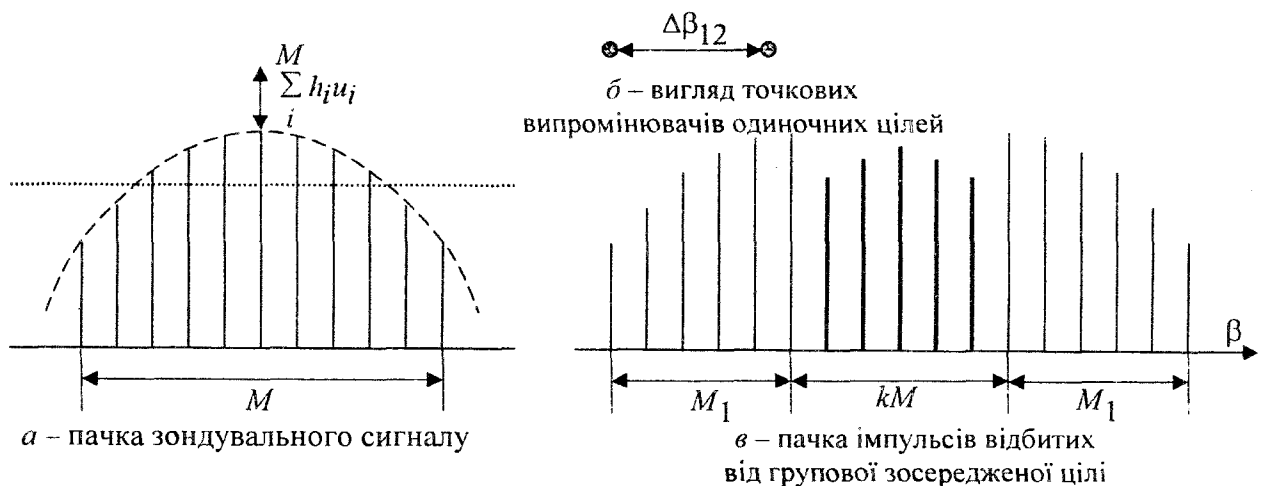


Рис.4. Вигляд пачки імпульсів відбитих від групової зосередженої цілі

З рис.4 випливає, що відмінними ознаками відбитої від ГЗЦ пачки імпульсів є:

- збільшення тривалості пачки й числа імпульсів у ній;
- амплітудні зміни імпульсів пачки.

Стійкою ознакою служить збільшення числа імпульсів пачки, яке може виконувати роль критичного параметра для реалізації завдання розпізнавання ГЗЦ.

Висновки

Технологічно обґрунтованими за результатами аналізу можна вважати:

- метод розпізнавання портрету відбитої пачки імпульсів при обробці вихідного сигналу приймача за спеціально розробленим алгоритмом;
- евристичні методи просторової фільтрації, близькі по фізичній сутності й алгоритмічній процедурі до алгоритму оптимального розрізнення [1], засновані на застосуванні цифрової антенної решітки і системи фільтрів-проекторів з погодженими й режекторними характеристиками.

Список літератури: 1. Ширман Я.Д., Манжос В.Н., Леховицкий Д.И. Некоторые этапы развития теории и техники разрешения радиолокационных сигналов // Радиотехника. – 1997. – №1. – С. 31-42. 2. Марпл-мл. С.Л. Цифровой спектральный анализ и его приложения : пер. с англ. – М. : Мир, 1990. – 584 с. 3. Чижов А.А. Сверхрелеевское разрешение. Т.1, 2. – М. : КРАСАНД, 2010. 4. Бондаренко Б.Ф., Платонов С.Ю., Тимчук В.Ю. Алгоритмы обработки , обеспечивающие высокое разрешение когерентных сигналов // Радиотехника. – 2003. – Т. 46. – С. 61-66.

*Вінницький національний
технічний університет*

Надійшла до редколегії 25.08.2011

МЕТОД РАСЧЕТА ОБЛАСТЕЙ НАИБОЛЕЕ ВЕРОЯТНОГО ПОЯВЛЕНИЯ МЕТЕОРНЫХ СЛЕДОВ, ИМЕЮЩИХ ТОЧКУ ЗЕРКАЛЬНОГО ОТРАЖЕНИЯ

Пропускная способность систем метеорной радиосвязи определяется количеством пригодных для передачи информации метеорных следов и их продолжительностью. Пригодным считается след, линейная электронная плотность которого является достаточной для обеспечения требуемого отношения сигнал/шум при заданных параметрах приемо-передающего оборудования, а его ориентация и протяженность таковы, что на следе наблюдается точка зеркального отражения радиоволны [1]. Протяженность следа, в пределах которой электронная плотность является достаточной для передачи информации с заданным качеством, будем называть «эффективной длиной метеорного следа».

Электронная плотность следа зависит от параметров метеорного тела (массы, скорости, плотности и химического состава) и является функцией высоты [2]. Условие достаточности уровня электронной плотности определяет верхнюю и нижнюю границу метеорной зоны, в пределах которой выполняется условие обеспечения связи. Данные границы и ориентация метеорного следа определяют его эффективную длину.

Точка зеркального отражения на следе образуется, если данный след лежит в плоскости, имеющей точку касания с эллипсоидом вращения, фокусами которого являются пункты передачи и приема информации, и проходит через точку касания [1]. Поскольку радианты метеорных потоков и спорадических метеоров имеют соответствующие вероятностные распределения [3], случайными будут и зенитные углы, а также приведенные азимуты (углы, измеренные относительно оси эллипсоида, а не направления на «север») метеорного следа. При этом расположение и размеры областей наиболее вероятного появления в зоне радиовидимости метеорных следов, обладающих точкой зеркального отражения («горячих областей») будет зависеть от протяженности радиолинии, а также времени года и суток [1].

Учет расположения и размеров «горячих областей» для метеорных потоков и спорадических метеоров позволяет для радиолиний различной протяженности правильно выбрать ориентацию и ширину диаграммы направленности передающих и приемных антенн и, тем самым, обеспечить максимальную пропускную способность систем метеорной радиосвязи.

Цель данной работы – разработка метода расчета областей с наибольшей вероятностью появления метеорных следов, пригодных для передачи информации по радиолиниям различной протяженности.

Для обеспечения статистической однородности оценок вероятности того, что метеороид, попавший на заданный элемент поверхности, образует след, пригодный для передачи информации, верхняя граница метеорной зоны, ограниченная зоной радиовидимости, разделяется на элементы поверхности равной площади с одинаковым расстоянием между центрами [4]. При расчетах метеороиды, попавшие на элемент поверхности, относят к центру данного элемента. Значения вероятностей вычисляются для всех точек в пределах зоны радиовидимости, а точки, для которых вероятности превышают установленное значение, относят к «горячей области».

При вхождении в атмосферу Земли происходит процесс абляции метеороида. Число свободных электронов на единицу длины метеорного следа определяют линейную электронную плотность α [эл/м]. Ее изменение вдоль метеорного следа представлено выражением [2, 5]

$$\alpha(t) = \alpha_{\max} \cos \gamma \cdot z(t), \quad (1)$$

где γ – зенитный угол;

$$z(t) = \begin{cases} \frac{9}{4} e^{-t} \left(1 - \frac{1}{3} e^{-t}\right)^2 & \text{при } -\ln 3 \leq t \leq 1.7 \\ 0 & \text{при } t \leq -\ln 3, t \geq 1.7 \end{cases} \quad (2)$$

В выражении (1) используется значение относительной высоты t , определяемое как

$$t = (h - h_{\max}) / H, \quad (3)$$

где h – высота атмосферы соответствующая точке на следе [км], $h_{\max}$ – высота точки следа с максимальной линейной электронной плотностью $\alpha_{\max}$ [км], $H = 6.4 + 0.09(h - 95)$ – приведенная высота атмосферы [6].

Высота максимума ионизации определяется соотношением [6]

$$h_{\max} = 47.4 + 12.76 \ln v. \quad (4)$$

Максимальная линейная электронная плотность $\alpha_{\max}$ вычисляется по эмпирической формуле [5]

$$\alpha_{\max} = 4.03 \cdot 10^{14} \frac{m(v - 8.15)^3}{H}, \quad (5)$$

где m и v – масса [кг] и скорость [км/с] метеороида при входе в метеорную область.

Объединяя выражения (1) – (5), получим зависимость линейной электронной плотности как функцию высоты:

$$\alpha(h) = 4.03 \cdot 10^{14} \frac{m(v - 8.15)^3}{H} \cdot \cos \gamma \cdot z(t). \quad (6)$$

На рис. 1 приведены графики изменения линейной электронной плотности вдоль метеорного следа, образованного метеороидом массой 0.5 г, входящим в атмосферу со скоростями 40–70 км/с, рассчитанные по формуле (6).

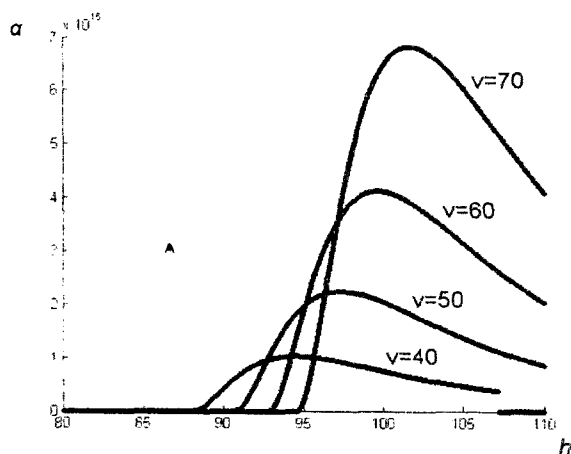


Рис. 1

На основании полученной зависимости электронной плотности как функции от высоты может быть вычислена эффективная длина метеорного следа при заданных параметрах радиолинии.

Эффективная длина метеорного следа определяется линейной электронной плотностью достаточной для обеспечения требуемого отношения сигнал/шум при заданных параметрах приемо-передающего оборудования.

Метеорные следы, электронная плотность которых не превышает $2.4 \cdot 10^{15}$ эл/м, принято называть недоуплотненными. При отражении от такого метеорного следа мощность сигнала на входе приемника равна [1]

$$P_{np} = \frac{P_{nep} G_{nep} G_{np} \sigma \lambda^3 \alpha^2 \cos^2 \mu \exp\left(-\frac{8\pi r_0}{\lambda \sec^2 \theta}\right)}{(4\pi)^3 r_{nep} r_{np} (r_{nep} + r_{np}) (1 + \sin^2 \theta \cos^2 \gamma)}. \quad (7)$$

где P_{nep} – мощность передатчика;

G_{nep}, G_{np} – коэффициенты направленного действия антенн передатчика и приемника;

σ – эффективная поверхность рассеяния электрона (томсоновское сечение рассеяния);

λ – длина волны;

α – линейная плотность электронов;

μ – угол между вектором электрического поля падающей волны и осью следа;

θ – угол падения передаваемой волны на след;

r_0 – начальный радиус метеорного следа;

γ – угол между метеорным следом и плоскостью, проведенной через пункты приема, передачи и отражающую точку метеорного следа;

r_{nep} и r_{np} – расстояния между передающей антенной и отражающей областью и приемной антенной и отражающей областью.

Мощность шума определяется напряженностью поля помех E_n на заданной частоте, которая может быть определена на основании эмпирических данных [7], и действующей высотой приемной антенны h_∂

$$P_{ш} = (E_n h_\partial)^2 / R_{ex}, \quad (8)$$

где действующая высота антенны

$$h_\partial = \frac{\lambda}{\pi} \sqrt{\frac{\eta G_{np} R_{ex}}{120}}, \quad (9)$$

R_{ex} – входное сопротивление приемника, η – коэффициент полезного действия антенны.

Очевидно, что требуемое отношение сигнал/шум на входе приемной системы может быть получено для значений α , превышающих значение $\alpha_{\min}$. Точки пересечения прямой $\alpha_{\min}$ и функции $\alpha(h)$ определяют высоту верхней h_v и нижней h_n границ метеорной зоны $h = (h_v - h_n)$, где обеспечивается необходимый для связи уровень линейной электронной плотности. Зенитный угол γ_z , расстояние ρ от центра Земли до верхней границы метеорной зоны h_v и вычисленная ширина метеорной зоны h определяют эффективную длину метеорного следа $l_{эф}$, в пределах которой электронная плотность следа достаточна для организации связи:

$$l_{эф} = \rho \cos \gamma_z - \sqrt{\rho^2 \cos^2 \gamma_z + h^2 - 2h\rho} \quad (10)$$

На рис. 2 приведена зависимость линейной электронной плотности от высоты, полученная на основании выражения (6) для метеороида массой 0.5 г и скоростью 50 км/с, при которых максимальное значение линейной электронной плотности $\alpha_{\max} = 2.2349 \cdot 10^{15}$. Значение $\alpha_{\min}$ рассчитано по формуле (7) для системы метеорной связи со следующими параметрами: $P_{nep} = 1$ кВт; $G_{nep} = G_{np} = 20$ дБ; $\lambda = 7.5$ м; длина трассы $s = 1000$ км. Учтено, что на частоте 40 МГц напряженность поля помех $E_n = 10^{-6}$ В/м [7]. Требуемое отношение сигнал/шум было выбрано равным 10, при котором для противоположных сигналов и использовании помехоустойчивого кодирования со скоростью $1/2$ обеспечивается вероятность ошибки $P_{ош} = 10^{-5}$ [8].

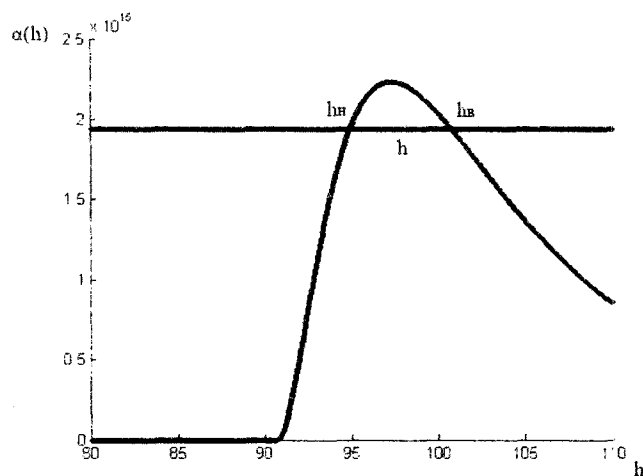


Рис. 2

В таблице приведены значения максимальной и минимальной электронной плотности, а также ширина метеорной зоны, для различных параметров метеорного тела.

$m [г]$	$v [км/с]$	$\alpha_{max} [э.л./м]$	$\alpha_{min} [э.л./м]$	$h [км]$
0.25	30	$1.7453 \cdot 10^{14}$	$1.9305 \cdot 10^{15}$	0
	50	$1.1174 \cdot 10^{15}$	$1.9374 \cdot 10^{15}$	0
	70	$3.4078 \cdot 10^{15}$	$1.9422 \cdot 10^{15}$	12.66
0.5	30	$3.4905 \cdot 10^{14}$	$1.9305 \cdot 10^{15}$	0
	50	$2.2349 \cdot 10^{15}$	$1.9374 \cdot 10^{15}$	5.9
	70	$6.8157 \cdot 10^{15}$	$1.9422 \cdot 10^{15}$	13.8
1		(переуплотненный след)		
	30	$6.9811 \cdot 10^{14}$	$1.9305 \cdot 10^{15}$	0
	50	$4.4698 \cdot 10^{15}$	$1.9374 \cdot 10^{15}$	15.94
		(переуплотненный след)		
	70	$1.3631 \cdot 10^{16}$	$1.9422 \cdot 10^{15}$	14.37
		(переуплотненный след)		

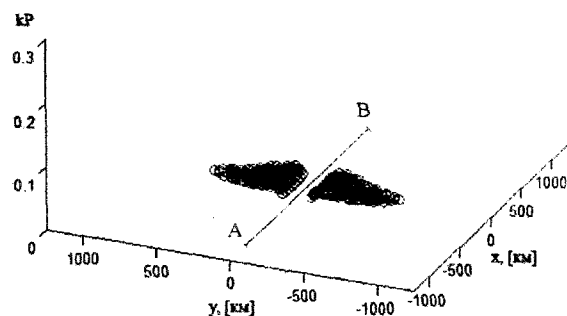
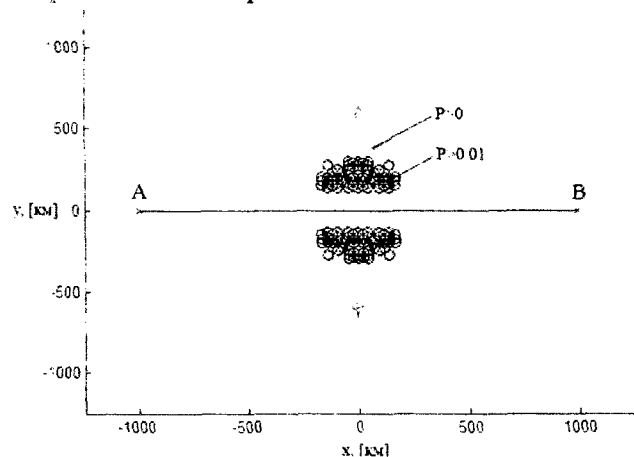
Расположение и размеры областей наиболее вероятного появления в зоне радиовидимости метеорных следов, обладающих точкой зеркального отражения, будет зависеть от протяженности радиолинии, эффективной длины следа и его ориентации относительно оси эллипсоида вращения, фокусами которого являются пункты передачи и приема информации.

На рис. 3 показано расположение метеорного следа в области h , где линейная электронная плотность превышает значение α_{min} , нижняя граница которой расположена на высоте $H = h_n$. Углы ψ и ϕ , а также полярный радиус ρ задают координаты точки входа метеороида в слой, а зенитный угол γ_z и приведенный азимут α определяют ориентацию метеорного следа в пространстве [4].

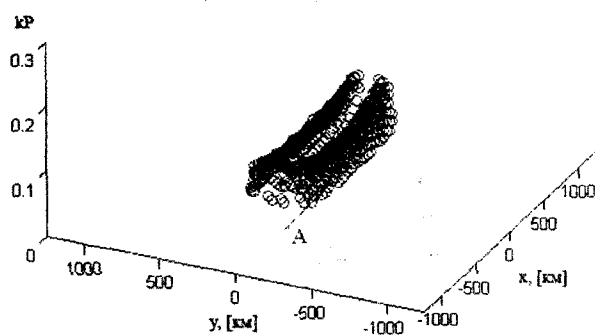
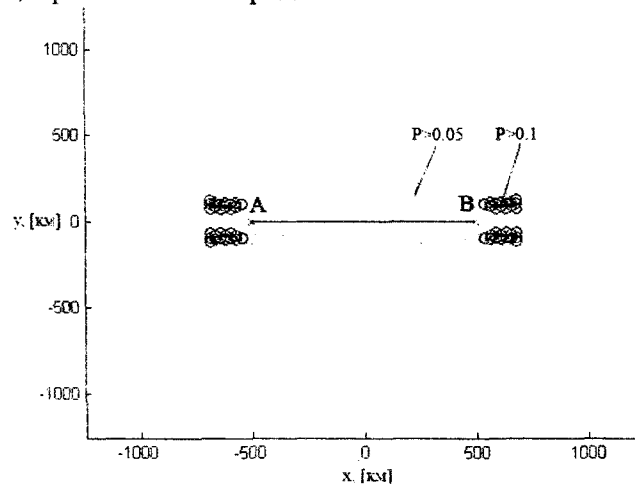
Для обеспечения статистической однородности оценок верхняя граница метеорной зоны, ограниченная зоной радиовидимости, разделяется на элементы поверхности, равной площади с одинаковым расстоянием между центрами [4]. При расчетах метеороиды, попавшие на элемент поверхности, относят к центру данного элемента. Вероятность того, что метеор, попавший в окрестность заданной точки $M_{BX}(x_{BX}, y_{BX}, z_{BX})$ с зенитным углом γ_z и азимутом α , образует след, имеющий зеркальную точку отражения, определяется выражением

$$P(x_{BX}, y_{BX}, z_{BX}) = \int_{\gamma_{min}}^{\gamma_{max}} w(\gamma_z) \int_{\alpha_{min}(\gamma_z)}^{\alpha_{max}(\gamma_z)} w(\alpha/\gamma_z) d\alpha d\gamma_z \quad (11)$$

а) протяженность радиолинии 2000 км



б) протяженность радиолинии 1000 км



в) протяженность радиолинии 500 км

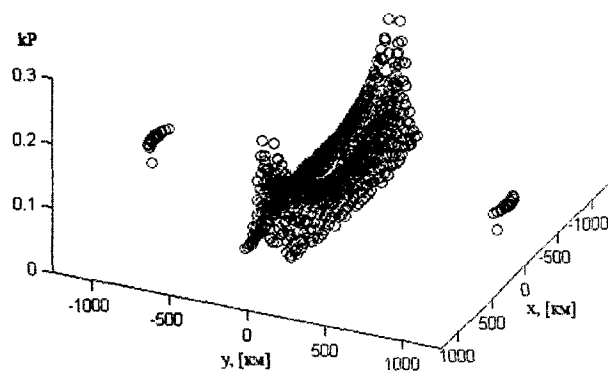
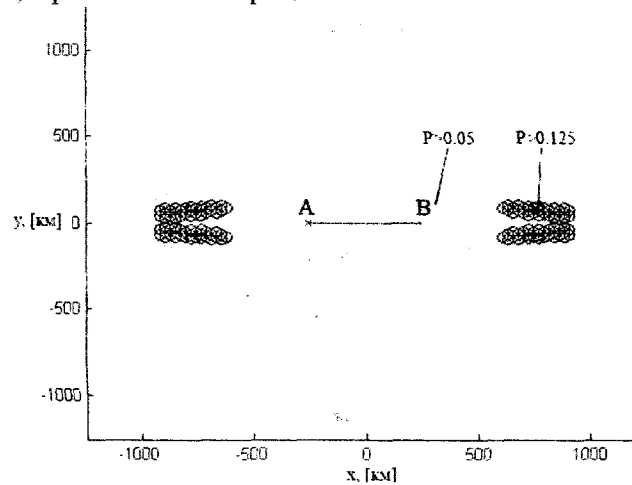
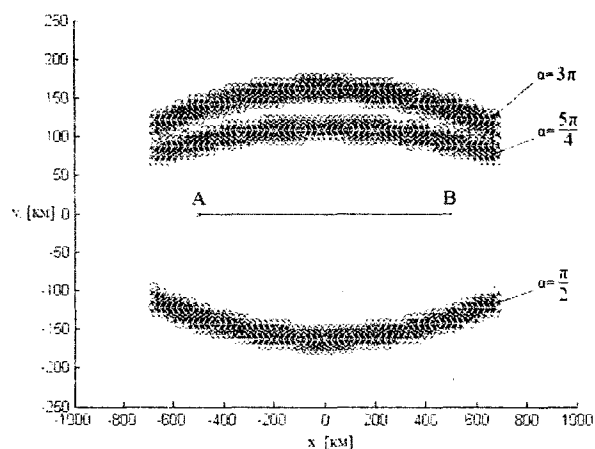


Рис. 4

а) протяженность радиолинии 1000 км



б) протяженность радиолинии 500 км

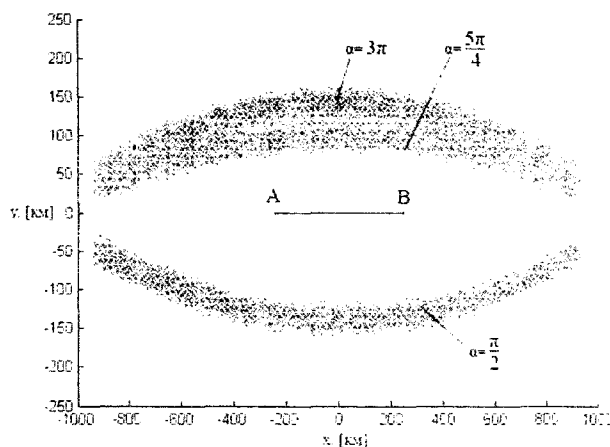


Рис. 5

В отличие от известных, предложенный метод позволяет рассчитывать «горячие области» для радиолиний различной протяженности по вероятности появления метеорных следов, обеспечивающих условия ведения радиосвязи. Введенное понятие эффективной длины метеорного следа позволило уточнить вероятность появления на следе точки зеркального отражения. При расчетах вероятности появления «подходящего» следа использованы априорные данные относительно плотностей распределения зенитных углов для спорадических метеоров и метеорных потоков.

Учет расположения и размеров «горячих областей» позволяет правильно выбрать ориентацию и ширину диаграммы направленности передающих и приемных антенн и, тем самым, обеспечить максимальную пропускную способность систем метеорной радиосвязи. Расчет «горячих областей» особенно актуален при выборе расположения базовых станций в ходе проектирования сетей метеорной радиосвязи, а также может быть использован при выборе пунктов передачи и приема для радиоастрономических наблюдений.

Список литературы: 1. Антитов И.Е., Коваль Ю.А., Обельченко В.В. Развитие теории и совершенствование радиометеорных систем связи и синхронизации. – Харьков : Коллегиум, 2006. – 308 с. 2. A. Herlofson. The theory of meteor ionization. Phys. SOC. Rep. Prog. Phys. 1948. Vol. 11. pp. 444-454. 3. T.E. Kaiser. Theory of the meteor height distribution obtained from radio-echo observations // Royal Astronomical Society. 1954. Vol. 114. P. 52-62. 4. Харченко Е.В. Метод оценки интервала рассеяния по запаздыванию при отражении сигналов от метеорных следов // Радиотехника. – 2010. – Вып. 160. – С. 56-61. 5. Белькович О.И. Статистическая теория радиолокации метеоров. – Казань : Изд-во КГУ, 1977. – 106 с. 6. A.A. Weiss. Elevation, Height, and Electron Density of Echoing Points of Meteor Trails // Australian Journal of Physics. 1959. Vol. 12. P. 65-76. 7. Ломан В.И., Захаров В.Э., Микрюков А.С., Хилевич С.В., Гряник М.В. Проектирование радиолиний : учеб. пособие. – К. : КВВИУС, 1988. – 336 с. 8. Скляр Е. Цифровая связь. Теоретические основы и практическое применение : 2-е изд., пер. с англ. – М. : Изд-дом «Вильямс», 2003. – 1104 с.

Институт радиофизики и электроники
им. А.Я.Усикова НАН Украины

Поступила в редколлегию 25.06.2011.

АДАПТАЦИЯ РАБОЧЕЙ ЧАСТОТЫ СОДАРА В УСЛОВИЯХ ИЗМЕНЯЮЩЕЙСЯ ПОМЕХОВОЙ ОБСТАНОВКИ

Введение

Широкий спектр современных научных и практических задач связан с оперативным оцениванием параметров атмосферного пограничного слоя (АПС). К одной из таких задач относится определение высотных профилей скорости ветра и турбулентности атмосферы в зоне аэропорта и в зоне подлета самолета к аэропорту. Перечень современных технических средств, используемых для решения этой задачи, включает: контактные датчики, метеозонды, радиопрофилеры, а также содары, активное применение которых началось в последние десятилетия. Радиопрофилеры позволяют оценить профили скорости и направления ветра с высот 1–2 км, метеорологические датчики оценивают скорость ветра, его направление, температуру в приземном слое до высот, ограниченных высотой метеорологических вышек, на которых они расположены (максимально до 150 м). Однако, согласно требованиям международной организации гражданской авиации ИКАО, для обеспечения безопасности взлетов и посадок самолетов наиболее важны измерения скорости ветра, инверсий на высотах до 500 м, где изменение сдвигов ветра и температуры имеет нелинейный характер и высокие градиенты [1]. По оценкам ИКАО самым эффективным средством определения метеопараметров в этом слое являются доплеровские содары. Например, в аэропорту Амстердама они применяются как для определения профилей скорости ветра, так и оценки прозрачности атмосферы над взлетно-посадочной полосой при появлении тумана [2]. В основу работы содаров положен метод акустического зондирования, заключающийся в отражении излученных содаром акустических волн от атмосферных турбулентностей, вызываемых температурной стратификацией атмосферы и действием ветра. Диапазон рабочих частот современных содаров широк – от сотен герц до ультразвуковых волн. Сильное затухание акустических волн в атмосфере ограничивает высоты зондирования содаров диапазоном до 100 – 1500 м. Высокая влажность, туман, осадки в виде дождя и снега могут существенно снижать заявленную в технических характеристиках дальность зондирования содара. Сопоставительный анализ результатов зондирования содаров метеорологической сети NOAA подтверждают, что при одинаковых значениях длительности импульса и излучаемой мощности дальность зондирования существенно отличается. Данный факт объясняется сильной частотной зависимостью отражения акустической волны от неоднородностей ее волнового фронта и описан во многих научных публикациях [3 – 5]. Кроме этого низкое отношение сигнал-шум влияет на точность оценивания основных метеорологических и физических параметров АПС. Одним из способов повышения отношения сигнал/шум является применение оптимальных частот зондирования содара. Однако обобщенного аналитического решения для нахождения оптимальных частот зондирования не существует. Причина данного факта – это влияние на отношение сигнал-шум принимаемого акустического сигнала внешних акустических помех, интенсивность которых велика.

Теоретические расчеты

Используя сходство методов акустического и радиозондирования можно получить выражение, связывающее отношение сигнал-шум на входе приемника с коэффициентом затухания α акустических волн, удельным отражением атмосферы σ и отражающим объемом V на фиксированной высоте зондирования R .

Коэффициент затухания акустических волн α для стандартной атмосферы и скорости распространения звука $c = 343$ м/с определяется выражением из [3]

$$\alpha = 4,96 \cdot f^2 \cdot 10^{-11} \cdot \text{м}^{-1}, \quad (1)$$

где f – рабочая частота содара, Гц.

Эффективную площадь рассеяния отражающего объема V можно рассчитать по формуле

$$S_{эф} = 4\pi V\sigma, \quad (2)$$

где σ – удельное отражение атмосферы, м^{-1} ; V – отражающий объем, м^3 .

Основной вклад в обратное рассеяние акустических волн вносят неоднородности температуры T [3], значение которых связано с удельным отражением атмосферы выражением

$$\sigma = 4 \cdot 10^{-3} (2\pi/\lambda)^{1/3} (C_T/T)^2, \quad (3)$$

где λ – длина акустической волны, м; C_T – среднеквадратическая разность температур в двух точках, находящихся на единичном расстоянии, $\text{К/м}^{1/3}$; T – температура, К.

Для системы, в которой передающая и приемная антенны совмещены, отражающий объем V определяется эффективной площадью приемо-передающей антенны $S_{ант}$ и длительностью зондирующего импульса τ :

$$V = \frac{c\tau}{2} R^2 \frac{\lambda^2}{S_{ант}}, \quad (4)$$

где R – дальность зондирования, м; $S_{ант}$ – эффективная площадь приемо-передающей антенны, м^2 ; τ – длительность зондирующего импульса, с.

На основании (1) – (4) для стандартной атмосферы при отсутствии промышленных шумов мощность принимаемого акустического сигнала определяется выражением

$$P_{np}(f) = 3,7 \cdot 10^{-3} \frac{C_T^2}{T^2} c^{2/3} \tau \cdot f^{1/3} P \frac{S_{ант}}{R^2} e^{-4,96 \cdot f^2 \cdot 10^{-11} R^2}, \quad (5)$$

где P – импульсная мощность акустического передатчика, Вт.

В работах [5, 6] приводятся примеры аналитических выражений, описывающие зависимость спектральной плотности мощности (СПМ) шумов от частоты для зоны аэропорта, городского транспорта и пример обобщенного варианта аналитического описания:

$$N_{трансп}(f) = 10^{-13} \cdot f^{-2}, \text{ Вт/Гц}, \quad (6)$$

$$N_{ав}(f) = 7 \cdot 10^{-11} \cdot f^{-3}, \text{ Вт/Гц}, \quad (7)$$

$$N(f) = 8,4 \cdot 10^{-21} + 0,13 \cdot f^{-4,67}, \text{ Вт/Гц}. \quad (8)$$

На основании (5) – (8) можно рассчитать отношение сигнал-шум на входе акустического приемника:

$$q(f) = \frac{P_{np}(f)}{\int_{f-\Delta f/2}^{f+\Delta f/2} N(f) df} = 3,7 \cdot 10^{-3} \frac{C_T^2}{T^2} c^{2/3} \tau \cdot P_u \cdot S_{np} \cdot Q(f, R), \quad (9)$$

где $Q(f, R)$ – коэффициент, который зависит от рабочей частоты содара и дальности зондирования; Δf – полоса пропускания акустического приемника, Гц.

Выражения частотно зависимого коэффициента $Q(f, R)$ для случаев описания СМГ формулами (6) – (8) имеют вид

$$Q_{\text{трансп}}(f, R) = \frac{f^{1/3} e^{-4,96 \cdot f^2 \cdot 10^{-11} R^2}}{R^2 \cdot \left[(f - \Delta f / 2)^{-1} - (f + \Delta f / 2)^{-1} \right]}, \quad (10)$$

$$Q_{\text{ав}}(f, R) = \frac{2 \cdot f^{1/3} e^{-4,96 \cdot f^2 \cdot 10^{-11} R^2}}{R^2 \cdot \left[(f - \Delta f / 2)^{-2} - (f + \Delta f / 2)^{-2} \right]}, \quad (11)$$

$$Q(f, R) = \frac{f^{1/3} \frac{1}{R^2} e^{-4,96 \cdot f^2 \cdot 10^{-11} R^2}}{8,4 \cdot 10^{-21} \cdot 2 \cdot \Delta f + 0,0354 \cdot \left[(f - \Delta f / 2)^{-3,67} - (f + \Delta f / 2)^{-3,67} \right]}. \quad (12)$$

Если учесть прямоугольную форму зондирующего импульса, то в выражения частотно зависимого коэффициента $Q(f, R)$ добавляется частотный множитель $\sin^2(\pi f \tau) / (\pi f)^2$, определяемый длительностью импульса τ , а частотно зависимый коэффициент становится функцией трех переменных $Q(f, R, \tau)$.

$$Q_{\text{трансп}}(f, R) = \frac{f^{1/3} e^{-4,96 \cdot f^2 \cdot 10^{-11} R^2}}{R^2} \cdot \frac{\sin^2(\pi f \tau)}{(\pi f)^2 \cdot \left[(f - \Delta f / 2)^{-1} - (f + \Delta f / 2)^{-1} \right]}, \quad (13)$$

$$Q_{\text{ав}}(f, R) = \frac{2 \cdot f^{1/3} e^{-4,96 \cdot f^2 \cdot 10^{-11} R^2}}{R^2 \cdot \left[(f - \Delta f / 2)^{-2} - (f + \Delta f / 2)^{-2} \right]} \cdot \frac{\sin^2(\pi f \tau)}{(\pi f)^2}. \quad (14)$$

$$Q(f, R, \tau) = \frac{f^{1/3} e^{-4,96 \cdot f^2 \cdot 10^{-11} R^2} \cdot \sin^2(\pi f \tau)}{(\pi f)^2 \left(8,4 \cdot 10^{-21} \cdot 2 \cdot \Delta f + 0,0354 \cdot \left[(f + \Delta f / 2)^{-3,67} - (f - \Delta f / 2)^{-3,67} \right] \right)}. \quad (15)$$

Длительность импульса τ выбирается кратной целому числу периодов рабочей частоты. Графики зависимостей коэффициентов $Q(f, R)$ и $Q(f, R, \tau)$ от частоты для ряда фиксированных высот R и длительности импульса равной 30 периодам рабочей частоты приведены на рис. 1, а результаты расчета оптимальных частот по формулам (10) – (14) сведены в табл. 1.

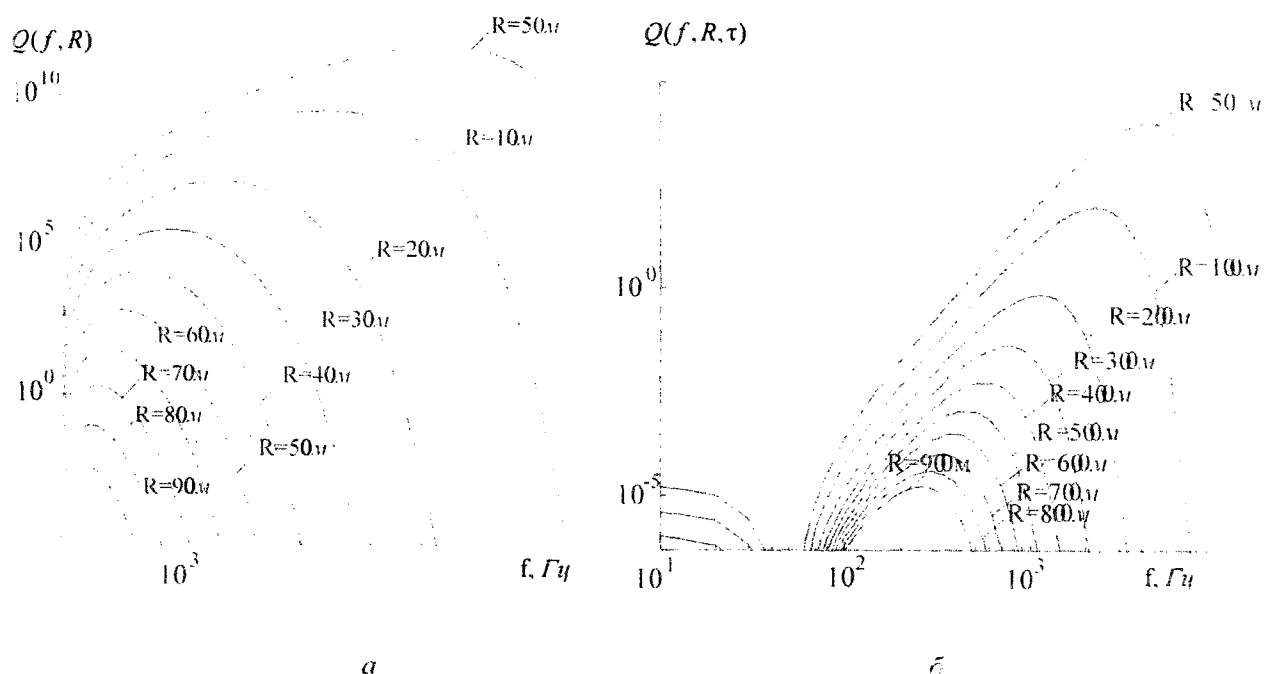


Рис. 1

Представленная на рис. 1 совокупность зависимостей соответствует обобщенному аналитическому описанию акустических помех.

Таблица 1

R, м	Без учета формы импульса			С учетом формы импульса		
	$f_{\text{опт. общ.}}, \text{Гц}$	$f_{\text{опт. тр.}}, \text{Гц}$	$f_{\text{опт. ав.}}, \text{Гц}$	$f_{\text{опт. общ.}}, \text{Гц}$	$f_{\text{опт. тр.}}, \text{Гц}$	$f_{\text{опт. ав.}}, \text{Гц}$
50	4510	3108	3710	4365	1177	2320
100	2342	1615	1915	2238	591	1176
200	1281	907	934	1047	313	554
300	963	713	638	744	227	315
400	807	622	473	568	182	267
500	716	586	386	446	154	164
600	664	457	324	380	142	104
700	619	443	272	331	126	89
800	587	384	154	281	111	67
900	571	321	126	251	102	48
1000	542	247	84	230	68	46

Анализ полученных данных свидетельствует о сильной зависимости величины оптимальной частоты содара от окружающей помеховой обстановки. Для выражений (6) – (8), не учитывающих форму излученного импульса, значения оптимальных частот для каждого из аналитических описаний СПМ шума отличаются не менее чем на 30 %. Такое существенное отличие подтверждает необходимость проведения адаптационной подстройки рабочей частоты содара по его месту установки и в процессе работы. При учете влияния прямоугольной формы излученного содаром импульса длительностью τ отличия оценок оптимальной частоты зондирования для аналитических описаний СПМ выражениями (13) – (15) достигают 3,6 раз.

В выражениях (10) – (15) СПМ внешних акустических помех описывается аналитическим выражением. Оптимальная частота содара определяется в результате нахождения максимума частотно зависимого коэффициента $Q(f, R, \tau)$. Для его нахождения используются соответствующие математические методы (например, градиентный). Несмотря на возможность обеспечения высокой точности нахождения оптимальной частоты аналитическими методами, практически целесообразно ограничиться точностью от 1 до 10 Гц. Она определяется возможностями аппаратуры. Такая точность оценки оптимальной частоты содара достижима без аналитического представления СПМ акустических шумов. При практических измерениях производится запись временной реализации внешних акустических помех, по которой вычисляется выборочная СПМ, аналитического описания которой мы не имеем. Полученная таким образом выборочная СПМ представляет собой распределение мощности шума на совокупности дискретных значений частоты. Если для записи временной реализации использовать устройство с параметрами звуковой карты компьютера (частота дискретизации 44 кГц), то временная реализация длительностью 1 с даст возможность рассчитать СПМ в частотной сетке с разрешением 1 Гц. Практически анализ временных реализаций шумов выполняется за интервал времени 10 или более секунд. Следовательно, нет необходимости получения аналитического выражения СПМ помехи, а достаточно значений ее выборочного представления.

Тогда можно сформулировать алгоритм нахождения оптимальной рабочей частоты содара:

- 1) произвести запись временной реализации внешних шумов длительностью не менее 1–10 с и вычислить по ней выборочную СПМ $S_{\text{выб}}(f) = \int N(f) df$;
- 2) задаться совокупностью высот зондирования, для которых необходимо определить оптимальные рабочие частоты содара;

- 3) определить оптимальные частоты из ряда, соответствующего выборочной СПМ, как те, на которых достигается максимум функции, описываемой выражением

$$Q(f_i, R) = f_i^{1/3} \frac{1}{R^2} e^{-4,96 \cdot f_i^2 \cdot 10^{-11} R^2} / S_{\text{выб}}(f_i), \quad i = 1 \dots N, \quad (16)$$

где N – длина выборки шума.

- 4) периодически действия 1)–3) повторять с целью автоподстройки под изменяющуюся со временем помеховую обстановку.

Экспериментальная проверка и выводы

Для проверки работоспособности разработанного алгоритма расчета оптимальной частоты содара были произведены записи временных реализаций шумов автотранспорта в условиях промышленных районов города, дизельных двигателей и шумов авиатранспорта в зоне аэропорта. На основании временных реализаций рассчитаны выборочные СПМ, примеры которых представлены на рис. 2. Кривым 1 и 2 рис. 2, *а* соответствуют временные выборки шума автотранспорта в различных местах проведения эксперимента. Кривой 3 на этом же рисунке соответствует запись шумов при работе дизельных двигателей электрогенераторов. Кривым 4–6 рис. 2, *б* соответствует запись шумов в центре взлетно-посадочной полосы и на расстояниях 100 и 500 м на подлете самолета к полосе.

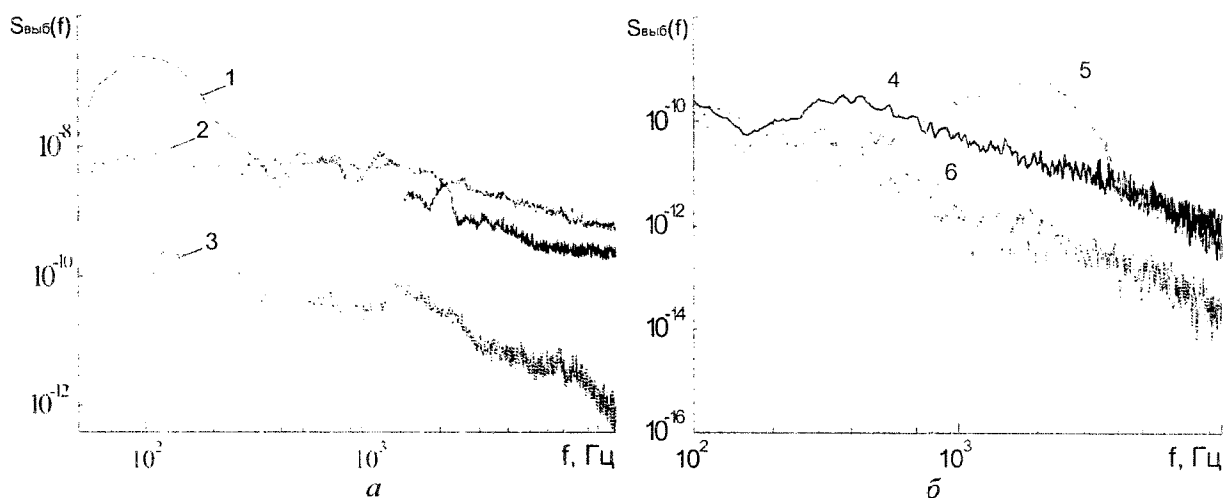


Рис. 2

В результате подстановки выборочных значений СПМ шумов в выражения (13) – (15) для совокупности фиксированных высот зондирования были построены зависимости коэффициента $Q(f, R, \tau)$ и определены значения оптимальных частот зондирования. На рис. 3, *а* приведена совокупность зависимостей коэффициента $Q(f, R, \tau)$ для СПМ шумов автотранспорта, соответствующей кривой 1 рис. 2, *а*. На рис. 3, *б* приведена совокупность зависимостей коэффициента $Q(f, R, \tau)$ для СПМ шумов авиатранспорта, соответствующих кривой 4 рис. 2, *б*. Рассчитанные значения оптимальных частот, соответствующие выборочным реализациям шумов автотранспорта и авиатранспорта, представлены в табл. 2.

Анализ данных, приведенных в табл. 2, показывает, что в основном с увеличением высоты зондирования наблюдается монотонное уменьшение значения оптимальной частоты. Данный факт подтверждается рядом публикаций [3, 4, 6] и соответствует теоретическим результатам, приведенным в табл. 1. Однако изменения значений оптимальной частоты с ростом высоты могут иметь значительные градиенты на высотах до 300 м. С ростом высоты эти отличия оказываются менее значительны и абсолютное значение оптимальной рабочей час-

тоты содара не превышает 400 Гц. Экспериментальные результаты также показывают, что малым высотам характерны более высокие абсолютные значения рабочей частоты содара, по сравнению с теоретическими, приведенными в табл. 1. На высотах свыше 500 м наблюдается обратная ситуация, то есть значения оптимальных частот меньше, чем теоретические, приведенные в табл. 1.

