Міністерство освіти і науки України
Вінницький національний технічний університет
Харківський національний економічний університет
Університет ЛІОН 2 ім. Люм'єра, Франція
Технічний університет «AGH», Польща
Білгородський державний університет, Росія
Інститут кібернетики НАНУ
Інститут інженерів з електротехніки та електроніки (IEEE),
Українська секція
Представництво «Microsoft України»
Асоціація «Інформаційні технології України»
Співтовариство IT-директорів України

«Інформаційні технології та ком'ютерна інженерія»

Тези доповідей Міжнародної науково-практичної конференції м. Вінниця, Україна 19-21 травня 2010 року

«Информационные технологии и компьютерная инженерия»

Тезисы докладов Международной научно-практической конференции г. Винница, Украина 19-21 мая 2010 года

Вінниця
ВНТУ
2010

УДК 004+681.3+621.3
ББК 32.97
І 54

Відповідальний редактор В. А. Лужецький

Матеріали статей опубліковані в авторській редакції

І 54 **Інформаційні** технології та коп'ютерна інженерія. Тези доповідей Міжнародної науково-практичної конференції. м. Вінниця, 19–21 травня 2010 року. – Вінниця: ВНТУ, 2010. – 487 с.
ISBN 978-966-641-356-0

Збірка містить матеріали доповідей Міжнародної науково-практичної конференції з сучасних проблем інформаційних технологій та комп'ютерної інженерії за вісьмома основними напрямками: інформаційні технології в технічних системах, методи та засоби обробки даних та сигналів, захист інформації в інформаційно-телекомунікаційних системах, моделювання комп'ютерних систем та компонентів, відмовостійкі комп'ютерні системи та компоненти, інформаційні технології в освіті, медицині, економіці та екології.

УДК 004+681.3+621.3
ББК 32.97

©Автори статей, 2010
©Упорядкування, Вінницький національний технічний університет, 2010

ISBN 978-966-641-356-0

ЗМІСТ

1. ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ТЕХНІЧНИХ СИСТЕМАХ

В.В. Древецький, М.М. Клепач, С.П. Воробюк 33
СИСТЕМА КОМПЛЕКСНОГО КОНТРОЛЮ ФІЗИЧНИХ ПАРАМЕТРІВ НАФТОПРОДУКТІВ

Д.В. Федасюк, Т.О. Муха 35
ЗАСТОСУВАННЯ ВИПАРОВУВАННЯ ДЛЯ ІНТЕНСИФІКАЦІЇ ТЕПЛОВІДВЕДЕННЯ

В.М. Дубовой, О.С. Сольський 37
ЗАДАЧІ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У ПРОБЛЕМІ ЗАХИСТУ РОСЛИН

О.В. Осадчук, Р.В. Криночкін 39
АВТОМАТИЗОВАНА ІНФОРМАЦІЙНА СИСТЕМА ЧАСТОТНОГО ВИМІРЮВАННЯ ТОВЩИНИ

П.Д. Лежнюк, О.А. Ковальчук 41
ОСОБЛИВОСТІ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ АВТОМАТИЗОВАНОЇ СИСТЕМИ КЕРУВАННЯ КАСКАДАМИ МАЛИХ ГІДРОЕЛЕКТРОСТАНЦІЙ

П.Д. Лежнюк, В.Ю. Прохватилов 43
ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ КОНТРОЛЯ И УПРАВЛЕНИЯ ТРАНЗИТНЫМИ ПОТОКАМИ МОЩНОСТИ В ЭЛЕКТРИЧЕСКИХ СИСТЕМАХ

М.Й. Бурбело, М.В. Никитенко 45
ВИМІРЮВАННЯ ІНФОРМАТИВНИХ ПАРАМЕТРІВ ТРИФАЗНИХ НЕСИМЕТРИЧНИХ ШВИДКОЗМІННИХ НАВАНТАЖЕНЬ ВУЗЛІВ ЕЛЕКТРИЧНИХ МЕРЕЖ
В.Ю. Кучерук, І.А. Дудатьєв 47
СИНЕРГЕТИЧНІ МЕТОДИ КЕРУВАННЯ ТЕПЛОЕНЕРГЕТИЧНИМИ ОБ’ЄКТАМИ
А.Ю. Берко 48
ФОРМАЛЬНА МОДЕЛЬ ПРОЦЕСІВ ІНТЕГРАЦІЇ ДАНИХ У ВІДКРИТИХ СИСТЕМАХ
В.П. Зінченко, Д.І. Конотоп 50
ЗАСТОСУВАННЯ СУЧАСНИХ КОМП’ЮТЕРНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ПРИ ПРОЕКТУВАННІ СКЛАДНОГО ТЕХНІЧНОГО ОБ’ЄКТА
Д.С. Замятін, В.Б. Щукін 52
ЗАСТОСУВАННЯ КОМП’ЮТЕРНИХ СИСТЕМ З ПАРАЛЕЛЬНОЮ АРХІТЕКТУРОЮ ДЛЯ ПРОГНОЗУВАННЯ ПАРАМЕТРІВ ТЕХНОЛОГІЧНОГО ПРОЦЕСУ В УМОВАХ ГІРНИЧО-ЗБАГАЧУВАЛЬНОГО КОМБІНАТУ
В.Й. Пастушенко, С.В. Шатний 54
РОЗРОБКА ПІДСИСТЕМ ТЕХНІЧНОГО ТА ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ АВТОМАТИЗОВАНОЇ СИСТЕМИ КЕРУВАННЯ ВОЛОГОЗАБЕЗПЕЧЕННЯМ
М.В. Плахотний, В.О. Дащенко 56
АЛГОРИТМІЧНЕ ТА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ СИСТЕМИ КЕРУВАННЯ СТАНКОМ З ЧПУ

В.Й. Пастушенко, А.В. Комар 58
РОЗРОБКА ТА ДОСЛІДЖЕННЯ НЕЙРОРЕГУЛЯТОРА ДЛЯ СИСТЕМИ УПРАВЛІННЯ ВУЗЛОМ АБСОРБЦІЇ
О.О. Семенова, А.О. Семенов, О.О. Войцеховська 60
ВИКОРИСТАННЯ ФАЗІ-КОНТРОЛЕРІВ У АТМ-МЕРЕЖАХ
С.М. Москвіна, С.А. Білоконь 62
СИСТЕМА ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ ДЛЯ УПРАВЛІННЯ ТЕПЛОТЕХНОЛОГІЧНИМ ОБ'ЄКТОМ
В.В. Джеджула 64
ІНФОРМАЦІЙНО–ВИМІРЮВАЛЬНА СИСТЕМА ДІАГНОСТИКИ ТЕПЛОНАСОСНОГО ОБЛАДНАННЯ
О.В. Кухарєва 66
АЛГОРИТМИ ONLINE-МАРШРУТИЗАЦІЇ ДЛЯ УПРАВЛІННЯ ТРАФІКОМ У МЕРЕЖАХ З ТЕХНОЛОГІЄЮ MPLS
Р.Н. Чижденко 68
АГЕНТНЫЙ ПОДХОД В ЗАДАЧЕ УПРАВЛЕНИЯ ДИНАМИЧЕСКИМ ОБЪЕКТОМ
М.В. Васильская, П.В. Северилов 70
ТЕХНОЛОГИИ ПОЛУЧЕНИЯ ФУНКЦИЙ ВЛИЯНИЯ ДЛЯ СЛОЖНЫХ СИСТЕМ
В.Ю. Болибрук 72
ОСОБЕННОСТИ СИСТЕМЫ УПРАВЛЕНИЯ СЕТЕВЫМИ СОЕДИНЕНИЯМИ НА БАЗЕ ПРОТОКОЛА RADIUS
О.П. Поволоцький 74
СПЕЦІАЛІЗОВАНІ КОМП’ЮТЕРНІ СИСТЕМИ GPS- НАВІГАЦІЇ

2. МЕТОДИ ТА ЗАСОБИ ОБРОБКИ ДАНИХ

Р.К. Мамедов, А.С. Муталлимова, Т.Ч. Алиев, 78
МЕРЫ БЛИЗОСТИ МЕЖДУ ОБЪЕКТАМИ, ПОВЫШАЮЩИЕ ДОСТОВЕРНОСТЬ РАСПОЗНАВАНИЯ ОБЪЕКТОВ В СИСТЕМАХ ТЕХНИЧЕСКОГО ЗРЕНИЯ

В.В. Баранник, С.А. Сидченко, В.В. Ларин 80
ФОРМИРОВАНИЕ ДЕШИФРИРУЕМО-СТОЙКОГО ПРЕДСТАВЛЕНИЯ ИЗОБРАЖЕНИЙ В СИСТЕМАХ КОМПРЕСИИ

Р.А. Мельник, Т.С. Климаш 82
ДОСЛІДЖЕННЯ ХАРАКТЕРИСТИК КОМПРЕСІЇ ТА ТОЧНОСТІ ПРИ АПРОКСИМАЦІЇ ВІЗУАЛЬНИХ ОБРАЗІВ

В.А. Лужецький, А.В. Кульчицький 84
ДОСЛІДЕННЯ ЧИСЛОВИХ МОДЕЛЕЙ ДАНИХ

Р.Н. Квєтний, В. Ю. Коцюбинський, Н.В. Казимірова 86
АДАПТИВНИЙ ПІДХІД ЩОДО ПРОГНОЗУВАННЯ ЧАСОВИХ РЯДІВ

Р.П. Базилевич, Р.К. Кутельмах, Б.О. Кузь 88
АЛГОРИТМІЧНЕ ЗАБЕЗПЕЧЕННЯ ДЛЯ РОЗПАРАЛЕЛЮВАННЯ ЗАДАЧІ КОМІВОЯЖЕРА ВЕЛИКОЇ РОЗМІРНОСТІ

Р.П. Базилевич, М.А. Влах, Н.І. Пелих 90
ФУНКЦІОНАЛЬНЕ НАПОВНЕННЯ ПРОГРАМНОЇ СИСТЕМИ З ШИРОКИМИ МОЖЛИВОСТЯМИ ДЛЯ ДЕКОМПОЗИЦІЇ СКЛАДНИХ СХЕМ

С.Н. Гриша, А.И. Муха 92
ИССЛЕДОВАНИЕ МЕТОДОВ РЕШЕНИЯ ЗАДАЧИ ОПТИМИЗАЦИИ КОРМОВЫХ РАЦИНОВ

В.М. Михалевич, О.В. Михалевич 94
ДОСЛІДЖЕННЯ МОЖЛИВОСТІ УЩІЛЬНЕННЯ ДАНИХ ЗА ДОПОМОГОЮ ЛІНІЙНИХ РЕКУРЕНТНИХ ПОСЛІДОВНОСТЕЙ ДРУГОГО ПОРЯДКУ
Э.И. Владимирский, Б.И. Исмайлов 96
СИНЕРГЕТИЧЕСКИЕ АСПЕКТЫ НЕЛИНЕЙНОГО РЕКУРРЕНТНОГО АНАЛИЗА ХАОТИЧЕСКОЙ ИНФОРМАЦИИ
Я.І. Виклюк 98
МАТЕМАТИЧНІ МЕТОДИ МОДЕЛЮВАННЯ ПРОСТОРОВИХ СИСТЕМ НА ОСНОВІ БРОУНІВСЬКИХ ФРАКТАЛЬНИХ РЕЛЬЄФІВ ТА НЕЧІТКОЇ ЛОГІКИ
И.А. Кулик, С.В. Костель 100
СИСТЕМА СЖАТИЯ ИНФОРМАЦИИ НА ОСНОВЕ БИНОМИАЛЬНЫХ ЧИСЕЛ
А.І. Купін, І.О. Музика 102
ГЕНЕТИЧНИЙ ПІДХІД ДО ОПТИМІЗАЦІЇ ПРОЦЕСІВ ЗБАГАЧУВАЛЬНОЇ ТЕХНОЛОГІЇ
Г.Г. Бортник, О.С. Городецька, О.В. Стальченко 104
ШВИДКИЙ АЛГОРИТМ ВЕЙВЛЕТ ПЕРЕТВОРЕННЯ НА БАЗІ ВЕЙВЛЕТА ХААРА
Д.С. Замятін, О.С. Дубровський 106
ВИЗНАЧЕННЯ МІНІМАЛЬНОГО НАБОРУ СЕМАНТИЧНИХ КОНСТРУКЦІЙ ДЛЯ ПІДТРИМКИ ПЛАТФОРМИ ВИВЧЕННЯ ТЕХНОЛОГІЙ ПРОГРАМУВАННЯ
О.Р. Чертов, М.В. Александрова 108
НЕОБХІДНІ ТА ДОСТАТНІ УМОВИ НА БАЗИС ДИАДНОГО ВЕЙВЛЕТ-ПЕРЕТВОРЕННЯ

О.В. Бісікало, І.А. Кравчук 110
АСОЦІАТИВНО-СТАТИСТИЧНИЙ МЕТОД МОРФОЛОГІЧНОГО АНАЛІЗУ СЛІВ
В.В. Кабачій, О.О. Чумаченко 112
ТЕХНОЛОГІЇ ІДЕНТИФІКАЦІЇ ЧАСОВИХ РЯДІВ НА ОСНОВІ ЙМОВІРНІСНОЇ НЕЙРОННОЇ МЕРЕЖІ ТА ЇЇ МОДИФІКОВАНИХ ВЕРСІЙ
Д.С. Замятін, О.І. Кобченко 114
МЕТОД ІМОВІРНІСНОГО АНАЛІЗУ КОДУ НА ЦІЛОЧИСЕЛЬНІ ПЕРЕПОВНЕННЯ
І.В. Мусійчук 116
РОЗРЯДНО-ЗРІЗОВИЙ МЕТОД ПАРАЛЕЛЬНОГО ПОРІВНЯННЯ ЧИСЛОВИХ МАРТИЦЬ У ФОРМІ З ПЛАВАЮЧОЮ КОМОЮ
В.А. Губернаторов 118
ПРИМЕНЕНИЕ МЕТОДА СЕЧЕНИЙ ДЛЯ КОНТРОЛЯ ФОРМЫ ПОВЕРХНОСТИ ПЯТНА ИЗЛУЧЕНИЯ В РЕАЛЬНОМ ВРЕМЕНИ
С.М. Захарченко, Н.Р. Кондратенко, О.О. Манаєва 120
ВИКОРИСТАННЯ ГЕНЕТИЧНОГО АЛГОРИТМУ В ЗАДАЧІ КЛАСТЕРИЗАЦІЇ АБОНЕНТІВ ІНТЕРНЕТ-ПРОВАЙДЕРА
Т.О. Гришанович 122
АЛГОРИТМ ВІДШУКАННЯ МІНІМАЛЬНОЇ ВІДСТАНІ МІЖ ВЕРШИНАМИ У ЧИСЛОВОМУ ГРАФІ МЕТОДОМ ПОШУКУ В ГЛИБИНУ
В.М. Дубовой, О.М. Москвін 124
АНАЛІЗ СЕМАНТИЧНОЇ ІНФОРМАЦІЇ ГІПЕРТЕКСТУ

В.А. Каплун 126
МОДЕЛЮВАННЯ ДАНИХ ДЛЯ ЗДІЙСНЕННЯ УЩІЛЬНЕННЯ ЧИСЛОВИХ ПОСЛІДОВНОСТЕЙ
Д.С. Демьяник 128
СИНТЕЗ ИНДИКАТОРНЫХ МАТРИЦ СИСТЕМ ВИЛЕНКИНА-КРЕСТЕНСОНА ФУНКЦИЙ
О.В. Романюк 130
НОВИЙ МЕТОД КУСКОВО-НЕПЕРЕРВНОЇ КВАДРАТИЧНОЇ АРОКСИМАЦІЇ ПЕРСПЕКТИВНОГО ТЕКСТУРУВАННЯ
М.П. Грищенко 132
ПІДСИСТЕМА АВТОМАТИЧНОЇ КЛАСИФІКАЦІЇ ТЕКСТОВИХ ДОКУМЕНТІВ НА ОСНОВІ ЧАСТОТНОГО АНАЛІЗУ КЛЮЧОВИХ СЛІВ

3. МЕТОДИ ТА ЗАСОБИ ОБРОБКИ СИГНАЛІВ

Ю.В. Стасев, А.А. Кузнецов, В.Н. Сай 135
СИНТЕЗ ДИСКРЕТНЫХ СИГНАЛОВ НА ОСНОВЕ СЕЧЕНИЯ ЦИКЛИЧЕСКИХ ОРБИТ ГРУППОВОГО КОДА И ИССЛЕДОВАНИЕ ИХ СВОЙСТВ
С.П. Белов, А.С. Белов 137
О ПОТЕНЦИАЛЬНЫХ ВОЗМОЖНОСТЯХ СЕЛЕКЦИИ ИНФОРМАЦИОННЫХ И НЕИНФОРМАЦИОННЫХ КОМПОНЕНТ РЕЧЕВЫХ СИГНАЛОВ
В.В. Баранник, В.В. Шинкарев 139
СЖАТОЕ ПРЕДСТАВЛЕНИЕ ДИФФЕРЕНЦИРОВАННЫХ ИЗОБРАЖЕНИЙ В СИСТЕМАХ АЄРОКОСМИЧЕСКОГО МОНИТОРИНГА

В.В. Палагін, О.А. Палагіна 141
ПОЛІНОМІАЛЬНИЙ ПІДХІД ДО ПОБУДОВИ МЕТОДІВ ТА СТРУКТУР СУМІСНИХ АЛГОРИТМІВ РОЗРІЗНЕННЯ СИГНАЛІВ ТА ОЦІНЮВАННЯ ЇХ ПАРАМЕТРІВ
Б.И. Исмайлов 143
КОНТРОЛЬ И АНАЛИЗ ВИБРАЦИОННЫХ СИГНАЛОВ ПО РЕКУРРЕНТНЫМ ДИАГРАММАМ
Т.В. Воробкало, О.С. Гавриш 144
АЛГОРИТМИ ВИМІРЮВАННЯ РАДІАЛЬНОЇ ШВИДКОСТІ ДЖЕРЕЛА ГАРМОНІЧНОГО СИГНАЛУ В РАДІОТЕХНІЧНИХ СИСТЕМАХ ПРИ НЕГАУССІВСЬКИХ ЗАВАДАХ
О.К. Колесницкий 146
ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ РАСПОЗНАВАНИЯ МНОГОМЕРНЫХ СИГНАЛОВ С ИСПОЛЬЗОВАНИЕМ ИМПУЛЬСНЫХ НЕЙРОННЫХ СЕТЕЙ
В.П. Семеренко, Н.С. Ткаченко 148
ПАРАЛЕЛЬНА ОБРОБКА БІНАРНИХ ЗОБРАЖЕНЬ В БІОМЕТРИЧНИХ СИСТЕМАХ ЗАХИСТУ
А.Г. Ведмедь, Е.С. Сакало 150
ВОССТАНОВЛЕНИЕ ИЗОБРАЖЕНИЙ С ИСПОЛЬЗОВАНИЕМ АНАЛИЗА ГЛАВНЫХ И НЕЗАВИСИМЫХ КОМПОНЕНТ
С.В. Омельченко, А.Ю. Трубчанинов 152
АВТОМАТИЧЕСКОЕ РАСПОЗНАВАНИЕ РЕЧЕВОЙ ИНФОРМАЦИИ
А.Г. Буда, Л.М. Куперштейн, О.М. Гуцол 154
ОСОБЛИВОСТІ КЛАСИФІКАЦІЇ СИГНАЛІВ ЗА ДИСКРИМІНАНТНИМИ ФУНКЦІЯМИ

В.В. Хом'юк, О.В. Дюдюн, М.В. Дзісь 156
МОДЕЛЮВАННЯ ПРОЦЕСІВ ОБРОБЛЕННЯ ТА КЛАСИФІКАЦІЇ СИГНАЛІВ ЗА РІЗНИЦЕВИМИ ЗРІЗАМИ
О.М. Ткаченко, О.В. Дзісь 158
РОЗПІЗНАВАННЯ ПЕРВИННИХ ОЗНАК ПРИ ПОБУДОВІ ФОНЕМНИХ ВОКОДЕРІВ
О.М. Ткаченко, О.Ф. Грійо Тукало 160
ПОШУК НАЙБЛИЖЧОГО ВЕКТОРА У КОДОВИХ КНИГАХ НА ОСНОВІ БІНАРНОГО ДЕРЕВА
Р.Б. Тушницький, І.В. Перевалова 162
ТРИСТУПЕНЕВИЙ МЕТОД ІЄРАРХІЧНОЇ ДЕКОМПОЗИЦІЇ ДЛЯ ПОБУДОВИ СКЕЛЕТОНІВ СКЛАДНОСТРУКТУРНИХ ЗОБРАЖЕНЬ
Р.В. Маслій 164
МЕТОД ВИЯВЛЕННЯ ОБЛИЧ НА ЗОБРАЖЕННІ З ВИКОРИСТАННЯМ МОДИФІКОВАНИХ ХААР-ПОДІБНИХ ОЗНАК
М.О. Рябий 166
ЗАСТОСУВАННЯ ФІЛЬТРІВ, ЗВОРОТНИХ ДО НИЗЬКОЧАСТОТНИХ ПРИ ОБРОБЦІ ЗОБРАЖЕНЬ
В.В. Мельніков 168
ЗАСТОСУВАННЯ МЕТОДІВ НАВЧАННЯ ПАРАЛЕЛЬНО-ІЄРАРХІЧНОЇ МЕРЕЖІ ДЛЯ РОЗПІЗНАВАННЯ ОБРАЗІВ
С.В. Хрущак 170
ДЕЛЬТА УЩІЛЬНЕННЯ МОВЛЕННЯ З ВИКОРИСТАННЯМ ІНТЕРВАЛЬНОГО ПРОГНОЗУВАННЯ
О.Д. Феферман 172
КЛАСТЕРИЗАЦІЯ МОВЛЕННЄВИХ ДАНИХ ПРИ СТВОРЕННІ КОДОВИХ КНИГ ДЛЯ УЩІЛЬНЕННЯ МОВИ

О.І. Прокопов 174
ВИМІРЮВАННЯ ОЦІНОК ПЕРІОДОГРАМ ІНТЕРФЕРЕНЦІЙНИХ СИГНАЛІВ
А.И. Молчановский, Нгием Лэ Куан 176
ПРОБЛЕМА СЕГМЕНТАЦИИ ДЛЯ ЗАДАЧИ ПОИСКА ИЗОБРАЖЕНИЙ
А.И. Молчановский, Буй Хиу Дат 178
МЕТОДОЛОГИЯ ТЕСТИРОВАНИЯ СИСТЕМ ПОИСКА ИЗОБРАЖЕНИЙ
А.И. Молчановский, В.А. Мистецкий 180
КЛАСТЕРИЗАЦИЯ ДАННЫХ ДЛЯ ЗАДАЧИ ПОИСКА ИЗОБРАЖЕНИЙ

4. ЗАХИСТ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

А.Я. Белецкий 183
СИНТЕЗ И АНАЛИЗ ГАРАНТИРОВАННО НЕВЫРОЖДЕННЫХ ШИФРУЮЩИХ (0, 1)-МАТРИЦ ВЫСОКОГО ПОРЯДКА
А.Я. Белецкий, Е.А. Аксентий 185
КОМПЛЕКС ПРОГРАММ ДЛЯ ИССЛЕДОВАНИЯ КРИПТОГРАФИЧЕСКИХ ПРИМИТИВОВ
А.Г. Корченко, В.Н. Кинзерявый, С.А. Гнатюк, А.Л. Панасюк 187
СИСТОЛИЧЕСКИЙ КРИПТОПРОЦЕССОР
Л.С. Сорока, А.А. Кузнецов, С.А. Исаев 189
ДИФФЕРЕНЦИАЛЬНЫЕ СВОЙСТВА МИНИ-ВЕРСИЙ БЛОЧНЫХ СИММЕТРИЧНЫХ ШИФРОВ

О.О. Кузнецов, Ю.М. Рябуха, Р.В. Сергієнко 191
ФОРМУВАННЯ ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ МАКСИМАЛЬНОГО ПЕРІОДУ ІЗ ВИКОРИСТАННЯМ ПЕРЕТВОРЕНЬ НА ЕЛІПТИЧНИХ КРИВИХ
В.Б. Дудикевич, Ю.Р. Гарасим 193
СТІЙКІСТЬ ТА ЖИВУЧІСТЬ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ В КОРПОРАТИВНИХ МЕРЕЖАХ ЗВ'ЯЗКУ
В.Б. Дудикевич, В.М. Стеренчук, Л.М. Ракобовчук 195
ЗАХИСТ ІНФОРМАЦІЇ В ПРОТОКОЛІ Н.323
В.Б. Дудикевич, І.Р. Опірський 197
КОМБІНОВАНА СИСТЕМА КОНТРОЛЮ ПОБІЧНОГО ВИПРОМІНЮВАННЯ ВОЛЗ
В.Б. Дудикевич, В.О. Ракобовчук 199
РЕАЛІЗАЦІЯ СИСТЕМИ БЕЗПЕКИ ЛОКАЛЬНОЇ ОБЧИСЛЮВАЛЬНОЇ МЕРЕЖІ З ДОСТУПОМ В ІНТЕРНЕТ НА БАЗІ FREEBSD
В.В. Хома 201
КРИПТОЛОГІЧНИЙ ПАКЕТ CRYPTOOL ТА ЙОГО ЗАСТОСУВАННЯ У НАВЧАЛЬНОМУ ПРОЦЕСІ
А.Д. Кожухівський, А.В. Сагун, О.А. Кожухівська 203
МАТЕМАТИЧНА МОДЕЛЬ АПАРАТНОЇ ЧАСТИНИ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ
В.И. Стецюренко, А.С. Чашинский, А.Г. Лукошко 205
ПРОГРАММНО-АППАРАТНЫЙ КОМПЛЕКС КРИПТОЗАЩИТЫ КАНАЛОВ СВЯЗИ

А.Д. Буханцов 207
О ПОДХОДЕ К СОВЕРШЕНСТВОВАНИЮ АЛГОРИТМА ЗАЩИТЫ ИНФОРМАЦИИ В СИСТЕМАХ МОБИЛЬНОЙ СВЯЗИ
І.А. Золотарьова, Н.А. Кошева 209
ЗАХИСТ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ В СИСТЕМАХ ДИСТАНЦІЙНОГО НАВЧАННЯ
В.Ю. Ковтун, С.П. Евсеев, О.Г. Король 211
АУТЕНТИФИКАЦИЯ ДАННЫХ С ИСПОЛЬЗОВАНИЕМ КЛЮЧЕВЫХ ХЕШИРУЮЩИХ ФУНКЦИЙ
С.А. Головашич, С.П. Евсеев, И.В. Московченко 213
ОЦЕНКА ЭФФЕКТИВНОСТИ ПРОЕКТИРОВАНИЯ АЛГОРИТМА БЛОЧНОГО СИММЕТРИЧНОГО ШИФРОВАНИЯ
С.П. Евсеев, А.И. Гончарова 215
ПОСТРОЕНИЕ МОДЕЛЕЙ АТАК НА ВНУТРИПЛАТЕЖНЫЕ БАНКОВСКИЕ СИСТЕМЫ
А.В. Петрашенко, Д.С. Замятин 217
МЕТОДЫ РАЗГРАНИЧЕНИЯ ДОСТУПА В НЕСТРУКТУРИРОВАННЫХ ТЕКСТОВЫХ ХРАНИЛИЩАХ
С.Б. Приходько 219
ЗАЩИЩЕННАЯ ПЕРЕДАЧА ЦИФРОВОЙ ИНФОРМАЦИИ НА ОСНОВЕ МАНИПУЛЯЦИИ БЕЛОГО ШУМА С ОГРАНИЧЕННОЙ ПОЛОСОЙ
В.А. Золотарьов 221
ВИБІР ТЕХНОЛОГІЙ ЗАХИСТУ ДАНИХ В КАНАЛАХ ЗВ'ЯЗКУ

И.Б. Трегубенко, О.В. Коваль 223
СТРАТЕГИЯ ЗАЩИТЫ ВИРТУАЛЬНЫХ ИНФОРМАЦИОННЫХ СТРУКТУР
Б.П. Томашевский 225
АНАЛИЗ ИЗВЕСТНЫХ МЕТОДОВ ПОСТРОЕНИЯ ШИФРОСИСТЕМ ДОКАЗУЕМОЙ СТОЙКОСТИ, ОБОСНОВАНИЕ КРИТЕРИЕВ И ПОКАЗАТЕЛЕЙ ИХ ЭФФЕКТИВНОСТИ
М.П. Боцула, І.А. Моргун 227
ПІДХІД ДО РОЗМЕЖУВАННЯ ПРАВ ДОСТУПУ В СИСТЕМІ ЕКСПЕРТНОЇ ОЦІНКИ МАТЕРІАЛІВ ДИСТАНЦІЙНИХ КУРСІВ
С.И. Приходько, Г.С. Цымбал 229
ПОИСК НЕЛИНЕЙНОЙ ФУНКЦИИ ДЛЯ НЕЛИНЕЙНЫХ УЗЛОВ ЗАМЕН АЛГОРИТМОВ ПОТОЧНОГО ШИФРОВАНИЯ
А.А.Смирнов, В.В. Босько 231
ДИНАМИЧЕСКОЕ УПРАВЛЕНИЕ ПРОЦЕССОМ МАРШРУТИЗАЦИИ ДАННЫХ В ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ
А.О. Поляков, І. Юрченко 233
НЕПЕРЕРВНІСТЬ ДОКУМЕНТООБІГУ З ВИКОРИСТАННЯМ МАРКЕРУ ДОСТУПУ
Д.А. Стеценко 235
МАТРИЧНЕ ШИФРУВАННЯ ДАНИХ З МОДИФІКАЦІЄЮ СЕКРЕТНОГО КЛЮЧА
А.В. Оводенко, С.А. Клюев 237
ИСПОЛЬЗОВАНИЕ ЧАСТОТНЫХ ХАРАКТЕРИСТИК ЯЗЫКА ПРИ ЭКСПЛУАТАЦИИ SQL ИНЪЕКЦИЙ

Б.Д. Будз 239
АКУСТИЧНИЙ КАНАЛ ВИТОКУ ІНФОРМАЦІЇ З ПЕРСОНАЛЬНИХ КОМП'ЮТЕРІВ
В.М. Карпінський 241
ВИБРАНІ АСПЕКТИ БЕЗПЕКИ ТА МОДЕЛЮВАННЯ БЕЗПРОВІДНИХ СЕНСОРНИХ МЕРЕЖ
В.С. Похил 243
МЕТОД ОЦЕНИВАНИЯ ФУНКЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ ИНФОРМАЦИОННО-УПРАВЛЯЮЩИХ СИСТЕМ БОРТОВОЙ АВИОНИКИ
О.В. Клювак 245
АНАЛІЗ ПІДХОДІВ ДО ВИРІШЕННЯ ЗАДАЧІ ЗАХИСТУ ДАНИХ ВІД НЕСАНКЦІОНОВАНОЇ ЗМІНИ В ІНТЕРНЕТ-ПЛАТІЖНИХ СИСТЕМАХ
В.А. Лужецький, М.Л. Гаєвський 247
ШВИДКІ КРИПТОГРАФІЧНІ ПЕРЕТВОРЕННЯ НА ОСНОВІ СИСТЕМ АЛГЕБРАЇЧНИХ ПОРІВНЯНЬ
В.А. Лужецький, В.В. Кичак 249
ПРИШВИДШЕННЯ ПРОЦЕСУ ОБЧИСЛЕННЯ ЗНАЧЕНЬ ХЕШ-ФУНКЦІЙ ПОБУДОВАНИХ НА ЕЛІПТИЧНИХ КРИВИХ
В.А. Лужецький, О.В. Філіппов 251
ХЕШУВАННЯ ДАНИХ З НЕРІВНОМІРНИМ РОЗБИТТЯМ НА БЛОКИ
В.П. Семеренко, Джан Янг 253
GSM-КОНТРОЛЕРИ ДЛЯ СИГНАЛІЗАЦІЇ ТА КЕРУВАННЯ

В.П. Семеренко, А.Ф. Дубров 255
ОБЪЕДИНЕНИЕ КРИПТОГРАФИИ И ПОМЕХОУСТОЙЧИВОГО КОДИРОВАНИЯ
В.А. Лужецький, А.В. Остапенко 257
МЕТОД БЛОКОВОГО ШИФРУВАННЯ НА ОСНОВІ ПСЕВДОВИПАДКОВОЇ ПОСЛІДОВНОСТІ КРИПТОПРИМІТИВІВ
О.П. Войтович 259
ДОСТОВІРНІСТЬ ПРИЙНЯТТЯ РІШЕННЯ В СИСТЕМАХ ЗАХИСТУ ІНФОРМАЦІЇ
Ю.П. Гульчак, Н.Ю. Харитонова 261
ОЦІНЮВАННЯ ПРОНИКНОЇ ЗДАТНОСТІ АКУСТИЧНИХ СИГНАЛІВ БУДІВЕЛЬНИХ КОНСТРУКЦІЙ
А.В. Дудатьєв,І. В. Шнайдер 263
ОЦІНЮВАННЯ ТА ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В СОЦІОТЕХНІЧНИХ СИСТЕМАХ
С.В. Князюк 266
БЕЗПЕКА ПРИВАТНОГО ЖИТТЯ В ГЛОБАЛЬНІЙ МЕРЕЖІ ІНТЕРНЕТ
Ю.В. Баришев 268
МАТЕМАТИЧНА МОДЕЛЬ ПСЕВДОНЕДЕТЕРМІНОВАНОГО ХЕШУВАННЯ ТА КРИПТОГРАФІЧНІ ПРИМІТИВИ ДЛЯ ЇЇ РЕАЛІЗАЦІЇ
О.В. Дмитришин 270
ВИКОРИСТАННЯ ОПЕРАЦІЇ МНОЖЕННЯ ЗА СЕКРЕТНИМ ЗНАЧЕННЯМ МОДУЛЯ
І.В. Бугорська 272
ПІДХОДИ ДО РЕЛІЗАЦІЇ ПЕРЕСТАНОВОК У БЛОКОВИХ ШИФРАХ

В.М. Дудатьєва, А.О. Гнатюк 274
ПСИХОЛОГІЧНІ АСПЕКТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

5. МОДЕЛЮВАННЯ КОМП'ЮТЕРНИХ СИСТЕМ ТА КОМПОНЕНТІВ

В.Б. Дудикевич, Н.М. Лужецька, А.Я. Горпенюк 277
ДОСЛІДЖЕННЯ КОНВЕЄРНОЇ СТРУКТУРИ СТЕПЕНЕВОГО ЧИСЛО-ІМПУЛЬСНОГО ФУНКЦІОНАЛЬНОГО ПЕРЕТВОРЮВАЧА

В.С. Осадчук, О.В. Осадчук, Ю.С. Кравченко, О.О. Селецька 279
ОПТИЧНИЙ ЧАСТОТНИЙ ПЕРЕТВОРЮВАЧ ДЛЯ ВИЗНАЧЕННЯ ЧАСУ ПЛАЗМОХІМІЧНИХ ПРОЦЕСІВ

О.В. Осадчук, Р.В. Криночкін, С.В. Барабан 281
СИСТЕМА КОНТРОЛЮ ТЕМПЕРАТУРИ НА ОСНОВІ ЧАСТОТНИХ ПЕРЕТВОРЮВАЧІВ З ВІД'ЄМНИМ ОПОРОМ

В.П. Кожем'яко, О.В. Кириченко 283
СПОСІБ ПАРАЛЕЛЬНОГО ФОРМУВАННЯ УЩІЛЬНЕННОЇ СУМИ ЧАСОІМПУЛЬСНИХ СИГНАЛІВ

В.П. Кожем'яко, С.В. Дусанюк, Л.О. Волонтир 285
МОДЕЛЮВАННЯ ПРОЦЕСУ ВІДТВОРЕННЯ ЗОБРАЖЕНЬ НА ОСНОВІ ЛОГІКО-ЧАСОВОГО БАЗИСУ

В.П. Кожем'яко, О.А. Іванов, І.А. Іванов 287
ЗАСТОСУВАННЯ ФОТОННИХ КРИСТАЛІВ У СУЧАСНИХ СИСТЕМАХ ОБРОБКИ ІНФОРМАЦІЇ

Й.Й. Білинський, К.Ю. Іоніна, В.В. Онушко 289
СЕНСОР ВОЛОГОСТІ НА ОСНОВІ СВІТЛОВОДНОЇ СТРУКТУРИ
В.І. Гавриш, Д.В. Федасюк, А.І. Косач 291
МОДЕЛЮВАННЯ НЕЛІНІЙНИХ ТЕПЛОВИХ ПРОЦЕСІВ ДЛЯ КРИСТАЛУ НА БАГАТОШАРОВІЙ ПІДКЛАДЦІ
Э.Е. Герман 293
НЕЧЕТКИЕ ПИД КОНТРОЛЛЕРЫ ДЛЯ СИСТЕМ УПРАВЛЕНИЯ НЕСТАЦИОНАРНЫМИ ОБЪЕКТАМИ
Н.М. Чайківський, О.М. Пігур-Пастернак 295
РОЗРОБКА СИСТЕМИ ДОСЛІДЖЕННЯ АУДІО-ДАНИХ
И.В. Гормакова 297
МЕТОДЫ СИНТЕЗА ПОСЛОВНО-ПОСЛЕДОВАТЕЛЬНЫХ УМНОЖИТЕЛЕЙ, ОПЕРИРУЮЩИХ В ПОЛЯХ ГАЛУА
Л.І. Д'яченко, Є. В. Мінов, С.Е. Остапов, П.М. Фочук 299
МОДЕЛЮВАННЯ ПАРАМЕТРІВ ПІДСИСТЕМИ ТОЧКОВИХ ДЕФЕКТІВ У НАПІВПРОВІДНИКОВИХ КРИСТАЛАХ
В.П. Кожем'яко, А.Д. Слободяник 301
АЛГОРИТМИ АВТОМАТИЗОВАНОЇ РОБОТИ КВАНТОВО-ХВИЛЬОВОГО СПЕКТРОЕНЕРГЕТИЧНОГО ПЕРЕТВОРЮВАЧА В ІНФОРМАЦІЙНО-ЕНЕРГЕТИЧНИХ МЕРЕЖАХ
В.Г. Дейбук, Г.П. Горський 303
МОДЕЛЮВАННЯ ЧАСТОТНОГО ШУМУ В РОБОТІ УНІВЕРСАЛЬНОГО КВАНТОВОГО ВЕНТИЛЯ ФРЕДКІНА

Л.Б. Ліщинська, Я.С. Рожкова, М.В. Барабан, М.А. Філинюк 305
ДОСЛІДЖЕННЯ «ЯКОСТІ» ОДНОКРИСТАЛЬНИХ УПІ
В.С. Осадчук, О.В. Осадчук, О.М. Ільченко 307
ЧАСТОТНИЙ ПЕРЕТВОРЮВАЧ ОПТИЧНОГО ВИПРОМІНЮВАННЯ НА ОСНОВІ ДВОХ МДН-ТРАНЗИСТОРІВ
В. М. Кичак, Г.Г. Бортник, Н.О. Пунченко 309
МОДЕЛЮВАННЯ АНАЛОГО-ЦИФРОВИХ ПЕРЕТВОРЮВАЧІВ
Л.Р. Бекирова 311
ЗАДАЧА ПОВЫШЕНИЯ БЫСТРОДЕЙСТВИЯ СПЕКТРОМЕТРИЧЕСКОЙ СИСТЕМЫ
К.В. Огородник, Л.Б. Ліщинська, С.Є. Фурса 313
ПРОГРАМА ДЛЯ РОЗРАХУНКУ ПАРАМЕТРІВ ПОТЕНЦІЙНО-НЕСТІЙКИХ ЧОТИРИПОЛЮСНИКІВ
В.А. Висоцька, Л.В. Чирун 315
ФОРМАЛЬНІ МОДЕЛІ СИСТЕМИ КЕРУВАННЯ КОНТЕНТОМ
Р.П. Шевчук, В.Й. Бегман 317
АНАЛІЗ МЕТОДІВ ОЦІНКИ ЯКОСТІ ПЕРЕДАЧІ МОВНИХ СИГНАЛІВ У ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ
А.В. Кожем'яко, Ю.О. Панасюк, А.В. Лілевський 319
ОДНОРІДНА СТРУКТУРА У СКЛАДІ КЛАСИФІКАТОРА СИГНАЛІВ
Г.Г. Бортник, М.Л. Мінов 321
МЕТОД КОРИГУВАННЯ НЕЛІНІЙНОСТІ АЦП

Т.Н. Боровская, Е.П. Хомин 323
ТЕХНОЛОГИИ КОНСТРУИРОВАНИЯ МОДЕЛЕЙ MNK-КЛАССА
Г.Г. Бортник, М.В. Васильківський, Л.Ф. Мінов 325
МЕТОД ПІДВИЩЕННЯ ТОЧНОСТІ ОЦІНЮВАННЯ СКЛАДОВИХ ДЖИТЕРУ В ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ
Т.Б. Мартинюк, І.В. Бондарчук, Є.В. Дубінін 327
НЕЙРОМЕРЕЖНИЙ КЛАСИФІКАТОР НА БАЗІ ПЕРСЕПТРОНА
А.А. Яровий, Р.С. Власюк, О.В. Крейчі 329
КОМП’ЮТЕРНЕ МОДЕЛЮВАННЯ НЕЙРОМЕРЕЖЕВОЇ ІНТЕЛЕКТУАЛЬНОЇ СИСТЕМИ ДЛЯ ЗАДАЧ ПРОГНОЗУВАННЯ СКЛАДОВИХ ХАРАКТЕРИСТИК ПРОФІЛЮ ЛАЗЕРНОГО ПРОМЕНЯ
І.Р. Арсенюк, О.Л. Зозовський 331
СИСТЕМА ПЕРЕДАЧІ ПОТОКОВИХ ДАНИХ В КОМП’ЮТЕРНИХ МЕРЕЖАХ
І.С. Колесник, І.І. Михайлова 333
МОДЕЛІ КОМП’ЮТЕРНИХ СИСТЕМ НА БАЗІ КОНЦЕПЦІЇ «РОЗПОДІЛ ВИРОБНИЦТВА»
І.С. Колесник, І.І. Михайлова 335
МОДЕЛЬ КОМП'ЮТЕРНОЇ СИСТЕМИ НА БАЗІ КОНЦЕПЦІЇ «МАСОВЕ ОБСЛУГОВУВАННЯ»
К.К. Кадомский, А.А. Каргин 337
КОНЦЕПТУАЛЬНАЯ МОДЕЛЬ СИСТЕМЫ УПРАВЛЕНИЯ МОБИЛЬНЫМ РОБОТОМ
А.Л. Карасёв, С.П. Дементьев 339
АНАЛИЗ СПИСКА СОЕДИНЕНИЙ СИНТЕЗИРУЕМЫХ HDL – МОДЕЛЕЙ ЦИФРОВЫХ СИСТЕМ

А.М. Царенко 341
ПРОГРАМНІ ЗАСОБИ ФОРМУВАННЯ ПЕРЕДАВАЛЬНОЇ ФУНКЦІЇ ЦИФРОВИХ ФІЛЬТРІВ З ГІПЕРКОМПЛЕКСНИМИ КОЕФІЦІЄНТАМИ

6. ВІДМОВОСТІЙКІ КОМП'ЮТЕРНІ СИСТЕМИ ТА КОМПОНЕНТИ

Л. В. Дербунович, М.А. Бережная, Я. Ю. Королева 344
ДИАГНОСТИЧЕСКАЯ ИНФРАСТРУКТУРА С ИНТЕЛЛЕКТУАЛЬНЫМИ СВОЙСТВАМИ В РЕКОНФИГУРИРУЕМЫХ МУЛЬТИПРОЦЕССОРНЫХ СИСТЕМАХ
Л.В. Дербунович, Д.Г. Караман 346
СИНТЕЗ САМОПРОВЕРЯЕМЫХ МОДУЛЕЙ ЗАЩИТЫ ДАННЫХ С ИСПОЛЬЗОВАНИЕМ САМОДВОЙСТВЕННЫХ ФУНКЦИЙ
А.А. Борисенко, А.Е. Горячев, Е.Л. Онанченко 348
ОБНАРУЖЕНИЕ И ИСПРАВЛЕНИЕ ОШИБОК В ПЕРЕСТАНОВКАХ
А.А. Борисенко, Д.В. Гутенко 350
ПРИНЦИПЫ ПОСТРОЕНИЯ ДЕШИФРАТОРОВ РАВНОВЕСНЫХ КОДОВ
А.А. Борисенко, В.В. Петров, С.Ю. Булатов 352
ОЦЕНКА ПОМЕХОУСТОЙЧИВОСТИ МАТРИЧНЫХ БИНОМИАЛЬНЫХ КОНЕЧНЫХ АВТОМАТОВ
О.Д. Азаров, О.В. Кадук, А.Г. Бас 354
ПЕРЕТВОРЕННЯ «АНАЛОГ – РОБОЧИЙ КОД – ЦИФРОВИЙ ЕКВІВАЛЕНТ» В АЦП, ЩО САМОКАЛІБРУЮТЬСЯ, З ВАГОВОЮ НАДЛИШКОВІСТЮ

О.Д. Азаров, О.В. Дудник, А.О. Росощук 356
ПЕРЕТВОРЕННЯ «ЦИФРОВИЙ ЕКВІВАЛЕНТ – РОБОЧИЙ КОД – АНАЛОГ» В ЦАП, ЩО САМОКАЛІБРУЮТЬСЯ, З ВАГОВОЮ НАДЛИШКОВІСТЮ
О.Д. Азаров, В.В. Рибак 358
ВИСОКОТОЧНІ ФУНКЦІОНАЛЬНІ ГЕНЕРАТОРИ АНАЛОГОВИХ СИГНАЛІВ НА ОСНОВІ ЦАП З ВАГОВОЮ НАДЛИШКОВІСТЮ
О.Д. Азаров, В.А. Гарнага, М.Ю. Теплицький 360
МОДЕЛІ АЧХ І ФЧХ ДВОТАКТНИХ ПІДСИЛЮВАЧІВ СТРУМУ НА ОСНОВІ СХЕМ ЗАМІЩЕННЯ ТРАНЗИСТОРІВ У ФОРМАТІ SPICE
О.Д. Азаров, О.Г. Муращенко 362
АЦП ПОРОЗРЯДНОГО НАБЛИЖЕННЯ З АНТИГЛІЧЕВИМ КОДУВАННЯМ
О.Д. Азаров, **М.Ю. Шабатура** 364
КОМПЕНСАЦІЯ ДИНАМІЧНИХ ПОХИБОК ПРИ ПРИСКОРЕНОМУ ПОРОЗРЯДНОМУ АНАЛОГО-ЦИФРОВОМУ ПЕРЕТВОРЕННІ З ВАГОВОЮ НАДЛИШКОВІСТЮ
В.М. Кичак, И.Ю. Кравцов 366
МЕТОД КОМПЕНСАЦИИ ПОМЕХ В АДАПТИВНЫХ АНТЕННЫХ РЕШЕТКАХ
Ю.О. Гунченко, О.В. Банзак 368
ПІДВИЩЕННЯ ЗАВАДОСТІЙКОСТІ МІКРОПРОЦЕСОРНИХ СИСТЕМ
И.А. Кулик, Е.М. Скордина 370
ФОРМИРОВАНИЕ КВАЗИРАВНОВЕСНЫХ КОДОВ НА ОСНОВЕ ДВОИЧНЫХ БИНОМИАЛЬНЫХ ЧИСЕЛ

А.М. Романкевич, А.В. Шурига 372
К ПРОБЛЕМЕ РАСЧЕТА НАДЕЖНОСТИ ОТКАЗОУСТОЙЧИВЫХ МНОГОПРОЦЕССОРНЫХ СИСТЕМ
М.О. Іщенко, О.Д. Персин, М.Ю. Балута 374
ЗАВАДОСТІЙКІСТЬ СИСТЕМИ ПЕРЕДАВАННЯ З ПРОСТОРОВО-ЧАСОВИМ КОДУВАННЯМ
Л.В. Крупельницький, О.О. Решетнік 375
СТРУКТУРНА І АЛГОРИТМІЧНА ОРГАНІЗАЦІЯ ШВИДКОДІЮЧИХ АЦП ПОРОЗРЯДНОГО ВРІВНОВАЖЕННЯ І ЦАП З ВАГОВОЮ НАДЛИШКОВІСТЮ
С. Альмадхоун, Е.Е. Сыревич, А.С. Шкиль 377
ПОИСК ОШИБОК ПРОЕКТИРОВАНИЯ В HDL– МОДЕЛЯХ ЦИФРОВЫХ УСТРОЙСТВ
В.А. Романкевич, К.В. Морозов 379
ОБ ОПТИМИЗАЦИИ ВЫЧИСЛЕНИЯ РЕБЕРНЫХ ФУНКЦИЙ В GL-МОДЕЛЯХ
Э.В. Фауре, Р. О. Бивзюк 381
МЕТОДЫ И СРЕДСТВА ФОРМИРОВАНИЯ ОСТАТКОВ В МНОГОКАНАЛЬНЫХ ПОМЕХОУСТОЙЧИВЫХ КОДЕКАХ
С.М. Захарченко, О.В. Бойко 383
САМОКАЛІБРОВАНИЙ ЦИКЛІЧНИЙ АЦП ІЗ ВАГОВОЮ НАДЛИШКОВІСТЮ
І.Д. Прокопов, О.І. Прокопов 385
ЦИФРОВІ ФІЛЬТРИ НА ПЛІС В СИСТЕМАХ ПЕРЕДАЧІ СИГНАЛІВ
В.Е. Федюкович 387
ПРОТОКОЛ АРГУМЕНТА ДЛЯ СЛОВА КОДА ГОППЫ И ОШИБКИ ОГРАНИЧЕННОГО ВЕСА

Л.Ю. Юрчук, С.В. Жульжик 389
ВИБІР ОПТИМАЛЬНОЇ КОНФІГУРАЦІЇ ВІДМОВОСТІЙКОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ
Л.А. Савицька 391
СПЕЦІАЛІЗОВАНИЙ ПРОЦЕСОР ДЛЯ УЩІЛЬНЕННЯ ДАНИХ
О.Д. Азаров, В.А. Гарнага 393
ДВОТАКТНІ ПІДСИЛЮВАЧІ ПОСТІЙНОГО СТРУМУ ДЛЯ БАГАТОРОЗРЯДНИХ АЦП І ЦАП ІЗ ВАГОВОЮ НАДЛИШКОВІСТЮ, ЩО САМОКАЛІБРУЮТЬСЯ
О.О. Решетнік 395
СУЧАСНІ ВИСОКОПРОДУКТИВНІ АЦП ПОРОЗРЯДНОГО ВРІВНОВАЖЕННЯ
С.В. Богомолов 397
СХЕМНА ОРГАНІЗАЦІЯ ВХІДНОГО КОМПЛЕМЕНТАРНОГО КАСКАДУ ДВОТАКТНОГО СИМЕТРИЧНОГО ПІДСИЛЮВАЧА ПОСТІЙНОГО СТРУМУ

7. ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ОСВІТІ, ЕКОЛОГІЇ ТА ЕКОНОМІЦІ

Б.І. Мокін, А.В. Писклярова 400
СИНТЕЗ МАТЕМАТИЧНИХ МОДЕЛЕЙ РІВНІВ СИНЕРГЕТИЧНОЇ УНІВЕРСИТЕТСЬКОЇ СИСТЕМИ
А.А. Тимченко 402
ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ДОКУМЕНТУВАННЯ ЖИТТЄДІЯЛЬНОСТІ

Б.І. Медведенко 404
ЗАСТОСУВАННЯ ТЕХНОЛОГІЇ «ELECTRONICS WORKBENCH» У ВИВЧЕННІ ДИСЦИПЛІН РАДІОЕЛЕКТРОННОГО ПРОФІЛЮ
В.Н. Анохин, В.В. Огурцов 406
ТРЕБОВАНИЯ К СОВРЕМЕННЫМ ЭЛЕКТРОННЫМ УЧЕБНЫМ МАТЕРИАЛАМ И РАСЧЁТ ТРУДОЗАТРАТ НА ИХ РАЗРАБОТКУ
А.М. Мельник, Р.М. Пасічник 408
СИСТЕМА АВТОМАТИЧНОЇ ГЕНЕРАЦІЇ ТЕСТОВИХ ЗАВДАНЬ
В.В. Войтко, С.В. Бевз, О.В. Гавенко 410
ПРОГРАМА ДЛЯ ПЕРЕВІРКИ ТЕКСТІВ НА ПЛАГІАТ
Є.В. Буров 412
ОПРАЦЮВАННЯ ЗНАНЬ В ІНТЕЛЛЕКТУАЛЬНІЙ ІНФОРМАЦІЙНІЙ СИСТЕМІ КЕРОВАНІЙ МОДЕЛЯМИ
П.О. Кравець 414
ІГРОВА МОДЕЛЬ З АРБІТРОМ КОЛЕКТИВНИХ РІШЕНЬ В УМОВАХ НЕВИЗНАЧЕНОСТІ
П.А. Помилуйко 417
ИНТЕЛЛЕКТУАЛЬНЫЕ ВЕБ-АГЕНТЫ ДЛЯ ПОИСКА И ПУБЛИКАЦИИ ИНФОРМАЦИИ
Д.Ю. Явтушкевич 419
АДАПТИВНІ КОМП'ЮТЕРНІ СИСТЕМИ В НАВЧАННІ

В.Б. Мокін, Л.М. Скорина 421
НОВИЙ ПІДХІД ЩОДО АВТОМАТИЗАЦІЇ ОПТИМІЗАЦІЇ ВПЛИВУ ПРОТИПАВОДКОВИХ СПОРУД НА ВОДНІ ОБ’ЄКТИ
В.Б. Мокін, В.Г. Сторчак 423
НОВИЙ ПІДХІД ДО ІДЕНТИФІКАЦІЇ ТА ФОРМАЛІЗАЦІЇ ГЕОІНФОРМАЦІЙНОЇ МОДЕЛІ ТРАНСПОРТНОЇ МЕРЕЖІ НА ОСНОВІ
ГІС-МОДЕЛЕЙ ЇЇ ЕЛЕМЕНТІВ
В.Б. Мокін, Д.Ю. Кульомін 425
АВТОМАТИЗАЦІЯ ПЕРЕВІРКИ ІНФОРМАЦІЙНОЇ ПОВНОТИ ТА НЕСУПЕРЕЧЛИВОСТІ В ГЕОІНФОРМАЦІЙНИХ СИСТЕМАХ ЕКОЛОГІЧНОГО МОНІТОРИНГУ ТА УПРАВЛІННЯ
В.Б. Мокін, В.Ю. Булига, К.Ю. Вознесенський 427
НОВИЙ ПІДХІД ДО МОДЕЛЮВАННЯ ЯКОСТІ ВОДИ У РІЧКОВИХ СИСТЕМАХ З ВИКОРИСТАННЯМ ЗАСОБІВ ПАРАЛЕЛЬНИХ ОБЧИСЛЕНЬ
В.Б. Мокін, Н.В. Гончар 430
ВИКОРИСТАННЯ ГІС-ТЕХНОЛОГІЙ ДЛЯ АНАЛІЗУ ПОТЕНЦІАЛУ ЗМЕНШЕННЯ ВИКИДІВ
ПРОМИСЛОВОСТІ УКРАЇНИ ЗА РАХУНОК ПРОЕКТІВ СПІЛЬНОГО ВПРОВАДЖЕННЯ
М.П. Боцула 432
ПРО ФОРМАЛІЗАЦІЮ ДАНИХ ЕКОЛОГІЧНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

Г.В. Горячев 434
СТВОРЕННЯ ІНФОРМАЦІЙНИХ РЕСУРСІВ ЕКОЛОГІЧНОГО МОНІТОРИНГУ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ WEB 2.0
Р.М. Пасічник, А.В. Ковбасістий 436
ПРОГНОЗУВАННЯ ОБСЯГІВ ВИПЛАТ СТРАХОВИХ КОМПАНІЙ
Є.Н. Федорчук, Н.М. Ткаченко 438
АЛГОРИТМ УПРАВЛІННЯ ІННОВАЦІЙНОЮ МОДЕЛЛЮ ВИРОБНИЧОГО КОМПЛЕКСУ
В.А. Северилов, Г.Ю. Дерман 440
МОДЕЛИ ДЛЯ АНАЛИЗА РИСКОВ РАЗВИТИЯ
Н.Р. Кондратенко, С.В. Лужецький 442
ІНФОРМАЦІЙНА СИСТЕМА ДЛЯ ПІДБОРУ ТА ОЦІНЮВАННЯ ПЕРСОНАЛУ
О.М. Кузьміна, Л.М. Захарченко 444
СУЧАСНИЙ АНАЛІЗ ДИНАМІКИ РОЗВИТКУ ЕКОНОМІЧНОЇ ДІЯЛЬНОСТІ ПІДПРИЄМСТВА ЗАСОБАМИ КОМП’ЮТЕРНОГО КОМПЛЕКСУ PROJECT EXPERT
Р.В. Резниченко 447
МОДЕЛЬ РАСПРЕДЕЛЕНИЯ ПРИБЫЛИ МЕЖДУ ПАРТНЕРАМИ ВИРТУАЛЬНЫХ ПРЕДПРИЯТИЙ
М.Ю. Лесів 449
ГЕОІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ПРОСТОРОВОГО АНАЛІЗУ ПРОЦЕСІВ ЕМІСІЇ ДІОКСИДУ ВУГЛЕЦЮ З ВРАХУВАННЯМ РОЗИ ВІТРІВ

С.П. Дерлеменко 451
ЗАДАЧА ОПТИМАЛЬНОГО РОЗПОДІЛУ ДЕКЛАРАЦІЙ З ПДВ МІЖ ІНСПЕКТОРАМИ В ІНФОРМАЦІЙНІЙ ТЕХНОЛОГІЇ АДМІНІСТРУВАННЯ ПОДАТКУ НА ДОДАНУ ВАРТІСТЬ
О.В. Чеборака, О.А. Ткачук 453
ПРОГНОЗУВАННЯ СОЦІАЛЬНО-ЕКОНОМІЧНИХ ПРОЦЕСІВ НА ОСНОВІ ІНТЕРВАЛЬНИХ НЕЧІТКИХ МНОЖИН ТИПУ-2

8. ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В МЕДИЦИНІ

С.М. Злепко, С.В. Павлов, А.П. Моторний 456
ІНФОРМАЦІЙНІ ОПТИКО-ЕЛЕКТРОННІ ТЕХНОЛОГІЇ ВИЗНАЧЕННЯ ФУНКЦІОНАЛЬНОГО СТАНУ ЛЮДИНИ-ОПЕРАТОРА
С.М. Злепко, О.П. Азархов, С.В. Костішин 458
ОЦІНЮВАННЯ ЯКОСТІ РЕАБІЛІТАЦІЙНОГО ПРОЦЕСУ НЕВРОЛОГІЧНИХ ХВОРИХ В УМОВАХ САНАТОРІЮ
Б.І. Яворський, Р.А. Ткачук 460
ПОБУДОВА ПРОТОТИПУ ЕКСПЕРТНОЇ СИСТЕМИ ДОСЛІДЖЕННЯ НЕЙРОТОКСИКАЦІЇ ЛЮДИНИ МЕТОДОМ ЕЛЕКТРОРЕТИНОГРАФІЇ
В.В. Фалендиш, Б.І. Яворський, М.В. Бачинський 462
ОЦІНЮВАННЯ ФУНКЦІОНАЛЬНОГО СТАНУ ЛЮДИНИ ЗА ВАРІАБЕЛЬНІСТЮ СЕРЦЕВОГО РИТМУ

Н.Т. Абдуллаев, О.А. Дышин, А.Д. Джабиева 464
АНАЛИЗ НЕСТАБИЛЬНОСТИ ВРЕМЕННОГО РЯДА КАРДИОИНТЕРВАЛОВ С ТОЧКИ ЗРЕНИЯ САМООРГАНИЗОВАННОЙ КРИТИЧНОСТИ
Н.Т. Абдуллаев, А.С. Аббаскулиев, К.Ш. Исмаилова 466
ПОДХОД К ОБРАБОТКЕ ЭЛЕКТРОМИОГРАФИЧЕСКИХ СИГНАЛОВ С ПОМОЩЬЮ АППАРАТА НЕЧЕТКИХ МНОЖЕСТВ
Л.С. Годлевский, И.В. Хихловская 468
ЦВЕТОВОЕ КОДИРОВАНИЕ ИЗОБРАЖЕНИЙ В МЕДИЦИНЕ
О.М. Роїк, Н.А. Дудатьєва 470
ПІДХІД ДО КЛАСИФІКАЦІЇ ЕКСТРЕМАЛЬНИХ СТАНІВ ЛЮДИНИ
Й.Й. Білинський, А.О. Мельничук, Т.М. Крисак 472
МЕТОД СЕГМЕНТАЦІЇ БІОЛОГІЧНИХ ОБ’ЄКТІВ УЛЬТРАЗВУКОВИХ ЗОБРАЖЕНЬ
С.В. Павлов, Р.В. Просоловский, Т.І. Козловська 474
ОПТИЧНІ ТЕХНОЛОГІЇ В КОНТЕКСТІ РЕАЛІЗАЦІЇ ІНТЕЛЕКТУАЛЬНИХ БІООКО-ПРОЦЕСОРНИХ ОПТИКО-ЕЛЕКТРОННИХ СИСТЕМ
Є.Б. Яворська, О.В. Гевко 476
МЕТОД РОЗДІЛЕННЯ СУМІШІ ЦИКЛОСТАЦІОНАРНИХ БІОСИГНАЛІВ
Н.Б. Шаховська, Н.І. Мельникова 478
ІНФОРМАЦІЙНА МОДЕЛЬ ЛІКУВАЛЬНИХ СИСТЕМ ПИЙНЯТТЯ РІШЕНЬ
Ю.П. Гульчак, Е.Ю. Гульчак 480
ПРОГРАМА ІМІТАТОР КОМП’ЮТЕРНОГО МОДЕЛЮВАННЯ ЗУБНИХ ПРОТЕЗІВ

А.Г. Григорович 482
СТРУКТУРА ІНФОРМАЦІЙНОЇ СИСТЕМИ «МЕДИЧНИЙ ПАСПОРТ»
Д.В. Коломиец 484
КЛАСТЕРИЗАЦИЯ МЕДИЦИНСКИХ СТАТИСТИЧЕСКИХ ДАННЫХ СРЕДСТВАМИ MICROSOFT ANALYSIS SERVER 2008

1. ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ТЕХНІЧНИХ СИСТЕМАХ

УДК 681.2:532.137

СИСТЕМА КОМПЛЕКСНОГО КОНТРОЛЮ ФІЗИЧНИХ ПАРАМЕТРІВ НАФТОПРОДУКТІВ

В.В. Древецький, д.т.н., доцент,
М.М. Клепач, програміст, С.П. Воробюк, магістр
Національний університет водного господарства і природокористування
klepachmm@ukr.net

Реалізація ефективних багатофункціональних вимірювальних систем для оперативного контролю фізико-хімічних характеристик нафтопродуктів потребує використання сучасних програмно-технічних засобів та прогресивних інформаційних технологій. Створення автоматизованих інформаційних систем є однією з галузей сучасних комп'ютерних технологій, що розвиваються найбільш швидко.

В розробленій системі для вимірювання в’язкості та густини нафтопродуктів використано капілярний метод і синтезований на його основі дросельний мостовий перетворювач (ДМП). Гідравлічна мостова схема утворена двома ламінарними та двома турбулентними дросельними елементами.

Принцип вимірювання полягає у неперервному прокачуванні досліджуваного нафтопродукту через ДМП та автоматичному астатичному зрівноваженні моста шляхом зміни об’ємної витрати продукту. За величиною об’ємної витрати і загального перепаду тиску на ДМП, визначених в момент рівноваги, розраховуються кінематична в’язкість та густина нафтопродукту.

На основі отриманих значень густини і в’язкості розраховуються інші показники якості нафтопродуктів, такі як октанове число бензину чи цетанове число дизельного палива. Передбачена можливість визначення температурних коефіцієнтів контрольованих величин.

Автоматичне зрівноваження мостової схеми, керування температурним режимом, збирання, первинне оброблення та проміжне зберігання інформації реалізовано на базі швидкодіючого програмованого логічного контролера (ПЛК) німецької фірми VIPA. Для розробки програмного забезпечення, конфігурування, параметризації та програмування контролера використовується інструментальне середовище WinPLC7. Загрузка програм в ПЛК і зв’язок з персональним комп’ютером здійснюється по інтерфейсу MPI за допомогою відповідного адаптера.

Візуалізацію та архівування даних реалізовано в системі диспетчерського управління і збору даних (SCADA-системі) Trace Mode російського виробника. Обмін даними в реальному часі між SCADA-системою та контролером VIPA System 100V ґрунтується на технології зв’язування і вбудови об’єктів для систем промислової автоматизації (OLE for Process Control). Vipa OPC-сервер, в основі котрого лежить технологія DA (Data Access), служить програмним інтерфейсом, що забезпечує збір технологічних даних, передачу команд керування та діагностику каналів зв’язку.

Підтримка контролером промислової швидкісної мережі Profibus-DP Slave позволяє легко інтегрувати розроблену систему в автоматизовані системи управління технологічними процесами вищого рівня, що забезпечує проведення технологічних процесів при оптимальних умовах, дозволяє підвищити точність контролю якості та визначення складу нафтопродуктів.

УДК 004.94

ЗАСТОСУВАННЯ ВИПАРОВУВАННЯ ДЛЯ ІНТЕНСИФІКАЦІЇ ТЕПЛОВІДВЕДЕННЯ

Д.В. Федасюк, д.т.н., професор
Т.О. Муха, аспірант, асистент
Національний університет «Львівська політехніка»

В наш час в результаті зростання потужностей різноманітних приладів, а також в результаті зменшення їхніх розмірів, збільшилася кількість теплової енергії, яка виділяється різними їх частинами. Інтенсивне нагрівання окремих елементів приладів знижує надійність їх роботи і загрожує виходом з ладу цих приладів. Тому при проектуванні приладів враховують допустимі температурні межі їх функціонування. Для забезпечення відповідного температурного режиму функціонування приладу виникає потреба ефективного тепловідведення.

Більшість систем тепловідведення, які використовуються в наш час, відводять тепло, обдуваючи поверхню потоком повітря, таким чином використовуючи явище конвекції для охолодження. Однак процес відведення тепла від нагрітого елемента можна інтенсифікувати завдяки використанню паралельно з конвекцією явища випаровування. Під час випаровування, при зміні агрегатного стану, тепло додатково відводиться у вигляді питомої теплоти.

Тому постає задача побудови адекватної моделі для процесу тепловідведення з використанням випаровування, яка б в свою чергу дала можливість порівняти вплив випаровування і конвекції на процес охолодження.

Порівняння кількості тепла, яке відводиться від тіла завдяки випаровуванню та завдяки конвекції, здійснюється на такій модельній задачі.

Розглядається нескінченна пластина товщиною D. На поверхні цієї пластини знаходиться тонкий шар рідини, товщина якого набагато менша за товщину пластини. Поверхня рідини зазнає впливу навколишнього середовища з нормальним атмосферним тиском $P_{\text{атм}}$, та температурою T_∞. В початковий момент часу і тверде тіло (пластина), і рідина мають однакову початкову температуру T_b. Знизу пластина нагрівається потоком тепла, який направлений по нормалі до поверхні пластини, і має величину q_0.

Процес теплопровідності в пластині описується системою диференціальних рівнянь:

$$\frac{\partial T_s}{\partial t} = \alpha \frac{\partial^2 T_s}{\partial x^2},$$

крайові умови: при $x = 0$ $k_s \dfrac{\partial T_s}{\partial x} = -q_0$, при $x = D$

$$k_s \frac{\partial T_s}{\partial x} = h_{fg} h \frac{M_f}{R \rho_a c_a} Le^{-\frac{2}{3}} \left(\frac{p_{f,sat}(T_s(D,t))}{T_s(D,t)} - \frac{p_{f,\infty}}{T_\infty} \right) + h\left(T_s(D,t) - T_\infty\right)$$

Початкові умови:

$$T_s(x, t = 0) = T_b.$$

Розв’язок знаходиться методом розділення змінних, а також за допомогою розробленого програмного забезпечення знаходиться методом сіток чисельний розв’язок поставленої вище задачі. Це дає змогу порівняти ці розв’язки та оцінити точність чисельного розв’язку.

УДК 004.891.2:632

ЗАДАЧІ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У ПРОБЛЕМІ ЗАХИСТУ РОСЛИН

В.М. Дубовой[1], д.т.н., професор, О.С. Сольський[2]
[1]Вінницький національний технічний університет
[2]Уманський національний університет садівництва
[1]sveta.vova.dub@gmail.com, [2]alex-2005z@rambler.ru

Через агрокліматичні умови останніх років, виведення значної кількості земель з обороту, впровадження нульового обробітку ґрунту, повсюдне ігнорування сівозміною, широкомасштабне та інтенсивне вирощування окремих енергетичних культур, порушення технології вирощування культурних рослин відбувається загострення фітосанітарної ситуації в сільськогосподарських угіддях. В цілому сільськогосподарським культурам та продукції рослинництва шкодять понад 400 видів шкідників, 200 збудників хвороб, 300 видів бур'янів. За підрахунком наукових установ Української академії аграрних наук в Україні втрати від шкідників, хвороб і бур'янів обчислюється в розмірі 33-48% потенційного врожаю. Тому, належний захист оброблюваних культур, є найбільш важливим завданням в аграрній політиці будь-якого сільськогосподарського підприємства.

Контроль та покращення фітосанітарної ситуації можливі лише при організації спільної роботи в межах всієї країни всіх державних служб, організацій, наукових закладів, виробників та реалізаторів, керівників господарств, які вносять свою частку в захист рослин (ЗР). Для ефективного вирішення даної проблеми потрібно збирати, обробляти великі об'єми інформації та видавати потрібні рекомендації. Це зумовлює актуальність розробки і впровадження мережевої

інформаційної технології (ІТ), яка базуються на сучасній комп'ютерній техніці. Дана ІТ є складною і повинна складатися з декількох підсистем (інформаційних технологій). В межах даної технології мають бути передбачені автоматизовані робочі місця для працівників центральної, обласних, районних державних інспекцій з захисту рослин, виробників та реалізаторів технічних та хімічних засобів ЗР, керівників (агрономів) сільськогосподарських підприємств, зв'язок між елементами ІТ має здійснюватись через Інтернет.

Основні задачі, які повинна вирішувати ІТ:

– збір та систематизація керівних документів в ЗР;

– розпізнавання шкідників, хвороб, бур’янів за їх ознаками;

– моніторинг, аналіз, прогнозування фітосанітарного стану районів, областей та країни в цілому та визначення заходів щодо його покращення;

– прогнозування часу появи, чисельності, розвитку шкідників та бур’янів;

– визначення часу настання сприятливих умов розвитку шкідників, хвороб;

– оповіщення керівників господарств про необхідність виконання спеціальних засобів захисту щодо запобігання поширенню шкідників, хвороб;

– вибір хімічних засобів для боротьби з шкідниками, хворобами та бур’янами;

– розрахунок економічних показників методів ЗР та доцільності їх використання;

– довідкова система.

Існуючі ІТ погано пристосовані до сучасних умов сільськогосподарського виробництва, нових проблем і можливостей аграріїв, і практично не розглядають підтримки заходів із ЗР. Розробка та впровадження даної мережевої технології буде великим кроком вперед в ЗР і одним із шляхів виведення агропромислового комплексу із кризи.

УДК 621.385.832.002

АВТОМАТИЗОВАНА ІНФОРМАЦІЙНА СИСТЕМА ЧАСТОТНОГО ВИМІРЮВАННЯ ТОВЩИНИ

О.В. Осадчук, д.т.н., професор, Р.В. Криночкін
Вінницький національний технічний університет
r@politex.org.ua

Розробка нових вимірювачів товщини матеріалів та покриттів з високими метрологічними якостями є актуальним завданням, пов'язаним з широкою сферою промислових та технологічних процесів. Створення таких високоефективних товщиномірів з низькою вартістю можливо шляхом застосування частотних перетворювачів з від'ємним опором (ЧПВО).

Такі сенсори-перетворювачі входять в якості чутливих елементів до загальної системи вимірювання і контролю товщини. Основними складовими частинами системи є: первинний ємнісний сенсор (планарної або плаской конструкції), частотний перетворювач на від'ємному опорі (ЧПВО) з вузлами захисту та керування живленням, частотомір на основі МК, з інтегрованим USB-трансівером (включає також вхідний обмежувач-підсилювач), драйвер інтерфейсу зв'язку та контролююче ПО. Функціональна схема системи приведена на рисунку.

Система працює наступним чином: зміна товщини вимірюваного матеріалу, приводить до зміни ємності чутливого елемента, яка в свою чергу впливає на еквівалентну ємність коливального контуру ЧПВО, що призводить до зміни частоти генерації на виході схеми. Завдання вхідного вузла полягає у перетворені коливань складної форми та змінної амплітуди у прямокутні з

амплітудами логічного нуля та одиниці, не змінюючи при цьому період коливань.

Вхідний сигнал, через буфер, потрапляє до основного робочого лічильника, що періодично отримує сигнали скиду від другого лічильника, що використовується в якості «часової бази», і формує т.зв. «часові ворота». Попередньо перед скидом підраховані значення основного лічильника записуються до оперативної пам’яті. Після цього проводиться операція ділення підрахованої кількості імпульсів на час підрахунку – отримане значення і буде шуканою частотою.

Виміряне значення частоти потрапляє до спеціального програмного забезпечення, що обраховує за товщину за відомою функцією перетворення, а також проводить первинну статистичну обробку даних, введення та обробку кореляційних функцій, індикацію виміряного значення тощо.

Такий підхід значно розширює можливості по обробці та аналізу даних від декількох сенсорів, надає можливість легкої інтеграції системи до АСК, підвищується загальна точність та надійність, відкривається шлях до адаптивних методів вимірювання та реакції на зовнішні (у т.ч. і сторонні) впливи.

УДК 621.316

ОСОБЛИВОСТІ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ АВТОМАТИЗОВАНОЇ СИСТЕМИ КЕРУВАННЯ КАСКАДАМИ МАЛИХ ГІДРОЕЛЕКТРОСТАНЦІЙ

П.Д. Лежнюк, д.т.н., професор, О.А. Ковальчук
Вінницький національний технічний університет
lpd@inbox.ru

Сучасні умови та особливості експлуатації малих ГЕС та їх каскадів на енергетичному ринку України вимагають вдосконалення інформаційного забезпечення і на цій основі підвищення рівня автоматизації процесів, пов’язаних з виробленням електроенергії.

Експлуатація малих гідроелектростанцій має ряд особливостей, порівняно з традиційними джерелами енергії. Невелика одинична потужність ГЕС, просторова розгалуженість генерування, наявність електричних та гідравлічних зв’язків між окремими ГЕС у каскаді, а також істотна залежність продуктивності малих ГЕС від впливу навколишнього середовища, призводить до ускладнень в процесі планування режимів їх роботи і робить неможливою ефективну експлуатацію таких станцій без впровадження сучасних засобів автоматизації та інформаційних технологій.

Автоматизовані системи керування (АСК) мають забезпечувати розв’язання задач, серед яких повна автоматизація інформаційного обміну між ГЕС та диспетчерським центром, контроль стану основного обладнання, його захист у анормальних режимах роботи та забезпечення надійності роботи ГЕС в цілому, забезпечення централізованого керування основними процесами,

маневреності ГЕС та максимальної ефективності використання запасів води протягом заданого періоду роботи, мінімізація кількості обслуговуючого персоналу.

Для реалізації вказаних задач необхідною умовою є забезпечення можливості централізованого керування об’єктом у реальному часі. Разом з тим, вказана умова не може бути забезпечена через просторову розгалуженість об’єктів та відсутність надійних каналів зв’язку між ними та диспетчерським центром. Виходячи з цього АСК з заданим переліком функцій будується як централізована система оперативного керування з децентралізацією функцій реального часу шляхом застосування локальних адаптивних систем автоматичного керування (САК).

Для цього виділяються опорні ГЕС, на яких встановлюються локальні АСК. З ними об’єднуються ГЕС нижчого ієрархічного рівня. При цьому істотно збільшується об’єм необхідної для оперативного моніторингу інформації та зростають вимоги щодо її якості. PLC-контролери таких об’єктів об’єднуються у локальну мережу Ethernet, що забезпечує можливість обміну даними між ними та сервером локальної АСК. Останній оснащується програмним забезпеченням, що дозволяє накопичувати та аналізувати ретроспективні дані власної локальної САК та САК під’єднаних ГЕС.

Реалізація АСК ГЕС забезпечує автономне програмне керування режимами роботи ГЕС відповідно до змін параметрів навколишнього середовища, дозволяє оперативно аналізувати й оптимізувати режими їх роботи. Інформаційне забезпечення створює умови для ефективного функціонування диспетчерського центру, для аналізу аварійних ситуацій, встановлення тенденцій зміни основних параметрів, а також для організації повноцінного інформаційного обміну між об’єктами керування та диспетчерським центром.

УДК 621.311

ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ КОНТРОЛЯ И УПРАВЛЕНИЯ ТРАНЗИТНЫМИ ПОТОКАМИ МОЩНОСТИ В ЭЛЕКТРИЧЕСКИХ СИСТЕМАХ

П.Д. Лежнюк[1], д.т.н., профессор, В.Ю. Прохватилов[2]
[1]Винницкий национальный технический университет,
[2]ООО «Хартеп», г. Харьков
lpd@inbox.ru

Электроэнергетическая система (ЭЭС) Украины имеет значительные перспективы относительно увеличения своих транзитных возможностей. Этому способствуют такие объективные факторы как территориальное расположение, высокий спрос на электроэнергию в соседних странах и наличие развитых магистральных электрических сетей. Транзитные потоки мощности, накладываясь на собственные потоки ЭЭС, вызывают дополнительные потери электроэнергии, уменьшают пропускную способность линий электропередачи, ухудшают качество электроэнергии. Очевидно, что этим факторам должна быть дана технико-экономическая оценка, результаты которой должны учитываться при формировании тарифа на транзит. Для оперативного мониторинга значений транзитной мощности, отслеживания путей транзита и определения влияния транзита на режимы ЭЭС создается оперативный информационно-управляющий комплекс (ОИУК), результатом функционирования которого является база данных для технико-экономических расчетов.

Одним из основных элементов ОИУК является автоматическая система контроля и управления

электропотреблением (АСКУЭ), функциональная схема которой приведена на рисунке.

По объему и содержанию информации, которая формируется АСКУЭ, должна обеспечить наблюдаемость и управляемость транзитными потоками мощности. Для этого на локальном уровне она концентрируется по технологическому, функциональному, территориальному (адресному) признаку и по оптоволоконной связи передается в диспетчерский центр. Исходя из особенностей задачи оптимального управления транзитами, информационное обеспечение должно отвечать условиям технической, коммерческой и интегральной составляющих наблюдаемости. При этом должна обеспечиваться управляемость перетоками.

УДК 621.317.7

ВИМІРЮВАННЯ ІНФОРМАТИВНИХ ПАРАМЕТРІВ ТРИФАЗНИХ НЕСИМЕТРИЧНИХ ШВИДКОЗМІННИХ НАВАНТАЖЕНЬ ВУЗЛІВ ЕЛЕКТРИЧНИХ МЕРЕЖ

М.Й. Бурбело, д.т.н., проф., М.В. Никитенко, аспірант
Вінницький національний технічний університет
MAX220387@meta.ua

В багатьох випадках динамічну компенсацію реактивної потужності необхідно поєднувати з симетруванням навантажень, що вимагає отримання додаткової інформації про параметри несиметрії.

Розроблено швидкодіючі вимірювальні канали для отримання інформації про активну та реактивну потужності, при побудові яких використано підхід, що оснований на використанні ортогональних миттєвих потужностей.

$$P(t) = \frac{1{,}5}{T/2}\int_{t-T/2}^{t}(u_\alpha i_\alpha + u_\beta i_\beta)dt; Q(t) = \frac{1{,}5}{T/2}\int_{t-T/2}^{t}(u_\beta i_\alpha - u_\alpha i_\beta)dt \quad (1)$$

Для отримання активної та реактивної умовних потужностей зворотної послідовності використаємо формули (2).

$$P_2(t) = \frac{1{,}5}{T/2}\int_{t-T/2}^{t}(u_\alpha i_\alpha - u_\beta i_\beta)dt; Q_2(t) = \frac{1{,}5}{T/2}\int_{t-T/2}^{t}(u_\beta i_\alpha + u_\alpha i_\beta)dt \quad (2)$$

Однак, перехідні характеристики вимірювального каналу для величин P_2, Q_2, мають значне перерегулювання, що негативно впливатиме на стійкість динамічної системи компенсації реактивної потужності.

Вирішенням даної проблеми може бути використання величин, які формуються за виразами (3)

$$P(t)=\frac{1{,}5}{T/2}\int_{t-T/2}^{t}(u_\alpha i_\alpha+u_\delta i_\delta)dt;\ Q(t)=\frac{1{,}5}{T/2}\int_{t-T/2}^{t}(u_\beta i_\alpha-u_\beta i_\delta)dt;$$

$$P_2(t)=\frac{1{,}5}{T/2}\int_{t-T/2}^{t}(u_\alpha i_\alpha-u_\delta i_\delta)dt;\ Q_2(t)=\frac{1{,}5}{T/2}\int_{t-T/2}^{t}(u_\beta i_\alpha+u_\beta i_\delta)dt, \quad (3)$$

де $u_\delta(\omega t)=u_\beta(\omega t-90^o)$, $i_\delta(\omega t)=i_\beta(\omega t-90^o)$.

Рис. 1. Перехідні характеристики вимірювального каналу для величин P_2, Q_2, що визначені за формулою (3)

На рис. 2 зображено структурну схему вимірювального каналу.

Рис. 2. Структурна схема вимірювального каналу, в якому P_2, Q_2 визначені за формулами (3)

Формування ортогональних напруг та струмів здійснюється за виразами:

$$u_\alpha(t)=\frac{1}{3}\left(u_{AB}(t)-u_{CA}(t)\right);\ u_\beta(t)=\frac{1}{\sqrt{3}}u_{BC}(t);$$

$$i_\alpha(t)=i_A(t);\ i_\beta(t)=\frac{1}{\sqrt{3}}\left(i_B(t)-i_C(t)\right).$$

УДК 531.3

СИНЕРГЕТИЧНІ МЕТОДИ КЕРУВАННЯ ТЕПЛОЕНЕРГЕТИЧНИМИ ОБ'ЄКТАМИ

В.Ю. Кучерук, д.т.н., професор,
І.А. Дудатьєв, студент
Вінницький національний технічний університет

У роботі на основі методів синергетичної теорії керування запропоновано розв'язок прикладної проблеми управління в складних динамічних системах типу "котельна установка".

Теплоенергетичні системи (ТЕС) є ключовими об'єктами сучасної техносфери, від ефективного функціонування яких залежить якість та безпека життєдіяльності населення. У зв'язку з цим необхідно забезпечити ефективне та безпечне функціонування цих систем, що є фундаментальною науково-технічною проблемою.

Сучасні ТЕС являють собою комплекси складних підсистем, які зв'язані між собою динамічною взаємодією та інформацією. Технологічні процеси (ТП) у існуючих ТЕС супроводжуються великими втратами енергії. Ці втрати напряму пов'язані з характером теплових та електромеханічних процесів, властивості яких залежать від принципу керування ТП. Тому актуальною є задача ефективного керування ТЕС, вирішення якої забезпечить безпечну та стійку роботу.

Результатом представленої роботи є розробка нових алгоритмів керування, які забезпечать ефективне, безпечне, ресурсозберігаюче керування процесами виробництва теплової та електричної енергії.

УДК 004.652

ФОРМАЛЬНА МОДЕЛЬ ПРОЦЕСІВ ІНТЕГРАЦІЇ ДАНИХ У ВІДКРИТИХ СИСТЕМАХ

А.Ю. Берко, к.т.н., доцент
Національний університет "Львівська політехніка"
BerkoAndriy@Ya.Ru

Характерною особливістю інформаційних ресурсів відкритих систем є їх гетерогенний характер. Це потребує інтеграції різнорідного контенту в єдиному середовищі зберігання, опрацювання та застосування. Інтеграція інформаційних ресурсів передбачає їх об'єднання при якому спільне використання є більш простим і ефективним ніж локальне застосування кожної складової. Метою інтеграції є отримання цілісної картини корпоративної бізнес-інформації на основі даних, отриманих з різних джерел. Інтеграція є процесом, який передбачає видобування, перетворення і завантаження (ETL) даних з різних систем та джерел в єдиний інтегрований набір даних, призначений для опрацювання і аналізу.

Пропонується опис процесу інтеграції даних у як формальної моделі, що складається з таких компонентів

- вихідна глобальна схема інтегрованих даних, описана в термінах деякої мови, визначеної на основі кінцевого алфавіту,
- вхідна схема джерела даних описана в термінах мови, визначеної на основі початкового алфавіту,
- відображення, задане у вигляді відповідностей між запитами до вихідних даних і запитами до вихідних даних.

Розроблено уніфіковану модель подання даних, як деякої формальної мови, яку застосовують для позначення

множини понять. Властивостями даних є синтаксис, семантика та структура, в такий спосіб, довільний набір даних D можна подати як формальну систему вигляду

$$D=<V, G, S, H>,$$

де V – множина значень даних, G – їх синтаксис, S – структура , H – семантика .

Враховуючи модель даних, подану вище, формальне визначення процесу інтеграції можна звести до дії над цими компонентами, замінивши опис $D^I=I(D_1,D_2,\ldots,D_N)$ на деталізований опис всіх складових визначення даних

$$D^I=<V^I,G^I,S^I,H^I>=I(<V_1, G_1, S_1, H_1>,<V_2, G_2, S_2, H_2>, \ldots, <V_N, G_N, S_N, H_N>),$$

де $<V_i, G_i, S_i, H_i>$, $i=1,2, \ldots, N$ – деталізоване формальне зображення i-го набору даних.

В такий спосіб, проблему інтеграції даних можна декомпонувати на окремі проблеми інтеграції значень даних, синтаксису, структури та семантики. Загальний оператор інтеграції даних I, при цьому може бути подано як комбінацію

$$I=<I^V, I^G, I^S, I^H>,$$

де I^V – оператор інтеграції значень, I^G – інтеграції синтаксису, I^S – інтеграції структури даних, I^H – інтеграції семантики. Процес інтеграції при цьому буде декомпоновано на відповідні підпроцеси, які можна описати формальною схемою виду

$$D^I=<V^I,G^I,H^I,S^I>=<I^V(V_1,V_2,\ldots,V_N),I^G(G_1,G_2,\ldots,G_N),I^S(S_1,S_2,\ldots,S_N),I^H(H_1,H_2,\ldots,H_N)>.$$

В основу роботи покладено модель подання даних як комплексного об’єкту, властивостями якого є синтаксис, структура та семантика. Проаналізовано особливості створення інтегрованих способів зображення даних на етапі їх переміщення від джерел утворення до інтегрованого кінцевого набору.

УДК 629.7.022

ЗАСТОСУВАННЯ СУЧАСНИХ КОМП'ЮТЕРНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ПРИ ПРОЕКТУВАННІ СКЛАДНОГО ТЕХНІЧНОГО ОБ'ЄКТА

В.П. Зінченко[1], к.т.н., доцент, Д.І. Конотоп[2], аспірант
Національного технічного університету України «КПІ»
[1]zinchenko.vp@gmail.com, [2]konotop.dmitriy@gmail.com

Основні етапи проектування складного технічного об'єкта (СТО) (на прикладі літака Ан-148) з використанням сучасних комп'ютерних інформаційних технологій КІТ представлені на рис. 1.

Рис. 1. Основні етапи проектування літака з використанням сучасних КІТ

Перший етап – технічне завдання (ТЗ) містить у собі вимоги до основних технічних даних літака.

Другий етап – майстер-геометрія (МГ) містить у собі розробку моделей літака на підставі вимог, визначених у ТЗ.

Третій етап – модель розподілу простору (МРП) передбачає компоновку конструкції, систем і обладнання відповідно до розробленої моделі МГ літака.

Четвертий етап – модель повного електронного визначення виробу (ПЕВВ) літака – рівень робочого проекту (РП).

МРП є основним етапом проектування СТО при ув’язці компонентів конструкції, систем й обладнання з використанням сучасних КІТ. МРП складається із двох етапів: МРП № 2-1 – рівень пророблення ескізного проекту й МРП № 2-2 – рівень пророблення технічного проекту.

МРП № 2-1 повинна бути представлена в глобальній системі координат літака. Формування складальних одиниць компонентів конструкції планера, силової установки, систем і обладнання здійснюється у власних локальних системах координат, ув'язаних із системою координат літака.

МРП №2-2 представлена набором відсіків і секцій, на які розбитий простір літака. Кожна модель відсіку або секції позиційована у своїй системі координат. Формування моделей складальних одиниць здійснюється у власних локальних системах координат, ув'язаних із системою координат відсіків або секцій. МРП №2-2 – більш детальне пророблення конструкції планера, силової установки, систем і обладнання літака на рівні технічного проекту. Результатом МРП є віртуальний макет літака, що використовується на наступних етапах проектування. При цьому використовується технологія паралельного проектування.

УДК 004

ЗАСТОСУВАННЯ КОМП'ЮТЕРНИХ СИСТЕМ З ПАРАЛЕЛЬНОЮ АРХІТЕКТУРОЮ ДЛЯ ПРОГНОЗУВАННЯ ПАРАМЕТРІВ ТЕХНОЛОГІЧНОГО ПРОЦЕСУ В УМОВАХ ГІРНИЧО-ЗБАГАЧУВАЛЬНОГО КОМБІНАТУ

Замятін Д.С., к.т.н., В.Б. Щукін, аспірант
Національний технічний університет України
«Київський політехнічний інститут»
VladMess@yandex.ru

Впровадження автоматизованих систем контролю технологічних параметрів на підприємствах гірничо-збагачувальної галузі практично завжди є виправданим. Про це свідчить наявність великої кількості факторів, які необхідно аналізувати та враховувати при налагодженні дробарок та обладнання на рудозбагачувальних фабриках.

Однією з найактуальніших проблем є підтримка в реальному часі оптимальних (планових) параметрів якості шихти, що подається на збагачення до рудозбагачувальних фабрик. Для вирішення цієї проблеми впроваджуються автоматизовані системи ефективного керування роботою кар'єрного транспорту. Це дозволяє певною мірою покращити ситуацію, але в цілому проблема залишається невирішеною. Перспективнішим шляхом до вирішення цієї задачі можна вважати попереднє прогнозування складу шихти в залежності від виконаних робіт в кар'єрі.

На рис. 1 наведена структурна схема стадій технологічного процесу. Вхідними параметрами даної структури є об'єми різновидів руд μ_1, μ_2,…, μ_N, де N — кількість наявних різновидів, які потрапляють на стадію

попереднього дроблення. Вихідним параметром є шихта (вихідна руда) R, яка використовується для подальшого збагачення в рудозбагачувальних фабриках. Параметри дробарки не розглядаються в даній роботі.

Рис. 1. Структурна схема стадій технологічного процесу

Раніше було показано, що при N=7 (кількості рудопотоків рівній семи) для ефективного вирішення задачі прогнозування параметрів якості вихідної сировини, яка подається на збагачення до рудозбагачувальної фабрики, необхідно використовувати комп'ютерну систему з паралельною архітектурою. Причому бажана продуктивність такої системи має становити не менше 2,6 ТФлопс.

Дані для прогнозу надходять до систем по комп'ютерній мережі підприємства, оброблюються і результат відправляється відповідальному персоналу для аналізу і керування збагачувальним обладнанням. Безпосередній користувач в прогнозуючій комп'ютерній системі відсутній. Отже параметр часу відклику в таких системах не є пріоритетним. Натомість важливу роль відіграє пропускна здатність (кількість виконуваних задач за одиницю часу) та оборотний час (час, що витрачається на очікування та обробку задачі).

УДК 681.32

РОЗРОБКА ПІДСИСТЕМ ТЕХНІЧНОГО ТА ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ АВТОМАТИЗОВАНОЇ СИСТЕМИ КЕРУВАННЯ ВОЛОГОЗАБЕЗПЕЧЕННЯМ

В.Й. Пастушенко[1], к.т.н., доцент, С.В. Шатний[2], магістр
Національний університет водного господарства та природокористування
[1]vteren@gmail.com, [2]sha_ser@mail.ru

Перспективним напрямком в розвитку меліоративних систем є розробка та впровадження децентралізованих систем автоматичного керування вологозабезпеченням сільськогосподарських культур із застосуванням новітніх технологій в області безпровідної телемеханіки, мікропроцесорної техніки та інформаційних систем на основі клієнт-серверної архітектури. Впровадження таких систем вирішує задачі енергозбереження та зниження затрат на обслуговування вже існуючих систем меліорації.

Система керування містить кілька рівнів, в залежності від структури та функцій меліоративної системи. Основою технічного забезпечення на нижньому рівні є гідравлічні регулятори двосторонньої дії, які встановлюються у відповідних каналах осушення/зволоження. Керування здійснюється за допомогою мікропроцесорного регулятора на основі контролера PIC18F4620, до якого через аналогові входи під’єднані відповідні давачі вологості ґрунту та рівня води в колодязі гідравлічного регулятора. Основною задачею є регулювання рівня води по заданому алгоритму шляхом

перемикання електромагнітних клапанів. До мікропроцесорного регулятора через інтерфейс RS-232 під'єднаний пристрій для безпровідної передачі даних. Даний пристрій розроблений на основі високотехнологічного модуля Radiocrafts RC1240, він дозволяє передавати дані бо радіоканалу з частотою 433 МГц. на дальність до 2-6 км. при умові прямої видимості передавача та приймача.

Наступним елементом системи керування є централізований пункт збору та передачі інформації, на якому встановлений безпровідний концентратор для обміну інформації з кожним регулятором. Основою пункту збору інформації є сервер архітектури IBM PC або сумісний, що має прямий доступ до мережі Інтернет. Таким чином організований сервер з WEB інтерфейсом, який транслює в мережу всі необхідні для синтезу алгоритмів керування дані. Інформаційним забезпеченням слугує операційна система Linux для архітектури x86 із системною оболонкою MCE. В даній оболонці містяться всі необхідні інструменти для створення і налаштування сервера. Також до сервера за допомогою протоколу 1-Wire під'єднані давачі кліматичної вимірювальної станції, зокрема, давач температури, вологості повітря, рівня опадів, швидкості вітру і забезпечується можливість реалізації відеотрансляції в режимі он-лайн. Таким чином забезпечується віддалене управління меліоративними об'єктами, для реалізації якого необхідно під'єднатися до сервера за допомогою програми-клієнта і отримати всі необхідні для подальшої обробки дані.

УДК 681.32

АЛГОРИТМІЧНЕ ТА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ СИСТЕМИ КЕРУВАННЯ СТАНКОМ З ЧПУ

М.В. Плахотний, к.т.н., доцент, В.О. Дащенко
Національний технічний університет України «КПІ»
ros_@ukr.net

Системи з числовим управлінням виконують інструкції спеціалізованої мови програмування (наприклад, G-код). Потім вони за допомогою інтерпретатора перетворюються з вхідної мови в команди управління головним приводом, приводами подач, контролерами управління вузлів станка.

Визначення положення інструмента станка виконує інтерполятор, який формує траєкторію руху ріжучого інструмента по зданому закону (з заданими швидкістю і точністю) між двома опорними точками контура деталі, координати яких вказані в управляючій програмі. Опорні точки характеризують початок і кінець траєкторії , по якій переміщується ріжучий інструмент.

В теперішній час найчастіше використовуються лінійні та кругові інтерполятори. Лінійні інтерполятори забезпечують формування траєкторії в вигляді лінії, кругові - формують траєкторію в вигляді кола або дуги. В розробленій програмі застосовуються комбінований метод де всі дуги замінюються відрізками, тому немає потреби розраховувати швидкості між опорними точками дуг.

Актуальним є питання розробки методів оптимізації руху інструмента на відрізку для зменшення часу обробки деталі. В статті розглядається метод склеювання відрізків,

який дозволяє зменшити час проходження по складній траєкторії.

Алгоритм проходження по траєкторії передбачає таку послідовність дій для кожного відрізку:

- розгін з стартової швидкості до максимальної швидкості;
- рух на максимальній швидкості;
- сповільнення.

Розроблений алгоритм полягає в тому що швидкість в кінцях відрізків можна не знижувати до мінімальної якщо двигуни можуть витримати зміну швидкості. Для цього розраховуються значення швидкостей в опорних точках траєкторії. Алгоритм складається з декількох етапів, які докладно викладені в статті. В розробленій програмі всі дуги замінюються відрізками, тому немає потреби розраховувати швидкості між опорними точками дуг.

Програма управління станком включає реалізацію функцій:

- швидке переміщення;
- лінійна інтерполяція;
- кругова інтерполяція;
- заміна площин інтерполяції;
- відображення важливої інформації в процесі роботи;
- контроль над допоміжними вузлами;
- графічне відображення траєкторії руху інструмента.

Наведені функції відповідають стандарту ISO 6983. Розроблена програма дозволяє управляти 4-х координатним фрезерним станком за допомогою G-кодів. Програма розпізнає всі основні G-коди та управляє приводами подач, головним приводом, приймає сигнали з датчиків, управління допоміжними вузлами станка.

УДК 681.516.75

РОЗРОБКА ТА ДОСЛІДЖЕННЯ НЕЙРОРЕГУЛЯТОРА ДЛЯ СИСТЕМИ УПРАВЛІННЯ ВУЗЛОМ АБСОРБЦІЇ

В.Й. Пастушенко[1], к.т.н., доцент, А.В. Комар[2], магістр
Національний університет водного господарства та природокористування
[1]vteren@gmail.com, [2]komarav@i.ua

Системи керування на базі П-, ПІ-, ПІД-регуляторів з постійними значеннями коефіцієнтів регулювання залишаються на сьогоднішній день найбільш поширеним типом промислових систем автоматичного керування. Розповсюдженість таких систем пояснюється достатньою якістю роботи таких систем керування, та простотою їх реалізації.

Важливим елементом комплексної системи автоматизованого управління вузлом абсорбції, при виробництві неконцентрованої азотної кислоти, є система регулювання концентрації азотної кислоти на виході абсорбера.

Абсорбер – нелінійний динамічний об’єкт керування по каналу витрата абсорбенту – концентрація продукту на виході, нелінійність якого обумовлена залежністю параметрів об’єкту від величин збурюючих дій. Тому при розробці системи управління таким об’єктом виникають труднощі при отриманні налаштувань регулятора, який генерує регулюючу дію за П-, ПІ-, ПІД-законом.

Розроблена система керування – каскадна САР концентрації азотної кислоти, в якій в якості ведучого регулятора використовується нейро-ПІД регулятор з

автоматичним налаштуванням коефіцієнта підсилення, часу ізодроми та часу диференціонування. Регулятор складається із трьох структурних блоків: блок із еталонною моделлю об’єкта, блок автоматичного підбору коефіцієнтів регулятора і блок, який чинить регулюючу дію на об’єкт. Еталонна модель представлена багатошаровою нейромережею. При виконанні синтезу регулятора враховувалась можливість необхідності комплексного налаштування параметрів нейромережі, таких як: кількість прихованих шарів, тип функції активації, кількість входів та виходів. Набір даних, який необхідний для навчання нейронної мережі, генерується шляхом подачі на систему випадкових регулюючих сигналів. Після ідентифікації об’єкту регулювання, відбувається процедура автоматичного підбору коефіцієнтів регулювання за допомогою генетичного алгоритму. Ступінь оптимальності підібраних коефіцієнтів визначається шляхом аналізу показників якості регулювання, які отримуються моделюванням керуючого впливу на нейромережу, як на модель динамічного об’єкту. Умовою зупинки процесу підбору коефіцієнтів слугують задовільні показники якості регулювання, або перевищення кількості епох виконання генетичних операторів. Після завершення процедури підбору коефіцієнтів регулювання, регулятор переходить в режим безпосереднього керування об’єктом. Таким чином відбувається автоматичне налаштування та оптимізація роботи регулятора при керуванні нелінійним динамічним об’єктом.

УДК 681.3

ВИКОРИСТАННЯ ФАЗІ-КОНТРОЛЕРІВ У АТМ-МЕРЕЖАХ

О.О. Семенова[1], к.т.н., ст. викл., А.О. Семенов[2], к.т.н., ст. викл., О.О. Войцеховська[3], асистент
Вінницький національний технічний університет
[1]Helene_S@ukr.net, [2]Semenov79@ukr.net, [3]Olga1085@rambler.ru

Сучасні інтелектуальні технології – фазі-логіка, нейронні мережі, генетичні алгоритми – характеризуються здатністю розв'язувати нові задачі та адаптуватися до нових ситуацій, використовуючи набутий досвід.

Відомі два основні способи впровадження інтелектуальних технологій. Перший полягає у розробленні спеціального програмного забезпечення для персональних комп'ютерів. Другий полягає у розробленні пристроїв, які можуть імітувати роботу людського мозку. Другий спосіб є більш ефективнім, хоча і менш поширеним.

Останнім часом до передачі інформації висуваються більш високі вимоги. Одному і тому самому абонентові можуть бути передані різні за характером повідомлення: рухомі зображення, комп'ютерні файли, електронна пошта, інформація із системи дистанційного навчання (у тому числі мультимедійна), фільми по кабельному телебаченню та ін. Причому джерела цієї інформації є, як правило, асинхронними. Інформація від одних джерел може надходити безупинно, від інших – час від часу. Швидкість надходження інформації від різних джерел є різною. Так, мовний потік надходить зі швидкістю 64 кбіт/с, а передача

рухомого зображення вимагає швидкості від 1,5 до 100 Мбіт/с.

Для узгодження різних вимог була запропонована нова технологія передачі, що одержала назву режиму асинхронної передачі (Asynchronous Transfer Mode – ATM). Ця технологія допускає запис будь-якого виду інформації у комірки фіксованої довжини.

Згідно моделі мережі з асинхронним способом передачі даних вхідний трафік, що надходить зі сторони абонента, поділяється на два типи. До першого типу відноситься трафік у реальному масштабі часу, а до другого – трафік у нереальному масштабі часу. Трафік першого типу використовують відео та мовні служби, а трафік другого типу використовують інформаційні служби. Всі повідомлення, які передаються від джерел служб зі сторони абонента, сегментуються в пакети фіксованої довжини – комірки – та зберігаються в буфері периферійних пристроїв апаратури абонентської посилки для очікування передачі. Коли буфер повний, нові комірки блокуються і втрачаються.

Використання інтелектуальних технологій у мережах з асинхронною передачею даних дасть можливість підвищити точність і ефективність керування трафіком при порівняно невеликих економічних витратах.

Для підвищення ефективності функціонування ATM-мереж необхідно розв'язати такі задачі:

– розробити структурну схему фазі-контролера трафіка;

– визначити принципи функціонування фазі-контролера трафіка;

– визначити терми та форми функцій належності вхідних та вихідної лінгвістичних змінних;

– промоделювати роботу розробленого фазі-контролера трафіка у програмі MatLab.

УДК 681.51

СИСТЕМА ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ В УПРАВЛІННІ ТЕПЛОТЕХНОЛОГІЧНИМ ОБ'ЄКТОМ

С.М. Москвіна[1], к.т.н., доцент,
С.А. Білоконь[2], аспірант
Вінницький національний технічний університет
[1]moskvina@ukr.net, [2]serge.belokon@gmail.com

Прийняття рішень в управлінні теплотехнологічними об’єктами є складною задачею, що зумовлена складністю процесів, які протікають під час технологічного процесу. Серед таких об’єктів є сушка будівельної кераміки. На сьогоднішній день процес сушіння сирцю будівельної кераміки на сучасних підприємствах по її виробництву розглядається як один з найважливіших, оскільки на даному етапі формуються початкові міцнісні характеристики цегли, які є важливі для укладки висушеного сирцю у садку на вагонетки для поміщення у тунельну піч. При відповідному сушінні сирцю цегли у піч надходить продукція, яка не містить тріщин, не є деформованою, у якої рівень пористості не виходить за межі допустимого.

Розвиток та широке впровадження інтелектуальних технологій в усі області людської діяльності на сьогоднішній день дозволяє переглянути підхід до моделювання та управління сушками будівельних виробів й дає значний потенціал щодо можливості їх удосконалення. При використанні нейронних мереж та нейронечіткого підходу можна на основі інформації щодо проходження процесів, зібраної за будь-який проміжок часу, розробити надбудову над існуючими системами, що дозволить вдосконалити як

систему управління, так і систему підтримки прийняття рішень при управлінні. Це дає можливість зменшення кількості браку вихідної продукції та відповідно підвищення її якості.

Авторами розроблений наступний алгоритм управління. На початку циклу сушіння визначається поточний температурний режим у сушці, після чого проводиться перевірка, чи задовольняє поточна температура умовам протікання технологічного процесу. У разі задовільних результатів за допомогою нейромережі прогнозується значення температури на наступному кроці. Якщо ж поточна температура не відповідає накладеним на неї обмеженням, проводиться розрахунок необхідного потоку теплоносія для підтримки режиму сушіння. Після цього розраховується відсоток, на який необхідно відкрити або закрити заслінку й безпосереднє переміщення заслінки. Після зміни потоку перевіряється час сушки сирцю на першій позиції. Якщо час менше встановленого, алгоритм повторюється знову, якщо ж ні – обирається рішення: необхідно вводити у зону сушіння дві нові вагонетки або ні. Якщо ні, алгоритм повторюється знову, у противному випадку у тунель подаються дві наступні вагонетки, відповідно рухаючи інші до зони виходу.

У відповідності з запропонованим вдосконаленим методом управління роботою сушки розроблена структура СППР, що включає блоки «Збір даних», «Аналіз даних», блок визначення відсотку відкриття заслінки та блок прийняття рішень.

Особливістю створеної СППР є те, що прийом рішень здійснюється за допомогою навченої нейронечіткої мережі й оператору пропонується рішення, визначене за допомогою системи, що зменшує вірогідність впливу людського фактору на зменшення якості вихідної продукції.

УДК 004.891.3

ІНФОРМАЦІЙНО–ВИМІРЮВАЛЬНА СИСТЕМА ДІАГНОСТИКИ ТЕПЛОНАСОСНОГО ОБЛАДНАННЯ

В.В. Джеджула, к.т.н., ст. викладач
Вінницький національний технічний університет
djedjula@inbox.vn.ua

Використання теплових насосів дозволяє отримати низько потенційне тепло з природних джерел, витрачаючи при цьому значно менше електричної енергії, ніж при безпосередньому її перетворенні на теплову. Коефіцієнт перетворення енергії COP в сучасних парокомпресійних теплових насосах складає 3…4,5, тобто, на 1 кВт електричної енергії можна отримати 3…4,5 кВт теплової.

Робота теплонасосного обладнання суттєвим чином залежить від багатьох факторів, серед яких є і такі, що безпосередньо до холодильного обладнання не відносяться: тепловтрати будівлі, що опалюється, тип ґрунту, де розташовано колектор, схема системи опалення, якість живлення електричною енергією та інші. Діагностику роботи агрегатів даного типу необхідно здійснювати в два етапи: вимірювання характерних величин і моделювання роботи системи. В сукупності підсистеми вимірювання і обробки складають інформаційно-вимірювальну систему.

До основних несправностей у роботі теплонасосного обладнання можна віднести: проблеми пов’язані з роботою терморегуляційного вентиля; несправності випарника пов’язані з зниженням коефіцієнту теплопередачі; несправності конденсатора пов’язані з зниженням коефіцієнту теплопередачі; проблеми запуску у холодний

період і регуляції тиску конденсації; недостатня або надлишкова кількість холодильного агенту; проблеми відбору теплоти ґрунтовим колектором; невідповідність системи опалення (охолодження) параметрам теплового насосу; руйнування клапанів і надлишкова потужність компресора; наявність у контурі домішків, що не конденсуються; передчасне дроселювання у газовому або рідинному трубопроводах; проблеми електроживлення; проблеми регулювання системи теплохолодопостачання.

Для діагностики теплонасосного обладнання пропонується ІВС, що складається з вимірювального блоку: 8-канального вимірювача, перетворювача інтерфейсу, сенсорів температури і тиску і обчислювального блоку, що складається з програми аналізу даних, яка функціонує на основі теорії нечіткої логіки та гібридних нейронних мереж в математичному пакеті Simulink. В процесі діагностики в програму поступає наступна інформація: температура фреону на виході з випарника; температура фреону на виході з конденсатора; тиск конденсації; тиск випаровування; температура ґрунтової води (вхід); температура ґрунтової води (вихід); температура рідинного ресивера; струм компресора; температура води системи опалення на вході в конденсатор; температура води системи опалення на виході з конденсатора; марка фреону; геометричні розміри фреонопроводів і ресивера; характеристики циркуляційних насосів; розрахункова потужність системи опалення; теплонадходження будівлі; тепловтрати будівлі; наявність обмерзання ТРВ і трубопроводів; наявність пульсацій системи; тип ґрунту і колектора.

Остаточний висновок про функціонування системи здійснюється в програмі після обробки інформації в обчислювальних і обчислювально-логічних блоках.

УДК 681.513

АЛГОРИТМИ ONLINE-МАРШРУТИЗАЦІЇ ДЛЯ УПРАВЛІННЯ ТРАФІКОМ У МЕРЕЖАХ З ТЕХНОЛОГІЄЮ MPLS

О.В. Кухарєва
Національний технічний університет України "Київський політехнічний інститут"
ostarkova@ukr.net

Швидке зростання телекомунікаційних мереж та поява нових сервісів є причиною створення нових засобів для запобігання перевантаженням у мережі та у випадку їх виникнення боротьби з ними. Таким цілям, зокрема, дуже добре відповідає технологія MPLS, що має численні переваги при управлінні трафіком у мультисервісних мережах. Архітектура MPLS дозволяє провайдерам послуг систематично застосовувати засоби управління трафіком та методи його передавання у мережі, зокрема, засновану на обмеженнях маршрутизацію (constraint-based routing – CBR).

Зазвичай процес обчислення та встановлення шляхів CBR розділяють на offline та online CBR. Offline CBR обчислює шляхи поза елементами мережі, на сервері. У такому випадку на вхід подається відома статична матриця вимог, та для неї на основі карти топології мережі обчислюються оптимальні шляхи. При цьому не відбувається адаптація до змін у стані мережі. Головне використання offline CBR – для оптимізації та планування мережі. Online CBR – механізм маршрутизації, що виконується безпосередньо на елементах мережі, отримуючи на вхід вимоги у порядку їх появи у мережі та

обчислюючи підходящий шлях для них. Таким чином, online CBR має найновішу інформацію про стан мережі та адаптується до її змін. Але алгоритми online CBR повинні задовольняти суворим вимогам, зокрема, щодо обчислювальної складності, часу збігу.

Одним з найбільш популярних та широко використовуваних алгоритмів у мережах MPLS є алгоритм знаходження найкоротшого шляху (shortest path first – SPF), що бере за основу кількість пересилань. Але це може призвести до небажаної концентрації трафіку на деяких шляхах мережі. Більш "розумним" алгоритмом маршрутизації є MIRA (Minimum Interference Routing Algorithm), метою якого є встановлення якомога більшої кількості шляхів, використовуючи поняття критичних каналів. Але даний алгоритм є дорогим щодо обчислень. Алгоритм DORA (Dynamic Online Routing Algorithm) динамічно встановлює шляхи з гарантованою смугою пропускання у мережах MPLS. Його мета –задовольнити якомога більше запитів щодо встановлення шляхів з зарезервованою смугою пропускання рівномірно по мережі. Пропонується online-алгоритм реконфігурації маршрутів мережі MPLS у випадку перевантажень у мережі, а також у випадку відмов вузлів та каналів. Алгоритм разом з деякими розглянутими вище існуючими алгоритмами реалізовано у програмному комплексі, призначеному для імітації роботі мереж з технологією MPLS, зокрема, для дослідження завантаженості елементів мережі (виявлення "вузьких" місць у мережі), аналізу та оптимізації характеристик мереж (середньої затримки, варіації затримки, проценту відкинутих пакетів), а також дослідження поведінки трафіку різних класів з метою забезпечення заданої якості обслуговування. Також порівняно основні показники якості обслуговування для реалізованих алгоритмів.

УДК 004.82

АГЕНТНЫЙ ПОДХОД В ЗАДАЧЕ УПРАВЛЕНИЯ ДИНАМИЧЕСКИМ ОБЪЕКТОМ

Р.Н. Чижденко
Донецкий национальный университет
chrom85@mail.ru

Современный уровень развития сферы игрового и мультимедийного ПО предъявляет высокий уровень требований к управляемым искусственным интеллектом (ИИ) объектам, как к автономным, так и группам таких объектов, реализующих определенную общую цель. Поведение наблюдаемых объектов зависит от управления, применяемого интеллектуальной компонентой, и зачастую сводится к определению в некотором смысле наилучшего, оптимального, варианта решения задачи (достижения цели) в текущих условиях, определяющих характеристики среды и объекта управления.

Рассматривается задача перемещения объекта в моделируемом окружении. Разработка алгоритмов перемещения объекта является одной из задач современных исследований в рассматриваемом направлении. Различные архитектуры таких алгоритмов традиционно разбивают на следующие классы:

– иерархические структуры – происходит разделение функций агента на высокоуровневые (планирование, командные действия) и низкоуровневые (базовые перемещения, действия);

– поведенческие структуры – конечное решение по управлению формируется специальным блоком на основе информации от всех модулей;

– гибридные структуры – реализуются несколькими уровнями иерархии, нижний исполнительный из которых функционирует на поведенческой основе.

Реализация агентных систем управления возможна с использованием интеллектуальных обучаемых средств, построенных на логических правилах, нейронных и нейрологических сетях.

Традиционно, модули, функционирующие на основе нечеткой логики, разрабатываются для решения отдельной задачи, например, управления отдельным параметром объекта. При необходимости достижения нескольких целей (зачастую взаимосвязанных), например, следование вдоль траектории и избегание столкновений с внешними объектами окружения, проектирование базы знаний происходит с учетом этих требований различными методами (сложные правила, блоки простых правил).

Агент расположен в среде, модель которой может быть как детерминированной, так и недетерминированной. В таком случае, под агентом понимают автономную сущность (реализованную программно, технически, формально), которая имеет возможность получать информацию о своем окружении и действовать, изменяя состояние, как свое внутреннее, так, возможно и состояние окружения (в т.ч. и других агентов). При агентном построении системы управления объект управления располагается в некоторой среде, сам же объект управления представляет собой оболочку для размещения агента.