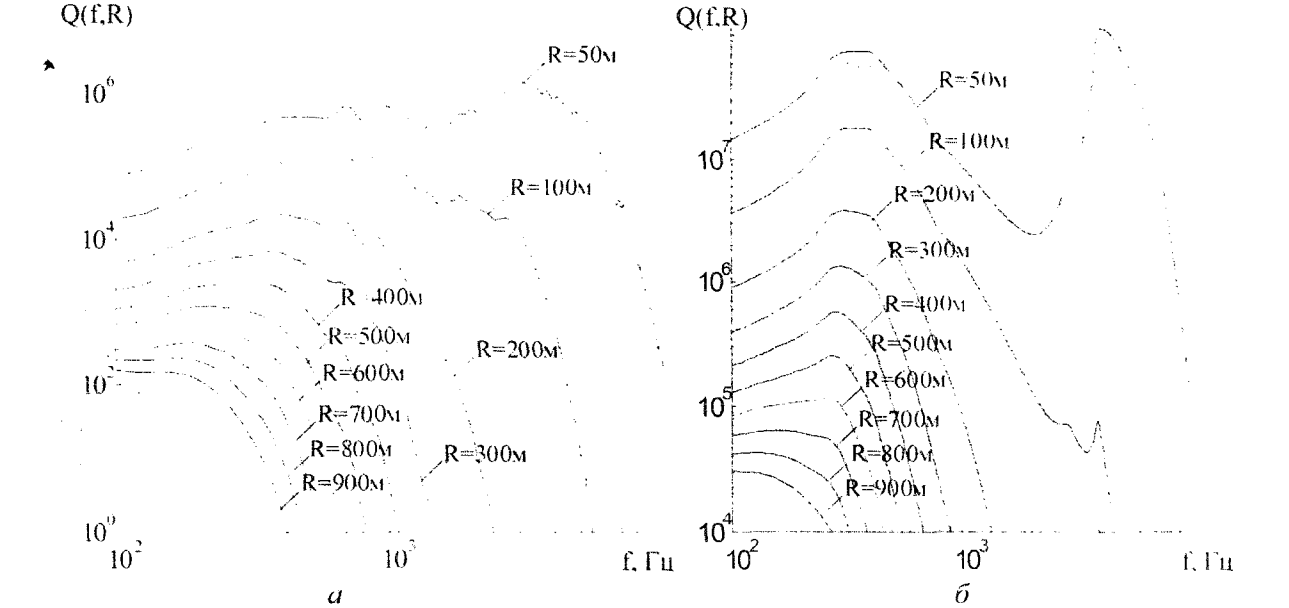


Рис. 3

Таблица 2

R, м						
	$f_{\text{опт. тр1}}, \text{Гц}$	$f_{\text{опт. тр2}}, \text{Гц}$	$f_{\text{опт. диз. ген}}, \text{Гц}$	$f_{\text{опт. ав1}}, \text{Гц}$	$f_{\text{опт. ав2}}, \text{Гц}$	$f_{\text{опт. ав3}}, \text{Гц}$
50	3090	2400	2200	4090	2355	3240
100	900	800	250	350	1490	1210
200	390	400	220	310	195	980
300	380	390	200	300	181	300
400	340	390	200	285	168	280
500	220	380	190	275	166	275
600	200	360	180	270	165	270
700	190	280	180	160	83	245
800	170	240	160	125	71	225
900	130	210	130	80	55	200
1000	111	200	124	76	52	195

Для различных мест установки содара, а значит и различной помеховой обстановки, отличия оптимальных частот зондирования могут достигать четырех раз, что наглядно подтверждают данные табл. 2 для высот 50 – 300 м. Такая ситуация наблюдается как для шумов автотранспорта, так и шумов авиации. Из табл. 2 также очевидно, что влияние шумов авиатранспорта на величину оптимальной частоты значительно больше по абсолютной величине, чем автомобильных. Данный факт можно объяснить отличиями спектральных характеристик шумов авиатранспорта, которые обусловлены различиями реактивных двигателей и взаимной ориентацией содара и самолета.

Таким образом, доказана работоспособность алгоритма оценки оптимальной частоты содара в изменяющейся окружающей помеховой обстановке.

Список литературы: 1. Doc 9817 AN/449. Руководство по сдвигу ветра на малых высотах. ИКАО, 2005. – 285 с. 2. *Jan Sondij* The meteorological observation infrastructure at Amsterdam airport schiphol. ICAO : Melbourne 2010. – 18 p. 3. *Красненко Н.П.* Акустическое зондирование атмосферы. Новосибирск: Наука, 1986. – 166 с. 4. *Ioannis Antoniou, Hans E. Jørgensen* On the Theory of SODAR Measurement Techniques (final reporting on WP1, EU WISE project NNE5-2001-297 Risø National Laboratory), Roskilde, Denmark 2003. – 60 p. 5. *Литл К.Г.* Акустические методы дистанционного зондирования нижней атмосферы. – ТИИЭР. – 1969. – Т.57, №4. – С. 22-230. 6. *Красненко Н.П., Раков Д.С.* Характеристики фонового окружающего шума в атмосфере и их взаимосвязь с параметрами среды // сб. трудов XVI сессии Российского акустического общества. Т.2. – М. : ГОЕС, 2005. – 357 с.

*Харьковский национальный
университет радиоэлектроники*

Поступила в редколлегию 23.06.2011

ВОЗБУЖДЕНИЕ КОНУСА С ПРОДОЛЬНОЙ ЩЕЛЬЮ ВО ВРЕМЕННОЙ ОБЛАСТИ МАГНИТНЫМ РАДИАЛЬНЫМ ДИПОЛЕМ

Введение

Изучение импульсного возбуждения структур, имеющих угловые размеры, представляет интерес для ученых. Импульсные режимы работы приборов и аппаратуры широко используются в телевидении, радиолокации, радионавигации и космической связи. В силу широкополосности [2] и способности формировать импульсные поля интерес представляют геометрически нерегулярные и щелевые структуры, например щелевые конусы [1]. Однако в связи с этим возникают трудности, связанные с построением адекватной математической модели физического процесса [4] и при решении соответствующей начально-краевой задачи. Использование существующих численно-аналитических и численных методов решения начально-краевых задач для структур с вершинами и ребрами нередко приводит к неустойчивым решениям, что влечет за собой появление физически противоречивых результатов [3]. Поэтому возникает необходимость проверки полученного решения путем сравнения с экспериментальными данными или решениями, полученными строгими аналитическими методами.

Цель работы – построение математической модели процесса возбуждения точечным импульсным источником конической антенны с продольными щелями и решение соответствующей модельной начально-краевой задачи с помощью строгих аналитических и численно-аналитических методов.

Общая постановка задачи

Электрический, $\chi = 1$, или магнитный, $\chi = 2$ диполь расположен в точке B_0 и возбуждает одиночный идеально проводящий полубесконечный круговой конус Σ с N продольными щелями (рис. 1). Уравнение конуса в сферической системе координат r, φ, θ задается в виде $\Sigma: \theta = \gamma$.

Необходимо определить в присутствии конуса и диполя электромагнитное поле $\vec{E}(\vec{r}, t)$, $\vec{H}(\vec{r}, t)$, удовлетворяющие уравнениям Максвелла, краевым условиям обращения в ноль тангенциальной составляющей поля E , условию причинности и условию ограниченности энергии. Для упрощения решения поставленной задачи используем потенциал Дебая $v^{(\chi)}$, через который выражаются составляющие электромагнитного поля [3, 5].

Для решения начально-краевой задачи для $v^{(\chi)}$ используем функцию Грина $G^{(\chi)}$, которая удовлетворяет:

1) волновому уравнению

$$\left(\Delta - \frac{1}{a^2} \frac{\partial^2}{\partial t^2} \right) G^{(\chi)}(\vec{r}, t) = -\delta(\vec{r} - \vec{r}_0) \delta(t - t_0), \quad \vec{r} \notin \Sigma;$$

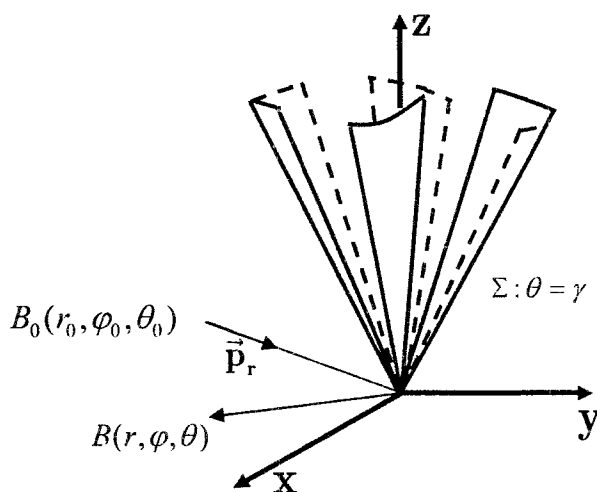


Рис. 1. Конус с продольными щелями

2) начальному условию (условию причинности)

$$G(\chi) = \frac{\partial G(\chi)}{\partial t} = 0, \quad t \leq t_0;$$

3) краевому условию

$$\frac{\partial \chi^{-1}}{\partial \mathbf{n} \chi^{-1}} \left(\frac{\partial G(\chi)}{\partial t} \right) \Big|_{\Sigma} = 0,$$

где $\mathbf{n}$ – внешняя нормаль;

4) условию ограниченности энергии.

Начально-краевая задача в такой постановке имеет единственное решение.

Ищем функцию G в виде $G = G_0 + G_p$, где G_0 – функция Грина в свободном пространстве:

$$G_0(\vec{r}, \vec{r}_0, t, t_0) = \frac{\delta(t - t_0 - R/a)}{4\pi R}, \quad R = |\vec{r} - \vec{r}_0|,$$

а G_p – искомая функция, соответствующая рассеянному конусом полю.

Далее будем рассматривать случай возбуждения конуса с продольной щелью магнитным радиальным диполем, т. е. при $\chi = 2$ и $N = 1$.

Метод решения

Для удобства отыскания функции Грина используем интегральное преобразование Мелера–Фока [5]:

$$\hat{F}(\tau) = \int_0^{+\infty} \text{sh } b F(b) P_{-\frac{1}{2}+i\tau}(\text{ch } b) db, \quad F(b) = \int_0^{+\infty} \tau \text{th } \pi \tau \hat{F}(\tau) P_{-\frac{1}{2}+i\tau}(\text{ch } b) d\tau.$$

Здесь

$$\text{ch } b(t) = \frac{t^2 a^2 - r^2 - r_0^2}{2rr_0}.$$

Запишем G_0 в виде интеграла Мелера–Фока:

$$G_0 = \int_0^{+\infty} \tau \text{th } \pi \tau \hat{G}_0(\tau) P_{-\frac{1}{2}+i\tau}(\text{ch } b) d\tau,$$

$$\hat{G}_0(r, \theta, \varphi, \tau) = \frac{a}{4\pi r r_0} \eta \left(t - \frac{r + r_0}{c} \right) \sum_{m=-\infty}^{+\infty} (-1)^m e^{im(\varphi - \varphi_0)} \frac{\Gamma(\frac{1}{2} - m + i\tau)}{\Gamma(\frac{1}{2} + m + i\tau)} F_{m\tau}(\theta, \theta_0),$$

где

$$F_{m\tau}(\theta, \theta_0) = \begin{cases} P_{-\frac{1}{2}+i\tau}^m(\cos \theta) P_{-\frac{1}{2}+i\tau}^m(-\cos \theta_0), & \theta < \theta_0, \\ P_{-\frac{1}{2}+i\tau}^m(-\cos \theta) P_{-\frac{1}{2}+i\tau}^m(\cos \theta_0), & \theta > \theta_0, \end{cases}$$

$P_{-\frac{1}{2}+i\tau}^m(\cos \theta)$ – функции Лежандра, $\Gamma(z)$ – гамма-функция, $\eta(z)$ – функция Хэвисайда.

Будем искать неизвестную функцию G_p в виде

$$G_p(b) = \int_0^{+\infty} \tau \operatorname{th} \pi \tau \hat{G}_p(\tau) P_{-\frac{1}{2}+i\tau}(\operatorname{ch} b) d\tau,$$

$$\hat{G}_p(\tau) = \sum_{m=-\infty}^{+\infty} z_{m\tau} U_{m,i\tau}(\theta, \varphi),$$

где $z_{m\tau}$ – известный коэффициент,

$$U_{i\tau}(\theta, \varphi) = \sum_{n=-\infty}^{+\infty} x_n^{(2)} \frac{P_{-1/2+i\tau}^n(\pm \cos \theta)}{\frac{d}{d\gamma} P_{-1/2+i\tau}^n(\pm \cos \gamma)} e^{in\varphi},$$

x_n – неизвестные коэффициенты, которые находятся с помощью СЛАУ-2, имеющей вид:

$$x_0^{(2)} \left\{ -D_{i\tau} + \ln \frac{1-u_2}{2} \right\} + \sum_{p=1}^{+\infty} x_p^{(2)} \frac{\varepsilon_p^{(2)}}{p} [P_p(u_2) + P_{-p}(u_2)] = \ln \frac{1-u_2}{2};$$

$$x_0^{(2)} [P_n(u_2) + P_{-n}(u_2)] + 2 \sum_{p=1}^{+\infty} x_p^{(2)} \varepsilon_p^{(2)} [V_{n-1}^{p-1}(u_2) + V_{-n-1}^{p-1}(u_2)] - 2x_n^{(2)} = \\ = P_n(u_2) + P_{-n}(u_2), \quad n = 1, 2, 3, \dots$$

Здесь

$$D_{i\tau}^{(2)} = \frac{ch\pi\tau}{\pi \sin^2 \gamma (0.25 + \tau^2)^2} \frac{1}{P_{-1/2+i\tau}^{-1}(\cos \gamma) P_{-1/2+i\tau}^{-1}(-\cos \gamma)},$$

$$\frac{1}{|n|} (1 - \varepsilon_n^{(2)}) = \frac{(-1)^{n+1} ch\pi\tau}{\pi \sin^2 \gamma} \frac{\Gamma(1/2 + i\tau + n)}{\Gamma(1/2 + i\tau - n)} \frac{1}{\frac{d}{d\gamma} P_{-1/2+i\tau}^n(\cos \gamma) \frac{d}{d\gamma} P_{-1/2+i\tau}^n(-\cos \gamma)}.$$

$$V_{n-1}^{m-1}(u) = \frac{n}{2(n-m)} [P_{n-1}(u)P_m(u) - P_n(u)P_{m-1}(u)],$$

$$u = \cos \frac{d}{2},$$

где d – ширина щели конуса.

Случай идеально проводящего конуса с продольной узкой щелью

Приведем аналитические выражения для случая конуса с продольной узкой щелью, т.е. при $1-u \ll 1$. В этом случае функция $U_{i\tau}(\theta, \varphi)$ будет иметь вид

$$U_{i\tau} = \frac{1}{\ln \frac{1-u}{2} B_{i\tau} \Phi_{i\tau}^0} \left\{ 2 \sum_{p=1}^{+\infty} \frac{\varepsilon_p}{p} \frac{P_{-1/2+i\tau}^p(\pm \cos \theta)}{P_{-1/2+i\tau}^p(\pm \cos \gamma)} + D_{i\tau}^{(2)} \sum_{n=1}^{+\infty} \frac{P_{-1/2+i\tau}^{-n}(\pm \cos \theta) \cos n\varphi}{\frac{d}{d\gamma} P_{-1/2+i\tau}^{-n}(\pm \cos \gamma)} \right\} + O \left(\frac{1-u}{\ln \frac{1-u}{2}} \right),$$

$$\text{где } B_{it} = D_{it}^{(2)} - 2 \sum_{p=1}^{+\infty} \frac{\varepsilon_p^{(2)}}{p}, \quad \Phi_{it}^0 = \frac{1}{D_{it}^{(2)} - 2 \sum_{p=1}^{+\infty} \frac{\varepsilon_p^{(2)}}{p}} - \frac{1}{\ln \frac{1-u}{2}}.$$

Численное решение

Проведен численный анализ распределения H_θ во временной области при фиксированных расстояниях от источника до вершины конуса r_0 , расстоянии от вершины конуса до точки наблюдения r , угла полураскрыва конуса γ , угла θ точки наблюдения при условии, что $\theta > 2\gamma$ и $t > (r + r_0)/a$, где a – скорость распространения сигнала в среде. При проведении численного эксперимента осуществлен переход от размерной величины t к безразмерной $\xi = at/(r + r_0)$, ($\xi > 1$). В соответствии с формулой для H_θ проведен расчет вышеуказанной зависимости при условии, что $r = 1$, $r_0 = 0.5$, $a = 1$.

На рис. 2 даны кривые зависимости составляющей электрического поля H_θ от временного параметра ξ при различных фиксированных значениях ширины щели, на рис. 3 показана зависимость поля от ξ в азимутальной плоскости.

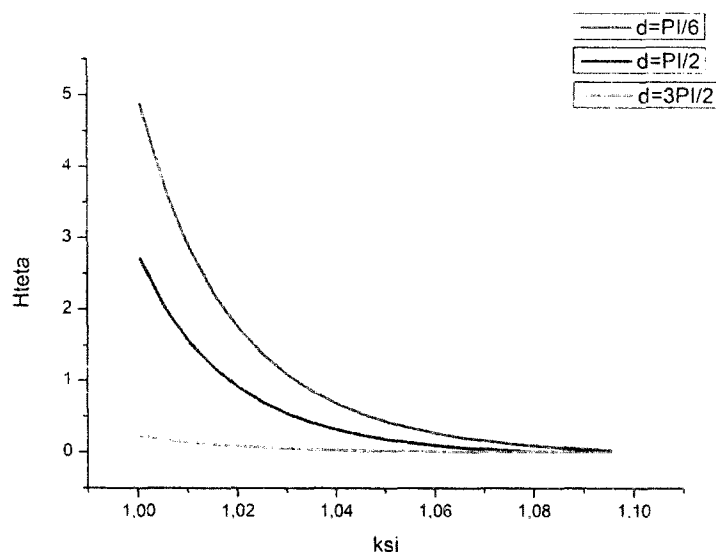


Рис. 2. Зависимость H_θ от ширины щели d

Из рис. 2 следует, что с уменьшением поверхности рассеяния (при расширении щели) наблюдается уменьшение поля напротив середины щели. При увеличении времени поле уменьшается (рис. 3).

Заключение

В работе построена математическая модель процесса возбуждения точечным импульсным источником конической антенны с продольными щелями. Для нахождения строгого аналитического решения использованы аппарат функции Грина и интегральное представление Мелара–Фока. Показано, что решение электродинамической задачи эквивалентно решению системы алгебраических линейных уравнений с вполне непрерывным оператором. Получено аналитическое решение в случае конуса с продольной узкой щелью. Проведен численный анализ одной из составляющих магнитного поля в зависимости от ширины щели и от временного параметра.

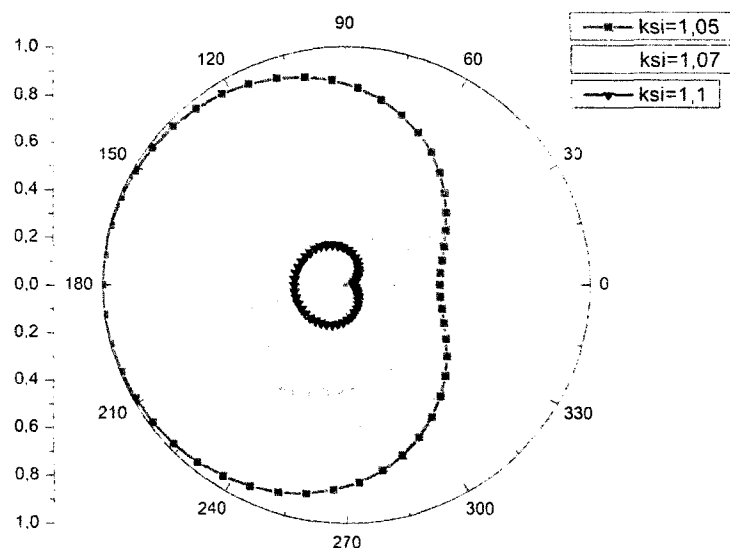


Рис. 3. Зависимость H_θ от временного параметра ξ в азимутальной плоскости

Список литературы: 1. Cheng S., Wu Z., Hallbjorner P., Hjort K., Rydberg A. Foldable and Stretchable Liquid Metal Planar Inverted Cone Antenna // IEEE Trans. on Antennas and Propagation. – 2009. – vol. 57, №12. – P. 3765-3771. 2. Amert A.K., Whites K.W. Miniaturization of the Biconical Antenna for Ultrawideband Applications // IEEE Trans. on Antennas and Propagation. – 2009. – vol. 57, №12. – P. 3728-3735. 3. Борисов В.В. Электромагнитные поля неустановившихся токов. – СПб. : Изд-во С.-Петерб. ун-та, 1996. – 208с. 4. Ильинский А.С., Кравцов В.В., Свеишиков А. Г. Математические модели электродинамики. – М. : Высш. шк., 1991. – 224с. 5. Дорошенко В. А, Кравченко В. Ф. Дифракция электромагнитных волн на незамкнутых конических структурах / под ред. В.Ф. Кравченко. – М. : ФИЗМАТЛИТ, 2009. – 272 с.

Харьковский национальный
университет радиоэлектроники

Поступила в редколлегию 09.06.2011

Н.И. СЛИПЧЕНКО, д-р физ.-мат. наук, В.А. ПИСЬМЕНЕЦКИЙ, канд. техн. наук,
Н.В. ГЕРАСИМЕНКО

ИССЛЕДОВАНИЕ И МОДЕЛИРОВАНИЕ ЭЛЕКТРОННЫХ СВОЙСТВ АМОРФНЫХ ПЛЕНОК α -Si:H

Введение

В современных условиях солнечные элементы (СЭ) являются долговечными, экологически чистыми и энергетически сбалансированными альтернативными источниками энергии.

В настоящее время 90 % выпускаемых фотопреобразователей (ФП) создаются на базе кремниевых структур и их модификаций, которые достаточно сложно описать классическими физико-математическими моделями.

В последнее время стремительно развивается и совершенствуется технология производства аморфных пленочных ФП на основе α -Si:H, CdTe и других соединений.

Обладая относительно низкими КПД (5 – 8 %), такие ФП выгодно отличаются от моно- и поликристаллических структур более простой рулонной технологией изготовления на основе применения автоматизированных технологических систем полунепрерывного действия.

В работе были исследованы характеристики аморфных пленок α -Si:H для создания ФП структур с применением ранее разработанных авторами аппроксимационных моделей [1].

Постановка задачи

Содержание водорода в аморфных пленках α -Si:H является доминирующим параметром, определяющим их микроструктурные, оптические и электронные свойства. Последние определяются глубокими локализованными состояниями, которые возникли из нейтральных оборванных связей. Связанный водород преобразует чистый α -Si:H в электронный качественный материал, устраняя оборванные связи. По этой причине в большинстве работ концентрацию водорода в пленках C_H принято считать структурным параметром пленок α -Si:H. На указанный параметр существенно влияют технологические факторы: температура подложки T_s при осаждении пленки, давление газовой смеси 25% SiH_4 + 75% Ar; скорости её прокачки через рабочий объем камеры.

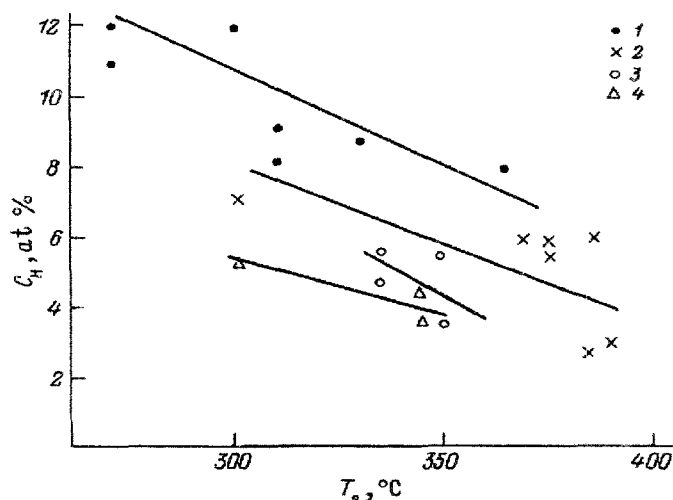


Рис. 1. Зависимости концентрации водорода от температуры осаждения пленки:

1 – $P = (7-8) \cdot 10^{-3} \text{ Тор}$, $r = 1 \text{ s.c.c.m.}$; 2 – $P = (2.5-3.5) \cdot 10^{-3} \text{ Тор}$, $r = 1 \text{ s.c.c.m.}$;
3 – $P = 3 \cdot 10^{-3} \text{ Тор}$, $r = 3 \text{ s.c.c.m.}$; 4 – при введении сетки в камеру $P = 7 - 10^{-3} \text{ Тор}$, $r = 1 \text{ s.c.c.m.}$

Согласно результатам исследований представленные на рис. 1 [1] зависимости процентного содержания водорода от температуры T_s осаждения пленки являются линейными и параметр C_H убывает с ростом T_s . При уменьшении давления газовой смеси и увеличения ее скорости прокатки концентрация водорода уменьшается. Таким образом, перечисленные технологические факторы действительно обеспечивают управление процентным содержанием водорода в процессе нанесения аморфных пленок α -Si:H.

Поэтому в дальнейшем основное внимание уделим исследованию структурных, оптических и электронных свойств аморфных пленок α -Si:H в зависимости от параметра C_H .

Исследование и электронных свойств аморфных пленок α -Si:H

Как известно, содержание водорода в пленках α -Si:H связано с формами его вхождения, видами связей с атомом Si и определяет микроструктуру, морфологию пленок. Влияние концентрации водорода (параметр C_H) на структурные свойства пленок сводится к тому, что при малых C_H (порядка 12 %) видимая микроструктура отсутствует, но при $C_H = 38$ % микроструктура проявляется как на поперечном сечении, так и на верхних поверхностях (наличие "бугристой" структуры). Пленки с высоким C_H имеют большую фракцию слабо связанного водорода, который скапливается в микропустотах.

Неоднородность структуры пленок проявляется в виде столбов, зерен и пузырьков, размеры которых растут с увеличением толщины пленки.

Установлено, что в α -Si:H, в зависимости от условий получения, содержатся две фазы, связанные с водородом: первая (обязательная) – случайным образом распределенные моногидриды Si-H, вторая – полигидриды типа $(Si-H_2)_n$, $Si-H_3$, $Si-H_2$ и кластеризованные Si-H группы. Полигидридные конфигурации обнаруживаются в пленках с выраженной микроструктурой. Установлено, что полигидридные связи характерны для «соединительной» ткани между колоннами, материал же в пределах колонн имеет низкую плотность дефектов и водород в нем находится в виде моногидридных групп Si-H.

Для количественной характеристики морфологии и структуры аморфной пленки используется микроструктурный параметр R.

Были исследованы зависимости микроструктурного параметра R от концентрации водорода C_H при разных технологиях нанесения пленок α -Si:H. На рис. 2 приведены экспериментальные данные для метода тлеющего разряда с использованием силан-гелиевых смесей при температуре подложки $T_s=260^\circ\text{C}$ (кривая 1), осаждения пленок методом MASD (кривая 2), метода магнетронного распыления при $T_s=260^\circ\text{C}$ (кривая 3) [1]. Данные методы позволяют получить все слои в едином технологическом цикле.

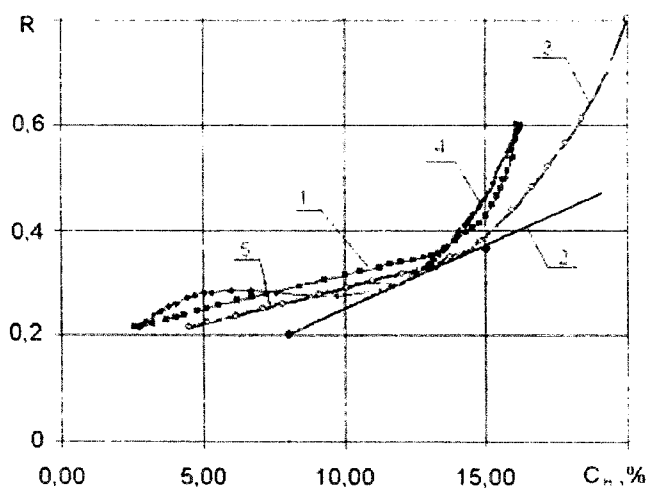


Рис. 2. Зависимости микроструктурного параметра R от концентрации водорода C_H при разных технологиях нанесения пленок α -Si:H

Соответственно, для этих технологий получены регрессионные уравнения:

(кривая 4)

$$R(C_H) = 3,373 \cdot 10^{-3} + 1,142 \cdot 10^{-1} \cdot C_H - 1,499 \cdot 10^{-2} \cdot C_H^2 + 6,277 \cdot 10^{-4} \cdot C_H^3 \quad (1)$$

(график 2)

$$R(C_H) = 1,483 \cdot 10^{-3} + 2,429 \cdot 10^{-2} \cdot C_H \quad (2)$$

(кривая 5)

$$R(C_H) = -2,948 \cdot 10^{-2} + 8,777 \cdot 10^{-2} \cdot C_H - 9,151 \cdot 10^{-3} \cdot C_H^2 + 3,459 \cdot 10^{-4} \cdot C_H^3 \quad (3)$$

Предложенные регрессионные уравнения позволяют выполнять прогнозные оценки значений микроструктурного параметра R для трех разных технологий

Из графиков следует, что на участке $C_H(5,0 - 15,0)$ зависимости $R(C_H)$ являются линейными, а при $C_H > 15,0$ (режим формирования качественных пленок) их поведение существенно различается для разных технологий.

Видно, что возрастание R происходит одновременно с возрастанием содержания водорода. Наиболее высокие величины R (до 0.8) наблюдаются для пленок α -Si:H, осажденных методом тлеющего разряда при $T_s=260$ °C и использование силан-гелиевых смесей [2] и методом магнетронного распыления при $T_s=260$ °C и вариациях парциального давления водорода в его смеси с аргонном [3]. В противоположность сказанному, методом MASD можно получить пленки α -Si:H с низким содержанием водорода, имеющие высокие R и содержащие дигидридные комплексы как в форме SiH_2 , и в форме $(SiH_2)_n$ (рис. 2). Следовательно, можно говорить о своеобразии технологий процесса осаждения и структуры рассматриваемых пленок α -Si:H.

Были проведены исследования зависимости фототока пленок α -Si:H от толщины. Как известно, вероятность прохождения неравновесных носителей падает с увеличением толщины аморфного слоя, а время жизни свободных носителей в аморфном кремнии мало и на расстоянии, определяемом их временем жизни, большая часть носителей рекомбинирует или захватывается ловушками. Таким образом, темп рекомбинации для неравновесных носителей в аморфном кремнии намного выше темпа генерации. Концентрация неравновесных носителей фотопроводимости обусловлена коэффициентом поглощения света и экспоненциально падает с толщиной пленки, но общее число сгенерированных пар с увеличением толщины пленки увеличивается. В результате общий фототок структуры в значительной степени зависит от толщины пленки.

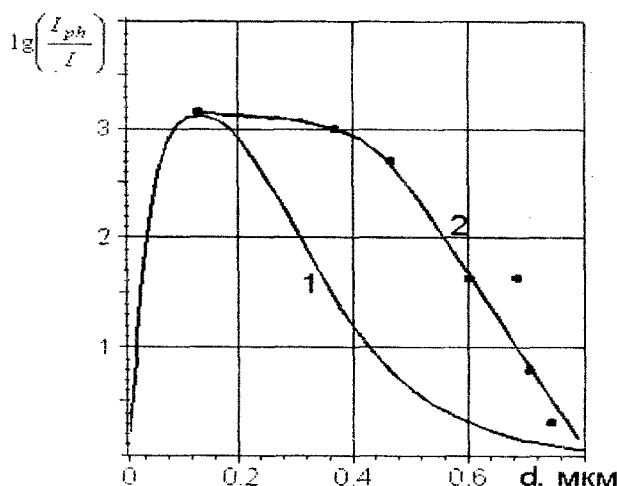


Рис. 3. Зависимости относительной величины фототока от толщины α -Si слоя в гетероструктуре при облучении светом с длиной волны 0.47 мкм; 1 – расчетная, 2 – экспериментальная [4]

Как показали численные расчеты и экспериментальные исследования (рис. 3), зависимость фототока в аморфных гидрогенизированных пленках от их толщины имеет неоднозначный характер.

Максимальное количество электронов фотопроводимости генерируется вблизи поверхности пленки, при этом длина их пролета для выхода из пленки увеличивается с ростом ее толщины. Для пленок толщиной более 0.3 мкм время пролета электронов фотопроводимости оказывается больше, чем их время жизни и часть электронов рекомбинирует, снижая общий фототок. Таким образом, имеется оптимальное значение толщины пленки α -Si:H, при котором фототок I_{ph} максимален, что наглядно иллюстрируется на рис. 3, где видно, что оптимальная толщина пленки составляет 0.2-0.4 мкм.

Аналогичные результаты по оптимизации толщины пленки CdS получены при исследовании пленочных солнечных элементов на основе CdS/CdTe в работе [5]. Следовательно, целесообразно проведение оптимизации технологических параметров по толщине аморфных пленок α -Si:H.

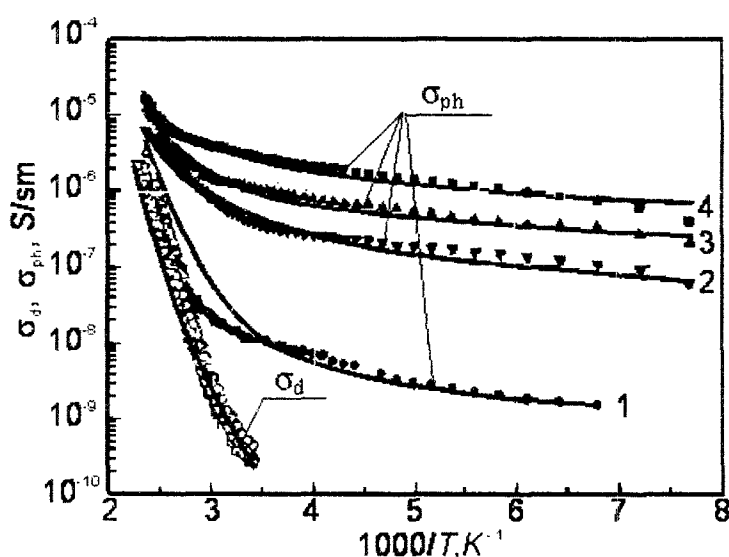


Рис. 4. Влияние технологических факторов на темновую и фотопроводимость аморфных гетероструктур α -Si:H/Si(c)

Были выполнены исследования температурных зависимостей темновой σ_d и фотопроводимости σ_{ph} пленок α -Si:H, полученных в результате разложения моносилана в высокочастотном тлеющем разряде. На рис. 4 представлены соответствующие графики, из которых следует, что проводимость имеет активационный характер. Толщина пленок (в скобках указаны номера образцов) составляла 0.6 мкм (4), 0.8 мкм (3), 0.9 мкм (2), 1 мкм (1). В качестве подложки при нанесении пленок использовалось кварцевое стекло. Пленки освещались монохроматическим светом с энергией кванта 1.85 эВ (0.67 мкм) и интенсивностью $10^{14} \text{ см}^{-2} \cdot \text{с}^{-1}$.

Для анализа температурных зависимостей σ_d и σ_{ph} будем использовать упрощенную модель [7] плотности состояний в щели подвижности, состоящей из четырех дискретных уровней (рис. 5). Уровни E_{tr} и E_{tm} с плотностью состояний N_{tr} и N_{tm} — эффективные уровни хвоста валентной зоны и зоны проводимости соответственно. Уровни E_D и $E_D + U$ — энергетические уровни состояний оборванных связей. Такое упрощенное представление плотности состояний в щели подвижности, как показано в работе [7], не приводит к качественным изменениям результатов численного расчета.

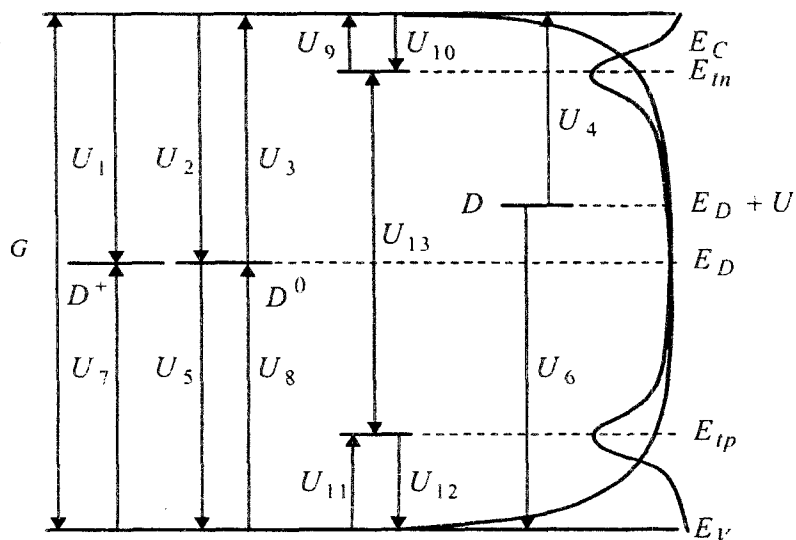


Рис. 5. Схематическое представление электронных переходов для упрощенной модели плотности состояний и вид плотности состояний в щели подвижности

На рис. 5 показаны вероятные переходы, которые учитывались при проведении исследований. Как и в модели [6, 7], в данной работе рассмотрены два возможных канала рекомбинации: прямой захват свободных электронов и дырок на D -центры (потоки U_1 , U_2 , U_5 и U_6) и туннельная рекомбинация между электронами, захваченными на состояния хвоста зоны проводимости, и дырками, захваченными на состояния хвоста валентной зоны U_{13} .

Увеличение плотности электронов в зоне проводимости обусловлено оптической генерацией G и переходами U_3 , U_4 , U_9 . Уменьшение плотности обусловлено переходами U_1 , U_2 и U_{10} .

В стационарном состоянии переходы уравновешены и суммарный поток равен нулю.

За счет оптической генерации G увеличиваются потоки U_4 , U_7 , U_8 , U_{10} , U_{12} , U_{13} . Но в соответствии с условием электронейтральности остальные потоки также изменяются. Уровни E_m и E_{tp} аналогичны ловушкам. Через них осуществляется прыжковая проводимость характерная для аморфных полупроводников.

Зависимость проводимости от температуры обусловлена, с одной стороны, естественным увеличением вероятности рассеяния свободных носителей на акустических и оптических фононах, что должно приводить к уменьшению проводимости с ростом температуры, а с другой – к увеличению времени жизни за счет уменьшения вероятности захвата горячих носителей ловушками и увеличения теплового выброса электронов из D^0 - и D^- -состояний и дырок из D^0 - и D^+ -состояний, что приводит к увеличению проводимости с повышением температуры. Слабая зависимость фотопроводимости от температуры в области низких температур объясняется тем, что температура аморфного кремния недостаточна для обеспечения теплового выброса электронов из ловушек и потоки U_3 , U_8 и U_7 (рис.5) практически отсутствуют.

Температурные зависимости σ_d , σ_{ph} зависят от механизма переноса носителей заряда. При низких температурах $T = (80 - 100)$ К имеет место прыжковый механизм проводимости, которая осуществляется за счет перескоков электронов на состояния хвоста зоны проводимости (поток U_{10}) и дырок на состояния хвоста валентной зоны (поток U_{12}).

Для средних температур $T = (250 - 300)$ К основной канал рекомбинации связан с прямым захватом свободных носителей через D-центры, обусловленные оборванными связями (потoki U_1 , U_2 и U_5 , U_6).

Из формулы для σ_{ph} , предложенной в работе для пленок α -Si:H p-типа, следует, что с ростом температуры фотопроводимость увеличивается по закону $\sigma_{ph} \sim \exp[(E_v - E_{ip})/2kT]$, где E_v – энергетическое положение потолка валентной зоны.

Физически это означает, что рост температуры увеличивает вероятность термического выброса дырок из ловушек в валентную зону, что вызывает увеличение потока дырок, которые захватываются на D^0 -центры. Это приводит к их перезарядке по схеме $D^0 + h \rightarrow D^+$. В результате увеличивается время жизни дырок и соответственно σ_{ph} .

На высоких температурах $T = (520 - 570)$ К наблюдается превышение темновой проводимости над фотопроводимостью ($\sigma_d > \sigma_{ph}$), влияние ловушек незначительно.

Достоверность полученных авторами результатов наглядно демонстрируется на рис. 6, где для сравнения приведены аналогичные температурные зависимости σ_{ph} из работы [7].

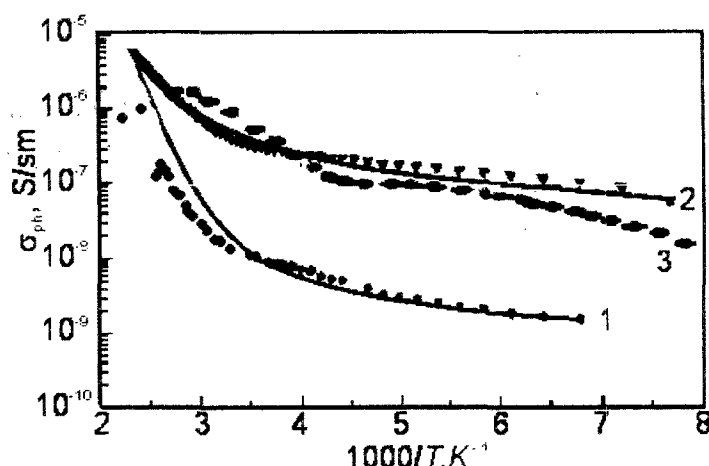


Рис. 6. Температурные зависимости фотопроводимости аморфных гетероструктур α -Si:H/Si:с 1 – нулевая концентрация водорода $C_H=0$; 2 – концентрация водорода $C_H=30\%$; 3 – зависимость σ_{ph} от температуры, полученная в работе [7]

Активационный характер зависимостей фотопроводимости от температуры указывает на возможность использования данных пленок в преобразователях солнечной энергии в электрическую. Результаты данных исследований также подтверждают, что значение фотопроводимости тонкой пленки аморфного кремния зависит от ее толщины.

Проведено исследование влияния различной концентрации водорода в аргоново-водородной плазме на электрические и оптические свойства пленок аморфного гидрированного кремния, полученных магнетронным методом. Значения запрещенной зоны E_g энергии активации E_a изменялись от 1,69 до 1,75 эВ и от 0,15 до 0,25 эВ соответственно.

Как известно, наличие водорода в аморфном кремнии снижает количество оборванных связей, увеличивая время жизни неравновесных носителей. Это выражается в уменьшении потоков U_1 , U_2 (рис.5) за счет снижения количества D-центров при неизменных потоках U_3 и U_{10} . Потоки, U_4 меняются слабо, так как больше определяются уровнем заполнения ловушек и коэффициентом теплового выброса. Таким образом, можно сделать вывод о том, что с увеличением степени гидрирования аморфных пленок, их проводимость должна возрастать.

В общем случае проводимость аморфного кремния определяется вероятностью возникновения цепочек таких локальных состояний, энергетические уровни которых достаточны

близки и пространственное расстояние оказывается малым для того, чтобы электроны или дырки могли переходить из одного локального состояния в другое, и при этом происходил перенос заряда через всю структуру.

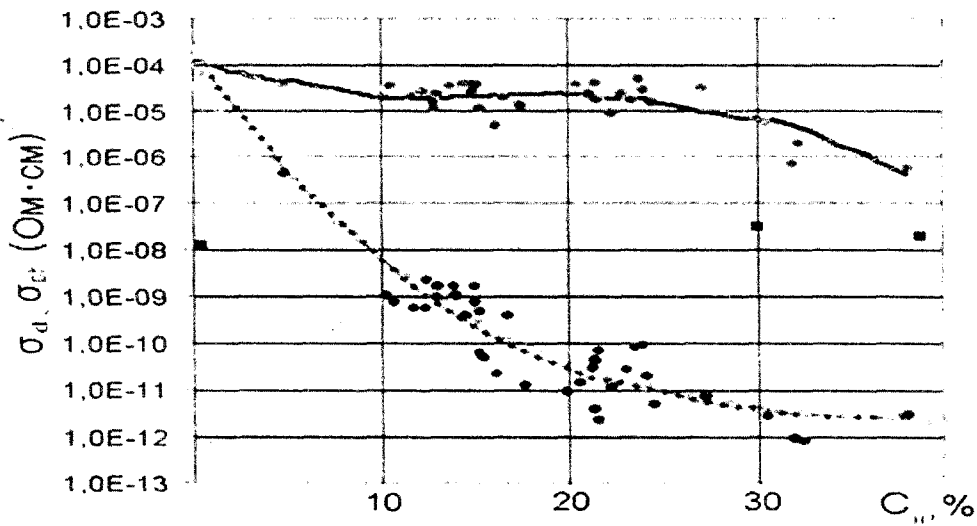


Рис. 7. Зависимость темновой и фотопроводимости пленок α-Si:H от концентрации водорода C_H [9]

Показано, что пленки могут быть разделены на три категории. Пленки первой категории содержат < 10 ат. % водорода, и их темновые проводимости σ_d резко уменьшаются при увеличении содержания водорода из-за обрыва провисших связей в запрещенной зоне. Вторая категория содержит пленки приборного качества, у которых C_H находится в интервале от 10 до 28 ат. % с фотопроводимостью в пределах от 8×10^{-6} до 3.5×10^{-5} (Ом см)⁻¹.

Третья категория содержит пленки, которые были получены при более низких температурах подложки ($T_s < 200^\circ\text{C}$). Фотопроводимость этих пленок на порядок ниже чем у пленок, содержащих 10 – 28 ат. % водорода. Это происходит главным образом из-за более высокой плотности состояний, которая уменьшает время жизни носителей, а также из-за более широкой запрещенной зоны, уменьшающей поглощение светового потока. Наблюдалось уменьшение на восемь порядков величины темновой проводимости по мере увеличения содержания водорода от 0 до ~40 ат. %.

Отношение SiH/SiH₂, измеренное ИК методом, уменьшается по мере увеличения содержания водорода, в результате растет плотность состояний в щели подвижности, уменьшается τ и соответственно σ_d . Рост σ_{ph} до оптимального значения при облучении связан со снижением числа оборванных связей и соответственно концентрации D-центров, при этом растет время жизни τ . Далее проявляется уменьшение отношения SiH/SiH₂.

Для аналитического представления зависимостей $\sigma_d = f(C_H)$ и $\sigma_{ph} = f(C_H)$ по экспериментальным данным, полученным в работе [9] и представленным на рис. 7 кружочками, получены уравнения регрессии 2-го, 3-го и 4-го порядков:

$$\sigma_d = \exp(-9,946) - 1,043 \cdot C_H + 1,625 \cdot 10^{-2} \cdot C_H^2$$

$$\sigma_d = \exp(8,971) - 1,307 \cdot C_H + 3,323 \cdot 10^{-2} \cdot C_H^2 - 2,968 \cdot 10^{-4} \cdot C_H^3$$

$$\sigma_{ph} = \exp(-8,355) - 6,759 \cdot 10^{-1} \cdot C_H + 5,966 \cdot 10^{-2} \cdot C_H^2 - 1,992 \cdot 10^{-3} \cdot C_H^3 + 2,035 \cdot 10^{-5} \cdot C_H^4$$

Авторами было исследовано влияние концентрации водорода в пленках α -Si:H на их спектры поглощения $\alpha(E)$. Показано, что в результате гидрирования происходит удаление части локализованных состояний на хвостах валентной зоны, уменьшение максимума коэффициента поглощения α , что приводит к возрастанию оптической ширины запрещенной зоны E_g за счет смещения вниз потолка валентной зоны E_v . В результате спектры поглощения смещаются в сторону больших энергий фотонов (рис. 8).

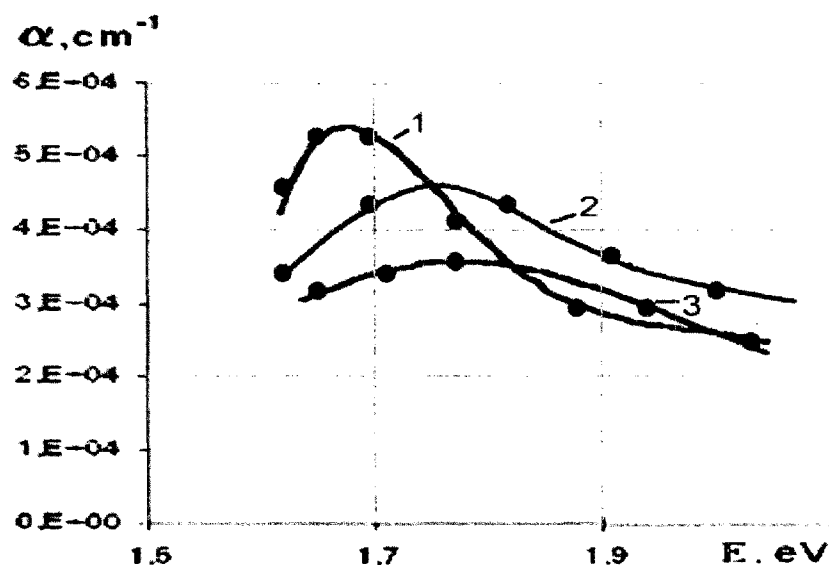


Рис. 8. Спектр поглощения кремниевых пленок на ситалловых подложках: в чистой аргонной среде (кривая 1), аргонно-водородной среде при концентрации водорода 30% (кривая 2), аргонно-водородной среде при концентрации водорода 40% (кривая 3)

Таким образом, поглощательная способность пленки уменьшилась и, следовательно, уменьшился коэффициент поглощения (рис. 8). Размытие спектра и его смещение в коротковолновую часть на 1,6 – 1,9 эВ связано с появлением дополнительных колебательных центров Si-H и H-Si-H в аморфной гидрированной структуре.

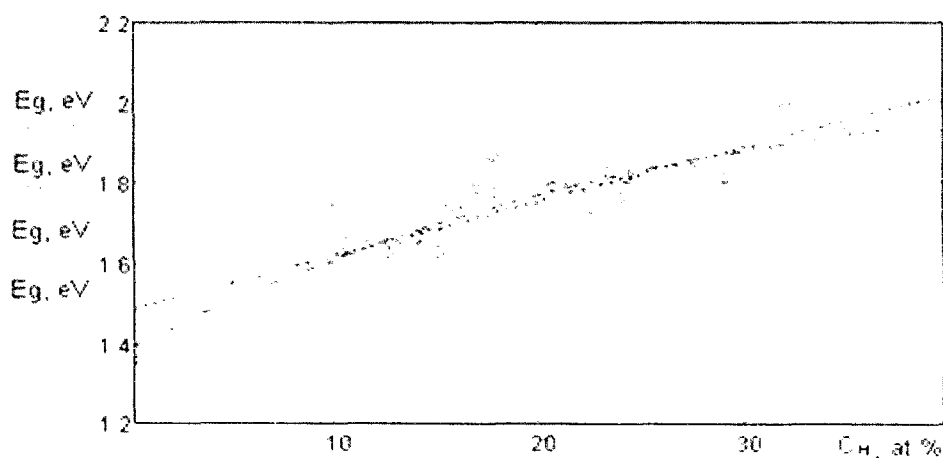


Рис. 9. Зависимость ширины запрещенной зоны пленок α -Si:H, осажденных реактивным магнетронным распылением, от концентрации водорода в пленке [9]

С учетом экспериментальных данных, полученных в работе [9] и представленных на рис. 9 кружочками, были построены аналитические зависимости ширины запрещенной зоны E_g

от концентрации водорода C_H первой, второй и третьей степени. Следует отметить, что аналогичное уравнение первой степени было получено в работе [9] методом наименьших квадратов. Анализ уравнений первой степени показывает, что коэффициенты a_0 и a_1 практически мало отличаются:

$$E_g = 1,481 + 1,357 \cdot 10^{-2} \cdot C_H$$

$$E_g = 1,5 + [C_H \times (0,0125 \pm 0,003)] \text{ из работы [9]}$$

$$E_g = 1,391 + 2,392 \cdot 10^{-2} \cdot C_H - 2,519 \cdot 10^{-4} \cdot C_H^2$$

$$E_g = 1,376 + 2,752 \cdot 10^{-2} \cdot C_H - 4,727 \cdot 10^{-4} \cdot C_H^2 + 3,721 \cdot 10^{-6} \cdot C_H^3$$

Результаты моделирования $E_g = f(C_H)$ с помощью уравнений второй и третьей степени практически совпадают и представлены на рис. 9 пунктирной и штрихпунктирной линиями.

Заключение

Полученные линейные зависимости концентрации водорода C_H от температуры осаждения пленки, давления газовой смеси и скорости ее прокачки через рабочий объем камеры обеспечивают управляемость параметром C_H .

Показано, что имеется оптимальная толщина пленок α -Si:H с точки зрения фототока и фотопроводимости. Полученные результаты исследований температурных исследований темновой и фотопроводимости хорошо коррелируют с аналогичными исследованиями выполненными Кузнецовым С.В. (МГУ им. В. Ломоносова, г. Москва).

Предложенные регрессионные модели зависимостей темновой и фотопроводимости, а также ширины запрещенной зоны от концентрации водорода позволяют выполнять предварительные прогнозные оценки этих параметров.

Список литературы: 1. Голикова О.А., Кузнецов А.Н., Кудоярова В.Х., Казанин М.М. Особенности структуры пленок аморфного гидрированного кремния, осажденных методом разложения силана на постоянном токе в магнитном поле // ФТП. – 1997. – Т. 31, № 7. – С.816-819. 2. P. Morin, Roca i Cabarrocas. MRS Proc., 336, 281 (1994). 3. N. Beldi. J. Non-Cryst. Sol., 164-166, 309 (1993). 4. Bykov M.A., Mazinov A.S. Optical spectral characteristics of thin-film constructions on the basis of hydrogenated amorphous silicon // Proceedings of SPIE. – 2005. -Vol. 6023. – P 60230Q1-60230Q9. 5. Хрипунов Г.С., Пленочные солнечные элементы NaCl/ITO/CdS/CdTe/Cu/Au. – Физика и химия твердого тела, т.6, №1(2005)с.149-152. 6. Кузнецов С.В., Теруков Е.И. Влияние хвостов зон α -Si:H на заполнение оборванных связей и величину фотопроводимости // ФТП. – 2001. – Т.35, вып. 6. – С.684-686. 7. Кузнецов С.В., Эффект Стеблера – Вронского и температурные зависимости фотопроводимости α -Si:H р-типа // ФТП. – 2000. – Т. 34, вып. 6. – С.748-752. 8. Быков М.А., Слипенченко Н.И., Зуев С.А. Модель токопереноса в гетероструктуре аморфный-монокристаллический кремний // Сб. науч. трудов 3-й Международ. науч. конф. «Электронная компонентная база микро-, опто и нанoeлектроники» – Харьков – Кацивели – 2010г. – С. 245-247. 9. M. Pinarbasi, N. Maley, M.J. Kushner, A. Myers, J.R. Abelson, J.A. Thornton. Effect of hydrogen on the microstructural, optical, and electronic properties of α -Si:H thin films deposited by direct current magnetron reactive sputtering // J. Vac. Sci. Technol. A, Vol. 7, № 3, May/Jun 1989. 10. G. Budaguan, A.A. Aivazov, A.A. Sherchenkov, A.V. Buriukov, V.D. Chernomordic, J.W. Metesellar. The properties of α -Si:H/c-Si heterostructures prepared by 55 kHz PECVD for solar cell application // Materials Research Society Symp. Proc. Vol. 485, 1998, p. 303-308.

ОЦЕНКА ТЕКУЩИХ УСЛОВИЙ ЗАГОРИЗОНТНОГО РАСПРОСТРАНЕНИЯ УКВ ПО ЗАДАННОМУ ПРОСТРАНСТВЕННОМУ РАСПРЕДЕЛЕНИЮ КОЭФФИЦИЕНТА ПРЕЛОМЛЕНИЯ ВОЗДУХА

Введение

Для повышения надежности и эффективности систем радиолокации, радионавигации связи необходимы сведения о текущих условиях распространения радиоволн вблизи радиогоризонта и за его пределами [1]. Задача диагноза условий распространения ультракоротковолни длительное время была предметом многочисленных экспериментальных и теоретических исследований и остается актуальной в настоящее время [1, 2].

Анализ известных методов расчета поля при распространении радиоволн над земной поверхностью содержат монографии [3 – 6] и ряд обзоров [2, 7 – 9]. В большинстве методов расчета, дающих в пределе точное решение, предполагается, что диэлектрическая проницаемость воздуха ϵ зависит только от одной координаты – высоты h над поверхностью Земли. Лишь в этом случае, как отмечает Е.Л. Фейнберг [3], из уравнений Максвелла можно вывести уравнение, по форме совпадающее с волновым уравнением, но с волновым числом, зависящим от координаты h . При этом принципиально можно получить решение уравнения методом аппроксимации произвольного высотного профиля $\epsilon(h)$ кусочно-линейной или кусочно-параболической функцией. Такой путь решения задачи используется для расчета коэффициента ослабления поля при распространении радиоволн над обширными акваториями, где зависимость $\epsilon(h)$ сохраняет свои особенности на больших расстояниях и практически определяет характер распространения радиоволн над водной поверхностью [2].

В прибрежных зонах и над сушей коэффициент преломления существенно зависит от горизонтальных координат, и эта зависимость подвержена весьма сильным суточным и сезонным изменениям. Для расчета поля за радиогоризонтом в этом случае можно вернуться к одной из первых попыток решения задачи дифракции на поверхности Земли, подробно рассмотренной в работе [3]. Анализируя полное решение, полученное методом параболического уравнения, Е.Л. Фейнберг отмечает, что «вблизи горизонта, в тени можно получить простой и важный результат: функция ослабления совпадает с той, которая получается для дифракции Френеля на некотором эквивалентном плоском экране». Этот вопрос также подробно анализируется в работе [10]. Заменять дифракцию от сферической поверхности Земли дифракцией Френеля от прямолинейного края плоского экрана, находящегося на расстоянии радиогоризонта, можно при выполнении двух условий. Во-первых, высоты источника h_1 и точки наблюдения h_2 над земной поверхностью должны удовлетворять неравенству [3]

$$\sqrt{h_{1,2}} \gg 10 \sqrt[3]{\lambda},$$

где λ – длина волны. Во-вторых, расстояние от границы геометрической тени до точки наблюдения должно быть значительно меньше, чем до поверхности Земли. Таким образом, область френелевской дифракции охватывает только сравнительно малые «погружения» в тень.

Область применимости дифракционного интеграла Френеля-Кирхгофа значительно расширяется, если в качестве граничного поля рассматривается поле волны, испытавшей воздействие неоднородной среды и земной поверхности при распространении от источника до некоторой плоскости Q (рис. 1) в средней части трассы. Результаты расчетов поля таким путем и сравнение их с экспериментальными данными приведены в работе [11].

В отличие от метода параболического уравнения, здесь нет ограничений на пространственную структуру диэлектрической проницаемости ϵ среды, кроме требования малости флуктуаций $\tilde{\epsilon}$ по сравнению со средним значением $\bar{\epsilon}$.

Ниже рассматривается методика приближенного расчета поля вблизи границы геометрической тени с применением дифракционного интеграла Френеля – Кирхгофа и расчетом граничного поля методом геометрической оптики (МГО).

Порядок расчета

Предположим, что известно поле $U_Q(\mathbf{r})$ на некоторой поверхности Q в средней части тропосферной трассы (см. рис.1), причем та часть поверхности, на которой $U_Q \neq 0$, находится в зоне прямой видимости передающей 1 и приемной 2 антенн. Тогда поле в точке наблюдения 2 приближенно можно найти, используя интегральную теорему Кирхгофа [12] и полагая, что при $x > 0$ источники отсутствуют. С другой стороны, U_Q – это поле источника излучения, испытавшее влияние неоднородной среды и поверхности Земли при распространении до поверхности Q . Если известно распределение в пространстве диэлектрической проницаемости $\epsilon(\mathbf{r})$ на этом участке трассы, то U_Q можно рассчитать методом геометрической оптики (МГО) [13].

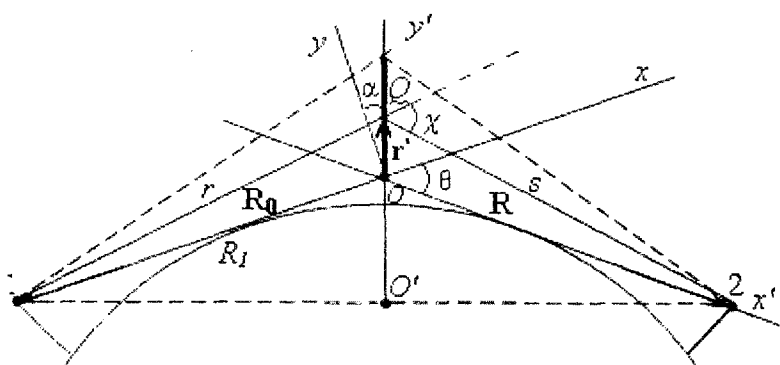


Рис. 1

Известно [13], что дисперсия уровня расходящейся сферической волны при распространении в среде со случайными неоднородностями в 10 раз меньше, чем в плоской волне. В нашем случае это позволяет пренебречь амплитудными флуктуациями и свести задачу к вычислению только флуктуаций фазы. При этом, как отмечается в работе [13], результаты вычислений могут сохранять силу и за пределами применимости

МГО. Амплитудные значения U_Q рассчитываются по интерференционным формулам [14], поскольку по условию область, в которой $U_Q \neq 0$, находится в зоне прямой видимости передающей антенны.

Такой путь расчета позволяет при малых углах $|\theta|$ (см. рис.1) получить непрерывное угловое распределение комплексных амплитуд поля как в зоне прямой видимости, так и в области геометрической тени для заданной выборочной функции (реализации) $\epsilon(\mathbf{r})$.

Граничное поле

Предположим, что в области распространения волны выполняется общее условие применимости МГО [13] – малое изменение диэлектрической проницаемости ϵ среды на расстоянии равном длине волны λ . Будем считать, что поле падающей волны в каждой точке приближенно имеет структуру плоской волны:

$$U = Ae^{j\psi} = Ae^{jk_0\varphi},$$

где $k_0 = 2\pi/\lambda$ – волновое число в вакууме, φ – фазовый путь волны (эйконал).

В этом случае справедливо уравнение эйконала [13]

$$(\nabla\varphi)^2 = \epsilon, \quad (1)$$

где $\nabla\varphi$ – градиент эйконала по направлению лучевой траектории l .

Решение уравнения (1) при малых изменениях $\varepsilon(\mathbf{r})$ можно найти методом возмущений. Пусть

$$\varepsilon(\mathbf{r}) = \bar{\varepsilon} + \tilde{\varepsilon}(\mathbf{r}), \quad (2)$$

причем среднеквадратическое отклонение σ_{ε} случайной составляющей $\tilde{\varepsilon}$ мало по сравнению со средним значением $\bar{\varepsilon}$. Следуя [13], представим φ в виде ряда

$$\varphi = \varphi_0 + \varphi_1 + \varphi_2 + \dots \quad (3)$$

и будем полагать, что φ_0 удовлетворяет уравнению

$$(\nabla\varphi_0)^2 = \bar{\varepsilon}. \quad (4)$$

При распространении волн в тропосфере справедливо неравенство $|\nabla\varphi_1| \ll |\nabla\varphi_0|$, причем $|\nabla\varphi_0| \approx 1$. Поэтому после подстановки (2) и (3) в уравнение эйконала (1) можно пренебречь слагаемым $(\nabla\varphi_1)^2$. Тогда с учетом (4) получается уравнение для вычисления поправки первого порядка φ_1 :

$$2(\nabla\varphi_0 \nabla\varphi_1) = \tilde{\varepsilon}. \quad (5)$$

Для нулевого приближения φ_0 можем записать

$$\nabla\varphi_0(\mathbf{r}) = \mathbf{l}\sqrt{\bar{\varepsilon}(\mathbf{r})}, \quad (6)$$

где $\mathbf{l}$ – единичный вектор касательной к «невозмущенной» лучевой траектории в точке $\mathbf{r}$.

Подставляя (6) в уравнение (5), получим

$$2(\nabla\varphi_0 \nabla\varphi_1) = 2\sqrt{\bar{\varepsilon}}(\mathbf{l} \nabla\varphi_1) = 2\sqrt{\bar{\varepsilon}} \frac{d\varphi_1}{dl} = \tilde{\varepsilon},$$

откуда

$$\varphi_1(L) = \frac{1}{2} \int_0^L \frac{\tilde{\varepsilon}(l)}{\sqrt{\bar{\varepsilon}}} dl. \quad (7)$$

В выражении (7) интегрирование ведется вдоль траектории l невозмущенного луча, а L – дистанция, пройденная волной. Невозмущенный эйконал, очевидно, $\varphi_0 = \sqrt{\bar{\varepsilon}}L$.

Поскольку в тропосфере $\bar{\varepsilon} \approx 1$, поправка первого порядка вдоль луча l

$$\varphi_1(L) \approx \frac{1}{2} \int_0^L \tilde{\varepsilon}(l) dl. \quad (8)$$

Если на участке L трассы тропосферного распространения волну приближенно можно считать плоской в области Q_1 волнового фронта, т.е. полагать $U(x) = Ae^{jkx}$, то для вычисления эйконала в области Q получаем выражение

$$\varphi(L, y, z) \approx \varphi_0(L) + \varphi_1(L, y, z) \approx \sqrt{\bar{\varepsilon}}L + \frac{1}{2} \int_0^L \tilde{\varepsilon}(x, y, z) dx. \quad (9)$$

Амплитудные значения граничного поля вычисляются с учетом коэффициента ослабления в области прямой видимости [14]:

$$V = \sqrt{1 + |\Phi|^2 D^2 - 2|\Phi|D \cos(2\pi\Delta r/\lambda)},$$

где $|\Phi|$ – модуль коэффициента отражения от плоской земной поверхности, Δr – разность хода между прямой и отраженной волнами, D – коэффициент, учитывающий уменьшение

$|\Phi|$ при отражении от сферической поверхности Земли. Значение $|\Phi|$ для волн горизонтальной и вертикальной поляризаций при малых углах скольжения γ в дециметровом диапазоне волн можно вычислить по формулам [14]

$$|\Phi_{gor}| = 1 - \frac{2 \sin \gamma}{\sqrt{\varepsilon_2 - 1}}, \quad |\Phi_{vert}| = 1 - \frac{2 \varepsilon_2 \sin \gamma}{\sqrt{\varepsilon_2 - 1}},$$

где ε_2 – диэлектрическая проницаемость поверхности Земли.

Разность хода Δr , угол скольжения γ и коэффициент расходимости D выражаются через приведенные высоты h_1' и h_2' , т.е. высоты точек излучения и наблюдения поля над плоскостью, касательной к земной поверхности в точке отражения:

$$\Delta r = \frac{2h_1' h_2'}{R}; \quad D = \left[\sqrt{1 + \frac{2R_1^2 h_1' h_2'}{a_3 (h_1' + h_2')^3}} \right]^{-1}; \quad \text{tg} \gamma \approx \gamma = \frac{h_1' + h_2'}{R_1}.$$

В этих выражениях a_3 – эквивалентный радиус Земли, R_1 – расстояние от источника излучения 1 до плоскости Q по поверхности Земли.

Для вычисления приведенных высот используются следующие соотношения [14]:

$$h_1' = h_1 (1 - \zeta^2), \quad h_2' = h_2 (1 - \zeta^2), \quad \zeta = R_1 / R_{np} = R_1 / (\sqrt{2a_3} (\sqrt{h_1} + \sqrt{h_2})),$$

где h_1 – высота фазового центра источника излучения над поверхностью Земли; h_2 – высота точки, в которой рассчитывается множитель ослабления на плоскости Q , относительно земной поверхности.

Обозначим модуль множителя ослабления на плоскости y, z как $V(\mathbf{r}')$. Тогда амплитуда граничного поля без учета диаграммы направленности антенны передатчика $|A(\mathbf{r}')| = A_0 V(\mathbf{r}')$.

Комплексная амплитуда граничного поля

$$A(\mathbf{r}') = |A(\mathbf{r}')| e^{jk\varphi} = A_0 V(\mathbf{r}') e^{jk\varphi}, \quad (10)$$

где φ – эйконал (9).

Поле в зоне дифракции Френеля

Предположим, что в результате решения первой части задачи найдено поле U_Q на плоскости Q (см. рис.1) и при $x > 0$ отсутствуют источники вторичных волн. Тогда расчет поля в точке наблюдения 2 сводится к хорошо известной задаче, которая решается с применением интегральной теоремы Гельмгольца – Кирхгофа [12]:

$$U(\mathbf{R}) = \frac{1}{4\pi} \oint_S \left\{ U \frac{\partial}{\partial n} \left[\frac{\exp(jks)}{s} \right] - \frac{\exp(jks)}{s} \frac{\partial U}{\partial n} \right\} dS, \quad (11)$$

где S – замкнутая поверхность, образованная плоскостью y, z и полусферой бесконечно большого радиуса; $s = |\mathbf{s}| = |\mathbf{R} - \mathbf{r}'|$ – расстояние от точки наблюдения до элемента dS в области Q ; $\frac{\partial}{\partial n}$ обозначает дифференцирование по направлению внутренней нормали $\mathbf{n}$ к поверхности интегрирования, $\mathbf{R}$ – радиус-вектор точки наблюдения 2, $\mathbf{r}'$ – радиус-вектор элемента dS в области Q .

Метод Кирхгофа расчета $U(\mathbf{R})$ предполагает равенства $U_Q(\mathbf{r}) = U(\mathbf{r})$; $\frac{\partial U_Q}{\partial n} = \frac{\partial U}{\partial n}$ в ограниченной области Q и равенство нулю поля U и его производных на всей остальной части поверхности S . При этом интеграл по полусфере обращается в нуль. В работе [3] показано, что такое приближение вполне допустимо в случае закрытых тропосферных трасс, когда точка пересечения касательных к поверхности Земли (точка O на рис. 1) находится выше земной поверхности.

Поле падающей волны в области Q запишем в виде

$$U_Q(\mathbf{r}') = A(\mathbf{r}') \frac{\exp(jkr)}{r},$$

где $r = |\mathbf{r}' - \mathbf{R}_0|$ – расстояние от источника до элемента dS , $A(\mathbf{r}')$ – комплексная функция, не зависящая от r и равная нулю за пределами области Q . Тогда

$$\frac{\partial U_Q}{\partial n} = \frac{A(\mathbf{r}')}{r} \left(jk - \frac{1}{r} \right) \cos(\mathbf{n}, \mathbf{r}).$$

Пренебрегая в производных по нормали слагаемыми, содержащими в знаменателях r^2 и s^2 , получим из (11) дифракционный интеграл Френеля – Кирхгофа [12]:

$$U(\mathbf{R}) = -\frac{j}{2\lambda} \iint_Q \frac{A(\mathbf{r}')}{rs} e^{jk(s+r)} [\cos(\mathbf{n}, \mathbf{r}) - \cos(\mathbf{n}, \mathbf{s})] dS. \quad (12)$$

Выражение (12) справедливо и в том случае, когда Q – часть сферической поверхности радиуса r_0 , совпадающей с фронтом падающей волны. В этом случае $\cos(\mathbf{n}, \mathbf{r}) = \cos(\mathbf{n}, \mathbf{r}_0) = 1$, и если обозначить $\chi = \pi - (\mathbf{r}, \mathbf{s})$, то интеграл (12) приводится к виду

$$U(\mathbf{R}) = -\frac{j}{\lambda} \iint_Q \frac{A(\mathbf{r}') \exp[jk(r+s)]}{rs} \frac{(1 + \cos \chi)}{2} dS. \quad (13)$$

В подынтегральном выражении (13) множитель $(1 + \cos \chi)/2$ – это коэффициент наклона [12], который, по определению, достигает максимума в центре первой зоны Френеля, т.е. при $\chi = 0$. В этом случае векторы $\mathbf{r}_0$ и $\mathbf{s}$ коллинеарны, а так как они пересекаются в точке $\mathbf{r}'$, то при $\chi = 0$ они лежат на одной прямой.

Таким образом, в однородной среде центр первой зоны Френеля всегда находится на прямой, соединяющей фазовый центр источника и точку наблюдения, независимо от выбора системы координат и начала вектора $\mathbf{r}'$. Этот факт имеет значение при расчетах поля на закрытых тропосферных трассах, поскольку в «общей» области диаграмм направленности приемной и передающей антенн получается весьма сложная фазовая структура поля.

Преобразуем общее выражение (13) так, чтобы учесть геометрические размеры трассы распространения радиоволн. Предположим, что источник излучения и точка наблюдения находятся на оси $O'x'$ прямоугольной системы координат x', y', z' , а область Q – на плоскости y', z' (см. рис. 1). Координаты элемента поверхности dS в области Q определяются радиус-вектором $\mathbf{r}'\{y', z'\}$.

Как правило, на тропосферных трассах размеры области Q , на которой $U_Q(\mathbf{r}') \neq 0$, значительно меньше расстояний от этой области до источника (R_0) и приемной антенны (R), т.е. выполняются неравенства:

$$R_0 = |\mathbf{R}_0| \gg |\mathbf{r}'|, \quad R = |\mathbf{R}| \gg |\mathbf{r}'|. \quad (14)$$

В силу неравенств (14) в знаменателе подынтегрального выражения (13) можно полагать $r \approx R_0$, $s \approx R$, а в показателе степени использовать разложения [15]:

$$r = |\mathbf{r}' - \mathbf{R}_0| \approx R_0 - \mathbf{r}'\mathbf{n}_0 + (\rho^2 / 2R_0) - \dots,$$

$$s = |\mathbf{R} - \mathbf{r}'| \approx R - \mathbf{r}'\mathbf{n}_s + (\rho^2 / 2R) - \dots,$$

где $\rho^2 = y'^2 + z'^2$, единичный вектор $\mathbf{n}_0$ направлен из точки $\mathbf{r}'$ в точку, где находится источник излучения, а единичный вектор $\mathbf{n}_s$ – из точки $\mathbf{r}'$ в точку наблюдения. Угол χ в случае тропосферных трасс средней протяженности составляет единицы градусов. Поэтому можно полагать $(1 + \cos \chi)/2 \approx 1$, и тогда выражение (13) с учетом (9) и (10) приводится к следующему виду:

$$U(\mathbf{R}) = \frac{k_0 e^{jk(R_0 + R)}}{j2\pi R_0 R} \iint_Q e^{-j\mathbf{K}\mathbf{r}'} \left[A(\mathbf{r}') \exp \left\{ \frac{jk\rho^2}{2} \left(\frac{1}{R_0} + \frac{1}{R} \right) \right\} \right] d^2 r', \quad (15)$$

где $\mathbf{K} = k\mathbf{n}_s - k\mathbf{n}_0$, $A(\mathbf{r}') = A_0 V(\mathbf{r}') \exp\{jk_0 \varphi_1(\mathbf{r}')\}$, $\varphi_1(\mathbf{r}') = \varphi_1(R_0, y', z)$ – поправка к эйконалу первого порядка.

Поскольку $|A(\mathbf{r}')| \neq 0$ в ограниченной области Q и $|A(\mathbf{r}')| = 0$ вне этой области, пределы интегрирования в (15) можно заменить бесконечными. Тогда интеграл (15) – это двумерное преобразование Фурье функции, записанной в квадратных скобках.

Для расчетов поля над сферической поверхностью Земли выбрана другая система прямоугольных координат, в которой ось x находится на границе геометрической «тени», а начало координат – на пересечении касательных к поверхности Земли, проведенных через точки расположения передатчика 1 и приемника 2 (см. рис. 1). Переход к новой координатной системе x, y, z соответствует параллельному переносу вдоль оси y' на величину отрезка OO' длиной y_0 и повороту на малый угол $\alpha = \theta/2 \ll 1$ вокруг оси z . В новой системе координат $z = z'$, $y = (y' - y_0) \cos \alpha \approx y' - y_0$.

Поскольку $\alpha \ll 1$, радиус-вектор $\mathbf{r}$ элемента dQ на плоскости y, z практически не изменяется, т.е. $\mathbf{r} \approx \mathbf{r}'$.

Обозначив $\rho_F = \sqrt{(y - y_0)^2 + z^2}$, для комплексной амплитуды поля в точке наблюдения $\mathbf{R}$ без учета детерминированного фазового сдвига $\Delta\psi = k(R_0 + R) - \pi/2$ получим окончательное выражение:

$$U(\mathbf{R}) = \frac{k}{2\pi R_0 R} \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} e^{-j\mathbf{K}\mathbf{r}} e^{\frac{jk\rho_F^2}{2} \left(\frac{1}{R_0} + \frac{1}{R} \right)} A_0 V(\mathbf{r}) e^{jk_0 \varphi_1(\mathbf{r})} d^2 r. \quad (16)$$

где k_0 – волновое число в вакууме, k – волновое число в воздухе при $\varepsilon = \bar{\varepsilon} = \text{const}$.

Результаты расчета

Пределы применимости выражения (16) определяются, кроме оговоренных требований к характеристикам трассы распространения радиоволн, условиями применимости первого приближения МГО. Эти условия в монографии [13] сформулированы в виде ограничений на дистанцию L , длину волны λ , размеры $d_{1,2}$ области Q_1 поверхности «входа» волны в неоднородную среду и главные радиусы кривизны фазового фронта волны $R_{\phi 1,2}$:

$$\frac{L}{\lambda} \ll \left[\left(\frac{2\lambda}{d_{1,2} \cos \theta_1} \right)^2 - \left| \frac{\lambda}{R_{\phi 1,2}} \right| \right]^{-1}, \quad (17)$$

где θ_1 – угол между ортом луча $\mathbf{l}^0$ и нормалью к поверхности Q_1 .

В нашем случае $\theta_1 \approx 0$, $R_{\phi 1,2} < 0$, т.к. фронт волны расходящийся (выпуклый). Известно [13], что условие $R_{\phi 1,2} < 0$ соответствует отсутствию каустик, если удовлетворяется необходимое условие применимости МГО

$$\lambda |\text{grade}| \ll \varepsilon. \quad (18)$$

При достаточно больших $|R_{\phi 1,2}|$ из (17) следует

$$\lambda L \ll d_{1,2}^2 / 4. \quad (19)$$

Если в (19) дистанция L соизмерима с расстоянием R_0 (см. рис. 1) и составляет несколько десятков километров, то при $d_{1,2} \sim 300$ м максимальная длина волны соответствует дециметровому диапазону.

Изложенная методика расчета использовалась для вычисления поля в зоне прямой видимости и за радиогоризонтом по высотным профилям индекса рефракции $N(h)$, измеренным над морем. Результаты расчетов и сравнение их с материалами экспериментальных исследований, выполненных в ИРЭ НАН Украины, приведены в работе [11]. В ходе этих экспериментальных работ передатчик располагался на борту самолета, совершавшего полеты на фиксированной высоте над поверхностью моря. Профиль индекса рефракции измерялся в средней части трассы длиной R .

На рис. 2 приведены результаты расчета множителя ослабления $V(R)$, выполненные для высоты передающей антенны $h_1 = 100$ м, приемной антенны – $h_2 = 25$ м и длины волны $\lambda = 0,35$ м. Профили 1 и 2 (рис. 2, а) близки к профилю в «стандартной» атмосфере, нанесенному сплошной линией. Сплошная линия на рис. 2, б соответствует экспериментальной измеренной зависимости $V(R)$, а штриховая и пунктирная – результатам расчета. Расстояние радиогоризонта передатчика $R_{p2} = 42$ км.

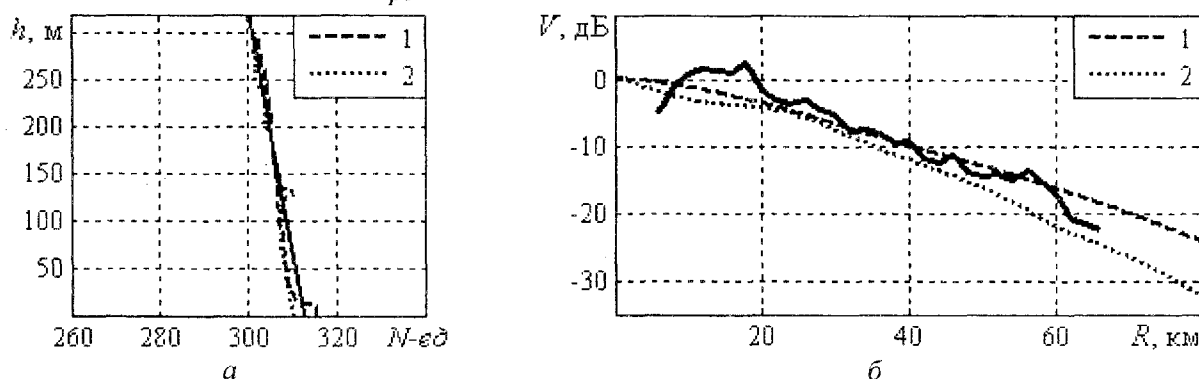


Рис.2

В работе [2] приведены экспериментально полученные над океаном зависимости множителя ослабления от высоты передатчика $V(h_1)$ для высотного профиля индекса рефракции $N(h)$, изображенного на рис. 3, а. При измерении зависимости $V(h_1)$ приемная антенна располагалась на высоте $h_2 = 30,5$ м на берегу океана. Передающая аппаратура находилась на борту самолета, траектория полета которого имела сложную форму с периодическим изменением высоты h_1 от 10 м до 1200 м. Профиль $N(h)$ (рис. 3, а) характеризуется наличием

мощного приповерхностного волновода. Применение описанной методики расчета к такому профилю индекса рефракции для длины волны $\lambda = 0,58$ м при протяженности трассы $R = 148$ км приводит к результатам, показанным на рис. 3, б штриховой линией. Сплошной линией нанесена экспериментальная зависимость $V(h_1)$ (по данным работы [2]).

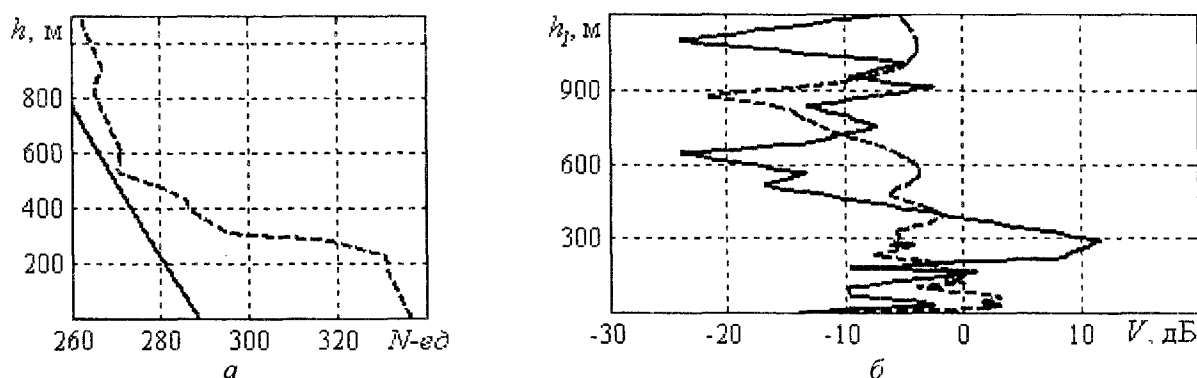


Рис.3

Как видно из рисунка, несмотря на то, что метод не предназначен для решения задач волноводного распространения радиоволн, расчетные и экспериментальные данные лучше согласуются именно в области высот до 200 м. В этом интервале высот отличие не превышает 10 дБ даже в том случае, если профиль $N(h)$ «сглаживается» для уменьшения градиента индекса рефракции в соответствии с условием (18). Для $h_1 > 200$ м расхождения достигают 20 дБ, и расчет позволяет лишь оценить характер зависимости $V(h_1)$ для этого профиля.

Выводы

Использование метода Кирхгофа с учетом неоднородности граничного поля в области пересечения диаграмм направленности передающей и приемной антенн позволяет получить оценки хода зависимости множителя ослабления V от высоты h и расстояния R по измеренной пространственной структуре индекса рефракции и получить трехмерную зависимость множителя ослабления от координат точки наблюдения.

В частном случае зависимости индекса рефракции N только от высоты h над поверхностью Земли при профилях $N(h)$ близких к «стандартной» атмосфере наблюдается хорошее количественное совпадение результатов расчета и экспериментальных данных как в зоне прямой видимости, так и за радиогоризонтом.

Опыт применения этой методики к данным, полученным в ИРЭ НАН Украины [11], показывает, что наименьшие количественные расхождения наблюдаются в тех случаях, когда профиль $N(h)$ не имеет ярко выраженных волноводных слоев, хотя и в этом случае общий ход расчетных кривых согласуется с экспериментальными данными, полученными в дециметровом диапазоне волн.

Сопоставление результатов расчета поля в области прямой видимости и за границей геометрической тени (в «зоне дифракции») с имеющимися экспериментальными данными показывает, что точность оценки поля и последующих расчетов дистанционной и высотной зависимостей множителя ослабления достаточна для классификации условий распространения в рамках нескольких характерных типов.

Список литературы: 1. *Диагностика условий распространения УКВ в тропосфере* / под ред. Г.И. Хлопова. – Киев : Наук. думка, 2010. – 264с. 2. *Хитни Г.В., Рихтер Ю.Х., Панперт Р.А., Андерсон К.Д., Баумгартнер Дж.Б.* Распространение радиоволн в тропосфере: Обзор // ТИИЭР. – 1985. – т.73, №2. – С.106-128. 3. *Фейнберг Е.Л.* Распространение радиоволн вдоль земной поверхности. – М. : АН СССР, 1961. – 546 с. 4. *Фок В.А.* Проблемы дифракции и распространения электромагнитных волн. – М. : Сов. радио, 1970. – 517с. 5. *Дальнее тропосферное распространение ультракоротких волн* /

Под ред. Б.А. Введенского и др. – М. : Сов. радио, 1965. – 418с. 6. *Татарский В.И.* Распространение волн в турбулентной атмосфере. – М.: Наука, 1967. – 226с. 7. *Шур А.А.* Характеристики сигнала в тропосферных радиолиниях. – М.: Связь, 1972. – 105с. 8. *R.K. Crane* A review of transhorizon propagation phenomena // *Radio Science*, vol. 16, No 5, Sept.-Oct. 1981, PP. 649-669. 9. *Высоковский Д.М.* Некоторые вопросы дальнего тропосферного распространения ультракоротких волн. – М. : Изд-е Акад.наук СССР, 1985. – 110с. 10. *Фок В.А.*, Дифракция Френеля от выпуклых тел // *УФН*. – 1950. – №43. – С.587-599. 11. *Жуков Б.В., Ключева А.Н., Петров В.А.* Оценка дистанционных зависимостей УВЧ радиополя над морем для произвольных высотных профилей коэффициента преломления воздуха // *Радиотехника*. – 2011. – Вып.164. – С. 58-65. 12. *Борн М., Вольф Э.* Основы оптики. – М.: Наука, 1973. – 719 с. 13. *Кравцов Ю.А., Орлов Ю.И.* Геометрическая оптика неоднородных сред. – М.: Наука, 1980. – 304с. 14. *Калинин А.И.* Распространение радиоволн на трассах наземных и космических радиолиний. – М.: Связь, 1979. – 296с. 15. *A.N. Klyueva and V.A. Petrov* Tropospheric Radiowave Propagation: Diffraction Field in the Fresnel Zon // *Telecommunications and Radio engineering*, – 2010. Vol 69, No.12. – P.1031 – 1039.

*Харьковский национальный
университет радиоэлектроники*

Поступила в редколлегию 23.06.2011.

МОДЕЛИРОВАНИЕ РАССЕИВАНИЯ ПОЛЯ ЭЛЕКТРИЧЕСКОГО РАДИАЛЬНОГО ДИПОЛЯ ОДИНОЧНЫМ ПОЛУПРОЗРАЧНЫМ КОНУСОМ С ПРОДОЛЬНЫМИ ЩЕЛЯМИ

Введение

Задачам рассеивания электромагнитных волн на идеально проводящих структурах посвящены работы [1 – 3]. Однако для практических приложений большой интерес представляют собой задачи дифракции на неидеально проводящих телах, в частности диэлектрических поверхностях. Конические структуры благодаря своим широкополосным свойствам нашли широкое применение в радиотехнике, радиофизике, радиоизмерениях. В отличие от задач дифракции волн на идеально проводящих конусах, решение которых было найдено как аналитически, так и численно, решение задачи рассеивания волн на диэлектрических конусах получено только численно [4]. Аналитические решения позволяют качественно изучить структуру рассеянного поля, его характерные особенности, а также свойства рассеивающих поверхностей, которые трудно выявить численно. В связи с отсутствием аналитического решения для диэлектрического конуса были предложены модельные задачи рассеивания волн на неидеально проводящих конусах [5]. Однако в краевых условиях импедансного типа, которые были использованы в таких задачах, отсутствует параметр, который содержит угол раскрытия конуса, влияющий на точность решения рассматриваемой задачи. Незамкнутые полупрозрачные поверхности, способные пропускать и отражать падающее поле, являются моделями неидеально проводящих структур и применяются в качестве элементов современных радиоэлектронных приборов. Наличие щелей на поверхности рассеивающего тела расширяет рамки их использования, но и усложняет процесс решения подобных задач в связи с появлением ребер, влияние которых также необходимо учитывать.

Цель работы – исследование модельной электродинамической задачи возбуждения электрическим радиальным диполем одиночного полупрозрачного конуса с периодическими продольными щелями, получение численных, а также аналитических решений.

Постановка задачи. Метод решения

В работе рассматривается задача о возбуждении одиночного полупрозрачного конуса с периодически прорезанными вдоль образующих конуса N щелями (рис. 1).

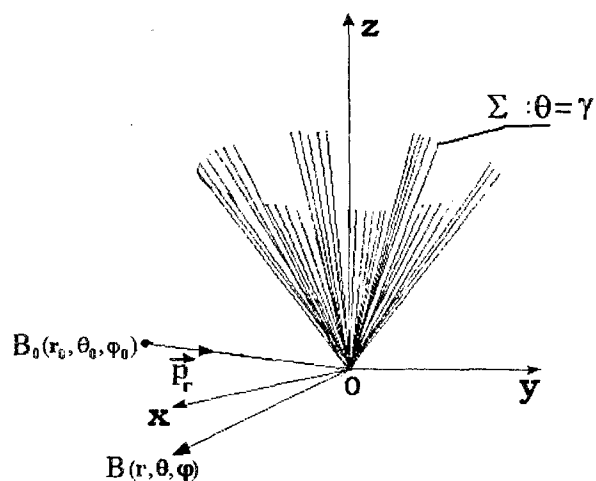


Рис. 1. Полупрозрачный конус с продольными щелями

В качестве источника возбуждения рассматривается электрический радиальный диполь, поле которого изменяется во времени согласно гармоническому закону вида $e^{ia\omega t}$, $a = \pm 1$. Для удобства решения задачи вводится сферическая система координат r, θ, φ с началом в вершине конуса. Коническая поверхность Σ в данной системе координат определяется уравнением $\theta = \gamma$; d – угловая ширина щели, середина которой проходит через плоскость $\varphi = 0$. Искомое полное электромагнитное поле $\vec{E}, \vec{H}$ представляется в виде суммы поля источника $\vec{E}_0, \vec{H}_0$ и поля, рассеянного конической структурой $\vec{E}_1, \vec{H}_1$:

$$\vec{E} = \vec{E}_0 + \vec{E}_1,$$

$$\vec{H} = \vec{H}_0 + \vec{H}_1,$$

Полное электромагнитное поле удовлетворяет следующим условиям:

1. Уравнениям Максвелла;
2. Краевому условию на поверхности конуса

$$\begin{cases} \vec{n} \times \left\{ \vec{n} \times \left[\vec{E}^+ + \vec{E}^- \right] \right\} = 2\tilde{P}^{(1)} \vec{n} \times L \left[\vec{H}^+ - \vec{H}^- \right], \\ \vec{n} \times \vec{E}^+ - \vec{n} \times \vec{E}^- = 0; \quad \sum : \theta = \gamma; \end{cases}$$

$$\tilde{P}^{(1)} = \frac{w}{q} W_1 \sin \gamma, \quad w = \sqrt{\mu/\varepsilon}, \quad q = iak, \quad \vec{E}^\pm = \vec{E}|_{\theta=\gamma \pm 0}, \quad k - \text{волновое число};$$

3. Условию на бесконечности в пространстве;
4. Условию ограниченности энергии.

Для удобства решения задачи вводим потенциалы Дебая υ , таким образом осуществляя переход от исходной электродинамической задачи к краевой задаче математической физики. В соответствии со структурой полного поля, общий потенциал Дебая представляется в виде суммы потенциалов:

$$\upsilon = \upsilon_0 + \upsilon_1.$$

где υ_0 – потенциал источника, υ_1 – потенциал, характеризующий отраженное от конической структуры поле. Воспользуемся интегральными преобразованиями Конторовича – Лебедева, вследствие чего получаем следующие выражения для искомого потенциала:

$$\upsilon_1 = \frac{2}{\pi^2} \int_0^{+\infty} \tau \operatorname{sh}(\pi\tau) \hat{\upsilon}_1 \frac{K_{i\tau}(qr)}{\sqrt{r}} d\tau, \quad \hat{\upsilon}_1 = \int_0^{+\infty} \upsilon_1 \frac{K_{i\tau}(qr)}{\sqrt{r}} d\tau,$$

где

$$\begin{aligned} \hat{\upsilon}_1 &= -a_{0,\tau} b_{0,\tau} U_{0,\tau}(\theta, \varphi), \\ U_{0,\tau}(\theta, \varphi) &= \sum_{n=-\infty}^{+\infty} x_n \frac{P_{-1/2+i\tau}^n(\pm \cos \theta)}{P_{-1/2+i\tau}^n(\pm \cos \gamma)} e^{inN\varphi}. \end{aligned} \quad (1)$$

$K_{i\tau}(qr)$ – функция Макдональда, $a_{0,\tau}$, $b_{0,\tau}$ – известные коэффициенты, $P_{-1/2+i\tau}^n(\pm \cos \theta)$ – функция Лежандра первого рода. Знак «+» в (1) соответствует области $0 < \theta < \gamma$, а «-» – области $\gamma < \theta < \pi$. x_n – неизвестные коэффициенты, являющиеся решениями следующей системы функциональных уравнений:

$$\begin{aligned} \sum_{n=-\infty}^{+\infty} \left(1 + 2W \frac{N|n|}{n} (1 - \varepsilon_n) \right) x_n e^{inN\varphi} &= 1 \text{ на лентах конуса,} \\ \sum_{n=-\infty}^{+\infty} N \frac{|n|}{n} (1 - \varepsilon_n) x_n e^{inN\varphi} &= 0 \text{ на щелях конуса,} \end{aligned}$$

где ε_n – известный матричный коэффициент, причем $\varepsilon_n = O(n^{-2})$ при $n \gg 1$.