Агенты в общем виде могут использовать следующие типы архитектуры: реактивная (принцип «стимул → реакция»), делиберативная (использование некоторых «рассуждений» на основе символьных представлений знаний) и когнитивная (принцип организации когнитивных систем).

УДК 62.50

ТЕХНОЛОГИИ ПОЛУЧЕНИЯ ФУНКЦИЙ ВЛИЯНИЯ ДЛЯ СЛОЖНЫХ СИСТЕМ

М.В. Васильская, аспирант, П.В. Северилов, аспирант
Винницкий национальный технический университет
taisaborovska@gmail.com

Сегодня многие технические системы – динамичные, многоуровневые, не имеющие достаточного опыта эксплуатации. Типовые примеры – системы мобильной связи и только зарождающиеся – биореакторрные системы. В условиях быстрых зменений в подсистемах желательно иметь функции для оценки влияния изменений в некоторой подсистеме на показатели эффективности системы в целом. Выбрана технология, сочетающая чисто эмпирические имитационные методы типа построения деревьев влияния и аналитические методы анализа чувствительности. Выбираем также технологию разработки базовой модели, максимально согласованную с технологией разработки программного обеспечения: - для описания вычислительной системы подход на базе "состояния" – матрично-векторной иерархической структуры, которая является компромиссом между удобством описания системы и размерностью; - выполняем иерархическую декомпозицию модели функционирования системы на малые - не больше десяти строк кода функциональные модули, каждый модуль тщательно тестируем, прежде чем включать в рабочую модель; - модули имитации поведения формируем как операторы перехода между состояниями:

- $x_{k+1} = A \cdot x_k + B \cdot u_k$ - линейная система,
- $Mu_{k+1} = Mu_{k+1} + Nast\left(Mu_k, dMu_k\right)$ - нелинейная

система;

- $Mu_{k+1} = Op(M_k, U_k, P)$ нелинейная система, объекты - матрицы состояния, U_k, P - управление и параметры.

Используем векторизацию вычислений. В данном случае суть векторизации в применении определенного оператора, который обрабатывает структуру данных определенного класса, - "состояние системы текущее" и выдает структуру данных "состояние распределенной системы следующее". Функции межуровневых связей определяются как переменные верхнего уровня, которые являются параметрами моделей нижнего уровня, а модели принадлежат к одному классу. Суть предлагаемых моделей в том, что связи между уровнями формируются как функции влияния технических показателей моделей нижнего уровня на показатели моделей верхнего уровня. Функции влияния являются многомерными, сложными, включают в себя нечеткую оптимизацию, агрегирование и др. На рисунке приведен пример пары: «состояние» и «оператор преобразования состояния» с применением векторизации.

$$smi^{(1)} := \begin{bmatrix} 7 \\ \begin{pmatrix} 7 & 2 & 5 \\ 4 & 3 & 6 \\ 5 & 0 & 0 \end{pmatrix} \\ \begin{pmatrix} 12 & 9 & 11 \\ 2 & 7 & 7 \\ 5 & 8 & 9 \\ 4 & 5 & 6 \end{pmatrix} \\ (4 \;\; 4 \;\; 3) \\ (22 \;\; 14 \;\; 12) \end{bmatrix}$$

$$Ypr3(sm, Vpr) := \left| \begin{array}{l} Vv2 \leftarrow vsa(sm_3) \\ S32 \leftarrow smH(Vpr, Vv2) \\ S33 \leftarrow sev(S32) \\ S4 \leftarrow fuf(S33) \\ S5 \leftarrow pup(S33) \\ BY \leftarrow kolVza(vp1, vp2) \\ S1 \leftarrow mean(BY_2) \cdot last(Vpr) \\ S2 \leftarrow BY_2 \\ rozpo \leftarrow delsum3(S2, S33, Vpr) \\ S31 \leftarrow rozpo_1 \\ qq \leftarrow (S1 \;\; S2 \;\; S31 \;\; S4 \;\; S5) \\ vyxod \leftarrow qq^T \end{array} \right.$$

$$By_1 = 3 \qquad By_2 = \begin{pmatrix} 6 \\ 5 \\ 7 \end{pmatrix}$$

В целом построена система рабочих моделей, позволяющая работать с имитационной моделью, как с реальным объектом.

УДК 004.724.2

ОСОБЕННОСТИ СИСТЕМЫ УПРАВЛЕНИЯ СЕТЕВЫМИ СОЕДИНЕНИЯМИ НА БАЗЕ ПРОТОКОЛА RADIUS

В.Ю. Болибрук, магистрант
Киевский национальный университет технологий и дизайна
20awesome@gmail.com

В настоящее время все большую значимость приобретает обеспечение защиты сетевых коммуникаций. Так как получение неавторизованного доступа к сетевым ресурсам зачастую является первым шагом к различным действиям разрушительного характера, создание качественной системы идентификации удаленных сетевых подключений представляется очень важным.

В настоящее время существует достаточно много различных систем сетевой идентификации на базе протокола RADIUS. Главной отличительной особенностью RADIUS систем контроля доступа является их ориентация преимущественно на работу под управлением различных версий ОС Unix. Использование данного программного обеспечения, однако, предполагает его тесную интеграцию как минимум с системами учета сетевых ресурсов и системами внутрисетевой авторизации в корпоративных сетях. Так как базовые версии демонов RADIUS редко бывают ориентированы на подобную интеграцию, их использование обычно подразумевает установку так называемых "патчей", работа которых обычно заключается в подмене стандартных модулей чтения конфигурации пользователей и сохранения статистики. Подобная

доработка, естественно, не ведет к повышению надежности работы программ, так как авторская документация на исходные тексты в большинстве случаев отсутствует, и модификация делается "методом проб и ошибок". Дополнительной проблемой для ориентированных на ОС Windows пользователей является перекомпиляция оригинальных исходных текстов.

Одной из серьезных проблем безопасности существующих систем является хранение зашифрованных алгоритмом DES паролей пользователей в текстовых файлах. Так как в настоящее время широко известен факт недостаточной криптостойкости стандартного алгоритма DES.

Устранением большинства существующих проблем могло бы стать создание демона RADIUS, построенного на базе современных стандартов программирования, обеспечивающего портирование на различные операционные системы, и изначально допускающего подключение внешних модулей авторизации и статистики.

Именно такое решение и было принято в нашей организации. В качестве языка программирования был выбран язык Java, как наиболее полно удовлетворяющий предъявленным требованиям.

В настоящее время создана тестовая версия демона RADIUS, поддерживающая модули авторизации и статистики, обеспечивающие обмен информацией с RDBMS Oracle. Модули авторизации и статистики реализованы с использованием технологии JDBC. Данный подход обеспечил возможность хранения пользовательских учетных записей в таблицах базы данных, благодаря чему получить информацию о паролях становится значительно труднее, т.к. для этого необходимо пройти процедуру авторизации сервера Oracle.

УДК 004.724.2

СПЕЦІАЛІЗОВАНІ КОМП'ЮТЕРНІ СИСТЕМИ GPS- НАВІГАЦІЇ

О.П. Поволоцький, магістрант
Київський національний університет технологій і дизайну
fargusllck@gmail.com

Будь-яка компанія або організація, що має у своєму розпорядженні автомобільний транспорт, безумовно, зацікавлена в його цільове використання і зниження до мінімуму матеріальних втрат. Власники ж особистих автотранспортних засобів зацікавлені в першу чергу в їх збереження і безпеки. Сьогодні вирішити ці та низку інших проблем, пов'язаних з утриманням різних видів транспорту, здатні супутникові системи моніторингу - системи GPS (GPRS).

У чому полягає сенс використання супутникової системи спостереження на транспортному підприємстві? Супутниковий моніторинг (супутникова система спостереження за транспортом) дозволяє встановити тотальний контроль за пересуванням будь-якої кількості транспортних засобів у режимі реального часу. Слідкування за транспортом, яке здійснюється за допомогою GPS системи, здатне виявити такі явища, як нецільове використання транспорту, недотримання встановленого маршруту, нецільове використання виділеного запасу палива. Результатом подібного контролю автотранспорту є негайне і істотне зменшення видаткової частини бюджету транспортної компанії. Системи спостереження за транспортом широко впроваджуються сьогодні в практику роботи підприємств, основною сферою

діяльності яких є вантажні й пасажирські перевезення. Затребуваними є системи GPS / GPRS моніторингу і в роботі «Швидкої допомоги», а також служб порятунку. Своєчасне отримання достовірної інформації про місцезнаходження і маршрут транспортного засобу є однією з головних умов ефективності будь-якого підприємства, яке використовує в своїй діяльності автотранспортні засоби. Використання систем супутникового стеження дозволяє вирішувати цілий ряд проблем, які постають перед транспортними підприємствами щодня. Припинення практики «лівих» рейсів та нецільового використання палива, упевненість у тому, що всі автомобілі точно слідують встановленим маршрутом, а запізнення відбулося з не залежних від водія причин - ось лише деякі переваги, які отримує компанія, яка встановила у себе системи GPS / GPRS моніторингу транспорту. Не дивно, що системи GPS / GSM є на сьогоднішній день абсолютними лідерами серед різних пристроїв стеження за автомобілем.

Впровадження систем GPS контролю передбачає встановлення на автотранспортні засоби мобільних терміналів, встановлення датчиків, а також організацію робочого місця, з якого буде вестися GPS моніторинг транспортних засобів.

Встановивши системи моніторингу автотранспорту GPS, підприємство або організація отримують постійний доступ до інформації про те, де знаходиться те або інше, що належить їй транспортний засіб. Практика показує, що GPS GSM моніторинг дозволяє також істотно збільшити термін експлуатації автопарку. Один з важливих моментів впровадження систем супутникового стеження транспорту є підвищення безпеки перевезень. З машини, обладнаної GPS трекером, водій може миттєво подати тривожний сигнал у випадку виникнення небезпечної ситуації. Прямими результатами впровадження в практику роботи транспортного підприємства систем супутникового стеження GPS є економія паливно-мастильних матеріалів, зменшення пробігу

автомобілів, підвищення дисципліни персоналу. Це далеко не повний перелік тих переваг, які отримує організація, яка використовує у своїй діяльності супутниковий моніторинг транспорту. Київ - місто, відомий своїм величезним кількістю транспорту і складною ситуацією на дорогах, як жоден інший місто країни, вимагає застосування подібних систем на будь-яких підприємствах, що мають власні автотранспортні засоби. Звичайно, системи супутникового спостереження автомобіля застосовуються не тільки в столиці - географія їх використання сьогодні виключно широка. Адже результатом впровадження системи, що здійснює контроль автомобілів, є істотне підвищення якості надаваних транспортних послуг та збільшення обсягу перевезень.

Системи спостереження за авто виявляються корисними не тільки для організацій, що мають власний автопарк, але і для власників особистого транспорту. В даний час пристрої GPS моніторингу автомобіля включаються до складу охоронних систем. Супутникове сигналізація, на відміну від звичайних охоронних систем, відноситься до систем активного захисту автомобіля. Будь-яка спроба проникнення в автомобіль, на який встановлена супутникова сигналізація, супроводжується оповіщенням власника автомобіля або диспетчерського пульта. супутникове стеження авто дозволяє його власникові завжди мати актуальну інформацію про місцезнаходження автомобіля в будь-який момент часу. Наявність систем GPS моніторингу (супутниковий моніторинг) допоможе власнику автомобіля не тільки в екстреній ситуації. Інформація, отримана за допомогою GPS трекера, дозволить водієві уникати пробок на дорогах, знизити ризик аварійної ситуації. GPS моніторинг авто дає можливість спостерігати за станом автомобіля і його двигуна, кількістю палива. Ще одна зручність, яке надає GPS моніторинг - навігація на незнайомій місцевості, можливість досягти будь-якого місця призначення у найкоротший термін.

2. МЕТОДИ ТА ЗАСОБИ ОБРОБКИ ДАНИХ

УДК 004.89:53.088:519.6:681.5

МЕРЫ БЛИЗОСТИ МЕЖДУ ОБЪЕКТАМИ, ПОВЫШАЮЩИЕ ДОСТОВЕРНОСТЬ РАСПОЗНАВАНИЯ ОБЪЕКТОВ В СИСТЕМАХ ТЕХНИЧЕСКОГО ЗРЕНИЯ.

Р.К. Мамедов[1], А.С. Муталлимова[2], Т.Ч. Алиев[3]
Азербайджанская государственная нефтяная академия
[1]rahim1951@mail.ru, [2]ayzberg69@mail.ru,
[3]alievtima18@rambler.ru

Для определения сходства изображения объекта из базы данных с изображением полученного объекта применяется некоторая мера близости между объектами (МБМО), с помощью которой получают численную оценку сходства изображений. Для этого проверяется близость измеряемых признаков, характеризующих объект. Общеизвестные МБМО Евклида, Манхэттена, Канберра, и т.п. обеспечивают подавление аддитивной погрешности и частичную минимизацию мультипликативной погрешности, не корректируя изменение масштаба. Хотя они являются математически обоснованными (удовлетворяют трем условиям метрики), с практической точки зрения, вследствие указанных выше свойств, их эффективность низкая. Поэтому, обязательным условием для эффективной МБМО является минимизация или полное подавление мультипликативной погрешности с масштабными изменениями изображений объектов. В докладе рассматриваются три МБМО удовлетворяющие указанным условиям и доказывается их эффективность:

1. МБМО минимизирующая влияние изменения масштабов и мультипликативной погрешностей изображений объектов при их распознавании:

$$Z_1 = \sum_{i=1}^{N} \left| \frac{x_i}{x_{cp}} - \frac{y_i}{y_{cp}} \right| \text{ при: } x_{cp} \neq 0 \text{ и } y_{cp} \neq 0$$

где: x_i, x_{cp} и y_i, y_{cp} – соответственно, значения и среднеарифметическая величина признаков распознаваемого и эталонного объектов; N – число признаков.

2. МБМО обеспечивающая инвариантность распознавания объектов к изменениям масштаба и мультипликативной погрешности их изображений:

$$Z_2 = \sum_{i=1}^{N} \left\| \frac{x_i - x_{i+1}}{y_i - y_{i+1}} \right| - \left| \frac{x_{i+2} - x_{i+3}}{y_{i+2} - y_{i+3}} \right\| \text{ при: } y_i \neq y_{i+1} \text{ и } y_{i+2} \neq y_{i+3}$$

где: x_i, x_{i+1}, x_{i+2}, x_{i+3} и y_i, y_{i+1}, y_{i+2}, y_{i+3} – соответственно, значения признаков распознаваемого и эталонного объектов

3. МБМО обеспечивающая высокую чувствительность к изменению данных и инвариантность распознавания объектов к мультипликативной и масштабной погрешностям их изображений. Первоначально, из массивов признаков распознаваемого объекта и эталона вычитаются их средние значения. Далее, с помощью формулы преобразования Фурье определяются спектры полученных массивов. В результате получают массивы комплексных чисел. Тогда указанная МБМО примет вид:

$$Z_3 = \sum_{i=1}^{n} \left| \frac{Re_i(S_{X'})}{Re_i(S_{Y'})} - \frac{Im_i(S_{X'})}{Im_i(S_{Y'})} \right|$$

при $Re_i(S_{Y'}) \neq 0$ и $Im_i(S_{Y^i}) \neq 0$

где: $Re_i(S_{X'})$, $Im_i(S_{X'})$ и $Re_i(S_{Y'})$, $Im_i(S_{Y^i})$ - соответственно, вещественные и мнимые части комплексных чисел полученных после преобразования Фурье, n – число элементов массивов.

УДК 681.32

ФОРМИРОВАНИЕ ДЕШИФРИРУЕМО-СТОЙКОГО ПРЕДСТАВЛЕНИЯ ИЗОБРАЖЕНИЙ В СИСТЕМАХ КОМПРЕСИИ

В.В. Баранник, д.т.н., с.н.с, С.А. Сидченко, к.т.н., В.В. Ларин
Харьковский университет Воздушных Сил
Barannik_V_V@mail.ru

Во всем потоке информации, циркулирующей в информационном пространстве, увеличивается доля видеоинформации. Процессы обработки и передачи данных в современных инфокоммуникационных системах включают в себя этапы компрессии, шифрования и помехоустойчивого кодирования. Недостатком рассмотренного подхода обработки данных является то, что системы шифрования не учитывают потенциальные возможности технологий компрессии относительно разрушения семантической структуры изображения. Предлагается строить дешифрируемо-стойкие преобразования, что означает дополнительное скрытие сообщений с использованием особенностей источника информации. Это позволит: повысить сложность дешифровки изображений для существующих систем обработки; снизить временные затраты на процесс реконструкции сжатых данных при выполнении требований относительно заданной сложности дешифрирования.

Формулируются требования, обеспечивающие реализацию функций сложностно-дешифрируемых преобразований.

1. Формирование кодовых конструкций должно осуществляться по интегральному принципу. В этом случае

формирование кодовых конструкций проводится в два этапа: формирование значения N, несущего информацию сразу о нескольких элементах сообщения A, т.е. $N = f(A)$, где N – значение кода, сформированное для исходного сообщения A на основе правила $f(\bullet)$; организация кодового C представления значения N, т.е. формирование кодового слова не для исходного сообщения, а для величины N: $C = f_к(N)$.

2. Исходное сообщение можно восстановить только в случае наличия полных сведений о векторе служебных данных S, т.е. если $S^{\bullet} = S$, то $A = f^{(-1)}(N)$. В противном случае при отсутствии хотя бы одного элемента вектора служебных данных точное восстановление исходного сообщения была бы невозможной, т.е. если $S^{\bullet} \neq S$, то $A \neq f^{(-1)}(N)$, где $f^{(-1)}(\bullet)$ – обратный оператор получения сообщения A по значению кода-номера N.

3. Должна изменяться двумерная структура изображения и в первую очередь та информация, которая отвечает за низкочастотные составляющие. Следовательно, кодовые структуры должны быть двумерными.

4. Элементы кодовой конструкции не должны соответствовать элементам исходного сообщения. Должно существовать как минимум одно промежуточное звено между процессом обработки исходных сообщений и формированием кодового слова сжатого представления, что позволит изменять структурное и статическое соответствие между исходным сообщением и кодовой комбинацией на выходе процесса сжатия.

5. На изменение семантической структуры изображения в процессе его сжатия не должны влиять характеристики обрабатываемых изображений, т.е. степень корреляции, степень насыщенности мелкими объектами.

УДК 004.93’14

ДОСЛІДЖЕННЯ ХАРАКТЕРИСТИК КОМПРЕСІЇ ТА ТОЧНОСТІ ПРИ АПРОКСИМАЦІЇ ВІЗУАЛЬНИХ ОБРАЗІВ

Р.А. Мельник, д.т.н., професор,
Т.С. Климаш, студент
Національний університет «Львівська політехніка»
ramelnyk@polynet.lviv.ua

Для отримання апроксимації зображення кольорове зображення перетворюємо у відтінки сірого. Кожна елементарна клітинка (піксель) приймає значення від чорного до білого кольору. Діапазон всіх можливих значень яскравості знаходиться в межах 0÷255

Рядок яскравості пікселів зображення апроксимуємо поліноміальною функцією вигляду:

$$P(\vec{A},\omega) = A_0 + A_1\omega + ... + A_m\omega^m, \qquad (1)$$

Приклад рядка яскравості пікселів та його апроксимації наведено на рис. 1.

Рис.1. Реальний та апроксимований ряд яскравості пікселів

Апроксимацію здійснюємо різними способами, керуючи довжиною та шириною рядка яскравості пікселів.

У випадку ширини рядка у два і більше пікселів для апроксимації подається усереднене у стовпчику значення яскравості. Рядок апроксимується повністю або почастинно, шляхом застосування алгоритму до частини рядка яскравості. Основним керуванням є степінь полінома та довжина слова його коефіцієнтів. Приклади апроксимації деяких зображень різними способами наведені в таблиці 1.

Таблиця 1 – Характеристики компресії та точності

Зображення	Характеристики	Спосіб апроксимації				
		По одному рядку	По два рядки	По одному рядку і по два стовпчики	По одному рядку і по три стовпчики	По два рядки і по три стовпчики
Рис. 3а	Степінь полінома	12	12	9	6	6
	Похибка, %	2,5696	2,6095	1,22	1,0085	1,13
	Сигнал/шум, дБ	31,80	31,66	38,22	39,92	38,88
	Розмір, біт/піксел	4,40	2,20	6,77	7,11	3,55
Рис. 3б	Степінь полінома	12	12	9	6	6
	Похибка, %	2,6836	2,7419	2,3021	2,2902	2,4192
	Сигнал/шум, дБ	1,42	31,23	32,75	32,80	32,48
	Розмір, біт/піксел	2,98	1,49	4,58	4,81	2,41
Рис. 3в	Степінь полінома	12	12	9	6	6
	Похибка, %	7,9949	8,0481	6,6830	6,3304	6,4055
	Сигнал/шум, дБ	21,94	21,88	23,50	23,97	23,86
	Розмір, біт/піксел	1,28	0,64	1,96	2,06	1,03
Рис. 3г	Степінь полінома	12	12	9	6	6
	Похибка, %	10,5255	10,5688	7,5839	6,7390	6,8523
	Сигнал/шум, дБ	19,55	19,51	22,40	23,42	23,28
	Розмір, біт/піксел	2,08	1,04	3,2	3,36	1,68
Рис. 3д	Степінь полінома	12	12	9	6	6
	Похибка, %	7,9177	8,101	6,6887	6,6898	6,9565
	Сигнал/шум, дБ	22,02	21,82	23,49	23,49	23,15
	Розмір, біт/піксел	2,77	1,39	4,26	4,48	2,24

УДК 681.3

ДОСЛІДЖЕННЯ ЧИСЛОВИХ МОДЕЛЕЙ ДАНИХ

В.А. Лужецький, д.т.н, професор,
А. В. Кульчицький, магістрант
Вінницький національний технічний університет
andriykulchitskiy@yandex.ru

Ущільнення інформації – це процес, метою якого є одержання більше компактного вихідного потоку інформаційних одиниць із деякого початкового некомпактного вхідного потоку за допомогою деякого їхнього перетворення.

Цей процес можна розділити на два рівно важливих етапи:

- моделювання;
- кодування.

Для створення оптимального методу ущільнення недостатньо розробити безліч алгоритмів. Необхідно правильно оцінити модель джерела інформації и обрати той алгоритм, який розроблявся на основі цієї моделі.

В даній роботі буде розглядатися метод ущільнення інформації на основі функціональних залежностей. Суть етапу моделювання даного методу в тому, що вхідні дані, що підлягають ущільненню, розглядаються як послідовність символів 0 і 1. Відповідно до числової моделі джерела даних, послідовність символів розбивається на блоки певної довжини l, і кожному символу в блоці відповідає своя певна вага w_i. Таким чином, вхідні дані представляються як послідовність чисел з деяким законом формування.

Для дослідження результатів моделювання створено

спеціальну програму мовою програмування java.

Дана програма складається з двох функціональних частин:

- блоку, що відповідає за моделювання;
- блоку візуалізації результатів.

Блок, що відповідає за моделювання, виконує такі дії:

- розбиття файлу на блоки заданої розмірності;
- проведення перетворень у блоках;
- представлення послідовності бітів числом, з деяким законом формування.

Блок візуалізації результатів відповідає за виведення графічних результатів на екран.

В результаті моделювання блок, що складається з n біт, представляється n-розрядним числом у певній системі числення, параметри якої задаються. Результатом дослідження є статистика появи всіх чисел, які можна отримати за допомогою n біт.

Для кращого представлення вхідних даних використовуються перетворення, такі як:

- значення за модулем;
- транспозиція бітів, яка починається з заданого біту;
- циклічний зсув.

Вплив на числову модель джерела вище зазначених перетворень не неоднозначний. Іноді він значний, а іноді ні.

В результаті проведених досліджень над різними типами інформації визначені такі фактори, що пливають на числову модель:

- розрядність блоків, на які розбивається файл;
- тип файлу;
- вміст файлу.

УДК 68.13

АДАПТИВНИЙ ПІДХІД ЩОДО ПРОГНОЗУВАННЯ ЧАСОВИХ РЯДІВ

Р.Н. Квєтний, д.т.н., професор,
В.Ю. Коцюбинський, к.т.н., доцент,
Н.В. Казимірова, аспірант
Вінницький національний технічний університет
nkazimirova@gmail.com

Процес прийняття рішень є одним із важливих етапів для будь-якої цілеспрямованої людської діяльності. Однією з особливостей фінансового ринку є його динамічність і різноманітність факторів, які впливають на ситуацію. Дана властивість ринку призводить до виникнення нових ризиків та нестабільних умов, що пов'язано з неможливістю передбачити зміни при роботі. Саме тому все більш необхідним стає точне і своєчасне визначення основних механізмів, що змінюють ситуацію та прогнозування основних тенденцій її зміни. В сучасних умовах дедалі актуальнішим стає нове завдання – представити майбутнє, яке не може інтерпретуватися як звичайне продовження минулого у зв'язку з тим, що це майбутнє набуває істотно відмінних форм і структур.

Дана робота спрямована на розробку алгоритмічного інструментарію для створення проблемно-орієнтованих систем підтримки прийняття рішень, які можуть бути ефективно застосовані для прогнозування поведінки об'єктів та ефективно використовуватися в умовах невизначеності.

Більшість методів технічного аналізу представлена математичними моделями різної складності, що описують

рух ринкових цін. На сьогодні є тільки один спосіб знаходження параметрів моделі - використання історичних рядів даних.

Практично всі попередні експертні системи моделювали процес прийняття експертом рішення як чисто дедуктивний процес. Проблема полягає у прийнятті рішень в умовах апріорної невизначеності, обумовленої неточністю або неповнотою вхідних даних, нечіткістю мети, стохастичною природою зовнішніх впливів, людським фактором та ін. Саме тому в системах підтримки прийняття рішень доцільно використовувати адаптивний підхід для прогнозування часових рядів. Даний підхід до прийняття рішень використовує асоціативні прийоми для пошуку ситуації, що виникали раніше. Розглядаючи новий випадок, шукається схожий прецедент в базі даних і пропонується варіант його рішення з витікаючими наслідками. Тобто, замість того, щоб кожного разу шукати рішення спочатку, можна спробувати використовувати рішення, прийняте в схожій ситуації у минулому, або адаптувати його до поточного випадку. Особливою перевагою адаптивного підходу є можливість накопичення знань про ситуації в зовнішній, по відношенню до об'єктів, базі даних і використання цих знань іншими об'єктами, підключеними до тієї ж бази.

В розробленій системі реалізовано механізм автоматичної класифікації прийняття рішень в залежності від очікуваного значення прибутку, як сигналу відкриття позиції, що підвищує ефективність прийняття рішень і надає можливість отримати максимальний прибуток при мінімальному ризику від здійснюваних фінансових операцій.

УДК 519.168

АЛГОРИТМІЧНЕ ЗАБЕЗПЕЧЕННЯ ДЛЯ РОЗПАРАЛЕЛЮВАННЯ ЗАДАЧІ КОМІВОЯЖЕРА ВЕЛИКОЇ РОЗМІРНОСТІ

Р.П. Базилевич, д.т.н., професор,
Р.К. Кутельмах, асистент, Б.О. Кузь, студент
Національний університет "Львівська політехніка"
rbaz@polynet.lviv.ua

Задача комівояжера має широке застосування: в транспортних системах, автоматизованому проектуванні, аналізі та синтезі хімічних сполук, кристалографії та інших. Переважна частина цих задач має велику та надвелику розмірність: сотні тисяч та мільйони змінних. Тому актуальною є розробка методології розв'язування такого класу задач за невеликий час з доброю якістю. Задача має факторіальну обчислювальну складність, тобто відноситься до важковирішуваних класу NP.

Точні методи, зокрема гілок та границь, а також існуючі евристичні, зокрема найкращий з них LKH, який має квадратичну обчислювальну складність, є непридатними для таких задач. Необхідною є розробка методів, що мають лінійну або лінійно-логарифмічну обчислювальну складність та забезпечують високу якість.

Запропонований метод має такі етапи:

1. Кластеризація робочого поля з виділенням підмножин з потужністю не більше 1000 – 15000 точок.
2. Розв'язування задачі в межах кожної підмножини – знаходження часткових розв'язків.
3. Зшивання часткових розв'язків в єдиний розв'язок.

4. Оптимізація розв’язку.

На кожному з цих етапів можливих є застосуванням ряду алгоритмів. Так, для кластеризації робочого поля розроблені такі підходи:

1. Алгоритм на основі поширення хвилі найменшими ребрами мережі Делоне.

2. Алгоритм на основі рівномірного поширення хвилі гранями – трикутниками тріангуляції.

3. Алгоритм на основі поширення хвилі найменшими гранями – трикутниками тріангуляції.

Кожен з цих алгоритмів створює підмножини специфічної форми та може бути використаним в залежності від структури робочого поля. Для знаходження часткових розв’язків задачі в межах кожної підмножини використовується найкращий з відомих евристичних алгоритмів – LKH. Він забезпечує високу якість. Для зшивання часткових розв’язків в єдиний формуються зони стикування кластерів у вигляді торів на межах кластерів, розглядаються точки цих зон, а для решти частини маршруту створюються фіксовані ребра з дуже малою віддалю. Оптимізація розв’язків здійснюється декількома алгоритмами: виділенням областей на межах трьох кластерів, скануванням за маршрутом та геометричним.

Як показали експерименти на ряду відомих тестів, розроблена методологія скорочує час розв’язання задачі в декілька раз при збереження практично такої самої якості як найкращі з існуючих евристичних алгоритмів.

Запропонована методологія забезпечує можливість широкого розпаралелювання задачі великої та надвеликої розмірності на багатопроцесорних та розподілених комп’ютерних системах.

УДК 519.168

ФУНКЦІОНАЛЬНЕ НАПОВНЕННЯ ПРОГРАМНОЇ СИСТЕМИ З ШИРОКИМИ МОЖЛИВОСТЯМИ ДЛЯ ДЕКОМПОЗИЦІЇ СКЛАДНИХ СХЕМ

Р.П. Базилевич, д.т.н., професор,
М.А. Влах, студент, Н.І. Пелих, студент
Національний університет "Львівська політехніка"
rbaz@polynet.lviv.ua

При розв'язуванні багатьох прикладних задач великої розмірності, зокрема транспортних, автоматизованого проектування та інших виникає потреба розбиття складної схеми на частини з заданими обмеженнями. Такими задачами, наприклад, є:

– однорівнева декомпозиція схеми на частини з заданим їх числом, з обмеженнями на число елементів в кожній частині, на параметри складових елементів та іншими;

– багаторівнева ієрархічна декомпозиція з заданим числом рівнів та параметрами розбиття на кожному рівні (зокрема, числом утворених підсхем, числами їх складових елементів та іншими);

– пакування схеми в підсхеми з заданими обмеженнями на числа елементів та зовнішніх зв'язків, зокрема пакування програмованих логічних матриць, кількість яких необхідно мінімізувати;

– розбиття транспортної задачі на частини та багато інших.

Всі виділені задачі відносяться до комбінаторних класу NP, тобто важковирішуваних. Їх обчислювальна складність – експонентна (показникова, факторіальна).

Розв'язування цих задач здійснюється в розробленій програмній системі в два етапи. На першому знаходиться деяке початкове рішення, на другому воно оптимізується. Методологічною основою для проектування базових алгоритмів системи вперше обрано запропонований Р.П. Базилевичом метод оптимального згортання схеми, який забезпечує виділення ієрархічно вкладених кластерів схеми, що відповідають її згусткам. В розроблених алгоритмах оперування здійснюється такими кластерами замість базових елементів схеми, що не тільки зменшує обчислювальну складність, але також дає кращі результати.

Базовими процедурами є:

– побудова дерева оптимального згортання схеми з виділенням ієрархічно вкладених кластерів. Параметрами є критерії об'єднання елементів та кластерів на кожному кроці згортки: числа внутрішніх та зовнішніх зв'язків, їх різниця, а також відносні - до числа складових елементів; довжини відфільтрованих зв'язків, числа об'єднуваних на кожному кроці елементів та кластерів, процент згорнених на кожному кроці кластерів та інші;

– послідовне виділення кластерів з заданими параметрами;

– паралельно-послідовне виділення кластерів з заданими параметрам;

– усунення бажаної кількості елементів з кластера;

– додаванням бажаної кількості елементів до кластера;

– обмін елементами та кластерами між підсхемами;

– вихід з локальних екстремумів та інші.

Як показали експерименти, для всіх досліджених відомих тестових задач отримані результати не є гіршими, а в багатьох випадках кращими, ніж досягнуті іншими методами.

УДК 51-77:004.4

ИССЛЕДОВАНИЕ МЕТОДОВ РЕШЕНИЯ ЗАДАЧИ ОПТИМИЗАЦИИ КОРМОВЫХ РАЦИНОВ

С.Н. Гриша, д.т.н., профессор, А.И. Муха, магистрант
Национальный технический университет Украины
«Киевский политехнический институт»
alexei.mukha@gmail.com

Решение конкретной задачи оптимизации связано с выбором математического метода, который приводил бы к конечным результатам с наименьшими затратами на вычисления или же давал возможность получить наибольший объем информации об искомом решении. Выбор того или иного метода в значительной степени определяется постановкой оптимизационной задачи, а также используемой математической моделью объекта оптимизации.

Экономико-математическая модель задачи оптимизации кормовых рационов для многопрофильных птицеводческих корпораций, производственная деятельность которых характеризуется рядом специфических свойств, представлена авторами в предыдущих публикациях. Ее особенностями является разреженность матрицы ограничений, а также большая ее размерность (более 8192 ограничений).

В предыдущих публикациях также был рассмотрен один из методов решения данной задачи – при помощи модуля Risk Solver Platform среды Excel. Проведенные вычислительные эксперименты показали, что задачу средних размерностей (до 100 рецептов, 100 ингредиентов, 75 веществ) можно решить этим методом менее чем за 1

минуту. Что же касается задач больших размерностей, то Excel накладывает ограничения на общий их размер, определяемые настройками системы (до 8192 ограничений, 2000 переменных).

Для решения данной задачи возможно применение табличного симплекс-метода. Поскольку матрица ограничений предложенной модели разрежена и имеет структурированный вид, это позволяет значительно сократить время выполнения итерации метода. Однако, как показали исследования, применение этого метода к данной задаче неэффективно из-за большой размерности симплекс-матрицы, что ведет к значительным временным затратам. Кроме того, при использовании табличного симплекс-метода количество ненулевых элементов матрицы ограничений растет от итерации к итерации.

Поэтому последующие исследования были направлены на поиск методов решения данной задачи с учетом указанных особенностей матрицы ограничений.

Проведенные эксперименты показали, что более эффективным для данной задачи является модифицированный симплекс-метод. Его использование позволяет за конечное число итераций получить оптимальное решение задач даже большой размерности (до 150 рецептов, 150 ингредиентов, 75 веществ) за приемлемое время (до 10 минут). Преимуществом этого метода является уменьшение количества вычислений за счет пересчета на каждой итерации не всей матрицы ограничений, а лишь обратной базисной матрицы, соответствующей текущей итерации.

Именно этот метод и был использован при реализации подсистемы оптимизации кормовых рационов в рамках интегрированной системы управления птицеводческой корпорации.

УДК 004.627+517.962.27

ДОСЛІДЖЕННЯ МОЖЛИВОСТІ УЩІЛЬНЕННЯ ДАНИХ ЗА ДОПОМОГОЮ ЛІНІЙНИХ РЕКУРЕНТНИХ ПОСЛІДОВНОСТЕЙ ДРУГОГО ПОРЯДКУ

В.М. Михалевич, д.т.н., професор, О.В. Михалевич, студент
Вінницький національний технічний університет
vmykhal@gmail.com

Вельми принадною виглядає перспектива ущільнення даних за допомогою алгоритмів, що базуються на перетворенні великих чисел у маленькі за допомогою певних нелінійних співвідношень, зокрема лінійних рекурентних послідовностей другого порядку.

Розглянемо узагальнені послідовності Фібоначчі, а саме послідовності для яких кожний член починаючи з третього дорівнює сумі двох попередніх:

$$\boldsymbol{u_1,\ u_2,\ldots,u_n = u_{n-2} + u_{n-1},\ldots\ \ n = 3,4,\ldots.} \qquad (1)$$

де u_1, u_2 - додатні цілі числа. Для таких послідовностей сформульовано та доведено наступну властивість: будь-яка послідовність чисел, що визначається співвідношенням (1), при $m>2$ містить 4 або 5 m-значних чисел.

Базуючись на замкненому співвідношенні для загального члена послідовності (1)

$$\boldsymbol{u_n = u_1 \cdot \frac{\alpha^{n-2}-\beta^{n-2}}{\sqrt{5}} + u_2 \cdot \frac{\alpha^{n-1}-\beta^{n-1}}{\sqrt{5}},\ldots.} \qquad (2)$$

де

$$\alpha = \frac{1+\sqrt{5}}{2},\quad \boldsymbol{\beta = \frac{1-\sqrt{5}}{2},\ldots.} \qquad (3)$$

отримано співвідношення для обчислення кількості k_n m-значних чисел послідовності (1) в залежності від значень m, u_1, u_2:

$$k_n = \begin{cases} 5, & \left\{\dfrac{0,5\cdot\lg 5+m-\lg\left\{\frac{u_2-u_1}{\alpha}+u_1\right\}}{\lg\alpha}\right\} \le \left\{\dfrac{1}{\lg\alpha}\right\} \approx 0,79 \\ 4, & \left\{\dfrac{0,5\cdot\lg 5+m-\lg\left\{\frac{u_2-u_1}{\alpha}+u_1\right\}}{\lg\alpha}\right\} > \left\{\dfrac{1}{\lg\alpha}\right\} \approx 0,79 \end{cases}, \quad (4)$$

де через $\{x\}$ позначена дробова частина числа x.

Для оцінки перспективності застосування перетворень цілих чисел за допомогою послідовностей (1), отримано оцінку кількості унікальних послідовностей за певних обмежень на перші два члени. Під множиною унікальних послідовностей розумітимемо такий набір послідовностей, для кожної з яких виконується наступна умова: дана послідовність не може бути отримана відкиданням скінченого числа $p>0$ перших членів будь-якої іншої послідовності даної множини. Для визначення множини унікальних послідовностей та обчислення їх кількості за наявності певних обмежень на діапазон зміни перших двох членів послідовності було побудовано графічну ілюстрацію до розташування таких послідовностей, розроблено спеціальний алгоритм та отримано співвідношення для обчислення числа унікальних послідовностей q_N

$$q_N = \frac{1}{2}\cdot N\cdot(N+1), \quad (5)$$

перші два члени яких задовольняють умови

$$u_2 - u_1 \le 0, \quad u_1 \in [1, N], \quad u_2 \in [1, N]. \quad (6)$$

Теоретично установлено, що щільність заповнення послідовності натуральних чисел членами послідовності (1) не залежить від діапазону зміни перших двох членів послідовності та надто мала, що зумовлює необхідність подальших пошуків. Експериментальна перевірка за підтвердила достовірність висновків для певного діапазону значень перших двох членів послідовності.

УДК 621.391

СИНЕРГЕТИЧЕСКИЕ АСПЕКТЫ НЕЛИНЕЙНОГО РЕКУРРЕНТНОГО АНАЛИЗА ХАОТИЧЕСКОЙ ИНФОРМАЦИИ

Э.И. Владимирский, к.т.н., Б.И. Исмайлов, н.с.
Азербайджанская государственная нефтяная академия

Мощный транспорт информационных потоков циркулирующих в таких отраслях как экономика, медицина, экология, актуализируют проблему их оперативного анализа и принятия решений.

Если рассматривать инфраструктуру транспорта информации в таких отраслях как открытую систему, то рост и интенсивность этих потоков приводит к усложнению информационной составляющей, и та в свою очередь вызывает нарастание хаотических процессов. Эволюционные траектории в пространстве состояний системы становятся чувствительными к малым информационным воздействиям (флуктуациям). В результате кумулятивного эффекта в определённый момент система может переходить с одной траектории эволюционного развития на другую. Так наступает точка бифуркации – точка ветвления вариантов развития. Ветвления, в свою очередь, катализируют инновационный всплеск, вызывающий интенсификацию различных форм взаимодействий информации.

Изложенное выше позволяет информационную среду определить как самоорганизующуюся коммуникативную систему. В комплексном фазовом пространстве, характеризующим поведение среды, выделяются состояния, которые притягивают к себе

возможные траектории эволюции информационных систем. Эти состояния определяются как информационные аттракторы, по аналогии с понятием странный аттрактор в теории динамического хаоса.

Однако традиционные методы анализа нелинейных процессов требуют значительного объёма информации, что естественно, усложняет принятие корректного решения (прогноза).

Фундаментальную перспективу представляет использование метода рекуррентного анализа нелинейных процессов, не предъявляющего особых требований к данным и дающего удовлетворительные результаты.

Нелинейный рекуррентный анализ катализирует реализацию такой важной проблемы как управление динамикой хаотических систем (информационных процессов), то есть посредством достаточно слабых воздействий переводить первоначально хаотические системы на требуемый динамический режим и тем самым стабилизировать их поведение.

В этой связи в работе предлагается структура интеллектуальной системы предсказуемости и управления хаотическими процессами, идеологической основой которых является нелинейный рекуррентный анализ.

Таким образом, использование ограниченного объёма анализируемой информации и нетрадиционной визуализации в виде рекуррентных диаграмм, позволит, формируя новые структуры, повысить эффективность управления в контексте принятия корректного решения.

Предложенная структура системы реализована в программной среде MATLAB/Simulink.

УДК 004.942, 004.891.2, 004.021

МАТЕМАТИЧНІ МЕТОДИ МОДЕЛЮВАННЯ ПРОСТОРОВИХ СИСТЕМ НА ОСНОВІ БРОУНІВСЬКИХ ФРАКТАЛЬНИХ РЕЛЬЄФІВ ТА НЕЧІТКОЇ ЛОГІКИ

Я.І. Виклюк, к.ф.-м.н., доцент, докторант
Буковинський університет
vyklyuk@ukr.net

Популяризація активного відпочинку та рекреації в останні роки призвела до швидкого зростання кількості туристично-рекреаційних комплексів. Як-правило поява нового комплексу, чи активізація вже існуючого призводить до розростання інфраструктури населеного пункту та розширення урбанізованих площ під забудову. Стрімкий розвиток туристичної галузі вимагає швидких, кількісних, адекватних математичних методів та методик при прийнятті рішень. Одною з найбільш актуальних задач туристичної галузі є прогноз структури та форми туристичних поселень та урбанізованих територій. Низький рівень адекватності класичних математичних моделей ставить перед науковцями питання про розробку та впровадження сучасних методів математичного моделювання, таких як SoftComputing та фрактальна геометрія.

Метою наукових досліджень просторової організації було вивести ідеалізовану теорію розбудови міст в рамках жорстких обмежень. Довгий час просторова організація міст описувалась за допомогою геометрії Евкліда. Однак ідеалізовані міста були далекі від реально існуючих. Основною проблемою була саме неможливість застосування класичної математики до реальних об’єктів. За допомогою геометрії

Евкліда можна виміряти такі фундаментальні величини, як довжина, площа, тощо. Однак в реальних містах базовою «цеглиною» в більшості випадків є одиночний будинок. Будинки в свою чергу утворюють квартали. Квартали складаються з будинків, які впорядковані за певними законами самоподібності та обмежені дорогами, що відділяють квартали один від одного. Квартали утворюють самоподібну структуру, що залежить від спеціалізації атракторів, навколо яких ведеться забудова міста. В якості атракторів може виступати завод, розважальний центр, церква, ринкова площа міста, тощо.

В роботі наведено огляд можливих підходів до моделювання форм населених пунктів. Наведено особливості розвитку та внутрішньої структури невеликих туристичних поселень.

Обґрунтовано та наведено алгоритм розрахунку вхідних параметрів моделі. Представлено алгоритм побудови нечіткої бази знань та поля імовірності на основі нечіткого виводу Сугено. Запропоновано метод врахування поля імовірності забудови при побудові броунівського самоафінного фрактального рельєфу. Розроблено математичні методи моделювання броунівського руху для множини атракторів. Наведено аналітичний вигляд рівнянь фрактальних зрізів при броунівському русі.

Розроблена методика моделювання фрактального росту населених пунктів представлена у вигляді покрокового алгоритму та структурної схеми.

Апробація алгоритму проводилась на туристичному курорті Українських Карпат – м. Ворохта. Отриманій фрактал за формою, розмірністю та ступеню схожості показав достатній рівень точності. Це підтверджує адекватність моделі.

До переваг такого підходу можна віднести можливість моделювання як форми так і динаміку зростання населеного пункту в часі за допомогою математичних фракталів.

УДК 621.397.6

СИСТЕМА СЖАТИЯ ИНФОРМАЦИИ НА ОСНОВЕ БИНОМИАЛЬНЫХ ЧИСЕЛ

И.А. Кулик, к.т.н., доцент, С.В. Костель, аспирант
Сумской государственный университет
eikt@ukr.net

Нумерационное кодирование информации позволяет сжимать данные с неизвестными или заранее не заданными вероятностными характеристиками. Одним из наиболее перспективных методов является метод биномиального нумерационного кодирования. Данный метод основан на применении числовой функции биномиальной системы счисления:

$$F = \sum_{i=0}^{r-1} x_i C_{n-r+i}^{k-q_i} , \qquad (1)$$

где n и k – параметры биномиальной системы счисления, r – длина биномиального числа, q_i – сумма единичных значений разрядов x_i от (r–1)-го разряда до (i+1)-го включительно.

Метод биномиального нумерационного кодирования ориентирован на сжатие информации представленной в двоичном виде. Сжимаемые данные разбиваются на двоичные последовательности определенной длинны, которые могут быть представлены в виде равновесных комбинаций с известным количеством единиц (весом). Задача биномиального нумерационного кодирования состоит в переходе от равновесной комбинации к биномиальному числу и последующем вычислении номера биномиального числа при помощи числовой функции (1).

Рисунок 1 – Структурная схема системы сжатия

Система сжатия информации на основе биномиальных чисел представлено на рисунке 1. Данная система состоит из счетчиков единиц (Сч1) и нулей (Сч0), блока управления (БУ), блока вычисления биномиальных коэффициентов (БВБК) и блока вычисления номеров (БВН). Блок управления определяет начало и конец равновесной комбинации, а так же реализует преобразование двоичной равновесной комбинации в биномиальное число. Счетчики нулей и единиц определяют индексы для биномиальных коэффициентов в числовой функции (1). Помимо этого, счетчик единиц определяет вес равновесной комбинации, который необходим для однозначного ее восстановления. Блок вычисления биномиальных коэффициентов реализован на базе запоминающего устройства. Блок вычисления номеров, реализованный на сумматоре, складывает вычисленные биномиальные коэффициенты в соответствии с (1).

Разработанная система сжатия на основе биномиальных чисел обладает достаточно высоким быстродействием и имеет относительно низкие аппаратурные затраты для своей практической реализации.

УДК 004.896

ГЕНЕТИЧНИЙ ПІДХІД ДО ОПТИМІЗАЦІЇ ПРОЦЕСІВ ЗБАГАЧУВАЛЬНОЇ ТЕХНОЛОГІЇ

А.І. Купін, к.т.н., доцент, І.О. Музика, аспірант
Криворізький технічний університет
MusicVano@mail.ru

Сучасний стан економіки країни вимагає від залізорудних підприємств підвищення якості своєї продукції та зниження її собівартості. Так якість концентрату вітчизняних гірничо-збагачувальних комбінатів (ГЗК) не перевищує 64–66 % на відміну від закордонних 68–70 %.

Рис. 1. Технологічна схема 1-ї стадії збагачення.
1 – бункер з рудою; 2 – конвеєр; 3 – змішувач; 4 – вентилі подачі води; 5 – кульовий млин МШР-4×5; 6 – спіральний класифікатор типу 12КСН; 7 – пульповодій; 8 – магнітні сепаратори 4УПБМ.

Досить перспективним напрямом при побудові систем автоматизації секціями збагачення на сьогодні є застосування

нейрокерування. Авторами запропонований альтернативний підхід оптимального керування на базі генетичних алгоритмів.

На рис. 1 представлена технологічна схема мокрого подрібнення та першої стадії збагачення залізної руди Північного ГЗК. Критерій ефективності керування можна сформулювати наступним чином. Потрібно визначити оптимальні сигнали керування: B_M, B_K – витрати води в млин та класифікатор відповідно, *м*^{3}/*год*, які б забезпечили максимально можливий вміст заліза в концентраті β, % на виході групи магнітних сепараторів. При цьому показники ефективності збагачення мають бути не нижче планових, а втрати в хвостах v, % не вище допустимих.

Рис. 2. Діаграми роботи генетичного алгоритму.

На рис. 2 зображені графіки зміни технологічних параметрів у часі. Генетичний алгоритм здійснює пошук оптимального режиму керування, змінюючи B_M і B_K. При цьому одним із збурювальних впливів є випадковий характер вмісту заліза α у вхідній руді. Проте можна побачити, що залежність вмісту заліза в концентраті β від часу має чітко виражений тренд збільшення.

Таким чином за попередніми оцінками, впровадження у виробництво інтелектуальної системи керування на основі генетичних алгоритмів дасть можливість стабілізувати якість концентрату на виході першої стадії збагачення на рівні 45–50 % і зменшити втрати в хвостах до 13–17 %.

УДК 621.372

ШВИДКИЙ АЛГОРИТМ ВЕЙВЛЕТ ПЕРЕТВОРЕННЯ НА БАЗІ ВЕЙВЛЕТА ХААРА

Г.Г. Бортник, к.т.н., доцент,
О.С. Городецька, к.т.н., ст. викладач,
О.В. Стальченко
Вінницький національний технічний університет
stal1978@ukr.net

У сучасних комп'ютерних засобах знаходять широке використання вейвлет перетворення. Дискретний сигнал $\{f_k\}$ з використанням масштабувальної функції ϕ_H, яка відповідає вейвлету Хаара ψ_H, перетворюється в неперервний сигнал $f(t)$ згідно виразу

$$f(t) = \sum_{k=1}^{N} f_k \phi_H (t-k). \qquad (1)$$

Коефіцієнти апроксимації дискретної послідовності $\{f_k^1\}$ і детальні коефіцієнти $\{d_k^1\}$ можна знайти так:

$$f^1 = \{f_k^1\}_{k=0}^{\frac{N}{2}} = \left\{ \frac{f_0+f_1}{2}, \frac{f_2+f_3}{2}, ..., \frac{f_{N-1}+f_N}{2} \right\}; \qquad (2)$$

$$\{d_k^1\}_{k=0}^{\frac{N}{2}} = \left\{ \frac{f_0-f_1}{2}, \frac{f_2-f_3}{2}, ..., \frac{f_{N-1}-f_N}{2} \right\}. \qquad (3)$$

Тоді неперервне вейвлет перетворення функції $f(t)$ з використанням вейвлета Хаара для $a=2$ і $t=2k$ $(k=0,1,...)$ може бути розраховане за формулою

$$L_{\psi H} f(2,2k) = \sqrt{\frac{2}{c_{\psi H}}} d_k^1, \qquad (4)$$

де $c_{\psi H}$ – коефіцієнт вейвлета Хаара.

Для відновлення сигналу $f(t)$ визначається апроксимувальний сигнал $f^1(t)$ і детальний сигнал $d^1(t)$:

$$f^1(t) = \sum_{k=0}^{N} f_k^1 \phi_H \left(\frac{t}{2} - k \right), \tag{5}$$

$$d^1(t) = \sum_{k=0}^{N} d_k^1 \psi_H \left(\frac{t}{2} - k \right). \tag{6}$$

Тоді $f(t) = f^1(t) + d^1(t)$. Цей алгоритм є однокроковим варіантом дискретного вейвлет перетворення, виконаним з використанням вейвлета Хаара. Слід відзначити, що всі обчислення можна повторити з використаням сигналу $f^1(t)$ замість $f(t)$. Крім того, на основі формули (4) можна визначити значення неперервного вейвлет перетворення для вейвлету Хаара за допомогою (3).

Загалом процедура визначення f^1 може бути представлена наступним чином

$$f^1 = Hf. \tag{7}$$

Процедура позначена символом H у даному випадку вказує, що застосовується цифровий фільтр з коефіцієнтами $\{h_0 = 1/2,\ h_1 = 1/2\}$, а потім сигнал проріджується, тобто зберігається кожен другий елемент послідовності. Відповідно співвідношення для визначення d^1 можна представити як

$$d^1 = Gf. \tag{8}$$

Символ G означає фільтрацію, яка супроводжується проріджуванням – децимацією, але з коефіцієнтами $\{g_0 = 1/2,\ g_1 = -1/2\}$. Таким чином, дискретний сигнал може бути відновлений без проміжного визначення відповідного неперервного за часом сигналу $f(t)$.

УДК 681.301

ВИЗНАЧЕННЯ МІНІМАЛЬНОГО НАБОРУ СЕМАНТИЧНИХ КОНСТРУКЦІЙ ДЛЯ ПІДТРИМКИ ПЛАТФОРМИ ВИВЧЕННЯ ТЕХНОЛОГІЙ ПРОГРАМУВАННЯ

Д.С. Замятін[1], к.т.н., доцент
О.С. Дубровський[2], магістрант
Національний технічний університету України
«Київський політехнічний інститут»
[1]dsz@ukr.net, [2]zdubrovsky@gmail.com

Однією з причин неготовності професійних програмістів гнучко підійди до вибору засобів декомпозиції предметної області, враховуючи специфіку завдання, є відсутність мови програмування, що охоплює всі синтаксичні конструкції, що застосовуються при вивчені технологій програмування. Метою запропонованої роботи є виділення синтаксичних конструкцій, множину яких повинна містити в собі платформа вивчення технологій програмування.

Для визначення тих конструкції у мовах програмування, які на сьогоднішній день згадаються найчастіше в Інтернеті, використовуємо пошук по наукових джерелах та по цитуванню в Інтернеті (Табл.1). Далі проаналізуємо синтаксичні конструкції, що мають найпопулярніші мови програмування (Рис.1). Вибірка мов здійснювалася на основі пошуку по Google Code.

У результаті розгляду можливостей мов програмування для створення платформи вивчення технологій програмування пропонується використовувати

мову Python, яка підтримує програмування у функціональному та остилі.

Популярність синтаксичних конструкцій програмування Табл.1

Концепція програмування	Цитування в Google, тис.	Цитування в Google Scholar, тис.	Співвідношення цитувань
Каррінг (Currying)	1 520	22	69
Лямбда-функція (Lambda-function)	252	24,4	10,30
Анонімна функція (Anonymous function)	6 640	218	30,45
Замикання (Closures)	913	47,3	19,30
«Ліниві» обчислення (Lazy evaluation)	295	8,86	33,29
Зпівставлення зі зразком (Pattern matching)	3 870	412	9,39
Часткове використання (Partial function)	876	30	29,2
Узагальнення (Generics)	2 190	804	2,72
Домішки (Mixins)	408	20	20,4

Рис.1 Наявність синтаксичних конструкцій у мовах програмування

Також потрібно доповнити мову Python такими конструкціями, як перевантаження функцій, каррінг, шаблони, домішки.

УДК 519.6

НЕОБХІДНІ ТА ДОСТАТНІ УМОВИ НА БАЗИС ДИАДНОГО ВЕЙВЛЕТ-ПЕРЕТВОРЕННЯ

О.Р. Чертов[1], к.т.н., доцент,
М.В. Александрова[2], студент
Національний технічний університет України “КПІ”
[1]chertov@i.ua, [2]rita.alexandrova@gmail.com

За допомогою вейвлет-перетворень (ВП) здійснюється частотно-часовий аналіз, результати якого містять як загальну частотну характеристику сигналу (розподіл енергії сигналу за частотними складовими), властиву класичному розкладенню Фур’є, так й інформацію про певні локальні координати, на котрих відбувається швидка зміна відповідних частотних складових сигналу. Це досягається за рахунок того, що ВП в якості базисних використовує солітоноподібні функції, графік яких має вигляд невеликих хвиль (вейвлетів).

Шляхом масштабування (диадне вейвлет-перетворення використовує число 2 в якості коефіцієнту масштабування) та зсуву початкової функції (материнського вейвлету) можна отримати базис простору $L^2(\square)$, тобто простору дійсних функцій, квадрат котрих є інтегрованим, за яким і розкладається сигнал.

Очевидно, що в якості материнського вейвлету не може бути взята довільна функція, адже умова утворення базису простору $L^2(\square)$ операціями зсуву та масштабування є необхідною. Більш того, визначення конкретного вигляду функцій, що можуть використовуватись в якості материнських вейвлетів

біортогональних базисів диадного ВП, зводиться до розв'язання масштабуючих рівнянь $\varphi(x)=\sqrt{2}\sum_{n\in\mathbb{Z}} h_n\varphi(2x-n)$, $\tilde{\varphi}(x)=\sqrt{2}\sum_{n\in\mathbb{Z}} \tilde{h}_n\tilde{\varphi}(2x-n)$. Функції $\varphi(x)$ та $\tilde{\varphi}(x)$ називаються масштабуючими або скейлинг-функціями та визначають вейвлети $\psi(x)$, $\tilde{\psi}(x)$ за формулами $\psi(x)=\sqrt{2}\sum_{n\in\mathbb{Z}} g_n\tilde{\varphi}(2x-n)$ та $\tilde{\psi}(x)=\sqrt{2}\sum_{n\in\mathbb{Z}} \tilde{g}_n\varphi(2x-n)$, де відповідні коефіцієнти обчислюються через скалярний добуток: $g_n=\langle\psi(x),\tilde{\varphi}(2x-n)\rangle$, $\tilde{g}_n=\langle\tilde{\psi}(x),\varphi(2x-n)\rangle$.