Используя аппарат рядов Фурье, получаем следующую систему линейных алгебраических уравнений (СЛАУ):

$$x_p = \frac{1}{2\kappa_p^{(v)}} WB_{0,p} - \frac{1}{2\kappa_p^{(v)}} W \sum_{n=-\infty}^{+\infty} B_{n,p} x_n, \quad (2)$$

где

$$B_{0,p} = \begin{cases} -\frac{1}{\pi} \frac{\sin(n-p) \frac{\pi dN}{2}}{n-p}, n \neq p, \\ 1 - \frac{dN}{2}, n = p, \end{cases}, \quad \frac{\pi dN}{2} \kappa_p^{(\nu)} = N(p+\nu) \frac{|p|}{p} (1-\varepsilon_p).$$

ν – известная величина.

При таком способе возбуждения на поверхности полупрозрачного конуса наводится только поверхностный радиальный ток, плотность которого в случае осесимметричного возбуждения имеет вид:

$$j_r = \frac{2ik}{\sin \gamma} \sum_{n=-\infty}^{+\infty} e^{inN\varphi} \int_0^{+\infty} \frac{H_{i\tau}^{(2)}(kr)}{\sqrt{r}} a_0(\tau, k) |n| (1-\varepsilon_n) x_n d\tau,$$

где

$$a_0(\tau, k) = \frac{\pi}{2r_0} \tau h \pi \tau e^{\pi \tau} H_{i\tau}^{(2)}(kr_0) \frac{1}{\sqrt{r_0}} P_{-1/2+i\tau}(\cos \gamma),$$

$H_{i\tau}^{(2)}(kr_0)$ – функция Ханкеля второго рода.

Случай узких конических секторов. Аналитическое решение

В случае узких конических секторов, при $1 - \frac{dN}{2\pi} \ll 1$, искомый потенциал Дебая принимает вид

$$u_1 = -\frac{2}{\pi^2} \beta \sum_{m,n=-\infty}^{+\infty} e^{i(m+nN)\varphi} \int_0^{+\infty} \frac{\tau sh \pi \tau a_\tau b_\tau}{G_{m+nN}(W) - 1 + \beta} \frac{P_{-1/2+i\tau}^{m+nN}(\pm \cos \theta)}{P_{-1/2+i\tau}^{m+nN}(\pm \cos \gamma)} d\tau + O\left(\frac{1}{W} \beta^2 \ln \frac{1}{\beta}\right),$$

где $\beta = 1 - \frac{dN}{2\pi}$, a_τ , b_τ – известные коэффициенты,

$$G_{m+nN}(W) = 2W \frac{(-1)^{m+nN} ch \pi \tau}{\pi} \frac{\Gamma(1/2 + i\tau + m + nN)}{\Gamma(1/2 + i\tau - m - nN)} \frac{1}{P_{-1/2+i\tau}^{m+nN}(\cos \gamma) P_{-1/2+i\tau}^{m+nN}(-\cos \gamma)}.$$

В случае осесимметричного возбуждения при $\theta_0 = \pi$, $m = 0$ получаем следующее выражение для потенциала Дебая:

$$u_1 = -\frac{2}{\pi^2} \beta \sum_{n=-\infty}^{+\infty} e^{inN\varphi} \int_0^{+\infty} \frac{\tau sh \pi \tau a_\tau b_\tau}{G_{nN}(W) - 1 + \beta} \frac{P_{-1/2+i\tau}^{nN}(\pm \cos \theta)}{P_{-1/2+i\tau}^{nN}(\pm \cos \gamma)} d\tau + O\left(\frac{1}{W} \beta^2 \ln \frac{1}{\beta}\right).$$

Численный эксперимент

В работе получены зависимости значений модулей коэффициентов СЛАУ (2) от параметров задачи возбуждения полупрозрачного конуса с одной продольной щелью.

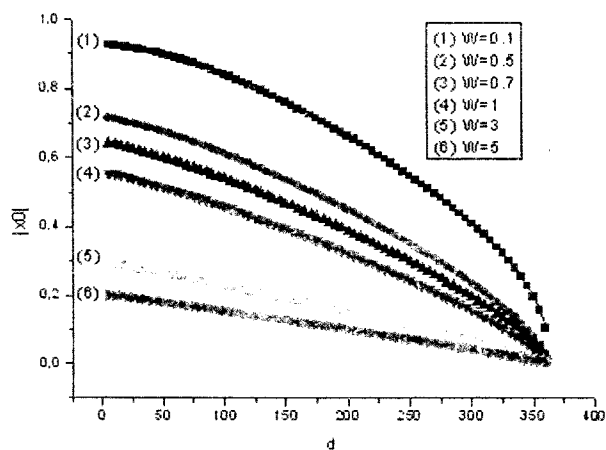


Рис. 2. Зависимость $|x_0|$ от ширины щели при разных значениях параметра полупрозрачности

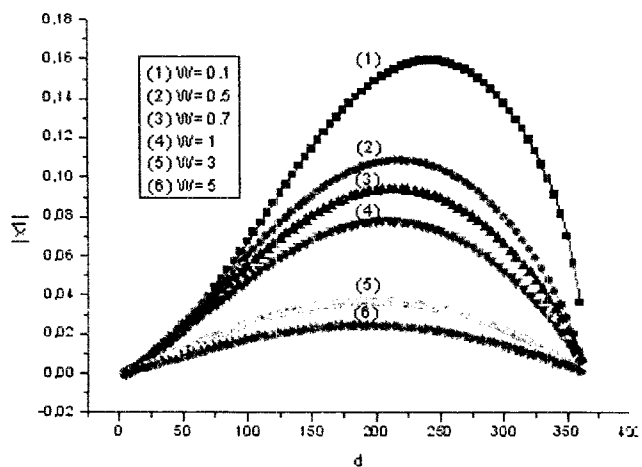


Рис. 3. Зависимость $|x_1|$ от ширины щели при разных значениях параметра полупрозрачности

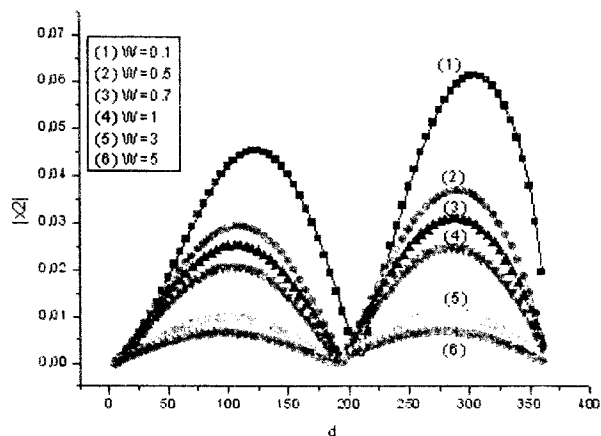


Рис. 4. Зависимость $|x_2|$ от ширины щели при разных значениях параметра полупрозрачности

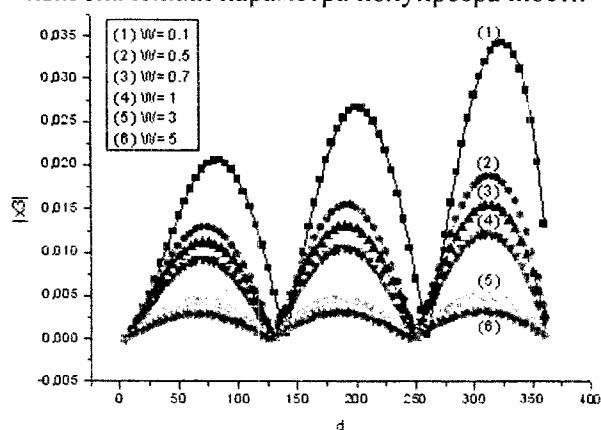


Рис. 5. Зависимость $|x_3|$ от ширины щели при разных значениях параметра полупрозрачности

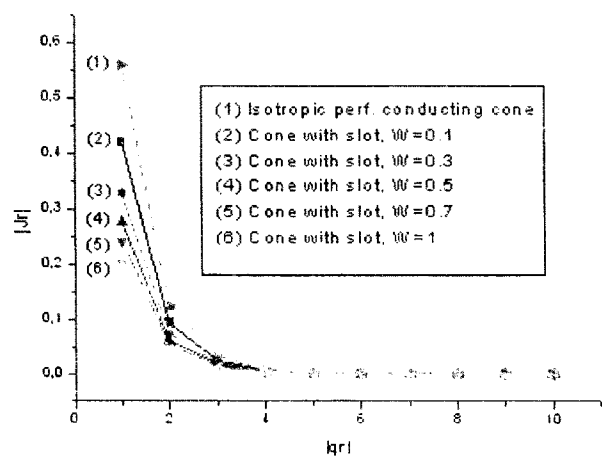


Рис. 6. Зависимость $|j_r|$ от $|q_r|$ при различных значениях параметра полупрозрачности при $\gamma = \pi/6$, $d = \pi/10$, $\varphi = d/2 + \pi/90$, а также аналогичная зависимость для сплошного идеально проводящего конуса

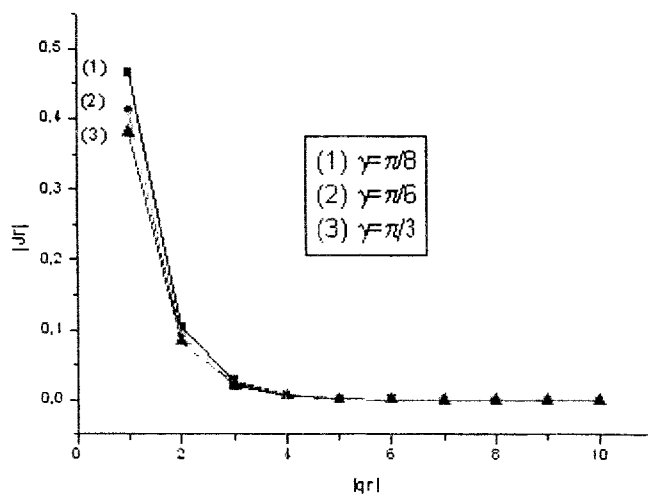


Рис. 7. Зависимость $|j_r|$ от $|q_r|$ при различных значениях угла раскрытия конуса при $W = 0.7$, $d = \pi/10$, $\varphi = d/2 + \pi/90$

На рис. 2 – 5 представлены графики зависимостей модулей коэффициентов x_0 , x_1 , x_2 , x_3 системы линейных алгебраических уравнений (2) от ширины щели при различных значениях параметра полупрозрачности. Из графиков можно заключить, что наибольшие значения коэффициентов достигаются при небольших значениях параметра полупрозрачности. При увеличении данного параметра значения коэффициентов уменьшаются. Также эти значения уменьшаются при расширении щели, что обусловлено уменьшением площади рассеивающей поверхности конуса. На рис. 6 и 7 представлены зависимости модуля одной из составляющих плотности поверхностного тока $|j_r|$ в зависимости от параметров задачи. Из вида графиков на рис. 6 можно заключить, что при увеличении параметра полупрозрачности модуль плотности поверхностного тока уменьшается. Также уменьшение этих значений происходит при удалении от вершины конуса источника, т.е. при увеличении значения $|qr|$, а при $|qr| > 4$ значения становятся близкими к нулю. На рис. 7 показаны зависимости модуля плотности поверхностного тока от $|qr|$ при различных значениях угла полураскрыва конуса. Таким образом, при увеличении угла полураскрыва конуса наблюдается уменьшение плотности поверхностного тока вследствие увеличения площади поверхности конуса.

Заключение

В работе впервые рассмотрена задача возбуждения полупрозрачного конуса с продольными щелями электрическим радиальным диполем с учетом угла полураскрыва конуса и изменения параметра полупрозрачности в зависимости от расстояния до его вершины. Моделирование поверхностных свойств такой структуры проводится с помощью усредненных краевых условий, содержащих угол раскрыва конуса. Задача решается с привлечением интегральных преобразований и аппарата рядов Фурье. Используемый метод решения позволяет получить численные и аналитические решения для особых случаев структуры. Проведено исследование зависимостей коэффициентов системы линейных алгебраических уравнений от параметров задачи. Исследовано поведение радиальной составляющей плотности поверхностного тока при осесимметричном возбуждении полупрозрачного конуса с одной щелью, получены аналитические результаты для частного случая структуры с узкими коническими секторами. В результате анализа полученных численных результатов можно делать вывод о том, что при осесимметричном возбуждении решение для полубесконечного конуса могут быть использованы при анализе свойств конечного незамкнутого полупрозрачного конуса.

Список литературы: 1. Хенл Х., Мауэ А., Вестфаль К. Теория дифракции : пер с нем.; под ред. Г.Д. Малюжинца. – М. : Мир, 1964. – 428с. 2. Фелсен Л., Маркувиц Н. Излучение и рассеяние волн: Пер. с англ. ; под ред. М.Л. Левина. – М. : Мир. – 1978. – Т1. – 552с.; Т2. – 558с. 3. Шестопалов В.П. Метод задачи Римана-Гильберта в теории дифракции и распространения электромагнитных волн. – Харьков : Изд-во Харьк. ун-та. 1971. – 400с. 5. Васильев Е.Н. Возбуждение тел вращения. – М. : Радио и связь, 1987. – 272с. 5. Bernard J.M.L., Lyalinov M.A. Electromagnetic scattering by a smooth convex impedance cone // J. of Appl. Math. – 2004. – V.69. – P.285-333.

Харьковский национальный
университет радиоэлектроники

Поступила в редколлегию 11.07.2011

О ПОСТАНОВКЕ ДИФРАКЦИОННОЙ ЗАДАЧИ ДЛЯ БИСТАТИЧЕСКОЙ ЗОНЫ СИСТЕМ РАДИОАКУСТИЧЕСКОГО ЗОНДИРОВАНИЯ АТМОСФЕРЫ

Введение

Радиоакустические системы зондирования (РАЗ) позволяют дистанционно, неконтактно измерять температуру воздуха и скорость ветра в атмосферном пограничном слое (АПС). Они находят применение как средство оценки условий распространения радиоволн, взлета и посадки самолетов, рассеяния загрязнений и прочих.

В своей более чем 50-летней истории метод РАЗ имел и периоды повышенного интереса и периоды полного отрицания [1]. Современный этап можно охарактеризовать, как стадию планомерного развития. В настоящее время в ряде развитых стран создано значительное количество систем РАЗ (рис. 1). В англоязычной литературе они именуются как RASS (Radio Acoustic Sounding System).



а



б

Рис. 1. Бистатические RASS:

а – фирмы Remtech (France, 1997), б – Radian Corporation (USA, 2003)

Однако их широкое внедрение ограничивают не решенные пока проблемы. Одной из них является отсутствие удовлетворительного решения дифракционной задачи.

Особенности современных систем РАЗ

Современное состояние определяется комплексом факторов, среди которых наиболее важными являются технические возможности, особенности объекта наблюдения и адекватность теоретического описания.

Многочисленные эксперименты позволили оптимизировать конструкцию систем РАЗ. Современные системы РАЗ создают, в основном, по бистатической схеме [2], и отличаются методами и реализациями систем компенсации ветрового сдвига. Альтернативный вариант, использовавшийся в более ранних конструкциях, дифракция в которых соответствует моностатической схеме, показан на рис. 2.

Апертуры антенн располагают в одной плоскости (рис. 3). Смещение по вертикали, как было сделано в RASS ИФА [1], сейчас не используется.

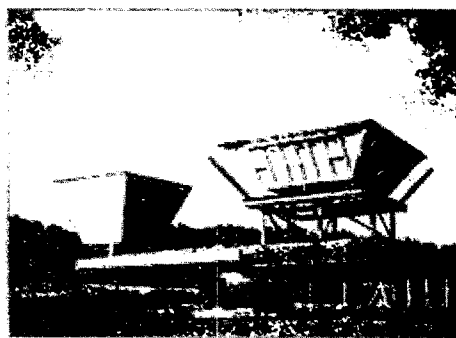


Рис. 2. Компенсация ветрового сдвига с помощью поворотной платформы (RASS фирмы Metech Germany, 1994)

Таким образом, наиболее актуальным является поиск решения дифракционной задачи для схемы, изображенной на рис. 3.

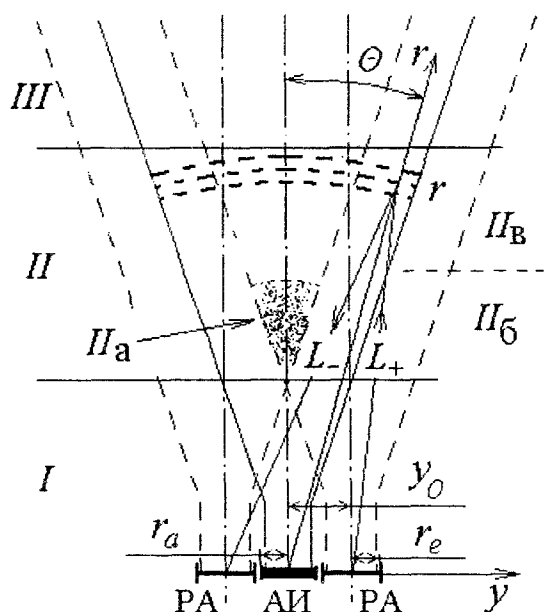


Рис. 3. Геометрическая схема взаимодействия полей в бистатических системах РАЗ

В состав систем РАЗ входит доплеровский лоцатор непрерывного излучения с разнесенными передающей и приемной радиоантеннами (РА). Такая конструкция обусловлена техническими сложностями создания совмещенного излучателя при необходимости получения высокого потенциала лоцатора. Зондирующий пакет акустических волн (показан жирными штриховыми линиями) формируется акустическим излучателем (АИ), который расположен посередине между радиоантеннами. Такое расположение определяется фокусирующим действием сферической поверхности акустического пакета.

Пространственное разрешение определяется размерами пакета акустических волн и диаграммами направленности (ДН) радиоантенн.

Одним из существенных недостатков такой схемы, является то, что с ее помощью невозможно получить данные с нижнего участка трассы зондирования. Этот участок особенно важен для сопоставления с данными наземных датчиков [3]. Следует заметить, что, конструкции, созданные по схеме аналогичной RASS, изображенной на рис.2, в этом отношении будут менее перспективны.

Особенности получения метеоинформации в бистатических системах РАЗ

На рис. 3 тонкими линиями показаны границы основных потоков мощности (ОПМ).

Внизу, в зоне нечувствительности (I), отраженный сигнал отсутствует. Вверху, на значительном удалении от антенн ($r \gg y_0$), разном y_0 можно пренебречь. Эту зону можно называть зоной моностатического приближения (III), и для вычисления температуры и ветра достаточно использовать решение дифракционной задачи в одном измерении (вдоль радиуса r). В бистатической зоне (II) сигнал существует, однако вычисление метеопараметров затруднено. Зависимости существенно усложняются. В них включаются параметры системы: разнос антенн y_0 , ширина ДН, протяженность пакета и прочие.

Получение численного решения затрудняют значительные размеры области взаимодействия. Экспериментальная оценка требует значительных затрат. Таким образом, для решения этой задачи возможен только теоретический подход. Однако в настоящее время прогресс в этой области, к сожалению, замедлился.

Наиболее важные моменты в формировании теоретических представлений метода РАЗ подробно описаны еще в [1].

Основные моменты решения дифракционной задачи РАЗ

Ранее существовало несколько ошибочных суждений, которые задержали развитие метода. Среди них можно выделить представление об отражателе как о точечной цели – радиолокационный подход. Также можно отметить представление о стоксовском механизме сдвига частоты принимаемого сигнала, что исключает возможность измерения температуры.

Здесь остановимся только на наиболее важных для дальнейшего решения моментах.

В работе [4] обоснован ряд фундаментальных положений метода. Это, во-первых, фокусировка поля отраженных электромагнитных волн, что позволило обосновать требования к бистатическому расположению антенн; это же впоследствии позволило отойти от локационных представлений. Во-вторых, что сдвиг частоты обусловлен доплеровским механизмом. Однако в этой работе использовано приближение точечных антенн.

В работе [5] анализируется пространственное распределение параметров принимаемого сигнала для систем РАЗ с апертурными антеннами. Как и в [4], рассматривается моностатическая зона. Показано, что сигнал представляет собой свертку распределений интенсивности возбуждения всех трех антенн. Этот шаг потребовал существенного усложнения аналитической модели. Хотя в моностатической зоне можно допустить ряд упрощений. В частности, использовано приближение дальней зоны для излучателей. Предполагалось, что апертура приемной антенны расположена в фокальной плоскости, на промежуточных этапах использовалось приближение геометрической оптики.

В бистатической зоне ряд этих приближений недопустим. Строгое решение может быть основано на разложении полей всех антенн по спектрам их пространственных гармоник. Но оно, очевидно, будет чрезвычайно громоздким. Поэтому здесь необходим поэтапный подход. Особенно важен этап выбора и обоснования приближений.

Условия решения задачи

Решение необходимо искать, основываясь на анализе физических факторов и технических возможностей систем РАЗ.

Физические условия определяют пространственное разрешение системы и уровень принимаемого сигнала. Их нужно учитывать, ставя задачу повышения информативности измерений. Тогда требования к ДН антенн и протяженности зондирующего пакета определяются размерами вихрей для турбулентной атмосферы и условиями выделения информации о слоях при устойчивой стратификации.

Сферическая расходимость акустических волн в свободном пространстве приводит к фокусировке отраженного электромагнитного поля. Совместно с ветровым сдвигом акустического пакета это определяет уровень сигнала и требования к местоположению антенн в горизонтальной плоскости.

К основным техническим особенностям систем РАЗ, которые необходимо учитывать при решении задачи можно отнести следующие. Во-первых, взаимосвязь y_0 с размерами апертур (r_a и r_e) и необходимой шириной ДН. Поэтому область соприкосновения ДН радиоантенн (l_a) нельзя опустить ниже определенного значения. Во-вторых, влияние выполнения условия Брэгга, которое в бистатической зоне приводит к существенному усложнению задачи.

Методика решения задачи

При решении нужно учитывать, что отражающий акустический пакет также является виртуальной антенной, и его действие наиболее удобно рассматривать с позиций теории антенн.

Упрощение аналитического решения возможно при использовании соотношений геометрической оптики и дифракции Фраунгофера. Однако их применение требует обоснования.

Наиболее важной является зависимость амплитуды сигнала от высоты – функция радиального взаимодействия (ФРВ). Отсутствие сигнала или недостаточный его уровень полностью исключают возможность получения информации. Эти условия существуют ниже области соприкосновения (рис. 3).

Высоту области соприкосновения можно определить на основании известных соотношений теории антенн. Только в данном случае нужно несколько скорректировать их

вывод. В частности действующую ширину ДН можно определить по уровню 0,1...0,2, так как доплеровский локатор имеет большой динамический диапазон. По этой же причине расстояние дальней зоны радиоантенн можно оценить по фазовому критерию для разности оптического хода равной $\pi/2$. Также на первом этапе можно считать фазовый фронт сферическим и предположить строгое выполнение условия Брэгга на всей поверхности пакета, что в первом приближении соответствует тонким пакетам.

В этом случае вид ФРВ определяется степенью перекрытия ОПМ (рис. 3). Она показывает, с какого уровня можно получить информацию. Качественно она определяется следующими факторами.

В нижней части трассы ФРВ равна нулю и измерения невозможны. Бистатистическую зону можно разделить на две части. В нижней части (IIб), по мере увеличения перекрытия ОПМ радиоантенн, сигнал будет возрастать. В этой части решение дифракционной задачи и определение соответствующих корректирующих функций (КФ) наиболее сложно. В спадающей части (IIв) эта задача несколько упрощается. И лишь в зоне моностатического приближения перекрытие можно считать полным, а КФ должна будет скомпенсировать только сферическую расхожимость волновых полей (r^{-1}).

Наиболее важным информационным параметром является доплеровский сдвиг частоты принимаемого сигнала Δf_d . Поэтому важно получить КФ для сдвига частоты. Но эта задача наиболее сложна. Рассмотрим схематически только некоторые ее начальные этапы.

В однородной изотропной атмосфере, в которой скорость звука c_a постоянна, изменение сдвига частоты определяется геометрическими соотношениями волновых полей. Зависит Δf_d от величины угла θ (рис. 3) и требует интегрирования по объему пакета. И если для тонких пакетов можно пренебречь радиальной протяженностью, то угловыми размерами пренебречь нельзя. Эта зависимость является функцией коррекции для Δf_d .

На первом этапе можно считать, что $r = c_a t$, где t – время. Поэтому достаточно сделать только оценку зависимости производных оптического пути по r при движении волн вверх L_+ и вниз L_- для различных участков зондирующего пакета. Общее изменение оптического пути определяется суммой $\Delta L_\Sigma = \Delta L_+ + \Delta L_-$. Из геометрических соотношений в направлении оси y производная оптического пути по радиусу в первом приближении:

$$\frac{\partial L_\Sigma}{\partial r} = 2 - \frac{y_0^2}{r^2} \cos^2 \theta + \frac{3}{4} \frac{y_0^4}{r^4}. \quad (1)$$

При оценке малости составляющих учтено, что в бистатистических системах $\theta_{\max} > y_0 r^{-1}$.

Локальное выполнение условия Брэгга изменяет соотношение вкладов сигнала, отраженного от различных участков пакета. Даже при тонких пакетах это приводит к погрешности измерения температуры (ΔT°) около $\pm 1...3^\circ\text{C}$.

Однако градиентные измерения, проводимые на нижних участках, требуют существенного снижения этой погрешности.

Предварительные результаты

Для апертурных антенн даже в зоне моностатического приближения выкладки становятся чрезвычайно громоздкими [5]. Поэтому здесь ограничимся представлением предварительных результатов, показывающих возможность снижения нижней границы получения информации.

Эти результаты получены при значительном числе приближений и ограничений, требующих отдельного описания. В частности, реальные антенны заменены точечными

излучателями, их ДН – гауссовскими кривыми ($U(\theta) = \exp(-a^2\theta^2)$), не учтена радиальная протяженность отражателя, но, тем не менее, учтена его сферичность.

В этом случае выражение для ФРВ имеет вид

$$F(r) = \frac{1 - 1.5(y_0/r)^2}{r} \exp\left[-2(a \cdot y_0/r)^2\right]. \quad (2)$$

Данная функция (рис. 4) показывает характер взаимодействия излучений, а ее поведение соответствует качественному описанию приведенному выше. Здесь обозначение зон преимущественно с обозначениями на рис. 3.

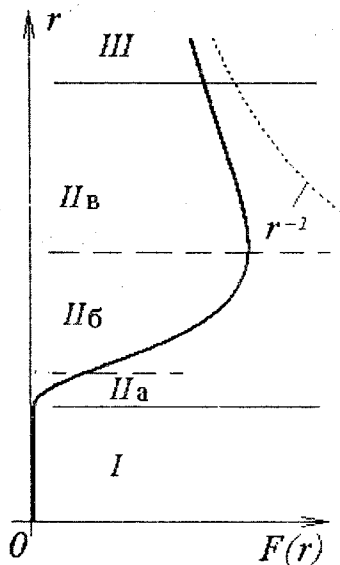


Рис. 4. Функция радиального взаимодействия полей в бистатических системах РАЗ

Представленная ФРВ соответствует результатам экспериментов, полученным на действующей системе РАЗ-10-20, созданной в ПНИЛ зондирования атмосферы ХИРЭ и в течение ряда лет использовавшейся для исследования условий РРВ в АПС вблизи границы суша-море [6]

Заметим только, что данная выше оценка ΔT также соответствует реальным значениям, а экспериментально полученная ФРВ располагалась несколько выше расчетной, что обусловлено сделанными приближениями.

Выводы

Соответствие экспериментальным данным позволяет говорить о правильности рассуждений и обоснованности всей методики использования приближений. Дальнейшее уточнение, в том числе и для доплеровского сдвига частоты принимаемого сигнала, потребует исключения тех приближений, которые не будут соответствовать поставленным задачам.

Решение дифракционной задачи в бистатической зоне систем РАЗ позволит снизить нижнюю границу измерения метеопараметров воздуха и существующими системами производить градиентные метеоизмерения в приземном слое (0...100 м) без метеорологических мачт.

Список литературы: 1. Каллистратова М.А., Кон А.И. Радиоакустическое зондирование атмосферы – М. : Наука, 1985. – 198с. 2. Ульянов Ю.Н., Ветров В.И., Максимова Н.Г. Радиоакустическое ветровое зондирование атмосферного пограничного слоя: история развития и перспективы // Вестник ХНУ. – №756. – С. 27-32. 3. Gerhard Peters, Barabara Hennemuth, Hans-Jurgen Kirtzel RASS Measured Temperature Gradients with a Bistatic Antenna Set-up, Proc. 9th Intl. Symp. Acoust. Rem. Sens., Vienna 167-170. 4. Кон А.И. Бистатическая система радиоакустического зондирования // Изв. АН СССР Физика атмосферы и океана. – 1981. – Т.17. – №6. – С.657-660. 5. Панченко А.Ю. Дифракция электромагнитных волн на акустических при радиоакустическом зондировании атмосферы Электромагнитные волны и электронные системы. – 1997. – Т.2, №5. – С.37-42. 6. Ульянов Ю.Н. Панченко А.Ю. Максимова Н.Г. Об использовании акустического и радиоакустического методов дистанционного зондирования АПС при получении метеоданных для оценки условий РРВ Радиотехника. – 2005. – Вып. 143. – С. 188-195.

Харьковский национальный университет радиозлектроники

Поступила в редколлегию 05.06.2011

КОНТРОЛЬ УРОВНЯ ВЫСОТЕМПЕРАТУРНЫХ ОБЪЕКТОВ МЕТОДОМ АКУСТИЧЕСКОЙ ЛОКАЦИИ

Введение

Контроль уровня высокотемпературных объектов (жидкие налипающие и сыпучие вещества при температуре поверхности более 50°C) представляет актуальную задачу. В [1] показано, что при контроле уровня высокотемпературных сред наблюдается снижение на 5 – 7 дБ среднего уровня, возникают существенные флуктуации (более 20 дБ) амплитуды сигнала, отраженного контролируемой поверхностью. Последние могут приводить к отказам акустических уровнемеров локационного типа в те моменты, когда амплитуда минимального отраженного сигнала ниже установленного в приборе порога обнаружения полезного сигнала.

В работе рассматриваются особенности функционирования акустических уровнемеров локационного типа при контроле уровня высокотемпературных сред. Для двух рабочих частот уровнемеров в открытых резервуарах проведены экспериментальные исследования временных зависимостей амплитуды отраженных сигналов и измеряемого временного интервала, пропорционального расстоянию до контролируемой поверхности.

Цель работы – исследование процессов в высокотемпературном канале распространения акустических волн и разработка рекомендаций, направленных на повышение работоспособности акустических уровнемеров локационного типа.

1. Методика проведения экспериментов и обработки результатов исследований

Исследования временных зависимостей амплитуды отраженного сигнала и измеряемого временного интервала пропорционального расстоянию до контролируемой поверхности были проведены в высокотемпературном канале «приемо-передатчик уровнемера – акустическая среда – высокотемпературная поверхность отражения», образованном в открытом сверху цилиндрическом резервуаре высотой около 1,2 м. Выбор открытого резервуара был обусловлен максимальным влиянием температурных неоднородностей коэффициента преломления воздуха, возникающих в нестандартном канале распространения на амплитуду отраженного сигнала [1], а его высота – возможностью экспериментального моделирования натуральных условий эксплуатации.

Высокотемпературные контролируемые объекты имитировались с помощью двух нагревателей, поочередно устанавливавшихся на дно резервуара. Температура отражающих поверхностей нагревателей составляла около 150 и 800°C . В качестве эталонного использовался канал с контролируемой поверхностью без источника теплового нагрева.

Для проведения исследований были использованы модифицированные приемо-передатчики акустического уровнемера [2, 3] с рабочими частотами 10 и 20 кГц. В процессе исследований для каждого зондирующего импульса информация об амплитуде огибающей отраженного сигнала и временном интервале, пропорциональном расстоянию до отражающей поверхности, транслировалась на ЭВМ. Постановка экспериментальных исследований на двух рабочих частотах была вызвана необходимостью определения оптимального частотного диапазона для контроля уровня высокотемпературных объектов. Структурная схема экспериментальной установки для проведения исследований представлена на рис.1.

Для исследования временных флуктуаций амплитуды огибающей применен коррелограммный метод спектрального оценивания [4, 5], в соответствии с которым спектральная плотность мощности (СПМ) дискретного случайного стационарного процесса определяется как

$$P(f) = T \sum_{k=-L}^L r[k] \exp(-j2\pi f k T), \quad -1/2T \leq f \leq 1/2T,$$

где f – частота, T – период дискретизации, $r[k]$ – корреляционная функция исследуемого случайного процесса, оценка которой может быть вычислена по имеющейся конечной выборке данных процесса $x[n]$, $n = 0, \dots, N-1$:

$$\hat{r}[k] = \frac{1}{N-|k|} \sum_{n=0}^{N-|k|-1} x[n+|k|]x[n], \quad (1)$$

где L – максимальное значение временного сдвига. Для уменьшения возможных искажений оценок СПМ за счет просачивания боковых лепестков применяется взвешивание оконной функцией [5, 6]. В этом случае оценка СПМ находится из выражения

$$\hat{P}(f) = T \sum_{k=-L}^L w[k] \hat{r}[k] \exp(-j2\pi f k T), \quad (2)$$

где $w[k]$ – оконная функция.

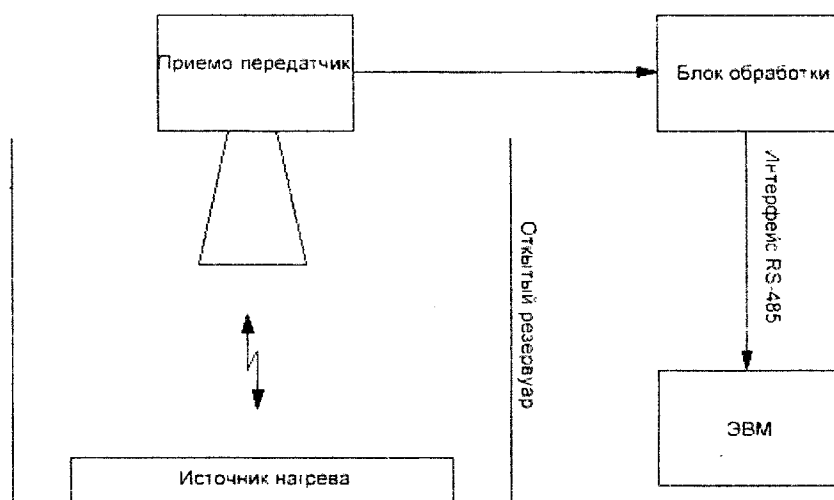


Рис. 1

С целью изучения влияния процессов, происходящих в высокотемпературном канале распространения, на величину амплитуды отраженного сигнала для обеих рабочих частот были найдены оценки СПМ флуктуаций амплитуды огибающей в соответствии с (2) для трех различных случаев:

- случай I – отсутствие источника теплового нагрева;
- случай II – присутствие источника теплового нагрева средней мощности ($t = 150^\circ\text{C}$);
- случай III – присутствие мощного источника ($t = 800^\circ\text{C}$).

Оценки СПМ находились по записям данных длиной $N = 2000 - 5000$ отсчетов, что для периода следования зондирующих импульсов уровнемера $T_c = T = 0.9$ с соответствовало времени наблюдения, равному 30 – 75 мин.

1.2. Результаты исследований

На рис. 2 приведены примеры типичных временных зависимостей амплитуды огибающей отраженного сигнала $A[n]$ для рабочей частоты 10 кГц, где рис.2, а соответствует случаю II, рис.2, б – случаю III. По осям ординат отложены значения огибающей амплитуды во внутриаппаратных единицах амплитуды (в.е.а.), а по осям абсцисс – номера отсчетов n . Видно, что для случая III наблюдаются более глубокие флуктуации

амплитуды. Это может быть объяснено тем, что с ростом температуры контролируемой поверхности в канале распространения формируются более «мощные» неоднородности коэффициента преломления, приводящие к увеличению рассеяния и поглощения отраженного акустического сигнала [7].

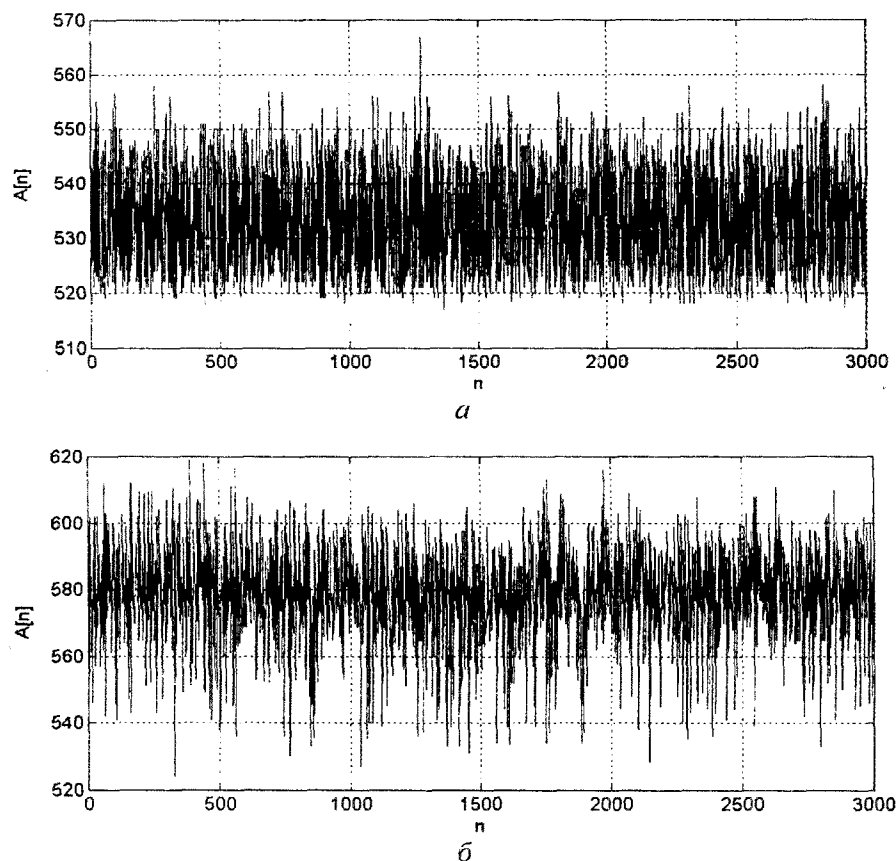


Рис. 2

На рис.3 представлен пример временной зависимости измеряемого времени задержки сигнала $t_{\text{зад}}[n]$, отраженного от контролируемой поверхности, на рабочей частоте 20 кГц для случая II. По оси ординат на этом рисунке отложены величины времени запаздывания отраженного сигнала, пропорциональные расстоянию до контролируемой поверхности во внутриаппаратных единицах времени (в.е.в.), а по оси абсцисс – номера отсчетов n . Из данных на рис. 3 видно, что время задержки отраженного сигнала ($t_{\text{сдв}} \approx 1200$ в.е.в.) в основном соответствует реальному расстоянию до контролируемой поверхности. Однако наблюдались случаи кратковременного отсутствия отраженного сигнала ($t_{\text{сдв}} \approx 0$) (см. рис.3). Также имели место ситуации, когда измеряемый временной интервал ($t_{\text{сдв}} \approx 2400$ в.е.в.), соответствовал примерно удвоенному расстоянию до контролируемой поверхности.

Первый случай ($t_{\text{сдв}} \approx 0$), когда отраженный сигнал отсутствует или его амплитуда ниже установленного порога, в блоке обработки уровнемера должен идентифицироваться как отказ приемо-передатчика.

Второй случай соответствует ситуации в канале распространения, при которой амплитуда первого отраженного сигнала была ниже установленного порога, а амплитуда сигнала, дважды прошедшего исследуемый канал, превышала порог обнаружения полезного сигнала. В этом случае в блоке обработки должно приниматься решение о том, что расстояние до контролируемой поверхности примерно в два раза превышает реальное.

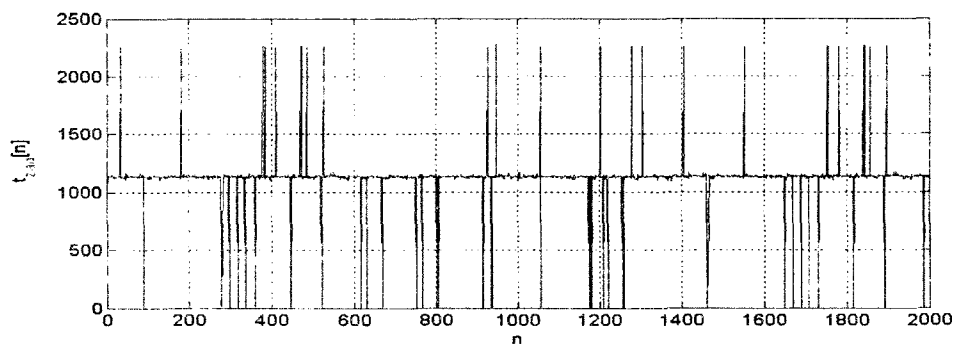


Рис. 3

Кроме того, имели место кратковременные ситуации (см. рис. 3), при которых временные запаздывания отраженного сигнала могли находиться в интервале $(0,5 \dots 1,5)t_{\text{зад}}$.

Следует отметить, что в процессе натурного контроля уровня битума при температуре контролируемой поверхности около 270°C наблюдались аналогичные кратковременные отказы и перескоки показаний уровня и на рабочей частоте 10 кГц .

На рис. 4 представлены оценки спектров СПМ для случаев II, III (соответствуют кривым II, III), полученные для частоты 20 кГц , а на рис. 5 – для частоты 10 кГц для всех трех случаев. По осям абсцисс отложена частота в относительных единицах fT .

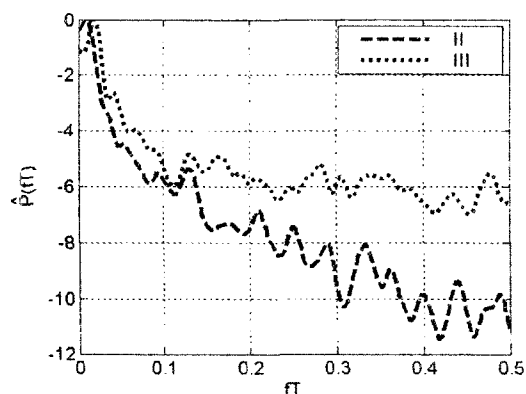


Рис. 4

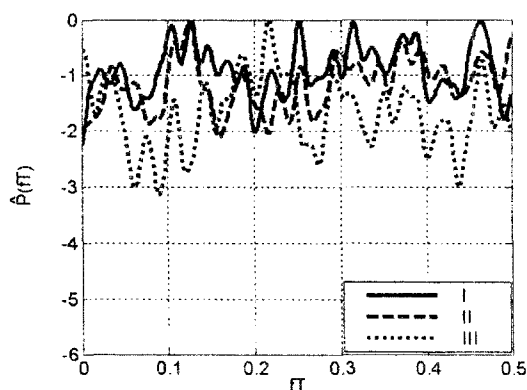


Рис. 5

Сравнение кривых на рис. 4 показывает, что с увеличением температуры источника теплового излучения спектры приобретают меньший наклон в области более высоких частот. Это поясняется тем, что с ростом температуры источника интенсивность и частота возникновения неоднородностей коэффициента преломления возрастает. Для рабочей частоты 10 кГц не характерна указанная зависимость (см. кривые I-III на рис.5). Это связано с тем, что для обеих частот были поочередно использованы одни и те же источники теплового нагрева. Они соответственно поочередно формировали одинаковые для обеих частот неоднородности коэффициента преломления. Как указано в [7], при одинаковых величинах неоднородностей коэффициента преломления их влияние снижается с ростом длины волны. Это также подтверждается и данными роста среднеквадратических отклонений (СКО) огибающей амплитуды принимаемого сигнала на высокой рабочей частоте, приведенных в таблице.

Сигнал	Случай I	Случай II	Случай III
20 кГц	0,88	5,4	17,9
10 кГц	5,2	9,5	12,6

Практический интерес представляет также изучение характера возникновения отказов в работе уровнемера в канале распространения со значительными флуктуациями уровня принимаемого сигнала. На рис. 6 представлена временная зависимость значений относительного времени задержки отраженного сигнала $t_{\text{зад}}[n]$ от момента подачи запускающего импульса для частоты 20 кГц в случае III. В указанном эксперименте было специально понижено усиление приемного тракта, чтобы выявить возможные периодичности появления отказов ($t_{\text{зад}} \approx 0$) измерения дальности. Оценка корреляционной функции для массива данных $t_{\text{зад}}[n]$, найденная по (1), приведена на рис. 7 и имеет вид, достаточно близкий к функции Дирака, что может свидетельствовать об отсутствии сколько либо выраженных периодичностей в появлении отказов измерения уровня, обусловленных влиянием высокотемпературного канала распространения. Возможным способом борьбы с кратковременными пропаданиями отраженного сигнала на трассах с флуктуациями может служить использование буфера показаний дальности в уровнемере, выдающего предыдущее измеренное значение дальности в случае отказа. Ввиду указанных особенностей корреляционной функции рис. 7, длину такого буфера можно ограничить одним или двумя измерениями.

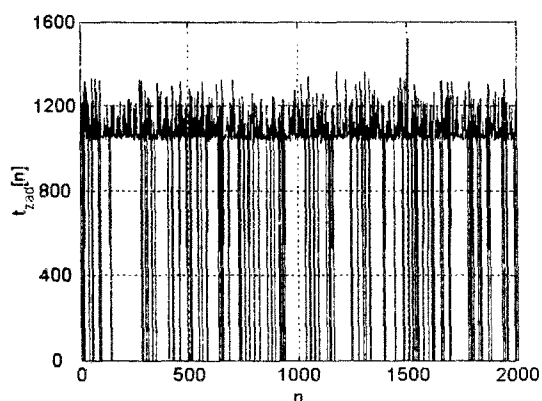


Рис. 6

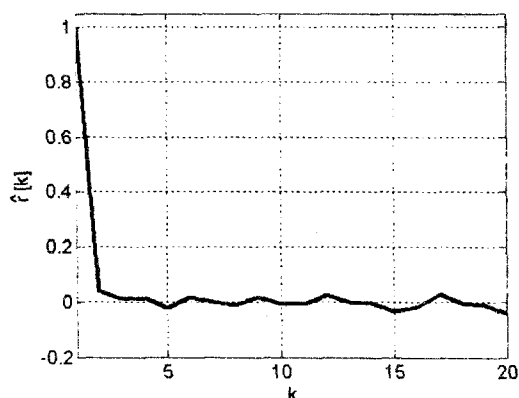


Рис. 7

1.3. Рекомендации по повышению работоспособности акустических уровнемеров

Результаты исследований подтверждают, что процесс контроля уровня высокотемпературных объектов сопровождается глубокими флуктуациями амплитуды отраженного сигнала (рис.2), которые увеличивают погрешность измерения уровня и могут приводить к кратковременным отказам, когда уровень отраженного сигнала ниже установленного порога. Наличие в высокотемпературном канале распространения существенных неоднородностей коэффициента преломления воздуха может также вызывать кратковременные существенные ошибки измеряемого временного интервала, а в итоге – расстояния до поверхности и уровня. Так, возможной причиной увеличения расстояния до контролируемой поверхности примерно в два раза (рис.3) могут быть акустические линзы, возникающие на неоднородностях коэффициента преломления [8]. Они существенно ослабляют первый отраженный сигнал и «усиливают» его во время повторного прохождения канала распространения. Появление ошибок измеряемого временного интервала в диапазоне $(0,5 \dots 1,5)t_{\text{зад}}$ связано с попаданием на вход приемного устройства сигналов, преломленных или рассеянных на границе неоднородности коэффициента преломления и затем переотраженных в направлении приемной антенны каким либо отражателем на внутренних стенках резервуара. Временная зависимость отказов (рис.7) свидетельствует, что они носят кратковременный, практически единичный, характер.

Оценки спектров на рабочей частоте 10 кГц (рис. 5) не выявили зависимости от температуры контролируемой поверхности. Величины СКО (см. табл.1) на частоте 20 кГц существенно выше для частоты 20 кГц, что свидетельствует об увеличении затухания амплитуды отраженного сигнала с ростом рабочей частоты.

Таким образом, для повышения надежности функционирования акустических уровнемеров в процессе контроля уровня высокотемпературных объектов целесообразно использовать низкочастотные приборы с запасом потенциала не менее 40 – 50 дБ [1].

Для обеспечения работоспособности акустических уровнемеров в системах управления и сбора данных требуется исключить попадание на их вход нештатной информации с кратковременных флуктуационных отказов и существенных ошибках контролируемого уровня, обусловленных особенностями распространения акустических волн в высокотемпературных каналах. Учитывая кратковременный, практически единичный характер флуктуационных отказов и ошибок (см. рис.7), работоспособность возможно обеспечить с помощью следующих доработок программного обеспечения уровнемера:

- информацию о кратковременном отказе приемо-передатчика (отраженный сигнал отсутствует или ниже порога) передавать с задержкой на несколько периодов, транслируя в систему последнюю до отказа информацию об уровне;

- ввести диапазон, в котором может изменяться контролируемый уровень за 2 – 4 последующих периода. Если измеренная величина выходит за рамки установленного диапазона, то в систему в течение нескольких периодов транслировать последнюю «правильную» информацию.

Выводы

Проведенные исследования подтвердили, что основной причиной неустойчивой работы акустических уровнемеров локационного типа в процессе контроля уровня высокотемпературных объектов является рассеяние и преломление акустических волн на неоднородностях коэффициента преломления воздуха в канале распространения «приемо-передатчик уровнемера – акустическая среда – высокотемпературная поверхность отражения».

Результаты исследований подтвердили предпочтительность использования более низких рабочих частот и, учитывая кратковременный характер отказов и сбоев контроля уровня, позволили предложить пути сохранения работоспособности акустических уровнемеров локационного типа в системах сбора данных.

Список литературы: 1. Жуков Б.В., Березин Е.И. Особенности функционирования акустических уровнемеров локационного типа при нестандартных условиях эксплуатации // Радиотехника. – 2009. – Вып.158. – С.21 – 26. 2. Жуков Б.В., Солярский Н.Ф. и др. Акустический уровнемер „Зонд-3М” Датчики и системы. – 2007. – №.2. – С.35 – 40. 3. Жуков Б.В., Солярский Н.Ф. и др. Низкочастотные модификации акустических преобразователей уровнемера “ЗОНД-3М”// Датчики и системы. – 2007. – №.3. – С.42 – 46. 4. P. Stoica, R.M. Moses. Introduction to Spectral Analysis. New Jersey: 1997. -319 p 5. С.Л. Марпл-мл. Цифровой спектральный анализ и его приложения. – М. : Мир, 1990. – 584 с. 6. Ф. Дж. Хэррис. Использование окон при гармоническом анализе методом дискретного преобразование Фурье. // ТИИЭР. – Т. 66, № 1. – 1978. – С. 60 – 96. 7. Красильников В.А. Звуковые и ультразвуковые волны. – М. : Физматгиз, 1960. – 560 с.

*Институт радиофизики и электроники
НАН Украины*

Поступила в редколлегию 25.07.2011

АНАЛИЗ СТРУКТУРНОЙ СКРЫТНОСТИ МНОГОУРОВНЕВЫХ ЛИНЕЙНЫХ СИГНАЛОВ ЦИФРОВЫХ СИСТЕМ ПЕРЕДАЧИ ИНФОРМАЦИИ НА ОСНОВЕ ШИРОКОПОЛОСНЫХ *xDSL* ТЕХНОЛОГИЙ

Введение

Потенциальная структурная скрытность сигналов является одним из важнейших требований информационной безопасности ведомственных систем связи (ВСС). При этом задачи по обеспечению скрытности ВСС ставятся, как правило, на сигнальном уровне, что предполагает выбор соответствующих характеристик и параметров сигнала, которые являются переносчиками информации [1].

В проводном сегменте ВСС для передачи мультимедийной информации широко применяются цифровые системы передачи информации (ЦСПИ) с широкополосными *xDSL* технологиями (*Digital Subscriber Line*), которые используют многоуровневые линейные сигналы [2 – 5]. Отметим также, что при построении сетей доступа используют в основном ЦСПИ зарубежного производства, со своими уровнем безопасности и алгоритмами взаимодействия.

В ряде работ [6, 7] на основе известного метода определения потенциальной структурной скрытности, не требующего знания алгоритма обработки сигнала в приемнике-обнаружителе нарушителя, проведен анализ структурной скрытности широкополосных сигналов, используемых в беспроводном сегменте ВСС. Однако анализ структурной скрытности сигналов, применяемых в проводных системах связи, пока отсутствует, что не позволяет провести комплексную оценку защищенности интегрированных ВСС от перехвата информации.

Цель работы – устранить существующий пробел и провести оценку потенциальной структурной скрытности широкополосных линейных сигналов, используемых в различных видах *xDSL* технологий, а также определить пути ее увеличения.

Основная часть

Потенциальная структурная скрытность определяется числом двоичных измерений (диз), которые необходимо осуществить для раскрытия структуры линейного сигнала. Общее выражение для потенциальной структурной скрытности имеет вид [8]:

$$S_P = \log_2 A \text{ [диз]}, \quad (1)$$

где A – ансамбль (арсенал) реализаций, определяемый количеством всех возможных значений каких-либо параметров сигнала.

Таковыми параметрами могут быть несущая частота, амплитуда, вид модуляции, структура линейного кода, параметры формы и временные характеристики сигнала, а также другие специфические параметры, зависящие от физического уровня конкретной технологии передачи сигналов. В общем случае скрытность зависит от способа построения конкретного вида сигнала, используемого для переноса информации.

Так как в современных проводных ЦСПИ применяются составные сложные сигналы, то структурная скрытность S_Σ в этом случае будет суммой структурной скрытности отдельных элементов сигнала

$$S_\Sigma = S_1 + S_2 + \dots + S_i = \log_2 A_1 + \log_2 A_2 + \dots + \log_2 A_i \text{ [диз]}, \quad (2)$$

где $A_1, A_2, \dots, A_i$ – количество (арсенал, ансамбль) всех возможных значений каждого из i -параметров составного сигнала.

Рассмотрим сначала задачу поиска и перехвата линейного сигнала проводной ЦСПИ на основе *xDSL* технологий с неизвестной несущей частотой в диапазоне частот от f_1 до f_2 . Теоретически для абсолютно точного решения этой задачи потребуется измерительная процедура бесконечной продолжительности.

Однако на практике время и точность любых измерений ограничена как возможностями аппаратуры нарушителя, так и практической целесообразностью. В рассматриваемом случае минимальное значение допустимой ошибки поиска сигнала по частоте может быть обусловлено, например, собственной нестабильностью частоты сигнала *xDSL* передатчика, влиянием ошибки измерения несущей частоты в приемнике-обнаружителе на качество приема перехватываемого сигнала и т.п.

Как известно [9], при описании статистических свойств какой-либо непрерывной случайной величины X обычно используется функция плотности вероятностей $w(x)$. Если устройство разведки частотного диапазона нарушителя не располагает какими-либо сведениями о рабочей частоте перехватываемого сигнала, то целесообразно использовать функцию равномерной плотности вероятностей $w(f)$ рабочей частоты f .

Предположим, что значения частоты сигнала легитимного модема $f_{ЛК}$ находятся в диапазоне D_f от частоты f_1 до частоты f_2 ($D_f = f_2 - f_1$) и имеют равномерную плотность вероятностей вида

$$w(f) = \frac{1}{D_f}. \quad (3)$$

Если шаг дискретизации по частоте Δf в приемнике-обнаружителе выбран так, что $N = D_f / \Delta f$ является целым числом (N – число одинаковых интервалов дискретизации), а среднеквадратическое отклонение (СКО) частоты σ_f для равномерной плотности вероятностей $\sigma_f = D_f / \sqrt{12}$ [9], то вероятность попадания P_n значения частоты $f_{ЛК}$ в заданный интервал поиска согласно [8]

$$P_n = \frac{1}{N} = \frac{\Delta f}{D_f} = \frac{\Delta f}{\sigma_f \cdot \sqrt{12}}. \quad (4)$$

В этом случае потенциальную скрытность сигнала S_f (1), которая определяется числом возможных значений параметра частоты легитимного модема $f_{ЛК}$ в диапазоне частот разведки сигнала, можно найти из выражения

$$S_f = - \sum_{n=1}^N P_n \cdot \log_2 P_n = \log_2(N) = \log_2\left(\frac{D_f}{\Delta f}\right) = \log_2\left(\frac{\sqrt{12} \cdot \sigma_f}{\Delta f}\right) = \log_2\left(\frac{\sigma_f}{\Delta f}\right) + 1,792. \quad (5)$$

График зависимости потенциальной скрытности S_f от отношения шага дискретизации Δf к СКО приведен на рис. 1.

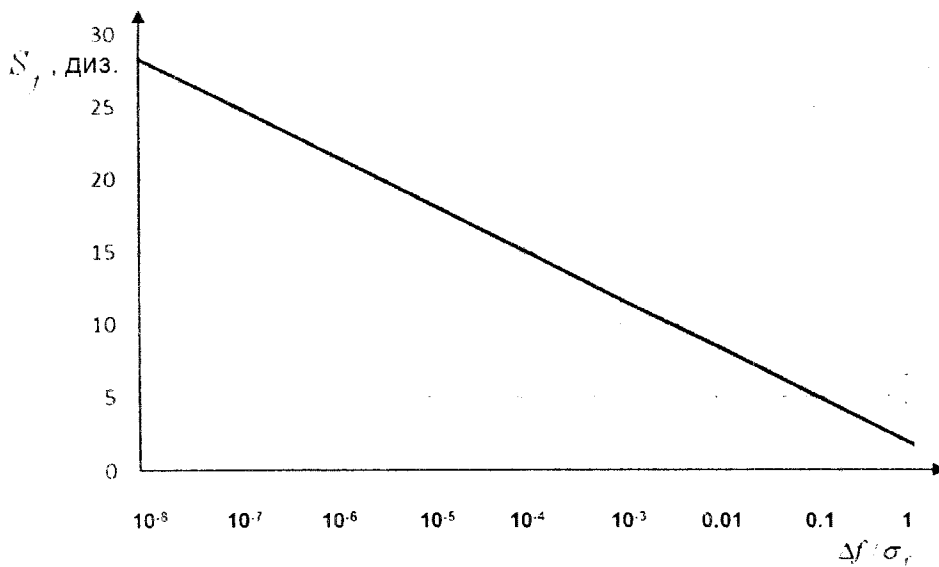


Рис. 1. График зависимости потенциальной скрытности S_f от отношения $\Delta f / \sigma_f$

Из рис. 1 видно, что увеличение стабильности частоты тактового генератора легитимного модема $f_{\text{ЛК}}$ (например, менее 10^{-6} ppm), приводящее к необходимости уменьшения шага дискретизации Δf в приемнике-обнаружителе нарушителя существенно повышает потенциальную структурную скрытность линейного сигнала xDSL модема.

Для увеличения скорости передачи информации в канале связи несущая частота $f_{\text{ЛК}}$ модема обычно модулируется; к примеру, может использоваться многопозиционная квадратурная амплитудная модуляция QAM-M (Quadrature Amplitude Modulation), уровень M которой задает количество различных значений вектора модулированного сигнала, т.е. $M = 2^n$ – размерность ансамбля сигналов, где $n = 2, 3, \dots, 15$ [2]. Тогда для сигнала QAM-M количество вариантов соответствия каждой точке сигнального ансамбля символа, который состоит из n бит, составляет $M!$ без учета ограничений кода Грея. Соответственно, структурная скрытность сигнального созвездия в виде прямоугольной решетки с M точками

$$S_{QAM} = \log_2(M!) \text{ [диз]}. \quad (6)$$

В современных проводных ЦСПИ широко используется система сигналов с многими поднесущими частотами, в основе которой лежит использование быстрого преобразования Фурье при синтезе сигнала на передаче и демодуляции его на приеме. Этот вид модуляции стандартизирован ANSI в качестве метода линейного кодирования для систем передачи данных и называется дискретной мультитоновой модуляцией DMT (Discrete Multi-tone Modulation).

Метод модуляции DMT основывается на принципе разделения диапазона частот, в котором осуществляется передача данных (от 35 кГц до 30 МГц), на N поддиапазонов шириной в 4,3125 кГц (8,6250 кГц). В зависимости от качества проводного канала связи каждая из N поднесущих частот использует QAM модуляцию со своим уровнем модуляции M_i , т.е. каждая поднесущая f_i несет n_i бит информации. Учитывая то, что база сигнала DMT приблизительно равна количеству поднесущих $B_c \approx N$, то потенциальная скрытность сигнала

$$S_{DMT} = \log_2(N) \text{ [диз]}. \quad (7)$$

На рис. 2 приведены графики зависимости потенциальной скрытности сигналов DMT $S_{DMT\ QAM} = \log_2(N) + \log_2(M!)$ от количества поднесущих частот N и различных значений размерности M ансамбля сигналов QAM .

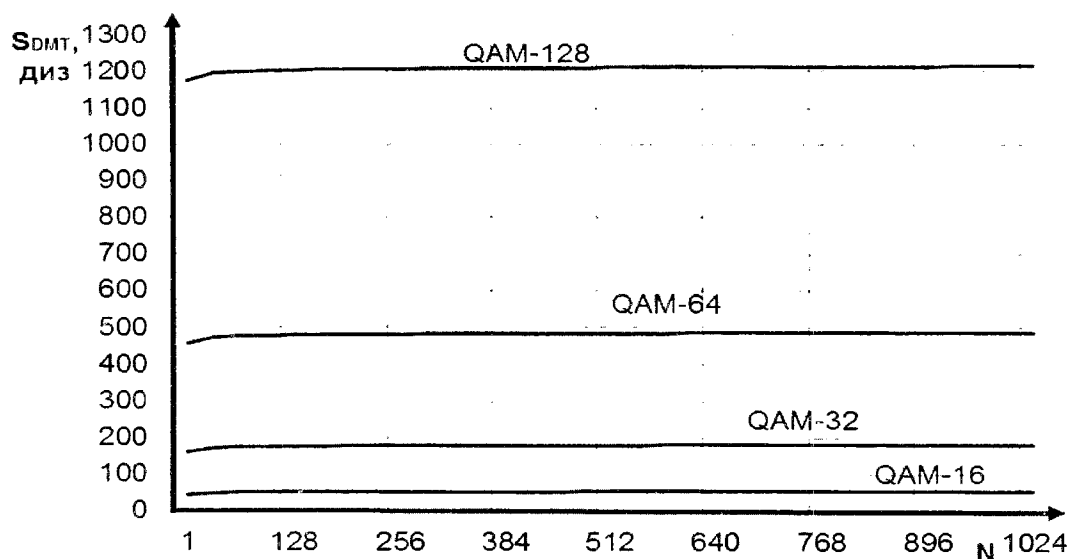


Рис. 2. Графики зависимости потенциальной скрытности $S_{DMT\ QAM}$ от числа поднесущих частот N и уровня M модуляции QAM

Как видно из графиков, скрытность сигналов DMT повышается с увеличением числа поднесущих частот f_i , кроме того на величину S_{DMT} существенно влияет размерность QAM .

Арсенал сигналов DMT можно существенно повысить, если использовать случайную перестановку передаваемых символов между поднесущими частотами f_i , согласованную между передатчиком и приемником. В этом случае арсенал $A_{DMT} = N!$ и потенциальная структурная скрытность увеличивается $S_{DMT} = \log_2(N!)$.

Возможна также реализация более сложного алгоритма взаимодействия между передатчиком и приемником ЦСПИ при реализации псевдослучайной перестройки частоты (ППЧ) поднесущих по согласованному закону. Это позволит значительно увеличить потенциальную скрытность сигналов DMT $S_{ППЧ} = 0,697 \cdot N \cdot \log_2 N$ [8].

Используя приведенные выше выражения для потенциальной скрытности отдельных параметров линейных сигналов, проведем общую оценку скрытности основных $xDSL$ технологий, которые применяются при построении проводных ЦСПИ для ВСС.

Симметричная технология $SHDSL$ использует сигналы многоуровневую амплитудно-импульсную модуляцию $PAM-M$ (*Pulse Amplitude Modulation*) с уровнем модуляции $M = 4, 8, 16, 32, 64, 128$ и формированием формы линейного сигнала с помощью фильтра приподнятого косинуса RC (*Raise Cosines*) (арсенал состояний коэффициента сглаживания фильтра $A_{RS} = 128$). Тогда потенциальная скрытность будет определяться арсеналом состояний всех составляющих сигнала

$$S_{SHDSL} = S_f + S_{QAM} + S_{RS} = \log_2 \left(\frac{\sqrt{12} \cdot \sigma_f}{\Delta f} \right) + \log_2(M!) + \log_2(A_{RS}). \quad (8)$$

Ассиметричная технология $ADSL$ использует многочастотные DMT сигналы с модуляцией QAM . Количество поднесущих частот $N = 256 \setminus 512$, а уровень QAM модуляции M

может меняться в широких пределах ($QAM - 4, QAM - 8, QAM - 16, \dots, QAM - 32768$). Уровень модуляции для каждой поднесущей частоты устанавливается отдельно и зависит от неравномерности частотной характеристики кабельной линии связи, а также от уровня шума в системе связи.

Потенциальная скрытность будет определяться арсеналом состояний всех составляющих сигнала

$$S_{ADSL} = S_f + S_{DMT} + S_{QAM} = \log_2 \left(\frac{\sqrt{12} \cdot \sigma_f}{\Delta f} \right) + \log_2 (N) + \log_2 (M!). \tag{9}$$

Высокоскоростная технология *VDSL* использует многочастотные *DMT* сигналы с модуляцией *QAM*. Количество поднесущих частот $N = 1024 \setminus 2048$, а уровень *QAM* модуляции M может меняться в широких пределах в зависимости от отношения сигнал/шум в проводном канале связи. Кроме того, в этой технологии для уменьшения перекрестных искажений в многопроводных линиях связи реализован принцип дискретного изменения уровня мощности P_c линейного сигнала в пределах от -17 до $+17$ дБм с шагом 1 дБм (арсенал $A_p = 34$). Потенциальная скрытность для технологии *VDSL* будет определяться арсеналом состояний всех составляющих линейного сигнала

$$S_{VDSL} = S_f + S_{DMT} + S_{QAM} + S_P = \log_2 \left(\frac{\sqrt{12} \cdot \sigma_f}{\Delta f} \right) + \log_2 (N) + \log_2 (M!) + \log_2 (A_p). \tag{10}$$

Используя выражения (8) – (10), можно провести сравнительный анализ структурной скрытности линейных сигналов различных *xDSL* технологий.

В таблице приведены данные о потенциальной структурной скрытности *SHDSL*, *ADSL* и *VDSL* технологий при различных значениях отдельных параметров линейного сигнала [10].

Вид технологии	Тип сигнала	Количество поднесущих N	Уровень модуляции M	Скрытность S , диз
<i>HDSL</i>	<i>PAM-16</i>	1	16	65
<i>SHDSL</i>	<i>PAM-128</i>	1	128	747
<i>ADSL</i>	<i>DMT QAM-256</i>	256	256	1720
<i>ADSL2</i>	<i>DMT QAM-1024</i>	512	1024	8839
<i>VDSL</i>	<i>DMT QAM-2048</i>	1024	2048	19700
<i>VDSL2</i>	<i>DMT QAM-4096</i>	2048	4096	43479

Полученные данные свидетельствуют о высокой потенциальной структурной скрытности современных цифровых технологий передачи информации по кабельным каналам связи. Особенно это относится к *VDSL* технологиям, использующим для передачи информации большое количество поднесущих частот и высокие уровни модуляции *QAM*.

Для увеличения структурной скрытности ВСС необходимо не только, по возможности, расширять ансамбли применяемых сигналов, но и использовать оригинальные методы формирования линейного сигнала в ЦСПИ собственной разработки, что позволит применять *xDSL* технологии в проводных сегментах ВСС для доступа к специализированным базам данных и передачи служебной информации.

Заключение

1) На основе известной методики проведена оценка потенциальной структурной скрытности многоуровневых линейных сигналов проводных ЦСПИ и получены новые данные о структурной скрытности сигналов современных *xDSL* технологий.

2) Для увеличения структурной скрытности сигналов, которые используются в *xDSL* технологиях, необходимо, по возможности, расширять ансамбль используемых сигналов, в том числе и используя дополнительные возможности физического уровня этих технологий.

3) Для увеличения защищенности ВСС необходимо использовать отечественные ЦСПИ, в которых реализованы оригинальные алгоритмы повышения структурной скрытности сигнала.

Список литературы: 1. Хорошко В. А., Чекатков А. А. Методы и средства защиты информации. – К. : ЮНИОР, 2003. – 504 с. 2. Балашов В. А., Лашко А. Г., Ляховецкий Л. М. Технологии широкополосного доступа *xDSL*. – М. : Эко-Трендз, 2009. – 256 с. 3. Цопа А. И. Выбор линейных сигналов и анализ их спектральных характеристик в системах передачи информации с использованием *xDSL* технологий. Радиотехника. – 2006. – Вып. № 146. – С. 66-74. 4. Шинкаренко И. В. Экспериментальная оценка защищенности мультимедийных цифровых систем передачи информации на основе *SHDSL* технологий / И. В. Шинкаренко, А. И. Цопа // Известия Вузов. Радиоэлектроника. – Київ : НТУ «КПИ», 2011. – Т. 54. – Вип. 5. – С. 30-36. 5. Дудка А. А. Прогнозирование зон обнаружения для кабельных линий связи в сети абонентского доступа на основе *VDSL* технологий / А. А. Дудка, А. И. Цопа, В. М. Шокало // Сучасний захист інформації. – Київ : ДУІКТ, 2010. – Вип. 3. – С. 45-53. 6. Захарченко Н. В. Структурная скрытность таймерных сигналов в системах с кодовым разделением сигналов / Н. В. Захарченко, В. В. Корчинский, Б. К. Радзимовский // Восточно-европейский журнал передовых технологий. – 2011. – №2/9(50). – С. 7-9. 7. Кувшинов О. В., Вознюк Р. В. Оцінка структурної критності широкосмугових сигналів // Зб. наук. праць ВІТІ НТУ «КПІ». – 2011. – № 1. – С. 106-111. 8. Каневский З. М. Теория скрытности / З. М. Каневский, В. П. Литвиненко. – Воронеж : ВГУ, 1991. – 144 с. 9. Вентцель А. Д. Курс теории случайных процессов. – М. : Наука. Физматлит, 1996. – 400 с. 10. Цопа А. И. Оценка предельной производительности проводных каналов связи с различными *xDSL* технологиями // Радиотехника. – 2010. – Вып. № 160. – С. 234-246.

Харьковский национальный
университет радиоэлектроники

Поступила в редколлегию 13.08.2011

ИССЛЕДОВАНИЕ ВЛИЯНИЯ ШУМОВ В РАДИОКАНАЛЕ НА РАБОТУ СИСТЕМЫ СИНХРОНИЗАЦИИ ОПОРНЫХ ГЕНЕРАТОРОВ

Введение

При решении большинства радиотехнических прикладных задач возникает необходимость в формировании и измерении частоты/фазы электрических колебаний. При этом подобные измерения часто требуют создания синфазных опорных колебаний, источники которых должны быть разнесены в пространстве на значительное расстояние. Такие проблемы возникают при построении систем телекоммуникаций, навигации и целого ряда других прикладных задач промышленности, строительства, медицины, мониторинга окружающей среды и т.п. [1].

Повышенные требования к системам синхронизации опорных генераторов предъявляются при создании измерительных систем, предполагающих осуществление измерений амплитуды и фазы микроволновых сигналов на трассе распространения радиоволн. В работе [2] предложена схема построения измерителя флуктуаций амплитуды и набега фазы микроволнового сигнала. Для обеспечения работы этого измерителя на обоих концах измерительной трассы необходимо формировать синхронные колебания с частотой 4 кГц . При этом начальные фазы низкочастотных сигналов переносятся в область микроволн, что дает возможность осуществлять измерения разности фаз микроволновых колебаний.

Для производства долговременных фазовых измерений по предложенной схеме использование независимых опорных генераторов, даже высокостабильных, не представляется возможным. В самом деле, опорные термостатированные кварцевые генераторы имеют относительную нестабильность частоты, в лучшем случае достигающей $10^{-8} - 10^{-10}$, причем последние представляют собой целую систему, имеющую внушительные габаритные размеры, массу и потребление электроэнергии. В этом случае расхождение разности фаз опорных генераторов частотой 4 кГц за сутки составит $12 - 1200$ градусов. Очевидно, что ни о каких долговременных фазовых измерениях в этом случае говорить не приходится.

С другой стороны, относительная нестабильность современных атомных стандартов частоты может достигать 10^{-13} и более, что может обеспечить разбег фаз указанных низкочастотных генераторов за сутки на уровне $0,012$ градуса. Но даже в этом случае невозможно производить сезонные измерения флуктуаций фазы микроволновых сигналов. Если же при этом принять во внимание стоимость атомных стандартов частоты и их совершенную непригодность для полигонных измерений, то целесообразность их использования для решения указанных задач неочевидна.

Таким образом, задача обеспечения синхронизации опорных генераторов на обоих концах измерительной трассы остается актуальной. В этом случае необходимо использовать открытый опорный канал связи для передачи синхронизирующего сигнала. При этом сам синхронизирующий сигнал является модулирующим сигналом для радиочастотного сигнала несущей. Поскольку опорный канал является открытым радиоканалом, его комплексный коэффициент передачи подвержен существенным изменениям в зависимости от условий распространения радиоволн. Дополнительно в этом случае необходимо учитывать влияние шумов естественного и искусственного происхождения. Все это приводит к флуктуациям амплитуды и полной фазы передаваемого радиосигнала, что в свою очередь приводит к значительным флуктуациям начальной фазы передаваемого опорного низкочастотного сигнала.

Цель работы – определение влияния амплитудных и фазовых шумов в опорном радиоканале на параметры синхронизации опорных низкочастотных генераторов измерителя комплексного коэффициента передачи микроволнового канала связи.

Описание и работа измерителя флуктуаций комплексного коэффициента передачи микроволнового канала связи

Рассмотрим работу измерителя флуктуаций комплексного коэффициента передачи микроволнового канала связи, прототип которого описан в [2]. Упрощенная структурная схема измерителя показана на рис. 1.

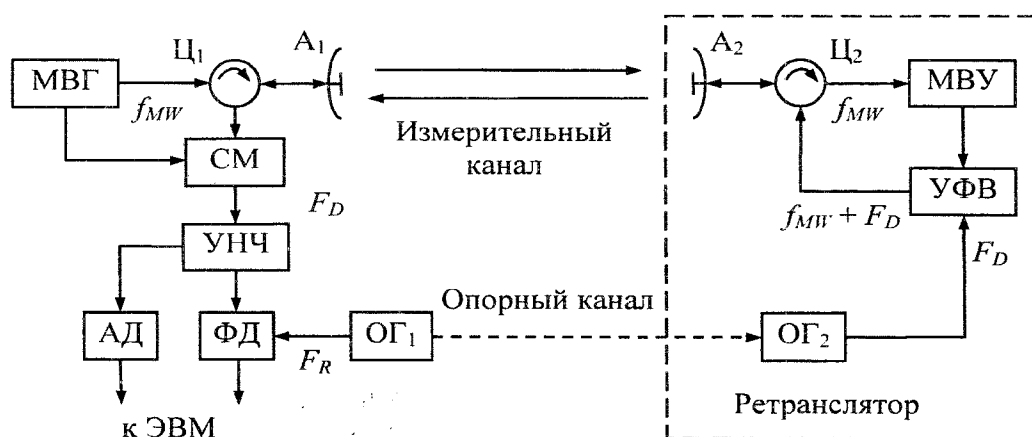


Рис. 1

Левая часть схемы образует собственно измерительную станцию, правая часть — ретранслятор.

Измерительная система состоит из: микроволнового генератора (МВГ), смесителя (СМ), усилителя низкой частоты (УНЧ), амплитудного детектора (АД), фазового детектора (ФД). Y-циркуляторов Π_1 и Π_2 , микроволновых антенн A_1 и A_2 , микроволнового усилителя (МВУ), управляемого фазовращателя (УФВ). На одном конце измерительной трассы размещается первый низкочастотный опорный генератор ($ОГ_1$). На противоположном конце измерительной трассы размещается другой низкочастотный опорный генератор ($ОГ_2$).

Микроволновый генератор формирует гармонические колебания, описываемые выражением

$$u_{MW}(t) = U_{MW} \cos(2\pi f_{MW} t + \varphi_{MW}), \quad (1)$$

где U_{MW} — амплитуда колебаний; f_{MW} — частота колебаний; φ_{MW} — начальная фаза колебаний.

Одновременно с этим опорный генератор $ОГ_1$ формирует низкочастотные опорные колебания вида

$$u_R(t) = U_R \cos(2\pi F_R t + \varphi_R), \quad (2)$$

где U_R — амплитуда опорных колебаний; F_R — частота опорных колебаний; φ_R — начальная фаза опорных колебаний.

Гармонические микроволновые колебания через микроволновый Y-циркулятор Π_1 подаются на вход микроволновой антенны A_1 и излучают в направлении ретранслятора радиоволну микроволнового диапазона. Пройдя через измерительный канал, эта радиоволна получает набег фазы

$$\Delta\varphi_{MW} = k d,$$

где d — расстояние между микроволновыми антеннами A_1 и A_2 ; k — волновое число, определяемое как

$$k = \frac{2\pi f_{MW}}{c}, \quad (3)$$

где c – скорость распространения микроволн в измерительном канале.

Принятые антенной A_2 через микроволновый Y-циркулятор Ц₂, эти колебания подают на микроволновый усилитель МВУ. Усиленные колебания подают на сигнальный вход управляемого микроволнового фазовращателя УФВ, который реализует периодически изменяющийся сдвиг фаз микроволновых колебаний. При этом, если за период T_D низкочастотного управляющего сигнала (сигнала опорного генератора ОГ₂), управляемый микроволновый фазовращатель вносит сдвиг фаз, изменяющийся от 0 до 2π , то можно говорить о смещении спектра микроволновых колебаний на частоту Доплера, определяемую как

$$\Omega_D = \frac{2\pi}{T_D} = 2\pi F_D. \quad (4)$$

Трансформированные по частоте микроволновые колебания, поступающие на вход антенны A_2 , имеют вид

$$u'_{MW}(t) = U_{MW} L_{ATT} \cos[2\pi(f_{MW} + F_D)t + kd + \varphi_{MW} + \varphi_D], \quad (5)$$

где L_{ATT} – множитель ослабления микроволновых колебаний в измерительном канале, принимающий во внимание все коэффициенты передачи всех звеньев измерительной системы; φ_D – начальная фаза низкочастотных колебаний опорного генератора ОГ₂.

Вторично прошедшие через измерительный микроволновый канал и принятые антенной A_1 микроволновые колебания, могут быть представлены как

$$u''_{MW}(t) = U_{MW} L_{ATT}^2 \cos[2\pi(f_{MW} + F_D)t + kd + k'd + \varphi_{MW} + \varphi_D], \quad (6)$$

где k' – волновое число трансформированных по частоте микроволновых колебаний.

С учётом того, что частота переизлучаемых ретранслятором микроволновых колебаний изменяется незначительно ($f_{MW} \gg F_D$), волновое число трансформированных по частоте микроволновых колебаний можно представить как

$$k' = \frac{2\pi(f_{MW} + F_D)}{c} \approx k. \quad (7)$$

Вторично принятые микроволновые колебания (6) перемножают в смесителе с исходными колебаниями (1), в результате чего на выходе смесителя получают колебания вида

$$u_{MIX}(t) = k_{MIX} U_{MW} L_{ATT}^2 \cos(2\pi F_D t + 2kd + \varphi_D), \quad (8)$$

где k_{MIX} – коэффициент передачи смесителя.

Как видно из (8), в результате гомодинного преобразования начальная частота и фаза микроволновых колебаний исходного и информационного сигналов взаимно вычитаются.

После усиления в низкочастотном усилителе и детектирования в амплитудном детекторе получают сигнал, пропорциональный L_{ATT}^2 , в общем случае являющийся флуктуирующей функцией. На выходе фазового детектора получают сигнал, пропорциональный разности фаз низкочастотных колебаний, также в общем случае являющийся флуктуирующей функцией,

$$\Delta\varphi_{MS} = 2\pi(F_D - F_R)t + 2kd + \varphi_D - \varphi_R = 2kd + \varphi_D - \varphi_R, \quad (9)$$

при условии, что $F_D = F_R$.

Анализ влияния точности синхронизации опорных генераторов на работу измерителя флуктуаций комплексного коэффициента передачи микроволнового канала связи

Выражение (9) справедливо для случая точного равенства частот опорных генераторов $ОГ_1$ и $ОГ_2$ и синхронной работе обоих генераторов с точностью до постоянной и не изменяющейся во времени разности фаз

$$\Delta\varphi_0 = \varphi_D - \varphi_R. \quad (10)$$

В этом случае информационным параметром фазоизмерительной системы будет величина $2kd$. Однако указанные генераторы не могут быть синфазными принципиально, поскольку они разнесены в пространстве на значительное расстояние и для их синхронизации используется дополнительный опорный канал. Изменение комплексного коэффициента передачи опорного канала приводит к изменению разности фаз опорных генераторов с течением времени, что в свою очередь приводит к погрешности измерения набега фазы микроволновых колебаний.

В работе [2] предложено использовать опорный сигнал, передаваемый через радиоканал, непосредственно для управления микроволновым фазовращателем. Однако это приводит к значительному влиянию параметров радиотракта на начальную фазу сигнала управления фазовращателем. Использование же в радиоприёмнике собственного термостатированного кварцевого генератора с фазовой автоподстройкой частоты позволяет значительно снизить влияние фазового шума радиотракта на сигнал управления фазовращателем.

В работе [3] предложено передавать низкочастотный синхронизирующий сигнал посредством радиоканала с использованием узкополосной частотной модуляции (ЧМ). Для реализации синхронной работы опорных генераторов на одном конце измерительной трассы располагают радиопередатчик, несущую которого модулируют колебаниями низкочастотного опорного генератора $ОГ_1$, а на другом конце измерительной трассы располагают радиоприемник, сигнал демодуляции которого используют для синхронизации опорного генератора $ОГ_2$.

Частотно-модулированный радиосигнал $a_{TX}(t)$, передаваемый в опорном радиоканале, может быть описан следующим выражением:

$$a_{TX}(t) = A_{TX} \cos \left[\left\{ 2\pi f_{RF} + m 2\pi F_R \cos(2\pi F_R t + \varphi_R) \right\} t + \varphi_{RF} \right], \quad (11)$$

где A_{TX} – амплитуда радиосигнала; f_{RF} – частота несущей радиосигнала; m – индекс модуляции радиосигнала; φ_{RF} – начальная фаза несущего колебания радиосигнала.

Модулированный радиосигнал, принятый ретранслятором, может быть записан в следующем виде как функция от времени $a'_{TX}(t)$:

$$a'_{TX}(t) = A'_{TX} \cos \left[\left\{ 2\pi f_{RF} + m 2\pi F_R \cos(2\pi F_R t + \varphi_R) \right\} t + \varphi_{RF} + \varphi(t) \right], \quad (12)$$

где A'_{TX} – амплитуда радиосигнала прошедшего через атмосферный канал связи; $\varphi(t)$ – фазовый сдвиг, вносимый опорным каналом связи в радиосигнал.

Амплитуду радиосигнала, прошедшего через атмосферный канал связи, можно приближённо считать постоянной, так как используется сигнал с угловой модуляцией. В качестве демодулятора в радиоприёмнике используют частотный детектор, тогда выражение для низкочастотного сигнала на его выходе будет

$$u_{RX}(t) = U_{RX} \cos \left[2\pi F_R t + \varphi_R + \zeta(t) \right], \quad (13)$$

где U_{RX} – амплитуда низкочастотного сигнала на выходе радиоприёмника; $\zeta(t)$ – фазовые шумы принятого низкочастотного сигнала, обусловленные присутствием амплитудных и фазовых шумов в радиоканале.

Для достижения синхронизации опорных генераторов в ретрансляторе низкочастотный сигнал, получаемый на выходе радиоприёмника, подают на вход системы фазовой автоподстройки частоты (ФАПЧ) высокочастотного кварцевого опорного генератора управляемого напряжением (ОГ₂). При этом сигнал на выходе частотно-фазового детектора системы ФАПЧ можно представить в виде:

$$u_{PD}(t) = K_{PD} m \frac{[\varphi_R + \zeta(t) - \varphi_D]}{2\pi}, \quad (14)$$

где K_{PD} – коэффициент преобразования детектора; φ_D – начальная фаза опорных колебаний на выходе опорного генератора ОГ₂.

Сигнал с выхода частотно-фазового детектора подают на фильтр нижних частот, который ослабляет шумы в управляющем сигнале, обусловленные фазовыми шумами принятого низкочастотного сигнала $u_{RX}(t)$. Таким образом, управляющий сигнал на входе генератора управляемого напряжением имеет следующий вид:

$$u_{CS}(t) = U_{CS} \frac{\varphi_R - \varphi_D}{2\pi}, \quad (15)$$

где U_{CS} – размах управляющего сигнала.

Выражение для опорного низкочастотного синхронизирующего сигнала на входе управляемого микроволнового фазовращателя может быть представлено в следующем виде:

$$u'_S(t) = U'_S \cos(2\pi F_D t + \varphi_D), \quad (16)$$

где U'_S – амплитуда низкочастотного синхронизирующего сигнала.

При этом в спектре опорного сигнала отсутствуют шумы, которые были в принятом низкочастотном сигнале, а система ФАПЧ отслеживает изменения начальной фазы принятого синхронизирующего сигнала с частотой $F_D = \Omega_D / 2\pi$. Таким образом, при достаточном отношении сигнал-шум в радиоканале, начальные фазы φ_R и φ_D сигналов опорных генераторов ОГ₁ и ОГ₂ приблизительно равны. Следовательно, введение генератора, управляемого напряжением, охваченного кольцом обратной связи фазовой автоподстройки частоты, позволяет снизить влияние амплитудных и фазовых шумов в опорном радиоканале на низкочастотный опорный сигнал в ретрансляторе микроволнового сигнала.

Экспериментальное исследование влияния дестабилизирующих факторов на точность синхронизации опорных низкочастотных генераторов

Рассмотрим подробнее влияние дестабилизирующих факторов на точность синхронизации опорных генераторов через атмосферный канал связи.

Исследование влияния радиоканала на точность синхронизации опорных генераторов связано с рядом проблем. В частности, для измерения разности фаз сигналов двух опорных генераторов необходимо создать высокостабильный помехозащищённый протяжённый канал связи, что в ряде случаев не представляется возможным. Для экспериментального исследования процессов синхронизации опорных низкочастотных генераторов был разработан эмулятор радиоканала, описанный в [4]. Структурная схема эмулятора радиоканала, вместе с аппаратурой синхронизации и измерительной аппаратурой, показана на рис. 2. Эмулирование радиоканала позволяет разместить всю аппаратуру синхронизации в одном месте в усло-

виях лаборатории и, таким образом, пропадают трудности, связанные с измерениями разности фаз опорных генераторов, удалённых друг от друга на значительное расстояние.

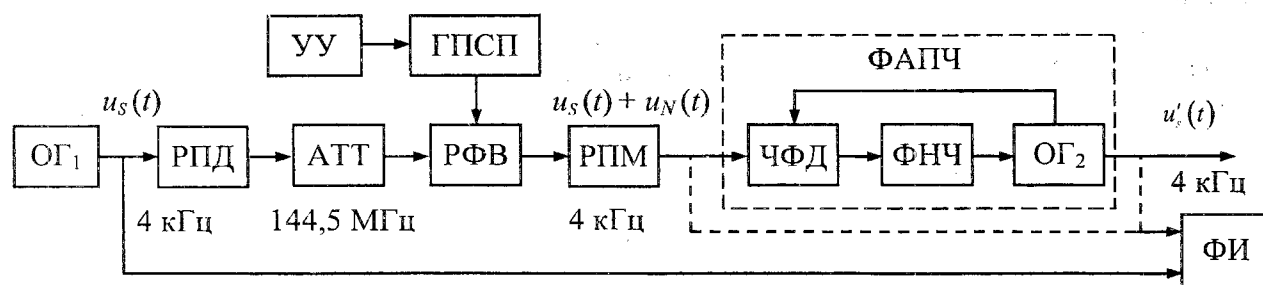


Рис. 2

На рис. 2 используются следующие обозначения: $ОГ_1$ – первый низкочастотный высокостабильный термостатированный опорный генератор; РПД – радиопередатчик; АТТ – аттенюатор; РФВ – управляемый радиочастотный фазовращатель; УУ – устройство управления; ГПСП – генератор псевдослучайной последовательности; РПМ – радиоприёмник; ФАПЧ – система фазовой автоподстройки частоты; ЧФД – частотно-фазовый детектор; ФНЧ – фильтр нижних частот; $ОГ_2$ – второй низкочастотный высокостабильный термостатированный опорный генератор, управляемый напряжением; ФИ – измеритель разности фаз; $u_s(t)$ – синхронизирующий низкочастотный сигнал; $u_N(t)$ – шумовая часть сигнала; $u'_s(t)$ – сигнал на выходе системы ФАПЧ.

Аппаратура синхронизации состоит из опорного генератора $ОГ_1$, радиопередатчика ЧМ сигнала РПД, радиоприёмника ЧМ сигнала РПМ и подстраиваемого генератора $ОГ_2$, охваченного кольцом обратной связи с фазовой автоподстройкой частоты.

Радиопередатчик передаёт тонально-модулированный ЧМ сигнал. Несущая частота радиосигнала была выбрана 144,5 МГц. Была предусмотрена возможность изменять индекс частотной модуляции в пределах от 0,5 до 2.

В качестве опорных генераторов на передающей и приёмной стороне используются термостатированные кварцевые генераторы «Сонет» и «Гиацинт» с частотами 10 и 5 МГц соответственно. Выходные сигналы опорных генераторов делят по частоте и приводят к величине 4 кГц.

Эмулятор радиоканала содержит регулируемый аттенюатор АТТ, управляемый радиочастотный фазовращатель РФВ, и низкочастотный генератор шума, состоящий из генератора псевдослучайной последовательности ГПСП и устройства управления УУ.

Регулируемый аттенюатор может вносить в сигнал ослабление в диапазоне от 0 до 40 дБ с дискретным шагом 10 дБ. В качестве регулируемого аттенюатора использовался набор фиксированных аттенюаторов. Регулируемый аттенюатор служит для ослабления радиосигнала в эмуляторе радиоканала, а также для изменения отношения сигнал-шум на выходе радиоприёмника.

Управляемый радиочастотный фазовращатель может вносить в радиосигнал непрерывно изменяемый фазовый сдвиг в диапазоне от 0 до 360 градусов. Фазовращатель был реализован на основе последовательного соединения трех квадратурных мостов, построенных на симметричных полосковых линиях, в квадратурные плечи которых включены варикапы. Варикапы используются при этом как нагрузка с изменяемой фазой коэффициента отражения, модуль которого всегда равен 1. При изменении управляющего напряжения на варикапе в пределах от 0,5 до 30 В фаза коэффициента отражения изменялась в пределах от 0 до 120 градусов. Закон изменения фазы коэффициента отражения от приложенного напряжения при этом принципиально нелинейный, однако использование микроконтроллерной техники позволило решить эту проблему путем предварительной калибровки всего фазовращателя.

Благодаря предложенным техническим решениям фазовращатель обладает высокой помехозащищённостью, малыми потерями (около $-0,55$ дБ) и высокой точностью реализуемого закона изменения фазового сдвига радиочастотного сигнала от подаваемого на его вход управления напряжения постоянного тока.

Низкочастотный генератор шума вырабатывает псевдослучайный низкочастотный сигнал, изменяющийся по амплитуде в пределах от $0,5$ до 30 В, который подается на вход управления радиочастотного фазовращателя. Длина последовательности может изменяться в пределах от 127 до 32767 неповторяющихся выборок. Частота выборок может изменяться от $7,62$ до $3,9$ кГц по закону $3900/2^n$, Гц. Частота выборки в $3,9$ кГц для формирования псевдослучайной последовательности выбрана близкой по величине к частоте передаваемого синхронизирующего сигнала 4 кГц, но не кратная ей. При помощи изменения параметров псевдослучайной последовательности и дополнительной фильтрации сигнала на выходе генератора шума с помощью обычного ФНЧ – моделируются фазовые шумы в радиоканале.

На рис. 3, а показана экспериментальная зависимость среднеквадратического отклонения (СКО) разности фаз опорных генераторов в зависимости от индекса модуляции передаваемого синхронизирующего сигнала. Измерения проведены при отношении сигнал-шум на выходе приёмника, равном $28,4$ дБ, и при отсутствии фазового шума в радиоканале. Также на рис. 3, б показана зависимость СКО набега фазы опорного сигнала в радиотракте в зависимости от индекса модуляции передаваемого синхронизирующего сигнала.

Здесь и далее измерения проводились на интервале 200 с с частотой выборки $2,5$ Гц, что соответствует 500 измерениям. Такое число измерений представляется достаточным для оценки статистических параметров измеряемых величин. В то же время, интервал 200 с соизмерим с длительностью переходных процессов в системе ФАПЧ. Следовательно, за этот интервал времени можно определить, находится ли исследуемая система в стационарном состоянии или нет.

Проводя анализ зависимостей, показанных на рис. 3, можно сделать вывод, что оптимальным индексом модуляции для данной системы синхронизации является $m = 1$, так как дальнейшее увеличение индекса модуляции существенно не улучшает точность синхронизации опорных генераторов, а только расширяет полосу частот радиосигнала.