Сучасна література з вейвлет-аналізу містить велику кількість теорем, що визначають умови на функції для утворення ними вейвлет-базису. В залежності від характеру доведення, способу реалізації чисельних алгоритмів, а також уподобань авторів, ці умови сформульовані в термінах функцій $\varphi(x)$, $\tilde{\varphi}(x)$, $\psi(x)$, $\tilde{\psi}(x)$, перетворення Фур'є відповідних фільтрів, матриць або операторів, елементами яких є коефіцієнти h_n, $\tilde{h}_n$, g_n, $\tilde{g}_n$ фільтрів.

Кожна з форм запису має як свої переваги, так і недоліки. Наприклад, матрична форма є найбільш вдалою для опису неоднорідних нестаціонарних перетворень, адже матричні рівняння не накладають умов на конкретний вигляд своїх елементів. Проте, запис в термінах коефіцієнтів фільтрів найкращим чином відображає характер реалізації деяких чисельних алгоритмів, зокрема алгоритму Малла.

УДК 004.9

АСОЦІАТИВНО-СТАТИСТИЧНИЙ МЕТОД МОРФОЛОГІЧНОГО АНАЛІЗУ СЛІВ

О.В. Бісікало[1], к.т.н., доцент, І.А. Кравчук[2], студент
Вінницький національний технічний університет
[1]obisikalo@gmail.com, [2]kravchuk-i@ukr.net

Створення автоматичного модуля синтаксичного аналізу є на сьогодні одним із найактуальніших завдань у комп'ютерній лінгвістиці, вирішення якого дозволило б досягти високого рівня формалізації мовних структур у різноманітних прикладних цілях.

Задачу отримання знань з природно-мовних (ПМ) текстів традиційно розв’язують за допомогою синтаксично-семантичного підходу, онтологій, а також моделей, побудованих на основі запитів до бази даних. Проте всі ці підходи вимагають значної попередньої роботи із залученням висококваліфікованих експертів.

Асоціативно-статистичний підхід до аналізу текстів призводить до побудови асоціативної семантичної мережі, яку складають пов’язані між собою слова тексту, що несуть основне семантичне навантаження. Для кожного поняття формується набір асоціативних зв'язків до/від інших понять, у сполученні з якими воно зустрічалося в тексті. Фізіологічна основа підходу полягає у природному накопиченні асоціацій між мовними образами та закріпленні рефлексів шляхом повторень.

В основу запропонованого методу морфологічного аналізу слів покладено ідеї Тьюринга та Хомського щодо формалізації природних шляхів опанування дитиною рідної мови. Розв’язок задачі побудови бази знань з

морфології будемо знаходити на основі виявлення в ПМ–конструкціях носіїв мови певних закономірностей. При цьому вхідну інформацію маємо у вигляді реляційної бази даних синтагматичних і парадигматичних зв'язків, що накопичуються в результаті аналізу текстів.

Результатом аналізу тексту є орієнтований граф, що узагальнює зв'язки між окремими словами речення. У кожній вершині графу міститься список спільнокореневих слів, для подальшого аналізу яких застосуємо граматику

$$G(T) = (V_T, V_N, S, P),$$

де V_T – алфавіт термінальних (основних) символів;

V_N – алфавіт не термінальних символів, $V_T \cap V_N = 0$;

S – стартовий символ;

P – кінцевий набір правил $\varphi \to \psi$.

Для поставленої задачі задамо:

V_N = *{СЛОВО; ПРЕФІКС; КОРІНЬ; СУФІКС};*

S = *СЛОВО.*

Необхідно статистично визначити V_T – набір морфем, або таких частин слова, що мають певні значення. Аналізуючи морфологічну структуру слова, визначимо базові правила з P: x є префіксом, якщо $y = xu$, z є суфіксом, якщо $y = uz$. В загальному випадку слово з префіксом та суфіксом має вигляд:

$$y = xuz.$$

Для можливості визначення окремих морфем з V_T задамо множини префіксів та суфіксів як:

$$Pref(L) = \{x \mid (\exists y \in L)\}, Pref \in V_T$$

$$Suf(L) = \{z \mid (\exists y \in L)\}, Suf \in V_T$$

Формальне визначення V_T і частини правил з P на основі статистичного аналізу множини текстів є перспективним компонентом лінгвістичного процесору.

УДК 681.324

ТЕХНОЛОГІЇ ІДЕНТИФІКАЦІЇ ЧАСОВИХ РЯДІВ НА ОСНОВІ ЙМОВІРНІСНОЇ НЕЙРОННОЇ МЕРЕЖІ ТА ЇЇ МОДИФІКОВАНИХ ВЕРСІЙ

В.В. Кабачій[1], к.т.н., доцент,
О.О. Чумаченко[2], магістрант
Вінницький національний технічний університет
[1]vkabachiy@svitonline.com, [2]olya.chumachenko@gmail.com

Мета дослідження полягає у підвищенні ефективності ідентифікації часових рядів на основі апарату модифікованих ймовірнісних нейронних мереж.

Ймовірнісні нейронні мережі – це інструмент, який дозволяє вирішувати задачі класифікації з високою точністю та швидкістю. Такі мережі можуть застосовуватись для опису і прогнозування поведінки об’єкта за набором ознак, які визначають поведінку цього об’єкта.

Ідентифікація часових рядів на основі класифікації зразків полягає в тому, що вибираються класи станів об’єктів, що досліджуються, які можуть бути задані як діапазонами зміни деяких параметрів, так і визначеними якісними характеристиками. По сукупності ознак, що визначають стан об’єктів знаходять відповідність належності кожного об’єкта в майбутньому понятті часу до визначеного класу. Це дозволяє дати прогноз стану об’єкту або вказати діапазон зміни параметрів, що характеризують його на період, що прогнозується.

В ймовірнісних нейронних мережах зразки класифікуються на основі оцінок їх близькості до сусідніх зразків. При цьому використовується ряд критеріїв

статистичних методів, на основі яких приймається рішення про те, до якого класу віднести ще не класифікований зразок. Формальним правилом при класифікації є те, що клас з найбільш щільним розподілом в області невідомого зразка, а також з найбільш високою апріорною ймовірністю, а також з більш високою ціною помилки класифікації буде мати перевагу у порівнянні з іншими класами.

Принцип навчання ймовірнісної нейронної мережі дещо відрізняється від принципів навчання інших типів мереж. Особливістю є те, що число нейронів в шарі зразків визначається числом самих зразків, а тому, параметрами мережі, що визначаються безпосередньо в ході навчання,є і кількість нейронів в шарі зразків, і значення їх ваг. Іншими словами, в ході навчання формується сама структура ймовірнісної нейронної мережі.

Модифікована ймовірнісна нейронна мережа враховує зміну керуючого параметру σ, який задає ширину ядерної функції Гауса, яка застосовується для оцінки щільності розподілу ймовірностей методом Парцена, тоді як в стандартній мережі, даний параметр завжди залишається сталим.

Врахування зміни параметру σ дозволяє контролювати форму класифікаційної поверхні, що відповідає навчальним зразкам. Це в результаті дозволяє досягти підвищення ефективності класифікації зразків даною мережею.

Перевагами використання даних мереж є висока швидкість навчання, що дає можливість адаптації навчання в режимі реального часу, додавання та видалення навчальних даних по мірі надходження нових. Крім того ймовірнісні нейронні мережі допускають наявність помилкових даних і корисні результати отримуються навіть на малих вибірках даних.

УДК 004.056

МЕТОД ІМОВІРНІСНОГО АНАЛІЗУ КОДУ НА ЦІЛОЧИСЕЛЬНІ ПЕРЕПОВНЕННЯ

О.І. Кобченко[1], студент,
Д.С. Замятін[1], к.т.н., доцент
Національний Технічний Університет України «КПІ»
[1]kob.mail@rambler.ru, [2]dsz@ukr.net

Методи статичного аналізу вихідного коду покликані вирішити проблему цілочисельних переповнень, що можуть викликати вразливості типу buffer overflow та спотворювати роботу програми. Факт переповнення теоретично можливий при використанні будь-яких арифметичних операцій, що вимагає від аналізатора перевірки програми при всіх можливих значеннях вхідного параметра(ів). В загальному випадку для перевірки можливості переповнення в програмі з одним параметром необхідно N ітерацій, де N – кількість значень в рамках типу змінної. В роботі запропоновано метод імовірнісного аналізу, що дозволяє зменшити кількість ітерацій до $2(\log_2 N+1)$ за рахунок побудови нерівності, вирішення якої дає інтервал значень, на яких виникає переповнення. Метод розрахований на аналіз ассемблерного коду, в який можуть бути сконвертовані програми, написані на більшості мов програмування високого рівня.

Сутність аналізу, покладеного в основу методу, полягає в побудові стеку станів для кожної інструкції програми, що дозволяє на кожному етапі перевірки відновити ланцюг арифметичних дій і побудувати на його основі лінійну нерівність. Вирішення останньої числовими методами (зокрема методом половинного ділення),

дозволяє отримати діапазон значень параметра, при яких виникає цілочисельне переповнення. Ефективність алгоритму очевидна для будь-якого розміру розрядної сітки:

Тип параметра	К-сть ітерацій (перебір)	К-сть ітерції (аналіз)
Short Int (8 біт)	256	16
Integer (16 біт)	65536	30
Long Int (32 біти)	4294967296	62

При аналізі на переповнення по кільком змінним ідея полягає в фіксації значеннь всіх змінних крім тієї, що буде перевірятись, з повторенням алгоритму для певного діапазону значень зафіксованих змінних. При цьому кількість ітерацій для двох параметрів буде $2M(\log_2 N+1)$, де M – кількість значень фіксованого параметра. Такий підхід дозволяє розробнику програми перевіряти параметри по черзі, зосереджуючись на більш небезпечних з точки зору можливого переповнення. Додатковою перевагою є можливість вирахування імовірності переповнення у вже задіяних програмах, що може бути визначена як $P=\prod_{i=1}^{k}(P(X_i))L/N$, де — імовірність появи значення зафіксованого параметра (при якому виникає переповнення), K – кількість зафіксованих параметрів, L— кількість значень параметра в інтервалі (отриманому в результаті аналізу).

Таким чином, запропонований в роботі метод імовірнісного аналізу дозволяє зменшити кількість ітерацій при перевірці коду на наявність цілочисельних переповнень, що дозволяє зекономити час та обчислювальні ресурси, дає можливість обчислити відносну імовірність переповнення та є універсальним для застосування за рахунок орієнтації на мову програмування ассемблер.

УДК 681.325.2

РОЗРЯДНО-ЗРІЗОВИЙ МЕТОД ПАРАЛЕЛЬНОГО ПОРІВНЯННЯ ЧИСЛОВИХ МАРТИЦЬ У ФОРМІ З ПЛАВАЮЧОЮ КОМОЮ

І.В. Мусійчук, аспірант
Вінницький національний технічний університет
irenkaua@o2.pl

Дуже часто в обчислювачах виникає необхідність порівняння даних, яке в свою чергу повинно задовільняти умовам оброблення інформації в реальному часі. Тому, була запропонована математична модель операції порівняння, подана в алгоритмічній формі, отримана на основі застосування принципів природного паралелізму оптичних обчислень до відомого класичного алгоритму додавання чисел в машинах з плаваючою комою.

Знакозмінні $N\times N$-вимірні матриці **A** і **B** подаються в формі з плаваючою комою в прямому коді у вигляді наборів із $S=(M+P+2)$ бінарних розрядних зрізів (РЗ), що мають розмірність відповідних матриць

$$\mathbf{A}=\left\{\mathbf{Sg}_{m_A=0},\mathbf{A}_{m_A=1},...,\mathbf{A}_{m_A=M},\mathbf{Sg}_{p_A=M+1},\mathbf{A}_{p_A=M+2},...,\mathbf{A}_{p_A=S}\right\};$$

$$\mathbf{B}=\left\{\mathbf{Sg}_{m_B=0},\mathbf{B}_{m_B=1},...,\mathbf{B}_{m_B=M},\mathbf{Sg}_{p_B=M+1},\mathbf{B}_{p_B=M+2},...,\mathbf{B}_{p_B=S}\right\}.$$

Припустимо, що тривимірні інформаційні масиви **Xm** і **Ym** зберігають РЗ мантис елементів відповідно матриць **A** і **B**, а **Xp** і **Yp** зберігають РЗ порядків елементів відповідно матриць **A** і **B**.

При порівнянні матриць за вищевказаним алгоритмом в нормалізованій формі можна виділити 3 етапи. На першому етапі на основі принципів позрізової паралельної обробки та цифрового часового інтегрування

виконується паралельне віднімання матриць порядків (**Xp**-**Yp**) як алгебраїчне паралельне додавання знакозмінних матриць (**Xp**+[-**Yp**]). Результат зберігається в тривимірному масиві проміжних сум матриць порядків **Sp** в вигляді просторового коду із (P+1) РЗ, поданих в доповняльному коді.

На другому етапі в залежності від матриць ознак **R** та **Sp(0)** організовано перетворення матриць мантис операндів, яке супроводжується відповідними змінами в матриці порядків **Sp(0:P)**. В разі необхідності збільшення матриці меншого порядку до більшого здійснюється як алгебраїчне додавання специфічної тривимірної матриці $\left\{\overline{\mathbf{Sp}_{(0)}}, 0, 0, \ldots, \overline{\mathbf{R}}\right\}$, поданої в прямому коді, до проміжної суми **Sp(0:P)**.За допомогою знакового РЗ цієї специфічної матриці враховано, що для елементів матриці **Sp(0:P)**, знак яких є додатнім, необхідно виконати віднімання одиниці, в іншому випадку – додавання одиниці. Дії по перетворенню матриці мантис та порядків операндів тривають до тих пір, поки порядки не стануть рівними **R**=**E**.

На третьому етапі отримані мантиси чисел, порядки яких на етапах 1 і 2 були вирівняні, тепер можна порівнювати. Суть процесу порівняння двох матриць **A** і **B** полягає у формуванні бінарної матриці **Vm** ознак, значення якої визначається в залежності від виконання такої умови:

$$\begin{cases} \mathbf{Vm}_{ij} = 1, \textit{якщо } \mathrm{a_{ij}} \le b_{ij}, i = \overline{1, N}, j = \overline{1, N} \\ \mathbf{Vm}_{ij} = 0, \textit{якщо } \mathrm{a_{ij}} > b_{ij}, i = \overline{1, N}, j = \overline{1, N}. \end{cases}$$

Матриця **Vm** формується з матриці **Rm**, якій відповідає поелементна рівність зрізів матриць, і матриці **Nm**, яка характеризує саме ознаку **A**<**B**, за тим самим принципом.

УДК 681

ПРИМЕНЕНИЕ МЕТОДА СЕЧЕНИЙ ДЛЯ КОНТРОЛЯ ФОРМЫ ПОВЕРХНОСТИ ПЯТНА ИЗЛУЧЕНИЯ В РЕАЛЬНОМ ВРЕМЕНИ

В.А. Губернаторов, аспирант
Государственный економико-технологический университет транспорта
pontiw@rambler.ru

В настоящее время в полиграфии, лазерной обработке материалов, локации, оптической связи и других областях техники ощущается необходимость более широкого внедрения оптико-электронных систем с автоматической корректировкой искажений формируемого светового излучения. Причинами этих искажений могут быть дестабилизирующее воздействие механических или климатических факторов, нестабильность характеристик источника излучения, возмущения в оптическом тракте, разъюстировка оптических элементов и т.п. Обеспечение приемлемого качества коррекции требует непрерывного динамического контроля характеристик светового излучения, например пространственного распределения его интенсивности, в том числе оценки отклонения указанного распределения от исходного или эталонного распределения.

Традиционный путь решения данной задачи включает формирование изображения пятна излучения $B(x, y)$ на светочувствительной поверхности фотоприемника с последующим преобразованием в сигнал $U(x, y)$, амплитуда которого в каждой точке разложения с координатами (x, y) соответствует интенсивности в $B(x, y)$,

т.е. $U(x, y) \leftrightarrow B(x, y)$ Далее сигнал $U(x, y)$ сравнивают с эталонным сигналом $W(x, y)$ для всех точек разложения сигналов. Сигналы $U(x, y)$ и $W(x, y)$ представляют собой некоторые поверхности, которые могут отличаться типом, коэффициентом относительного масштаба, вектором относительной координатной привязки и углами относительных поворотов в трехмерном пространстве. Поэтому сравнение этих поверхностей должно производиться с учетом всех возможных ситуаций, что требует огромного объема вычислений и затруднительно для осуществления в реальном времени. В практически важных случаях требуемое сравнение поверхностей $U(x, y)$ и $W(x, y)$ может быть реализовано с помощью излагаемого ниже нового метода сечений.

Эксперименты показывают, что для изображений пятен лазерных пучков в результате действия разнообразных дестабилизирующих факторов невозможно точно измерять координаты их энергетических центров, однако точность можно существенно повысить, используя вычисление коэффициента формы изображений с последующей их классификацией на “хорошие” и “плохие”. Сравнительный анализ показывает, что предложенные методы позволяют измерять координаты центра лазерных изображений с точностью определения точки привязки не менее чем 1-2 элемента разложения, что по точности превышают известные, например, на основе определения центра масс с помощью моментных признаков, в среднем в 1,5 раза.

В соответствии с изложенным методом сечений сравнение поверхностей сводится к сравнению их коэффициентов формы и не требует поэлементного сравнения с учетом всех случаев отличия их типов, коэффициента масштаба, относительного сдвига и поворота в пространстве.

УДК 004.8

ВИКОРИСТАННЯ ГЕНЕТИЧНОГО АЛГОРИТМУ В ЗАДАЧІ КЛАСТЕРИЗАЦІЇ АБОНЕНТІВ ІНТЕРНЕТ-ПРОВАЙДЕРА

С.М. Захарченко, к.т.н., доцент,
Н.Р. Кондратенко, к.т.н., професор,
О.О. Манаєва, студент
Вінницький національний технічний університет
sleeepy@meta.ua

Перед будь-яким Інтернет-провайдером постає задача тарифікації власних послуг відповідно до деяких критеріїв. Розв'язання цієї та інших задач покладається, як правило, на білінгову систему. Однією з важливих її складових є розробка тарифних планів, яка вимагає формування компактних груп абонентів із подібними потребами.

Виділенням серед множини $I=\{I_1, I_2, \ldots, I_n\}$ деяких об'єктів m однорідних підмножин, таких, щоб об'єкти всередині підмножин були в певному сенсі подібними, а об'єкти з різних підмножин – відмінними, займається задача кластеризації. Найбільш прямий спосіб її розв'язання полягає в повному переборі всіх можливих розбиттів на кластери та знаходженні такого розбиття, яке веде до оптимального (мінімального) значення цільової функції.

Методи повного перебору – єдина група методів, які дають змогу завжди відшукати оптимальний розв'язок, але є залежними від розмірності задачі. Роботу класичного алгоритму повного перебору можливо оптимізувати, застосовуючи прийом динамічного програмування. При

цьому значно скорочується обсяг обчислень, і в той же час така процедура завжди збігається до оптимального розв'язку. Проте проблема часу отримання розв'язку не зникає повністю. Тому для розв'язання цієї задачі доцільно використати наближені методи, зокрема генетичні алгоритми.

Запропонуємо генетичний алгоритм розв'язання задачі в даній постановці. Для формалізованого опису особини (одного з множини можливих розв'язків) будемо застосовувати неоднорідну хромосому (рис. 1), тобто таку, що містить дві складові. Перша складова являє собою лінійний масив розмірності n, що містить гени - номери об'єктів:

Рис. 1 – Неоднорідна хромосома

Для виділення в межах хромосоми окремих кластерів введено другу складову – набір маркерів розбиття M_1, …, M_m. Окрім того, кожній хромосомі з простору можливих розв'язків ставиться у відповідність значення цільової функції.

Над початковою популяцією будемо послідовно проводити операції схрещування, мутації та відбору кращих за критерієм цільової функції особин. Багатократним повторенням описаної процедури досягається мінімізація цільової функції та прийнятна точність отриманого розв'язку.

УДК 519.1

АЛГОРИТМ ВІДШУКАННЯ МІНІМАЛЬНОЇ ВІДСТАНІ МІЖ ВЕРШИНАМИ У ЧИСЛОВОМУ ГРАФІ МЕТОДОМ ПОШУКУ В ГЛИБИНУ

Т.О. Гришанович
Київський національний університет ім. Т.Шевченка
grtanja@rambler.ru

Поняття числового графа отримало значне застосування і оскільки подання графів у вигляді числових значно відрізняється від відомих представлень, виникає необхідність побудувати для них найбільш вживані алгоритми.

Робота присвячена реалізації алгоритму відшукання мінімальної відстані між вершинами числового (натурального арифметичного) графа за допомогою методу пошуку в ширину.

На вході алгоритм отримує кількість вершин графа (Count) та множину твірних (IntegerSet) та номери вершин, відстань між якими шукається (p1 та p2).

```
//Функція перевірки на суміжність вершин
    function Connected(p1, p2: integer): boolean;
      if (p1<>p2) then
      for k:=0 to Length(IntegerSet)-1 do
        if p1+p2=IntegerSet[k] then
          Result:=true;
            end;
//Функція обчислення мінімального шляху між вершинами
    function BuildWay(p1, p2: integer): boolean;
      Distance: integer;  //Відстань між вершинам
```

```
Q, Levels: array of integer;  Used: array of boolean;
Position, Length, Point, i: integer: integer; // допоміжні змінні
        for i:=1 to Count do //Масив "використаних" точок
          Used[i]:=false;
          Used[p1]:=true;
          Levels[p1]:=0; // Встановлення "глибини" дерева
          //Формування черги
          Q[1]:=p1; Position:=1; Length:=1;
          //Пошук в ширину
  while (Position<=Length) and not(Q[Position]=p2) do
   for i:=1 to Count do
       if not Used[i] and Connected(Q[Position], i) then
         Inc(Length);
         Q[Length]:=i;
         Levels[i]:=Levels[Q[Position]]+1;
         Used[i]:=true;
   Inc(Position);
          Distance := 0;
          if (Q[Position]=p2) then
            ShortestWay:=(p2);
            Result := true;
        while not(p2=p1) do
              Point:=p2;
                for i:=1 to Count do
      if      Used[i]      and      Connected(p2,      i)      and
(Levels[i]<Levels[Point]) then
                  Point:=i; ShortestWay:=ShortestWay+(Point);
                  Inc(Distance);
              p2:=Point;
         else   Result := false.
```

На виході алгоритму отримуємо мінімальну відстань між двома заданими вершинами (Distance) та список вершин, що входять до даного маршруту (ShortestWay).

УДК 681.324

АНАЛІЗ СЕМАНТИЧНОЇ ІНФОРМАЦІЇ ГІПЕРТЕКСТУ

В.М. Дубовой[1], д.т.н., професор
О.М. Москвін[2], аспірант
Вінницький національний технічний університет
[1]sveta.vova.dub@gmail.com, [2]moskvin.aleksey@gmail.com

Підтримка семантичної інформації набуває широкого застосування як у пошукових системах, так і у звичайному програмному забезпеченні, де має місце інтелектуальний аналіз великих обсягів даних, їх систематизація та синтез рішень на їх основі. Проблемою що постає у таких системах є визначення важливості зв'язків між інформаційними одиницями. На даний момент найбільш вживаним і розробленим є структурний аналіз, який не враховує предметну належність матеріалу. До таких реалізацій можна віднести загальновідомий Google Page Rank.

Ідеї застосування та впровадження засобів машинного аналізу даних були запропоновані консорціумом W3 у 1999 році і активно впроваджуються на практиці. Основною метою використання семантичної інформації є перехід від аналізу гіпертексту, його інформаційних та структурних характеристик, призначеного, фактично, для користувача, до формалізованих даних, призначених для машин та інтелектуальних агентів.

Семантична інформація, формалізована за допомогою семантичної мережі, основу якої складають онтології, є інформаційною моделлю преметної області, що має вигляд орієнтованого графа, вершини якого відповідають об'єктам

предметної області, а дуги задають відношення між ними. Об'єктами можуть бути поняття, події, властивості, процеси.

Онтології в системах штучного інтелекту є новим кроком у поданні й інтеграції знань та даних, вони надають одночасно високі рівні виразності та формалізації опису предметної галузі.

В роботі розв'язується задача аналізу гіпертекстової структури на основі семантичної інформації. Пропонується проводити аналіз важливості гіпертекстових зв'язків між суміжними ресурсами. В основі ідеї оцінки лежить пошук перетинів онтологій, представлених множиною предикативних виразів формалізованих за допомогою мови RDF/OWL, і розрахунок потужності перетинів в частково невизначеному вигляді. Базовою апріорною інформацією для здійснення аналізу є наявні гіпертекстові зв'язки. Результатом пошуку перетинів онтологій є розподіл, що характеризує вірогідність перетину, необхідний для оцінки ваги зв'язків між інформаційними одиницями.

Система оцінки, що пропонується, повинна працювати в умовах неповної інформації про загальну семантичну структуру гіпертексту. Наявними є лише дані для суміжних інформаційних одиниць, що пов'язано з розмірністю мереж, їх постійним збільшенням і модифікацією.

Метою наведенного аналізу є подальше створення методу оптимізаці ієрархічної гіпертекстової структури і оптимізації досяжності інформаційних одиниць у їх підмережі на основі семантичних даних.

Запропонований підхід до оцінки зв'язків підмережі інформаційних ресурсів для її подальшої оптимізації, дозволить зберегти оптимальну досяжність фрагментів гіпертексту в умовах неповної інформації про структуру мережі, що сприятиме підвищенню ефективності використання гіпертекстових ресурсів.

УДК 681.39

МОДЕЛЮВАННЯ ДАНИХ ДЛЯ ЗДІЙСНЕННЯ УЩІЛЬНЕННЯ ЧИСЛОВИХ ПОСЛІДОВНОСТЕЙ

В.А. Каплун, старший викладач
Вінницький національний технічний університет
valuka58@gmail.com

У доповіді розглядаються результати проведених досліджень, що стосуються здійснення ущільнення вхідних повідомлень, представлених у вигляді послідовності додатних чисел певної розрядності. Аналіз ущільнення методами, які базуються на обчисленні відхилень, показав, що обсяг ущільненої послідовності значною мірою залежить і від формату файлів вхідних повідомлень, і від розрядності чисел вхідної послідовності, і від методу ущільнення згідно запропонованої класифікації, і від параметрів цих методів (кількості констант, груп або піддіапазонів, які приймали участь в обчисленні). Крім того, результати комп'ютерних досліджень показали, що кожен із запропонованих методів ущільнення дозволяє здійснити ефективне ущільнення лише у разі певних властивостей вхідної послідовності цілих чисел. Степінь ущільнення інформації залежить від закону розподілу, якому відповідає вхідний потік початкової інформації. Для запропонованих методів найбільший коефіцієнт ущільнення досягається, коли значення чисел вхідної послідовності розподілені за нормальним законом. Але реальні послідовності можуть відповідати і іншим законам розподілу. Тому для досягнення найбільшого коефіцієнта ущільнення потрібно відповідним чином здійснювати перетворення вхідної послідовності чисел, тобто, здійснити моделювання чисел вхідної послідовності.

Для підвищення ефективності ущільнення пропонується перед виконанням ущільнення здійснювати додаткову процедуру перетворення первинної послідовності до послідовності, яка матиме властивості, що задовольнять кожному конкретному методу ущільнення. Запропоновано декілька підходів до моделювання вхідного потоку даних.

Одним з таких підходів може бути введення ваг розрядів чисел вхідної послідовності (наприклад, степені основи деякої системи числення). Це може забезпечити значне зменшення обсягу ущільнених даних.

Може бути застосований і такий підхід, при якому вхідна послідовність заміняється на певним чином відфільтровану. Наприклад, ущільненню пропонується піддавати послідовність середніх значень за модулем чисел вхідної послідовності. Для деяких запропонованих методів ущільнення такий підхід може значно зменшити обсяг результуючого повідомлення.

Ще один з підходів до моделювання вхідної послідовності базується на властивостях деяких законів розподілу. Доведено, що послідовність сум чисел, згрупованих певним чином, розподілена за законом, наближеним до нормального. Отже, можна ущільнювати не безпосередньо послідовність чисел вхідного повідомлення, а послідовність значень, які є результатами відповідних перетворень над числами цих груп. У цьому випадку деякі з запропонованих методів ущільнення також можуть показати себе досить ефективними, оскільки розмір вхідної послідовності може виявитись набагато меншим, так само, як і значення відхилень.

Звичайно, ущільнена інформація бути представлена значеннями самих відхилень, додатковою інформацією, необхідною для здійснення зворотного перетворення. Але це компенсуватиметься тим, що значення відхилень, отриманих шляхом застосування запропонованих методів ущільнення, стануть досить малими, а степінь ущільнення при цьому може значно зрости.

УДК 519.711

СИНТЕЗ ИНДИКАТОРНЫХ МАТРИЦ СИСТЕМ ВИЛЕНКИНА-КРЕСТЕНСОНА ФУНКЦИЙ

Д.С. Демьяник, аспирант
Национальный авиационный университет, Киев
Deniska-85@inbox.ru

Базис Виленкина-Крестенсона представляет собой набор ортонормированных функций. Матрица функций Виленкина-Крестенсона (ВКФ) может быть получена кронекеровским возведением в степень матрицы дискретно-экспоненциальных функций (ДЭФ), поэтому системы ДЭФ можно считать частным случаем систем ВКФ. Для реализации быстрых преобразований Фурье (БПФ) в базисе ВКФ требуется меньший объём вычислений, чем для БПФ в базисе ДЭФ аналогичного порядка. Это одно из свойств данного семейства функций, позволяющих говорить о перспективе их практического применения. Другим их полезным свойством является возможность синтеза на порядки большего количества симметричных систем преобразования, чем для систем ДЭФ. Симметричные матрицы преобразования интересны тем, что графы прямого и обратного БПФ, использующих эти матрицы, выглядят одинаково.

Факт наличия огромного количества таких матриц позволяет применять их в криптографических целях, поскольку спектральное отображение дискретной последовательности представляет собой криптограмму, правильная расшифровка которой возможна только при наличии «правильной» матрицы преобразования.

Семейство ВКФ характеризуется двумя параметрами: m - порядок системы ДЭФ (или основание системы счисления) на основе, которой строится система ВКФ, и n - кронекеровская

степень (разрядность кодовых комбинаций), в которую возводится матрица ДЭФ. Дочерние (в том числе и симметричные) матрицы ВКФ могут быть получены путём соответствующей перестановки строк исходной матрицы. Однако такой способ поиска симметрических матриц является весьма неэффективным. На практике для поиска и хранения симметричных систем ВКФ удобно пользоваться индикаторными матрицами. Индикаторными матрицами систем ВКФ являются такие невырожденные в кольце вычетов по модулю m квадратные n-го порядка матрицы M с элементами, принадлежащими множеству вычетов $Z_m \in \{0,\ 1,\ldots,\ m\text{-}1\}$, с помощью которых устанавливается однозначное соответствие

$$y = (xM)_m$$

между номером $x \in \overline{0, N-1}$ строки исходной матрицы ВКФ, записанном в m - ичной системе счисления и поданном в виде вектора, и номером строки y новой системы ВКФ, поданным таким же образом. Такие матрицы обладают симметрией относительно побочной диагонали.

В докладе обсуждается программа, производящая синтез индикаторных матриц систем ВКФ. Программа осуществляет последовательный перебор всех возможных матриц с определенными пользователем параметрами m и n, являющихся симметричными относительно вспомогательной диагонали матрицами. После генерации очередной матрицы программа находит её определитель по модулю m и, если он не имеет общих делителей с m, записывает эту матрицу в сокращённом виде в файл. После окончания поиска всех индикаторных матриц имеется возможность вывода на экран любой из них. Впоследствии найденные при помощи данного алгоритма матрицы могут быть использованы как в приложениях в криптографии, так и для БПФ в различных базисах ВКФ.

УДК 004.925.4

НОВИЙ МЕТОД КУСКОВО-НЕПЕРЕРВНОЇ КВАДРАТИЧНОЇ АРОКСИМАЦІЇ ПЕРСПЕКТИВНОГО ТЕКСТУРУВАННЯ

О.В. Романюк, аспірант
Вінницький національний технічний університет
oksana_gelika@mail.ru

Основною задачею комп'ютерної графіки є синтез високореалістичних графічних зображень, які відтворюють найменші деталі поверхні об'єктів зображення. Досягти рельєфності можна за рахунок зміни геометричної моделі об'єкта шляхом її розбиття на велику кількість полігонів та зміни їх орієнтації. Такий підхід дає реалістичний результат, але вимагає потужних обчислювальних засобів. Крім того, набором полігонів дуже складно відобразити мілкі деталі на поверхні об'єктів, такі як пори, тріщини, щілини тощо.

Альтернативою зміні геометричної моделі об'єкта є використання текстур, які накладаються на об'єкт. Більш реалістичний результат отримують при перспективно-коректному текстуруванні, але його реалізація вимагає виконання трудомісткої операції ділення для кожного пікселя зображення. Тому задача спрощення процедури перспективно-коректного текстурування є актуальною.

Серед відомих методів апроксимації перспективно-коректного текстурування виділяють лінійну, квадратичну, кубічну, бі-квадратичну та бі-кубічну апроксимації, які передбачають розрахунок коефіцієнтів апроксимації, складність розрахунку яких зростає з підвищенням порядку апроксимувальних кривих. Інший підхід до апроксимації полягає у розбитті рядка растеризації на декілька рівних

відрізків та використання лінійної, квадратичної чи кубічної інтерполяції для розрахунку текстурних координат у межах отриманих відрізків. Чим більша кількість відрізків, тим точніший розрахунок. Але у цьому випадку потрібно розраховувати точні значення текстурних координат у точках, між якими проводиться інтерполяція.

При квадратичній апроксимації рядок растеризації ділиться на два рівних відрізка. На тому відрізку, де текстурні координати приймають значення [0,5;1], квадратична апроксимація дає гарний результат. Другий відрізок рядка растеризації потребує більш точної апроксимації.

Нехай значення текстурної координати уздовж рядка растеризації змінюється від менших значень до більших. Оберемо чотири опорні точки так, щоб перша і четверта опорні точки були відповідно початковою і кінцевою точками рядка растеризації, третя опорна точка розбивала рядок растеризації навпіл, друга опорна точка розбивала ліву половину рядка растеризації навпіл. Оскільки квадратична апроксимація потребує точних значень текстурних координат у опорних точках, то для апроксимації першої половини рядка растеризації використовуються точні значення текстурних координат у першій, другій та третій опорних точках, а для апроксимації другої половини – у першій, третій та четвертій опорних точках.

Квадратичну апроксимацію пропонується виконувати квадратичною кривою Безьє, оскільки вона передбачає розрахунок лише одного коефіцієнта апроксимації.

Таким чином, запропонований метод дозволяє підвищити точність квадратичної апроксимації малих значень текстурних координат з використанням лише однієї додаткової опорної точки.

УДК 681.3.01

ПІДСИСТЕМА АВТОМАТИЧНОЇ КЛАСИФІКАЦІЇ ТЕКСТОВИХ ДОКУМЕНТІВ НА ОСНОВІ ЧАСТОТНОГО АНАЛІЗУ КЛЮЧОВИХ СЛІВ

М.П. Грищенко, магістрант
Національний технічний університет України
“Київський політехнічний інститут”

При значному зростанні електронного документообігу постає завдання автоматичної класифікації великого потоку документів за обмеженої участі користувача та з прийнятною якістю і швидкодією. В основному використовуються наступні методи класифікації: асоціативно-статистичний аналіз, синтаксично-семантичний та наочно-геометричні методи з використанням нейромережевих класифікаторів (класифікатор Гросберга – ART, сітка Кохонена – SOM).

Одним з найшвидших способів сортування вхідного потоку документів по категоріям є задання для кожної рубрики набору ключових слів, які дозволяють віднести документ до даної тематики. Список ключових слів в даному випадку є простим семантичним образом рубрики.

Недолік методу в тому, що в описаному вигляді він застосовується лише за умов створення бази ключових слів вручну.

Розроблена програма-класифікатор позбавляє користувача рутинної та складної роботи і створення семантичних рубрик бере на себе. Виконується це наступним чином: адміністратор системи документообігу вказує програмі рубрики та віднесені до них «навчальні» множини документів. Програма виділяє в текстах значимі

слова, за допомогою підключеного морфологічного модулю, яким є словник Ханспела (Hunspell), приводить їх до лексем (перших словоформ). Після приведення слів до нормалізованої форми отримані результати мають велику розмірність, яку можна значно зменшити без погіршення якості класифікації, якщо видалити інформаційні шуми - слова, що не впливають на результати класифікації. Це так звані «стоп-слова» (прийменники, сполучники, займенники і т.п.) – видаляються за допомогою складеного вручну невеликого списку, а також слова, які зустрічаються рідко – тут важливо правильно обрати діапазон значущих слів (якщо встановити його дуже широким, до ключових потраплять допоміжні слова, вузьким – можна втратити змістові значення, терміни). Далі визначається критерій інформаційної ваги кожного слова (mutual information ain), обчислюється за формулою:

$$MI(x_j, C_i) = \sum_{x_j \in \{0,1\}} \sum_{C \in \{0,1\}} P(x_j, C_i) \log \frac{P(x_j, C_i)}{P(x_j) P(C_i)},$$

де: x_j - признак наявності слова в документі,

C_i - тематичний розділ,

$$P(x_j = 1) = 1 - P(x_j = 0) = \frac{\textit{кільк. документів, в яких зустріч. } x_j}{\textit{загальна кількість документів}}$$

$$P(C_i = 1) = 1 - P(C_i = 0) = \frac{\textit{кільк. документів класу } C_i}{\textit{загальна кількість документів}}$$

Зі списку ключових слів для кожної рубрики формується пошуковий запит, що застосовується для множини нових документів. Таким чином отримуємо список документів, віднесених до конкретних тематичних рубрик.

Класифікація за описаними семантичними правилами значно ефективніша, ніж по складеним вручну спискам ключових слів.

3. МЕТОДИ ТА ЗАСОБИ ОБРОБКИ СИГНАЛІВ

УДК 621.391

СИНТЕЗ ДИСКРЕТНЫХ СИГНАЛОВ НА ОСНОВЕ СЕЧЕНИЯ ЦИКЛИЧЕСКИХ ОРБИТ ГРУППОВОГО КОДА И ИССЛЕДОВАНИЕ ИХ СВОЙСТВ

Ю.В.Стасев, д.т.н., профессор,
А.А. Кузнецов, д.т.н, профессор, В.Н. Сай, с.н.с.
Харьковский университет Воздушных Сил
kuznetsov_alex@rambler.ru

Построение современных радиосистем управления и связи с многостанционным доступом сопряжено с разработкой больших ансамблей дискретных сигналов с улучшенными ансамблевыми и корреляционными свойствами. Их практическое использование позволяет реализовать многостанционный доступ с кодовым разделением каналов и обеспечить высокие показатели помехозащищенности и имитостойкости радиоканалов управления.

Проведенные исследования показали, что развитый математический аппарат алгебраической теории блоковых кодов позволяет синтезировать большие ансамбли дискретных сигналов с особыми корреляционными свойствами. В основе синтеза больших ансамблей дискретных сигналов лежит формирование кодовых слов группового кода с требуемыми дистанционными и структурными свойствами, теоретически обоснованные правила сечения циклических орбит синтезированного кода, формирование множества лидеров орбит группового кода (посредством сечения его циклических орбит) и оценка ансамблевых и корреляционных свойств синтезированных дискретных последовательностей. Дистанционные свойства формируемых дискретных

последовательностей непосредственно связаны с кодовыми характеристиками и весовым спектром алгебраических кодов. Мощность формируемых ансамблей дискретных сигналов определяется числом циклических орбит группового кода.

В данной работе проводятся исследования корреляционных и ансамблевых свойств дискретных сигналов, построенных на основе сечения циклических орбит группового кода. Выводятся аналитические выражения для оценки ненулевых компонентов весового спектра групповых кодов и соответствующих уровней блоковых выбросов функции корреляции, оцениваются мощности формируемых ансамблей дискретных сигналов.

Проведенные исследования показали, что применяя методы алгебраических блоковых кодов известные классы двоичных дискретных сигналов с одно и двух уровневой функцией корреляции (m-последовательности и сигналы Голда) представляются в виде множества лидеров (выбранных представителей) циклических орбит соответствующего двоичного группового кода. Кроме того, предлагаемый подход позволяет получить новые классы сигналов с n-уровневой функцией корреляции. Значения боковых выбросов функции корреляции определяются весовым спектром использованного кода.

Наиболее перспективным направлением дальнейших исследований является синтез недвоичных дискретных сигналов с особыми свойствами. Следуя предлагаемому подходу в этом случае для синтеза дискретных сигналов необходимо использовать недвоичные групповые коды, а функцию корреляции рассчитывать с учетом взаимной коррелированности элементов дискретных сигналов. Данное направление позволит существенно повысить абонентскую емкость сетей радиосвязи с кодовым разделением каналов.

УДК 621.391

О ПОТЕНЦИАЛЬНЫХ ВОЗМОЖНОСТЯХ СЕЛЕКЦИИ ИНФОРМАЦИОННЫХ И НЕИНФОРМАЦИОННЫХ КОМПОНЕНТ РЕЧЕВЫХ СИГНАЛОВ[1]

С.П. Белов[1], к.т.н., профессор
А.С. Белов[2], к.т.н., старший преподаватель
Белгородского государственного университета
[1]belov@bsu.edu.ru, [2]belov_as@bsu.edu.ru

Достаточно часто в различных задачах, связанных с обработкой звуковых сигналов речевого диапазона, возникает необходимость различения их на информационные и неинформационные компоненты.

В докладе предлагается осуществлять реализацию указанной процедуры, используя знания об особенностях распределения энергии информационных и неинформационных компонент анализируемых сигналов в частотной области.

При этом на основе анализа существующих в настоящее время методов частотного представления сигналов, делается вывод о необходимости применения для вычисления долей их энергий в выбранных частотных интервалах речевого диапазона нового метода, основанного на использовании субполосных матриц.

Применение этого математического аппарата дает возможность адекватно учесть свойство сосредоточенности энергии звуков речи

[1] Исследования выполнены при поддержке гранта РФФИ № 10-07-00326-а

(информационных компонент) в малом количестве достаточно узких частотных интервалов, что позволяет достичь максимального энергетического выигрыша, а, следовательно, минимизировать вероятность принятия отрезков информационных компонент звуковых сигналов речевого диапазона за неинформационные (шумовые), которые распределены довольно равномерно по всей оси частот.

Результаты вычислительных экспериментов, полученные при использовании алгоритмов, созданных на основе данного метода, позволяют говорить о высокой точности определения долей энергии анализируемых сигналов в частотной области.

Таким образом, применение алгоритмов, разработанных на базе нового метода вычисления точных значений долей энергии обеспечивает потенциально возможную селекцию информационных и неинформационных компонент речевых сигналов.

УДК 681.32

СЖАТОЕ ПРЕДСТАВЛЕНИЕ ДИФФЕРЕНЦИРОВАННЫХ ИЗОБРАЖЕНИЙ В СИСТЕМАХ АЄРОКОСМИЧЕСКОГО МОНИТОРИНГА

В.В. Баранник, д.т.н., с.н.с, В.В. Шинкарев
Харьковский университет Воздушных Сил
Barannik_V_V@mail.ru

Процессы доставки видеоданных в системах аэрокосмического мониторинга связаны с решением противоречия между своевременностью доставки информации и ее достоверностью. Данное противоречие обусловлено постоянным ростом объемов видеоданных и повышенными требованиями относительно полноты и достоверности получаемой информации. Направление решения выявленного противоречия состоит в сокращении объемов передаваемых видеоданных за счет их компрессии с заданной степенью достоверности. Большинство методов сжатия данного класса базируются на получении дифференцированного представления (ДП) изображений. В результате чего достигается декорреляция видеоданных и формирование комбинаторных объектов. Организация комплексного сокращения избыточности основывается на неравновесном позиционном кодировании. Однако в случае обработки насыщенных изображений будут образовываться массивы ДП, содержащие одновременно как фрагменты с большим динамическим диапазоном, так и с ограниченным динамическим диапазоном. Поэтому для выхода из такой ситуации и дополнительного повышения степени сжатия предлагается учитывать двухградационность динамических диапазонов массивов дифференциального представления реалистических изображений. Значит цель исследований заключается в развитии неравновесного представления дифференцированных изображений с учетом их

двухградационности. Необходимо учитывать следующие требования: величина классифицирующего порога должна вычисляться при наименьшем количестве дополнительной служебной информации; обеспечивались бы условия для быстрого и наиболее точного построения перфорированных чисел. В зависимости от степени детализации при оценке динамического диапазона возможны следующие варианты построения перфоратора.

1. Формировать классификатор на основе значений элементов массива дифференциального представления. В этом случае построенный динамический диапазон наиболее точно отражает структурные особенности дифференциального представления. Соответственно обеспечивается наилучшее разделение массива ДП на перфорирующие уровни.

2. Формировать классификатор на базе усреднения динамического диапазона всего массива ДП.

3. Формировать перфорирующий порог на основе взвешенного усреднения динамических диапазонов элементов МДП.

Это обосновывает необходимость формирования перфорирвоанных неравновесных позиционных чисел для дифференциального представления изображений, что позволит: выявить закономерности перфорированности динамических диапазонов дифференциального представления насыщенных мелкими деталями изображения; обеспечить потенциальные возможности для дополнительного сокращения избыточности дифференциально-представленных изображений в случаях нестационарности структурных свойств изображений. Разрабатывается подход относительно формирования перфорирующего порога (классификатора, перфоратора), позволяющего построить перфорирующие числа на базе неравновесных позиционных чисел. Построение перфоратора проводится с учетом структурных особенностей динамических диапазонов элементов массива дифференциального представления в условиях отсутствия дополнительного использования служебной информации.

УДК 621.37:621.391

ПОЛІНОМІАЛЬНИЙ ПІДХІД ДО ПОБУДОВИ МЕТОДІВ ТА СТРУКТУР СУМІСНИХ АЛГОРИТМІВ РОЗРІЗНЕННЯ СИГНАЛІВ ТА ОЦІНЮВАННЯ ЇХ ПАРАМЕТРІВ

В.В. Палагін, к.т.н., доцент,
О.А. Палагіна, к.т.н., доцент
Черкаський державний технологічний університет
palahin@yahoo.com

При розгляді загальної теорії статистичної обробки сигналів виділяється два самостійні напрями, які добре вивчені і знайшли широке своє застосування для рішенні багатьох практичних задач. Перший напрям стосується питань перевірки статистичних гіпотез і використовується для вирішення таких прикладних завдань, як виявлення сигналів, розрізнення і розпізнавання на тлі завад, де рішення вноситься з певної дискретної множини. Другий напрям стосується оцінювання параметрів сигналів на тлі завад, які, як правило, є безперервними величинами. З іншого боку існує велика кількість задач, де необхідно сумістити ці два напрями теорії статистичної обробки сигналів, що призводить до побудови двофункціональних правил вибору рішень при сумісному розрізненні сигналів та оцінки їх параметрів.

Показано, що узагальнені методи, які застосовуються для побудови таких двофункціональних правил (Байесівський метод, метод максимальної правдіподібності та інш), не обмежують клас випадкових величин, але на практиці широке застосування знайшли в основному гауссівські моделі випадкових сигналів, що в

більшості пояснюється зручністю використання математичного апарату.

З іншого боку інтерес до негауссівських моделей сигналів та завад, як найбільш узагальнених, постійно зростає і використання «класичних» підходів викликає певні труднощі, пов'язані як з отриманням таких рішень, так і їх реалізацією.

В роботі пропонується використання двофункціонального правила обробки вхідних вибіркових значень $\mathbf{X}$

$$\Delta[\mathbf{X}] = \mathrm{F}\{\Delta_{\mathrm{p}}[\mathbf{X}], \Delta_{\mathrm{o}}[\mathbf{X}]\},$$

де $\Delta_{\mathrm{p}}[\mathbf{X}]$ - функція розрізнення гіпотез, в основу якої покладено застосування поліноміальних вирішальних правил (ВП), оптимальні коефіцієнти якого знаходяться згідно моментного асимптотично нормального критерію якості, $\Delta_{\mathrm{o}}[\mathbf{X}]$ - функція оцінювання параметрів сигналів, в основу якої лежить метод максимізації полінома.

Особливістю запропонованого підходу є те, що він дозволяє будувати поліноміальні ВП на основі моментно-кумулянтного опису випадкових величин. Показано, що при лінійній обробці вибіркових (при степені поліномів $s = 1$) значень отримуються рішення, які повністю співпадають з відомими підходами при врахуванні гауссівських моделей випадкових величин. При нелінійній обробці ($s \geq 2$) враховується статистика третього і вище порядків у вигляді коефіцієнтів асиметрії, ексцесу і т.д., що характеризує негауссівські моделі випадкових величин.

Показано, що врахування таких параметрів дозволяє суттєво покращити результати оцінки параметрів у вигляді зменшення дисперсії оціночних значень та зменшити ймовірності помилок поліноміальних ВП в порівнянні з відомими результатами.

УДК 621.391

КОНТРОЛЬ И АНАЛИЗ ВИБРАЦИОННЫХ СИГНАЛОВ ПО РЕКУРРЕНТНЫМ ДИАГРАММАМ

Б.И. Исмайлов, н.с.
Азербайджанская государственная нефтяная академия

Эксплуатационный контроль технического состояния силового энергетического оборудования сопровождается сбором, обработкой, анализом и интерпретацией большого объёма экспериментальной вибрационной измерительной информации.

Оценке технического состояния контролируемого устройства и принятию решения по корректировке его режима работы предшествует осмысление совокупности собранной, технологической и статистической информации, а также формализованных знаний экспертов в данной предметной области.

Для обеспечения эффективного анализа и визуализации обобщённой информации, расшифровки и прогнозирования состояния контролируемого оборудования, предлагается проведение рекуррентного анализа с построением рекуррентных диаграмм. Применение рекуррентных диаграмм с их выразительным представлением протекающих вибрационных процессов и их сложных взаимосвязей в виде 2-х и 3-х мерных графических образов, обеспечит более доходчивое их, процессов, восприятие с подключением эмоциональной сферы.

УДК 621.391

АЛГОРИТМИ ВИМІРЮВАННЯ РАДІАЛЬНОЇ ШВИДКОСТІ ДЖЕРЕЛА ГАРМОНІЧНОГО СИГНАЛУ В РАДІОТЕХНІЧНИХ СИСТЕМАХ ПРИ НЕГАУССІВСЬКИХ ЗАВАДАХ

Т.В. Воробкало[1], к.т.н., доцент
О.С. Гавриш[2], к.ф.-м.н., доцент
Черкаський державний технологічний університет
[1]ptv@ukr.net, [2]hackee74@yahoo.com

Радіолокаційні системи вимірюють не тільки різні геометричні величини, які характеризують розташування об’єкту (відстань до об’єкту, напрям на об’єкт), але і параметри руху об’єкту. Одним з важливих параметрів руху, що підлягає визначенню в радіосистемах є швидкість: радіальна та кутова.

В даній роботі ставиться задача визначення радіальної швидкості руху джерела випромінювання гармонічного сигналу. Радіальна швидкість є проекція вектора швидкості руху джерела на напрям “приймач-випромінювач”. В РЛС для визначення радіальної швидкості використовується ефект Допплера – зміна частоти електромагнітних коливань, що приймаються, при зміні відстані між приймачем і випромінювачем радіохвиль.

Так як корисний сигнал завжди приймається в присутності завад, то поставлена в роботі задача має статистичний характер і зводиться до оцінювання частоти допплерівського зсуву сигналу.

Зазвичай для оцінювання параметрів сигналів, що приймаються на фоні завад використовуються класичні

методи. Відомо, що класичні методи оцінювання параметрів є оптимальними при знаходженні оцінок параметрів сигналів, що приймаються в умовах впливу гауссівських завад. Але на практиці, часто характер розподілу завад відрізняється від гауссівського, тобто завади є негауссівськими і необхідно використовувати інші методи. Одним з таких методів є метод максимізації поліному, який базується на використанні степеневих стохастичних поліномів та моментно-кумулянтному описі випадкової величини.

Тому в роботі, відповідно до метода максимізації полінома, побудовані алгоритми оцінювання допплерівського зсуву частоти до третього степеня стохастичного поліному включно і відповідно до них побудовані блок-схеми вимірювання радіальної швидкості руху джерела випромінювання гармонічного сигналу.

Проведено аналіз асимптотичних властивостей кожного степеневого алгоритму, для чого було знайдено і проаналізовано аналітичні вирази дисперсій оцінок, які описують їх точністні характеристики. В результаті аналізу алгоритмів встановлено, що з ростом степеня поліному точність оцінювання підвищуються. Ефективність опрацювання параметрів сигналу залежить від того, наскільки статистичний характер завади відрізняється від гауссівської моделі. А саме, чим більше кумулянтні коефіцієнти вищих порядків відрізняються від нуля, тим точніші алгоритми.

Отримані результати можуть бути використані для вдосконалення існуючих доплерівських радіолокаційних систем, що працюють в умовах впливу на корисний сигнал негауссівських завад.

УДК 681.3:591.3

ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ РАСПОЗНАВАНИЯ МНОГОМЕРНЫХ СИГНАЛОВ С ИСПОЛЬЗОВАНИЕМ ИМПУЛЬСНЫХ НЕЙРОННЫХ СЕТЕЙ

О.К. Колесницкий, к.т.н., доцент
Винницкий национальный технический университет
okk_vin@mail.ru

Главная цель функционирования интеллектуальных систем – решать когнитивные задачи не хуже человека.

Человек воспринимает образы с помощью органов чувств (глаза, уши, нос і т.д.), которые являются многокомпонентными рецепторами. Эти многокомпонентные рецепторы выдают многоканальную информацию в виде совокупности сигналов (импульсных). Центральная нервная система (ЦНС) человека имеет дело не с самим образом, а с результатом воздействия этого образа на рецепторы. Для ЦНС образом является совокупность импульсных сигналов, которые генерируются рецепторами, а затем проходят сложную обработку. Поэтому при построении нейроморфных интеллектуальных систем новых поколений большое значение имеет решение проблемы распознавания многомерных сигналов.

Постановка задачи:

- Необходимо распознать n динамических сигналов (сигналы мультисенсоров газов, сигналы антенных решеток, параметры сложных динамических объектов и т.п.)

- Все n сигналов поступают одновременно (параллельно) и ограничены на временном отрезке
- Результат распознавания необходимо получать в реальном времени – сразу по окончании сигналов.

Варианты решения:

- Корреляционные методы – не подходят, т.к. необходимо много параллельно работающих корреляторов
- Традиционные нейронные сети – не подходят, т.к. зачастую для получения решения необходимо несколько итераций и работают с отсчетами входных сигналов или их признаками
- Импульсные нейронные сети – подходят, т.к. 1) приспособлены к распознаванию динамических образов без их предварительного преобразования в вектор признаков; 2) многозадачны (информация о входных потоках циркулирует в рекуррентной нейронной сети и на выход одновременно могут быть поданы результаты разных задач при помощи разных групп считывающих нейронов); 3) распознают с предвидением (любой динамический процесс может быть распознан даже по неполной информации о нем, т.е. даже раньше, чем он завершится). 4) имеют простую процедуру обучения (обучаются не все нейроны сети, а только выходные считывающие нейроны).

В докладе рассматривается информационная технология распознавания многомерных сигналов с помощью импульсных нейронных сетей, структуры и модели нейронных елементов и сети в целом, а также результаты компьютерного моделирования.

УДК 681.325

ПАРАЛЕЛЬНА ОБРОБКА БІНАРНИХ ЗОБРАЖЕНЬ В БІОМЕТРИЧНИХ СИСТЕМАХ ЗАХИСТУ

В.П. Семеренко, к.т.н., доцент,
Н.С. Ткаченко, студентка
Вінницький національний технічний університет
VPSemerenko@mail.ru

В останні роки велика увага приділяється проблемі розробки обчислювальних алгоритмів, які можуть бути ефективно відображені на архітектуру комп'ютерних систем з паралельною обробкою даних.

Будемо розглядати дві задачі обробки бінарних зображень в біометричних системах захисту: кодування бінарних зображень та їх розпізнавання.

Зручним математичним апаратом для кодування бінарних зображень є булева алгебра кубічних функцій. Ця алгебра є ізоморфною традиційній булевій алгебрі логічних функцій. Операціям кон'юнкції, диз'юнкції та заперечення в булевій алгебрі логічних функцій відповідають операції перетину, об'єднання та доповнення кубів в булевій алгебрі кубічних функцій, а нормальним формам відповідають кубічні покриття.