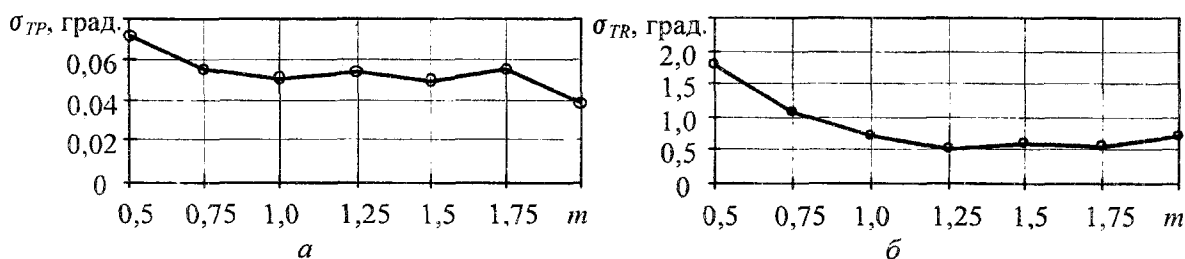


Рис. 3

На рис. 4, а показана экспериментальная зависимость СКО разности фаз опорных генераторов в зависимости от ширины спектра фазового шума при отношении сигнал-шум на входе приёмника, равном $38,4$ дБ, и при индексе модуляции передаваемого синхронизирующего сигнала $m = 1$. Рядом на рис. 4, б показана зависимость СКО набега фазы опорного сигнала в радиотракте в зависимости от ширины спектра фазового шума, при таких же параметрах радиоканала.

Из графиков, показанных на рис. 4, следует, что система синхронизации наиболее чувствительна к низкочастотным фазовым шумам, спектральные составляющие которых попадают в полосу пропускания системы ФАПЧ. Также следует отметить, что при увеличении ширины спектра фазового шума более чем 244 Гц происходил срыв синхронизации в системе ФАПЧ. Это связано с искажениями передаваемого синхронизирующего сигнала.

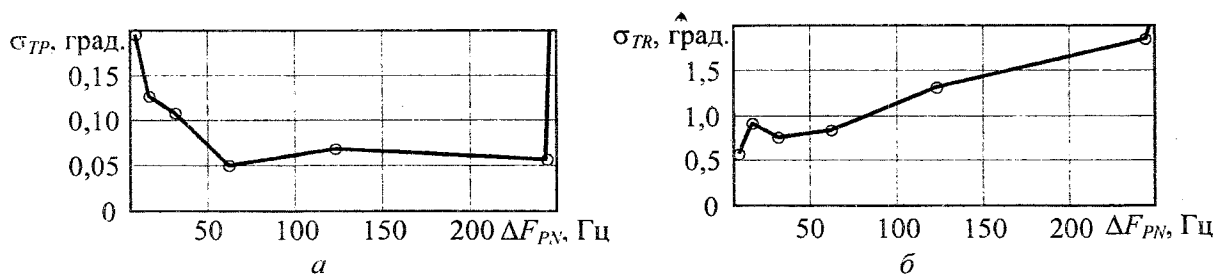


Рис. 4

На рис.5, *а* показана экспериментальная зависимость СКО разности фаз опорных генераторов, в зависимости от отношения сигнал-шум в радиоканале, при отсутствии фазового шума, и при индексе модуляции передаваемого синхронизирующего сигнала $m = 1$. Рядом на рис. 5, *б* показана зависимость СКО набега фазы опорного сигнала в радиотракте в зависимости от отношения сигнал-шум, при таких же параметрах радиоканала.

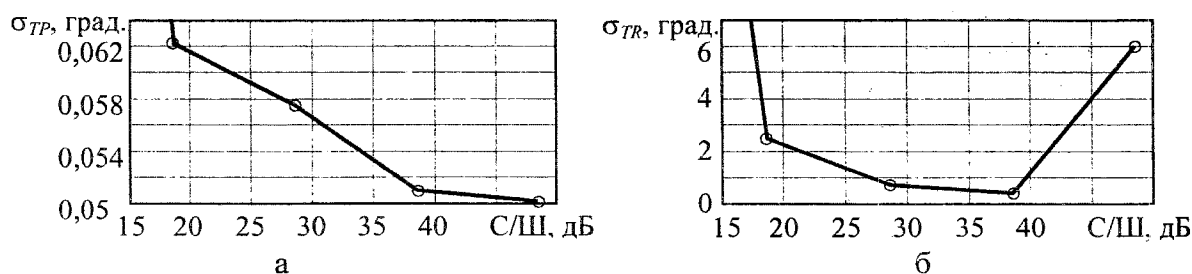


Рис. 5

При анализе рис. 5 видно, что при отношении сигнал-шум на выходе радиоприёмника выше 18,4 дБ точность работы системы синхронизации существенно не зависит от амплитудных шумов в радиоканале. Однако при отношении сигнал-шум на выходе радиоприёмника менее 18,4 дБ происходит срыв синхронизации в системе ФАПЧ. Это связано с тем, что для передачи синхронизирующего сигнала используется частотная модуляция. Кроме того, сигнал управления системой ФАПЧ проходит через пороговое устройство, что улучшает отношение сигнал-шум, но приводит к срыву синхронизации, если уровень входного сигнала оказывается ниже порогового значения.

На рис.6, *а* показана экспериментальная зависимость СКО разности фаз опорных генераторов при совместном воздействии амплитудных и фазовых шумов, в зависимости от отношения сигнал-шум в радиоканале, при ширине спектра фазового шума, равной 7,62 Гц, и при индексе модуляции передаваемого синхронизирующего сигнала $m = 1$. Рядом на рис. 6, *б* представлена зависимость СКО набега фазы опорного сигнала в радиотракте в зависимости от отношения сигнал-шум, при таких же параметрах радиоканала.

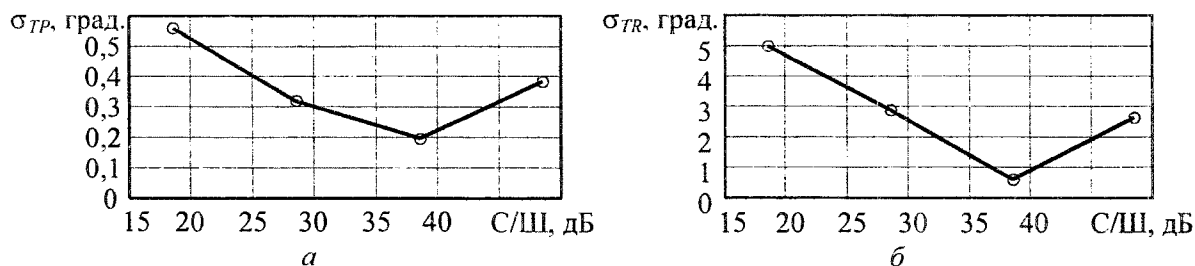


Рис. 6

Совместный анализ графиков на рис. 4 – 6 позволяет сделать вывод, что при отношении сигнал-шум на выходе приёмника более 28 дБ воздействием амплитудных и фазовых шумов на работу системы синхронизации можно пренебречь. Однако совместное воздействие амплитудных и фазовых шумов на передаваемый синхронизирующий сигнал существенно проявляется при величине отношения сигнал-шум на выходе приёмника менее 28 дБ.

Выводы

1. Проведен анализ влияния дестабилизирующих факторов на точность синхронизации опорных низкочастотных генераторов, осуществляемой через атмосферный канал связи посредством модуляции радиосигнала синхронизирующим сигналом.

2. Приведены результаты экспериментального исследования влияния амплитудных и фазовых шумов в радиотракте на точность синхронизации низкочастотных опорных генераторов. Показано, что оптимальным, с точки зрения ширины спектра радиосигнала и минимума среднеквадратического отклонения разности фаз опорных генераторов, для данной системы является индекс модуляции радиосигнала равный единице.

3. Подтверждено, что при отношении сигнал-шум на выходе приёмника более 28 дБ, воздействием амплитудных и фазовых шумов на работу системы синхронизации можно пренебречь.

Таким образом, показана возможность работы системы синхронизации двух низкочастотных опорных генераторов через атмосферный канал связи посредством модуляции радиосигнала синхронизирующим сигналом, а также обосновано требование к отношению сигнал-шум на входе системы фазовой автоподстройки частоты управляемого генератора. Доказано, что ошибками фазовой синхронизации опорных генераторов при известных системных допущениях можно пренебречь. При этом можно производить исследования комплексного коэффициента передачи микроволнового канала связи с высокой точностью, не зависящей от параметров опорного канала связи. Относительные неустойчивости частот опорного и синхронизируемого генераторов, составляющие всего 10^{-7} , не сказываются на долговременных фазовых измерениях. Только длина опорного канала связи (в первом приближении равная длине микроволновой измерительной трассы) определяет величину дополнительной ошибки измерения фазовых флуктуаций на микроволновой измерительной трассе. Однако при длине волны синхронизируемых опорных низкочастотных колебаний, равной 75 км, влиянием длины трассы на эту составляющую ошибки можно пренебречь.

Список литературы: 1. Гимплевич Ю. Б., Широков И. Б., Поливкин С. Н. Радиоволновые гомодинные измерительные преобразователи в системах контроля параметров технологических процессов // Современные проблемы радиотехники и телекоммуникаций «РТ – 2011» : Материалы 7-й междунар. молодежной науч.-техн. конф., 11 – 15 апр. 2011 г. – Севастополь : Изд-во СевНТУ, 2011. – С. 35 – 37. 2. Shirokov I. B., Sinitsyn D. V., Martynyuk D., Jandieri G. V. Multipath Angle-of-Arrival, Amplitude and Phase progression Measurements on Microwave Line-of-Sight Links // Proc. EuCAP'06. – Nice, France, 2006. — 6 p. 3. Сердюк И. В., Широков И. Б. Исследование воздействия фазового шума на систему синхронизации генераторов через атмосферный канал связи // Сб. науч. трудов СВМИ им. П.С. Нахимова ВМС ВСУ, Севастополь, 2010. – Вып.1 (1). – С. 48 – 53. 4. Сердюк И. В. Модель атмосферного канала связи с фазовым шумом // Матер. 20-й Междунар. Крымской микроволновой конференции «СВЧ техника и телекоммуникационные технологии» (КрыМиКо'2010), Севастополь, 2010. — С. 343—344.

Севастопольский национальный
технический университет

Поступила в редколлегию 11.08.2011

ИССЛЕДОВАНИЕ СПЕКТРА ВЫХОДНОГО СИГНАЛА НЕЛИНЕЙНОЙ СИСТЕМЫ В РЕЖИМЕ СТОХАСТИЧЕСКОГО РЕЗОНАНСА

Введение

В радиотехнике и теории связи проблема надежной передачи сигналов неотделима от методов повышения помехоустойчивости. В современных условиях борьба с помехами выдвигается на первый план. Созданы корректирующие коды, оптимальные фильтры, используется обнаружение методом накопления, вопросы приема сигналов рассматриваются с позиции теории статистических решений и т.д. [1].

Вместе с тем, исследования, проведенные физиками в 90-е годы [2], привели к парадоксальным выводам. Наличие шума на входе нелинейных систем, обладающих эффектом так называемого стохастического резонанса (СР), позволяет выделить слабый (по сравнению с шумом) гармонический сигнал из аддитивной смеси с белым шумом. Эффект СР характеризует отклик нелинейной системы на слабый входной сигнал, который заметно усиливается при определенном значении интенсивности шума на входе. При этом выходные параметры нелинейной системы, такие как коэффициент усиления и отношение сигнал/шум, имеют отчетливо выраженный максимум [2].

1. Анализ нелинейной системы с помощью рядов Вольтерра

Для получения сигнала на выходе нелинейной системы в аналитическом виде обычно применяются ряды Вольтерра. Они описаны как «степенные ряды с памятью», отображающие выходной сигнал нелинейной системы в виде степеней входного сигнала $x(t)$ [3]. Для описываемой ниже системы будем пользоваться следующей формой записи ряда

$$y(t) = \sum_{n=1}^{\infty} \frac{1}{n!} \int_{-\infty}^{\infty} du_1 \dots \int_{-\infty}^{\infty} du_n g_n(u_1, \dots, u_n) \prod_{r=1}^n x(t - u_r), \quad (1)$$

где $y(t)$ – выходной сигнал; $x(t)$ – входной сигнал; $g_n(u_1, \dots, u_n)$ – ядра, которые описывают рассматриваемую систему.

Следует отметить, что ядро первого порядка $g_1(u_1)$ является импульсной характеристикой линейной цепи. Таким образом, ядра более высокого порядка можно рассматривать как импульсные характеристики высокого порядка, которые служат для описания различных порядков нелинейности.

Фигурирующий в соотношении коэффициент $\frac{1}{n!}$ большинством авторов не используется. Он введен А. Бедросяном и Д. Райсом [3] с целью упрощения полученных выражений.

Существенную роль в проводимом анализе играет n -кратное преобразование Фурье, которое выглядит следующим образом

$$G_n(f_1, \dots, f_n) = \int_{-\infty}^{\infty} du_1 \dots \int_{-\infty}^{\infty} du_n g_n(u_1, \dots, u_n) \exp[-j(f_1 u_1 + \dots + f_n u_n)], \quad (2)$$

Величина G_0 тождественно равна нулю, так как в рассматриваемом случае ряд Вольтерра начинается с $n=1$, а не с $n=0$, что соответствовало бы активной системе (когда есть выходной сигнал при отсутствии входного) либо противоречило принципу причинности.

$G_1(f_1)$ – передаточная функция линейной цепи.

Таким образом, преобразование ядра Вольтерра n -го порядка является аналогом передаточной функции n -го порядка.

Полные формулы вида (1) представляют собой бесконечные ряды, причем трудоемкость вычисления n -го члена с увеличением n быстро возрастает, однако при анализе систем связи членами ряда Вольтерра выше второго или третьего порядка можно пренебречь [3].

2. Расчет и анализ спектральной плотности мощности выходного колебания

В качестве модели рассмотрим нелинейную систему, описываемую уравнением

$$\dot{y}(t) = -y(t) - y^3(t) + x(t). \quad (3)$$

Здесь $x(t)$ – входной сигнал, представляющий собой аддитивную смесь гармонического сигнала и нормального шума. Как показано в [4], данная система обладает эффектом СР. Используя приведенные в [3] аналитические выражения для спектральной плотности мощности гармоник сигнала на выходе нелинейной системы, получим соответственно

- для первой гармоники

$$S(f_0) = \delta(f - f_0) \left| \frac{A}{2} G_1(f_0) + \frac{A^3}{16} G_3(f_0, f_0, -f_0) + \frac{A}{4} \int_{-\infty}^{\infty} W_1(f_1) G_3(f_1, -f_1, f_0) df_1 \right|^2, \quad (4)$$

- для второй гармоники

$$S(2f_0) = 0, \quad (5)$$

- для третьей гармоники

$$S(3f_0) = \delta(f - 3f_0) \left| \frac{A^3}{48} G_3(f_0, f_0, f_0) \right|^2. \quad (6)$$

Теперь, подставляя в выражения (4) – (6) полученные в [4] значения нелинейных передаточных функций $G_k(\bullet)$, найдем соответственно частотные зависимости спектральной плотности мощности гармоник выходного сигнала нелинейной системы в следующем виде:

- первая гармоника

$$S(\omega_0) = A^2 \frac{16\omega_0^2(1 + \omega_0^2) + [2(1 + \omega_0^2)(2 - 3W_1) - 3A^2]^2}{64(1 + \omega_0^2)^2} \delta(\omega - \omega_0), \quad (7)$$

- вторая гармоника

$$S(2\omega_0) = 0, \quad (8)$$

- третья гармоника

$$S(3\omega_0) = \frac{A^6}{64(1 + 9\omega_0^2)(1 + \omega_0^2)^2} \delta(\omega - 3\omega_0). \quad (9)$$

Здесь A – амплитуда гармонического сигнала на входе системы, W_1 – спектральная мощность шумовой составляющей на входе системы. Далее для повышения наглядности и удобства расчетов в полученных формулах используется круговая частота ω_0 вместо f_0 .

Проанализируем полученные выражения. Так, формула (9) показывает, что при условии стохастического резонанса, которому соответствует $A < 1$ [2], третья гармоника выходного сигнала принимает малые значения. Исследование выражения (7) позволяет определить области значений спектральной плотности мощности входного шума W_1 , при котором наблюдается возрастание амплитуд выходного сигнала с ростом величины W_1 , для этого в таблице приведены выражения для частных производных амплитуды первой гармоники выходного колебания:

$$\frac{\partial S(\omega_0)}{\partial W_1} = -6 \left[2(1 + \omega_0^2)(2 - 3W_1) - 3A^2 \right]$$

$$\frac{\partial S(\omega_0)}{\partial A} = \frac{A}{2(1 + \omega_0^2)} \left[\omega_0^2 + \frac{(x - B)(x - 3B)}{16(1 + \omega_0^2)} \right],$$

где $B = 3A^2$, $x = 2(1 + \omega_0^2)(2 - 3W_1)$.

Видно, что производная $\partial S(\omega_0)/\partial W_1$ равна 0 при значении плотности мощности шума

$$W_{1m} = \frac{2}{3} - \frac{A^2}{2(1 + \omega_0^2)}, \quad (10)$$

что соответствует абсциссе точки минимума функции $S(\omega_0)$. Если мощность шума превышает значение, полученное по формуле (10), то мощность спектральной составляющей на частоте первой гармоники возрастает с ростом шума. В случае, когда амплитуда сигнала принимает значение

$$A = 2\sqrt{\frac{1 + \omega_0^2}{3}}, \quad (11)$$

зависимость $S(\omega_0)$ становится монотонной, а значит, спектральная плотность сигнала на выходе возрастает при возрастании мощности шума от $W_{1m} = 0$. Таким образом, при $W_1 > W_{1m}$ имеет место выделение первой гармоники полезного сигнала, причем все более эффективное при возрастании мощности шума на входе. График, приведенный на рис. 1, иллюстрирует данный вывод.

Рассмотрим частную производную $\partial S(f_0)/\partial A$. Очевидно, что здесь все величины, кроме $(x - B)(x - 3B)$, положительно определены. Тогда легко найти, что выражение для частной производной неотрицательно при $W_1 \geq 3/2$. Следовательно, при $W_1 \geq 3/2$ имеет место возрастание мощности первой гармоники с ростом мощности входного шума.

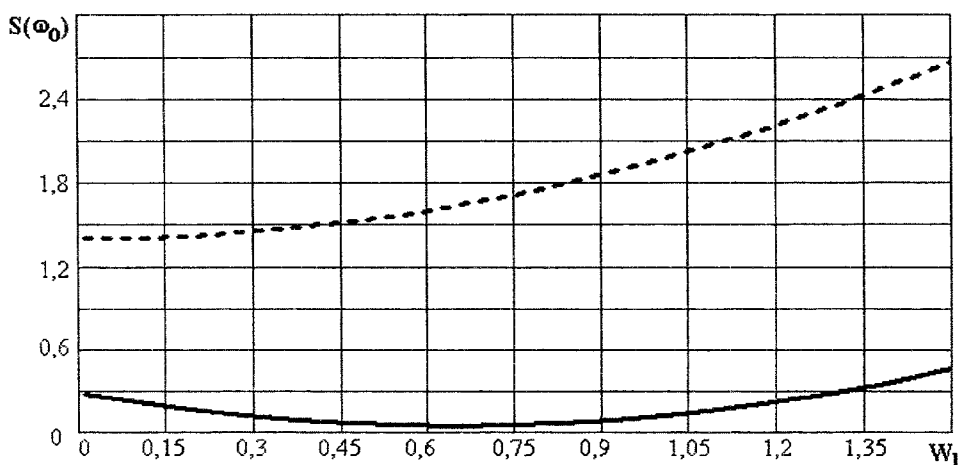


Рис. 1. График зависимости спектральной плотности мощности первой гармоники на выходе рассматриваемого нелинейного устройства $S(\omega_0)$ от спектральной мощности шума на частоте $\omega_0 = 0,1$ [сплошная линия - амплитуда первой гармоники $A = 0,2$, пунктир - амплитуда вычислена по формуле (11)]

Спектральная плотность мощности $S(\omega_0)$ является функцией трех переменных: A, ω_0 и W_1 . Введем в рассмотрение две функции: двумерную амплитудную характеристику $S_a(A, W_1)$ и амплитудно-частотную характеристику $S_a(\omega_0, W_1)$, графики которых построены на рис.2 и 3 соответственно.

Рис. 2 показывает, что при заданной амплитуде входного гармонического сигнала A спектральная плотность мощности $S(\omega_0)$ имеет один минимум, а при заданной плотности мощности шума W_1 величина $S(f_0)$ монотонно возрастает с ростом A . Графики, приведенные на рис.3, показывают, что при заданной амплитуде первой гармоники A и частоте ω_0 , функция $S(f_0)$ имеет единственный минимум при значении W_{1m} , которое является решением уравнения $2(1 + w_0^2)(2 - 3W_{1m}) - 3A^2 = 0$; далее с ростом W_1 величина $S(f_0)$ монотонно возрастает.

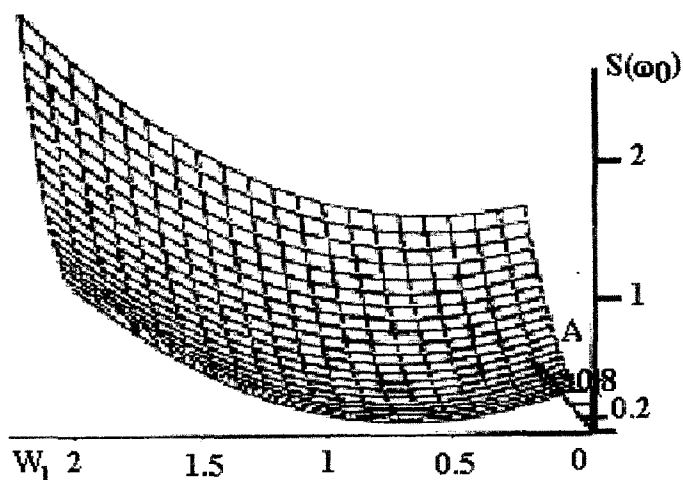


Рис. 2. График зависимости спектральной плотности мощности первой гармоники на выходе рассматриваемого нелинейного устройства $S(\omega_0)$ от амплитуды первой гармоники A на входе и спектральной плотности мощности шума на входе W_1

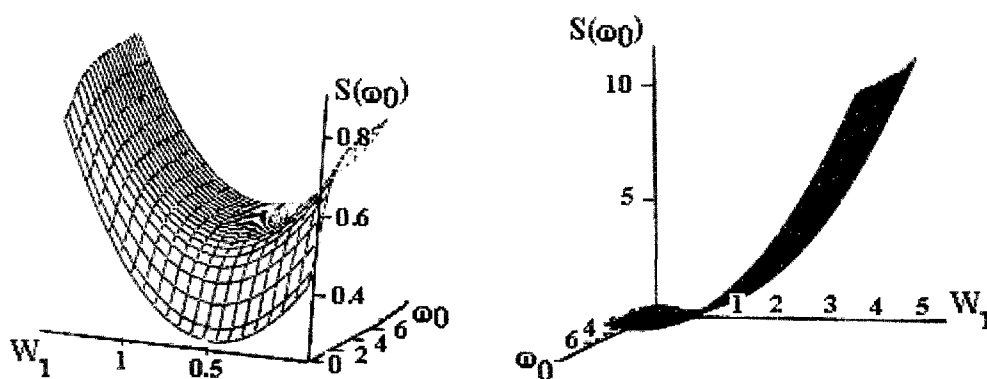


Рис. 3. Графики зависимости спектральной плотности мощности первой гармоники на выходе рассматриваемого нелинейного устройства $S(\omega_0)$ от циклической частоты первой гармоники на входе ω_0 и спектральной плотности мощности шума на входе W_1

Выводы

С помощью метода рядов Вольтерра проведен анализ нелинейного уравнения, описывающего реакцию нелинейной системы, в которой имеет место эффект стохастического резонанса, на воздействие колебания в виде смеси гармонического сигнала и нормального шума. Показано, что стохастический резонанс проявляется в усилении гармонического сигнала при возрастании уровня входного шума.

Введены и рассчитаны нелинейные передаточные характеристики системы, с помощью которых вычислены значения амплитуды входного сигнала, ограничивающей снизу область стохастического резонанса. Показано, что передаточные характеристики являются преобразованием ядра Вольтерра n -го порядка.

Введены, рассчитаны и построены двумерные нелинейные амплитудная и амплитудно-частотная характеристики, в результате анализа которых получены выражения для оптимальных значений амплитуды сигнала и спектральной плотности мощности шума, ограничивающих область стохастического резонанса. Показаны области монотонного возрастания амплитуды сигнала с ростом интенсивности шума.

Получив с помощью рядов Вольтерра аналитические выражения для различных частотных составляющих, можно в дальнейшем определить и проанализировать одно из важнейших соотношений в теории связи и радиотехнике: отношение сигнал/шум на выходе для рассматриваемого нелинейного устройства.

Список литературы: 1. Харкевич А.А. Борьба с помехами. – М. : Наука, 1965. – 275с. 2. Анищенко В.С., Нейман В.Б., Мосс Ф., Шиманский-Гайер Л. Стохастический резонанс как индуцированный шумом эффект увеличения степени порядка // Успехи физических наук. – 1999. – Т. 169, № 1. – С. 7–37. 3. Бедросян А., Райс Д. Свойства выходного сигнала систем, описываемых рядами Вольтерра (нелинейных систем с памятью), при подаче на вход гармонических колебаний и гауссова шума // ТИИЭР. – 1971. – Т. 59, № 12. – С.58–82. 4. Харченко О.И., Чумаков В.И., Складрук В.Л. К расчету отклика нелинейной системы с памятью с применением рядов Вольтерра // Зб. наук. праць АВМС ім. П.С. Нахімова.-Севастополь : АВМС ім. П.С. Нахімова, 2001.-Вип.3(3).-С.110-115.

Академия ВМС им. П.С. Нахимова,
г. Севастополь

Поступила в редколлегию 09.09.2011

МЕТОДЫ ПОВЫШЕНИЯ ОТКАЗОУСТОЙЧИВОСТИ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ

Введение

Основной задачей телекоммуникационных систем является расширение сферы предоставляемых услуг и повышение их качества. Очевидно, что успешное решение этой задачи возможно только при высокой экономической эффективности работы сети, а именно – в случае значительной надёжности и помехоустойчивости передачи наряду с низкой стоимостью передаваемого информационного бита. Всё это делает актуальным развитие таких направлений в технике телекоммуникаций, как разработка совершенных устройств и методов уплотнения и подходов к повышению достоверности и надёжности передачи.

Эффективность управления телекоммуникационными инфраструктурами на базе современных информационных, сетевых и компьютерных технологий требует создания мультисервисных сетей телекоммуникаций общего пользования и телематических служб, образованных терминалами многофункционального и интеллектуального типа с повышенной пропускной способностью для удовлетворения постоянно растущих потребностей общества в телекоммуникации. Решение этой проблемы неразрывно связано с повышением уровня технического обеспечения телекоммуникационных систем (ТС), реализованного многофункционального терминального комплекса для интеграции процессов обслуживания и управления передачей информации.

При этом задача повышения уровня технического обеспечения систем телекоммуникаций (СТ) решается путем создания многофункциональных и интеллектуальных терминальных комплексов с внедрением инфокоммуникационных технологий, которые относятся к наиболее актуальным задачам. Такая масштабная информатизация в первую очередь связана с повышением качества функционирования ТС, главным звеном которых являются многофункциональные терминальные комплексы на основе функционально-блочных систем (модемы, шлюзы, интерфейсы, концентраторы, мосты, терминальные мультиплексоры и элементы управления), представляющие собой распределённые системы управления на базе TMN (Telecommunication Management Network).

Исследуемые *эффективность и помехоустойчивость* системы являются комплексными характеристиками *качества функционирования ТС*, образованных терминалами многофункционального и интеллектуального типа, отражают способность системы обеспечивать заданные технические, экономические и эксплуатационные характеристики при выполнении возложенных на нее абонентских, информационных и сетевых функций в рамках системы обмена речевой, видео и неречевой информации.

Среди ученых стран СНГ и других зарубежных стран, занимающихся проблемами *повышения эффективности и помехоустойчивости* СТ и их технического обеспечения, можно выделить работы В.А. Котельникова, Г.П. Захарова, В.П. Бакалова, Н.Б. Зелигера, В.П. Шувалова, Л.Н. Финка, В.Н. Гордиенко, Ф.Г. Мамедова, О.С. Чугреева, В.О. Шварцмана, В.А. Игнатова, А.Н. Гасанова, Н.В. Захарченко, П. Беккера, И.А. Ушакова, Э.А. Якубайтиса, L. Kleinrock, K. Shannon, O. Serlin, D. Ting, M. Schwartz и др.

Работы указанных авторов подготовили базу для развития нового научного направления в создании систем передачи и приема цифровой информации, связанного с разработкой методов расчета показателей качества функционирования технических средств в сетях телекоммуникации. Однако в этих работах недостаточно внимания уделено созданию многофункциональных ТК для передачи и приёма речевой и неречевой информации при их совместном обслуживании. Кроме того, эти решения не охватывают всей проблемы повышения эффективности и помехоустойчивости ТК СТ.

В направлении повышения эффективности элементов и устройств вычислительной техники и систем управления ТС важные результаты получены в работах Б.П.Терентьева, В.В.Губарева, С.И.Сахарчука, В.Н.Четверикова, Т.М.Алиева, В.С.Шибанова, Н.Г.Фарзана, В.В.Лебедянцева, В.П.Дьяконова, К.М.Имамвердиева, Р.Т.Гумбатова, J.Grabner, J.Wieselman и др. Однако применение этих результатов для улучшения качества функционирования ТК с внедрением современных технологий возможно при существенных ограничениях на эффективность использования канальных и терминальных ресурсов.

Значительный вклад в фундаментальные исследования, направленные на создание новых ЭВМ и их использование в пионерских системах управления технологическими процессами, энергетическими и другими объектами, в том числе военного назначения, для систем автоматизации научного эксперимента, был сделан академиком В.М. Глушковым, основоположником информатики в Украине, и многими ведущими учеными основанного им Института кибернетики НАН Украины.

Важнейшей проблемой является повышение отказоустойчивости телекоммуникационных систем (ТС). В соответствии с [1] отказоустойчивость основана на реализации в полном или усеченном виде цепочки действий:

- прогнозирование (fault forecasting) возможности появления (проявления) дефекта и возникновения отказа вследствие этого дефекта;
- предупреждение (fault prevention) появления (проявления) дефекта и возникновения отказа;
- обнаружение (fault detection) появления (проявления) дефекта, ошибки вычислений, отказа;
- идентификация (fault diagnosis) причины, вида и места дефекта (отказа);
- парирование (fault tolerance) последствия дефекта и возникновения отказа.

Последнее действие может включать: реконфигурацию (fault removal) структуры (архитектуры) путем исключения отказавшего компонента из конфигурации, замены работоспособным и восстановление вычислительного процесса (fault recovery). Механизмы отказоустойчивости должны быть инвариантны по отношению к типам дефектов, вызывающих отказы.

Одним из важных свойств телекоммуникационных систем и систем управления критическими объектами является отказоустойчивость. Классически под отказоустойчивостью вычислительной (телекоммуникационной) системы понимается способность устранения последствий неисправностей элементов и программного обеспечения за счет использования аппаратной, информационной и алгоритмической избыточности [2].

Повышение отказоустойчивости предполагает подавление влияния отказов и сбоев на работу ТС. Оно осуществляется с помощью средств контроля и коррекции ошибок, а также средств автоматического восстановления вычислительного процесса после проявления неисправности, включая аппаратную, программную и временную избыточность, на основе которых реализуются различные варианты отказоустойчивых архитектур. Повышение отказоустойчивости – это способ предотвращения отказа системы. Поэтому разработка новых методов повышения отказоустойчивости ТС является актуальной задачей.

Основные методы обеспечения отказоустойчивости ТС

Наряду с термином «отказоустойчивая система» в эквивалентном смысле встречаются термины «системы высокой готовности», «устойчивые и эластичные к сбоям и отказам системы», «системы непрерывной и постоянной готовности». Однако термины трактуются по-разному отдельными разработчиками, поставщиками и потребителями. Рассмотрим трактовки некоторых терминов.

Высокая Готовность (High Availability). Все системы высокой готовности обеспечивают устойчивость к отказам и сбоям благодаря применению принципа избыточности. Конфигурация системы обеспечивает ее быстрое восстановление после обнаружения неисправности, для чего используются избыточные аппаратные и программные средства. Для современных

систем высокой готовности характерно использование технологии “горячей” замены отказавшего узла.

Эластичность к сбоям (Fault Resiliency). Ряд специалистов делят весь диапазон систем высокой готовности на две части, при этом в верхней части оказываются системы, эластичные к сбоям. Эластичность к сбоям определяет более короткое время восстановления, которое позволяет системе быстро «откатиться» назад при обнаружении неисправности.

Устойчивость к сбоям (Fault Tolerance). Устойчивые к сбоям системы (“отказоустойчивые системы”) имеют в своем составе избыточную аппаратуру для всех функциональных блоков, включая процессоры, источники питания, подсистемы ввода/вывода и подсистемы дисковой памяти. Если соответствующий функциональный блок неправильно работает, всегда имеется горячий резерв, и неисправность в любом блоке не может вывести систему из строя. В ряде отказоустойчивых систем избыточные аппаратные средства можно использовать для распараллеливания обычных работ.

Непрерывная готовность (Continuous Availability). Лучшими среди отказоустойчивых систем являются системы, обеспечивающие непрерывную готовность. Система с непрерывной готовностью, если она работает корректно, позволяет ликвидировать как плановые, так и неплановые простои и проводить модернизацию (upgrade) и обслуживание системы в оперативном режиме (режиме on-line). Разработка подобной системы охватывает как аппаратные средства, так и программное обеспечение. Очень важным дополнительным требованием к таким системам является сохранение уровня производительности в случае отказа какого-либо компонента.

Следует отметить, что понятие «непрерывная готовность» все-таки подразумевает возможность сбоя в работе системы. Однако если типичное значение коэффициента готовности для обычной вычислительной (телекоммуникационной системы) системы составляет около 99 %, то для систем непрерывной готовности этот параметр устанавливается на уровне не менее 99.999 %.

Именно системы непрерывной готовности обеспечивают наивысший возможный уровень гарантии *работоспособности системы*. Помимо того, что непрерывная готовность является проверенной технологией, она представляет собой простое, простое в использовании, прозрачное для приложений и базирующееся на стандартах решение.

Постоянная готовность (Permanent Availability). Это скорее теоретическое понятие. Коэффициент готовности для такого рода систем принимается равным 100 %, т.е. предполагается отсутствие сбоев в работе, что практически недостижимо.

Выбор того или иного уровня готовности определяется теми последствиями, которые будут иметь для конкретного объекта отказы управляющей системы.

Фирмы-изготовители предлагают специальные средства для построения *отказоустойчивого нижнего уровня ТС*. Типичным является применение специальных модулей для построения дублированных управляющих систем (УС) с «горячим» резервированием. Структура подобной системы приведена на рис. 1.

Она содержит два идентичных контроллера (основной и резервный), арбитр и схему коммутации выходных сигналов. Входные сигналы от объекта поступают в оба контроллера.

Широко применяются также троированные структуры. На рис. 2 приведена схема, иллюстрирующая работу троированной системы. Как и в предыдущем примере, входные сигналы и другая информация поступают одновременно в три идентичных между собой контроллера, в которых синхронно выполняется одна и та же программа. После очередного цикла получения результатов для управления объектом они от каждого контроллера поступают на мажоритарную схему «2 из 3», формирующую интегральный результат. *Отказоустойчивость обеспечивается на всех уровнях:* от сети управления до блоков питания плат ввода-вывода. Для достижения максимальной надежности системы обеспечивается резервирование следующих компонентов и функций: ЛВС, контроллеров, системы SCADA, станции архивной регистрации и сервера отчетов, операторских рабочих станций, сетевых серверов и концентраторов.

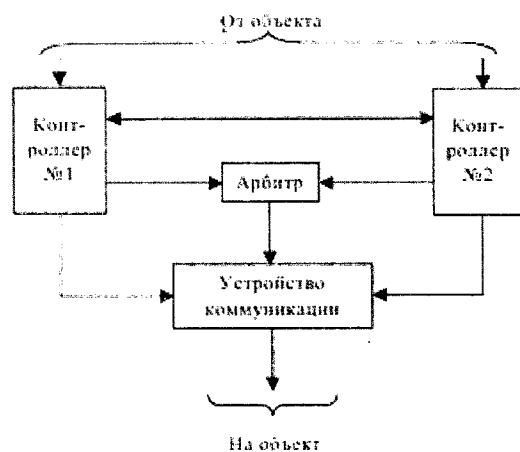


Рис. 1. Структура дублированной УС

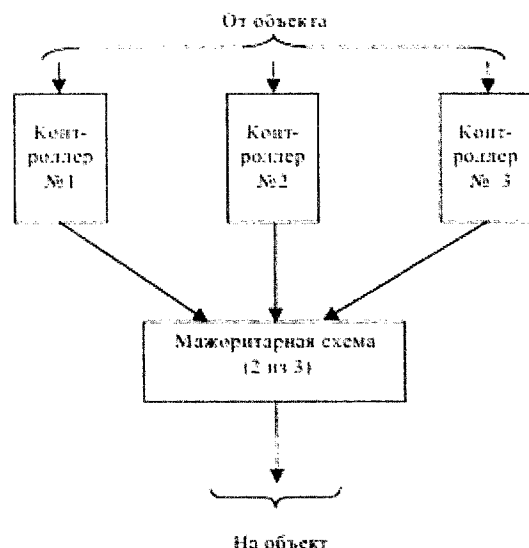


Рис. 2. Структура троированной системы

Отказоустойчивость ЛВС осуществляется протоколом, обеспечивающим гарантированную передачу данных по сети, и мощными свойствами самовосстановления. Резервируемая сеть конфигурируется в виде двойного кольца, обеспечивающего реконфигурацию при отказе любого сегмента магистрали. При реконфигурации изменяется маршрутизация технологических данных, что обеспечивает бесперебойную работу системы. Оба кольца сети постоянно находятся в активном состоянии, причем одно из них работает как сеть данных, а другое – как диагностическая сеть. В редких случаях отказов первой сети вторая захватывает поток данных, гарантируя их целостность.

Системные сообщения передаются по обеим сетям для снижения статистической частоты ошибок. Оперативное обнаружение отказов и сбор данных о производительности коммуникационных каналов системы выполняются индивидуально для каждого устройства. При обнаружении отказа устройство, в котором возникла проблема, автоматически отключается от остальной системы до устранения неисправности.

Каждое устройство в сети обладает несколькими резервированными функциями, что обеспечивает максимальную надежность системы в целом.

Например, все устройства системы управления имеют дублированную схему подключения к каждой из сетей данных, в результате чего достигается четырехкратное резервирование. Контроллер «Овации» можно сконфигурировать с несколькими резервированными функциями, включая дублирование материнских плат процессора, источников питания и ка-

налов связи. Уровень резервирования контроллера выбирается в соответствии с техническими требованиями заказчика. При дублировании процессоров обеспечивается основное и резервное управление с полностью безударным автоматическим переключением между процессорами при сбое или отказе. Автоматическое включение резерва может инициироваться широким набором событий, включая: отказ управляющего процессора; отказ сетевого адаптера; отказ интерфейса ввода – вывода; пропадание питания в управляющем процессоре; перезапуск управляющего процессора.

Как только управление переходит к резервному процессору, неисправный процессор можно отключить, отремонтировать и подключить обратно без оказания воздействия на выполнение алгоритмов управления. После перезапуска восстановленный процессор обнаруживает, что его партнер находится в режиме управления и принимает на себя резервную роль. Управляющий процессор обнаруживает наличие резервного процессора и настраивается на работу с резервом.

Для построения отказоустойчивого верхнего уровня ТС могут использоваться отказоустойчивые серверы. Так, в общепромышленном секторе нашли применение отказоустойчивые серверы Stratus Technologies [3].

В основе технологии Stratus Continuous Processing лежат три фактора:

1. Аппаратная отказоустойчивость с резервированием всех компонентов. При этом используется жёсткая (потактовая) синхронизация процессов и данных в дублирующих друг друга компонентах. Все компоненты архитектуры Continuous Processing работают параллельно и согласованно для того, чтобы не просто минимизировать время незапланированного простоя, а предотвратить его возникновение. Таким образом, в случае отказа одного из них потери данных и остановки сервера не происходит.

2. Программное обеспечение повышенной устойчивости. В сервере используются программные средства для предотвращения случайных сбоев в аппаратуре.

3. Архитектура активного сервиса. Подразумевается возможность горячей замены любого компонента (включая процессоры) без остановки приложений. После замены компоненты автоматически включаются в работу.

Конструкция заменяемых блоков исключает ошибку при снятии/установке, поэтому замена может производиться пользователем самостоятельно. Сервер автоматически извещает центр поддержки о происшествии или неисправности, после чего, при необходимости, нужный блок доставляется для замены.

Критерии отказоустойчивости ТС

При оценке эффективности функционирования ТС возникает необходимость выделения подсистем и других элементов для описания поведения их в системе. Каждая из подсистем ТС исследуется в соответствии со своими частными критериями. Показано [4], что если отдельные подсистемы функционируют относительно независимо, то оптимизация по частным критериям подсистем обеспечивает оптимальное функционирование подсистемы в целом, когда критерий эффективности системы является монотонной функцией эффективности функционирования каждой из подсистем. В общем случае, когда имеет место сложная корреляция процессов функционирования различных элементов системы (а именно так обстоит дело на практике) это может не соблюдаться.

Естественно, что эффективность ТС, как сложной системы, не может быть оценена по одному критерию. Значение каждого из показателей качества ТС в той или иной мере характеризует эффективность функционирования ТС, т.е. степень соответствия его назначению – максимально быстро удовлетворять требования по вводу, обработке и выводу информации. Причем, между ними может существовать взаимосвязь.

Таким образом, критерий эффективности ТС является векторным. На практике его применять неудобно. Общий подход к решению проблемы выбора критерия эффективности предложен в [4]. В соответствии с этим подходом на практике можно использовать следующие варианты:

1. Из множества показателей следует выбрать один, наиболее важный.

2. Можно попытаться уменьшить размерность критерия, введя взвешенную сумму различных показателей, при этом, однако, выбор численных значений весовых коэффициентов остается трудной задачей.

3. Можно попытаться отыскать некоторый более общий показатель, поглощающий все остальные частные показатели системы. Очень часто такой показатель является критерием эффективности надсистемы.

В соответствии с третьим вариантом можно предложить интегральный подход, когда эффективность какой-либо подсистемы оценивается через степень влияния ее характеристик на показатели эффективности всей системы, в которую входит данная подсистема. Такой подход оправдан тем, что, в конечном итоге, для системы важны показатели ее подсистемы, рассматриваемой как «черный ящик». Например, для системы управления технологическим объектом важными являются интегральные характеристики всего ТС в целом, т.е. его внешние характеристики, а множество внутренних характеристик его подсистем и компонентов является малозначимым.

Для подсистем ТС, выполняющих расчетные задачи моделирования в реальном или ускоренном масштабах времени, главным качеством является достижение необходимой производительности, при которой цикл моделирования выполняется за заданный промежуток времени. Невыполнение цикла моделирования за заданный промежуток времени фактически является *отказом* подсистемы. И наоборот, гарантированное выполнение цикла моделирования за заданный промежуток времени является одним из свойств ее *отказоустойчивости*. Подобные подсистемы ТС, в частности, применяются в системах поддержки принятия решения, в моделирующих вычислительных комплексах, предназначенных для отработки систем управления космическими аппаратами и бортовых систем управления [5].

Производительность применяется для оценки качества вычислительных систем, одной из разновидностей которых является ТС. К настоящему времени сформулированы несколько различных показателей производительности вычислительной системы (ВС) [6 – 9]. Такими показателями могут быть, например:

- производительность, рассчитанная как среднее число задач, которые могут быть выполнены в единицу времени;
- относительная пропускная способность – усредненное отношение числа обслуженных запросов к числу поступивших в единицу времени;
- коэффициент использования (отношение среднего времени работы ВС к общему времени функционирования с учетом простоев).

Еще большее многообразие понятий наблюдается в определениях параметров производительности ВС при выполнении конкретных прикладных программ, например [68-70], от средних значений времен выполнения отдельных операций, времен отклика ВС на различные запросы до времен выполнения "смесей" команд и/или процедур, времени выполнения классических численных и/или "эталонных" задач.

Зачастую упомянутые показатели рассматриваются как критерии эффективности ВС общего применения для различных приложений.

Такой показатель, как номинальная производительность, характеризует "потенциальную" возможность ВС, т.е. максимально возможную физическую скорость обработки данных. Реальная или эффективная производительность зависит от множества факторов, как заложенных при проектировании ВС (соотношение характеристик быстродействия ее компонентов, дисциплина их обслуживания), так и являющихся характеристиками операционных систем и прикладных программных процессов конкретных систем контроля и управления (характеристики потоков данных, степень "накладных расходов" при работе подсистемы ввода-вывода операционной системы). Эффективная производительность ВС равна произведению номинальной производительности и коэффициента (вероятности) загрузки ВС.

При известной номинальной производительности коэффициент (вероятность) загрузки можно использовать в качестве показателя эффективной производительности ВС. Под коэф-

фициентом загрузки имеется в виду отношение полезного времени работы системы к общему времени функционирования системы с учетом простоев. Коэффициент загрузки характеризует реальную пропускную способность системы. Коэффициент загрузки широко применяется как критерий качества при исследовании ВС общего назначения.

Увеличение коэффициента загрузки системы при фиксированной номинальной производительности увеличивает пропускную способность системы. Для моделирующей подсистемы это выражается в увеличении вероятности гарантированного выполнения цикла моделирования за заданный промежуток времени, т.е. в увеличении *отказоустойчивости*.

В связи с этим возникает задача определения коэффициента загрузки подсистем ТС.

ТС функционируют в реальном масштабе времени. Это означает, что времена отклика ТС $T_{iотк}$ по каждой i -й функции управления не должны превышать предельных интервалов времени $T_{iпр}$, определяемых спецификой управляемого объекта. Если $T_{iотк} > T_{iпр}$, то в этом случае ухудшается качество управления, что может привести к нарушению работы управляемого объекта.

Времена отклика ТС являются суммарным временем нескольких составляющих: времени преобразования аналогового сигнала в цифровой код, первичной обработки, времени вычислительных процедур соответствующей задачи, передачи результатов обработки в модули управления исполнительными механизмами, в рабочие станции для визуализации, архивирования и пр. Следовательно, и для каждой временной составляющей существует предельное ограничение.

Поэтому, одним из главных критериев отказоустойчивости подсистем ТС является способность выполнять i -ю функцию за время, не превышающее заданное директивное время $T_{дир}$, с требуемой вероятностью D_i .

Например, для коммуникационной подсистемы ТС это означает, что заявки по передаче сообщений от задачи одного абонента линии вычислительной сети (ЛВС) к задаче другого абонента должны обслуживаться за какое-то ограниченное время с требуемой вероятностью.

Для прикладной программы (приложения), состоящей из набора задач и выполняющей одну из функций ИУС, это означает выполнение ее за время, не превышающее $T_{дир}$, заданное проектировщиком ИУС, с требуемой вероятностью D . В частности, для подсистем ТС, выполняющих расчетные задачи моделирования в реальном или ускоренном масштабах времени, это означает, что цикл моделирования должен выполняться за время, не большее заданного директивного времени $T_{дир}$ с требуемой вероятностью D .

В работе [10] для управляющих ВС реального времени данный критерий трактуется как «надежное выполнение набора задач управления».

В понятии «надежного выполнения задач» отказ управляющего ТС трактуется не только как потеря его работоспособности, но и как невыполнение требуемых задач за время $T_{дир}$. Такой отказ может иметь место даже при безотказном функционировании аппаратуры и программного обеспечения ТС, отвечающего принципам «высокая готовность» (High Availability) и «непрерывная готовность» (Continuous Availability). Причинами такого отказа в некорректно спроектированных ТС могут быть неучтенные проектировщиком информационных управляющих систем (ИУС) внезапные изменения параметров объекта управления из-за случайных динамических изменений условий его функционирования или параметров окружающей среды, случайные изменения объемов данных и объемов вычислений по программам задач, задержки выполнения приложений вследствие некоторых типов прерываний, конфликты процессов при обращении к общим ресурсам и пр.

Время выполнения задач может также существенно увеличиваться и превышать директивное время из-за случайных неисправностей (сбоев или отказов) компонентов ТС.

Вследствие случайного характера указанных явлений и эффектов, времена выполнения задач и их фрагментов (программных модулей), а также наборов задач в целом необходимо рассматривать, в общем случае, как случайные величины, а процесс выполнения наборов задач в управляющих ТС – как случайный процесс.

В связи с этим возникают *вопросы оценки вероятности успешного завершения набора задач* за заданное директивное время в ТС с заданной производительностью вычислительных ресурсов, прогнозирования успешного завершения набора задач непосредственно при их выполнении в ТС, управления вычислительными процессами для предотвращения угрозы отказа.

Поэтому возникает задача прогнозирования времени выполнения набора задач на вычислительных ресурсах ТС.

В некоторых работах (например, [11-13]) это время рассматривается как совокупность длительностей между событиями, связанными с выполнением заданной программы, либо как некоторая относительная величина, характеризующая изменение предполагаемого времени выполнения программы относительно некоторого эталона. Известны также многочисленные отечественные и зарубежные разработки и исследования по прогнозированию или даже точному расчету времени выполнения наборов задач (в том числе – взаимосвязанных) в параллельных ВС – в предположении, что время решения каждой задачи заранее известно, т.е. является детерминированным (а неслучайным, как в рассматриваемом нами подходе); к таким работам можно отнести, в первую очередь, фундаментальные и комплексные исследования, проведенные в [14]).

Применительно к управляющим ВС, включая управляющие ТС, проблема оценок такого рода получила название математического прогнозирования времени выполнения сложных наборов задач (программных комплексов) и нашла решение в [10, 15-18].

Принципиально, что эти наборы рассмотрены в наиболее трудоемких версиях – с произвольными информационными и логическими связями между задачами – и потому названы комплексами взаимосвязанных работ (КВР) – задач и/или их параллельно-последовательных фрагментов (подзадач, процессов), а в общем случае – программных модулей. Во многих публикациях (например, в [19]) аналогичные структуры именуются как “графы задач”. В предлагаемом подходе КВР следует рассматривать как графовую модель рабочей нагрузки.

В работах [10, 15 – 18] под математическим прогнозированием времени выполнения конкретного, заданного пользователем КВР понимается определение в статике (т.е. до реализации задач в ТС) стохастических оценок времени T реализации КВР (среднего значения, дисперсии, функции $F(t)$ распределения времени T) и определение вероятности D завершения КВР за время, не превышающее заданное $T_{\text{дир}}$, в ТС с заданной конфигурацией и производительностью его вычислительных ресурсов.

Другой задачей, требующей решения, является задача определения параметров производительности ТС реального времени, в которой набор из S задач выполнялся бы за время, не большее директивного времени $T_{\text{дир}}$ с заданной вероятностью D .

Составной частью исследования по обеспечению надежного выполнения взаимосвязанных задач в вычислительных системах реального времени является проблема диспетчеризации (планирования, расписания) наборов задач (программных модулей) по вычислительным ресурсам ВС.

В настоящее время существует большое количество публикаций, посвященных решению этой проблемы. Традиционный интерес к данной проблеме и ее актуальность обусловлены в основном двумя факторами:

- возможностью получения существенного эффекта – заметного уменьшения общего времени выполнения заданного набора задач – при незначительных издержках на разработку и функционирование конкретного алгоритма диспетчеризации;
- непрекращающимся стремлением к “синтезу” оптимальных дисциплин диспетчеризации по различным критериям.

В данной работе на основе методологии [16 – 18] необходимо решить задачу формальной оценки и выбора дисциплин динамической диспетчеризации работ КВР по вычислителям ТС при случайных временах выполнения работ КВР – с целью минимизации времени выполнения каждого заданного КВР, что должно повысить отказоустойчивость ТС.

В связи с этим возникают вопросы оценки вероятности успешного завершения набора задач за заданное директивное время в ТС с заданной производительностью вычислительных ресурсов, прогнозирования успешного завершения набора задач непосредственно при их выполнении в ТС, управления вычислительными процессами для предотвращения угрозы отказа.

Поэтому возникает задача прогнозирования времени выполнения набора задач на вычислительных ресурсах ТС.

В некоторых работах (например, [11-13]) это время рассматривается как совокупность длительностей между событиями, связанными с выполнением заданной программы, либо как некоторая относительная величина, характеризующая изменение предполагаемого времени выполнения программы относительно некоторого эталона. Известны также многочисленные отечественные и зарубежные разработки и исследования по прогнозированию или даже точному расчету времени выполнения наборов задач (в том числе – взаимосвязанных) в параллельных ВС – в предположении, что время решения каждой задачи заранее известно, т.е. является детерминированным (а неслучайным, как в рассматриваемом нами подходе); к таким работам можно отнести, в первую очередь, фундаментальные и комплексные исследования, проведенные в [14]).

Применительно к управляющим ВС, включая управляющие ТС, проблема оценок такого рода получила название математического прогнозирования времени выполнения сложных наборов задач (программных комплексов) и нашла решение в [10, 15-18].

Принципиально, что эти наборы рассмотрены в наиболее трудоемких версиях – с произвольными информационными и логическими связями между задачами – и потому названы комплексами взаимосвязанных работ (КВР) – задач и/или их параллельно-последовательных фрагментов (подзадач, процессов), а в общем случае – программных модулей. Во многих публикациях (например, в [19]) аналогичные структуры именуются как “графы задач”. В предлагаемом подходе КВР следует рассматривать как графовую модель рабочей нагрузки.

В работах [10, 15 – 18] под математическим прогнозированием времени выполнения конкретного, заданного пользователем КВР понимается определение в статике (т.е. до реализации задач в ТС) стохастических оценок времени T реализации КВР (среднего значения, дисперсии, функции $F(t)$ распределения времени T) и определение вероятности D завершения КВР за время, не превышающее заданное $T_{\text{дир}}$, в ТС с заданной конфигурацией и производительностью его вычислительных ресурсов.

Другой задачей, требующей решения, является задача определения параметров производительности ТС реального времени, в которой набор из S задач выполнялся бы за время, не большее директивного времени $T_{\text{дир}}$ с заданной вероятностью D .

Составной частью исследования по обеспечению надежного выполнения взаимосвязанных задач в вычислительных системах реального времени является проблема диспетчеризации (планирования, расписания) наборов задач (программных модулей) по вычислительным ресурсам ВС.

В настоящее время существует большое количество публикаций, посвященных решению этой проблемы. Традиционный интерес к данной проблеме и ее актуальность обусловлены в основном двумя факторами:

- возможностью получения существенного эффекта – заметного уменьшения общего времени выполнения заданного набора задач – при незначительных издержках на разработку и функционирование конкретного алгоритма диспетчеризации;
- непрекращающимся стремлением к “синтезу” оптимальных дисциплин диспетчеризации по различным критериям.

В данной работе на основе методологии [16 – 18] необходимо решить задачу формальной оценки и выбора дисциплин динамической диспетчеризации работ КВР по вычислителям ТС при случайных временах выполнения работ КВР – с целью минимизации времени выполнения каждого заданного КВР, что должно повысить отказоустойчивость ТС.

Особенности данного исследования, отличающие ее от известных работ по аналогичной проблематике, заключаются в следующем:

- дисциплины и диспетчеризации исследуются на основе методологии [17 – 19] математического прогнозирования времени выполнения сложных наборов задач с произвольными информационными и логическими взаимозависимостями между задачами, называемыми комплексами взаимосвязанных работ;

- времена выполнения работ могут быть различны и рассматриваются как случайные величины;

- рассматривается выполнение КВР в неоднородных (несимметричных) вычислительных подсистемах ТС с параллельными вычислительными ресурсами; в этом случае одни и те же работы могут выполняться на вычислителях разных типов, но имеющих различную производительность, а следовательно, – с различными временами выполнения одной и той же работы.

Важными критериями отказоустойчивости ТС также являются [20]:

- высокая надежность его функционирования;

- контроль и управление всеми параметрами критической системы в реальном масштабе времени;

- обеспечение диагностирования и восстановления работоспособности всех подсистем за допустимое разработчиком время;

- обеспечение требуемой глубины диагностирования ТС или его компонентов в реальном масштабе времени за минимальное число тестовых проб или наблюдений.

Поэтому необходимо решить задачу разработки и исследования принципов организации процессов диагностирования неисправностей вычислительных средств ТС и использования дополнительных средств асинхронного резервирования процессов, которые должны обеспечивать не только *диагностирование* и локализацию неисправностей вычислительных ресурсов параллельных ТС и корректное восстановление процессов, но и включать математические методы оценки влияния случайных неисправностей на время выполнения сложных наборов задач.

Необходимо также исследовать и разработать методы, приводящие к существенному уменьшению времени тестирования и диагностирования ТС в процессе эксплуатации на основе создания общей модели организации и проведения диагностического эксперимента, включающего условные и безусловные алгоритмы поиска дефектов с использованием IEEE стандартов тестопригодного проектирования.

Следующим важным критерием отказоустойчивости подсистем ТС, функционирующих в реальном времени, является готовность подсистемы. В [1] готовность (availability) определена как свойство доступности ресурсов системы для предоставления требуемых услуг. Например, в отношении ЛВС под этим термином следует понимать отношение суммарного времени пребывания системы в состояниях, когда ЛВС не работает из-за отсутствия заявок либо, когда идет передача сообщения, и при этом нет других заявок, ожидающих обслуживания, к общему времени функционирования системы [21].

Под готовностью подсистемы Q будет пониматься величина, равная отношению времени работы данной подсистемы, когда в ТС нет заявок, ожидающих обслуживания данной подсистемой.

Заключение

ТС является сложной отказоустойчивой системой, состоящей из подсистем, которые могут включать большое количество взаимодействующих элементов. Для его исследования будут применяться методы аналитического и имитационного моделирования.

Динамику выполнения в ТС программных приложений, реализующих новые функции ИУС, можно представить как набор взаимосвязанных последовательно-параллельных программных модулей (задач, работ) или комплекс взаимосвязанных работ (КВР).

Критерий качества ТС является векторным. Основными показателями качества, используемыми как критерии отказоустойчивости ТС и его подсистем, функционирующих в реальном масштабе времени, в дальнейших исследованиях являются:

- надежность выполнения функций – способность выполнять функции за время, не превышающее $T_{идир}$, с требуемой вероятностью D_i для i -й функции;
- готовность – способность обслуживания запросов без ожидания начала обслуживания;
- обеспечение диагностирования и восстановления работоспособности всех подсистем за допустимое разработчиком время.

Список литературы: 1. Харченко В.С. Гарантоспособность и гарантоспособные системы: элементы методологии // Радиотехнические и компьютерные системы. – 2006. – № 5. – С.7-19. 2. Додонов А.Г., Кузнецова М.Г., Горбачик Е.С. Введение в теорию живучести вычислительных систем. – К. : Наук. думка, 1990. – 184 с. 3. Internet: Homepage of Stratus Computer Inc.: <http://www.stratus.com>. 4. Котух В.Г., Мирошник М.А. Разработка методов повышения отказоустойчивости и надежности функционирования компонентов телекоммуникационных систем и сетей // Радиотехника. – 2011. – Вып. 164.- С.190 – 197. 5. Бережная М.А. Методы проектирования нечетких устройств принятия решений на основе программируемых логических интегральных микросхемах // Технология приборостроения. – 2009. – №2 – С. 92-97. 6. Феррари Д. Оценка производительности вычислительных систем. – М. : Мир, 1981. – 576 с. 7. Сигнаевский В.А., Коган Я.А. Методы оценки быстродействия вычислительных систем. – М. : Наука, 1991. – 256 с., 8. Богуславский Л.Б., Ляхов А.И. Методы оценки производительности многопроцессорных вычислительных систем. – М. : Наука, 1992. – 213 с. 9. Hennessy J., Patterson D. Computer Architecture: A Quantitative Approach. – Morgan Kaufmann Publishers Inc., 1996. 10. Ignatushchenko V.V. A principle of dynamic control of parallel computing processes on the basis of static forecasting // Proc. of the 10-th Int. Conf. on Parallel and Distributed Computing Systems (PDCS-97). – New Orleans, USA. – Oct. 1997. – P. 593–597. 11. Смелянский Р.Л. Модель функционирования распределенных вычислительных систем // Вестник МГУ. Сер. 15. Вычисл. матем. и киберн. – 1990. – № 3. – С. 3-21. 12. Смелянский Р.Л. Об инварианте поведения программ // Вестник МГУ. Сер. 15. Вычисл. матем. и киберн. – 1990. – № 4. – С. 54-60. 13. Калиниченко Д.В., Капитанова А.П., Ющенко Н.В. Методы и средства прогнозирования времени выполнения последовательных программ // Методы математического моделирования. – М. : МГУ, 1997. – №2. – С. 23-27. 14. Барский А.Б. Параллельные процессы в вычислительных системах. Планирование и организация. – М. : Радио и связь, 1990. – 256 с. 15. Игнатущенко В.В. Надежность и отказоустойчивость: аналогии, различия, эффекты // Открытые системы. – 1998. – № 4-5. – С. 13-17. 16. Игнатущенко В.В., Клушин Ю.С. Прогнозирование выполнения сложных программных комплексов на параллельных компьютерах: прямое стохастическое моделирование // Автоматика и телемеханика. – 1994. – № 11. – С. 142-157. 17. Игнатущенко В.В., Подшивалова И.Ю. Динамическое управление параллельными вычислительными процессами на основе статического прогнозирования их выполнения // Автоматика и телемеханика. – 1997. – № 5. – С. 160-173. 18. Игнатущенко В.В., Подшивалова И.Ю. Динамическое управление надежным выполнением параллельных вычислительных процессов для систем реального времени // Автоматика и телемеханика. – 1999. – № 6. – С.142-157. 19. Adve V.S. and Vernon M.K. A Deterministic Model for Parallel Program Performance Evaluation // 1993. <http://www.cs.rice.edu/adve/publications.html>. 20. Ястребенецкий М.А., Васильченко В.М. и др. Безопасность атомных станций. Информационные и управляющие системы / под ред. М.А. Ястребенецкого. – К. : Техніка, 2004. – 472 с. 21. Елисеев В.В. Оценка характеристик ЛВС нижнего уровня ИВС энергоблока ВВЭР-1000 // Радиотехника и информатика. – 2004. – № 4. – С. 88-93.

Харьковский национальный
университет радиотехники,
Украинская государственная академия
железнодорожного транспорта

Поступила в редколлегию 25.08.2011

СИНТЕЗ И АНАЛИЗ КРИПТОГРАФИЧЕСКИХ СИСТЕМ

УДК 621.391:519.2:519.7

Стандартизация алгоритмов шифрования. Требования к проекту национального стандарта блочного симметричного шифрования на современном этапе развития криптографии / И.Д. Горбенко, И.В. Лисицкая // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2011. – Вып. 166. – С. 5 – 10.

Излагается оценка результатов прошедшего украинского конкурса по выбору национального стандарта БСШ и уроки, вынесенные из участия в конкурсе специалистами кафедры БИТ ХНУРЕ. Обсуждаются полезные результаты пройденного пути. Отмечается необходимость продолжения работы по углубленному изучению опыта и достижений современной криптографии и поиска своего вклада в теорию и практику блочного симметричного шифрования, дальнейшего осмысления обширного набора требований к национальному стандарту и поиску путей эффективного их выполнения. Приводятся требования к современным блочным шифрам и одно из предложений по их дальнейшему улучшению.

Библиогр.: 11 назв.

УДК 621.391:519.2:519.7

Стандартизація алгоритмів шифрування. Вимоги до проекту національного стандарту блочного симетричного шифрування на сучасному етапі розвитку криптографії / І.Д. Горбенко, І.В. Лисицька // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2011. – Вип. 166. – С. 5 – 10.

Викладається оцінка результатів минулого українського конкурсу з вибору національного стандарту БСШ та уроки, винесені з участі в конкурсі фахівцями кафедри БИТ ХНУРЕ. Обговорюються корисні результати пройденого шляху. Відзначається необхідність продовження роботи з поглибленого вивчення досвіду і досягнень сучасної криптографії та пошуку свого внеску в теорію і практику блокового симетричного шифрування, подальшого осмислення великого набору вимог до національного стандарту і пошуку шляхів ефективного їх виконання. Наводяться вимоги до сучасних блокових шифрів і одна з пропозицій щодо їх подальшого поліпшення.

Бібліогр.: 11 назв.

UDC 621.391:519.2:519.7

Standardization of cryptographic algorithms. Requirements for the project of a national standard block of a symmetric encryption at the present stage of development of cryptography / I.D. Gorbenko, I.V. Lisitska // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2011. – № 166. – P. 5 -10.

Evaluation results of the Ukrainian competition for the option of a national standard BSSH and lessons learned from participation in the competition department of specialists BIT KNURE are presented. The results of the present day state of art are discussed. The need for continuing work on an in-depth study of the experience and achievements of modern cryptography, and find their contribution to the theory and practice of block symmetric encryption, to further understanding of a broad set of requirements for national standards and finding ways to effectively implement them. The requirements for a modern block ciphers and one of the suggestions for further improvement are given.

Ref.: 11 items.

УДК 621.3.06

Влияние свойств булевых функций S-блока на стойкость современных симметричных блочных шифров / Р.В. Олейников, А.В. Казимиров // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2011. – Вып. 166. – С. 11 – 16.

Приведен обзор криптографических свойств булевых функций и узлов нелинейной замены, используемых в современных симметричных криптографических примитивах. Выполнен анализ S-блоков известных симметричных блочных алгоритмов шифрования, сделаны выводы о влиянии взаимосвязи ряда свойств булевых функций S-блоков на криптографическую стойкость блочных шифров.

Табл. 1. Библиогр.: 17 назв.

УДК 621.3.06

Вплив властивостей булевих функцій на стійкість сучасних симетричних блокових шифрів / Р.В. Олійников, О.В. Казимиров // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2011. – Вип. 166. – С. 11 – 16.

Наведено огляд криптографічних властивостей булевих функцій і вузлів нелінійної заміни, які використовуються у сучасних симетричних криптографічних примітивах. Виконано аналіз S-блоків відомих симетричних блокових алгоритмів шифрування, зроблені висновки про вплив взаємозв'язку ряду властивостей булевих функцій S-блоків на криптографічну стійкість блокових шифрів.

Табл. 1. Бібліогр.: 17 назв.

UDC 621.3.06

Impact of S-box Boolean function properties on the modern symmetric block ciphers strength / R.V. Oliynykov, O.V. Kazymyrov // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2011. – № 166. – P. 11 – 16.

The overview of cryptographic properties of Boolean functions and S-boxes used in modern symmetric cryptographic primitives is given. The analysis of the known symmetric block ciphers S-boxes is carried out, the inferences about the impact of some Boolean functions properties on cryptographic strength of block ciphers are drawn.

1 tab. Ref.: 17 items.

УДК 621.391:519.2:519.7

Об участии S-блоков в формировании максимальных значений линейных вероятностей блочных симметричных шифров / И.В. Лисицкая, В.В. Ковтун // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2011. – Вып. 166. – С. 17 – 25.

Приводятся дополнительные аргументы по обоснованию новой точки зрения к оценке безопасности блочных шифров к атакам дифференциального и линейного криптоанализа, состоящей в том, что максимумы средних вероятностей дифференциалов и линейных корпусов (MADP и MALHP) от свойств используемых в шифрах S-блоков не зависят. Показатели стойкости шифров к этим атакам определяются практически только размером битового входа в шифр. Этот вывод подтверждается результатами экспериментов по определению максимальных значений смещений таблиц линейных аппроксимаций уменьшенных моделей шифра Rijndael, а также шифров, представленных на прошедший украинский конкурс по выбору национального стандарта блочного симметричного шифрования при использовании в них S-блоков с различными значениями показателей нелинейности.

Табл. 6. Библиогр.: 20 назв.

УДК 621.391:519.2:519.7

Про участь S-блоків у формуванні максимальних значень лінійних ймовірностей блокових симетричних шифрів / І. В. Лисицька, В. В. Ковтун // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2011. – Вип. 166. – С. 17 – 25.

Наводяться додаткові аргументи щодо обґрунтування нової точки зору з оцінки безпеки блочних шифрів до атак диференціального та лінійного криптоанализу, що складається в тому, що максимуми середніх ймовірностей диференціалів і лінійних корпусів (MADP і MALHP) від властивостей використовуваних в шифрах S-блоків не залежать. Показники стійкості шифрів до цих атак визначаються практично тільки розміром бітового входу в шифр. Цей висновок підтверджується результатами експериментів з визначення максимальних значень зсувів таблиць лінійних апроксимацій зменшених моделей шифру Rijndael, а також шифрів, представлених на минулий український конкурс з вибору національного стандарту блокового симетричного шифрування при використанні в них S-блоків з різними значеннями показників нелінійності.

Табл. 6. Бібліогр.: 20 назв.

UDC 621.391:519.2:519.7

About participation of S-blocks in formation of the maximum values of linear probabilities of block symmetric code numbers / I.V. Lisitsky, V.V. Kovtun // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. -- 2011. -- № 166. -- P. 17 – 25.

Additional arguments are adduced about substantiation of a new view point on the estimation of a block ciphers numbers security against attacks of differential and linear cryptanalysis consisting in that maxima of mean probabilities of differentials and linear cases (MADP and MALHP) don't depend on the properties of S-blocks used in the code numbers. Indicators of the code numbers stability to these attacks are defined practically only by the size of a bit input in the ciphers. This conclusion is proved by the results of experiments on definition of the maximum values of displacement of Rijndael cipher reduced models linear approximations tables, and also the ciphers presented to the past Ukrainian competition for the choice of the national standard of block symmetric enciphering with the use in them of S-blocks with various values of nonlinearity indicators.

Ref.: 11 items.

Каскадное универсальное хеширование по рациональным функциям алгебраических кривых / Г.З. Халимов // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2011. – Вып. 166. – С. 26-31.

Представлено решение задачи построения каскадного универсального хеширования на основе произведения функциональных полей алгебраических кривых. Рассмотрены свойства двухкаскадного хеширования по функциональным полям кривой Эрмита, Ферма вида $x^{(q-1)/3} + y^{(q-1)/3} + 1 = 0$ с большим числом точек и проективной прямой. Получены оценки вероятности коллизии, сложности вычислений и ключевого пространства для многокаскадного хеширования. Каскадное хеширование эффективно увеличивает размер хешируемых данных и выравнивает вероятность коллизии с изменением длины данных. Применение многокаскадного универсального хеширования $l - Ch_t(M)$ с одной и той же функцией хеширования на всех каскадах в $\sqrt[k]{k}$ раз уменьшает вероятность коллизии.

Табл. 1. Библиогр.: 6 назв.

УДК 681.3.06

Каскадне універсальне гешування по раціональним функціям алгебраїчних кривих / Г.З. Халімов // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2011. – Вип. 166. – С. 26 – 31.

Представлено рішення задачі побудови каскадного універсального гешування на основі добутку функціональних полів алгебраїчних кривих. Розглянуто властивості двохкаскадного гешування за функціональними полями кривої Ерміта, Ферма $x^{(q-1)/3} + y^{(q-1)/3} + 1 = 0$ з великим числом точок і проективної прямої. Отримано оцінки ймовірності колізії, складності обчислень і ключового простору для багатокаскадного гешування. Каскадне гешування ефективно збільшує розмір гешуємих даних і вирівнює ймовірність колізії зі зміною довжини даних. Застосування багатокаскадного універсального гешування $l - Ch_t(M)$ з однією і тією ж функцією гешування на всіх каскадах в $\sqrt[k]{k}$ разів зменшує ймовірність колізії.

Табл. 1. Бібліогр.: 6 назви.

UDC 681.3.06

Cascade universal hashing of rational functions algebraic curves / G.Z. Khalimov // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2011. – № 166. – P. 26 – 31.

The solution of the problem of constructing the cascade universal hashing based on the product function fields of algebraic curves is presented. The properties are considered of two cascade hashing over the Hermite curve functional fields, Ferma curve of the type $x^{(q-1)/3} + y^{(q-1)/3} + 1 = 0$ with a large number of points and the projective line. The estimates of collisions probability, the computational complexity and key space for multistage hashing are obtained. Cascade hashing e increases ffectively the size of data and aligns the probability of collisions with a change in the length of the data. Application of multistage universal hashing $l - Ch_t(M)$ with the same hash function at all stages in $\sqrt[k]{k}$ time reduces the probability of collisions.

1 tab. Ref.: 6 items.

УДК 681.3.06

Схема хамелеон-подписи на основе ДСТУ 4145-2002 / К.А. Погребняк, Ю.М. Ленишина // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2011. – Вып. 166. – С. 31-39.

Предлагается усовершенствование национального стандарта электронной цифровой подписи ДСТУ 4145-2002, за счет внедрения хеш-функции специального вида – хеш-хамелеона. Новая схема обеспечивает свойства непередаваемости электронной цифровой подписи и скрытости сообщения. Детально описываются алгоритмы формирования и проверки хамелеон-подписи, а также развернутые протоколы опровержения поддельной подписи. Приводятся результаты экспериментальных исследований предложенной схемы по критерию сложности вычислений.

Табл. 4. Ил. 3. Библиогр.: 9 назв.

УДК 681.3.06

Схема хамелеон-підпису на основі ДСТУ 4145-2002 / К.А. Погребняк, Ю.М. Ленишина // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2011. – Вип. 166. – С. 31 – 39.

Пропонується вдосконалення національного стандарту електронного цифрового підпису ДСТУ 4145-2002, за рахунок впровадження геш-функції спеціального виду – геш-хамелеону. Нова схема забезпечує властивості непередаваності електронного цифрового підпису та прихованості повідомлен-

ня. Детально описані алгоритми формування та перевірки хамелеон-підпису, а також розгорнуті протоколи спростування підробленого підпису. Наводяться результати експериментальних досліджень запропонованої схеми за критерієм складності обчислень.

Табл. 4. Іл. 3. Бібліогр.: 9 назв.

UDC 681.3.06

Chameleon-signature scheme based on DSTU 4145-2002 standard / K.A. Pogrebnyak, I.M. Lyenshyna // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2011. – № 166. – P. 31 – 39.

Improvement of DSTU 4145-2002 national standard for digital signature by implementation of hash function of a special form – the chameleon hash are proposed. The new scheme provides such properties as non-transferability of digital signature and message hiding. Algorithms of creation and verification of chameleon-signature as well as extended denial protocols are described in detail. The experimental studies results of the proposed scheme on the criterion of computational complexity are provided.

4 tab. 3 fig. Ref.: 9 items.

УДК 681.3.06

Анализ возможностей уменьшения вычислительной сложности ЭЦП DSTU 4145-2002 при использовании нормального базиса / О.А. Мельникова, О.Н. Товма // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2011. – Вып. 166. – С. 40 – 43.

Анализируются характеристики известных алгоритмов вычисления инверсии элементов поля $GF(2^m)$ при использовании нормального базиса. Приведено сравнение теоретических и экспериментальных оценок вычислительной сложности лучших вариантов алгоритмов с соответствующими оценками алгоритма, рекомендованного DSTU 4145-2002 и IEEE P 1363. Сформулированы рекомендации по выбору лучших вариантов для программной реализации с привязкой к параметрам, рекомендованным DSTU 4145-2002.

Табл. 2. Ил. 1. Библиогр.: 7 назв.

УДК 681.3.06

Аналіз можливостей зменшення обчислювальної складності ЕЦП DSTU 4145-2002 за умов використання нормального базису / О.А. Мельникова, О.М. Товма // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2011. – Вип. 166. – С. 40 – 43.

Аналізуються характеристики відомих алгоритмів обчислення інверсії елементів поля $GF(2^m)$ за умов використання нормального базису. Приведено порівняння теоретичних та експериментальних оцінок обчислювальної складності найкращих варіантів алгоритмів із відповідними оцінками алгоритму, який рекомендовано DSTU 4145-2002 та IEEE P 1363. Сформульовані рекомендації по вибору найкращих варіантів для програмної реалізації з прив'язкою до параметрів, рекомендованих DSTU 4145-2002.

Табл. 2. Іл. 1. Бібліогр.: 7 назв.

UDC 681.3.06

Analysis of the possibilities to decrease the computational complexity of electronic signature DSTU 4145-2002 when using a normal basis / O.A. Melnikova, O.N. Tovma // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2011. – № 166. – P. 40 – 43.

Characteristics of the known inversion algorithms in $GF(2^m)$ in case of normal basis use are analyzed. Theoretical and experimental estimations of the best algorithms' computational complexity are compared with the proper estimations of the algorithm, recommended by DSTU 4145-2002 and IEEE P 1363 standards. Recommendations for choosing the best variants of inversion algorithms for program implementation considering the parameters of DSTU 4145-2002 are given.

2 tab. 1 fig. Ref.: 7 items.

УДК 681.3.06

Многокаскадное универсальное хеширование по рациональным функциям максимальной кривой третьего рода / А.Г. Корченко, Е.В. Котух, А.А. Бойко // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2011. – Вып. 166. – С. 44 – 49.

Представлено многокаскадное универсальное хеширование по кривой Сузуки над конечным полем. Получены оценки универсального хеширования, сложности вычисления хеш кода для двухкаскадного хеширования и многокаскадного хеширования в схеме, когда во внутреннем каскаде используется хеширование по проективной прямой.

Табл. 2. Библиогр.: 5 назв.

УДК 681.3.06

Багатокаскадне універсальне ґешування по раціональним функціям максимальної кривої третього роду / *А.Г. Корченко, Е.В. Котух, А.А. Бойко* // Радіотехніка. Всеукр. міжвід. наук.-техн. зб. – 2011. – Вип. 166. С. 44 – 49.

Представлено багатокаскадне універсальне ґешування по кривій Сузукі над кінцевим полем. Отримано оцінки універсального ґешування, складності обчислення хеш коду для двокаскадного хешування і многокаскадного ґешування в схемі, коли у внутрішньому каскаді використовується ґешування по проективній прямій.

Табл. 2. Бібліогр.: 5 назви.

UDC 681.3.06

Multistage universal hashing of rational functions maximal curve of the third genus / *A.G. Korchenko, E.V. Kotukh, A.A. Boiko* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2011. – № 166. – P. 44 – 49.

Multistage universal hashing by Suzuki curve over a finite field is presented. Estimates were obtained for universal hashing, complexity of computing a hash code for two-stage hashing and hash in a multistage scheme, when used in an internal cascade hashing on the projective line.

2 tab. Ref.: 5 items.

УДК 621.391:519.2:519.7

Большие шифры – случайные подстановки / *И.В. Лисицкая, А.А. Настенко* // Радіотехніка : Всеукр. міжвед. науч.-техн. сб. – 2011. – Вып. 166. – С. 50 – 55.

Приводится обоснование подхода к оценке дифференциальных и линейных свойств современных шифров и его применение для анализа случайных показателей шифров Rijndael и ГОСТ с целью подтверждения концепции о подчинении свойств современных шифров свойствам случайных подстановок.

Табл. 6. Библиогр.: 11 назв.

УДК 621.391:519.2:519.7

Великі шифри – випадкові підстановки / *І.В. Лисицька, А.А. Настенко* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2011. – Вип. 166. – С. 50 – 55.

Наводиться обґрунтування поїдходу до оцінки диференціальних та лінійних властивостей сучасних шифрів та його застосування до аналізу показників випадковості шифрів Rijndael та ГОСТ з метою підтвердження концепції про підпорядкування властивостей сучасних шифрів властивостям випадкових підстановок.

Табл. 6. Бібліогр.: 11 назв.

UDC 621.391:519.2:519.7

Great ciphers – casual substitution / *I.V. Lisitskaya, A.A. Nastenka* // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2011. – № 166. – P. 50 – 55.

The substantiation of the approach to an estimation of differential and linear properties of modern block ciphers is given. This approach is applied to the analysis of Rijndael and GOST block ciphers randomness indicators with the aim to accept the concept on submission of modern block ciphers to random substitutions properties.

6 tab. Ref.: 11 items.

УДК 681.3.06

Обоснование и выбор критериев и показателей оценки комбинированных ИОК / *И.Д. Горбенко, П.А. Кравченко, Л.В. Макутонина* // Радіотехніка : Всеукр. міжвед. науч.-техн. сб. – 2011. – Вып. 166. – С. 56 – 63.

Проводится анализ существующих комбинированных инфраструктур открытых ключей, предлагаются критерии их оценки, проводится сравнение рассмотренных схем по выдвинутым критериям.

Табл. 1. Ил. 1. Библиогр.: 5 назв.

УДК 681.3.06

Обґрунтування та вибір критеріїв та показників оцінки комбінованих ІВК / *І.Д. Горбенко, П.О. Кравченко, Л.В. Макутоніна* // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2011. – Вип. 166. – С. 56 – 63.

Проводиться аналіз існуючих комбінованих інфраструктур відкритих ключів, пропонуються критерії їх оцінки, проводиться порівняння наведених схем за цими критеріями.

Табл. 1. Ил. 1. Библиогр.: 3 назви.

UDC 681.3.06

Justification and selection of criteria and indicators for estimating the combined PKI / I.D. Gorbenko, P.O.Kravchenko, L.V. Makutonina // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2011. – № 166. – P. 56 – 63.

The analysis of existing combined public key infrastructures is carried out, criteria for their evaluation are offered, a comparison of the considered schemes is performed by these criterias.

1 tab. 1 fig. Ref.: 3 items.

УДК 621.3.06

Анализ требований к генераторам случайных и псевдослучайных последовательностей установленных в стандартах AIS 20 и AIS 31 / Ю.И. Горбенко, Д.Э. Хряпин, В.И. Бондаренко // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2011. – Вып. 166. – С.64 – 69.

Приведен сравнительный анализ требований к генераторам случайных и псевдослучайных последовательностей, которые установлены в стандартах AIS 20 и AIS 31. Проанализированы требования к разным функциональным классам ДГСР, и определена иерархическая зависимость между ними. Статья содержит классификацию некоторых существующих схем генерации псевдослучайных последовательностей согласно с требованиями AIS 20. Рассмотрены требования к физическим генераторам случайных последовательностей, которые описаны в AIS 31.

Табл. 2. Библиогр.: 6 назв.

УДК 621.3.06

Аналіз вимог до генераторів випадкових і псевдовипадкових послідовностей встановлених в стандартах AIS 20 та AIS 31 / В.І. Бондаренко, Ю.І. Горбенко, Д.Е. Хряпін // Радіотехніка : Всеукр. міжвід. наук.-техн. сб. – 2011. – Вип. 166. – С.64 – 69.

Наведено порівняльний аналіз вимог до генераторів випадкових і псевдовипадкових послідовностей, що встановлено в стандартах AIS 20 та AIS 31. Проаналізовано вимоги до різних функціональних класів ДГВР, та встановлено ієрархичну залежність між ними. Стаття містить класифікацію деяких існуючих схем генерації псевдовипадкових послідовностей згідно до вимог AIS 20. Розглянуто вимоги до фізичних генераторів випадкових послідовностей, які описані в AIS 31.

Табл. 2. Библиогр.: 6 назв.

UDC 621.3.06

Analysis of requirements on random and pseudorandom number generators in the AIS 20 and AIS 31 standards / V.I. Bondarenko, U.I. Gorbenko, D.E. Khriapin // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2011. – №166. – P.64 – 69.

A comparative analysis of the requirements on generators of random and pseudorandom sequences that are installed in the AIS 20 and AIS 31 standards is presented. Authors analyzed the requirements on different functional classes DRNG are analyzed and hierarchical relationships between them are defined. A classification of some existing schemes pseudo-random number generators according to the AIS 20 is given. The requirements for physical random number generators described in AIS 31 are examined.

2 tab. Ref.: 6 items.

УДК 681.3.07

Актуальность атаки на связанных ключах для аппаратных реализаций средств КЗИ / А.А. Шевчук // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2011. – Вып. 166. – С. 70 – 75.

Рассматривается фундаментальная уязвимость аппаратных реализаций ЭЦП для атаки на связанных ключах в условиях недоверия разработчику. Приводится краткий обзор в мировой практике успешного выполнения подобных атак. Описывается метод проведения атаки.

Ил. 4. Библиогр.: 6 назв.

УДК 681.3.07

Актуальність атаки на зв'язаних ключах для апаратних реалізацій засобів КЗІ / О.А. Шевчук // Радіотехніка : Всеукр. міжвід. наук.-техн. сб. – 2011. – Вип. 166. – С. 70 – 75.

Наведено дослідження щодо фундаментальних вразливостей апаратних реалізацій ЕЦП для атаки на зв'язаних ключах, в умовах недовіри розробнику. Наводиться світовий досвід успішного використання цих атак. Описується метод виконання атаки.

Ил. 4. Библиогр.: 6 назв.

Urgency of attack on the related keys for hardware realizations of DSS / A.A. Shevchuk // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2011. – № 166. – P. 70 – 75.

Fundamental vulnerability of hardware realizations DSS for attack to the related keys in the conditions of mistrust to the developer is considered. The short review in world practice of successful performance of similar attacks is given. The method of carrying out an attack is described.

4 fig. Ref.: 6 items.

МЕТОДЫ, МЕХАНИЗМЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

УДК 004.056.5

Положение по обработке и защите персональных данных ХНУРЭ / М.Ф. Бондаренко, Н.С. Лесная, А.А. Ткач, В.Н. Караваев, А.И. Шумов // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2011. – Вып. 166. – С. 76 – 83.

В соответствии с Законом Украины "О защите персональных данных" разработано "Положение по обработке и защите персональных данных в ХНУРЭ", которое регулирует деятельность Университета по вопросам обработки и защите персональных данных в информационных (автоматизированных) системах и в картотеках персональных данных. Положение определяет субъектов отношений, связанных с персональными данными в Университете, понятия, состав, порядок доступа, общие правила, принципы обработки и обеспечения безопасности персональных данных, права и обязанности субъектов персональных данных и Университета, а также общий порядок организации их защиты в Университете.

Библиогр.: 13

УДК 004.056.5

Положення про обробку та захист персональних даних ХНУРЕ / М.Ф. Бондаренко, Н.С. Лесна, О.О. Ткач, В.М. Караваєв, О.І. Шумов // Радіотехніка : Всеукр. міжвід. наук.-техн. сб. – 2011. – Вип. 166. – С. 76 – 83.

Відповідно до Закону України "Про захист персональних даних" розроблено "Положення про обробку та захист персональних даних в ХНУРЕ", яке регулює діяльність Університету з питань обробки та захисту персональних даних в інформаційних (автоматизованих) системах та в картотеках персональних даних. Положення визначає суб'єктів відносин, пов'язаних із персональними даними в Університеті, поняття, склад, порядок доступу, загальні правила, принципи обробки та забезпечення безпеки персональних даних, права та обов'язки суб'єктів персональних даних та Університету, а також загальний порядок організації їх захисту в Університеті.

Бібліогр.: 13

UDC 004.056.5

Regulations of the KNURE personal data processing and protection / M.F. Bondarenko, N.S. Lesna, O.O. Tkach, V.M. Karavaev, O.I. Shumov // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2011. – № 166. – P. 76 – 83.

According to the Law of Ukraine "On the personal data protection" "Regulations of the KNURE personal data processing and protection" is developed, it regulates the University activities for processing and protection of personal data in information (automated) systems and in card indexes of personal data. Regulations determine the subjects of relations associated with the personal data in the University, concepts, structure, access procedures, general rules, processing and securing principles of personal data, rights and duties of personal data subjects and the University, as well as the general order of their protection organization at the University.

Ref.: 13 items.

УДК 343.982.3, 004.89

Анализ биометрических систем аутентификации и идентификации с использованием гибридных интеллектуальных методов для защиты от не санкционированного доступа / П.А. Филоненко, Е.А. Винокурова // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2011. – Вып. 166. – С. 84 – 93.

Изложены результаты анализа схем биометрической аутентификации и идентификации личности, предложенных стандартами зарубежных стран, и актуальность применения их в Украине. Рассмотренные биометрические схемы дают возможность выбрать из множества методов более подходящий под конкретный вид защиты от НСД. При этом условия такие схемы становятся более гибкими и устойчивыми от атак злоумышленника. Направление биометрической криптографии актуально

для дальнейшего изучения и внедрения в сфере информационной безопасности.

Табл. Ил.: 7. Библиогр.: 10 назв.

УДК 343.982.3

Аналіз біометричних систем автентифікації та ідентифікації з використанням гібридних інтелектуальних методів для захисту від несанкціонованого доступу / П.О. Філоненко, О.А. Вінокурова // Радіотехніка : Всеукр. міжвід. наук.-техн. сб. – 2011. – Вип. 166. – С.84 – 93.

Викладено результати аналізу схем біометричної аутентифікації та ідентифікації особистості, запропонованих стандартами зарубіжних країн і актуальність застосування їх в Україні. Розглянуті біометричні схеми дають можливість вибрати з безлічі методів такі, які більш підходять під конкретний вид захисту від НСД. За цієї умови такі схеми стають більш гнучкими і стійкими від атак злоумисника. Таким чином напрямок біометричної криптографії є актуальним для подальшого вивчення і впровадження в сфері інформаційної безпеки.

Табл. 2. Іл. 7. Бібліогр.: 10 назв.

UDC 343.982.3, 004.89

Analysis of biometric systems for authentication and identification using hybrid intellectual methods to protect unauthorized access / P.A. Filonenko, E.A. Vynokurova // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2011. – № 166. – P. 84– 93.

The results of the schemes analysis for personal biometric authentication and identification, proposed by foreign countries' standards and the relevance of their application in Ukraine are presented. The considered biometric schemes give the opportunity to choose out of a variety of methods more appropriate for a specific kind of protection unauthorized access. At this rate such schemes have become more flexible and resistant to malicious attacks. Thus the direction of biometric cryptography is relevant to further study and implementation of information security.

2 tab. 7 fig. Ref.: 10 items.

УДК 004.056

Методы анализа процессов контроля качества программного обеспечения используемые при проектировании и разработке систем обработки криптографической информации / Д.А. Семченко, А. А. Замула // Радіотехніка : Всеукр. міжвід. науч.-техн. сб. – 2011. – Вып.166. – С.94 – 98.

Рассмотрены основные методы анализа программного обеспечения, которые позволяют достичь структурированной и систематической оценки при проведении тестирования в соответствии с требованиями, выдвигаемыми к системе. Затраты на проведение тестирования оцениваются от 25 до 50% денежных средств потраченных на разработку программного обеспечения. Поэтому актуальной является разработка новых и усовершенствование существующих методов анализа обеспечения контроля качества программного обеспечения.

Ил 3. Библиогр.: 11 назв.

УДК 004.056

Методи аналізу процесів контролю якості програмного забезпечення, що використовуються при проектуванні та розробки систем обробки криптографічної інформації / Д.О. Семченко, О. А. Замула // Радіотехніка : Всеукр. міжвід. наук.-техн. сб. – 2011. – Вип. 166. – С. 94 – 98.

Розглянуто основні методи аналізу програмного забезпечення, які дозволяють досягти структурованої та систематичної оцінки при проведенні тестування відповідно до вимог, що висуваються до системи. Витрати на проведення тестування оцінюються від 25 до 50% грошових коштів, витрачених на розробку програмного забезпечення. Актуальною є розробка нових і вдосконалення існуючих методів аналізу забезпечення контролю якості програмного забезпечення.

Іл 3, Бібліогр.: 11 назви

UDC 004.056

Methods for analysis of quality control processes used in software design and development of systems for handling cryptographic information / D.A. Semchenko, A. A. Zamula // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2011. – № 166. – P. 94 – 98.

The basic methods that help to achieve structured and systematic evaluation and testing is offered. Evaluation and testing procedures have a high cost in practice – expenditures in this sector are estimated with 25 % up to 50 % of the software development time and costs, therefore is development of new and improvement existing analysis techniques for ensuring quality control software is actual.

3 fig. Ref.: 11 items.

УДК 621.34

Структурно-информационные портреты информационной системы в условиях неопределенности на примере Dos-атаки / С.Г. Семенов // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2011. – Вып.166. – С.99 – 106.

Предложен подход к моделированию информационной системы в условиях априорной неопределенности. Построены расширенный фазовый и наблюдаемые структурно-информационные портреты информационной системы в условиях воздействия Dos-атаки. Проведен сравнительный анализ полученных портретов и выявлены структурные особенности поведения исследуемой системы. Построены проекции наблюдаемых структурно-информационных портретов на плоскости. Осуществлен выбор и оценка информативных переменных (характеристик) наиболее полно описывающих состояние системы.

Табл. 1. Ил. 3. Библиогр.: 8 назв.

УДК 621.34

Структурно-інформаційні портрети інформаційної системи в умовах невизначеності на прикладі Dos-атаки / С.Г. Семенов // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2011. – Вип.166. – С.99 – 106.

Пропонується підхід щодо моделювання інформаційної системи в умовах априорної невизначеності. Побудовані розширений фазовий і спостережувані структурно-інформаційні портрети інформаційної системи в умовах дії Dos-атаки. Проведений порівняльний аналіз одержаних портретів і виявлені структурні особливості поведінки досліджуваної системи. Побудовані проекції спостережуваних структурно-інформаційних портретів на площині. Здійснений вибір і оцінка інформативних змінних (характеристик) що якнайповніше описують стан системи.

Табл. 1. Ил. 3. Библиогр.: 8 назв.

UDC 621.34

Structurally-informative portraits of the informative system in conditions of vagueness by the example of Dos-attack / S. Semenov // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2011. – №166. – P. 99 – 106.

An approach is offered to the design of the informative system in conditions of a priori vagueness. The extended phase and the looked after structurally-informative portraits of the informative system in the conditions of influence of Dos-attack are built. The comparative analysis of the got portraits is conducted and the structural features of behavior of the explored system are revealed. The projections of the observed structurally-informative portraits are built on a plane. The choice and estimation of informing variables (descriptions) is carried out, describing most completely the state of the system.

1 tab. 3 fig. Ref.: 8 items.

УДК 681.322

Оценка эффективности динамических алгоритмических преобразователей / Е.Е. Малафеев, Е.Е. Малафеев // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2011. – Вып.166. – С. 107 – 111.