Пропонується кожний прямокутний фрагмент початкового зображення розміром $n \times n$ пікселей представляти як поле узагальненої карти Карно і далі проводити його мінімізацію за методом Рота. В результаті буде отримано кубічне покриття, тобто матриця, розміром $m \times k$, де $m = 2\log_2 n$, а значення k залежить від характеру зображення, в середньому, $k \approx m$. Окрім ущільнення початкових даних, перевагами логічних

методів представлення зображень є їх точність, можливість виконання різних перетворень (фільтрація, переміщення) і, найголовніше, можливість використання сучасних методів розпаралелювання обчислень. Мінімізація функцій за методом Рота передбачає виконання великої кількості однотипних елементарних операцій над операндами кубічних функцій, які легко реалізуються як на матрично-конвеєрних (систолічних) обчислювачах в мікроелектронному виконанні, так і при використанні багатопотокового програмування.

В біометричних системах захисту задача аналізу зображень полягає в порівнянні заданого зразка зображення з еталонними зображеннями, які в ущільненому вигляді зберігаються в базі даних. Зображення, яке надходить з відеокамер спостереження і повинно бути розпізнане, також може бути представлено в логічній формі. Оскільки аналіз зображень відбувається в режимі реального часу, тому мінімізація зображення від відеокамер не проводиться, а відразу починається процес порівняння із ущільненими еталонами зображень із бази даних. В булевій алгебрі кубічних функцій процедура порівняння реалізується за допомогою операції перетину кубів, що дозволяє працювати з операндами різного ступеню мінімізації.

Для підвищення швидкості роботи системи на етапі аналізу зображень також може бути використана матрично-конвеєрна архітектура, яка дозволяє проводити одночасне порівняння з групою еталонних зображень. Може бути поставлена або задача точного збігу двох зображень, або збігу із заданою похибкою.

УДК 004.032 26

ВОССТАНОВЛЕНИЕ ИЗОБРАЖЕНИЙ С ИСПОЛЬЗОВАНИЕМ АНАЛИЗА ГЛАВНЫХ И НЕЗАВИСИМЫХ КОМПОНЕНТ

А.Г. Ведмедь, аспирант, Е.С. Сакало, аспирант
Харьковский национальный университет радиоэлектроники
medwed1986@gmail.com

Существует целый ряд практических задач, когда наряду со сжатием изображения с помощью анализа главных компонент необходимо производить их «очистку» от различного рода возмущений, помех, аномальных выбросов, пятен, теней и т.п., что может быть реализовано на основе анализа независимых компонент.Анализ независимых компонент рассматривается как расширение анализа главных компонент на задачу слепой сепарации независимых источников из их линейных смесей. При этом с анализом главных компонент тесно связаны такие понятия как некоррелированность и гауссовский характер распределения данных, в то время как анализ независимых компонент связан со статистической независимостью и негауссовскими распределениями. В задачах обработки изображений на первый план выходит проблема восстановления исходного векторного сигнала по искаженным наблюдениям. При этом особый интерес представляет синтез рекуррентных адаптивных процедур, позволяющих проводить обработку информации в реальном времени по мере поступления новых данных. Наша цель – обсуждение унифицированных процедур обучения нейросетей в рамках единой архитектуры типа «bottle-neck», которые обеспечивают решение как задач анализа главных компонент (компрессии изображений), так и

анализа независимых компонент (слепой идентификации и сепарации сигналов).

Предлагаются алгоритмы обучения трехслойной нейронной сети для слепой сепарации сигналов с предварительным их отбеливанием. Каждый из трех слоев сети, имея одинаковую структуру, решает разные задачи. Так, в первом слое производится отбеливание, во втором – сепарация, а в третьем – оценивание базисных векторов. Поскольку в задачах обработки изображений главной задачей является сепарация источников, выходной слой часто может и не потребоваться. Немаловажно также и то, что подобные нейронные сети являются автоассоциативными, т.е. их входной сигнал одновременно является и обучающим.

Для обработки изображений на основе слепой сепарации и анализа независимых компонент на основе нейросетевого подхода среди возможных архитектур наиболее предпочтительными являются сети с прямым распространением информации, допускающие использование рекуррентных алгоритмов обучения, что, в свою очередь, позволяет обрабатывать данные в последовательном режиме по мере их поступления. В этом плане определенную перспективу имеет нейросетевой метод обработки многомерных смесей сигналов на основе совместного использования анализа независимых и главных компонент, и он может быть реализован как в рамках элементарной однослойной архитектуры путем поочередного использования различных алгоритмов обучения, и в рамках архитектур типа «бутылочное горлышко». Модифицированные рекуррентные процедуры «отбеливания», сепарации и оценивания базисных векторов независимых компонент, обеспечивают высокую скорость сходимости и характеризуются простотой вычислительных моделей.

УДК 681.32

АВТОМАТИЧЕСКОЕ РАСПОЗНАВАНИЕ РЕЧЕВОЙ ИНФОРМАЦИИ

С.В. Омельченко, к.т.н., доцент
А.Ю. Трубчанинов, магистр
Харьковский национальный университет радиоэлектроники

Актуальными являются прикладные задачи ориентированные на создание современных технических систем с возможностью управлением голосом на основе современных теоретических и технических достижений. При этом на практике для разработки конкретных автоматических систем распознавания техничской информации достаточен существенно ограниченным объем словаря.

Целью статьи является построение алгоритмов распознавания речи в условиях действия помех.

Поставленная задача распознавания решается с использованием модели линейного предсказания.

Для решения задач производится предварительная сегментация произносимых диктором слов. Для этого находят временные границы начала и конца слова. С целью получения динамических признаков распознаваемого цифрового сигнала производится разбиение слов на блоки равной длины.

Для построения алгоритмов распознавания речи в качестве признаков использованы результаты выбеливания решетчатых фильтров, коэффициенты отражения и логарифмы отношения площадей сечений голосового тракта.

Для вычисления оценок коэффициентов авторегрессии использован метод максимальной энтропии Бурга.

Рассмотрено решение задачи распознавания речи с использование процедур динамического программирования, необходимой для нелинейной временной нормализации.

Для проверки предложенных алгоритмов распознавания речи были проведены экспериментальные исследования. Качество распознавания сигналов оценивалось средней вероятностью правильного распознавания, которая получалась на контрольных выборках реализаций методом статистических испытаний.

Показана возможность повышения качества адаптивного распознавания речи с учетом помеховой обстановки. Экспериментально получено, что при принятии решения с одновременным использованием спектрально-полосных признаков, признаков вокализованности и дисперсии результатов выбеливания средняя вероятность правильного распознавания слов P=0,96.

Для алгоритмов распознавания слов речи по оценкам коэффициентов отражения и использовании одного эталона на каждое из слов получена средняя вероятность правильного распознавания 0,91, а шести эталонах на каждое слово - средняя вероятность правильного распознавания 0,975.

Проведенные исследования алгоритмов распознавания, подтверждают возможность получения приемлемого качества распознавания речевых сигналов в условиях действия коррелированных помех.

УДК 621.391.19

ОСОБЛИВОСТІ КЛАСИФІКАЦІЇ СИГНАЛІВ ЗА ДИСКРИМІНАНТНИМИ ФУНКЦІЯМИ

А.Г. Буда, к.т.н., доцент,
Л.М. Куперштейн, к.т.н., доцент,
О.М. Гуцол, аспірант
Вінницький національний технічний університет
up.your.irons@gmail.com

Серед розповсюджених методів контрольованої класифікації образів, наприклад, у медичній діагностиці, які використовують функції відстані, правило найближчого сусіда, а також дискримінантні функції, саме останній підхід використано для апаратної класифікації сигналів. Цей метод модифіковано таким чином, що зникає необхідність у формуванні дискримінантних функцій (ДФ) вигляду

$$g_i(Z) = w_{i1} \cdot z_1 + \ldots + w_{in} \cdot z_n, \qquad (1)$$

де w_{ij} - ваги, z_j - j-й елемент вхідного вектора, $j = \overline{1,n}$.

Для класифікації пропонується застосувати спосіб оброблення матриці даних $\boldsymbol{A^t}$ за різницевими зрізами, елементи якого вигляду $a_{ij} = w_{ij} \cdot z_j$ є доданками відповідних ДФ $g_i(Z)$ (1). Суть цього підходу полягає в тому, що послідовно у кожному циклі оброблення всі елементи матричного масиву зменшуються на загальну компоненту (загальний складник серед всіх елементів, що додатні і не дорівнюють нулю) у кожному стовпці, тобто у кожному циклі формується різницевий зріз елементів у всіх стовпцях масиву.

В процесі оброблення елементів матриці $\boldsymbol{A}^t$ ($t = \overline{1, N}$, де N – кількість циклів оброблення) послідовно виконуються такі операції:

1) визначення мінелемента в кожному стовпці матриці $\boldsymbol{A}^t$;

2) формування невпорядкованої матриці $\overline{\boldsymbol{A}}^t$ як двовимірного різницевого зрізу;

3) впорядкування матриці $\overline{\boldsymbol{A}}^t$ в процесі транспозиції (просування) праворуч до краю всіх нульових елементів у кожному рядку.

Кожний отриманий нульовий рядок матриці $\overline{\boldsymbol{A}}^t$ свідчить про те, що відповідна ДФ не є максимальною, тому елементи цього рядка з подальшого оброблення вилучаються. При цьому формується нульове значення відповідного елемента у вихідному векторі $\boldsymbol{Y}$ класифікації. Процес оброблення завершується з обнулінням останнього рядка матриці $\boldsymbol{A}^N$, при цьому формується одиничне значення відповідного елемента вектора $\boldsymbol{Y}$, яке вказує на належність вхідного образу до певного класу.

Застосування способу оброблення за різницевими зрізами дозволяє розширити функціональні можливості за рахунок того, що можна ввести зовнішній поріг класифікації, а також виконувати підсумовування мінелементів, що в подальшому використовується для визначення ваг.

УДК 681.34

МОДЕЛЮВАННЯ ПРОЦЕСІВ ОБРОБЛЕННЯ ТА КЛАСИФІКАЦІЇ СИГНАЛІВ ЗА РІЗНИЦЕВИМИ ЗРІЗАМИ

В.В. Хом'юк, к.т.н., доцент,
О.В. Дюдюн, студент,
М.В. Дзісь, студент
Вінницький національний технічний університет
NickD047@Gmail.com

При дослідженні процесів оброблення та класифікації сигналів за методом різницевих зрізів труднощі викликає задача з визначення часових характеристик цих процесів. Це пов'язано з тим, що застосування методу різницевих зрізів надає адаптивного характеру будь-якому процесу, оскільки на величину часових характеристик в цьому випадку впливає не тільки розмірність масиву, який обробляється, але й розподіл елементів у масиві. Тому в даній роботі було досліджено два види розподілу чисел в одновимірному масиві для оброблення і у двовимірному масиві для класифікації чисел, а саме нормальне і рівномірне розподілення.

Головною задачею досліджень було визначення кількості циклів оброблення для загального випадку (випадкового набору вхідних даних), а для процесу класифікації визначалось також мінімальне, максимальне і середнє значення кількості циклів.

Для оцінювання ефективності процесу порогового оброблення було побудовано та реалізовано в середовищі Mathcad імітаційну модель процесу, що дозволяє дослідити залежність кількості циклів від значення порогу, кількості

елементів вхідного масиву та параметрів закону розподілу значень його елементів для нормального та рівномірного законів розподілу.

В результаті проведення імітаційних експериментів виявлено, що кількість циклів обробки вхідного масиву залежить, в основному, від співвідношенння між значенням порогу та значеннями елементів, кількості повторюваних елементів та різницею між сусідніми за значенням елементами. Тривалість процесу практично не залежить від закону розподілу вхідних даних при великих діапазонах змін значень елементів. Крайніми є два випадки оброблення масивів. У першому з них сума мінімальних елементів перевищує значення порогу або кількість елементів масиву співрозмірна із значенням порогу. При цьому процес завершиться на першій ітерації. В другому випадку кожен з елементів масиву відрізняється на одиницю від сусіднього за значенням елемента, тоді кількість ітерацій процесу буде максимальною і рівною розмірності масиву, якщо їх сума не перевищує поріг.

Результати моделювання представлено у вигляді тривимірних графіків часових залежностей, по двох вісях яких відкладено розмірність вхідного масиву чисел та середньоквадратичне відхилення σ відповідно. Для моделювання порогового оброблення по двох вісях відкладено розмірність вхідного масиву чисел і величина зовнішнього порогу оброблення відповідно.

Отримані результати моделювання дозволяють не тільки підтвердити теоретичні припущення, а й за наявністю часових характеристик відповідної елементної бази розрахувати часові витрати для конкретного обчислювального засобу.

УДК 621.39

РОЗПІЗНАВАННЯ ПЕРВИННИХ ОЗНАК ПРИ ПОБУДОВІ ФОНЕМНИХ ВОКОДЕРІВ

О.М. Ткаченко[1], к.т.н., доцент,
О.В. Дзісь[2], студент
Вінницький національний технічний університет
[1]ant@vstu.vinnica.ua, [2]AlexDz47@Gmail.com

Ущільнення мовленнєвих сигналів під час їх передавання дозволяє підвищити ефективність використання частотної смуги каналів зв'язку. Відомо, що застосування фонемних вокодерів дозволяє досягти найвищий ступінь ущільнення. При цьому можна забезпечити передавання мовленнєвого потоку зі швидкістю 300 біт/с. Проте для реалізації фонемного вокодера необхідно розв'язати дві достатньо складні наукові задачі:

– розпізнати у мовленнєвому потоці деякі акустичні одиниці (фонеми);
– синтезувати на їх основі якісний мовленнєвий сигнал.

У роботі розглянуто шляхи підвищення фонетичної коректності (ФК) розпізнавання. Для дослідження було обрано три найбільш поширені параметричні моделі представлення мовленнєвих даних:

– коефіцієнти лінійного прогнозування (LPC);
– лінійні спектральні частоти (LSF);
– кепстральні коефіцієнти (CC) .

Для аналізу методів обчислення відстаней було обрано такі метрики:

– евклідова метрика (EM);

– зважена евклідова метрика (ЗЕМ);

– дві спеціальні метрики для LPC (CM1 та CM2 відповідно);

При проведенні дослідження було використано матеріал англомовної бази даних TIMIT, яка включає достатньо великий набір дикторів та фраз, розмічених на фонеми.

Дослідження параметричних моделей показало, що використання кепстральних коефіцієнтів дає кращі результати, ніж LPC та LSF за однакових умов. При аналізі метрик найвищий показник (58%) було досягнуто при використанні ЗЕМ для кепстральних коефіцієнтів.

Для підвищення показника ФК запропоновано використовувати методи кластеризації. Це дозволило підвищити ФК на 11-27% для різних метрик та параметричних моделей, при цьому найвище значення - 78% досягнуто при використанні ЗЕМ для кепстральних коефіцієнтів.

Важливою передумовою побудови україномовного фонемного вокодера, є створення бази даних первинних ознак для українського усного мовлення. Однією із основних проблем при створенні такої бази даних є сегментація мовлення. Для її вирішення запропоновано використовувати методи розпізнавання. Оскільки під час сегментації немає необхідності виконувати обчислення у реальному масштабі часу, то є можливість застосування більш складних алгоритмів обробки.

Отримані результати дослідження було застосовано для розробки програми автоматизованої сегментації акустичних мовленнєвих баз даних.

УДК 621.39

ПОШУК НАЙБЛИЖЧОГО ВЕКТОРА У КОДОВИХ КНИГАХ НА ОСНОВІ БІНАРНОГО ДЕРЕВА

О.М. Ткаченко[1], к.т.н., доцент,
О.Ф. Грійо Тукало[2], студент
Вінницький національний технічний університет
[1]alextk1960@gmail.com
[2]xxmargoxx@gmail.com

Передача мовленнєвих сигналів у неущільненому вигляді потребує швидкісних каналів зв'язку через великі обсяги даних. Саме тому в сучасних системах цифрового зв'язку застосовується ущільнення мовлення, зокрема з використанням кодових книг (КК).

Об'єктом квантування в КК є лінійні спектральні частоти (LSF). Проте у реальному масштабі часу практичне застосування методів квантування обмежено через різке зростання витрат пам'яті та часу на пошук кодованого вектора у КК. Тому підвищення ефективності пошуку найближчого вектора у КК є актуальною науковою задачею.

Для скорочення часу пошуку найближчого вектора у КК запропоновано метод пошуку по бінарному дереву, вперше введений при кодуванні зображень. Пошук по дереву значно ефективніший пошуку по лінійних структурах, оскільки час пошуку визначається висотою дерева, яка в середньому є пропорційною двійковому логарифму кількості вузлів.

Пошук здійснюється за таким рекурсивним алгоритмом: спочатку здійснюється перехід до вузла-нащадка, ближчого до вхідного вектора, ніж поточний

(ліве піддерево); при досягненні листового вузла відбувається обчислення відстані до вектора КК, який належить листу; при зворотньому русі по дереву перехід до іншого нащадка (правого) здійснюється у разі, якщо він знаходиться на відстані, не більшій мінімальної, знайденої до цього моменту.

З метою прискорення процесу обчислення, алгоритм пошуку використовує інкрементальне обчислення відстаней між вхідним вектором і вузлами дерева.

У роботі розглядалося кілька способів розбиття області параметрів при створенні дерева: вздовж середньої точки, вздовж ковзаючої середньої точки, модифікація останнього, коли додатково враховувалося співвідношення сторін прямокутних регіонів. В ході досліджень найкращі результати були отримані при пошуку по дереву, отриманому для розбиття вздовж ковзаючої середньої точки.

Оскільки для будь-якого вектора LSF параметрів виконується

$$\forall f, \quad f_i < f_{i+1}, \quad i = 1..5,$$

LSF займають лише верхню частину прямокутної області (над побічною діагоналлю – в двомірному просторі). З урахуванням цієї специфіки було запропоновано повернути осі координат на 45 градусів проти годинникової стрілки, перерахувавщи відповідні параметри в КК. Це дало можливість скоротити час пошуку за рахунок штучного досягнення більшої симетричності розбиття дерева.

Таким чином, складність обчислень при пошуку з застосуванням бінарного дерева для впорядкування векторів КК склала 4 – 5% від складності обчислень при повному пошуку, витрати пам’яті при цьому в середньому збільшилися в 3 рази.

УДК 004.93’14

ТРИСТУПЕНЕВИЙ МЕТОД ІЄРАРХІЧНОЇ ДЕКОМПОЗИЦІЇ ДЛЯ ПОБУДОВИ СКЕЛЕТОНІВ СКЛАДНОСТРУКТУРНИХ ЗОБРАЖЕНЬ

Р.Б. Тушницький, І.В. Перевалова
Національний університет «Львівська політехніка»
ruslan4yk@lp.edu.ua, bilo4k@inbox.ru

Скелетони зображень широко використовують для розпізнавання символів, визначення хромосом, представлення топології, під час пошуку та порівняння 3D об’єктів. Зіставлення за скелетонами може містити часткове зіставлення, тобто об’єкт може бути знайдений як частина більшого об’єкту, або навпаки. Прикладами застосувань, які використовують скелетони є: віртуальна навігація, реєстрація, анімація, науковий аналіз, визначення форми, пошук за формою. Крім цього, скелетони використовують коли є потреба у відносній позиції штрихів у зображенні.

Під час побудови скелетону складноструктурного зображення виникає задача його декомпозиції на сегменти, до яких застосовують процедуру скелетонізації. Для вирішення поставленої мети розроблено триступеневий метод ієрархічної декомпозиції, який дає змогу покрити зображення кластерами трьох видів – кластерами-прямокутниками, замкнутими регіонами та зв’язними областями. Розроблений метод дає змогу адаптуватись до характерних особливостей зображень при їх опрацюванні.

На попередньому кроці скануванням зображення з пікселів-мікрооб’єктів формуємо мікрокластери. Для формування кластерів вищих рівнів застосовуємо

процедуру згортання. На рис. 1 наведено фрагмент 3-ступеневого ієрархічного дерева.

Рис. 1. Фрагмент 3-ступеневого ієрархічного дерева

Для побудови скелетону складноструктурного зображення до кожної зв'язної області застосовуємо алгоритм Hilditch із скануючим вікном розміром 4×4. На рис. 2 наведено етапи побудови скелетону для зображення медичного образу. Внаслідок його декомпозиції отримано 9 зв'язних областей (рис. 2, *б*). Побудований скелетон наведено на рис. 2, *в*.

а *б* *в*

Рис. 2. Формування скелетону: *а* – вхідне зображення, *б* – декомпозоване зображення, *в* – побудований скелетон

Властивості скелетонів рекомендуються для застосування в автоматизованих системах зберігання і пошуку даних різної фізичної природи, для аналізу форми та структурного аналізу.

УДК 621.3

МЕТОД ВИЯВЛЕННЯ ОБЛИЧ НА ЗОБРАЖЕННІ З ВИКОРИСТАННЯМ МОДИФІКОВАНИХ ХААР-ПОДІБНИХ ОЗНАК

Р.В. Маслій, асистент
Вінницький національний технічний університет
romas@ukr.net

Останнім часом значно зріс інтерес до дослідження задачі виявлення облич (ВО) на зображенні, це пояснюється виникненням багатьох застосувань в яких ВО є першим кроком для подальшої обробки зображення обличчя: розпізнавання облич, розпізнавання емоцій, гендерна класифікація, інтерфейс «людина-комп'ютер», відеоспостереження, відеоконференції, контроль доступу, пошук зображень за контекстом, підрахунок відвідувачів тощо. І якщо для людини задача ВО є досить простою, при створенні автоматичної системи ВО потрібно враховувати ряд факторів, які впливають на достовірність виявлення, а саме: зміни освітлення, ракурс голови, нахил голови, вираз обличчя, зміни зовнішності, неоднорідність фону, зміни масштабу обличчя, зміни пози, перекриття обличчя іншими об'єктами, умови спостереження тощо.

Найкращі результати на сьогоднішній день демонструють методи ВО, які базуються на зовнішньому вигляді. Ці методи розглядають ВО як задачу класифікації з двома класами (обличчя/не обличчя). Найбільш ефективними для рішення цієї задачі класифікації є нейромережеві методи та boosting-методи.

Для ВО у фронтальному ракурсі на напівтонових зображеннях нейромережеві методи демонструють хороші

результати щодо достовірності виявлення (низьким рівнем помилок першого та другого роду) але швидкість роботи цих методів не дозволяє їм оброблювати зображення у режимі реального часу. Boosting-методи навпаки, дозволяють здійснювати ВО на зображеннях в режимі реального часу, але з вищими рівнями помилок першого та другого роду, що пов'язано з пропуском частково закритих або затінених облич.

Метою роботи є створення boosting-методу ВО, в якому для збільшення достовірності ВО пропонується використати для побудови слабких класифікаторів у каскаді сильних класифікаторів модифіковані Хаар-подібні ознаки (ХПО). Модифікація ХПО полягає у використанні замість обчислення суми значень пікселів у темних та світлих прямокутних областях ХПО кількості локальних бінарних шаблонів (ЛБШ), які приєднанні до певної ХПО. Як відомо ЛБШ ознаки робастні щодо змін освітлення та часткового закриття облич, тому їх використання у поєднанні з ХПО дозволить зменшити помилки першого та другого роду при використанні boosting-методів у випадку виявлення частково закритих або затінених облич та при цьому несуттєво знизити швидкість ВО.

Тренувальний та верифікаційний набори позитивних прикладів для розробленого методу складаються з зображень облич зібраних у базах ORL, Yale, FERET. Тренувальний та верифікаційний набори негативних прикладів складаються з областей зображень, зібраних у Internet, на яких відсутні обличчя.

Для тестування розробленого методу ВО застосовується база облич BioID, яка містить зображення облич з різними варіаціями освітлення, фону, розмірами обличчя, невеликими відхиленнями у позі.

УДК 519.652:519.254

ЗАСТОСУВАННЯ ФІЛЬТРІВ, ЗВОРОТНИХ ДО НИЗЬКОЧАСТОТНИХ ПРИ ОБРОБЦІ ЗОБРАЖЕНЬ

М.О. Рябий, аспірант
Національний авіаційний університет
smayluk@ukr.net

В роботах [1; 2] запропоновані двовимірні низькочастотні та зворотні до них контрастні фільтри, що можуть мати використання при обробці цифрованих зображень. Нижче подано результати практичної апробації використання зазначених фільтрів на різних типах цифрованих реалістичних зображень.

Суть експерименту полягала в наступному: попередньо було відібрано 60 зображень без спотворень та артефактів різного розміру та деталізації; кожне зображення підлягало обробці низькочастотним фільтром різної потужності (умовно позначимо Н2.0, Н3.0, Н4.0) за ступенем їх згладжування; з подальшим застосуванням контрастного фільтра, зворотного до низькочастотного (відповідно К2.0, К3.0, К4.0), тобто, відбулося відновлення зображень.

Мірою оцінки якості відтворення зображень обрано показник *PSNR*, що визначається за формулою:

$$PSNR = 10 \cdot \lg\left(255^2 / \sigma_\varepsilon^2\right),$$

де σ_ε^2 – дисперсія похибки відтворення. При цьому загальновідомо, що зміни в зображенні не сприймаються людським оком, якщо рівень *PSNR* більший 35.

В таблиці (табл. 1) наведено результати експериментального дослідження низькочастотного та

контрастного фільтрів та середнє значення по 60 експериментам. Дослідження показало що спотворення зображення є незначним, показник *PSNR* дає нам можливість стверджувати, що контрастування після низькочастотної фільтрації не призводить до втрат які могли б бути помітні для людського ока.

Таблиця 1

Значення *PSNR* після застосування фільтрації

Зображення	Н2.0-К2.0	Н3.0-К3.0	Н4.0-К4.0
1	69,86	58,24	53,32
2	63,45	51,50	51,28
3	73,71	62,08	56,93
…	…	…	…
і т.д.	…	…	…
…	…	…	…
59	74,21	64,31	51,04
60	69,66	55,82	52,77
Усереднені.	70,31	57,76	52,56

Отриманий результат може мати застосування при різних типах цифрової обробки зображень, в тому числі і як складова при реалізації методів стиснення з втратами.

УДК 658.012:681.32:621.38

ЗАСТОСУВАННЯ МЕТОДІВ НАВЧАННЯ ПАРАЛЕЛЬНО-ІЄРАРХІЧНОЇ МЕРЕЖІ ДЛЯ РОЗПІЗНАВАННЯ ОБРАЗІВ

В.В. Мельніков
Державний економіко-технологічний університет транспорту
scon@yandex.ru

Для навчання ПІ мережі для розпізнавання образів будемо використовувати комбінований метод, що містить методи навчання, засновані на корекції помилок (error-correcting learning) і на пам'яті (memory based learning).

Послідовність комбінованого методу навчання ПІ мережі для розпізнавання образів:

1. Побудова структури ПІ мережі обраного зображення.
2. Застосування методу навчання, заснованого на пам'яті. Класифікатором на основі k-*найближчих* сусідів, що використовується в даному методі, є число рівнів ПІ мережі.
3. Побудова структури ПІ мережі еталонного зображення.
4. Застосування методу навчання, заснованого на корекції помилок. Критерієм, що використовується для верифікації в даному методі, є коефіцієнт кореляції на нульовому рівні ПІ мережі.
5. Проведення корекції помилок для коефіцієнтів кореляції на нульовому, першому, середньому, передостанньому й третьому з кінця рівнях. Корекція проводиться доти, доки параметри мережі не прийдуть до

абсолютно рівноважного стану (+1), або перевищать його. Якщо значення параметрів приводить до (-1) або абсолютно нерівновагого стану, то робиться висновок про неприналежність зображення до даного образу.

Найважливіші технічні переваги запропонованого комбінованого методу навчання ПІ мережі, які реалізовані в новому програмному засобі, в порівнянні з попередніми програмними засобами й методами, закладеними в ньому, наступні: точність вимірювання після корекції енергетичних центрів фрагментів плям лазерних пучків склала 0,01 елементу розкладання (у порівнянні з 1,2 елементів розкладання). При цьому відсоток «хороших» зображень склав 38,4% (у порівнянні з 50%), що підвищує загальний відсоток коректного розпізнавання до 92,5% (84,8%). Однак, показник «середній час розпізнавання», на початковому рівні при навчанні ПІ мережі становить: 60 с (30 с).

При розпізнаванні статичних образів (зображень людських облич) середній відсоток коректного розпізнавання на нульовому рівні ПІ мережі підвищився: 93,75% (80%). Також відзначаємо значне зростання середнього відсотка коректного розпізнавання статичних образів при побудові порівневих кореляційних кривих: 84% (у порівнянні з 5%). Показник «середній час розпізнавання» на початковому рівні при навчанні ПІ мережі становить: 10,73 с (12 с).

УДК 621.39

ДЕЛЬТА УЩІЛЬНЕННЯ МОВЛЕННЯ З ВИКОРИСТАННЯМ ІНТЕРВАЛЬНОГО ПРОГНОЗУВАННЯ

С.В. Хрущак аспірант
Вінницький національный техничний університет
hsv@mail.ru

Переважна більшість алгоритмів ущільнення мови, які застосовуються в IP-телефонії, використовують модель лінійного прогнозування для опису та кодування сигналу, відповідно до якої спектральна інформація про сигнал описується 10-ма коефіцієнтами лінійного прогнозування (LPC). Для більш ефективного квантування та подальшої інтерполяції коефіцієнти LPC, як правило, перетворюють на лінійні спектральні пари (LSP) та квантують їх за допомогою кодових книг. Дані LSP коефіцієнти мають залежності між елементами як в середині фрейму, так і між сусідніми фреймами, що говорить про високий рівень надлишковості при використанні даних коефіцієнтів. Врахування кореляції між коефіцієнтами дозволяє зменшити обсяг даних, необхідних для опису параметрів мовленнєвого сигналу, і таким чином зменшити вимоги до пропускної здатності каналу передачі мовленнєвої інформації.

Для врахування кореляції між коефіцієнтами одного фрейму використовується векторне квантування коефіцієнтів LSP. При цьому набір коефіцієнтів LSP розглядається як один вектор $C = (c_1, c_2, ..., c_{10})$, для якого відбувається пошук найближчого квантованого значення у

спеціальній таблиці - векторній кодовій книзі, яка представляє собою набір векторів значень коефіцієнтів $K = (C_1, C_2, \ldots, C_m)$, де m – розмір кодової книги. Для врахування кореляції між послідовними фреймами запропоновано метод дельта-ущільнення з прогнозуванням наступного відліку, який дозволяє зменшити кількість бітів, необхідних для опису коефіцієнтів прогнозування, за рахунок передачі різниці між індексами сусідніх фреймів. Для подальшого зменшення обсягів даних, що передаються, використовується зменшення вікна дельти між індексами сусідніх фреймів на основі інтервального прогнозу для індексу наступного фрейму на основі набору попередніх значень. При ущільненні на приймальну сторону також передається дельта між прогнозованим та реальним значеннями. Дослідження різних методів інтервального прогнозу показало, що вони забезпечують більшу точність прогнозування індексів коефіцієнтів, порівняно з екстраполяцією.

На основі запропонованого інтервального методу було удосконалено існуючий вокодер MELP, який дозволяє отримати гарну якість мовленнєвого сигналу на бітовій швидкості 2800 Біт/с. Використання данного методу дозволило зменшити необхідну бітову швидкість для кодеку до 2400 Біт/с. Створено програмний засіб для IP-телефонії, який використовує даний покращений кодек MELP для передачі мовлення по мережі.

Результати дослідження запропонованого методу за спектральним спотворенням показали, що використання методу дельта-ущільнення з інтервальним прогнозуванням дозволяє зменшити обсяг інформації для опису фрейму сигналу до 48 бітів без суттєвої втрати якості синтезованого мовлення.

УДК 621.39

КЛАСТЕРИЗАЦІЯ МОВЛЕННЄВИХ ДАНИХ ПРИ СТВОРЕННІ КОДОВИХ КНИГ ДЛЯ УЩІЛЬНЕННЯ МОВИ

О.Д. Феферман, аспірант,
Вінницький національний технічний університет
oleg.feferman@gmail.com

Для ущільнення мовленнєвих сигналів широко застосовують методи на основі лінійного прогнозування. Замість коефіцієнтів лінійного прогнозування на практиці використовують лінійні спектральні пари (LSP).

Для підвищення степені ущільнення LSP квантують за допомогою таблиць, які називаються кодовими книгами. Скалярні кодові книги не потребують складних обчислень і великих витрат пам’яті. Векторні кодові книги дозволяють досягти більшої степені ущільнення при тій же якості синтезованого звуку, що і скалярні. Один з основних недоліків векторного квантування – висока тривалість пошуку вектора у кодовій книзі, що заважає обробляти мовленнєві сигнали в режимі реального часу.

Пропонується новий підхід до впорядкування векторів у кодовій книзі, який дозволяє досягти зменшення складності обчислень. Підхід базується на створенні структурованих векторних кодових книг. Кодова книга розбивається на класи, що не перекриваються між собою та містять різну кількість векторів. Кожен вхідний вектор також можна віднести до певного класу, при цьому пошук відповідного йому класу зводиться до простої процедури порівняння та не вимагає значних обчислювальних витрат.

Математична модель упорядкування векторів базується на відношенні мажорування. Нехай задано вектори $X = (x_1, x_2, .., x_n), Y = (y_1, y_2, .., y_n)$. Говорять, що Y слабо мажорує X (позначається $X \prec_w Y$), якщо:

$$\sum_{i=1}^{k} x_i \le \sum_{i=1}^{k} y_i, k = 1,2,..,n$$

Мажоризація дозволяє розмістити вектори у чіткій послідовності, але для довільних векторів LSP побудова такої послідовності не завжди можлива. Тому ці вектори розбиваються на групи (рівні), а відношення мажорування застосовується не до самих векторів, а до створених рівнів. Ця операція називається структуризацією векторних кодових книг. Структуризація має на меті скорочення обчислювальних витрат на пошук квантованого вектора у кодовій книзі, що є найближчим до вхідного вектора.

Структуровані кодові книги будуються для кожного підвектора незалежно. Основна ідея методу прискореного пошуку полягає у тому, що найближчі до вхідного вектора квантовані вектори в кодовій книзі знаходяться на тому ж або сусідніх рівнях, що і вхідний вектор. За рахунок цього з'являється можливість значно скоротити число кандидатів на відбір і, відповідно, зменшити час пошуку.

Пошук найближчого вектора відбувається в два етапи: пошук рівня мажоризації, якому належить вхідний вектор та пошук найближчого до вхідного квантованого вектора на знайденому рівні мажоризації та кількох сусідніх рівнях. Перевірка відношення мажорування призводить до набагато менших обчислювальних витрат порівняно з обчисленням відстані.

Результати проведених досліджень показали, що структурування кодових книг дозволяє зменшити обчислювальну складність та збільшити швидкість пошуку в кодовій книзі.

УДК 621.317

ВИМІРЮВАННЯ ОЦІНОК ПЕРІОДОГРАМ ІНТЕРФЕРЕНЦІЙНИХ СИГНАЛІВ

О.І. Прокопов, студент
КНУ ім. Т.Г.Шевченко
alexprokopov@mail.ru

Великий час розрахунків спектральних оцінок періодограм не дає можливості проводити їх вимірювання з необхідною розділовою здатністю в реальному часі. Забезпечити високу розділову здатність можливо за рахунок операцій усереднення спектральних складових при збільшені часу спостережень. Існуючі стендові системи реалізовані на базі мікропроцесорних пристроїв і мають в своєму складі контролери типу МС2721 і АЦП1107ПВ2, які не можуть проводити розрахунки спектральних оцінок в реальному часі. Перехід до обладнання закордонного виробництва потребує багато коштів.

Тому метою роботи є підвищення продуктивності обчислень усереднення спектральних оцінок періодограм та апаратної реалізації з використанням ПЛІС технології фірми ALTERA.

Розглянемо усереднення спектральних характеристик дискретного перетворення Фур'є (ДПФ) :

$$F(f)=\frac{1}{P}\sum_{i=1}^{P} x_i(f), \qquad (1)$$

де $x_i(f)$ - ДПФ вектора вхідного сигналу;

P - кількість інтервалів спостереження на проміжках часу T = $L \cdot \Delta t$.

ДПФ на проміжку часу $P \cdot L \cdot \Delta t$:

$$x(l \cdot \Delta f) = \frac{1}{PL} \sum_{i=0}^{P \cdot L-1} r(i \cdot \Delta t) W_{P \cdot L}^{i \cdot P \cdot l} . \qquad (2)$$

Врахуємо особливості $W_{P \cdot L}^{P \cdot l}$:

$$W_{P \cdot L}^{P \cdot l} = \exp\left\{ -j \frac{2\pi P l}{PL} \right\} = \exp\left\{ -j \frac{2\pi l}{L} \right\}.$$

Вираз (2) має вигляд:

$$x(l \cdot \Delta f) = \frac{1}{PL} \sum_{i=o}^{PL-1} r(i \cdot \Delta t) \cdot W_L^{i \cdot l} . \qquad (3)$$

Введемо заміну $i = pL + l$, де p=0,1,...,P-1 і представимо (3) у вигляді подвійної суми:

$$X(l \cdot \Delta f) = \frac{1}{L} \sum_{l=0}^{L-1} W_L^l \cdot 1/P * \sum_{p=0}^{P-1} r(p \cdot L + l) \Delta t . \qquad (4)$$

Обчислення значень спектральних складових по виразу (4) для всіх значень спектральних складових можливо виконати в два етапи. На першому етапі здійснюється усереднення значень проріджених відліків, а на другому етапі проводиться одне швидке перетворення Фур'є (ШПФ) проріджених відліків. Виграш у часі:

$$\frac{V_n}{V} = \frac{P \frac{L}{2} \log L}{\frac{L}{2} \log L} \approx \text{P},$$

де V_n - об'єм обчислень методом усереднення періодограм (1); V-об'єм обчислень по алгоритму, представленому (4), де обчислюється тільки одна процедура ШПФ.

Час обчислення порівняно з методом запропонованим в (1), зменшується в P разів , де P приймає значення від 20 до 50.

УДК 004.4

ПРОБЛЕМА СЕГМЕНТАЦИИ ДЛЯ ЗАДАЧИ ПОИСКА ИЗОБРАЖЕНИЙ

А.И. Молчановский, ст. преподаватель,
Нгием Лэ Куан, студент
Национальный технический университет Украины
«Киевский политехнический институт»
lequan.vn89@gmail.com

В условиях развития информационных технологий происходит стремительное увеличением объемов информации, в следствии чего необходимо разрабатывать методы структуризации этой информации с целью последующего поиска. В области поиска изображений на данный момент разработано достаточное количество эффективных систем, общим недостатком которых является узкая специализированность.

Сегментированность является одним из основных параметров изображения. Количество сегментов, их размер, взаимное месторасположение и цвет задают основную структуру изображения.

Поэтому анализ сегментированности является одной из самых важных задач при поиске похожих изображений.

В разработанной системе для разбиения изображения на сегменты используется эффективный алгоритм сегментации на графах.

Суть алгоритма заключается в том, что каждый пиксель изображения представляет собой вершину графа. Вначале строятся двунаправленные ребра между всеми соседними вершинами и для каждого ребра рассчитывается его вес, как эвклидово расстояние между точками в

пространстве (координатами) и их цветовыми компонентами RGB. После этого все ребра сортируются по найденным весам. Далее находится минимальное остовое дерево с помощью алгоритма Красскала, после чего получаются не пересекаемые множества вершин графа, которые и будут являться сегментами изображения.

Для ускорения работы алгоритма изображение на входе уменьшается и проходит через sharp-фильтр, который увеличивает контрастность переходов между объектами, упрощая тем самым разбиение изображения на сегменты.

После разбиения изображения на сегменты необходимо проанализировать полученные результаты. Для этого сегменты сортируются по мощности, рассчитывается площадь самых больших сегментов относительно размеров входящего изображения, определяется их центр и цветовое содержимое.

Такой анализ проходят все изображения и информация про сегменты добавляется в цифровые wavelet-эскизы в базе данных.

Входящее изображение так же проходит через модуль анализа сегментированности. После этого, полученные данные о сегментации входящего изображения попарно сравниваются со значениями сегментации всех изображений в базе данных.

Результатом сравнения является некоторая числовая оценка схожести сегментной структуры изображений. Эта оценка является одной из компонент общей оценки схожести входящего изображения и изображения в базе данных.

Применение этого подхода для поиска схожих изображений улучшил результаты поиска, так как сегментная структура является важным фактором при сравнении изображений.

УДК 004.4

МЕТОДОЛОГИЯ ТЕСТИРОВАНИЯ СИСТЕМ ПОИСКА ИЗОБРАЖЕНИЙ

А.И. Молчановский, ст. преподаватель
Буй Хиу Дат, студент
Национальный технический университет Украины «Киевский политехнический институт»
bhdatik@gmail.com

В условиях развития компьютерных технологий неуклонно растут объемы информации, в следствии чего остро становится вопрос структуризации и поиска необходимых данных. Изображения составляют большую часть информации в интернете, однако системы поиска схожих графических файлов либо узко-специализированы, либо имеют плохую эффективность. Именно поэтому задача создания эффективной и универсальной системы поиска изображений в данный момент является очень актуальной.

Изначальной задачей для исследования проблем поиска является классификация объектов поиска по семантическим признакам. Все изображения были разбиты на 12 классов: автомобили, блок схемы, города, животные, космос, мультипликация, рисунки, пейзажи, портреты, графика-тушь, логотипы, макросъемка.

Во время создания собственной системы поиска изображений возникает очевидный вопрос: «Как можно оценить её эффективность и сравнить с другими системами»? Для решения этой проблемы была разработана методология тестирования систем поиска схожих изображений. Такая система должна принимать на

входе файл от пользователя и выдавать множество изображений, схожих с входящим.

Для каждого входящего изображения выставляются оценки от 0 до 10 баллов по четырем параметрам: сегментированность (количество ярко выраженных объектов), контрастность (оценка четкости переходов между объектами), цветовая насыщенность (количество разных цветов), количество оттенков (оценка количества оттенков одного цвета (для всех цветов изображения)). Оценка параметров проводится экспертом.

По этим оценкам были отобраны эталонные изображения, у которых определенная характеристика оценивается в 0, 3, 5, 7, 10 баллов. Эталоны служат для упрощения оценки изображений экспертами.

К оценке результирующих изображений добавляется еще две характеристики от 0 до 10 баллов: семантическая схожесть результата с входящим изображением (сюжет, тематика и т.д.) и цветовая схожесть.

Для тестирования была создана база изображений объемом в 150 изображений.

После оценивания системы экспертами по вышеуказанной схеме проводится статистическая обработка полученных данных (расчет и сравнения математических ожиданий оценок входящего и результирующего изображений, расчет среднеквадратического отклонения оценок результатов от оценок входящих изображений и т.д.). Полученные зависимости можно использовать в качестве оценки качества поиска системой.

Данная методология позволяет оценивать эффективность разработанной системы поиска изображений. С помощью наведенной методологии была протестирована система Retrievr.

УДК 004.4

КЛАСТЕРИЗАЦИЯ ДАННЫХ ДЛЯ ЗАДАЧИ ПОИСКА ИЗОБРАЖЕНИЙ

А.И. Молчановский, ст.преп., В. А. Мистецкий, студент
Национальный технический университет Украины «Киевский политехнический институт»
mikxman@gmail.com

За последние годы наблюдается очень стремительное развитие информационных технологий. Компьютеризация затронула все сферы жизни, в следствии чего объемы цифровой информации значительно возросли. В связи с этим очень остро становится вопрос структуризации и поиска различных видов информации. Значительную часть цифровой информации занимают изображения, именно поэтому создание универсальных систем поиска изображений имеет высокую актуальность на сегодняшний день.

При разработке системы поиска схожих изображений мы столкнулись с проблемой большой вычислительной емкости процесса поиска. Это связано в первую очень большими объемами базы данных.

Для решения проблем производительности необходимо использовать разные подходы для распараллеливания вычислений и оптимизации поиска.

Одним из таких подходов является кластеризация данных.

Кластеризация подразумевает собой разбиение всей области данных на некоторые сегменты (кластеры) по определенному критерию.

В разрабатываемой системе каждое изображение представляется в виде некоторого эскиза, в основе которого лежит 32 цветовых блока, каждый из которых определяется тремя компонентами RGB.

В этом смысле каждое изображение является точкой в 32x3-мерном пространстве. Поэтому задача кластеризации является задачей разбиения этого пространства на области, в каждой из которых расстояние между точками не превышает некоторого порогового значения.

Расстоянием между эскизами будем считать эвклидово расстояние между точками в пространстве. Это же расстояние и является мерой схожести между эскизами изображений.

Таким образом мы можем отделить группы схожих изображений внутри самой базы данных. Это позволяет отсекать множество заранее не похожих изображений во время поиска, что значительно уменьшает затраты на вычислительные ресурсы и следовательно, уменьшает время поиска, которое для систем поиска в реальном времени является очень критичным.

Существует множество алгоритмов и подходов для кластеризации данных. Это алгоритм K-средних, нейронные сети Кохонена, метод «просеивания» и многие другие.

Для решения нашей задачи, был использован алгоритм кластеризации quality threshold, в основе которого лежит принцип разбиения множества точек на кластеры с определенным порогом расстояния между точками в пределах одного кластера. Это гарантирует то, что внутри одного кластера любая пара точек будет иметь схожесть, меньшую пороговой.

Применение такого подхода позволило значительно сократить время и ресурсоемкость поиска.

4. ЗАХИСТ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

УДК 512.83

СИНТЕЗ И АНАЛИЗ ГАРАНТИРОВАННО НЕВЫРОЖДЕННЫХ ШИФРУЮЩИХ (0, 1)-МАТРИЦ ВЫСОКОГО ПОРЯДКА

А.Я. Белецкий, д.т.н., профессор
Национальный авиационный университет
abelnau@ukr.net

Одна из важнейших проблем, возникающей при разработке матричных алгоритмов шифрования, состоит в формировании гарантированно невырожденных двоичных шифрующих матриц $\boldsymbol{M}$; при этом порядок циклической группы, образуемой степенями $\boldsymbol{M}$ в кольце вычетов по mod 2, должен быть максимально возможным. Или, другими словами, совокупность элементов указанной группы, которую назовем $\boldsymbol{M}$ - группой, должна обладать свойствами *m*-последовательности (свойствами *m*-полноты).

Пусть L_n есть мощность $\boldsymbol{M}$ - группы. Степени $\boldsymbol{M}$ образуют *m*-последовательность (т.е. последовательность максимальной длины), если

$$L^n=2^n-1,$$

где n – порядок матрицы.

Один из возможных методов синтеза двоичных матриц с указанными свойствами базируется на использовании составных кодов Грея (СКГ), образуемых произведением простых кодов Грея, определители которых по mod 2 равны единице. Тем самым, двоичные матрицы любого порядка, отвечающие СКГ, оказываются гарантированно невырожденными. Множество простых

кодов Грея составляет полную группу, представленную в табл. 1.

Таблица 1. Полная группа простых операторов Грея

Обозначение оператора	Выполняемая операция
1	Инверсная перестановка
2	Прямое КГ левостороннее
3	Обратное КГ левостороннее
4	Прямое КГ правостороннее
5	Обратное КГ правостороннее

В докладе иллюстрируются компьютерные программы, с помощью которых осуществляется процедура выбора СКГ G, обеспечивающих $m-$полноту двоичным шифрующим матрицам $\boldsymbol{M}$ $n-$го порядка, и проверка кодов G на отсутствие «артефактов». В частности, получены СКГ, доставляющие $m-$полноту матрицам $\boldsymbol{M}$ 256-го порядка: G_1=24334225, G_2=25224334 и G_3=2222535224.

Множество $m-$полных шифрующих матриц $\boldsymbol{M}$ можно существенно расширить за счет специальной группы линейных преобразований $\boldsymbol{g}$ над СКГ G, формирующих матрицы $\boldsymbol{M}$. В группу $\boldsymbol{g}$ входят такие операции как круговая прокрутка простых операторов, образующих СКГ G, на произвольное число шагов циклического сдвига; поразрядная и (или) полная инверсия, обращение, сопряжение операторов, составляющих исходный СКГ, а также любые комбинации перечисленных выше преобразований. Следует отметить, что $m-$полнота является инвариантной к «дружному» циклическому сдвигу строк и столбцов матрицы $\boldsymbol{M}$ $n-$го порядка, а это, по крайней мере, дополнительно в n раз увеличивает мощность множества $m-$полных матриц.

УДК 681.3.07

КОМПЛЕКС ПРОГРАММ ДЛЯ ИССЛЕДОВАНИЯ КРИПТОГРАФИЧЕСКИХ ПРИМИТИВОВ

А.Я. Белецкий, д.т.н., профессор,
Е.А. Аксентий, студент
Национальный авиационный университет
abelnau@ukr.net

Как известно, криптостойкие системы могут быть построены на основе многократного (итерационного) применения относительно простых криптографических преобразований (примитивов). Родоначальник компьютерной криптографии Клод Шеннон еще в середине пятидесятых годов прошлого столетия предложил алгоритм зашифрования открытых текстов, содержащий всего лишь два криптографических примитива. Один из примитивов осуществляет операцию нелинейной подстановки (замены) элементов шифруемого текста (Substitution). Вторым примитивом (по Шеннону) является оператор перестановки (Permutation). Указанная пара примитивов (Substitution + Permutation) совместно образуют один раунд криптографического преобразования так называемой SP-сети.

В современных шифраторах используются и другие криптографические примитивы, к числу которых относятся: гаммирование, циклический сдвиг, скользящее кодирование и ряд других.

В докладе рассматривается комплекс программ, в котором реализованы указанные выше криптографические примитивы нелинейной подстановки байтов шифруемого текста и перестановки элементов блока.

Нелинейная подстановка байтов построена на основе преобразования

$$y = (x \oplus \alpha)_{\varphi}^{-1} \otimes A \oplus \beta, \qquad (1)$$

в котором аддитивные компоненты α и β, а также невырожденная по mod 2 квадратная (0, 1)-матрица A и неприводимый полином φ, являются вариативными параметрами преобразования (1). Значения всех параметров преобразования, а именно, размеры векторов, порядок матрицы и степень неприводимого полинома выбраны равными восьми.

Алгоритм перестановки, как и подстановки, задается преобразованием (1), согласно которому элемент блока, расположенный в ячейке по адресу $\tilde{o}$ пересылается в ячейку по адресу y. Элементы перестановки для блоков длины N указаны в табл. 1.

Таблица 1. Элементы перестановки шифруемых блоков

Степень полинома	***N*** = 64	***N*** = 128	***N*** = 256	***N*** = 512
8	–	–	Бит	2 бита
7	–	Бит	2 бита	Полубайт
6	Бит	2 бита	Полубайт	Байт
5	2 бита	Полубайт	Байт	Слово
4	Полубайт	Байт	Слово	Дв. слово

Разработанная на языке C++ программа моделирования криптографических примитивов предоставляет возможность проводить статистические исследования примитивов в широком диапазоне изменения параметров преобразования. Интерфейсы криптопримитивов достаточно просты и удобны не только для выполнения научных исследований, но и с успехом могут быть использованы в учебном процессе.

УДК 004.056.55

СИСТОЛИЧЕСКИЙ КРИПТОПРОЦЕССОР

А.Г. Корченко, д.т.н., профессор
В.Н. Кинзерявый, аспирант
С.А. Гнатюк, аспирант
А.Л. Панасюк, студент
Национальный авиационный университет
aspirans@nau.edu.ua

В настоящее время для обеспечения конфиденциальности информации применяются криптографические алгоритмы. Использование устройств, позволяющих защитить информацию посредством выполнения процедур шифрования, является одним из наиболее эффективных средств борьбы с несанкционированным доступом. Вопросы реализации криптографических алгоритмов в реальном времени остаются по-прежнему актуальными.

Программная реализация криптографических алгоритмов не позволяет достичь достаточно высокой скорости шифрования и требует значительных дополнительных ресурсов, поэтому ее не эффективно использовать в системах реального времени, особенно в случаях передачи значительного объема данных.

Большинство криптосистем используют циклические типовые функции. Эту особенность можно использовать для повышения производительности цифровых устройств, составив алгоритм, предусматривающий конвейер данных и отобразив его на систолическую структуру, в которой очередной блок получает данные с предыдущего.

Целью работы является построение алгоритма систолического криптопроцессора, предусматривающего конвейер данных и реализацию системы шифрования Advanced Encryption Standard (AES).

При конвейерной обработке среднее время шифрования или дешифрования одного блока уменьшается с увеличением количества блоков шифрования или дешифрования данных.

С целью минимизации задержек в разрабатываемой структуре некоторые преобразования необходимо осуществлять путем соответствующих коммутаций сигнальных линий шин данных. Средняя скорость шифрования одного блока данных будет расти с увеличением объема обрабатываемой информации.

Предлагается систолический криптопроцессор, реализующий систему шифрования AES. Криптопроцессор содержит шину ключа, шину входящих данных, синхронизирующую шину, модуль начальной обработки данных, 10 модулей шифрования, модуль формирования результата и шину исходящих данных. С помощью управляемой синхронизирующей шины обеспечивается конвейерная обработка данных в модулях шифрования. По данным предварительного исследования, при обработке больших объемов данных, указанный метод дает возможность значительно увеличить скорость шифрования данных. Быстродействие достигается за счет использования систолической организации криптопроцессора при реализации криптографического алгоритма.

Предложенный систолический криптопроцессор может быть использован в средствах шифрования информации и системах ее обработки для расширения их возможностей.

УДК 681.3.06

ДИФФЕРЕНЦИАЛЬНЫЕ СВОЙСТВА МИНИ-ВЕРСИЙ БЛОЧНЫХ СИММЕТРИЧНЫХ ШИФРОВ

Л.С. Сорока, д.т.н, профессор,
А.А. Кузнецов, д.т.н, профессор, С.А. Исаев
Харьковский национальный университет
им. В.Н. Каразина
kuznetsov_alex@rambler.ru

Важным показателем эффективности современных информационно-телекоммуникационных систем и технологий является безопасность информации. Наибольшее развитие среди механизмов обеспечения безопасности информации получили блочные симметричные шифры, которые обеспечивают высокие показатели стойкости и вычислительной эффективности. Таким образом, разработка, исследование и сертификация отечественных блочных симметричных крипоалгоритмов является важной научно-технической задачей, тесно связанной с выполнением ряда государственных научно-технических программ и проектов.

Проводимый в настоящее время в Украине конкурс блочных симметричных шифров направлен на отбор алгоритмов-кандидатов, использующих отработанные при проведении международных конкурсов AES и NESSIE подходы и учитывающих, в тоже время, возможности существующих методов криптоанализа, в том числе, наиболее развитых методов дифференциального и линейного криптоанализа. В докладе представлены результаты исследований дифференциальных свойств мини-версий шифров DES, ГОСТ 28147-89, FIPS-197, а также

блочных симметричных шифров, которые были поданы на криптоконкурс Украины. При разработке мини-версий учтены особенности алгебраической организации и структуры шифров, а также опыт построения мини-версии блочного симметричного шифра Rijndael, отобранного и принятого в качестве национального стандарта шифрования США (FIPS-197).

Исследования состояли в построении таблиц XOR разностей, оценке максимальных значений переходов и сравнении их с асимптотическим показателем среднего значения максимума полных дифференциалов. Полученные результаты показали, что использование нелинейных узлов замен с улучшенными показателями, введение динамически зависимых от раундового ключа криптопримитивов существенно повышает запас стойкости блочных симметричных шифров. Так, мини-версия поданного на конкурс алгоритма ADE достигает асимптотических значений максимумов переходов в таблице XOR разностей уже на четвертом раунде. Для мини-версии шифра Rijndael аналогичный показатель достигается после пяти раундов. Это свидетельствует о существенном повышения «запаса прочности» шифра ADE за счет введении динамически изменяемых на каждом раунде в зависимости от используемых ключей криптопримитивов. Установлена прямая зависимость между свойствами нелинейных узлов замен (нелинейностью и автокорреляцией соответствующих булевых функций, описывающих внутреннюю структуру S-блока) и дифференциальными свойствами шифра в целом. В частности, показано, что повышение нелинейности булевых функций и снижение их автокорреляции позволяет при фиксированном числе раундов шифрования существенно снизить величину максимальных значений переходов в таблице XOR разностей.

УДК 681.3.06

ФОРМУВАННЯ ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ МАКСИМАЛЬНОГО ПЕРІОДУ ІЗ ВИКОРИСТАННЯМ ПЕРЕТВОРЕНЬ НА ЕЛІПТИЧНИХ КРИВИХ

О.О. Кузнецов[1], д.т.н., професор, Ю.М. Рябуха[1], Р.В. Сергієнко[2], к.т.н.
[1]Харківський університет Повітряних Сил
[2]Львівський військовий університет Сухопутних військ

Криптографічні перетворення на еліптичних кривих являють собою потужний математичний апарат, який широко застосовується для побудови доказово стійких криптографічних засобів захисту інформації. Використання алгебраїчних кривих в криптоперетвореннях забезпечує порівнянну стійкість при набагато меншій довжині ключа. Відповідно до цього аналіз, розробка та дослідження криптографічно стійких генераторів псевдовипадкових послідовностей на алгебраїчних кривих є перспективним напрямком досліджень.

У роботі проведено дослідження відомого генератору псевдовипадкових послідовностей на еліптичних кривих, який описано у стандарті NIST SP 800-90. Було встановлено наступні недоліки: циклову функцію генератору, що забезпечує максимальний період формованої псевдовипадкової послідовності внутрішніх станів та відповідних точок еліптичних кривих невизначено; формування псевдовипадкової послідовності біт із послідовності точок кривої шляхом вибірки блоку молодших бітів та їх конкатенація не задовольняє вимогам статистичної

розрізненості. Таким чином, відомий генератор псевдовипадкових послідовностей на еліптичних кривих (NIST SP 800-90) не задовольняє в повній мірі сучасним вимогам.