Рассмотрены принципы построения динамических алгоритмических преобразователей и способы их настройки. Для оценки эффективности динамических алгоритмических преобразователей предлагается использовать количество модификаций алгоритма, реализуемых запутанным алгоритмом. Показано, что операторный состав влияет на характеристики запутанного алгоритма. Предложена процедура выбора операторного состава, реализующего наибольшее количество модификаций заданного алгоритма.

Табл. 6. Ил. 1. Библиогр.: 11 назв.

УДК 681.322

Оцінка ефективності динамічних алгоритмічних перетворювачів / Є.Є. Малафєєв, Є.Є. Малафєєв // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2011. – Вип.166. – С. 107 – 111.

Розглянуто принципи побудови динамічних алгоритмічних перетворювачів і способи їх налаштування. Для оцінки ефективності динамічних алгоритмічних перетворювачів пропонується використовувати кількість модифікацій алгоритму, що реалізуються заплутаним алгоритмом. Показано, що операторний склад впливає на характеристики заплутаного алгоритму. Запропоновано процедуру вибору операторного складу, що реалізує найбільшу кількість модифікацій заданого алгоритму.

Табл. 6. Ил. 1. Библиогр.: 11 найм.

UDC 681.322

Estimation of dynamic algorithmic converters efficiency / Ye.Ye. Malafeev, Ye.Ye. Malafeev // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2011. – № 166. – P. 107 – 111

Principles of dynamic algorithmic converters construction and ways of their adjustment are considered. It is offered to use quantity of the algorithm modification sold by obfuscated algorithm for an estimation of dynamic algorithmic converters efficiency. It is shown, that the operational structure influences characteristics of the obfuscated algorithm. Procedure of a choice of the operational structure realizing the greatest quantity of the algorithm modification is offered.

6 tab. 1 Fig. 1. Ref.: 11 items.

УДК 621.39:65.012.8

Обоснование плана защиты объектов от конкурентной разведки / В.И. Заболотный, А.А. Абузова, Б.В. Волобуев // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2011. – Вып.166. – С. 112 – 116.

Рассмотрены пути обоснования плана защиты информации о материальных объектах в условиях ведения конкурентной разведки и её составляющей – технической разведки. Предложен алгоритм определения характеристик и их значений, подлежащих защите, путём дезинформации и сокрытия. Математический аппарат алгоритма – моменты и регрессионный анализ случайных величин.

Табл. 2. Библиогр.: 8 назв.

УДК 621.39:65.012.8

Обґрунтування плану захисту об'єктів від конкурентної розвідки / В.І. Заболотний, А.А. Абузова, Б.В. Волобуєв // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2011. – Вып. 166. – С.112 – 116.

Розглянуті шляхи обґрунтування плану захисту інформації про матеріальні об'єкти в умовах ведення конкурентної розвідки та її складової – технічної розвідки. Запропоновано алгоритм визначення характеристик, та їх значень, що підлягають захисту шляхом дезинформації та приховування. Математичний апарат алгоритму – моменти та регресійний аналіз випадкових величин.

Табл. 2. Бібліогр.: 8 назв.

UDC 621.39:65.012.8

Justification of the plan for the objects protection against of a competitive intelligence / V.I. Zabolotnyi, A.A. Abuzova, B.V. Volobuiev // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2011. – № 166. – P. 112 – 116.

The ways to justify the plan for protection of the information about the material objects in terms of competitive intelligence and its component – technical intelligence are considered. An algorithm for determining the characteristics and values to be protected by deception and concealment is offered.

2 tab. Ref.: 8 items.

УДК 681.142:681.3

Методы контроля и диагностики данных в классе вычетов / С. А. Мороз, В.А. Краснобаев, А.А. Замула // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2011. – Вып. 166. – С. 117 – 124.

Предложены метод контроля и метод диагностики информации, представленной в КВ, которые основаны на использовании ортогональных базисов для полной системы оснований $\{m_i\}$ КВ, а также совокупности проекций $A_i = (a_1, a_2, \dots, a_{i-1}, a_{i+1}, \dots, a_n, a_{n-1})$ числа A по модулю m_i . Приведен конкретный пример контроля и диагностики данных в КВ для КСПОЦИ с однобайтовой разрядной сеткой. Использование предложенных методов позволяет упростит техническую процедуру контроля и диагностики данных, представленных в КВ, а также повысить оперативность проведения этой процедуры.

Табл. 5. Библиогр.: 2 назв.

УДК 681.142:681.3

Методи контролю та діагностики даних у класі лишків / С.А. Мороз, В.А. Краснобаєв, А.А. Замула // Радіотехніка : Всеукр. межвед. науч.-техн. сб. – 2011. – Вып. 166. – С. 117 – 124.

Запропоновано метод контролю і метод діагностування інформації, яка представлена у класі лишків. Ці методи базуються на використанні ортогональних базисів для повної системи основ $\{m_i\}$ КЛ, а також на сукупності проекцій $A_i = (a_1, a_2, \dots, a_{i-1}, a_{i+1}, \dots, a_n, a_{n-1})$ числа A по модулю m_i . Приведено конкретний приклад контролю і діагностування даних в КЛ для КЗПОЦИ з однобайтовою розрядною мережею. Використання запропонованих методів дозволяє спростити технічну процедуру контролю і діагностування даних, які представлені у КЛ, підвищити оперативність проведення даної процедури.

Табл. 5. Бібліогр.: 2 назв.

UDC 681.142:681.3

Methods of data monitoring and diagnosis in residue classes / S. Moroz, V. Krasnobaev, A. Zamula // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2011. – №166. – P. 117 – 124.

Methods of data monitoring and diagnosis in residue classes are presented. These methods are founded on the orthonormal basis usage for the complete basis $\{m_i\}$ of residue classes and for the complex projection $A_i = (a_1, a_2, \dots, a_{i-1}, a_{i+1}, \dots, a_n, a_{n+1})$ of number A modulo m_i . Particular example of data monitoring and diagnosis in residue classes for CMTPDI with one-byte bit grid is shown. The usage of the proposed methods allows to simplify the technical procedure of data monitoring and diagnosis in residue classes and to enhance the efficiency of processing.

Tab. 5. Ref.: 2 items.

СИНТЕЗ И АНАЛИЗ СИГНАЛОВ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

УДК 621.391.1

Методы построения и исследования свойств производных нелинейных рекуррентных последовательностей / И.Д. Горбенко, А.А. Замула, Р. И. Киянчук // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2011. – Вып. №166. – С. 125 – 133.

Получены аналитические выражения для оценки характеристик корреляционных функций одного класса дискретных последовательностей, а именно, характеристических дискретных последовательностей и полученных на их основе, так называемых, производных характеристических дискретных последовательностей.

Бібліогр.: 4 назв.

УДК 621.391.1

Методи побудови та дослідження властивостей похідних нелінійних рекуррентних послідовностей / І.Д. Горбенко, О.А. Замула, Р.І. Кіянчук // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2011. – Вип. №166. – С. 125 – 133.

Отримано аналітичні вирази для оцінки характеристик кореляційних функцій одного класу дискретних послідовностей, а саме, характеристичних дискретних послідовностей та отриманих на їх основі, так званих, похідних характеристичних дискретних послідовностей.

Бібліогр.: 4 назви

UDC 621.391.1

Methods for constructing and studying properties of the derivatives of nonlinear recurrence sequences / I.D. Gorbenko Ph.D., A.A. Zamula Cand., R.I. Kiyanchuk // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2011. – № 166. – P. 125 – 133.

The analytical expressions are obtained to characterize the correlation functions of a class of discrete sequences, namely, the characteristic of discrete sequences and obtained from them, the so-called derivatives characteristic of discrete sequences.

Ref.: 4 items.

УДК 621.396

Встраивание данных в контейнеры-изображения с использованием сложных дискретных сигналов / А.А. Кузнецов, А.А. Смирнов // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2011. – Вып. 166. – С. 134 – 141.

Исследуется эффективность стеганографических методов встраивания информации в неподвижные контейнеры-изображения с использованием технологии прямого расширения спектра, исследуются зависимости величины вносимых искажений и вероятности возникающих ошибок при извлечения информационных данных от пропускной способности стеганоканала. Предлагается использование адаптивно формируемых ансамблей слабокоррелированных (квазиортогональных) дискретных сигналов для встраивания информационных данных. Показано, что за счет минимизации коэффициента корреляции формируемых дискретных сигналов и используемых контейнеров удастся существенно снизить вероятность ошибочного извлечения встроенных данных.

Ил. 10. Бібліогр.: 7 назв.

УДК 621.396

Вбудовування даних в контейнери-зображення з використанням складних дискретних сигналів / О.О. Кузнецов, О.А. Смирнов // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2011. – Вип. 166. – С. 134 – 141.

Проводяться дослідження ефективності стеганографічних методів вбудовування інформації в нерухомі контейнери-зображення з використанням технології прямого розширення спектру, досліджуються залежності величини спотворень, що вносяться, і вірогідності виникаючих помилок при вилученні інформаційних даних від пропускної спроможності стеганоканала. Пропонується використання адаптивно формованих ансамблів слабокоррелірованих (квазіортогональних) дискретних сигналів для вбудовування інформаційних даних. Показано, що за рахунок мінімізації коефіцієнта кореляції формованих дискретних сигналів і використовуваних контейнерів вдається істотно понизити вірогідність помилкового вилучення вбудованих даних.

Іл. 10. Бібліогр.: 7 назв.

UDC 621.396

Building of information in containers-images with the use of complex discrete signals / A.A. Kuznetsov, A.A. Smirnov // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2011. – № 166. – P. Radiotekhnika : All-Urk. Sci. Interdep. Mag. – 2011. – N 166. – P. 134 – 141.

Researches of efficiency of steganographic methods of building-in of information are conducted in immobile containers-images with the use of technology of direct spread of spectrum, dependences of size of the brought in distortions and probability of errors are probed at extractions of informative data on the steganographic channel carrying capacity. The use of the adaptive formed bands of discrete signals is offered for building of information. It is shown that due to minimization of coefficient of correlation of the formed discrete signals and in-use containers it becomes possible to reduce substantially the probability of erroneous extraction of built-in data.

10 fig. Ref.: 7 items.

УДК 621.396.253

Дискретные сигналы с многоуровневой функцией корреляции / А.А. Кузнецов, А.А. Смирнов, В.Н. Сай // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2011. – Вып. 166. – С. 142 -152.

Рассматриваются групповые коды и исследуются их структурные свойства с точки зрения разложения множества кодовых слов на непересекающиеся циклические орбиты. Предлагается метод формирования больших ансамблей дискретных сигналов с многоуровневой функцией корреляции. Формирование дискретных сигналов основано на сечении ненулевых циклических орбит группового кода. Показано, что предлагаемый метод обобщает некоторые ранее известные двоичные сигналы (субортогональные последовательности и коды Голда) и позволяет в общем случае синтезировать дискретные последовательности с многоуровневой функцией корреляции.

Ил. 14. Библиогр.: 9 назв.

УДК 621.396.253

Дискретні сигнали з багаторівневою функцією кореляції / О.О. Кузнецов, О.А. Смирнов, В.Н. Сай // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2011. – Вип. 166. – С. 142 -152.

Розглядаються групові коди і досліджуються їх структурні властивості з погляду розкладання безлічі кодових слів на непересічні циклічні орбіти. Пропонується метод формування великих ансамблів дискретних сигналів з багаторівневою функцією кореляції. Формування дискретних сигналів засноване на перетині ненульових циклічних орбіт групового коду. Показано, що запропонований метод узагальнює деякі раніше відомі двійкові сигнали (субортогональні послідовності і коди Голда) і дозволяє в загальному випадку синтезувати дискретні послідовності з багаторівневою функцією кореляції.

Іл. 14. Бібліогр.: 9 назви.

UDC 621.396.253

Discrete signals with a multilevel correlation function / A.A. Kuznetsov, A.A. Smirnov, V.N. Say // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2011. – № 166. – P. 142 -152.

Group codes are considered and their structural properties are investigated in terms of decomposing them into non-overlapping cyclical orbits. A method of forming big ensembles of discrete signals with a multi-level correlation function is suggested. The formation of discrete signals is based on cuts of group code non-zero cyclical orbits. The work shows that the suggested method generalizes some discrete signals known before (suborthogonal sequences and Gold codes) and generally makes it possible to synthesize binary sequences with a multi-level correlation function.

14 fig. Ref.: 9 items.

УДК 343.982.3

Анализ информационных признаков отпечатков пальцев и сканирующих устройств / П.А. Филоненко // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2011. – Вып.166. – С.153 -158.

Приводится анализ актуальной и распространенной биометрической характеристики человека, а именно отпечаток пальца, исследования глобальных и локальных признаков для облегчения понимания и применения в биометрических системах защиты от несанкционированного доступа и систем аутентификации и идентификации пользователя. Развитие и применения биометрической характеристики в международных стандартах и анализ сканирующих устройств отпечатков пальцев.

Табл. 1. Ил. 4. Библиогр.: 5 назв.

УДК 343.982.3

Аналіз інформаційних ознак відбитків пальців і скануючих пристроїв / П.А. Філоненко // Радіотехніка : Всеукр. міжвід. наук.-техн. сб. – 2011. – Вип.166. – С.153 – 158.

Наводиться аналіз актуальною і поширеною біометричною характеристикою людини, а саме відбиток пальця, дослідження глобальних і локальних ознак для полегшення розуміння і застосування в біометричних системах захисту від несанкціонованого доступу та систем автентифікації та ідентифікації користувача. Розвиток і застосування біометричної характеристики в міжнародних стандартах та аналіз скануючих пристроїв відбитків пальців.

Табл. 1. Іл. 4. Бібліогр.: 5 назв

UDC 343.982.3

Analysis of information features and fingerprint scanners / P.A. Filonenko // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2011. – №166. – P.153 -158.

The analysis of current and widespread human biometric fingerprint is given, namely, the study of global and local features to facilitate understanding and application of biometric systems to protect unauthorized access and authentication systems and user identification. The development and application of biometric characteristics in the international standards and analysis of scanning devices fingerprints are described.

1 tab. 4 fig. Ref.: 5 items.

УДК 621.373.072.9

Исследование синхронизированного автогенератора с нелинейной обратной связью / В.В. Рапин // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2011. – Вып. 166. – С. 159– 164.

Предложен автогенератор в режиме синхронизации на основном тоне периодическим полигармоническим сигналом с нелинейной обратной связью, которая обеспечивает не только широкую полосу синхронизации автогенератора, но и исключает влияние гармонических составляющих внешнего сигнала синхронизации на спектр сигнала автогенератора. Получены выражения, представляющие относительную амплитуду второй гармонической составляющей сигнала автогенератора в различных режимах работы. Использование таких автогенераторов в следящих фильтрах позволяет обеспечить широкую полосу захвата и низкий уровень высших гармонических составляющих выходного сигнала.

Ил. 2. Библиогр.: 8 назв.

УДК 621.373.072.9

Дослідження синхронізованого автогенератора з нелінійним зворотнім зв'язком / В. В. Рапін // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2011. – Вип.166. – С. 159– 164.

Запропонований автогенератор в режимі синхронізації на основному тоні періодичним полігармонічним сигналом з нелінійним зворотнім зв'язком, який забезпечує не лише широку смугу синхронізації автогенератора, але і виключає вплив гармонічних складових зовнішнього сигналу синхронізації на спектр сигналу автогенератора. Отримані вирази, що представляють відносну амплітуду другої гармонічної складової сигналу автогенератора в різних режимах роботи. Використання таких автогенераторів в стежачих фільтрах дозволяє забезпечити широку смугу захоплення і низький рівень вищих гармонічних складових вихідного сигналу.

Іл. 2. Бібліогр.: 8 назв.

UDC 621.373.072.9

Investigation of the synchronized oscillator with nonlinear feedback / V.Rapin // Radiotekhnika: All-Ukr. Sci. Interdep. Mag. – 2011. – № 166. – P. 159– 164.

An oscillator in the mode of synchronization on the basic tone by a periodic nonharmonic signal with a nonlinear feedback is presented. This feedback provides not only a wide band of synchronization of the oscillator but also eliminates the external synchronizing signal high harmonics action on the spectrum of the

oscillator signal. The equations describing a relative amplitude of the oscillator signal second harmonic in the different modes are derived. The utilization of such oscillators in tracking filters results in a wide capture band and low level of the high harmonics of the output signal.

Fig.2. Ref.: 8 items.

УДК 621.396.9: 519.684.6: 004.272.26

Обработка радиолокационных сигналов в параллельных вычислительных системах / А.И. Литвин-Попович // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2011. – Вып. 166. – С. 165–172.

Рассмотрена параллельная реализация процедуры параметризации спектров рассеянных сигналов в РЛС вертикального зондирования атмосферы. Применение высокопроизводительной параллельной вычислительной системы позволило повысить точность оценивания при сохранении высокого темпа выдачи результатов. В качестве вычислительных устройств использованы универсальные и графические процессоры.

Ил. 11. Библиогр.: 9 назв.

УДК 621.396.9: 519.684.6: 004.272.26

Обробка радіолокаційних сигналів в паралельних обчислювальних системах / А.І. Литвин-Попович // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2011. – Вип. 166. – С. 165–172.

Розглянуто паралельну реалізацію процедури параметризації спектрів розсіяних сигналів в РЛС вертикального зондування атмосфери. Використання високошвидкісної паралельної обчислювальної системи дозволило підвищити точність оцінювання при збереженні високого темпу видачі результатів. В якості обчислювальних пристроїв використані універсальні та графічні процесори.

Іл. 11. Бібліогр.: 9 назв.

UDC 621.396.9: 519.684.6: 004.272.26

Radar signal processing in parallel computing systems / A.I. Litvin-Popovich // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2011. – № 166. – P. 165–172.

Parallel realization of a backscattered signal spectra parameterization has been considered. Using a high-performance parallel computing system, it has been possible to improve precision of the results obtained by a radar wind profiler, while maintaining a high temporal resolution of the obtained results. As computing devices, both the universal processors (CPUs) and graphical processors (GPUs) were used.

11 fig. Ref.: 9 items.

УДК 621.396

Методы многопозиционной модуляции шумовых сигналов / Р.М. Дидковский, С.С. Гузнин // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2011. – Вып. 166. – С. 173 - 179.

Предложены пять методов многопозиционной модуляции шумовых сигналов, полученных на базе фазовой манипуляции. Методами имитационного вычислительного эксперимента получены оценки потенциальной помехоустойчивости данных методов. Исследовано влияние параметров и структуры сигнала на помехоустойчивость системы. Выполнен сравнительный анализ помехоустойчивости различных методов многопозиционной модуляции. Определены оптимальные схемы модуляции.

Ил. 5. Библиогр.: 8 назв.

УДК 621.396

Методи багатопозиційної модуляції шумових сигналів / Р.М. Дідковський, С.С. Гузнін // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2011. – Вип. 166. – С. 173 - 179.

Запропоновано п'ять методів багатопозиційної модуляції шумових сигналів, отриманих на базі фазової маніпуляції. Методами імітаційного обчислювального експерименту отримано оцінки потенційної завадостійкості даних методів. Досліджено вплив параметрів та структури сигналу на завадостійкість системи. Виконано порівняльний аналіз завадостійкості різних методів багатопозиційної модуляції. Визначено оптимальні схеми модуляції.

Іл. 5. Бібліогр.: 8 назв.

UDC 621.396

Multiple-bits noise signals modulation scheme / R.M. Didkowsky, S.S. Huznin // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2011. – № 166. – P. 173 - 179.

Five methods of multiple-bits noise signals modulation, based on a phase shift keying is offered. Estimation of a bit-error performance is obtained for these methods using computer simulation. Influence of signal parameters and signal structure on the system performance is investigated. A comparative analysis of a bit-

error probability is conducted for different multiple-bits modulation schemes. Optimal modulation schemes are determined.

5. fig. Ref.: 8 items.

УДК 621.396.96

Выбор технологически обоснованного метода оценки состава групповой сосредоточенной цели / В.М. Кичак, Е.С. Ленков, В.М. Лоза // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2011. – Вып. 166. – С.180 - 185.

Анализируются теоретически разработанные методы "сверхрелеевого" разрешения с точки зрения их практической реализуемости в обзорных РЛС ПВО, на основе которого акцентируется внимание на двух группах методов, отвечающих требованиям технологической приемлимости, с конкретизацией задач их детальной разработки.

Ил. 4. Библиогр. : 4 назв.

УДК 621.396.96

Вибір технологічно обґрунтованого методу оцінки складу групової зосередженої цілі / В.М. Кичак, Е.С. Ленков, В.М. Лоза // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2011. – Вип. 166. – С. 180 - 185.

Аналізуються теоретично розроблені методи "надрелеєвського" розрізнення з погляду їх практичної реалізації в оглядових РЛС ППО, на основі якого акцентується увага на двох групах методів, що відповідають вимогам технологічної прийнятності, з конкретизацією завдань їх детальної розробки.

Іл. 4. Бібліогр. : 4 назви.

UDC 621.396.96

Technologically justified method for estimation of the multiple grouped target content / V.M. Kichak, E.S. Lenkov, V.M. Loza // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2011. – № 166. – P. 180 - 185.

Theoretically developed methods of "super Raleigh" resolution in terms of their practical application to the air defense scanning radars are analyzed; based on this resolution attention focuses on two groups of the methods meeting criteria of technological plausibility with concrete definition of the problems of their detailed development.

4 fig. Ref.:4 items

УДК 621.371.35

Метод расчета областей наиболее вероятного появления метеорных следов, имеющих точку зеркального отражения / Е.В. Харченко // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2011. – Вып. 166. – С. 186 – 192.

Предложен метод расчета зон наибольшей вероятности появления метеорных следов с точкой зеркального отражения для радиолиний различной протяженности. При расчете учтены линейная электронная плотность следа, зависящая от скорости и массы метеороида, а также зенитные углы, определяемые радиантами спорадических метеоров и метеорных потоков.

Табл. 1. Ил. 5. Библиогр.: 8 назв.

УДК 621.371.35

Метод розрахунку областей найбільш ймовірної появи метеорних слідів, що мають точку дзеркального відображення / О.В. Харченко // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2011. – Вип. 166. – С. 186 – 192.

Запропоновано метод розрахунку зон найбільшої ймовірності появи метеорних слідів з точкою дзеркального відображення для радіоліній різної протяжності. При розрахунку враховано лінійну електронну щільність сліду, що залежить від швидкості і маси метеороида, а також зенітні кути, обумовлені радіантами спорадичних метеорів і метеорних потоків.

Табл. 1. Іл. 5. Бібліогр.: 8 назв.

UDC 621.371.35

Methods for calculation of areas of the most likely emergence of the meteor trails having the mirror reflection point / O.V. Kharchenko // Radiotekhnika: All-Ukr. Sci. Interdep. Mag. – 2011. – № 166. – P. 186 – 192.

The method for calculation of the areas of the most likely emergence of meteor trails having the mirror reflection point for the radio links of different lengths is proposed. When calculating, the linear electron den-

sity of the meteor trail, depending on the velocity and mass of the meteoroid, as well as zenith angles, defined by radiants of sporadic meteors and meteor showers are taken into account.

1 tab. 5 fig. Ref.: 8 items.

УДК 551.501.793

Адаптация рабочей частоты содара в условиях изменяющейся помеховой обстановки / О.В. Зубков, Г.И. Сидоров // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2011. – Вып. 166. – С. 193 - 199.

Доказана необходимость подстройки рабочей частоты содара в условиях изменяющейся помеховой обстановки с целью увеличения отношения сигнал/шум. Получены выражения для расчета оптимальной рабочей частоты содара и разработан алгоритм ее оценивания с использованием выборочной спектральной плотности мощности внешних шумов. Доказана работоспособность разработанного алгоритма с использованием экспериментальных реализаций шумов автотранспорта и шумов в зоне аэропорта.

Табл. 2. Ил. 3. Библиогр.: 6 назв.

УДК 551.501.793

Адаптація робочої частоти содара в умовах змінної завадової обстановки / О.В. Зубков, Г.І. Сидоров // Радіотехніка : Всеукр. міжвід. наук.-техн. сб. – 2011. – Вип. 166. – С. 193 - 199.

Доведена необхідність підстроювання робочої частоти содара в умовах змінної завадової обстановки з метою збільшення відношення сигнал/шум. Отримані вирази для розрахунку оптимальної робочої частоти содара і розроблений алгоритм її оцінювання з використанням вибіркової спектральної щільності потужності зовнішніх шумів. Доведена працездатність розробленого алгоритму з використанням експериментальних реалізацій шумів автотранспорту і шумів в зоні аеропорту.

Табл. 2. Іл. 3. Бібліогр.: 6

UDC 551.501.793

Sodar operation frequency adaptation under the conditions of changing noise situations / O.V. Zubkov, G. I. Sidorov // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2011. – № 166. – P. 193 - 199.

The necessity of sodar operation frequency fine tuning under the conditions of noise changing aimed for a signal/noise ratio increase is proved. The calculation expressions for the sodar optimum operation frequency are derived and its estimation algorithm using the selective external spectral noise power density is developed. The efficiency of the developed algorithm, using the experimental noise realizations of motor transport and noise in an airport area, is proved.

2 tab. 3 fig. Ref.: 6 items.

УДК 517.958:537.8

Возбуждение конуса с продольной щелью во временной области магнитным радиальным диполем / А. В. Артюх, В. А. Дорошенко // Радиотехника: Всеукр. межвед. науч.-техн. сб. – 2011. – Вып. 166. – С.200 - 204.

Построена математическая модель возбуждения конуса с продольными щелями магнитным радиальным диполем во временной области. Показано, что начально-краевая электродинамическая задача сводится к решению системы алгебраических линейных уравнений с вполне непрерывным оператором. На основании полученных аналитических выражений проведен численный эксперимент для одной из составляющих магнитного поля в случае конуса с продольной щелью.

Ил. 3. Библиогр.: 5 назв.

УДК 517.958:537.8

Збудження конуса з позовдовжньою щілиною у часовій області магнітним радіальним диполем / А. В. Артюх, В. А. Дорошенко // Радіотехніка: Всеукр. міжвід. наук.-техн. сб. – 2011. – Вип. 166. – С. 200 - 204.

Побудовано математичну модель збудження конуса з позовдовжніми щілинами магнітним радіальним диполем у часовій області. Показано, що початково-крайова електродинамічна задача зводиться до розв'язання системи алгебраїчних лінійних рівнянь з цілком неперервним оператором. На підставі отриманих аналітичних виразів проведено чисельний експеримент для однієї зі складових магнітного поля у випадку конуса з позовдовжньою щілиною.

Іл. 3. Бібліогр.: 5 назв.

UDC 621.375.8

Excitation of the cone with a longitudinal slot by a magnetic radial dipole in the time domain / A.I. Slipchenko, V.A. Doroshenko // Radiotekhnika: All-Ukr. Sci. Interdep. Mag. – 2011. – №166. – P. 200 - 204.

The mathematical model for excitation of the cone with longitudinal slots by a magnetic radial dipole in time domain is built. It is shown that the initial-boundary electrodynamic problem is reduced to the system of linear algebraic equations with a completely continuous operator. The numerical analysis for one of the magnetic field components for the cone with a longitudinal slot based on the derived analytical results is carried out.

3 fig. Ref.: 5 items.

УДК 621.315.592

Исследование и моделирование электронных свойств аморфных пленок α -Si:H / Н.И. Слипченко, В.А. Письменецкий, Н.В. Герасименко // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2011. – Вып. 166. – С. 205 - 213.

Приведены результаты исследований влияния базовых технологических факторов: температуры осаждения пленки, давления газовой смеси и скорости ее прокачки через рабочий объем камеры на концентрацию водорода в осажденных аморфных пленках α -Si:H. Исследованы зависимости темновой и фотопроводимости, коэффициента оптического поглощения и ширины запрещенной зоны указанных пленок от параметра C_H , а так же их температурные характеристики. Для аналитического описания исследованных зависимостей предложены аппроксимационные модели.

Ил. 9. Библиогр.: 10 назв.

УДК 621.315.592

Дослідження і моделювання електронних властивостей аморфних плівок α -Si:H / М.І. Слипченко, В.О. Письменецкий, М.В. Герасименко // Радіотехніка: Всеукр. міжвід. наук.-техн. зб. – 2011. – Вип. 166. – С. 205 - 213.

Наведено результати досліджень впливу базових технологічних факторів: температури осадження плівки, тиску газової суміші та швидкості її прокачування через робочий об'єм камери на концентрацію водню в осаджених аморфних плівках α -Si:H. Досліджено залежності темрової і фотопровідності, коефіцієнта оптичного поглинання і ширини забороненої зони зазначених плівок від параметра C_H , а так само їх температурні характеристики. Для аналітичного опису досліджених залежностей запропоновані апроксимаційні моделі.

Іл. 9. Бібліогр.: 10 назв.

UDC 621.315.592

Investigation and simulation of electronic properties of α -Si:H amorphous films / N.I. Slipchenko, V.A. Pismenetsky, N.V. Guerasimenko // Radiotekhnika: All-Ukr. Sci. Interdep. Mag. – 2011. – № 166. – P. 205 - 213.

The results of investigations into the effect of the basic technological factors: temperature, film deposition, the pressure of the gas mixture and its rate of pumping through the working volume of the chamber on the concentration of hydrogen in amorphous films deposited α -Si:H are presented. The dependence of the dark and photoconductivity, and absorption of the optical bandgap of these films on the parameter of C_H , as well as their temperature characteristics are studied. Approximation models are offered for analytical description of the investigated dependences.

9 fig. Ref.: 10 items.

УДК 621.371.34

Оценка текущих условий загоризонтного распространения УКВ по заданному пространственному распределению коэффициента преломления воздуха / В.А. Петров, А.Н. Ключева, О.Л. Павлова // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2011. – Вып.166. – С. 214 - 222.

Рассматривается метод оценки поля в области геометрической тени для произвольного распределения индекса рефракции в тропосфере. Для расчета поля в зоне дифракции Френеля источников вторичного излучения используется метод геометрической оптики и интеграл Френеля-Кирхгофа. Результаты расчетов согласуются с экспериментальными данными, которые получены в дециметровом диапазоне волн.

Ил.3. Библиогр.: 15 назв.

УДК 621.371.34

Оцінка поточних умов загоризонтного поширення УКВ за заданим просторовим розподілом коефіцієнта заломлення повітря / В.А. Петров, А.М. Ключева, О.Л. Павлова // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2011. – Вип.166. – С. 214 - 222.

Розглядається метод оцінювання поля в області геометричної тіні для довільного розподілу індексу рефракції у тропосфері. Для розрахунку поля в зоні дифракції Френеля джерел вторинного випромінювання застосовується метод геометричної оптики та інтеграл Френеля-Кирхгофа. Результати розрахунків узгоджуються з експериментальними даними, що отримані у дециметровому діапазоні хвиль.

Л. 3. Бібліогр.: 15 назв.

UDC 621.371.34

Estimation of current conditions transhorizon UHF propagation for a given spatial distribution of the refractive index of air / V.A. Petrov, A.N. Klyueva, O.L. Pavlova // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2011. – №166. P. 214 - 222.

A method for estimation of the wave field in the geometric shadow for the arbitrary distribution of the refractive index in the troposphere is considered. The geometrical optics and Fresnel-Kirchhoff integral are used to calculate the field in the Fresnel diffraction region of the secondary radiation sources. The results conform to the experimental data obtained in the UHF band.

3 fig. Ref.: 15 items.

УДК 517.958:537.8

Моделирование рассеивания поля электрического радиального диполя одиночным полупрозрачным конусом с продольными щелями / В.А. Дорошенко, Ю.Д. Шимук // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2011. – Вип.166. – С. 223 - 227.

Рассмотрена модельная электродинамическая задача о возбуждении одиночного полупрозрачного конуса с продольными щелями электрическим радиальным диполем. Показано, что исходная задача сводится к краевой задаче математической физики относительно потенциалов Дебая, а последняя – к системе линейных алгебраических уравнений. Исследованы зависимости коэффициентов системы, а также одной из составляющих плотности поверхностного тока от параметров задачи.

Л. 7. Библиогр.: 5 назв.

UDC 517.958:537.8

Моделювання розсіювання поля електричного радіального диполя поодиноким напівпрозорим конусом із повздовжніми щілинами / В.О.Дорошенко, Ю.Д. Шимук // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2011. – Вип.166. – С. 223 - 227.

Розглянуто модельну електродинамічну задачу про збудження поодиноким напівпрозорим конусом із повздовжніми щілинами електричним радіальним диполем. Показано, що вихідна задача зводиться до крайової задачі математичної фізики відносно потенціалів Дебая, а остання – до системи лінійних алгебраїчних рівнянь. Досліджено залежності коефіцієнтів системи, а також однієї із складових щільності поверхневого току від параметрів задачі.

Л. 7. Бібліогр.: 5 назв.

UDC 517.958:537.8

Mathematical modeling of a resistive cone with a longitudinal slot excitation by a monochromatic source / V. A. Doroshenko, Y.D. Shimuk // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2011. – №166. – P. 223 - 227.

The given work is dedicated to a model electromagnetic problem of a single semitransparent cone with longitudinal slots excitation by an electric radial dipole studying. It is shown that the original problem can be reduced to a boundary one of mathematical physics relatively to the Debye's potentials. The obtained initial-boundary problem can be reduced to the system of linear algebraic equations. The dependencies of the system coefficients and one of the surface current density components on the problem parameters are investigated.

7 fig. Ref.: 5 items.

УДК 621.371.3:551.510.52

О постановке дифракционной задачи для бистатической зоны систем радиоакустического зондирования атмосферы / Н. И. Слипченко, Лю Чан, А.Ю. Панченко // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2011. – Вип.166. – С. 228 - 232.

Внедрению метода радиоакустического зондирования в практику метеоизмерений препятствует ряд проблем. Среди них отсутствие строгого решения задачи дифракции электромагнитных волн на искусственном отражателе, сформированным ограниченным в пространстве пучком акустических волн. Общее решение крайне громоздко.

Показаны приближения, допустимые в данной задаче, которые получены с позиций теории антенн. Обсуждаются условия и методика решения задачи. Представлены предварительные результаты решения дифракционной задачи в бистатической зоне. В частности, показано изменение уровня принимаемого сигнала как функции высоты зондирования (функция радиального взаимодействия полей).

Ил. 4. Библиогр.: 6 назв.

УДК 621.371.3:551.510.52

До постановки дифракційної задачі для бістатичної зони систем радіоакустичного зондування атмосфери / М. І. Сліпченко, Лю Чан, О.Ю. Панченко // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2011. – Вип.166. – С. 228 - 232.

Впровадженню метода радіоакустичного зондування у практику метеовимірювань перешкоджає ряд проблем. Серед них відсутність строгого розв'язку задачі дифракції електромагнітних хвиль на штучному відбивачі, що сформовано обмеженням у просторі пучком акустичних хвиль. Загальний розв'язок у край ускладнено.

Показано наближення, що можливі у даній задачі, які отримано з урахуванням засад теорії антен. Обговорюються умови та методика розв'язку задачі. Представлено попередні результати розв'язку дифракційної задачі в бістатичній зоні. Зокрема показано зміну рівня сигналу, що прийнято, в залежності від висоти зондування (функція радіальної взаємодії полів).

Ил. 4. Бібліогр.: 6 назв.

UDC 621.371.3:551.510.52

About statement of the diffraction problem for bistatic zone of radio acoustic atmospheric sounding / N.I. Slipchenko, Liu Chang, A.Yu. Panchenko // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2011. – № 166. – P. 228 - 232.

A number of problems prevent introduction of the radio acoustic sounding method into practice of meteor measurements. There is no rigorous solution among them of the problem of electromagnetic waves diffraction on the artificial reflector formed by the acoustic waves beam limited in space. The general solution is extremely cumbersome.

Approximations acceptable in the given problem obtained in the context of the antenna theory are shown. Conditions and methods of the problem solution are presented. Tentative results of the diffraction problem solution in the bistatic zone are shown. Specifically, variation of the received signal level as a function of the sounding height is shown (the fields radial interaction function).

4 fig. Ref.: 6 items.

УДК: 681.128.82

Контроль уровня высокотемпературных объектов методом акустической локации / Б.В. Жуков, К.В. Нетребенко, А.В. Одновол // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2011. – Вып. 166. – С. – 233 – 238.

Для двух рабочих частот представлены результаты экспериментальных исследований процесса контроля уровня высокотемпературных объектов методом акустической локации. Предложены пути повышения работоспособности акустических уровнемеров.

Табл. 1 Ил. 7. Библиогр.: 7 назв.

УДК: 681.128.82

Контроль рівня високотемпературних об'єктів методом акустичної локації / Б.В. Жуков, К.В. Нетребенко, А.В. Одновол // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2011. – Вип. 166. – С. – 233 – 238.

Для двох робочих частот представлені результати експериментальних досліджень у процесі контролю рівня високотемпературних об'єктів методом акустичної локації. Запропоновано шляхи підвищення працездатності акустичних рівневимірювачів.

Табл.1. Ил.7. Бібліогр.: 7 назв.

UDC: 681.128.82

*** Control of level of high temperature objects with the acoustic location method / B.V. Zhukov, K.V. Netrebenko, A.V.Odnovol // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2011. – № 166. – P. 233 – 238.**

The results of experimental researches in control level of high-temperature objects for two operating frequencies are presented. The ways of improving working capacity of acoustic level gauges are proposed.

1 tab. 7 fig. Ref.: 7 items.

УДК 621.391.7

Анализ структурной скрытности многоуровневых линейных сигналов цифровых систем передачи информации на основе широкополосных xDSL технологий / И.В. Шинкаренко, А.А. Дудка, А.И. Цопа // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2011. – Вып.166. – С. 239 – 244.

Представлен анализ структурной скрытности линейных сигналов, применяемых в современных проводных системах передачи информации на основе различных xDSL технологий.

Табл. 1. Ил. 2. Библиогр.: 10 назв.

УДК 621.391.7

Аналіз структурної скритності багаторівневих лінійних сигналів цифрових систем передачі інформації на основі широкосмугових xDSL технологій / І.В. Шинкаренко, О.О. Дудка, О.І. Цопа / Радиотехніка : Всеукр. міжвід. наук.-техн. зб. – 2011. – Вип.166. – С. 239 – 244.

Представлено аналіз структурної скритності лінійних сигналів, що застосовуються в сучасних проводних системах передачі інформації на базі різних xDSL технологій.

Табл. 1. Іл. 2. Бібліогр.: 10 назви.

UDC 621.391.7

Structural analysis of the multi-level linear signals secrecy of digital information transmission systems based on broadband xDSL technologies / I. Shynkarenko, O. Dudka, O. Tsopa // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2011. – № 166. – P. 239 – 244.

The paper presents an analysis of structural secrecy linear signals used in today's wired data transmission systems based on various xDSL technologies.

1 tab. 2 fig. Ref.: 10 items.

УДК 621.3.018.12

Исследование влияния шумов в радиоканале на работу системы синхронизации опорных генераторов / И. Б. Широков, И. В. Сердюк // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2011. – Вып.166. – С. 245 – 253.

Представлены результаты теоретического и экспериментального исследования системы фазовой синхронизации низкочастотных опорных генераторов, осуществляемой через радиоканал. Представлены результаты экспериментального исследования зависимости плотности распределения вероятности мгновенной разности фаз опорного генератора и генератора управляемого напряжением, в зависимости от ширины спектра фазового шума в радиоканале. Приводится анализ влияния амплитудных и фазовых шумов в радиоканале на работу системы фазовой синхронизации опорных генераторов через атмосферный канал связи.

Ил. 6. Библиогр.: 4 назв.

УДК 621.3.018.12

Дослідження впливу шумів в радіоканалі на роботу системи синхронізації опорних генераторів / І.Б. Широков, І. В. Сердюк // Радиотехніка : Всеукр. межвед. научн.-техн. сб. – 2011. – Вип. 166. – С. 245 – 253

Представлено результати теоретичного і експериментального дослідження системи фазової синхронізації низькочастотних опорних генераторів, яка здійснюється через радіоканал. Представлено результати експериментального дослідження залежності щільності розподілу вірогідності миттєвої різниці фаз опорного генератора і генератора керованого напругою, залежно від ширини спектру фазового шуму в радіоканалі. Наведено аналіз впливу амплітудних і фазових шумів в радіоканалі на роботу системи фазової синхронізації опорних генераторів через атмосферний канал зв'язку.

Іл. 6. Бібліогр.: 4 назви.

UDC 621.3.018.12

The research of noises influence in a radio channel to the reference oscillators' synchronization system operation / I. B. Shirokov, I. V. Serdyuk // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2011. – № 166. – P. 245 – 253.

The results of theoretical and experimental research of the phase synchronization system of low frequency reference oscillators, that carried out through the radio channel are presented. The results of experi-

mental research of the probability density dependence by the instantaneous phases difference of reference oscillator and voltage-controlled oscillator, depending on the width of the phase noise spectrum in the radio channel, are presented. The analysis of amplitude and a phase noise influence in the radio channel to the operation of the phase synchronization system of the reference oscillators through the atmospheric communication channel is presented.

6 fig. Ref.: 4 items.

УДК 621.372(075)

Исследование спектра выходного сигнала нелинейной системы в режиме стохастического резонанса / О.И. Харченко // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2011. – Вып. 166. – С. 254 – 258.

Рассмотрена возможность использования эффекта стохастического резонанса (СР) для выделения гармонического сигнала из аддитивной смеси сигнала с шумом. Для представления сигнала на выходе нелинейной системы в аналитическом виде использовались ряды Вольтерра. Проведен анализ двумерных амплитудных и амплитудно-частотных характеристик системы. Получены выражения для спектральной плотности мощности первой и третьей гармоник выходного сигнала. Определены условия эффективного выделения полезного сигнала в режиме СР нелинейной системы.

Табл. 1. Ил. 3. Библиогр.: 4 назв.

УДК 621.372(075)

Дослідження спектру вихідного сигналу нелінійної системи в режимі стохастичного резонансу / О.І. Харченко // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2011. – Вип. 166. – С. 254 – 258.

Розглянуто можливість використання ефекту стохастичного резонансу (СР) для виділення гармонічного сигналу з адитивної суміші сигналу із шумом. Для подання сигналу на виході нелінійної системи в аналітичному вигляді використано ряди Вольтерра. Проведено аналіз двувимірних амплітудних та амплітудно-частотних характеристик системи. Отримано вирази для спектральної густини потужності першої та третьої гармонік вихідного сигналу. Визначено умови ефективного виділення корисного сигналу в режимі СР нелінійної системи.

Табл. 1. Іл. 3. Бібліогр.: 4 назви.

UDC 621.372(075)

Investigation of output signal spectrum of nonlinear system in stochastic resonance regime / O.I. Kharchenko // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2011. – № 166. – P. 254 – 258.

The possibility to use the effect of stochastic resonance (SR) for the selection of a harmonic signal from an additive mixture of signal and noise is considered. Volterra series is used to represent the signal at the output of the nonlinear system in the analytical form. The analysis of two-dimensional amplitude and the amplitude-frequency characteristics of the system is carried out. Expressions are derived for the power spectral density of the first and third harmonics of the output signal. The conditions for efficient allocation of the desired signal in the SR regime of nonlinear system are defined.

1 tab. 3 fig. Ref.: 4 items.

УДК 681.326

Методы повышения отказоустойчивости телекоммуникационных систем / В.Г. Котух, М.А. Мирошник, С.Н. Селевко // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2011. – Вып. 166. – С. 259 – 268.

В результате исследований, посвященных существенному повышению отказоустойчивости ТКС на основе внедрения в процессы проектирования моделей и методов, обеспечивающих необходимые характеристики функциональности и восстановления работоспособности и его компонентов в реальном масштабе времени, получены следующие результаты: Сформулированы критерии качества с позиции отказоустойчивости, дающие возможность оценки его характеристик при работе в реальном масштабе времени. Предложен метод, позволяющий повысить отказоустойчивость выполнения на параллельных вычислительных подсистемах задач, реализующих новые функции интеллектуальной поддержки. Сформулирована задача разработки принципов организации процессов диагностирования неисправностей технических средств и использования дополнительных средств асинхронного резервирования процессов, которые обеспечивают диагностирование, локализацию неисправностей, корректное восстановление процессов, математические методы оценки влияния случайных неисправностей на время выполнения сложных наборов задач.

Іл. 2. Библиогр.: 21 назв.

Методи підвищення відмовостійкості телекомунікаційних систем / В.Г. Котух, М.А. Мірошник, С.М. Селевко // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2011. – Вип. 166. – С. 259 – 268.

В результаті досліджень, присвячених суттєвого підвищення відмовостійкості ТКС на основі впровадження в процеси проектування моделей і методів, які забезпечують необхідні характеристики функціональності та відновлення працездатності і його компонентів в реальному масштабі часу, отримані наступні результати: Сформульовано критерії якості з позиції відмовостійкості, що дають можливість оцінки його характеристик при роботі в реальному масштабі часу. Запропоновано метод, що дозволяє підвищити відмовостійкість виконання на паралельних обчислювальних підсистемах завдань, що реалізують нові функції інтелектуальної підтримки. Сформульовано завдання розробки принципів організації процесів діагностування несправностей технічних засобів і використання додаткових засобів асинхронного резервування процесів, які забезпечують діагностування, локалізацію несправностей, коректне відновлення процесів, математичні методи оцінки впливу випадкових несправностей на час виконання складних наборів завдань.

Іл. 2. Бібліогр.: 21 назва.

UDC 681.326

Methods to improve the resiliency of telecommunications systems / V.G. Kotuh, M.A. Miroshnik, S.N. Selevko // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. – 2011. – № 166. – P. 259 – 268.

The following results were obtained as a result of research in the significant increase in resilience of TCS based on the introduction to the processes of models and methods design which provide the necessary characteristics of functionality and disaster recovery and its components in real time: The quality criteria in terms of resiliency are formulated, they enable evaluation of its performance when operating in real time. The method making it possible to increase resilience of performing parallel computing subsystem tasks, implementing new features of the intellectual support.

The problem of developing the principles of organization of the processes of diagnosing failures of technical means and the use of additional means of asynchronous backup processes that provide diagnosis, fault isolation, proper recovery processes, mathematical methods for evaluating the effect of random failures during the execution of complex sets of tasks.

2 fig. Ref.: 21 items.

**ЗБІРНИК НАУКОВИХ ПРАЦЬ
РАДІОТЕХНІКА**
Випуск 166
Російською, українською та англійською мовами

**СБОРНИК НАУЧНЫХ ТРУДОВ
РАДИОТЕХНИКА**
Выпуск 166
На русском, украинском и английском языках

Коректор Л.І. Сащенко

Підп. до друку 29. 09 2011. Формат 60х90/8. Папір офсет. Гарнітура Таймс. Друк. ризограф.
Ум. друк. арк. 16,4. Обл.-вид. арк. 13,9. Тираж 300 прим. Зам. № 116. Ціна договір.

Харківський національний університет радіоелектроніки (ХНУРЕ)
Просп. Леніна, 14, Харків. 61166.

Оригінал-макет підготовлено і збірник надруковано у ПФ „Колегіум”, тел. (057) 703-53-74.
Свідоцтво про внесення суб’єкта видавничої діяльності до Державного реєстру видавців.
Сер. ДК №1722 від 23.03.2004