При проведенні досліджень було розроблено удосконалений метод, який, на відміну від відомих, за рахунок додаткового введення рекурентних перетворень, що реалізуються, наприклад, за допомогою лінійних рекурентних регістрів зі зворотними зв'язками, дозволяє формувати послідовності псевдовипадкових чисел максимального періоду, що підвищує ефективність та розширює можливості практичного використання. Розроблений метод заснований на зведенні задачі знаходження таємного ключа до вирішення теоретико-складної задачі дискретного логарифмування у групі точок еліптичної кривої і дозволяє формувати псевдовипадкові послідовності максимального періоду.

Запропонований метод формування псевдовипадкових послідовностей максимального періоду із використанням перетворень на еліптичних кривих знімає обидва виявлених недоліки відомого генератору псевдовипадкових послідовностей на еліптичних кривих (генератору, описаному у стандарті NIST SP 800-90): запропоновано використовувати лінійні рекурентні перетворення, які забезпечують формування максимального періоду послідовностей внутрішніх станів і відповідних точок еліптичної кривої; формування вихідної псевдовипадкової послідовності шляхом зчитування одного найменш значущого біту (біту парності) із координат точок еліптичної кривої задовольняє вимогам статистичної розрізненості.

Таким чином, запропонований генератор псевдовипадкових послідовностей задовольняє сучасним вимогам та може бути використаний у криптографічних засобах захисту інформації від несанкціонованих дій.

УДК 001.4

СТІЙКІСТЬ ТА ЖИВУЧІСТЬ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ В КОРПОРАТИВНИХ МЕРЕЖАХ ЗВ'ЯЗКУ

В.Б. Дудикевич, д.т.н., професор, Ю.Р. Гарасим
Національний університет «Львівська політехніка»
garasym_yr@polynet.lviv.ua

При дослідженні стійкості та живучості систем захисту інформації (СЗІ) корпоративних мереж зв'язку (КМЗ) важливим кроком є встановлення умов, при яких у них існує рівновага. Область рівноваги знаходиться між нижнім та верхнім порогами поза межами впливу дестабілізуючих факторів, тобто включає в себе гомеокінетичне плато (аналогія з екосистемами) (рис. 1.). Розміщення границь цієї області змінюється з еволюцією системи захисту, будь-яка дія щодо зміни системи впливає на розміщення та розміри області стійкості. В результаті практично неможливо визначити розміщення цих границь і, відповідно, бути впевненим, що СЗІ все ще знаходиться в області стійкості. При роботі зі складними системами «основний акцент переноситься з максимізації ймовірності успіху на мінімізацію ймовірності невдачі». Іншими словами, перебуваючи поруч із станом рівноваги слід замість приділення основної уваги «зусиллям, які призведуть до досягнення стану рівноваги», лише намагатися виключити можливість «виходу за межі» визначеної області, що охоплює цей стан, тобто підтримувати СЗІ КМЗ в області стійкості.

Властивість СЗІ залишатися в області стійкості називають «живучістю». Адаптивними є системи, які

«змінюють свою поведінку таким чином, щоб залишатися в області стійкості навіть при наявності дестабілізуючих факторів». Наведемо перелік факторів, які слід враховувати здійснюючи зміни в складних СЗІ КМЗ:

Рис. 1. Підтримання системи на гомеокінетичному платі

1) Принциповий взаємозв'язок між природою самої системи та природою дестабілізуючих для неї факторів та досить тонкий їхній баланс. 2) «Просторову» та «часову» пам'яті СЗІ, які збільшують ризик викликати непередбачувані наслідки в просторі та в часі. 3) Непостійний характер меж області стійкості системи, що позбавляє можливості точного передбачення наслідків впливу зовнішніх змін на область стійкості та живучість системи.

При проектуванні СЗІ КМЗ слід «прагнути, в першу чергу, до запобігання невдачі, а не до досягнення успіху». Це зміщує інтереси від підвищення ефективності до досягнення живучості системи».

УДК 004.6

ЗАХИСТ ІНФОРМАЦІЇ В ПРОТОКОЛІ Н.323

В.Б. Дудикевич, д.т.н., професор, В.М. Стеренчук,
Л.М. Ракобовчук, к.т.н, доцент
Національний університет «Львівська політехніка»
nebster4@gmail.com

IP-телефонія є одним із пріорітетних напрямків розвитку телефонного зв'язку. З кожним роком кількість абонентів, які використовують IP-телефонію (VoIP – Voice Internet Protocal) для проведення голосових переговорів, збільшується. Це пов'язано, насамперед, з меншою вартістю передачі даних за допомогою мережі Інтернет. Вже не тільки окремі користувачі, але й цілі підприємства намагаються використовувати Інтернет як основний засіб міжміського зв'язку. Системи передачі голосу по IP, так само як і традиційні телефонні системи, ні в якому разі не можна вважати захищеними від прослухування. Оскільки комерційна інформація звичайно є конфіденційною, питання безпеки такого зв'язку є все більш актуальним. Тому метою даної публікації було охарактеризувати основні проблеми захисту інформації в протоколі Н.323.

З сигнальної інформації, що курсує між кінцевим пунктом і сторожем, можна витягувати IP-адреси і дані про одержувача, після чого голосові пакети, що передаються за допомогою протоколу передачі даних в реальному часі, можна буде перехопити, на їх дорозі між кінцевими пунктами і декодувати за допомогою відповідного голосового кодека. Разом з копіюванням і, відповідно, перехопленням пакетів в мережі, в Н.323 можна використовувати ще одну можливість контролю -

конференцію через вузол управління багатобічним зв'язком (Multipoint Control Unit, MCU). По закінченню прослухування сигнальних даних MCU втручається за допомогою конференції, а потім змішує і копіює голосові пакети, так що їх можна декодувати. Таке включення конференції зазвичай неможливо не відзначити, оскільки час затримки збільшується, а якість передачі мови в більшості випадків знижується. В будь-якому разі сигнальні і голосові пакети необхідно ізолювати. Для цього існує маса можливостей, вибір яких залежить від передбачуваного середовища передачі - Internet, Intranet або Extranet.

Таким чином, захист інформації в VOIP потребує проведення подальших досліджень, у тому числі удосконалення це може бути досягнуто, наприклад, шляхом розробки комплексного захищеного VOIP-протоколу, який би мав такі властивості:

1) використовувався не тільки в комп’ютерних мережах, але й у мережах GSM-операторів, щоб захистити весь шлях розповсюдження інформації;

2) базувався на клієнт-серверній архітектурі (особливо це важливо в разі організації голосових конференцій;

3) використовував тільки високонадійні алгоритми шифрування інформації;

4) забезпечував узгоджене функціонування засобів шифрування та вокодера для зменшення затримок у часі при передачі даних.

Слід зазначити, що створення комплексного протоколу IP-телефонії, який би підтримував також стільниковий зв’язок, вимагає проведення додаткового дослідження, оскільки мобільні телефони не підтримують передачу даних у форматах, які використовуються в IP-мережах.

УДК 681.3

КОМБІНОВАНА СИСТЕМА КОНТРОЛЮ ПОБІЧНОГО ВИПРОМІНЮВАННЯ ВОЛЗ

В.Б. Дудикевич[1], д.т.н., професор,
І.Р. Опірський[2], аспірант
Національний університет «Львівська політехніка»
[1]vdudykev@polynet.lviv.ua, [2]hitman@point.lviv.ua

Існуючі системи контролю побічних випромінювань засновані на принципі послідовного пошуку сигналів за частотою, що вимагає достатньо великого часу для обстеження комп'ютерних приміщень і комп'ютерних мереж.

Дослідження рівня побічних електромагнітних випромінювань і наведень (ПЕВІН) від засобів обчислювальної техніки (ЗОТ) ґрунтується на загальних принципах інженерних вимірювань напруженості високочастотного (ВЧ) поля. Специфіка цих вимірювань полягає в тому, що, по-перше, вимірювані сигнали є малопотужними, по-друге, заздалегідь складно передбачити спектральну картину ВЧ поля конкретного ЗОТ. Тому вимірюванню рівня сигналів ПЕВІН завжди передує їх верифікація від інших сигналів в радіоефірі.
Інформативними ПЕВІН називаються сигнали, які представляють собою ВЧ несучу, що модулюється інформацією, яка обробляється на ЗОТ, наприклад, зображенням, що виводиться на монітор, даними, що обробляються на пристроях введення-виводу тощо.

Для проведення антенних вимірювань існує декілька типів вимірювальних приладів: селективні вольтметри, вимірювальні приймачі, аналізатори спектру. Комбінована

система оперативного контролю на базі акустооптичних Фур'є-процесів дозволить зайняти провідне місце в системі контролю випромінювань через цілий ряд переваг:

- по швидкодії, раціональності побудови, багатофункціональності і багатоканальності - перевершує відомі приймачі;
- простота виконання перетворення Фур'є, яке використовуються не тільки при аналізі спектру сигналу, але і є базовою, ключовою операцією при виконанні функцій кореляції, згортки сигналів, узгодженій фільтрації не залежно від структури вхідних сигналів;
- володіючи двома степенями свободи, оптичні системи здатні обробляти велике число одновимірних сигналів.

Узагальнюючи характеристики одновимірних спектроаналізаторів з тимчасовим інтерфейсом, відзначимо, що ці пристрої дозволяють отримати розширення по частоті, обернено пропорційне часу інтеграції: порядка десятки Герц, число дозволених частот $10^3 \div 10^4$.

Оскільки оптичні системи виконують математичні операції із швидкістю світла, то їх продуктивність обмежується лише швидкістю введення і виведення даних. Сучасні акустооптичні процесори дозволяють реалізувати одночасно $10^2 \div 10^3$ паралельних частотних каналів при використанні однієї просторової координати і $10^4 \div 10^6$ паралельних частотних каналів при використанні двох просторових координат, а так само дозволяють отримати розширення по частоті, зворотньопропорційне часу інтеграції.

УДК 004.6

РЕАЛІЗАЦІЯ СИСТЕМИ БЕЗПЕКИ ЛОКАЛЬНОЇ ОБЧИСЛЮВАЛЬНОЇ МЕРЕЖІ З ДОСТУПОМ В ІНТЕРНЕТ НА БАЗІ FREEBSD

В.Б. Дудикевич, д.т.н., професор,
В.О. Ракобовчук, к.т.н, доцент
Національний університет «Львівська політехніка»
vovka3796@yandex.ru

Проблема захисту інформації на даному етапі розвитку інформаційних технологій, як ніколи, є актуальною. Щодня хакери піддають загрозі багато ресурсів, намагаючись отримати до них доступ за допомогою спеціальних атак.

Метою даної роботи була розробка захищеного Інтернет-шлюза локальної обчислювальної мережі з вбудованими правилами доступу до глобальних ресурсів і захистом від розповсюджених атак як зовні так і зсередини мережі є актуальною.

Проведений аналіз сучасних операційних систем для застосування їх в IT інфраструктурі дав можливість виділити наступні переваги FreeBSD:

- FreeBSD добре документована і стандартизована;
- наявність відкритого доступу до оновлень, виправлень, вихідного коду та бази даних повідомлень про помилки;
- BSD-ліцензія дозволяє вільно використовувати та модифікувати ОС під конкретні потреби.

Відповідно розробка захищеного Інтернет-шлюза була виконана на базі операційної системи FreeBSD. В роботі також проаналізовано сучасні проблеми інформаційної безпеки в мережах, і запропоновано такі заходи безпеки, як застосування

пакетного фільтра PF-FILTER та проксі-сервера SQUID. Проведені практичні дослідження і дані рекомендації по побудові захищеного Інтернет-шлюза і впровадження його в інформаційну інфраструктуру.

В результаті роботи розроблено шлюз з вбудованим захистом для безпечного доступу користувачів локальної мережі до Інтернету, а також розроблено політику безпеки. Вибрана ОС FreeBSD як найбільш доступна, надійна, безпечна для серверних мереж, а також гнучка в налаштуванні.

В роботі приведено порівняльні характеристики трьох пакетних фільтрів IPFW, PF-FILTER, IP-FILTER - найпопулярніших застосувань для FreeBSD. В результаті підсумовування і зведення всіх характеристик і особливостей пакетних фільтрів для FreeBSD було запропоновано застосовувати для реалізації безпечної роботи шлюза PF-FILTER. Крім того, можна сказати, що firewall надає надійний захист, але все ж накладає певні обмеження і досить трудомісткий для налаштування доступу для різних користувачів з розмежуванням прав. Використовуючи його, важко піддавати аналізу файли логування firewall. Тому було вирішено додатково впровадити проксі сервер на робочій станції.

Відповідно були проведені дослідження з проксі-сервером і досягнуті важливі практичні результати:

– чітке відстежування трафіку і управління доступом користувачів до конкретних ресурсів Інтернет.

– усунунення проблеми авторизації за обліковими записами Windows-користувачів мережі та обліку трафіку термінальних користувачів.

– побудована система, що дозволяє економити до 30% трафіку.

Для автоматизації процесу створення правил доступу до ресурсів створено показова програма на мові Python і апробована на базі тестової системи.

УДК 621.395

КРИПТОЛОГІЧНИЙ ПАКЕТ CRYPTOOL ТА ЙОГО ЗАСТОСУВАННЯ У НАВЧАЛЬНОМУ ПРОЦЕСІ

В.В. Хома, д.т.н., професор
Національний університет "Львівська політехніка"
khoma59@gmail.com

Захист інформації в інформаційно-телекомунікаційних системах не мислимий без застосування сучасних криптографічних засобів. Саме тому до системи підготовки фахівців з інформаційної безпеки важливо запроваджувати інструментарій, що дозволить не лише набути практичних навиків у застосуванні найбільш популярних криптографічних протоколів, але забезпечить розуміння суті й особливостей криптографічних перетворень, загроз і ризиків, які можуть виникати у реальних системах. В цьому сенсі заслуговує на увагу криптологічний пакет CrypTool, що розвивається на засадах відкритого програмного забезпечення європейськими університетами.

У пакеті CrypTool реалізовано практично всі сучасні криптологічні функції. Головне вікно програми містить 10 меню, серед яких Crypt/Decrypt, Digital Sygnatures/PKI, Indiv. Procedures, Analysis.

Меню Crypt/Decrypt містить засоби дослідження найбільш відомих історичних шифрів, найпопулярніших сучасних симетричних блокових алгоритмів (DES, IDEA, AES та ін.) і асиметричних – RSA. Частина криптоалгоритмів розміщена в меню Indiv. Procedures, зокрема алгоритм Diffie-Hellman. Тут доступними є також засоби візуалізації і анімації деяких алгоритмів, зокрема Enigma, Nihilist, DES з можливістю їх покрокового дослідження.

В меню Digital Sygnatures/PKI включено засоби, що дозволяють ознайомитися із технологією створення та верифікації цифрового підпису, а також генеруванням, зберіганням і висвітленням параметрів публічних та приватних ключів (алгоритмів RSA, DSA і на еліптичних кривих).

Меню Indiv. Procedures окрім вже згаданих засобів візуалізації окремих алгоритмів, розміщено набір програм до обчислення хеш-функцій, засоби кодування і стиснення даних, формування випадкових послідовностей та оцінки якості паролю. Для зручності в окремому підменю зібрано засоби, що стосуються найпопулярнішого асиметричного алгоритму RSA – генерування простих чисел, тестування чисел та факторизація чисел, а також демонстрування RSA в режимі шифрування/дешифрування і цифрового підпису.

В меню Analysis є засоби, що уможливлюють проведення автоматичного криптоаналізу як історичних, так і сучасних симетричних блокових та асиметричних алгоритмів, а також хеш-функцій.

При застосуванні в навчальному процесі пакету CrypTool виявлено деякі обмеження. Наприклад, не допускається опрацювання текстових документів в кириличному алфавіті. В наявному арсеналі інструментів криптоаналізу історичних шифрів не представлено методи Kasiski та Friedman. Для криптоаналізу сучасних блокових алгоритмів, реалізовано лише метод прямого перебору ключів, причому відбір правильної версії із множини дешифрованих документів базується лише на оцінці їх ентропії. Як наслідок, криптоаналіз стає неможливим, якщо дані перед шифруванням були стиснені. Крім того, режим CBC (зв’язування блоків шифрограми) алгоритму DES не передбачає використання вектора ініціалізації, а відтак не дозволяє підняти стійкість шифрограм, а режим CFB (зворотний зв’язок за шифрограмами) взагалі відсутній.

УДК 681.3

МАТЕМАТИЧНА МОДЕЛЬ АПАРАТНОЇ ЧАСТИНИ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

А.Д. Кожухівський, д.т.н., професор,
А.В. Сагун, к.т.н., ст. викладач,
О.А. Кожухівська, аспірантка
Черкаський державний технологічний університет
andrejdk@mail.ru

Задача визначення оптимальної апаратної структури, яка здатна забезпечити нормальну роботу системи захисту сегменту мережі, може бути розв'язана за умови детермінування основних вхідних, вихідних та внутрішніх потоків та параметрів загроз системи інформаційної безпеки і побудови імітаційної моделі. Система захисту інформації (СЗІ) може бути представлена у вигляді моделі, що складається з деякого набору засобів захисту (ЗЗ). На вхід ЗЗ поступають потоки запитів несанкціонованого доступу (НСД). Далі ці потоки розріджуються, утворюючи вихідний потік.

Ймовірність забезпечення захисту розглядається як ймовірність відсутності запитів НСД до ресурсів, що захищаються, і визначається як $Z(t) = 1 - F(t)$ за умови, що $F(t)$ є функцією розподілу випадкової величини $\tau_{НСД}$. Оскільки потік НСД розподілений за законом Пуассона, оцінку захищеності можна отримати за наступною формулою: $Z(t) = e - \sum \lambda_i q_i t$, а інтенсивність потоку пропущених запитів за наступною формулою: $H(t) = \sum \lambda_i q_i t$.

Розроблена імітаційна модель дозволяє відтворити обслуговування безлічі завдань при будь-яких заданих статистичних відомостях про вхідні потоки і ресурси інформаційної системи (ІС). В якості прикладу була розроблена математична модель системи протидії НСД за умови, що існуючі загрози розподіляються так: троянські програми (55%), мережні черв'яки (30%), інші Spyware (15%). Така модель інформаційного захисту є ІС з випадковим вибором програм обробки інформаційних заявок. Імітаційне моделювання моделі ІС виконано мовою GPSS.

Для випадкового вибору програм обробки в моделі використовується дискретна випадкова функція DISR. Функція DISR використовує значення випадкових величин, що генеруються програмним датчиком GPSS RN5. ІС імітується пристроєм з ім'ям SYST. Блок ADVANCE здійснює затримку оброблюваної заявки (транзакта) в залежності від типу потенційної загрози відповідно до значення функції DISR.

Беручи до уваги розмір черги QUEUE, їх кількість ETM1, ETM2 та розмір потенційного транзакта загрози, можна розрахувати величину програмного (апаратного) буфера пам'яті апаратної платформи захисту. Аналізуючи коефіцієнт завантаження приладу UTIL та розмір потенційного транзакту інформаційної загрози, можна розрахувати продуктивність процесора, необхідну для нормального функціонування системи протидії НСД з врахуванням подальшого її розширення.

УДК 004.056.5

ПРОГРАММНО-АППАРАТНЫЙ КОМПЛЕКС КРИПТОЗАИТЫ КАНАЛОВ СВЯЗИ

В.И. Стецюренко[1], к.т.н., доцент,
А.С. Чашинский[2], А.Г. Лукошко[3]
Объединенный институт проблем информатики
НАН Беларуси
[1]witas@newman.bas-net.by, [2]chashinski@gmail.com,
[3]andrew.lukoshko@gmail.com

В специализированных сетях в процессе обработки и обмена данными требуется криптографическая защита передаваемой по каналам связи информации.

Программно-аппаратный комплекс безопасности (ПАКБ) реализует принцип прозрачного шифрования.

В связи с тем, что ПАКБ должен поддерживать принцип прозрачного шифрования на канальном уровне (уровень 2 модели OSI), комплекс создан в виде сетевого моста.

Аппаратная реализация ПАКБ состоит из двух устройств, основой которых является плата, содержащая сокет для процессора Core 2 Duo, слоты для оперативной памяти типа DDR3, два USB-разъема, три встроенных сетевых Ethernet-порта 1 Гбит.

Следует отметить, что устройства не содержат винчестеров, поэтому рабочая ОС находится на flash-накопителях, с которых происходит загрузка.

Для ПАКБ создана собственная сборка операционной системы на основе ядра Linux, основанная только на исходных текстах от разработчиков и не использующая другие системы сборки.

В основе системы лежат два компонента: ядро операционной системы Linux (объем архива с исходными текстами 64 МБайт) и набор базовых утилит командной строки Busybox (объем архива с исходными текстами 2 МБайта). После инициализации ядра и создания файловой системы /dev запускается стартовый скрипт, который настраивает сетевые карты, сетевой экран, соединение типа «мост», а затем выполняет приложение, реализующее перехват пакетов, шифрование сетевого трафика по алгоритму BelT, генерацию пакетов с зашифрованными данными и отправку в сеть.

Перехват, анализ и отправка зашифрованных/расшифрованных пакетов в сеть реализованы с использованием таких библиотек, как libpcap и libnet. Библиотека libpcap предназначена для извлечения пакетов из сети и их анализа. Использование библиотеки libpcap позволяет создать мощный фильтр, сравнимый с тем, что присутствует в утилите tcpdump. Библиотека libnet предназначена для генерации пакетов произвольного формата и отправки в сеть.

Перехваченный трафик шифруется криптографическим алгоритмом «BelT» – СТБ П 34.101.31-2007. Данный алгоритм представляет собой симметричный алгоритм блочного шифрования (размер блока 128 бит, ключ 256 бит), который принят в качестве предстандарта шифрования в Республике Беларусь Программная реализация алгоритма для ПАКБ была реализована коллективом разработчиков Объединенного института проблем информатики НАН Беларуси.

УДК 004.056

О ПОДХОДЕ К СОВЕРШЕНСТВОВАНИЮ АЛГОРИТМА ЗАЩИТЫ ИНФОРМАЦИИ В СИСТЕМАХ МОБИЛЬНОЙ СВЯЗИ

А.Д. Буханцов, к.т.н., с.н.с.
Белгородский государственный университет
bukhantsov@bsu.edu.ru

В настоящее время вопросы защиты информации (оцифрованной речи и данных) в системах мобильной связи приобретают практическое значение. К услугам подвижной радиосвязи многие категории пользователей прибегают чаще, чем проводной. Для проведения переговоров, содержащих коммерческую, банковскую, нотариальную, врачебную и многие другие виды тайн, необходимо обеспечить необходимую степень защиты. Кроме того, сотовая связь активно используется для доступа к Интернет. Самый надежный путь – применение специально разработанных приставок к мобильным станциям, использующих проверенные экспертами алгоритмы шифрования, например, ГОСТ 28147-89 или иные стандарты шифрования данных. При таком подходе необходимо обеспечить дополнительными устройствами всех пользователей сотовой связи, нуждающихся в проведении закрытых переговоров, а также организовать распределение соответствующих ключей.

Предлагаемый подход позволяет повысить защищенность речи и данных без применения дополнительных технических устройств. Можно «перепрограммировать» используемые мобильные станции

для реализации новых способов защиты, например, силами и средствами операторов мобильной связи.

Общий принцип шифрования речи и данных в системах сотовой связи стандарта GSM состоит в наложении гаммы на оцифрованную речь. Как правило, для решения такой задачи используется комбинированная схема из линейных рекуррентных регистров (ЛРР), вырабатывающих псевдослучайную последовательность (ПСП). При этом объем ключа шифрования определяется общим числом ячеек регистров и составляет 64 бита.

Некоторые варианты алгоритма шифрования данных А5, опубликованные в открытых источниках, обладают довольно низкой криптостойкостью. Очевидно, одним из путей повышения криптостойкости алгоритма является увеличение периода повторения ПСП, которую формирует комбинированная схема.

Предлагаемый подход направлен на совершенствование методологического аппарата, позволяющего для заданной сложной схемы из нескольких ЛРР определить период повторения ПСП. При этом смежной задачей является поиск варианта композиции ЛРР, реализующего максимальное (или рациональное) значение периода ПСП при соблюдении ограничений на объем ключа (64 бита). Ограничения на объем ключа дают возможность использовать мобильные станции различных поколений и производителей, а также существующий алгоритм формирования ключа в SIM-карте.

Более совершенные алгоритмы защиты информации на основе предлагаемого подхода могут применяться и в других системах связи, где используется поточное шифрование данных. Такие схемы защиты обеспечивают, как правило, более высокие скорости передачи защищенных данных по сравнению с блочными системами шифрования.

УДК 681.32

ЗАХИСТ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ В СИСТЕМАХ ДИСТАНЦІЙНОГО НАВЧАННЯ

І.А. Золотарьова[1], к.е.н., професор,
Н.А. Кошева[2], к.т.н., доцент,
[1]Харківський національний економічний університет
[2]Харківська національна юридична академія України ім. Ярослава Мудрого
[1]is@ksue.edu.ua, [2]n_kosheva@mail.ru

В інформаційному середовищі, в якому можна легко видозмінювати та адаптувати твори, велике значення набуває захист інтелектуальної власності. Цифрове середовище загострило питання охорони авторських прав, створивши недобросовісним користувачам широкі можливості для їх порушення. Але інформаційні технології, створивши нові проблеми, одночасно запропонували й шляхи їх вирішення. Найбільш ефективними з них уявляється поєднання техніко-юридичного та технологічного способів, тобто удосконалення правової охорони особистих прав автора та створення та широкого використання технічних засобів захисту інтелектуальної власності.

Як при платній, так і при безкоштовній системах дистанційного навчання додатково виникають проблеми, які вимагають своєчасного рішення, а саме: авторизація користувачів для доступу до даних, захист авторських прав, захист від копіювання інформації.

Тобто при будь-яких формах навчання інформація повинна захищатися від знищення, модифікації, підміни, копіювання, несанкціонованого доступу і блокування.

Для вирішення цих питань пропонується застосовувати методи стеганографії. Основними положеннями сучасною комп'ютерними стеганографії є наступні: методи приховання повинні забезпечувати автентичність і цілісність файлу, передбачається, що противникові повністю відомі можливі стеганографичні методи, безпека методів ґрунтується на збереженні стеганографичним перетворенням основних властивостей відкрито файлу, що передавється при внесенні до нього секретного повідомлення і деякою невідомою противникові інформації – ключа, навіть якщо факт приховання повідомлення став відомий противникові через спільника, витягання най секретнішого повідомлення представляє складне обчислювальне завдання.

Аналіз інформаційних джерел комп'ютерної мережі Internet дозволяє вправити вивід, що в даний час стеганографичні системи активно використовуються для вирішення наступних основних завдань:

1. Захист конфіденційної інформації від несанкціонованого доступу;
2. Подолання систем моніторингу і управління мережевими ресурсами;
3. Камуфляжі програмного забезпечення;
4. Захист авторського права на деякі види інтелектуальної власності.

Зупинимося детальніше на захисті права від піратства. На комп'ютерні графічні зображення наноситься спеціальна мітка, яка залишається невидимою для очей, але розпізнається спеціальним ПО. Таке програмне забезпечення вже використовується в комп'ютерних версіях деяких журналів. Даний напрям стеганографії призначений не лише для обробки зображень, але і для файлів з аудио- і відеоінформацією і покликаний забезпечити захист інтелектуальної власності.

УДК 681.3.06

АУТЕНТИФИКАЦИЯ ДАННЫХ С ИСПОЛЬЗОВАНИЕМ КЛЮЧЕВЫХ ХЕШИРУЮЩИХ ФУНКЦИЙ

В.Ю. Ковтун[1], к.т.н., с.н.с.,
С.П. Евсеев[2], к.т.н., О.Г. Король[2]
[1]Национальный авиационный университет
[2]Харьковский национальный экономический университет
[1]vladislav.kovtun@gmail.com, [2]evseev_serg@inbox.ru

Важным элементом современных систем защиты информации являются механизмы обеспечения целостности и аутентичности обрабатываемых и передаваемых данных. К ним относятся: цифровые подписи, коды подтверждения подлинности, хеширующие функции и другие механизмы безопасности.

Одним из наиболее эффективных методов обеспечения аутентичности и целостности данных без использования дополнительных механизмов является применение ключевых хеширующих функций. Их практическое применение позволяет реализовать вычислительно эффективные механизмы проверки подлинности данных для обеспечения целостности и аутентичности обрабатываемой и передаваемой информации.

В докладе рассматриваются известные методы формирования ключевых хеширующих функций, исследуются их криптографические свойства и устойчивость к различным атакам. Проводятся сравнительные исследования криптографических

хеширующих функций, представленных в рамках общеевропейского конкурса NESSIE и национального конкурса США. В ходе проведенных исследований установлено, что по соотношению криптографическая стойкость/вычислительная эффективность наиболее перспективными являются универсальные хеширующие функции, которые позволяют обеспечить доказуемый уровень коллизий (столкновений, совпадений хеш-образов), который определяется алгебраическими свойствами применяемых преобразований.

В результате проведенных исследований показано, что в основе построения универсальных хеширующих функций лежат методы теории чисел и колец многочленов, вероятность коллизий для таких методов определяется групповыми свойствами классов вычетов и алгебраическими свойствами колец многочленов. В тоже время, существующие подходы к построению универсальных хеширующих функций не позволяют реализовать высокую криптографическую стойкость. Применяемые в композиции с универсальным хешированием методы шифрования (например, в алгоритме UMAC) обеспечивают требуемый уровень криптографической стойкости, но свойства универсальности, т.е. теоретической обоснованности уровня коллизий при этом теряются. Другими словами, существующие методы и алгоритмы ключевого универсального хеширования не позволяют в полной мере обеспечить современные вероятностно-временные требования.

Перспективным направлением дальнейших исследований является разработка ключевых универсальных хеширующих функций, которые обеспечат высокий уровень криптографической стойкости и вычислительной эффективности.

УДК 681.3.06

ОЦЕНКА ЭФФЕКТИВНОСТИ ПРОЕКТИРОВАНИЯ АЛГОРИТМА БЛОЧНОГО СИММЕТРИЧНОГО ШИФРОВАНИЯ

С.А. Головашич[1], к.т.н., С.П. Евсеев[2], к.т.н., И.В. Московченко[3]
[1]Генеральный директор ООО «КРИПТОМАШ»
[2]Харківський національний економічний університет
[3]Военный колледж сержантского состава Национального технического университета “Харьковский политехнический институт”
[1]sg@cryptomach.com, [2]evseev_serg@hneu.edu.ua, [3]larry_green@mail.ru

Наиболее распространённым подходом предварительного анализа современных криптоалгоритмов в целом, и БСШ в частности, является оценка трёх показателей: устойчивости алгоритма к известным криптоаналитическим атакам, производительности программной реализации алгоритма на современных ПК и “статистической безопасности” (формирование “хороших” псевдослучайных последовательностей). Проведенный анализ шифров-конкурсантов на стандарт БСШ Украины показал, что алгоритмы “Мухомор” и “Калина” обладают рядом идентичных недостатков и специфических особенностей.

Конструкция схемы разворачивания ключей алгоритмов “Калина” и “Мухомор” не гарантирует биективность отображения исходного (пользовательского) ключа в рабочую последовательность цикловых ключей

шифрования и поэтому осложняет решение задачи оценки размерности пространства значений цикловых ключей.

Проведенное моделирование на уменьшенной схеме “разворачивания” ключа, подтвердило возможность существования достаточно большого класса эквивалентных ключей для выбранной конструкции схемы “разворачивания”.

Проведенное исследование показало, что все три рассмотренные алгоритма унаследовали от общего прототипа AES его “структурные” свойства. Это свойство проявляется в сохранении “структурных” свойств текста при шифровании блока данных на нулевых или других, специальным образом подобранных, цикловых ключах. Для преодоления этих “структурных” свойств, авторы БСШ “Калина” и “Мухомор” использовали набор констант в схеме разворачивания ключа, а в случае алгоритма “Лабиринт” – сложение с константами использовалось внутри функции шифрования. Проведенный анализ показал, что преодолеть указанное свойство в рассмотренных алгоритмах можно путем замены “регулярной” байтовой перестановки на специальным образом подобранную “нерегулярную” перестановку. “Нерегулярная” перестановка, в сочетании с применением операции сложения с переносом, позволит полностью устранить указанные структурные свойства. При этом фиксированная байтовая перестановка в обоих случаях имеет нулевые затраты на реализацию. Такая замена позволит отказаться от применения XOR-сложения с константой на выходе F-функции алгоритма “Лабиринт” (для случаев $L_B > 128$), что позволит сэкономить, как минимум, одну микрооперацию. Данное усовершенствование будет воплощено во второй версии алгоритма “Лабиринт”.

УДК 621.391

ПОСТРОЕНИЕ МОДЕЛЕЙ АТАК НА ВНУТРИПЛАТЕЖНЫЕ БАНКОВСКИЕ СИСТЕМЫ

С.П. Евсеев, к.т.н., А.И. Гончарова
Харьковский национальный экономический университет
evseev_serg@inbox.ru

В развитии рыночных отношений главенствующую роль играют коммерческие банки, аккумулирующие огромные финансовые потоки. Информационные банковские системы становятся одной из наиболее уязвимых сторон современного банка, притягивающие к себе злоумышленников, как из числа персонала банка, так и со стороны. Нарушение работы банковских систем приводит к потере не только конфиденциальной информации банка, но и к экономическим ущербам, как банка, так и его клиентов, что создает общенациональную проблему.

Для обеспечения защиты банковской информации в ВПБС на различных уровнях используются криптографические механизмы, однако, бурный рост вычислительной техники, создание систем и технологий кибертерроризма приводит к появлению новых угроз (активных и пассивных атак) и взлому подсистемы защиты ВПБС. Одним из наиболее уязвимых мест в системе электронных платежей является пересылка платежных и других сообщений между банками, между банком и банкоматом, между банком и клиентом. Для защиты платежных сообщений используется система защищенной электронной почты (СЗЭП), предназначенная для обмена

электронными сообщениями в формате SMF-70 через сеть передачи данных произвольного типа в соответствии с критериями НД ТЗІ 2.5-004-99.

Для совершенствования подсистемы защиты ВПБС в условиях появления новых угроз необходим постоянный анализ риска проведения той или иной атаки (реализации угрозы). Перечень угроз, оценки вероятностей их реализации, а также модель нарушителя служат основой для проведения анализа риска и формулирования требований к системе защиты ВПБС. Однако в полной мере все это невозможно выполнить без построения и анализа модели реализации угроз и моделей пассивных и активных атак. Моделирование процесса реализации угроз безопасности ВПБС целесообразно осуществлять на основе рассмотрения логической цепочки: “угрозы – источник угрозы – метод реализации – уязвимость – последствия”. На основании проведенных вычислений, разработана общая структура подсистемы защиты информационных ресурсов во ВПБС. Для построения общей структуры подсистемы безопасности информационной безопасности ВПБС и моделей атак выбран функциональный тип математических моделей, называемый моделями “черного ящика”.

На основании разработанной общей структуры подсистемы защиты информационных ресурсов построены математические модели основных видов пассивных и активных угроз на внутриплатежные банковские системы.

Проведенные исследования показали, что для обеспечения безопасности банковской информации во ВПБС используются криптографические алгоритмы шифрования, обеспечивающие аутентичность и целостность сообщений. Разработанные математические модели позволяют оценить степень эффективности основных типов атак, что облегчает выбор необходимых средств и методов защиты информации во ВПБС.

УДК 681.32

МЕТОДЫ РАЗГРАНИЧЕНИЯ ДОСТУПА В НЕСТРУКТУРИРОВАННЫХ ТЕКСТОВЫХ ХРАНИЛИЩАХ

А.В. Петрашенко, к.т.н., доцент
Д.С. Замятин, к.т.н., доцент
Национальный технический университет Украины «Киевский политехнический интитут»
dsz@ukr.net

Одним из перспективным подходов к упрощению поиска и систематизации неструктурированных текстовых ресурсов на сегодня является создание хранилищ. В предыдущих работах авторов предложен эффективный способ организации подобных хранилищ на основе унифицированного набора операций. Однако в них не рассмотрены вопросы разграничения доступа, которые особо актуальны для корпоративных ресурсов, к которым могут предъявляться требования сохранения целостности, конфиденциальности или доступности. Применение известных подходов к разграничению доступа, в частности, на основе матрицы доступа вызывает трудности, в связи с отсутствием формального описания существенных свойств ресурсов. Таким образом, задачей данной работы является адаптация способа использования матрицы доступа к применению в неструктурированных текстовых хранилищ.

В соответствии с общепринятым подходом под хранилищем W будем понимать множество документов D_i, представленных набором значений атрибутов A_i. Основной сложностью в выделении групп документов, к которым применимы конкретные функции системы, является

отсутствие определенного атрибута *A*, гарантировано присутствующего у всех $D_i \in W$ и описывающего тип документа. Более того, даже если для данного хранилища возможно выделить такой атрибут, разделение доступа на его основе не будет достаточно гибким, т.к. в дальнейшем набор атрибутов для данного типа может быть изменен.

Например, если до 2008 года документы одного типа имели набор атрибутов A_1^*, а после – A_2^*, то для системы эти документы будут разных типов. С другой стороны, доступ для всех подобных документов будет разрешен пользователям, принадлежащим к одной категории, т.е. для каждого типа придется вводить одинаковые правила доступа, что приведет к избыточности, и, как следствие, к потенциальным проблемам с целостностью.

В данной работе, вместо понятия «тип документа» для неструктурированных текстовых хранилищ предлагается использовать понятие *шаблон документа*, который формально определяется набором атрибутов и их значений. В терминах унифицированных операций подобный шаблон можно записать как пересечение нескольких хранилищ, полученных в результате применения операции выборки. Например, для документов типа *P*, изданных до 2008 г.:

$$W.where(A(\text{“Тип”}) = \text{“P”}) \cap W.where(A(\text{“Год”}) < \text{“2008”}),$$

где *W.where(<условие>)* – операция выборки, фильтрующая документы в зависимости от условия; $\cap$ - операция пересечения хранилищ.

В соответствии с этой формулой может быть определена категория пользователей, которая впоследствии будет использована в строке матрицы доступа.

УДК 681.3:519.62

ЗАЩИЩЕННАЯ ПЕРЕДАЧА ЦИФРОВОЙ ИНФОРМАЦИИ НА ОСНОВЕ МАНИПУЛЯЦИИ БЕЛОГО ШУМА С ОГРАНИЧЕННОЙ ПОЛОСОЙ

С.Б. Приходько, к.т.н., доцент
Национальный университет кораблестроения
sprikhodko@nuos.edu.ua

В последнее время для защиты передаваемой информации предпринимаются попытки использования негармонических несущих сигналов и новых видов манипуляции. Одной из таковых является манипуляция случайного процесса (stochastic process shift keying, SPSK) – метод кодирования цифровой информации, при котором на заданном временном интервале определенный случайный процесс представляет соответствующее значение бита либо комбинацию значений битов. Для реализации SPSK известны подходы, основанные на применении различных математических моделей: уравнений авторегрессии/скользящего среднего, стохастических дифференциальных уравнений (СДУ), симметричных нелинейных преобразований коэффициента эксцесса и асимметрии случайного процесса. Однако все существующие на сегодня подходы с точки зрения защиты информации имеют существенный недостаток, связанный с тем, что информационные случайные несущие для разных значений битов либо их комбинаций имеют разные значения числовых характеристик (например, эксцесса). А это, в свою очередь, ухудшает защищенность информации. Возникает вопрос: нельзя ли улучшить степень защиты за счет того, чтобы информационные случайные несущие для разных значений

битов либо их комбинаций имели близкие значения числовых характеристик? Оказывается это возможно. Цель данной работы состоит в том, чтобы показать эту возможность и предложить соответствующий способ для ее реализации.

Предлагаемый способ основан на применении нелинейных СДУ, с помощью которых формируется информационная несущая в виде белого шума с ограниченной полосой (БШОП). Суть этого способа, который назовем манипуляцией БШОП (band-limited white noise shift keying, BLWNSK), состоит в следующем. Сначала с помощью нелинейного СДУ, через параметры которого вводится информация, формируем случайный процесс (сигнал). Потом этот процесс нормализуем с помощью нелинейного преобразования. И мы получаем нормализованный случайный сигнал (НСС). На основе СДУ для НСС по его ординатам формируем БШОП, который используется в качестве информационной несущей и обеспечивает защиту передачи информации. В данном случае сама операция преобразования НСС в белый шум является обратимой, то есть из белого шума можно получить НСС. Далее для передачи в канале связи используем квадратурную амплитудную модуляцию. Полученный сигнал подвергаем обратным преобразованиям. Сначала из принятого сигнала восстанавливаем БШОП. Затем по ординатам БШОП на основе СДУ для НСС получаем этот сигнал. И наконец, по НСС оцениваем параметры СДУ, через которые вводилась информация. Оценку параметров осуществляем либо с помощью корреляционного приемника, либо обобщенным методом моментов.

В качестве примера реализации предложенного способа рассмотрено нелинейное СДУ 2-го порядка, два параметра которого используются для ввода информации. Построение СДУ для НСС осуществляется предложенным ранее автором методом.

УДК 681.32

ВИБІР ТЕХНОЛОГІЙ ЗАХИСТУ ДАНИХ В КАНАЛАХ ЗВ'ЯЗКУ

В.А. Золотарьов, к.т.н., доцент
Харківський національний університет радіоелектроніки
V.Zolotaryov@gmail.com

Побудова захищеної відкритої мережі – багатопараметричне завдання. При його розв’язанні обирається технологія передачі даних і обґрунтовуються захищені способи передачі даних відкритими каналами зв’язку. Для оптимального вибору технології обміну даними слід враховувати телекомунікаційні ресурси, які перебувають у розпорядженні замовника; фінансові кошти, які можуть бути виділені під відповідну телекомунікаційну інфраструктуру; обмеження, які продиктовані міркуваннями безпеки інформації; специфіка інформації, що передається. В докладе запропоновані критерії якими слід керуватися при виборі захищених технологій, а також типові умови, виходячи з яких обирається технологія захисту.

Перший варіант - захищена відкрита мережа на лінійних шифраторах. Створюється на базі ненадійного програмного забезпечення для обміну значними обсягами інформації високого рівня критичності. В такому випадку найраціональніше використовувати технологію шифрування на фізичному рівні (лінійних шифраторів). Взаємодія кожної пари територіально віддалених об’єктів здійснюється по виділеному фізичному каналу, закритому парою таких шифраторів. Для мережі повної зв’язності

об’єктів кількість шифраторів пропорційна кількості каналів, які використовуються.

Варіант другий – відкрита мережа на базі криптомаршрутизаторів. Створюється відносно велика мережа з великою кількістю користувачів і нерегулярними інформаційними потоками. Об’єднана мережа будується на базі неперевірених програм, а обробка інформації виконується засобами універсальних обчислювальних платформ. Для розглянутих умов найраціональніше рішення – технології віртуальних корпоративних мереж (на канальному або мережевому рівні, в залежності від того, які технічні засоби та які протоколи використовуються для організації об’єднаної мережі). При цьому на кожну локально-обчислювальну мережу можна використовувати один криптомаршрутизатор, не залежно від кількості об’єктів, які спряжені в мережі.

Варіант третій - абонентське шифрування на транспортному рівні. У розпорядженні організації є абонентські пункти та програми з достатнім рівнем надійності. Крім того, для зазначених абонентських пунктів можуть бути виконані технологічні обмеження, які включають розміщення на ПК закладних пристроїв і знижують вплив людського фактору (у більшості варіантів ці ПК повинні відноситися до функціонально-замкнених автоматичних робочих місць (АРМ)).

Варіант четвертий - абонентське шифрування на прикладному рівні. Застосовується тоді, коли організація потребує епізодичний обмін критичною інформацією незначного обсягу високого рівня критичності. Обмін організується на базі існуючої відкритої телекомунікаційної мережі організації. Для ПК у захищеній мережі використовуються лише сертифіковані програми, які дозволяють зашифрувати повідомлення та розмістити їх на захищені носії.

УДК 004.056:681.3.06

СТРАТЕГИЯ ЗАЩИТЫ ВИРТУАЛЬНЫХ ИНФОРМАЦИОННЫХ СТРУКТУР

И. Б. Трегубенко[1], к.т.н.,
О. В. Коваль[2], ст. преподаватель
Черкасский государственный технологический университет
[1]irttri@rambler.ru, [2]ovk655@mail.ru

Вредоносное программное обеспечение, использующее виртуализацию, может в ближайшем будущем являться угрозой не только для организаций, но и для конечных пользователей. Поэтому при использовании виртуализации необходимо грамотно спланировать стратегию защиты виртуальной инфраструктуры.

Все виртуальные системы, к которым может быть осуществлен доступ, не должны быть неуправляемыми и должны поддерживаться в соответствии с корпоративными стандартами безопасности. Необходимо организовать жесткий контроль над развертыванием виртуальных машин на серверах компании и не позволять уязвимой системе работать в ее сети.

Защиту необходимо поддерживать не только внутри самой виртуально машины, но также нужно защищать образы виртуальных систем. Часто системные администраторы уделяют большое внимание защите файлов внутри гостевой системы, однако забывают о защите файлов сервера виртуализации. В свете того, что существуют переносные винчестеры большой емкости, злоумышленник может записать на него всю виртуальную инфраструктуру с множеством связанных виртуальных машин и работать с ней уже в домашних условиях.

Необходимо использовать специализированные решения для защиты серверов виртуализации. В пределах серверов виртуализации можно использовать системы обнаружения или предотвращения вторжений (Intrusion Detection/Prevention Systems, IDS/IPS). Работа этих систем зачастую завязана на физическое расположение компьютеров, что усложняет работу по защите виртуальной инфраструктуры ввиду легкой переносимости виртуальных машин на другое оборудование.

Для распространения конфиденциальной информации в виртуальных машинах необходимо использовать специализированные защищенные платформы виртуализации, например продукт VMware ACE, который позволяют шифровать содержимое дисков виртуальных машин, защищая их паролем, и применять к ним различные политики безопасности.

Виртуальные машины, сами по себе могут использоваться для обеспечения безопасности, для изоляции критически важных систем друг от друга. Однако виртуальную систему достаточно легко развернуть на подходящей платформе. Это требует повышенного контроля, так как вовремя не обновленные системы могут являться точкой проникновения злоумышленников во внутреннюю сеть компании. Нельзя забывать и о внутренних угрозах, необходимо правильно разграничивать права доступа персонала к информационным ресурсам, содержащимся в виртуальных системах. В больших масштабах необходимо использовать специализированное программное обеспечение для контроля над сетевой инфраструктурой и средства обнаружения вторжений, что на данном этапе не достаточно наработаны. Проблемы автоматизации роботы специалиста по безопасности, в том числе в виртуальных средах, остается актуальной задачей.

УДК 681.32

АНАЛИЗ ИЗВЕСТНЫХ МЕТОДОВ ПОСТРОЕНИЯ ШИФРОСИСТЕМ ДОКАЗУЕМОЙ СТОЙКОСТИ, ОБОСНОВАНИЕ КРИТЕРИЕВ И ПОКАЗАТЕЛЕЙ ИХ ЭФФЕКТИВНОСТИ

Б.П. Томашевский, н.с.
Академия сухопутных войск
oficer2007@ukr.net

Мощным механизмом обеспечения требуемой достоверности являются методы помехоустойчивого кодирования.

Для обеспечения конфиденциальности информации традиционно используют криптографические механизмы защиты информации. Особое место занимают симметричные и несимметричные ТКС, которые строятся с использованием алгебраических блоковых кодов и позволяют совместить помехоустойчивое кодирование и защиту информации для интегрированного решения задач обеспечения требуемой достоверности и конфиденциальности передачи данных в КСиС.

Проведенные исследования показали, что применение методов помехоустойчивого кодирования позволяет получить требуемые показатели достоверности, но при этом, внесенная избыточность приводит к значительному уменьшению показателя конфиденциальности. Таким образом, возникает задача поиска интегрированных механизмов (одним приемом) обеспечения требуемых показателей и достоверности и конфиденциальности. Для решения возникшей задачи используются теоретико-кодовые схемы.

Среди асимметричных ТКС особое место занимает схема Нидеррайтера, которая позволяет при равных условиях со схемой Мак Элиса обеспечить максимальную относительную скорость кодирования (близкую к единице). Тем самым, интегрировано обеспечить требуемые показатели конфиденциальности, достоверности и оперативности.

Для ее построения используются проверочная матрица с полиномиальной сложностью декодирования и матрицы маскировки X, P и D.

Открытым ключом в криптосистеме Нидеррайтера является матрица H_X, секретным (закрытым) ключом являются матрицы маскировки – X, P, D. Закрытая информация (кодограмма) представляет собой синдром и вычисляется по правилу $S_X = e \cdot H_X^T$, где вектор e – вектор длины n и веса $\leq t$, который несет конфиденциальную информацию (информационное сообщение, подлежащее закрытию).

Вместе с тем, использование данной схемы возможно только на двоичных кодах, т.к. при формировании кодограммы используется процедура равновесного кодирования, позволяющая преобразовать информационную последовательность в вектор ошибки длиной n, что существенно сужает область применения длинных помехоустойчивых кодов в данной схеме.

Таким образом, перспективным направлением дальнейшего развития схемы Нидеррайтера является разработка процедуры равновесного кодирования для m-ичных кодов, что позволит, применяя в данной схеме АГК, обеспечить повышение показателей достоверности и конфиденциальности.

УДК 004.031.42

ПІДХІД ДО РОЗМЕЖУВАННЯ ПРАВ ДОСТУПУ В СИСТЕМІ ЕКСПЕРТНОЇ ОЦІНКИ МАТЕРІАЛІВ ДИСТАНЦІЙНИХ КУРСІВ

М.П. Боцула[1], к.т.н., доцент,
І.А. Моргун[2], аспірант
Вінницький національний технічний університет
[1]botsual@gmail.com, [2]proftua@gmail.com

З розповсюдженням навчального матеріалу в глобальній мережі Інтернет постає задача розмежування прав і ролей доступу до курсів дистанційних систем навчання. Серед безлічі відомих моделей розмежування прав DAC, MAC, RBAC і існуючих підходів авторизації в глобальній мережі Інтернет OpenID, OAuth найбільш популярним і найчастіше вживаним залишається метод авторизації по імені користувача (логіну) і паролю, так звана однофакторна аутинфікація. В тезах наводиться приклад реалізації методу аворизації по логіну і паролю із використанням технологій REST і веб-фреймворків програмування ExtJS, Django.

В запропонованій авторами моделі оцінки матеріалів дистанційних курсів існує три ролі користувачів — "Автор", "Експерт" і "Студент". Кожна із ролей має свої права на редагування, перегляд, оцінку матеріалу певного дистанційного курсу.

"Студент" має право на перегляд матеріалу, виставлення оцінки за певними запропонованими критеріями. "Автор" має право на створення, редагування, перегляд курсу, перегляд оцінок свого курсу. "Експерт" має право на перегляд курсу, перегляд оцінок певного

курсу і виставлення результуючої оцінки матеріалу на базі оцінок від користувачів групи "Студент" і власної оцінки.

Використаний підхід авторизації базується на клієнт-серверній технології. Клієнт використовує звичайний веб-браузер для доступу к сторінці з вводом логіну і паролю. Далі користувач вводить свої реєстраційні данні і відсилає їх на сервер для перевірки. Пересилка даних від веб-браузера користувача до сервера відбувається по технології AJAX. Обробник на серверній стороні, закріплений за певною адресою і реагуючий на команди передані по протоколу HTTP, методом GET, перевіряє надіслані дані. Обробка на сервері відбувається на базі технології REST і веб-фреймворку Django.

Після вдалої авторизації користувача створюється сесійний ключ і надається доступ до привілегійованної сторінки відповідно із його правами доступу. Якщо при авторизація були введені не вірні логін і пароль – користувачу надається можливість повторно вести свої данні.

Використаний підхід авторизації користувачів в системі експертної оцінки матеріалів дистанційних курсів дистанційного навчання надає можливість легко і гнучко представляти доступ до привілегійованих веб-сторінок для користувачів на базі їх ролей і прав. При розробці були використаний клієнт-серверний підхід і open-source технології: ExtJS, REST, Django. Успішно здійснено практичну апробацію підходу у Центрі дистанційної освіти Вінницького національного технічного університету.

УДК 004.056.57:656.2

ПОИСК НЕЛИНЕЙНОЙ ФУНКЦИИ ДЛЯ НЕЛИНЕЙНЫХ УЗЛОВ ЗАМЕН АЛГОРИТМОВ ПОТОЧНОГО ШИФРОВАНИЯ

С.И. Приходько, к.т.н., доцент,
Г.С. Цымбал, аспирант
Украинская государственная академия железнодорожного транспорта
galina.tsymbal@yahoo.com

Выбор нелинейной функции для нелинейных узлов замен (НУЗ) алгоритмов поточного шифрования является открытой и актуальной задачей. В последних исследованиях основное внимание уделяется формированию НУЗ на основе сильно нелинейных булевых функций, так же именуемых как бент-функции.

На основе требования к функциям-кандидатам для формирования НУЗ можно сформировать основную систему неравенств, основываясь на критических требования:

$$\begin{cases} N_s = \min\{d(S,\varphi)\} \geq N_{smm} \\ AC(f) = \max_{s\neq 0}\left|\sum_{ч} \hat{f}(x)\,\hat{f}(x\oplus s)\right| = \max_{s\neq 0}\left|\hat{r}(s)\right| \leq AC_{mp} \end{cases}, \quad (1)$$

где N_{smm} – необходимое значение нелинейности, AC_{mp} – необходимое значение автокорреляции.

Так же основываясь на некритичных условиях сформируем дополнительную систему ограничений:

$$\begin{cases} C_б \geq C_{бmp} \\ KI(k) \geq KI_{mp}(k) \\ KP_f(k) \geq KP_{mp}(k) \\ M_f \leq M_{fmm} \\ \deg(f) \geq \deg(f)_{mp} \end{cases}, \quad (2)$$

где $C_{бтр}$ – необходимое значение сбалансированности, $KI_{тр}(k)$ – необходимое значение корреляционного иммунитета, $KP_{тр}(k)$ – необходимое значение критерия распространения, M_f – вычислительная сложность, $M_{fтт}$ – необходимое значение вычислительной сложности, deg(f) - алгебраическая степень, deg(f)$_{тр}$ - требуемое значение алгебраической степени.

Пусть имеется (n, m, t) - эластичная функция. Доказано что, если F–(n, m, t) - эластичная функция, а G-подстановка на V_m, нелинейность которой равна N_g, то P=GoF - это (n, m, t) - эластичная функция, обладающая следующими параметрами:

1. Нелинейность P удовлетворяет соотношению:

$$N_p \geq 2^{n-1} - 2^{n-\frac{1}{2}m}.$$

2. Алгебраическая степень P равна m–1.

Заметим также, что (n, m, t)-эластичная функция дает 2^m-1 различных сбалансированных корреляционно-иммунных порядка t функций на V_n.

Можно предположить, что выбирая, подстановку G с заданными параметрами частично удовлетворяющим ограничениям (1) и (2), то можно получить P- эластичную функцию, которая порождает 2^m-1 различных сбалансированных корреляционно-иммунных порядка t функций на V_n. Из порожденных функций выбираем ту, что удовлетворяет ограничениям (1) и (2).

Таким образом, данный способ позволяет получить функцию, которая будет пригодной для формирования НУЗ алгоритмов поточного шифрования.

УДК 629.381

ДИНАМИЧЕСКОЕ УПРАВЛЕНИЕ ПРОЦЕССОМ МАРШРУТИЗАЦИИ ДАННЫХ В ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ

А.А. Смирнов, к.т.н., доцент, В.В. Босько
Кировоградский национальный технический университет

Обеспечение требуемых вероятностно-временных характеристик современных компьютерных систем и сетей возможно на основе комплексного подхода к управлению сетевыми ресурсами с использованием современных методов и алгоритмов маршрутизации данных. В условиях высокой интенсивности входных потоков информации наиболее перспективным направлением представляется разработка методов динамического управления процессом маршрутизации данных в телекоммуникационной сети.

В докладе представлены результаты, полученные в ходе математического моделирования процесса маршрутизации в телекоммуникационной сети (ТКС), проведена оценка эффективности разработанного метода в сравнении с известными подходами (построенными на принципах однопутевой и многопутевой маршрутизации и статического управления в многопротокольных узлах связи) с квитированием и без него.

Показано, что использование разработанного метода при высокой загрузке ТКС позволит до 1,5 раз уменьшить среднее время доставки информационных пакетов в системах передачи данных с квитированием и до 4 раз в системах без квитирования.

Исследовано влияние времени мониторинга телекоммуникационной сети на точность прогнозирования поведения трафика. Показано, что одним из способов определения точности прогноза поведения трафика является вычисление энтропии распределения эмпирических вероятностей переходов с уровня на уровень квантования, характеризующих поведение трафика.

На основе полученных в результате исследования результатов подтверждена гипотеза о целесообразности управления сетевыми ресурсами (регулирования информационных потоков) с периодичностью T = 2 ...5 с.

В соответствии с результатами сравнительного анализа современных технологий в ТКС, а также проведенной оценкой разработаны рекомендации по практическому применению предложенного метода. Показано, что использование возможностей современных методов адаптивного сжатия и кодирования (например, MPEG-4), уменьшения психовизуальной избыточности, управления параметрами передачи цифровой информации (протоколы RTP, UDP), адаптивной маршрутизации и механизмов их взаимодействия позволит обеспечить передачу информации с требуемыми показателями качества.

Проведенное имитационное моделирование подтвердило достоверность разработанной математической модели ТКС и как следствие сделанных на основе ее анализа выводов и рекомендаций. Это подтверждается в частности тем, что «расчетная» кривая зависимости среднего времени доставки информационных пакетов от интенсивности потока информации уверено попадает в «усредненный» доверительный интервал, соответствующий доверительной вероятности 0,95, аналогичной экспериментальной зависимости.

УДК 681.3:31

НЕПЕРЕРВНІСТЬ ДОКУМЕНТООБІГУ З ВИКОРИСТАННЯМ МАРКЕРУ ДОСТУПУ

А.О. Поляков, к.т.н., І. Юрченко, студент,
Харківський національний технічний університет
Polyakov.Andrey@gmail.com

За останні роки системи документообігу набули стрімкого розвитку. Вони складають специфічний розділ інформаційної безпеки аналізу та синтезу систем захищеного документообігу. В свою чергу в таких системах сформувалась проблема неперервності, яка складається у наступному: сутності (документи), що породжуються та обробляються системою, повинні зберігати позначку безпеки при будь-якому перетворенні їхнього вигляду.

У наш час під позначкою безпеки прийнято розуміти електронний цифровий підпис (ЕЦП). Законом України про ЕЦП встановлено, що цифровий підпис в електронному документі вважається юридично рівнозначним чорнильному підпису в документі на паперовому носії при одночасному виконанні необхідних умов. Наявність таких умов показує, що юридична сутність чорнильного підпису на паперовому документі і ЕЦП електронного документу рівнозначні далеко не завжди, що створює певні труднощі при переході від паперового документа до електронного і навпаки.

Вимоги до позначки безпеки паперового документу повинні бути наступні:

– позначка повинна бути нерозривно пов'язана з трьома сутностями: з автором документу, з вмістом документу та з його основою (папером).

– повинна бути позначка, що перевіряється, тобто мати можливість здійснити перевірку незмінності змісту.

Для паперових документів на сьогоднішній момент існує ряд позначок, які звуться штрих-кодом (баркодом). Існують два типи штрих-кодів:

– лінійні;
– двовимірні.

Лінійні штрих-коди читаються в одному напрямку (по горизонталі). Застосовуються для ідентифікації документу (наприклад, поштові відправлення, одиниці зберігання, частини для складення, і т.п.). Такі штрих-коди дозволяють кодувати невеликі обсяги інформації (до 20-30 символів, зазвичай цифр).

Двовимірні штрих-коди (2D) є двомірними матричними штрих-кодами, які призначені для кодування тексту або даних бінарного типу. Такі штрих-коди дозволяють кодувати дані обсягом до 3 Кбайт. Серед найбільш відомих 2D штрих-кодів штрих-код Data Matrix в даний час є найбільш ефективним, так як він вже стандартизований і має найбільшу ємність кодування даних.

Для збереження цілісності електронний документ засвідчується цифровим підписом (ЦП), після чого електронний документ кодується в 2D штрих-код при цьому використовується код виправлення помилок Ріда-Соломона. Після чого друкований документ доповнюється отриманим штрих-кодом.

Перевірка ЦП друкованого документа виконується в два етапи. На початку, зчитується і розпізнається штрих-код і здійснюється корекція помилок. Після чого виділяються електронний документ та його ЦП, а потім здійснюється перевірка ЦП. Таким чином. використовуючи штрих-код DataMatrix, можна вирішити проблему безперервності документообігу.

УДК 519.711(045)

МАТРИЧНЕ ШИФРУВАННЯ ДАНИХ З МОДИФІКАЦІЄЮ СЕКРЕТНОГО КЛЮЧА

Д.А. Стеценко, м.н.с.
Національний авіаційний університет
stetsenkoda@ukr.net

Як відомо будь-який алгоритм шифрування будується на основі так званих примітивів, простих криптографічних перетворень, вірно підібрана послідовність та сукупність яких забезпечує криптографічну стійкість алгоритму шифрування. Тому є актуальним створення нових та вдосконалення старих криптографічних примітивів. Пропонується алгоритм матричного шифрування даних з використанням матриць, які відповідають за модифікацію матриць зашифрування та розшифрування. В якості матриць зашифрування пропонується використовувати (0,1)- матриці n-го порядку, які породжуються складовими перетвореннями Грея, оскільки матриці даного типу є гарантовано невиродженими и для них існують досить прості методи знаходження матриці оберненої до даної.

Якщо *X*, *Y* – двійкові вектори, що представляють відповідно відкриті та зашифровані дані, а $MK = M^k$ - матриця зашифрування, то шифрування задається рівнянням $Y = X \otimes MK$, де $\otimes$ - оператор матричного добутку по mod 2. Розшифрування здійснюється відповідно за допомогою матриці розшифрування $\overline{MK} = M^{-k}$ за правилом $X = Y \otimes \overline{MK}$. В цьому випадку секретним ключем будуть виступати три параметри: складовий код

Грея (СКГ), який породжує матрицю *M*, *n* – порядок матриці та число *k*.

Для поліпшення якості шифрування пропонується застосовувати матриці модифікації, які будуть використовуватись для зміни матриць зашифрування та розшифрування на кожному кроці зашифрування чи розшифрування даних відповідно. В якості матриці, яка відповідає за модифікацію матриці зашифрування MK, будемо використовувати матрицю *MZ*, яка формується шляхом піднесення матриці *M* до випадкового степеня *z*: $MZ = M^Z$. Після зашифрування кожного вхідного блоку даних, матриця *MK* змінюється за такою формулою: $MK = MK \otimes MZ$. В свою чергу матриця $\overline{MZ} = \overline{M}^Z$ (обернена до матриці *MZ*), що відповідає за модифікацію матриці розшифрування $\overline{MK}$, формується підчас процесу зашифрування та прикріплюється до шифрограми. Для запобігання потенційних слабкостей алгоритму, матрицю $\overline{MZ}$ пропонується прикріплювати до шифрограми в зашифрованому вигляді. Матриця $\overline{MZ}$ зашифровується базовою матрицею зашифрування *MK*, тим самим формуючи матрицю $C = \overline{MZ} \otimes MK$, яка і прикріплюється до шифрограми. При розшифруванні з шифрограми зчитується матриця *C* та знаходиться матриця $\overline{MZ} = C \otimes \overline{MK}$. Відповідно до процесу зашифрування, матриця $\overline{MK}$ на кожному етапі розшифрування змінюється за формулою: $\overline{MK} = \overline{MK} \otimes \overline{MZ}$.

УДК 004.65.3

ИСПОЛЬЗОВАНИЕ ЧАСТОТНЫХ ХАРАКТЕРИСТИК ЯЗЫКА ПРИ ЭКСПЛУАТАЦИИ SQL ИНЪЕКЦИЙ

А.В. Оводенко[1], к.т.н., доцент,
С.А. Клюев[2], бакалавр
Донецкий национальный технический университет
[1]ovoda@i.ua, [2]sergeykl@ukr.net

SQL инъекции (SQL injection) - это класс ошибок основанный на внедрении в запрос произвольного SQL кода.

Ошибки данного класса, на сегодняшний момент, являются одними из наиболее распространенных ошибок ведущих к утечкам информации.

Принцип данной атаки основан на недостаточной фильтрации входных данных, хотя были отмечены и ошибки в самих СУБД, которые вели к возможности выполнения произвольных запросов.

В общем случае проведение атаки сводится к следующему алгоритму:

Найти уязвимый модуль.

Выяснить модель и версию СУБД.

Выяснить вид запроса для эксплуатации уязвимости.

Провести эксплуатацию уязвимости.

Классические SQL инъекции подразумевают возможность вывода информации или вывода сообщений об ошибке.

Если вывод информации или сообщений об ошибке не происходит по причинам фильтрации выводимых

сообщений либо иным причинам, то классические SQL – инъекции становятся бесполезными.

Blind SQL injection – это класс уязвимостей при которых не происходит вывод данных из БД в прямом виде, но при этом запрос к базе данных выполняется и это влияет на работу всей системы [1]. При атаке данного рода уязвимая система обычно возвращает два состояния работы в зависимости от сформированного запроса “правда” или “ложь”, что является достаточным условием для успешной эксплуатации уязвимости.

Атака Blind SQL injection является достаточно «тяжелой» и затянутой по времени атакой и, несмотря на то, что существует большое количество алгоритмов и методик оптимизации запросов и сокращения времени перебора, в основном, они специфичны для каждой конкретной СУБД. Использование частотных характеристик конкретного языка даёт возможность сократить время перебора и количество запросов необходимых для эксплуатации уязвимости путем оптимизации запросов под символы с наибольшей вероятностью появления и используя фонетические особенности языка. Для получения статистических данных было обработано 986971956 слов английского языка. На основании этих данных были построены статистические таблицы, которые могут быть использованы для оптимизации алгоритмов перебора.

УДК 004.35

АКУСТИЧНИЙ КАНАЛ ВИТОКУ ІНФОРМАЦІЇ З ПЕРСОНАЛЬНИХ КОМП'ЮТЕРІВ

Б.Д. Будз, асистент
Національний університет "Львівська політехніка"
budz_lviv_ua@ukr.net

Під час циркулювання інформації в персональному комп'ютері, від моменту її вводу і до моменту передавання чи запам'ятовування, вона піддається трансформації і різноманітним видозмінам. Оскільки оброблення інформації здійснюється технічними засобами, утворюються технічні канали, через які можливий її витік, що може призвести до порушення її конфіденційності.

Як джерело витоку можуть бути тракти в яких безпосередньо приймають участь в оброблені і передаванні конфіденційних даних, так і апаратні засоби, які не приймають безпосередньої участі. На цей час цей ефект можна побачити через паразитні наведення і завдяки реалізації програмних закладок. Паразитні наведення розглянуті досить детально, розвитку програмних закладок сприяє використання стаціонарних комп'ютерів в усіх сферах економіки, як правило виконаних в незахищеному виконанні і не сертифікованих.

Принцип роботи програмних закладок базується на властивості апаратних засобів створювати паразитні випромінювання завдяки програмним звертанням до них. Зокрема це можуть бути електромагнітні, акустичні, вібраційні чи візуальні.

Електромагнітний технічний канал витоку інформації відомий давно. В останній час дослідники активно демонструють можливості акустичного каналу, який

несправедливо вважають безпечним і беруть до уваги лише тоді, коли циркулює мовна інформація. Одним з способів використання акустичного каналу для перехоплення конфіденційної інформації є розпізнавання натиснення клавіш, кожна з яких має унікальний "акустичний слід". Почути натиснення можна або через телефонну трубку (під час розмови) або через закладні пристрої. Крім того центральний процесор також може бути джерелом акустичного каналу, оскільки під час переходу в режим очікування видає характерний звук.

Оскільки при натисненні клавіші утворюється не лише звук а й вібрація, яка може розповсюджуватись на предмети які стоять поруч з робочою станцією, можливість перехоплення даних суттєво розширюється.

Перехопити інформацію з розглянутих вище каналів на великих відстанях можна оптико-електронним перетворювачем, наприклад лазерним мікрофоном. Цим пристроєм можна перехоплювати акустичні звуки які модулюються віконним склом, або які модулюються об’єктами, які стоять поруч і є джерелом вібрації так як і скло.

Отже, використання незахищених комп’ютерів для оброблення конфіденційної інформації може призвести до втрати конфіденційності, якщо не приймати міри щодо запобіганню витоку. Використанню технічних каналів як, деколи єдиний, канал витоку інформації сприяє загальнодоступність портативного вимірювального обладнання і незайнятість висококваліфікованих спеціалістів з технічною спеціальністю. Розроблення ефективних засобів протидії витоку через електромагнітний канал штовхає зловмисників шукати інші технічні канали для отримання конфіденційних даних. Використання акустичного каналу є також небезпечним, що потребує застосування додаткових мір захисту.

УДК 621.396; 004.942

ВИБРАНІ АСПЕКТИ БЕЗПЕКИ ТА МОДЕЛЮВАННЯ БЕЗПРОВІДНИХ СЕНСОРНИХ МЕРЕЖ

В.М. Карпінський
Тернопільський національний технічний університет
vkarpinskyi@gmail.com

В безпровідних сенсорних мережах (БСМ) можуть виникати нештатні режими роботи, зумовлені різного типу зловмисними діями. Тому актуальною є розробка заходів протидії наявним атакам та моделювання їх ефективності.

Запобігання деяким атакам на БСМ вбачається у:

1) для зовнішніх атак та атак на канальному рівні – застосуванні звичайного шифрування та автентифікації, використовуючи спільний ключ проти більшості зовнішніх атак на протоколи маршрутизації БСМ. До основних видів атак, які не враховуються при методах шифрування на канальному рівні та автентифікації, належать атаки червоточини (Wormhole), що зводяться для створення просторово-часового тунелю, та атаки типу лавина чи “флуд” (HELLO Flood). Методи захисту на канальному рівні, котрі використовують спільний ключ, загалом неефективні за наявності атак інсайдерів або компрометуючих вузлів.

2) для атак багатократної ідентичності (Sybil Attack) – а) традиційному застосуванні асиметричної криптографії, проте генерування та верифікація цифрових підписів знаходиться поза можливістю сенсорних вузлів; б) поділяння кожним вузлом унікального симетричного ключа з довіреною базовою станцією – єдиний вихід.

3) для атак типу лавина HELLO – перевірці

двонаправленості зв’язку перед застосуванням відчутніших заходів, заснованих на отриманому за допомогою цього з’єднання повідомлення – найпростіший захист. Протоколу перевірки ідентичності достатньо для запобігання атакам типу лавини HELLO.

4) для атак типів червоточина та воронкова (Sinkhole) – ретельне запроектування протоколів маршрутизації, в яких червоточинна та воронкова атаки виявились би неефективними. Це обґрунтовується тим, що від червоточинної та воронкової атак дуже важко захиститись, особливо, якщо вони поєднуються.

5) для вибіркової переадресації (Selective Forwarding) – а) використанні багатошляхової маршрутизації, б) застосуванні багатьох переплетених шляхів.

6) автентифікація широкотрансльованих повідомлень (Broadcast) і перевантаження (Flooding) – обґрунтовується тим, що за наявності довірених базових станцій зловмисники не будуть здатні широкотранслювати повідомлення та перевантажити ними з будь-якої базової станції. Автентифікація широкотрансльованих повідомлень також корисна для локалізованих взаємодій вузла.

7) використанні метаданих, якщо розмір мережі обмежений або топологія збудована чи контрольована належним чином – тоді метадані (глобальні знання) можуть бути перевагою в підходах щодо захисту, враховуючи, що істотний виклик в забезпеченні захисту великих сенсорних мереж вносить їхня притаманна однорідна організація, децентралізована структура. Використовуючи цю інформацію, базова станція може відтворити топологію всієї мережі. Радикальні або підозрілі зміни в топології могли б вказати на компрометацію вузла, завдяки чому була б ужита відповідна протидія.

УДК 629.735

МЕТОД ОЦЕНИВАНИЯ ФУНКЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ ИНФОРМАЦИОННО-УПРАВЛЯЮЩИХ СИСТЕМ БОРТОВОЙ АВИОНИКИ

В.С. Похил, аспирант
Военный институт телекоммуникаций и информатизации НТУ Украины «КПИ»
v.pohyl@gmail.com

Результаты анализа данных об авиапроисшествиях свидетельствуют о значительном ухудшении состояния безопасности полетов, а анализ причин возникновения событий и инцидентов в гражданской авиации свидетельствуют о том, что приблизительно 80% из них произошли по вине экипажей и диспетчеров управляющих воздушным движением летательных аппаратов (ЛА). Это приводит к тому, что разработчики воздушных судов стараются автоматизировать всё большее число функций по управлению самолетом на различных этапах полета, возложив их на бортовые информационно-управляющие системы (БИУС) ЛА. Это, в свою очередь, приводит к повышению их ответственности за функциональную безопасность (ФБ) самолета, усложнению, а следовательно и повышению требований к указанному свойству данных систем. Актуальность работы обусловлена необходимостью создания методологического аппарата анализа и обеспечения ФБ информационно-управляющих систем (ИУС) критического применения на примере БИУС ЛА. Предлагаемый метод анализа и оценивания ФБ содержит следующие этапы:

– на первом этапе определяются все функции выполняемые каждой подсистемой БИУС, связанной с безопасностью ЛА и осуществляется представление их структур в виде графов и матриц связности элементов;

– на втором этапе определяется возможность наступления катастрофического состояния при невыполнении каждой из функций отдельной подсистемой БИУС, путем оценки величины ущерба, который повлечет за собой отказ той или иной функции безопасности ($Ф_Б$);

– на третьем этапе проводится анализ критичности всех функций безопасности, для которых значение нормированного показателя ущерба не равно 0, а также оценка удельной критичности отдельных элементов с позиций ФБ (данная процедура основана на требованиях по проведению анализа критичности отказов элементов сложных систем);

– на четвертом этапе оценивается показатель функциональной безопасности отдельной функциональной подсистемы БИУС, выполняющей одну из $Ф_Б$, который учитывает суммарную удельную критичность всех функций подсистемы БИУС, для полного множества $Ф_Б$ системы, риск, связанный с ФБ, определяемый вероятностью эксплуатационного отказа $Ф_Б$ системы и нормированным в пределах [0, 1] показателем ущерба, возможного при отказе $Ф_Б$).

Определение показателя функциональной безопасности и степени критичности отдельных элементов, ответственных за работоспособность критичной подсистемы необходимо при обеспечении ФБ БИУС ЛА - для определения компонентов, повышению надежности которых необходимо уделить внимание в первую очередь. Кроме того, это позволяет определить перечень возможных способов и средств повышения ФБ данной системы и оценить их эффективность.

УДК 004.7.056.5:336.717.1

АНАЛІЗ ПІДХОДІВ ДО ВИРІШЕННЯ ЗАДАЧІ ЗАХИСТУ ДАНИХ ВІД НЕСАНКЦІОНОВАНОЇ ЗМІНИ В ІНТЕРНЕТ-ПЛАТІЖНИХ СИСТЕМАХ

О.В. Клювак, аспірант
Університет банківської справи Національного банку України (м. Київ)
Oksana_Klyuvak@bigmir.net

Автентичність та конфіденційність є найважливішими функціями захисту даних, які передаються по відкритих каналах. На сьогоднішній час є відомими два підходи до вирішення задачі захисту даних, які передаються по таких каналах, зокрема в електронній комерції, і базуються на виробленні контрольної комбінації: 1) створення MAC – Message Authentification Code – коду аутентифікації повідомлень. Дві сторони, котрі беруть участь в обміні даних (зокрема, для інтернет-платіжної системи – покупець (власник платіжної картки) та продавець (торгова точка)), використовують спільний ключ. Щоб надіслати повідомлення отримувачу, відправник обчислює код аутентифікації повідомлення як функцію повідомлення та ключа. Повідомлення із доданим до нього значення MAC надсилається отримувачу. Отримувач виконує аналогічні обчислення із повідомленням, використовуючи той самий секретний ключ, та отримує своє значення MAC. Обчислене значення MAC порівнюється із значенням MAC, яке надійшло разом із повідомленням); 2) створення MDC – Manipulation Detection Code – коду виявлення маніпуляцій (з даними).

Порівнюючи вищеподані підходи, можна зробити висновок, що підхід на основі MAC потребує для обчислення контрольної комбінації секретного ключа, другий же підхід

цього не потребує. Потенційний зловмисник не може обчислити MAC для довільного, створеного ним повідомлення, але може обчислити MDC, оскільки для цього непотрібно ніяких секретних даних. Тому, MAC може передаватися від відправника до отримувача даних по відкритому каналу, тоді як для передачі MDC необхідний захищений канал (табл. 1).

Таблиця 1 – Порівняльні характеристики підходів до вирішення задачі контролю незмінності масивів даних в інтернет-платіжних системах

Параметр порівняння	**Підхід**	
	Обчислення MAC	**Обчислення MDC**
Перетворення даних, яке використовується	Криптографічне перетворення (функція шифрування).	Одностороння функція, функція необоротного стиснення інформації.
Секретна інформація, яка використовується	Секретний ключ.	Не використовується.
Можливість для третьої сторони обчислити контрольну комбінацію	Зловмисник не може обчислити контрольну комбінацію, якщо йому невідомий секретний ключ.	Зловмисник може обчислити контрольну комбінацію для будь-якого блоку даних.
Зберігання та передача контрольної комбінації	Контрольна комбінація може зберігатися і передаватися разом із захищеним масивом даних.	Контрольна комбінація повинна зберігатися і передаватися окремо від захищеного масиву даних.
Додаткові умови	Потребує попереднього розподілу ключів між учасниками інформаційного обміну.	Не потребує попередніх дій.
Області, в яких підхід має переваги	Захист від несанкціонованих змін даних при їх передачі.	Одноразова передача масиву даних, контроль незмінності файлів даних та програм.

Отже, для передачі даних із використанням MDC необхідний канал, який би забезпечував лише достовірність даних. Відповідно, вимога конфіденційності є відсутньою, а отже, робить цей метод зручним при одноразовій передачі даних. Саме тому, застосування підходу на основі створення коду аутентифікації повідомлень є резонним в електронній комерції, зокрема при розрахунках за допомогою банківських платіжних карток, адже зазвичай покупець використовує свій платіжний засіб неодноразово, а тому забезпечення конфіденційності є необхідною умовою у інтернет-розрахунках.

УДК 681.32

ШВИДКІ КРИПТОГРАФІЧНІ ПЕРЕТВОРЕННЯ НА ОСНОВІ СИСТЕМ АЛГЕБРАЇЧНИХ ПОРІВНЯНЬ

В.А. Лужецький, д.т.н., професор,
М.Л. Гаєвський, магістр з ІБ
Вінницький національний технічний університет

Останнім часом багато вчених відходять від стандартних методів побудови блокових шифрів. Основою багатьох таких методів є використання різних теоретико числових перетворень.

Основна ідея запропонованого способу шифрування полягає у виконанні обчислень з використанням матриці Уолша:

$$\mathbf{C} \equiv (\mathbf{H} \times \mathbf{M}) \bmod \mathrm{m},$$

$$\mathbf{M} \equiv (\mathbf{H} \times \mathbf{C}) \bmod \mathrm{m},$$

де **H** – матриця Уолша порядку N;

M – вектор відкритого повідомлення;

m – модуль;

C – вектор зашифрованого повідомлення.

Вектор відкритого повідомлення **M** складається з блоків даних розрядністю L = var:

$$\mathbf{M} = \{\mathrm{m}_1, \mathrm{m}_2, ..., \mathrm{m}_g\},$$

У запропонованому способі існують два змінних параметри перетворення, які залежать від секретного ключа K: N – розмірність перетворень, яка визначається функцією $f_1(K)$, і n – розрядність даних, яка визначається функцією $f_2(K)$.

$$N = f_1(K)$$

$$n = f_2(K)$$

Розрядність блоку даних L дорівнює добутку розмірності перетворення та розрядності даних.

$$L = N \cdot n$$

Таким чином, розрядність блоку L також змінна величина.

Для забезпечення оптимального рівня крипостійкості та швидкості шифрування даних рекомендується виконувати 12 раундів перетворень. Розшифрування повідомлення виконується в зворотному до зашифрування порядку.

Для визначення змінних параметрів перетворення пропонується використовувати регістр зсуву з лінійним зворотнім зв'язком. Початковий стан регістра представляє собою секретний ключ. Оскільки стандартом AES рекомендується використовувати секретний ключ розміром не менше 128 розрядів, пропонується використовувати такий поліном для побудови лінійного регістра зсуву зі зворотнім зв'язком:

$$f(x) = x^{128} + x^{7} + x^{2} + x + 1$$

Такий генератор випадкових чисел буде мати максимальний період:

$$T = 2^{128} - 1$$

Вихідна послідовність псевдовипадкових чисел ділиться на послідовності по 5 біт, 3 з яких визначають розмірність перетворень, а 2 – розрядність даних. Можливі варіанти розмірності перетворень такі:

2, 4, 8, 16, 32, 64, 128, 256.

Можливі варіанти розрядності даних:

8, 16, 32, 64

Перевагою швидкого перетворення Уолша є те, що його реалізація вимагає тільки операцій додавання і віднімання в кількості $N \cdot \log_2 N$, що забезпечує достатньо високу швидкість шифрування інформації. Отримано оцінку середньої швидкості шифрування (2,4 оп./біт), що свідчить про покращення значення цього критерію порівняно з іншими блоковими шифрами.

УДК 681.3.07

ПРИШВИДШЕННЯ ПРОЦЕСУ ОБЧИСЛЕННЯ ЗНАЧЕНЬ ХЕШ-ФУНКЦІЙ ПОБУДОВАНИХ НА ЕЛІПТИЧНИХ КРИВИХ

В.А. Лужецький, д.т.н., професор,
В.В. Кичак, студент
Вінницький національний технічний університет
vvkychak@gmail.com

Еліптичні криві є найбільш перспективною структурою для побудови криптографічних алгоритмів, що обраховують в один бік, з перебірною складністю алгоритмів. У доповіді розглядається підхід до пришвидшення процесу обчислення значень хеш-функцій побудованих на еліптичних кривих.

Для еліптичної кривої *E(K)* з циклічною групою $\langle Q \rangle$ великого простого порядку *r* функції $h{:}k \rightarrow x_{kP}$, що ставиться у відповідність невід'ємному цілому числу $k<r/2$ координату x_{kP} точки *kP* обраховують в один бік і немає колізій.

Повідомлення *M* розбивається на блоки даних розрядністю *n*:

$$M = \{m_1, m_2, ..., m_L\}.$$

В процесі хешування обчислюється така послідовність хеш-значень h_0, h_1,…, h_{L+1}, де h_0 – початкове (задане) значення хеш-функції, h_{L+1} – остаточне значення хеш-функції для повідомлення *M*.

Проміжні значення хеш-функцій обчислюються за формулою:

$$h_i = (h_i^{'} P) \bmod p, \quad i = 1, 2 ... L+1,$$

де P – точка групи точок еліптичної кривої $E_p(a,b)$;

p – просте число.

$$h_i^{'} = h_{i-1} \oplus m_i .$$

Для множення точки P на число $h_i^{'}$ останнє представляється у двійковому вигляді:

$$h_i^{'} = \sum_{i=0}^{n-1} a_i \cdot 2^i ,$$

тоді добуток $h_i^{'} P \bmod p$ обчислюється за формулою:

$$h_i^{'} \cdot P \bmod p = \left(\sum_{i=0}^{n-1} a_i \cdot (2^i \cdot P) \right) \bmod p.$$

Для пришвидшення обчислень пропонується попередньо розрахувати значення $2^i P$ шляхом подвоєння точки еліптичної кривої і зберігати ці значення в пам'яті. В процесі множення буде здійснюватись додавання тільки тих значень $2^i P$, для яких a_i=1. Порівняно з безпосереднім множенням кількість додавань зменшує в середньому в 3 рази.

Ще більший виграш за кількістю операцій додавання досягається при використанні перетворення двійкового коду з цифрами 0 і 1 у двійковий код з цифрами -1, 0 і 1. В основі такого перетворення лежить властивість $1+2+2^2+\ldots+2^m=2^{m+1}-1$, тобто послідовність з m+1 одиниць, що розташовані поруч заміняються тільки двома одиницями, одна з яких має знак мінус.

Відомо, що таке перетворення двійкового коду забезпечує в середньому 0,33n одиниць в коді (n – розрядного коду). З урахуванням цього виграш за кількістю додавань складає 4,5 рази.

Точка еліптичної кривої – P отримується з точки P заміною координати y на координату $-y$, тому в пам'яті достатньо зберігати тільки значення $2^i P$, а значення $-2^i P$ обчислюються, шляхом інвертування.

УДК 681.3

ХЕШУВАННЯ ДАНИХ З НЕРІВНОМІРНИМ РОЗБИТТЯМ НА БЛОКИ

В.А. Лужецький, д.т.н., професор,
О.В. Філіппов, магістрант
Вінницький національний технічний університет
phil-oleg@ukr.net

Відомі методи хешування, які передбачають розбиття повідомлення (даних) на блоки однакової довжини і виконання певного фіксованого набору арифметичних і логічних операцій над цими блоками даних.

У доповіді розглядається новий підхід до хешування, який принципово відрізняється від усіх відомих методів хешування. Цей підхід полягає в тому, що розбиття початкового повідомлення здійснюється на блоки різної довжини і над кожним з блоків виконується своя специфічна послідовність операцій.

Для реалізації цього підходу пропонується метод хешування, який детально розглядається в доповіді.

Метод хешування:

1. Для поточного значення хеш-функції формуються ознаки розрядності поточного блоку даних і виконуваної операції.

2. Виконуються операції згідно з ознакою типу операції над поточним значенням хеш-функції і поточним блоком даних.

Пункти 1, 2 виконують певну кількість разів, яка визначається виходячи з ознаки розрядності блоку даних і розрядності хеш-значення.

Початкові дані мають вигляд $M = m_0 \| m_1 \| m_2 \| \ldots \| m_{N-1}$, де m_i – поточний блок даних певної розрядності.

У процесі хешування формується така послідовність хеш-значень $h_0, h_1, h_2, \ldots h_N$, де h_0 – початкове значення хеш-функції, h_N - результат хешування початкового повідомлення.

Нехай розрядність процесора $l_{пр}$, тоді початкове і поточні значення хеш-функції розбиваються на підблоки довжиною $l_{пр}$. Кількість таких підблоків дорівнює: $K = L_H / l_{пр}$, де L_H – довжина хеш-значення.

Отже $h_i = h_{i,1} \| h_{i,2} \| \ldots h_{i,k}$, для $i = 0 \div (N-1)$

Ознака виконуваної операції формується як значення функції: $S_O = f(h_{i,k})$

Ознака розрядності блока даних визначається за формулою: $S_P = f^*(h_{i,(k-1)})$

Розрядність поточного блока даних дорівнює $l_i = (S_P + 1) \cdot l_{пр}$,

Поточний блок даних розбивається на підблоки довжини $l_{пр}$, тобто він представляється як конкатенація S_P підблоків $m_i = m_{i,1} \| m_{i,2} \| \ldots \| m_{i,(Sp+1)}$

Згідно з ознакою виконуваної операції здійснюється обчислення $h^{(g)}_{i,l} = h^{(g-1)}_{i,l} \overset{S_O}{\otimes} m_{i,g}$, де $g = 1 \div (S_P + 1)$, $l = 1 \div k$.

Поточне значення хеш-функції h_{i+1} формується як конкатенація результатів обчислень

$$h_{i+1} = h^{(Sp+1)}_{i,1} \| h^{(Sp+1)}_{i,2} \| \ldots \| h^{(Sp+1)}_{i,k}$$

Як операції для хешування пропонується використовувати бінарні операції: логічне додавання (OR), логічне множення (AND), додавання за модулем 2 (XOR), додавання за модулем $2^{l_{пр}}$.

Блок повідомлення m_{N-1} у загальному випадку може мати розрядність, що відрізняється від розрядності, яка визначається ознакою, тому пропонується доповнювати блок до потрібної розрядності кодом числа N і певною кількістю розрядів псевдовипадкової послідовності.

УДК 681.32

GSM-КОНТРОЛЕРИ ДЛЯ СИГНАЛІЗАЦІЇ ТА КЕРУВАННЯ

В.П. Семеренко, к.т.н., доцент,
Джан Янг, студент
Вінницький національний технічний університет
sm@vstu.vinnica.ua

Останнім часом все більшого розповсюдження отримують нові технології для охорони і керування на основі GSM-сигналізації. Вони мають широку сферу використання: від промислових об’єктів і банкоматів до міських квартир і автомобілів.

Принцип дії GSM-сигналізації полягає в отриманні та обробці спеціальним контролером інформації від встановлених на об’єкті давачів і, у випадку появи аварійної ситуації, передачі повідомлення на мобільний телефон користувача. Повідомлення може бути голосовим або у вигляді SMS для одного чи для кількох телефонних номерів. Давачі можуть реагувати на виникнення різних нештатних ситуацій в режимі охорони: рух зловмисника, витік води чи газу, пожежа та ін.

Головним компонентом всієї системи є GSM-контролер. Більшість GSM-контролерів, які випускаються різними фірмами, можна класифікувати на багатофункціональні пристрої та пристрої базового рівня.

Найпростіші контролери базового рівня (GSM 3×5 MINI, GSA-04UM) мають 1-2 входи для підключення вхідних давачів, один вихід, малу кількість телефонних номерів для виклику, настроювання за допомогою готового шаблону.

Багатофункціональні контролери (CCU6225, AT-200) мають вбудований GSM-модем і гнучку програмовану систему контролю. Їх найголовніша перевага – можливість користувачеві за допомогою функцій віддаленого керування самостійно приймати заходи проти порушників або усувати аварійні ситуації. Передбачається можливість періодичного тестування системи для підтримки її в стані високої готовності.

З кожним роком такі системи контролю стають все більш інтелектуальними і є невідємною складовою житла 21 століття – “розумного дому”.

Звичайно, такі пристрої поки що достатньо дорогі і вимагають складного програмування за допомогою комп’ютера. Часто в інженерній практиці або в домашніх умовах виникає потреба в створенні недорогої системи сигналізації, але з набором спеціальних функцій.

Пропонується розробка такої системи GSM-сигналізації на основі контролера S3C2410A фірми Samsung. Цей контролер, який випускається вже більше двох років, розрахований на нижній ціновий діапазон і вже зарекомендував себе як високонадійний пристрій, що має відмінну продуктивність при малому енергоспоживанні.

GSM-контролер на базі S3C2410A може приймати інформацію від багатьох давачів, які можуть об’єднуватися в групи різної конфігурації. Програмування контролера відбувається на основі його власних команд за допомогою комп’ютера або складних SMS.

УДК 681.325

ОБЪЕДИНЕНИЕ КРИПТОГРАФИИ И ПОМЕХОУСТОЙЧИВОГО КОДИРОВАНИЯ

В. П. Семеренко, к.т.н., доцент,
А.Ф. Дубров, студент,
Винницкий национальный технический университет
VPSemerenko@mail.ru

В настоящее время становится актуальной защита информации при передаче ее по компьютерным сетям и каналам передачи данных. В этом случае необходимо решать две задачи: защищать данные от атмосферных помех и возможных неисправностей аппаратуры, а также обеспечивать секретность передаваемой информации.

Объединить методы помехоустойчивого кодирования и криптографии можно при использовании единого математического аппарата – теории линейных последовательностных машин (ЛПМ), на основе которой описываются как циклические коды, так и поточное шифрование. Предлагается и на стороне передатчика и на стороне приемника использовать аппаратную реализацию ЛПМ в виде соответствующих регистров сдвига.

На стороне передатчика кодер в виде $(n-k)$-разрядного регистра сдвига в течение n временных тактов выполняет операцию умножения k-разрядного информационного вектора $I(x)$ на порождающий многочлен $g_k(x)$, а шифратор в виде n-разрядного регистра сдвига с обратными связями выполняет операцию деления n-разрядного кодового вектора $C(x)$ на порождающий многочлен $g_{cr}(x)$. Поскольку разряды

вектора $C(x)$ начинают формироваться на следующем такте после начала поступления вектора $I(x)$, поэтому кодер и шифратор начинают и заканчивают работу практически одновременно, с разницей лишь в один такт.

Задача дешифрирования на стороне приемника основана на том, что в n-управляемой n-разрядной ЛПМ для любых двух известных состояний S_i и S_j существует n-разрядная последовательность $U(t)$, такая что

$$S_j + A^n \times S_i = \left| A^{n-1}B, A^{n-2}B, \ldots, AB, B \right| \times U(t), \quad GF(2), \qquad (1)$$

где A и B – характеристические матрицы ЛПМ.

В (1) состояние S_j является зашифрованным кодовым вектором, состояние S_i является начальным состоянием S_{beg} шифратора, которое является секретным, а приемной стороне передается лишь ключ $A^n \times S_{beg}$. В результате за один такт легко определяется $U(t)$, т.е. восстанавливается исходный кодовый вектор $C(x)$. Далее декодер в виде ($n-k$)-разрядного регистра сдвига с обратными связями в течение n тактов выполняет операцию деления вектора $C(x)$ на порождающий многочлен $g_k(x)$ и восстанавливает исходный вектор $I(x)$. Начальное состояние кодера и декодера принимается нулевым.

Таким образом, на стороне приемника отсутствует устройство дешифрирования, не нужны сведения отдельно о структуре шифратора и его начальном состоянии, нужен лишь ключ, в котором в компактной форме скрыта информация о шифраторе. Важным достоинством предложенной схемы является то, что ошибки в кодовом векторе, вызванные помехами в канале передачи данных, не влияют на задачу дешифрирования.

УДК 004.056.55

МЕТОД БЛОКОВОГО ШИРФРУВАННЯ НА ОСНОВІ ПСЕВДОВИПАДКОВОЇ ПОСЛІДОВНОСТІ КРИПТОПРИМІТИВІВ

В.А. Лужецький, д.т.н., професор,
А.В. Остапенко, аспірант
Вінницький національний технічний університет
asja87@gmail.com

Потреба вирішення проблеми захисту електронної інформації обумовлює актуальність розробки програмних шифрів та перспективи їх розвитку. Пропонується будувати блоковий шифр використовуючи псевдовипадкову (з точки зору криптоаналітика) послідовність криптопримітивів. Ідея цього методу полягає в тому, що перетворення на кожному із раундів складається з елементарних перетворень набір і послідовність виконання яких визначаються ознаками, що формуються з ключової інформації .

Входячи з вищесказаного пропонується модель блокового шифру:

$$\sum=\{\mathbf{M}, \mathbf{K}, \mathbf{F_E}, \mathbf{F_D}, \mathbf{Q}, \mathbf{B}, \mathbf{C}\},$$

де $\mathbf{M}=\{m_i\}$ – множина відкритих повідомлень;

$\mathbf{K}=\{k_i\}$ – множина ключів;

$\mathbf{F_E}=\{F_{Ei}\}$ – множина функцій зашифрування;

$\mathbf{F_D}=\{F_{Di}\}$ – множина функцій розшифрування;

$\mathbf{Q}=\{q_i\}$ – множина ознак;

$\mathbf{B}=\{b_i\}$ – множина базових операцій;

$\mathbf{C}=\{c_i\}$ – множина криптограм.

Запропонована множина **Q**, залежно від ознаки $q \in Q$, на базі використання визначених операцій **B**, буде

визначати певний вигляд функції перетворення *F()* та алгоритму шифрування в цілому.

Виходячи із запропонованої моделі блокового шифру розглянемо метод блокового шифрування який використовує псевдовипадкову послідовність перетворень. Суть даного методу полягає в шифруванні блоків даних змінної довжини шляхом формування ключа шифрування у вигляді множини раундових підключів, виділення з ключової інформації сукупності ознак, які визначають для поточного раунду кількість підблоків та їх розмірність (структура блоку), вид перетворення для їх почергового зашифрування (структура перетворення), побудованого на основі набору базових операцій.

Процес формування ознак передбачає виділення на кожному етапі шифрування із ключової інформації $k \in K$ (поточного раундового підключа k_r) певних видів ознак:

- ознака, що визначає кількість підблоків Q_{pb} (кількість гілок);
- ознака, що визначає розрядність підблоку Q_{rp} (біт);
- ознака, що визначає вид перетворення Q_{vp} (його номер).

Розглянуті види ознак, дозволяють обробляти блоки змінної довжини розрядністю від 16 до 320 біт. Для одного раунду шифрування може бути побудовано 4096 різних модифікацій алгоритмів шифрування. Причому, алгоритм шифрування складається з відомих операцій, але порядок їх застосування та структура оброблюваних ним блоків визначається секретним ключем.

УДК 681.3

ДОСТОВІРНІСТЬ ПРИЙНЯТТЯ РІШЕННЯ В СИСТЕМАХ ЗАХИСТУ ІНФОРМАЦІЇ

О.П. Войтович, к.т.н., доцент
Вінницький національний технічний університет
o_voytovych@mail.ru

Для забезпечення конфіденційності та цілісності інформації, що представлена у вигляді предметів, нанесена на папері або збережена в електронному вигляді і знаходиться на території певного об'єкту застосовують комплексні системи захисту, які включають блоки спостереження, аналізу, прийняття рішень, виконання певних дій, у відповідності до прийнятого рішення.

Зазвичай блок спостереження – це сенсор. Блоки аналізу, прийняття рішень та виконання певних дій найчастіше представлені певною групою осіб або однією особою, тобто надійність такої системи залежить від людського фактору, і є набагато нижчою в порівнянні із такою, в якій усі блоки реалізовані автоматично.

Для реалізації систем аналізу та прийняття рішень, мережа, що утворюється системою сенсорів працює за принципом нейронної мережі. Кожен сенсор системи представлений нейроном віртуальної нейронної мережі, яка і виконує роль аналізатора та системи прийняття рішень.

Сенсор фіксує певний параметр(и) и зберігає поточні дані. У випадку зміни параметру та перевищення ним порогового значення, генерується тривожний сигнал до інших сенсорів, які в цей час можуть знаходитись в пасивному режимі. Сусідні сенсори активуються та генерують відповідний сигнал, передають дані щодо ситуації навколо них.

Параметри виміряні сенсорами використовуються для ухвалення рішень про подію, що відбувається, і лише їх точність забезпечує правильність на всіх рівнях управління, а недостовірність – призводить до прийняття неправильних рішень, що в свою чергу може спричинити значні втрати. В більшості випадків методика визначення необхідної точності вимірювань в різноманітних технічних системах проходять за однієї методикою. Відмінність є лише у способах знаходження тієї чи іншої величини.

В результаті прийняття рішення при наявності похибок вимірювань є повна група несумісних подій: А – система визначила атаку, що відбулася; Б – система не визначає атаки, атаки немає; В – атаки немає, система генерує тривожний сигнал; Г – атака відбулась, система її не визначила.

Ймовірність Р(В) = α визначає величину ризику першого роду (хибної тривоги), а ймовірність Р(Г) = β - величину ризику другого роду (пропущеної атаки). Тоді інструментальна метрологічна достовірність прийняття рішення системою визначається Д = 1 - α - β.

Щоб визначити необхідну точність вимірювання по і-му параметру, необхідно визначити допустиму величину ризику хибної тривоги α або пропущеної атаки β через величини α_i та β_i за цим параметром.

В задачах захисту інформації ризики хибної тривоги та пропущеної атаки оцінюються для таких систем: системи автентифікації (в тому числі біометричної), фільтрація спаму, антивірусні системи, системи виявлення вразливостей, запобігання вторгнень, системи пожежної та охоронної сигналізації.

В даній роботі пропонується методика визначення ризику хибної тривоги α, пропущеної атаки β та достовірності Д, в системах прийняття рішення при технічному захисті інформації.

УДК 621.396

ОЦІНЮВАННЯ ПРОНИКНОЇ ЗДАТНОСТІ АКУСТИЧНИХ СИГНАЛІВ БУДІВЕЛЬНИХ КОНСТРУКЦІЙ

Ю.П. Гульчак, к.т.н., доцент,
Н.Ю. Харитонова, студент
Вінницький національний технічний університет
jurigulchak@rambler.ru

Багато підприємств, фірм, організацій мають орендовані або власні виробничі та офісні приміщення, тому актуальною є проблема визначення характеристик таких приміщень з точки зору інформаційної безпеки, зокрема звукопроникність. Від рівня акустичних сигналів в приміщенні і за його межами залежить можливість зняття інформації та її несанкціонованого використання. Таким чином, під час вибору приміщення для конфіденційних переговорів необхідно приділити увагу конструктивним особливостям даних приміщень з точки зору звукоізоляційних властивостей окремих елементів та матеріалів і особливостей розповсюдження в них віброакустичного сигналу.

Існуючі пристрої і методики оцінки рівня акустичних сигналів вимагають великих затрат і додаткового технічного забезпечення, тому запропоновано спрощену методику визначення затухання акустичних сигналів при проходженні через матеріали конструкцій будівель та пристрій для її реалізації.

Для визначення норм захисту приміщень по акустичному каналу використовується вираз

$$D=L_c - Q - L_з,$$

де D – співвідношення сигнал/завада;

L_c – рівень мовного сигналу;

$L_з$ – рівень завад.

Мета звукопроникності вважається досягнутою, якщо співвідношення сигнал/завада на границі периметру приміщення зменшується до рівня, коли зловмисник не зможе якісно вирішити задачі виявлення і аналізу потрібного сигналу

Запропонована методика вимірювань базується на ідеї порівняння рівнів звукового тиску у кількох точках простору, безпосередньо біля джерела акустичного сигналу і за межами приміщення. Відносний рівень затухання сигналу в децибелах розраховує мікроконтролер і за спеціальним алгоритмом видає інформацію щодо рівня звукоізоляції будівельної конструкції.

Подальший аналіз даних дозволяє створити карту проникності акустичних сигналів в межах периметру виділених об’єктів та в окремих точках зони досяжності зловмисника.

До складу пристрою входять такі базові вузли і блоки: мікрофони, вхідні акустоелектричні перетворювачі, узгоджувальний пристрій (підсилювач), АЦП, мікроконтролер.

В результаті проектування було створено багатоканальний пристрій і з його допомогою проведені виміри в окремих точках елементів будівель. Порівняння із типовими значеннями, поданими в довідковій літературі показало, що рівень похибки є прийнятним і отримані дані дозволяють розробити комплекс заходів по нейтралізації даного каналу витоку інформації шляхом звукоізоляції чи інших додаткових заходів.

УДК 002.001

ОЦІНЮВАННЯ ТА ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В СОЦІОТЕХНІЧНИХ СИСТЕМАХ

А.В. Дудатьєв, к.т.н., доцент,
І.В. Шнайдер, студент
Вінницький національний технічний університет

Сучасне суспільство характеризується постійним зростанням кількості користувачів глобального інформаційного простору. Крім відомих переваг, це нажаль обумовлює інформаційну незахищеність і як наслідок виникнення певних загроз, які впливають на загальний стан як окремого об’єкта так і суспільства в цілому і можуть викликати конфліктний стан. Сучасні конфліктні ситуації характеризуються тим, що у конфліктах беруть участь складні технічні системи. Загальна теорія конфліктів, зокрема, у соціальних, соціотехнічних системах дозволяє сформулювати загальні положення щодо причин їх виникнення, протікання та методів їх вирішення. Формалізація життєвого циклу конфлікту дозволяє вирішити актуальні задачі, а саме: причини виникнення конфлікту, мету сторін, задіяних у конфлікті, компромісні дії, які можуть сприяти вирішенню конфліктної ситуації. Останнім часом актуальними є проведення так званих інформаційних атак або війн. Мета таких заходів у більшості випадків формулюється, як спроба реалізації лідерства на відповідному сегменті ринку, тобто викликана конкуренцією у боротьбі за лідерство або проведенні психологічної атаки, що характерно для сучасного тероризму. У цьому випадку

забезпечення комплексної безпеки зводиться до забезпечення інформаційної безпеки, практична реалізація якої полягає у розв'язку двох задач: безпосереднього захисту своїх інформаційних ресурсів від ймовірного несанкціонованого доступу та отримання певної інформації щодо дій своїх конкурентів з метою упередження можливих несанкціонованих дій і як наслідок зменшення негативних наслідків.

Таким чином, можна констатувати, що проблема аналізу причин виникнення конфліктних ситуацій у соціотехнічних системах та розробка методів щодо їх вирішення є актуальною, оскільки її рішення дозволить забезпечити комплексний інформаційний захист та оптимізувати процеси підготовки та прийняття управлінських рішень та мінімізувати ймовірні ризики.

Розвиток загальної теорії безпеки полягає у створенні узагальнених взаємопов'язаних положень та залежностей між складовими комплексної безпеки, такими як техногенна, економічна, екологічна тощо. Інтегральною характеристикою захищеності об'єкту є політика інформаційної безпеки (ПІБ), яка повинна підтримувати необхідний рівень захищеності у часі, тобто враховувати динамічний характер як небезпек, так і механізмів захисту.

Разом із врахуванням небезпечних, як внутрішніх так і зовнішніх чинників, вхідними параметрами для розробки ефективної ПІБ є певні вказівки та замовлення служби безпеки та її підрозділу інформаційно-аналітичної служби (ІАС). Це повністю об'єктивний процес, оскільки служба безпеки підприємства в більшості випадків є замовником ПІБ. Рішення задачі забезпечення необхідного рівня інформаційної безпеки, формалізується практично у вигляді двох задач. Рішення першої задачі, тобто оцінювання та забезпечення необхідного рівня захищеності забезпечується на етапі проектування системи захисту

інформації (СЗІ). Результатом розв’язку першої задачі є розроблена політика інформаційної безпеки та синтезована, оптимальна за певними показниками система захисту інформації.

Друга задача вирішується на етапі експлуатації СЗІ. Для організації комплексного захисту і ефективної протидії потенційним порушникам або ймовірним конкурентам, прийняття управлінських рішень щодо забезпечення ефективного функціонування об’єкту захисту повинні ґрунтуватися на результатах повного аналізу і оцінювання, існуючих і потенційних загроз. Рішення цієї задачі ускладнюється у зв’язку із суттєвою невизначеністю, яка пов’язана із динамічною природою всіх елементів системи. У зв'язку з цим ІАС повинна забезпечити впорядковане накопичення, науково обґрунтоване узагальнення і аналіз інформації відносно різних напрямів, що впливають на захист конфіденційної інформації, і на цій основі виконання прогнозу подальшого розвитку подій, їх можливий вплив на стійкість і життєспроможність об’єкту захисту. Розв’язок другої задачі виконується у площині організаційного захисту і передбачає цілу низку заходів, таких як організація служби безпеки, інформаційно - аналітичної служби тощо.

Автори запропонували метод для оцінювання та забезпечення необхідного або достатнього рівня забезпечення захисту інформаційних ресурсів з урахуванням можливих конфліктних ситуацій, що можуть виникнути у сучасних соціотехнічних системах.

УДК 004.56

БЕЗПЕКА ПРИВАТНОГО ЖИТТЯ В ГЛОБАЛЬНІЙ МЕРЕЖІ ІНТЕРНЕТ

С.В. Князюк, аспірант
Вінницький національний технічний університет
edu@svk.me

Глобальна мережа Інтернет стала невід'ємною складовою життя сучасної людини. Кожного дня мільйони користувачів звертаються до послуг пошукових систем, шукають своїх друзів та знайомих в соціальних мережах, планують поїздку та прокладають найкоротший шлях за допомогою сервісів Інтернет-карт, або ж листуються між собою з використанням електронної пошти безкоштовних поштових серверів. Засоби Інтернет-серфінгу значно полегшують життя, допомагаючи знайти або ж передати необхідну інформацію з будь-якого куточка планети.

Доступність безкоштовних сервісів та їх широка функціональність захоплює кожного Інтернет користувача, і відвертає увагу від важливості інформації, яку ми лишаємо про себе у тій чи іншій системі. Починаючи з наших реєстраційних даних, які ми свідомо вводимо і закінчуючи приватними матеріалами, які відправляємо своїм близьким знайомим, друзям та родичам, з впевненістю, що крім відправника та одержувача ніхто інший до них доступу не матиме.

Ретельна увага підчас роботи в мережі допоможе зрозуміти скільки важливих даних ми лишаємо про себе. Повна інформація про інтереси та смаки користувача Інтернету, його теперішній стиль життя та наміри, як і інші деталі приватного життя потрапляють у бази даних, які не

мають належного контролю. Можна впевнено сказати, що весь обсяг інформації потрапляє у масиви даних за ініціативи її власника. Головними джерелами являються як соціальні мережі, де ми розміщуємо свої фото та відео, як поштові системи, за допомогою яких ми листуємося зі своїми друзями та колегами, як особисті web-сторінки, де іноді розміщують все що тільки можна про себе та коло своїх знайомих, так і пошукові системи, де ми шукаємо необхідні нам словосполучення. Пошукові запити, які ми вводимо в системах пошуку, описують коли, де, що і як ми збираємось робити чи зробили – все що тільки можна собі уявити. Школярі розповідають про свої захоплення, студенти - про рівень своїх знань, науковці – про вид своєї діяльності та що саме важливе – про напрям думок, шукаючи різні наукові праці, результати досліджень та існуючі патенти. Так безробітні розповідають про свої можливості, освіту та соціальний статус, хворі – про стан свого здоров'я, а злочинці – знищують собі алібі. Якщо вірно скомбінувати інформацію всіх, задіяних служб Інтернету та за певний час - отримаємо загальну картину, яка опише поточні та майбутні дії особи і може принести як негативні так і позитивні наслідки, що вже залежить від тих, хто має доступ до цих даних. Розглянуті статистичні данні пояснять значимість проблеми та стрімкий розвиток. Певні приклади наочно продемонструють як дані збираються, групуються і прикріпляються до тої чи іншої особи. З'ясуємо ким дана інформація може бути використана та звернемо увагу на існуючі факти використання інформації, які привернули увагу.

Таким чином спробуємо зрозуміти як необхідно користуватись мережею та як до неї ставитись після усвідомлення цих проблем. Це однаково важливо, як для звичайних користувачів, так і для працівників спецслужб та дослідників.

УДК 004.56:004.424.47

МАТЕМАТИЧНА МОДЕЛЬ ПСЕВДОНЕДЕТЕРМІНОВАНОГО ХЕШУВАННЯ ТА КРИПТОГРАФІЧНІ ПРИМІТИВИ ДЛЯ ЇЇ РЕАЛІЗАЦІЇ

Ю.В. Баришев, аспірант
Вінницький національний технічний університет
yuriy.baryshev@gmail.com

Відкритість алгоритмів хешування породжує низку проблем, що пов'язані зі сталою послідовністю операцій, що виконуються на кожній ітерації хешування. Однак засекречення цих алгоритмів не може стати адекватним рішенням цих проблем. Це обумовлено низкою факторів, найбільш значущими з яких є такі три: наявність людського фактору в розробці алгоритмів хешування, можливість декомпіляції виконуваних файлів зловмисниками, потреба в доведенні стійкості алгоритмів підприємцям, які їх будуть використовувати. Виходом із ситуації є реалізація концепції псевдонедетермінованого хешування. Дана концепція випливає з автоматного опису процесу хешування.

Відомо, що недетермінований автомат описується п'ятіркою $\{S, A \cup \{\varepsilon\}, s_0, \delta', D\}$, де S – множина станів автомата; A – вхідний алфавіт; ε – вхідне повідомлення нульової довжини; s_0 – початковий стан, $s_0 \in S$; δ' – відображення виду $S \times A \to S$; D – множина кінцевих станів, $D \subseteq S$. Частковим випадком недетермінованого автомата є детермінований, який описується такою п'ятіркою $\{S, A, s_0, \delta, D\}$, де δ – функція, що реалізує

відображення $S \times A \to S$. Очевидно, що хешування може бути реалізовано лише за допомогою детермінованого автомата, оскільки, за визначенням, в результаті виконання процесу хешування над одним й тим самим повідомленням необхідно отримувати одне й те саме хеш-значення. Тому вживається термін псевдонедетерміноване хешування, тобто таке, яке є детермінованим, але описується з точки зору зловмисника недетермінованим автоматом. Для реалізації даної концепції пропонується така математична модель, або, як її ще прийнято називати, конструкція:

$$h_i = f_{v_i}\left(h_{i-1}, m_i\right),$$

де h_i – проміжне хеш-значення, отримане після обробки блока даних, що хешуються, m_i $\left(i = \overline{1,l}\right)$; h_0 – вектор ініціалізації; $f_{v_i}\left(\cdot\right)$ – функція ущільнення, що належить певній скінченній множині функцій F; v_i – вектор керування, що належить певній множині векторів V.

Отже, таке хешування описується шісткою $\left\{S, A, h_0, F, h_l, V\right\}$, однак, якщо вектори керування будуть закриті від зловмисника, то для нього хешування буде описуватись п'ятіркою $\left\{S, A, h_0, F, h_l\right\}$, що представляє собою недетермінований автомат.

Впровадження псевдоенедетермінованої концепції спричинює перегляд вимог до криптографічних примітивів в напрямку їх послаблення, оскільки очікується збільшення нелінійності всього процесу хешування за рахунок того, що операції, які виконуватимуться на кожному раунді будуть закриті від зловмисника. Пропонується використання низки криптографічних примітивів, які базуються на операціях додавання, виключного або, логічного додавання, логічного множення, циклічного зсуву та інвертування.

УДК 004.056.55

ВИКОРИСТАННЯ ОПЕРАЦІЇ МНОЖЕННЯ ЗА СЕКРЕТНИМ ЗНАЧЕННЯМ МОДУЛЯ

О.В. Дмитришин, аспірант
Вінницький національний технічний університет
olexanderdm@gmail.com

В криптографії, під час розробки криптографічних засобів захисту використовують різні криптопримітиви. Зокрема, операцію множення за модулем, яка нелінійним чином зв'язує переважну більшість бітів вихідного блоку даних від вхідного. На сьогоднішній день розробники шифрів використовують операцію множення за відкритим модулем 2^n, $2^n \pm 1$, оскільки використання фіксованого модуля спрощує реалізацію операції множення та пошуку взаємно простих чисел, обернено мультиплікативних за заданим модулем.

Так, наприклад, в симетричних блокових шифрах операцію множення використовують як:

- деяку модифіковану операцію інверсії, оскільки відомі значення множника та модуля;
- допоміжну операцію для зав'язки підблоків даних, при цьому не вимагається пошук обернено мультиплікативних елементів;
- безпосередній криптопримітив, для того, щоб перетворення було зворотне, необхідно знаходити обернено мультиплікативні елементи.

Проте, встановлено, що доцільно використовувати різні значення модулів, оскільки в такому випадку для двох послідовних множень буде отримано дві групи несумісних

операцій множення за різними модулями, які не задовольнятимуть асоціативному закону:

$$a\cdot(b\cdot c)\neq(a\cdot b)\cdot c.$$

Операцію множення n-бітних чисел достатньо ефективно реалізують сучасні процесорах, проте множення за змінним модулем, вимагає, щоб модуль не був більшим за 2^n.

Для вирішення даної проблеми та з метою усунення залежностей між модулями пропонується використовувати таке множення за секретним значенням модуля:

$$X\times A \bmod m=\begin{cases} X\cdot A' \bmod m', \text{ якщо } X<m', \\ (X-m')\cdot A'' \bmod m''+m', \text{ якщо } X\geq m', \end{cases} \quad (1)$$

де m', m'' – n-бітні модулі, $m'=\overline{2^{n-2};3\cdot 2^{n-2}}$, $m''=2n-m'$;

A', A'' – взаємно прості числа з m' і m'' відповідно.

Використання таких двох послідовних множень за різними модулями утворює групи несумісних операцій. Окрім того, оскільки значення модуля залишається невідомим, то це дозволяє протидіяти криптоаналізу на основі мультиплікативних диференціалів.

Якщо замість операції множення «×» в формулу (1) підставити операцію додавання «+», то отримаємо:

$$[X+A] \bmod m=\begin{cases} [X+A'] \bmod m', \text{ якщо } X<m', \\ [(X-m')+A''] \bmod m''+m', \text{ якщо } X\geq m', \end{cases} \quad (2)$$

де A', A'' – n-бітні доданки, $A'<m'$ і $A''<m''$.

Послідовне використання операції додавання згідно (2) дозволяє отримувати групи несумісних операцій, які не задовольнятимуть асоціативному закону:

$$a+(b+c)\neq(a+b)+c.$$

УДК 681.3.07

ПІДХОДИ ДО РЕЛІЗАЦІЇ ПЕРЕСТАНОВОК У БЛОКОВИХ ШИФРАХ

І.В. Бугорська, магістр з інформаційної безпеки
IT-група «RIA-Allegro»

Відомо, що блокові шифри можуть будуватися з використанням тільки двох основних операцій: підстановки або заміни і перестановки. В сучасних шифрах ці операції застосовують разом в межах одного блоку. Це значно обмежує можливості операції перестановки щодо забезпечення стійкості шифру.

У доповіді розглядається нова концепція побудови блокових шифрів і підходи до її реалізації. Ця концепція полягає в тому, що операції перестановок реалізуються в межах блоків, розміри яких відрізняються від розмірів блоків, в межах яких реалізуються операції підстановок.

Повідомлення, яке потрібно зашифрувати, розбивається на блоки розміром N елементів (бітів або байтів). У процесі зашифрування для реалізації перестановок елементів кожен з таких блоків може розглядатися як або одновимірний, або двовимірний, або тривимірний масив елементів. У будь-якому з цих випадків початковим представленням блоку є одновимірний масив $\mathbf{M} = \{m_0, m_1, ..., m_{N-1}\}$.

Для одновимірного випадку перестановки елементів відбуваються за таким правилом. Якщо елемент розташований на i-й позиції, то він переставляється на позицію з номером, що обчислюється за формулою:

$$j = (a \cdot i + b) \bmod N,$$

де a і b - цілі додатні числа, НСД(a, N)=1.

Для реалізації перестановок, що базуються на двовимірному представленні блоку, необхідно виконати такі перетворення. Одновимірний масив розмірності N перетворюється у двовимірний розмірності $p \times q$: $\mathbf{M}[i] \to \mathbf{M}[i, j]$. При цьому можливі такі напрямки формування $\mathbf{M}[i, j]$:

$$\left\| \begin{matrix} m_{11} & \cdots & m_{1p} \\ \cdots & \cdots & \cdots \\ m_{q1} & \cdots & m_{qp} \end{matrix} \right\| \quad \left\| \begin{matrix} m_{11} & \cdots & m_{1p} \\ \cdots & \cdots & \cdots \\ m_{q1} & \cdots & m_{qp} \end{matrix} \right\| \quad \left\| \begin{matrix} m_{11} & \cdots & m_{1p} \\ \cdots & \cdots & \cdots \\ m_{q1} & \cdots & m_{qp} \end{matrix} \right\| \quad \left\| \begin{matrix} m_{11} & \cdots & m_{1p} \\ \cdots & \cdots & \cdots \\ m_{q1} & \cdots & m_{qp} \end{matrix} \right\|$$

У сформованому масиві здійснюється циклічний зсув елементів у рядках або у стовпцях за вказаними напрямками. Після цього двовимірний масив перетворюється в одновимірний. Порядок формування масиву $\mathbf{M}[i]$ задається одним із напрямків.

При реалізації перестановок на основі тривимірного представлення блоку виконуються такі перетворення. Одновимірний масив перетворюється у тривимірний розмірності $p \times q \times h$: $\mathbf{M}[i] \to \mathbf{M}[i, j, k]$. При цьому можливі такі варіанти формування $\mathbf{M}[i, j, k]$. Вибирається одна із площин S_{ik}, S_{ij}, або S_{jk} і формується двовимірний масив. Потім збільшується на одиницю відповідна координата і формується черговий двовимірний масив (зріз).

У сформованому масиві здійснюється циклічний зсув елементів у рядках або у стовпцях для кожного зі зрізів. Інший варіант перетворення полягає у виборі зрізу, паралельного деякій площині і здійсненні одного, двох або трьох поворотів цього зрізу за годинниковою стрілкою.

Після цього тривимірний масив перетворюється в одновимірний.

УДК 681.3.07

ПСИХОЛОГІЧНІ АСПЕКТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

В.М. Дудатьєва, асистент,
А.О. Гнатюк, студент
Вінницький національний технічний університет

Комплексний захист інформації передбачає систему організаційних і технічних заходів і засобів для перекриття можливих каналів витоку інформації, а також реалізацію ефективної політики безпеки та використання кваліфікованих кадрів.

Розробку заходів, які забезпечують максимальну безпеку доцільно здійснювати з урахуванням принципу перекриття можливих каналів витоку інформації. Існують такі основні носії інформації: людина, документи, засоби зв'язку, зокрема такі, як телефони, телефакси та комп'ютерні системи та мережі. Відомий факт, що найслабшою ланкою в цьому ланцюгу є людський фактор. Людина має свої звички, інтереси, слабкості, через які на неї можна впливати, внаслідок чого отримати доступ до потрібної інформації, минаючи всю систему захисту. Корінь проблеми полягає в етико-психологічній підготовці кадрів. Практично всі великі підприємства, корпорації вкладають великі кошти в апаратні засоби захисту інформації, в аналіз, моніторинг, розробку внутрішньої політики безпеки і в останню чергу звертають увагу на психологічну підготовку спеціалістів, що найчастіше і приводить до краху всієї системи захисту. В загальному вигляді система заходів щодо забезпечення інформаційної безпеки може бути такою: обмеження доступу до інформації, розробка і втілення різноманітних

організаційних заходів, які спрямовані на перевірку надійності працівників, спеціальне навчання працівників тощо. Необхідно також враховувати, що інформація, яка складає основу безпеки підприємства може бути цікавою для конкурентів, які, у свою чергу, для отримання цієї інформації можуть застосовувати різні засоби і методи, у тому числі і методи конкурентної розвідки. У таких випадках забезпечення інформаційної безпеки стає задачею для всього колективу.

Для того, щоб суттєво зменшити витік інформації через людину, необхідно більше уваги приділяти спеціальній підготовці фахівців, які будуть мати доступ до конфіденційної (стратегічної) інформації компанії. Нескладно впливати на людину в момент, коли у неї проблеми в особистому житті чи на роботі. Людина в такі моменти потребує психологічної підтримки, співчуття, розуміння її проблеми. Вирішувати цю проблему складно, тому доцільно проводити психологічний моніторинг у колективі, що дозволить контролювати загальний стан, настрій працівників, попередження виникнення різноманітних конфліктів. Необхідно також проведення ефективної політики щодо заохочень і покарань, консультування керівників і співробітників з особистих питань тощо. При цьому потрібно завжди пам’ятати, що некваліфікована допомога може лише погіршити ситуацію та збільшити ризики для компанії. Щоб такого не сталося, необхідно для вирішення таких задач звертатися до кваліфікованих спеціалістів. Також мають бути реалізовані попередні заходи, починаючи з моменту прийняття працівника на роботу, а саме: укладання трудового договору, підписання угоди про збереження конфіденційної інформації, службової таємниці, матеріальної відповідальності, ознайомлення під розпис з посадовою інструкцією.

5. МОДЕЛЮВАННЯ КОМП’ЮТЕРНИХ СИСТЕМ ТА КОМПОНЕНТІВ

УДК 621.374

ДОСЛІДЖЕННЯ КОНВЕЄРНОЇ СТРУКТУРИ СТЕПЕНЕВОГО ЧИСЛО-ІМПУЛЬСНОГО ФУНКЦІОНАЛЬНОГО ПЕРЕТВОРЮВАЧА

В. Б. Дудикевич, д.т.н., професор,
Н.М. Лужецька, ассистент,
А.Я. Горпенюк, к.т.н., доцент
Національний університет "Львівська політехніка"
gorpenuk_ay@polynet.lviv.ua

Степеневі число-імпульсні функціональні перетворювачі (ЧІФП) широко використовуються у вимірювальній та обчислювальній техніці. Актуальною залишається задача підвищення максимальної частоти роботи таких перетворювачів, вирішення якої дозволяє застосовувати вищу частоту квантування і збільшувати точність вимірювання. Однак підвищення максимальної частоти роботи класичних ЧІФП тягне за собою зменшення їх розрядності, що збільшує похибку перетворення ЧІФП. Для вирішення проблеми залежності максимальної частоти роботи ЧІФП від його розрядності було розроблено конвеєрні структурні елементи ЧІФП. Їх максимальна частота роботи значно вища за частоту класичних структур і не залежить від розрядності, що дозволяє підвищувати частоту квантування вимірювальних перетворювачів. Однак, якщо конвеєрний ЧІФП має зворотні зв'язки, його похибка перетворення зростає через затримку сигналу зворотного зв'язку конвеєрною структурою. В таких випадках виникає проблема дослідження і підвищення точності ЧІФП.

В доповіді розглянуто результати синтезу конвеєрної структури степеневого ЧІФП, її особливості та відмінності від класичної структури степеневого ЧІФП. Наголошено на необхідності імітаційного моделювання конвеєрного степеневого ЧІФП з метою дослідження його характеристик. Подано результати дослідження показників роботи конвеєрного степеневого ЧІФП, отримані за допомогою його імітаційної моделі. Зокрема показано, що діапазон зміни аргументу X розробленої конвеєрної структури відповідає діапазону класичної структури і визначається співвідношенням: $2^n < X < 2^{(n+1)}$, де n – розрядність структури. Максимальна частота роботи розробленої конвеєрної структури не залежить від розрядності структури і всього вдвічі менша за максимальну частоту f_0 переключення тригера обраної елементної бази. Натомість максимальна частота роботи класичної структури степеневого ЧІФП значно меньша і визначається співвідношенням: $\mathrm{f_m} = 1/\left(3t_{sm(n)}\right)$, де $t_{SM(n)}$ – час спрацювання n – розрядного комбінаційного суматора. Точність розробленої конвеєрної структури, не зважаючи на значну затримку сигналу зворотного зв'язку, є достатньо високою. Граничні значення абсолютної похибки перетворення не перевищують двох одиниць молодшого розряду (в класичної структури – одиниця молодшого розряду). Цей незначний програш в абсолютних показниках точності з надлишком компенсується порядковим виграшем в максимальній частоті роботи, що дозволяє стосовно розробленої конвеєрної структури степеневого ЧІФП значно зменшити вагу одиниці молодшого розряду результату перетворення.

Результати дослідження розробленої конвеєрної структури степеневого ЧІФП дозволяють констатувати, за всіма основними показниками роботи, її перевагу над класичною структурою степеневого ЧІФП.

УДК 621.3.049

ОПТИЧНИЙ ЧАСТОТНИЙ ПЕРЕТВОРЮВАЧ ДЛЯ ВИЗНАЧЕННЯ ЧАСУ ПЛАЗМОХІМІЧНИХ ПРОЦЕСІВ

В.С. Осадчук, д.т.н., професор, О.В. Осадчук д.т.н., професор, Ю.С. Кравченко к. ф.-м.н., доцент, О.О. Селецька, аспірант
Вінницький національний технічний університет

Базовим елементом системи управління плазмохімічних технологічних процесів є безперервний моніторинг їх фізичних та технологічних параметрів , який здійснюється за рахунок збору та обробки інформації від спеціальних сенсорів. Одними із найбільш ефективних та інформативних методів визначення часу плазмохімічних процесів є оптичні методи. Високої точності в таких системах можна досягнути використовуючи оптоелектронні сенсори на основі транзисторних структур з від'ємним опором.

Для технологічної операції видалення фоторезисту використовується апарат "Плазма – НД 125 ФМ". Час плазмохімічного процесу задається в технологічній програмі, яка є програмним забезпеченням для блоку керування апаратом. Отримання об'єктивної інформації про хід процесу плазмохімічного травлення стає можливим завдяки використанню оптичного частотного перетворювача спектру випромінювання плазми (рис. 1).

Рис. 1 – Електрична схема оптичного частотного перетворювача

Розроблено вимірювальний блок для визначення моменту закінчення процесу плазмохімічного травлення у складі системи управління плазмохімічним процесом. Структурна схема блоку у складі такої системи подана на рис. 2.

Рис. 2 – Структурна схема системи управління плазмохімічним процесом видалення фоторезисту

УДК 621.382: 681.586.776

СИСТЕМА КОНТРОЛЮ ТЕМПЕРАТУРИ НА ОСНОВІ ЧАСТОТНИХ ПЕРЕТВОРЮВАЧІВ З ВІД'ЄМНИМ ОПОРОМ

О.В. Осадчук, д.т.н., проф., Р.В. Криночкін, Барабан С.В.
Вінницький національний технічний університет
serg@politex.org.ua

Сучасний стан розвитку систем контролю фізичних величин вимагає створення та розробку систем, які базуються на нових наукових дослідженнях. Дані дослідження забезпечують подальший перспективний розвиток для таких систем. В роботі представлено систему контролю температури на основі поєднання вимірювальних перетворювачів з покращеними метрологічними параметрами для дослідження об’єкту контролю і сучасних інформаційних технологій для сприймання, обробки, зберігання і передачі виміряних даних.

Розроблена система складається з комплекту частотних перетворювачів температури на основі транзисторних структур з від'ємним опором, вхідного вузла з високочастотними перемикачами, USB-частотоміра, драйверу, програмного забезпечення. Основні особливості розробленої системи контролю температури: покращена точність і чутливість вимірювання температури за рахунок використання перетворювачів температури з частотним виходом на основі транзисторних структур з від'ємним опором; інтеграція з USB-інтерфейсом ПК; живлення від ПК; зберігання виміряних даних на ПК у

вигляді файлу даних; повідомлення про вихід температури за встановлені межі через SMTP-сервер.

Система дозволяє: автоматично вимірювати температуру без втручання оператора в необхідний час і реєструвати вихід температури відносно заданих значень; видавати інформацію про температуру в текстовому і графічному вигляді та зберігати результати вимірювання тривалий час; сигналізувати про вихід температури за встановлені межі.

Система контролю температури має зручний інтерфейс, який повністю інтегрований з сучасним ПК. Лицьова панель розробленого програмного забезпечення для системи представлена на рис. 1.

Рис. 1 – Інтерфейс програмного забезпечення для системи контролю температури на основі частотних перетворювачів з від'ємним опором

УДК 681.32

СПОСІБ ПАРАЛЕЛЬНОГО ФОРМУВАННЯ УЩІЛЬНЕННОЇ СУМИ ЧАСОІМПУЛЬСНИХ СИГНАЛІВ

В.П. Кожем'яко, д.т.н., професор
О.В. Кириченко, аспірант
Вінницький національний технічний університет
sanino2@inbox.ru

Згідно теореми граничного ущільнення логіко-часових інтервалів [1] пропонується досягнення максимально можливого схемотехнічного ущільнення паралельних часових інтервалів при формуванні часового інтервалу сумарної тривалості.

З метою забезпечення можливості отримання нормованої суми сигналів, паралельно-часові інтервали в виді часоімпульсних сигналів, логічно об'єднуються згідно диз'юктивного об'єднання логіко-часового перетворення (ЛЧП), внаслідок чого формується ущільнений часоімпульсний сигнал.

Одночасно з цим визначають в кожний поточний момент часу кількість присутніх часових інтервалів, зменшених на одиницю, що необхідне для формування інтегрального сигналу, пропорційного по величині сумі тривалості часових інтервалів групи за винятком тривалості об'єднаного часового інтервалу, причому інтегральний сигнал отримують шляхом інтегрування за часом сигналу, пропорційного кількості, зменшеній на одиницю, часових інтервалів, присутніх в кожен поточний момент часу існування опорного часоімпульсного сигналу, у момент закінчення якого до нього починають додавати

додатковий часоімпульсний сигнал, який отримують в результаті перетворення інтегрального сигналу в тривалість імпульсу, внаслідок чого отримують часоімпульсний сигнал, тривалість якого дорівнює сумі тривалості часових інтервалів групи.

На Рис.1 зображена схема пристрою, що реалізує запропонований спосіб.

Рис.1 Схема пристрою

$1_1 - 1_n$-входи, на які подаються імпульси одиничних сигналів, задаючи тимчасові інтервали, перетворювач 2 кодів, що накопичує суматор 3, віднімаючий лічильник 4, дешифратор 5 нуля, генератор 6 тактових імпульсів, елементи «АБО» 7 і 8, елементи «І» 9 і 10, інвертор 11, лічильник, що підсумовує 12, багаторазовий комбінаційний суматор 13 і вихід 14.

Внаслідок просторового граничного ущільнення тривалостей часової групи інтервалів отримується вихідний часоімпульсний сигнал.

УДК 621.328

МОДЕЛЮВАННЯ ПРОЦЕСУ ВІДТВОРЕННЯ ЗОБРАЖЕНЬ НА ОСНОВІ ЛОГІКО-ЧАСОВОГО БАЗИСУ

В.П. Кожем'яко[1], д.т.н., професор,
С.В. Дусанюк[1], Л.О. Волонтир[2],
[1]Вінницький національний технічний університет,
[2]Вінницький національний аграрний університет,
[1]kvp@vstu.vinnica.ua, [2]milavolontyr@yandex.ru

Логіко-часові перетворення, відомі також як KVP–перетворення, не потребують складних та великих за обсягом обчислень, що значно спрощує процедуру розпізнавання та відтворення зображень. У процесі оброблення формується система визначників, яка функціонально залежіть від вхідної інформації та ефективно працює для різних типів вхідних сигналів, зводячи їх до логіко-часового базису. Тому актуальною є задача розроблення структурної організації відеоінформаційних систем на основі оптоелектронної елементної бази з використанням методів логіко-часового відтворення зображень.

При формуванні градацій яскравості на основі логіко-часових функцій (ЛЧФ), які можуть приймати тільки два значення ("логічного 0" або "логічної 1"), величина кожної градації яскравості є пропорційною сумарної тривалості існування "логічної 1" логіко-часової функції за період її існування. Таким чином для відтворення зображень логіко-часова функція може бути утворена детермінованим імпульсним періодичним сигналом. Ефективну яскравість елемента зображення визначає закон Тальбота:

$$L_{еф} = \frac{1}{T_K}\int L(t)dt,$$

при $1/T_K > f_{КЧМ}$, де $f_{КЧМ}$ – критична частота миготіння.

Формування градацій яскравості на основі логіко-часових функцій з двома значеннями ("логічного 0" або "логічної 1") визначається інтегралом ЛЧФ і зводиться до формування T_j за період T_K. З великої кількості можливих варіантів формування градацій яскравості практичне значення мають тільки варіанти, що реалізуються на основі регулярних структур.

Варіант 1. Всі відрізки існування кратні Δ-інтервалу і інтеграл ЛЧФ визначається формулою:

$$\int f\left(t, t_1, \ldots, t_m, \Delta_1, \ldots, \Delta_m\right) = m\Delta + C.$$

Даному варіанту природно дати назву - метод додавання мінімальної тривалості існування "логічної 1" ЛЧФ.

Варіант 2. Інтеграл ЛЧФ визначається формулою:

$$\int f\left(t, t_1, \ldots, t_m, T_1, \ldots, T_m\right) = (T_1 + \ldots + T_m) + C.$$

В даному випадку відрізки існування ЛЧФ повинні мати тривалості, які відповідають ряду геометричної прогресії $1:2:4:\ldots:2^j:2^{j+1}:\ldots:2^n$, де $1 \le j \le n$ ціле число.

Даному варіанту природно дати назву - метод суми відрізків різної тривалості існування "логічної 1" ЛЧФ.

В обох варіантах величину кожної градації яскравості визначає формула:

$$L_i = \frac{L_{max}}{T_K}\sum_{j=1}^{m} T_j,$$

де T_j – тривалість існування j–тої "логічної 1" *i*–тої логіко-часової функції за період T_K.

УДК 004.32

ЗАСТОСУВАННЯ ФОТОННИХ КРИСТАЛІВ У СУЧАСНИХ СИСТЕМАХ ОБРОБКИ ІНФОРМАЦІЇ

В.П. Кожем'яко д.т.н., професор,
О.А. Іванов, магістрант,
І.А. Іванов, студент
Вінницький національний технічний університет
ali-arab@mail.ru

Сучасне становище високопродуктивних систем обробки даних напряму пов’язано із нанотехнологіями. Без них неможливе виготовлення процесорних елементів, елементів пам'яті, логічних елементів, що зменшують розміри та піднімають продуктивність вище названих систем.

Ще одним напрямком покращення характеристик є введення паралелізму на всіх етапах обробки, так як саме завдяки паралельним методам обробки інформації можливе суттєве збільшення швидкості.

Також актуальним є заміна (повна або часткова) елементної бази що базується на застарілих електричних технологіях на більш продуктивну оптоелектронну. Вище названі проблеми вимагають радикально нового підходу до організації обчислювальних процесів, та розробки нових типів обчислювальних елементів. Все це приводить до введення у обчислювані системи фотонних кристалів, як аналогів існуючих елементів. Введення фотонних кристалів дасть можливість реалізувати всі поставлені задачі по підняттю швидкості та якості обробки, завадо-захищеності, зменшенню розмірів систем до нанорівня.

Також відкриваються перспективи для простої інтеграції у вже існуючі системи обробки та лінії передачі даних.

У тезах доповіді представлено основні властивості фотонних кристалів як найбільш перспективної елементної бази для реалізації високошвидкісних обчислювальних систем і середовищ. Властивості фотонних кристалів дають можливість повністю замінити існуючу електронну базу на оптичну. Використовуючи неоднорідності такого роду структур можна реалізувати, підсилюючі каскади, поділювані потужності, елементи керування та логіки.

Наприклад пасивний фільтр, та дільник потужності можуть бути реалізовані на основі двовимірних фотонних кристалів природного опалу, канали яких виготовлені за методом двофотонної полімеризації (Рис.1), можливе застосування нанотехнологій для більш точного вирощення каналів, що значно покращує параметри системи.

Рисунок 1 – Елементи для фільтрації та дільник потужності

УДК 543.275.1.08

СВІТЛОВОДНИЙ ГІГРОМЕТР ТОЧКИ РОСИ З БАГАТОРАЗОВИМ ВІДБИТТЯМ

Й.Й. Білинський, д.т.н., професор,
К.Ю. Іоніна, магістрант, В.В. Онушко
Вінницький національний технічний університет
skorpio-26-85@ukr.net

На даний час існує велика кількість вимірювачів вологості газів, які мають ряд недоліків, а саме низьку точність та чутливість у всьому діапазоні вимірювань. Тому необхідне суттєве вдосконалення вимірювачів вологості, направлене на підвищення їх стабільності, чутливості та точності вимірювань.

В роботі запропоновано за рахунок багатократного відбиття підвищити чутливість гігрометра, яка забезпечується залежністю коефіцієнта відбиття від кількості k відбиттів та відносного коефіцієнта заломлення n_1: $R(n_1) = 0.5[R_{\perp}^{k}(n_1) + R_{\Pi}^{k}(n_1)]$. Кількість відбиттів залежить від розмірів полого світловода та кута, під яким вводяться промені.

Для усунення впливу градієнта температур поверхні кювети, який не забезпечує однакового відбивання променів джерела світла по всій довжині кювети, запропоновано конденсаційний гігрометр (рисунок 1), що містить джерело світла 1, порожнистий світловод 2 у вигляді кювети з конусоподібним торцем введення-виведення випромінювання та віддзеркалювальним торцем, фотодетектор 3, кілька термоелектричних регульованих охолоджувачів 4 та вимірювачів температури 5, блок регулювання та обчислення 6, причому

конусоподібний торець оптично зв'язаний з виходом джерела світла та фотодетектором, вхід блока регулювання та обчислення електрично зв'язаний з фотодетектором, а вихід з'єднаний з входом джерела світла, виходи вимірювачів температури електрично зв'язані з входами блоку регулювання та обчислення, а виходи блоку регулювання та обчислення з'єднані з термоелектричними регульованими охолоджувачами.

Рисунок 1 — Структура світловодного гігрометра

При визначенні моменту випадіння роси блок регулювання та обчислення попередньо усереднює значення температур всіх охолоджувачів, а потім видає керуючий сигнал на датчик температури для фіксування температури точки роси. В пристрої не потрібно проводити повірку після кожного вимірювання відносно еталонної вологості, оскільки величину відносної вологості газу блок регулювання та обчислення визначає розрахунково з необхідною точністю по виміряному значенню температури точки роси.

Запропонований гігрометр має більш високу точність та чутливість завдяки використанню багаторазового відбиття світлового променя від поверхні пустотілого світловода та наявності кількох охолоджувачів та вимірювачів температури.

УДК 536.24

МОДЕЛЮВАННЯ НЕЛІНІЙНИХ ТЕПЛОВИХ ПРОЦЕСІВ ДЛЯ КРИСТАЛУ НА БАГАТОШАРОВІЙ ПІДКЛАДЦІ

В.І. Гавриш, к.ф-м., доцент,
Д.В. Федасюк д.т.н., професор, А.І. Косач, аспірант
Національний університет «Львівська політехніка»
ikni_pz@lp.edu.ua

Побудова розв'язків як аналітичних так і чисельних для задач теплопереносу має наукове, практичне та економічне значення. Теплові режими конструкцій у значній мірі визначають їх якісні та кількісні показники і характеризуються температурними полями. Розподіл температур у просторі та часі отримується у результаті дослідження побудованої математичної моделі явища теплопереносу як результат аналітичного або чисельного розв'язування, чи проведення експерименту з фізичною моделлю. У деяких випадках математичне моделювання є єдиним джерелом інформації про температурні поля конструкцій, наприклад, поля в окремих елементах чи вузлах мікроелектронних пристроїв, поля в елементах літаючих апаратів, енергетичних установок, які є недоступними для датчиків температури або теплового потоку. Тому побудова математичних моделей теплових режимів для різного роду конструкцій, які піддаються температурним впливам, є важливою задачею, оскільки багато якісних та кількісних показників оцінки поведінки конструкцій частіше визначаються, виходячи з температурних режимів роботи. Задачі моделювання теплових режимів значно ускладнюються для термочутливих конструкцій кусково-однорідної структури. У зв'язку з цим розглядається

термочутливий кристал, в області якого діють рівномірно розподілені внутрішні джерела тепла, потужність яких є такою, що дорівнює q_0, на термочутливій багатошаровій підкладці, віднесений до прямокутної декартової системи координат із початком на граничній поверхні кристалу. На поверхнях спряження кристалу та шарів підкладки відбувається ідеальний тепловий контакт, а на граничних поверхнях кристалу та підкладки здійснюється конвектний теплообмін із зовнішнім середовищем зі сталою температурою t_c.

Математична модель нестаціонарного процесу теплопровідності запишеться у вигляді

$$\lambda(t,z)\cdot\frac{\partial^2 t}{\partial z^2}=c_v(z)\frac{\partial t}{\partial \tau}-q_0 S_+(z_1-z),$$

$$t(0,z)=t_c,\ \lambda_1\left.\frac{\partial t}{\partial z}\right|_{z=0}=\alpha_0(t|_{z=0}-t_c),\ \lambda_n\left.\frac{\partial t}{\partial z}\right|_{z=z_n}=\alpha_n(t_c-t|_{z=z_n}),$$

де $t(\tau,z)$ - шукане температурне поле; $\lambda(t,z)=\lambda_1(t)+\sum_{i=1}^{n-1}\left[\lambda_{i+1}(t)-\lambda_i(t)\right]\cdot S_-(z-z_i)$ - коефіцієнт теплопровідності всієї конструкції; $\lambda_1(t)$ - коефіцієнт теплопровідності кристалу; $\lambda_i(t)\ (i=2,3,...,n)$ - коефіцієнти теплопровідності шарів підкладки; τ - час; $c_v(z)=c_v^{(1)}+\sum_{i=1}^{n-1}\left[c_v^{(i+1)}-c_v^{(i)}\right]\cdot S_-(z-z_i)$ - об'ємна теплоємність всієї конструкції; $S_\pm(\zeta)$ - асиметричні одиничні функції; α_0,α_n - коефіцієнти тепловіддачі з граничних поверхонь $z=0$ кристалу та $z=z_n$ n-го шару підкладки, z_1,z_i - товщина кристалічного шару та i-го шару підкладки відповідно. Запропоновано побудову розв'язку для нелі-нійної крайової нестаціонарної задачі теплопровідності.

УДК 519.92

НЕЧЕТКИЕ ПИД КОНТРОЛЛЕРЫ ДЛЯ СИСТЕМ УПРАВЛЕНИЯ НЕСТАЦИОНАРНЫМИ ОБЪЕКТАМИ

Э.Е. Герман, ассистент
Национальный технический университет
"Харьковский политехнический институт"
EdGerman@mail.ru

Развитие новых информационных технологий в сочетании с широким использованием современных микроконтроллеров, ПЛИС, сетей на одном кристалле позволяет создавать высокопроизводительные робастные, самонастраивающиеся, распределенные вычислительные системы, обладающие искусственным интеллектом. Методы нейро-нечеткого управления обеспечивают возможности реализации систем, которые успешно выполняют задачи управления сложными нелинейными и нестационарными объектами, где классические методы обработки данных и управления трудно применимы.

В докладе представлен метод проектирования нечетких ПИД контроллеров (НПИДК), основанный на параметрическом подходе формирования управляющих воздействий путем анализа экспертных знаний операторов, управляющих мультипроцессорной системой.

При формировании структуры НПИДК определяется его тип, который зависит от характеристик имеющихся нечетких экспертных протоколов управления и выбранного подхода к проектированию контроллера. При параметрическом подходе лингвистическое описание нечеткого блока контроллеров имеет вид:

Если (сигнал ошибки *e* –...),
тогда (коэффициент усиления –...)
Структурная схема контроллера представлена на рис. 1:

Рис. 1. Структурная схема НПИДК.

При таком подходе блок нечеткого вывода (БНВ) может формировать как единый коэффициент усиления, так и отдельно для каждого канала: пропорционального, интегрального и дифференциального.

Рассматривая тип функций принадлежности (ФП) в БНВ, предлагается использовать либо гауссовы кривые, либо равнобедренные треугольные ФП. Такие ФП обеспечивают минимальное число параметров, необходимых для их построения. В первом случае это координата максимума h и коэффициент концентрации φ, во втором – координата максимума h и носитель нечеткого множества $(h\text{-}a, h+a)$.

Показано, что для минимизации базы правил число ФП, как для входного параметра (ошибки), так и для выходного (коэффициент усиления) сводится к минимуму. Три ФП используются, когда основная база правил формируем согласно экспертным оценкам. Две ФП обеспечивают минимизацию параметров нечеткой настройки для их дальнейшей численной оптимизации.

Показано применение нечетких ПИД контроллеров в мультипроцессорной системе управления ростовыми установками для выращивания крупногабаритных монокристаллов в опытном производстве ИСМА НАН Украины в г. Харьков.

УДК 004.357

РОЗРОБКА СИСТЕМИ ДОСЛІДЖЕННЯ АУДІО-ДАНИХ

Н.М.Чайківський, студент,
О.М. Пігур-Пастернак, викладач
Дрогобицький державний педагогічний університет імені Івана Франка
olia-ukr@ukr.net

Протягом останніх років спостерігається інтенсивне впровадження технології ЦОС (цифрова обробка сигналів) у комп'ютеризовані системи обробки інформації. Виробниками комп'ютерної техніки розроблено велику кількість середовищ, що відтворюють, записують, синтезують і розпізнають різноманітні звуки. А розпізнавання мови перейшло з мрій науковців у практичне використання і вже зараз включене у вибіркові опції в останніх версіях Microsoft Office.

Рис. 1 – Інтерфейс комп'ютерної системи опрацювання аудіо-даних

Результатом проведених досліджень є розроблена програма (рис. 1), в якій користувач має можливість працювати із аудіо даними: записувати і відтворювати різноманітні звуки та мелодії, перетворювати формат

збереження аудіо-даних. Крім цього система дозволяє проводити дослідження звукових коливань, які цифровим методом закодовані в аудіо-даних, у вигляді електричних коливань звукової частоти (аналогових «портретів») і визначати «портрети» періодів коливань мовних звуків. У розробці алгоритмів використовувались функції і методи середовища програмування Borland C++Builder 6.

Алгоритми визначення «портрету» періоду коливань мовного звуку полягає у тому, що

- записується мовний звук користувача і зберігається в аудіо-файлі;
- виконується побудова аналогового «портрету» аудіо-даних, які записані у файлі;
- аудіо-дані розбиваються на ділянки тривалістю в 30 мс і визначаються усі екстремальні точки кривої звукового сигналу;
- визначається період коливань мовного звуку як період коливань ділянки між двома подібними екстремальними точками.

Таким чином будується точний «портрет» кожного вимовленого звуку (рис. 2) і заноситься до бази звукових «портретів» користувача.

Розроблену систему зручно використовувати не тільки для запису чи прослуховування звукових файлів, а й досліджувати їх. І, маючи базу мовних звуків користувача, можна ідентифікувати чітко вимовлене слово по звуках, а це у свою чергу дозволяє перетворити вимовлене слово у текст у текстовому редакторі.

Рис. 2. Визначений «портрет» періоду коливань звуку «У»

УДК 681.32

МЕТОДЫ СИНТЕЗА ПОСЛОВНО-ПОСЛЕДОВАТЕЛЬНЫХ УМНОЖИТЕЛЕЙ, ОПЕРИРУЮЩИХ В ПОЛЯХ ГАЛУА

И.В. Гормакова, аспирант НТУ «ХПИ»
ira.gormakova@mail.ru

В настоящее время потребность в компактных схемах, способных работать с многоразрядными данными, дала толчок к разработке высокоскоростных схем с параллельной обработкой данных. В цифровых устройствах обработки информации, криптосистемах, в системах помехоустойчивого кодирования и т.д. широко используются арифметические модули, функционирующие в полях GF(2^p). В системах кодирования с обнаружением и исправлением ошибок операции суммирования и умножения в поле GF(2^p) являются основными. В криптосистемах операции в поле GF(2^p) используются при реализации алгоритмов в эллиптических кривых.

В перечисленных выше устройствах составными модулями, которые во многом влияют на сложность и время работы системы, являются арифметические модули. Операция сложения в поле GF(2^p) эквивалентна простой побитовой операции XOR. Операции умножения и возведения в квадрат требуют более сложной схемной реализации. Другие арифметические операции, такие как инверсия и возведение в степень, могут быть представлены через операции умножения и возведения в квадрат. Умножению в конечных полях посвящено множество научных работ, в которых рассматриваются различные способы представления элементов поля (нормальный

базис, полиномиальный или стандартный базис), образующие полиномы поля (триномиалы, пентономиалы), а также представлены различные архитектуры умножителей (разрядно-последовательные, параллельные, пословно-последовательные).

В докладе представлен метод синтеза пословно-последовательного умножителя в поле $GF(2^p)$. Элементы поля имеют стандартный базис представления.

Представлены основные методы построения умножителей в полях Галуа. Показано, что разрядно-последовательные умножители имеют наиболее простую архитектуру, однако время выполнения операции умножения составляет p тактов. В параллельных умножителях операция умножения выполняется за один такт, однако аппаратные затраты и площадь на кристалле достаточно велики. Пословно-последовательные умножители наилучшим образом соответствует требованиям временных (время выполнения алгоритма), аппаратных (количество логических вентилей) и пространственных (площадь на кристалле) затрат.

Представленный в докладе пословно-последовательный умножитель состоит из унифицированных блоков, которые позволяют просто реализовать умножитель на ПЛИС типа FPGA,что дает возможность легко модифицировать архитектуру умножителя при изменении длины операндов, длины слова, образующего полинома поля. Изменение образующего полинома при сохранении степени полинома p требует лишь изменения правил настройки сети клеточных автоматов, входящих в состав умножителя, при полном сохранении их структуры.

Сформулированы требования к тестопригодности умножителей в полях Галуа. Разработан алгоритм синтеза проверяющих тестов для всех составных блоков умножителя.

УДК 004.942; 548.4

МОДЕЛЮВАННЯ ПАРАМЕТРІВ ПІДСИСТЕМИ ТОЧКОВИХ ДЕФЕКТІВ У НАПІВПРОВІДНИКОВИХ КРИСТАЛАХ

Л.І. Д'яченко, асистент, Є.В. Мінов,
С.Е. Остапов, д.т.н., професор, П.М. Фочук
Чернівецький національний університет
імені Юрія Федьковича
lilya.d82@gmail.com

Досконалі знання структури та кінетики точкових дефектів у напівпровідникових кристалах є основою створення високоякісного базового матеріалу для детекторів рентгенівського випромінювання. Лише це дозволить досягти найвищої детектуючої здатності та чутливості пристроїв, і тому сучасна техніка очищування кристалів від домішок висуває на передній план задачу дослідження власних дефектів.

Велику допомогу у розумінні структури будь-яких точкових дефектів можуть надати засоби комп'ютерного моделювання, які вже давно стали стандартним методом дослідження фізичних явищ. Не дивлячись на велику кількість математичних пакетів, таких, як Mathematica, MathCAD та інших, які дозволяють моделювати фізичні процеси різного типу, засобів зі спеціалізованими можливостями на ринку практично немає.

Для моделювання структури та динаміки власних точкових дефектів напівпровідникових кристалів було розроблено спеціалізоване програмне забезпечення (ПЗ). ПЗ дозволяє побудувати температурні та тискові залежності концентрації носіїв з врахуванням власних точкових дефектів в напівпровідникових кристалах, а

також моделювати процес охолодження з довільними вхідними даними які зберігаються в файлі формату *.xls або подаються у вигляді графіків.

Розроблена програма має конструктор рівнянь електронейтральності з синтаксичним аналізатором. Це означає, що програмний комплекс дає можливість проводити розрахунки параметрів будь-яких напівпровідникових кристалів. Єдиною умовою є те, що нові рівняння повинні супроводжуватися відповідними константами рівноваги, що пов‘язують їх з відомими величинами. Програма дозволяє створювати різні конфігураційні файли для розрахунку параметрів різноманітних напівпровідникових кристалів.

Програмний комплекс містить засоби для побудови тривимірної моделі системи точкових дефектів кристалу на основі серії мікрофотографій по глибині зразка. ПЗ надає користувачу можливість фільтрування дефектів за величиною, а також ручного коректування розпізнаного зображення. Математичний блок дозволяє виконати статистичну обробку зображень точкових дефектів та побудувати відповідні гістограми.

Існує можливість експортувати всі результати роботи програми в MS Excel, а також роздрукувати необхідні таблиці та графіки.

З усього вищенаведеного можна зробити висновок, що розроблений програмний комплекс надає широкий спектр можливостей для дослідження структури власних точкових дефектів напівпровідникових кристалів, а також для обробки результатів хімічних експериментів з реальними кристалами CdTe. Можливість отримання тривимірного зображення зразків значно спрощує процес аналізу підсистеми власних дефектів у вирощених напівпровідникових кристалах.

УДК 681.321

АЛГОРИТМИ АВТОМАТИЗОВАНОЇ РОБОТИ КВАНТОВО-ХВИЛЬОВОГО СПЕКТРОЕНЕРГЕТИЧНОГО ПЕРЕТВОРЮВАЧА В ІНФОРМАЦІЙНО-ЕНЕРГЕТИЧНИХ МЕРЕЖАХ

В.П. Кожем'яко, д.т.н., професор,
А.Д. Слободяник, к.т.н., доцент
Вінницький національний технічний університет

В роботі розглядається проблема створення технічної системи - квантово-хвильовий спектроенергетичний перетворювач (КХСП), що являє собою пристрій спектроенергетичного перетворення частоти випромінювання, який оснований на акумулюванні, перетворенні енергії випромінювання. Активні робочі середовища використовують для резонансної оптичної накачки парів лужних металів, в яких здійснюється заселення верхніх атомних рівнів, що зумовлює інверсне заселення відносно нижче розміщених енергетичних рівнів і оптично активні речовини, які є придатними для реалізації ефекту Комптона. Падаюче випромінювання реєструють за допомогою чутливих детекторів, антен, фотоприймачів і застосування логічних елементів дає змогу аналізувати спектральний склад випромінювання та здійснювати селекцію сигналів необхідної частоти відповідної енергії. Автоматизують весь процес перетворення частоти випромінювання системою зворотного зв'язку.

При допомозі приймачів випромінювання і пов'язаних з ними логічних елементів аналізатора відбувається селекція падаючого випромінювання на окремі спектральні діапазони. Випромінювання деякої ширини спектру $\hbar(\omega+\Delta\omega)$ потрапляє на аналізатор, в якому відбувається аналіз (декодування) виду енергетичного спектру (оптичний, радіочастотний, рентгенівський, γ-випромінювання, космічні промені і т.д.).

Вхідними пристроями аналізатора є оптичні коліматори, коливальні контури з чутливими антенами, детектори γ-випромінювання. Демодулююча система – оптично активне середовище, в якому відбувається розкладання складного за спектром випромінювання на окремі частоти ω_0. Тоді моноскладові випромінювання потрапляють на блок приймачів випромінювання. Між демодулюючою системою і блоком приймачів існує зворотній зв'язок. На виході з такої системи отримується сигнал заданої частоти ω_0, що відповідає енергії $\hbar\omega_0$. Блок з оптично активними середовищами працює на відомих фізичних закономірностях та явищах резонансу, інтерференції, дифракції, дисперсії, фотоефекту, ефекту Комптона. Ця система робить селекцію та взаємне перетворення вхідного сигналу за відповідними частотами, тобто за енергією.

Така система КХСП відповідає вимогам, що має такі характеристики:

1. – регулярного, або впорядкованого, пристрою, що складається з елементів або частин, взаємопов’язаних і діючих як одне ціле;

2. – сукупності або групи елементів, необхідних для виконання деякої операції, тобто дії для досягнення поставленої мети.

В загальному система КХСП характеризується як сукупність взаємодіючих елементів, призначених для виконання необхідної цілком визначеної операції.

УДК 004.032.5; 004.94

МОДЕЛЮВАННЯ ЧАСТОТНОГО ШУМУ В РОБОТІ УНІВЕРСАЛЬНОГО КВАНТОВОГО ВЕНТИЛЯ ФРЕДКІНА

В.Г. Дейбук, д.ф.-м.н., професор, Г.П. Горський, магістр
Чернівецький національний университет
імені Юрія Федьковича
v.deibuk@chnu.edu.ua

В рамках моделі Ізінга для ланцюжка чотирьох взаємодіючих ядерних спінів розглянуто роботу чотирирозрядного квантового вентиля Фредкіна. Вентиль Фредкіна – це універсальний зворотний квантовий логічний элемент контрольованого обміну, який обмінює вміст двох розрядів (квантових бітів, КвБ), якщо контролюючий КвБ знаходиться у стані логічної 1 і не виконує цього у протилежному випадку. Стан системи спінів в даному випадку задається сильним статичним магнітним полем (СМП). Орієнтація спіну за напрямком СМП відповідає станові логічного 0, а проти – станові логічної 1. Керування системою здійснюється за рахунок поперечного обертового радіочастотного магнітного поля (РЧМП). На таких квантових регістрах будується квантовий комп’ютер на ядерному магнітному резонансі (ЯМР).

Незбурена система n взаємодіючих спінів у СМП володіє набором з 2^n енергетичних рівнів, кожен з яких відповідає одному з можливих булевих станів КР розрядності n. Керуюче РЧМП розглядається як збурення. В розглядуваній квантовій системі під дією РЧМП можливі лише переходи з інверсією будь-якого одного з розрядів. Таким чином будь-який квантовий алгоритм в такій системі – це сукупність дозволених переходів між станами системи

під дією РЧМП. При цьому частота РЧМП послідовно настроюється в резонанс з частотою кожного з дозволених алгоритмічних переходів. Якщо немає явища декогерентизації, тобто всі можливі булеві стани системи є стабільними і спіни можуть виконувати роль КвБ необмежено довгий час, то результат дії такого алгоритму – це перерозподіл ймовірностей реалізації між станами системи.

Моделювання роботи квантового вентиля Фредкіна на ЯМР виконано шляхом числового розв'язання нестаціонарного рівняння Шредінґера для квантової системи, яка репрезентує КР. При цьому розглянуто алгоритми, для яких в операції обміну обов'язково бере участь старший (4-й) КвБ, який обмінюється з будь-яким з інших КвБ, а решта КвБ розглядаються як контролюючі. В результаті аналізу розглянуто вплив параметрів системи на чіткість роботи вентиля Фредкіна і вплив частотного шуму на ймовірність правильної відповіді.

Аналіз коректності роботи вентиля Фредкіна, показало, що для 4-х КвБ КР чіткість роботи вентиля Фредкіна істотно знижується, якщо обмінна взаємодія різко спадає з відстанню між спінами. Знайдено параметри та умови коректної роботи описаної системи.Дослідження впливу частотного шуму на роботу вентиля Фредкіна у чотирирозрядному КР виконано для двох механізмів шуму: неточності задання частоти РЧМП і неконтрольованого зсуву енергетичних рівнів системи. У першому випадку ймовірність правильної відповіді знижується з 1 до 0.5, якщо відносна похибка задання частоти складає $\pm 1.25 \cdot 10^{-4}$, у другому випадку таке ж зниження ймовірності правильної відповіді відбувається, якщо відносний зсув енергетичних рівнів складає приблизно 0.012-0.013 від відстані між ними. Отримані результати дозволяють вести напрямлений пошук систем для реалізації ЯМР квантового процесора.

УДК 621.374

ДОСЛІДЖЕННЯ «ЯКОСТІ» ОДНОКРИСТАЛЬНИХ УПІ

Л.Б. Ліщинська, к.т.н., доцент, Я.С. Рожкова, студент, М.В. Барабан, аспірант, М.А. Філинюк, д.т.н., професор
Вінницький національний технічний університет

Проведені дослідження коефіцієнта «якості» УПІ на базі одноперехідного, біполярного та польового транзисторів. В залежності від частоти при різних значеннях основних фізичних параметрів транзисторів:

а)

б)

в)

г)

Рисунок 1 – частотні залежності коефіцієнту якості при різних значеннях $R_{б2}$ (а), $C_{б1}$ (б) ОТ та $R_б$ (в), C_{k1} (г) БТ.

Для УПІ на базі ОТ зі зростанням величини $R_{б2}$, коефіцієнт якості зростає пропорційно зростанню частоти Ω. Такі самі тенденції спостерігаються й для $R_{б1}$. В свою чергу збільшення ємності $C_{б1}$ призводить також до незначного зростання досліджуваного коефіцієнту.

Для УПІ на базі БТ спостерігаються протилежні залежності: зі зростанням $R_б$ на 6 *Ом* (4 - 10 *Ом*), коефіцієнт якості спадає. Зростання ємності $C_{к1}$ збільшує досліджуваний коефіцієнт.

УДК 681.586.776:621.382

ЧАСТОТНИЙ ПЕРЕТВОРЮВАЧ ОПТИЧНОГО ВИПРОМІНЮВАННЯ НА ОСНОВІ ДВОХ МДН-ТРАНЗИСТОРІВ

В.С. Осадчук, д.т.н., професор, О.В. Осадчук, д.т.н., профессор, О.М. Ільченко, аспірант
Вінницький національний технічний університет
alenail_86@mail.ru

Серед відомих методів перетворення потужності оптичного випромінювання особливе місце має подання вимірюваної інформації в формі частотного сигналу, що використовується в радіовимірювальних схемах на основі транзисторних структур з від'ємним опором. Використання частотного сигналу в якості інформативного параметра первинних перетворювачів характеризується високою завадостійкістю, простотою та значною точністю перетворення в цифровий код, зручністю комутацій в багатоканальних вимірювальних системах.

На рис.1 представлена схема частотного оптичного перетворювача на основі двох МДН-транзисторів VT1 і VT2 з чутливим кремнієвим сонячним елементом (КСЕ).

Рисунок 1 – Електрична схема частотного оптичного перетворювача на основі двох МДН-транзисторів

Самозбудження і стійкість роботи автогенератора перетворювача обумовлені вибором робочої точки на вольт-амперній характеристиці (ВАХ). Для вибору робочої точки було визначено ВАХ (рис.3) на основі еквівалентної схеми (рис.2) та складених для неї рівнянь Кірхгофа.

Рисунок 2 – Еквівалентна схема перетворювача по постійному струму

Рисунок 3 – Сімейство статичних ВАХ перетворювача

Схема на рис. 1 має електронну перебудову частоти генерації. З рис. 4 видно, що зміна частоти генерації має лінійний характер при зміні напруги живлення в широких межах

Рисунок 4 – Залежність зміни частоти генерації від напруги живлення при різних значеннях напруги керування: 1) Uк=4,2В; 2) Uк=4,4В; 3) Uк=4,6В; 4) Uк=4,8В; 5) Uк=5В; 6) Uк=5,2В; 7) Uк=5,4В; 8) Uк=5,6В

УДК 681.325

МОДЕЛЮВАННЯ АНАЛОГО-ЦИФРОВИХ ПЕРЕТВОРЮВАЧІВ

В.М. Кичак, д.т.н., професор,
Г.Г. Бортник, к.т.н., доцент, Н.О. Пунченко
Вінницький національний технічний університет
sbortnyk@gmail.com

Аналого-цифрові перетворювачі (АЦП) є одними з найважливіших пристроїв сучасних та перспективних комп'ютерних систем, що суттєво впливають на їх граничні можливості, як за швидкодією, так і за динамічною точністю. Складність аналізу процесів аналого-цифрового перетворення різних класів сигналів полягає в тому, що АЦП відносяться до нелінійних інерційних пристроїв і тому повна модель перетворювача повинна враховувати ці обидві властивості, що є надзвичайно складною задачею.

Метою роботи є розробка методу ідентифікації моделі АЦП з урахуванням нелінійності характеристик перетворення та шумових ефектів, що виникають при аналого-цифровому перетворенні.

Для врахування динамічних властивостей АЦП пропонується модель, що містить аналоговий перетворювач (АП) (який може розглядатись як лінійне інерційне коло) та ідеальний безінерційний квантувач (КВ) з рівноступінчастою симетричною передатною характеристикою. Енергетичний спектр сигналу на виході АЦП дорівнює добутку квадрату модуля його коефіцієнта передачі на вхідний енергетичний спектр:

$$G_{\text{вих}} = (f_i) = \left|K(f_i)\right|^2 \cdot G_{\text{вх}}(f_i). \qquad (1)$$

Застосуємо параметричне представлення характеристик $K(f_i)$. Тому модель частотної характеристики можна визначити за допомогою відповідних параметрів $b_1, b_2, \ldots b_j$. На базі визначеної частотної характеристики можна знайти вихідний сигнал АЦП, що є результатом впливу блоку АП в даній моделі. Частотна характеристика не може бути повною динамічною характеристикою АЦП, тому що потрібно зважати ще на особливості проходження сигналу $L[x]$ блоком КВ. Тому для врахування нелінійності АЦП в його модель уведено додатковий рівномірно розподілений шум в інтервалі $[-0{,}5h, 0{,}5h]$.

Ефективне число розрядів є найбільш узагальненою характеристикою перетворення. Інерційність АЦП та нелінійність їх характеристики перетворення зменшують ефективне число розрядів. При моделюванні АЦП таке зменшення за рахунок інерційності враховується шляхом використання частотної характеристики $K(f)$, а нелінійність перетворення імітувалась збільшенням кроку квантування. Для цього введемо в шумовий інтервал мультиплікативно два параметри, що будуть моделювати збільшення ширини кроку квантування

$$A = \left[-0{,}5 \cdot \alpha \cdot \beta \cdot h; -0{,}5 \cdot \alpha \cdot \beta \cdot h\right], \qquad (2)$$

де α – параметр, що враховує нелінійність АЦП;

β – параметр, що враховує інерційні властивості АЦП.

Тоді ефективність числа розрядів АЦП з урахуванням (2) прийме вигляд

$$n_{\text{еф.}} = \frac{S/N + 20\lg k - 20\lg\alpha - 20\lg\beta - 4{,}8}{6{,}02}. \qquad (3)$$

Використавши процедуру визначення $n_{\text{еф.}}$ для кількох значень частоти, можна одержати частотну залежність ефективного числа розрядів АЦП.

УДК 681.325.5.181.4

ЗАДАЧА ПОВЫШЕНИЯ БЫСТРОДЕЙСТВИЯ СПЕКТРОМЕТРИЧЕСКОЙ СИСТЕМЫ

Л.Р. Бекирова, к.т.н., доцент
Азербайджанская государственная нефтяная академия

При исследовании наземных объектов, в том числе при оперативном определении и оценке пожаров и взрывов в быту и промышленных объектах, трубопроводах, при контроле параметров обстановки в зонах происхождения чрезвычайных событий, при обнаружении негативных случаев, возникающих от воздействия природных и техногенных факторов в зонах проводки нефтяных и газовых трубопроводов, при оценке состояния сельскохозяйственных и природных растений, а также при оценке экологического состояния окружающей среды и других важных проблем из-за ряда преимуществ в последнее время очень широко распространен и подтвердил себя как рациональный метод для определения различных свойств исследуемых объектов метод дистанционного зондирования по сравнению с другими методами.

К техническим характеристикам системам основанным на применении этого метода и расположенным на борту летательного аппарата, из-за влияния различных внутренних и внешних факторов предъявляются специальные требования и их усовершенствование является актуальной задачей.

С целью повышения достоверности результатов измерения спектрометрических комплексов, являющихся одной из подспутниковых систем и для улучшения таких

характеристик, как быстродействие, весо-габаритные показатели и потребление энергии, применение микропроцессоров и микроконтроллеров как в процессе обработки данных и прдставалении результатов, так и в процессе измерения является целесообразным.

Это дает возможность предварительной обработки результатов измерения в каждом канале и проведении соответствующих расчетов с целью коррекции погрешностей канала. Если учесть скорость летательного аппарата, то можно обосновать потребность высокого быстродействия спектрометрического комплекса. При расположении комплекса на борту беспилотного летательного аппарата эти требования еще более ужесточаются

Применение жидких кристаллов в оптических блоках спектрометрического комплекса, обладающие малыми весо-габаритными показателями и потребляющие малую энергию и позволяющие электронное управление, дает возможность исключить некоторые отрицательные свойства N-канальных комплексов с механическим модулятором.

В таких системах гибкость структуры обеспечивается использованием программируемых многофункциональных измерительных систем, связь между которыми выполняет соответствующее программное обеспечение. В отличие от информационных систем, применяемых в наземных исследованиях, в спектрометрических системах дистанционного зондирования обеспечение интеллектуальности не ограничивается измерением полезных оптико-физических параметров исследуемых объектов.

УДК 621.3.088

ПРОГРАМА ДЛЯ РОЗРАХУНКУ ПАРАМЕТРІВ ПОТЕНЦІЙНО-НЕСТІЙКИХ ЧОТИРИПОЛЮСНИКІВ

К.В. Огородник, к.т.н., Л.Б. Ліщинська, к.т.н., доцент, С.Є. Фурса, к.т.н.
Вінницький національний технічний університет
kostok@yandex.ru

При проектуванні радіоелектронної апаратури широке застосування отримало використання імітансних та хвилевих параметрів чотириполюсників. Перші, як правило, використовуються в діапазоні низьких та високих частот, а другі – в діапазоні надвисоких частот. Авторами розроблено ряд нових непрямих методів для вимірювання цих параметрів стосовно саме потенційно-нестійких чотириполюсників. Розроблені методи передбачають розрахунки для перетворення безпосередньо вимірюваних величин (модуль та фаза комплексних коефіцієнтів відбиття) у шукані величини (матриці імітансних та хвилевих параметрів чотириполюсника). Щоб автоматизувати вказаний процес розроблено математичний апарат та комп’ютерну програму. Зовнішній вигляд інтерфейсу даної програми показано на рис. 1.

Для наочності виконуваних розрахунків та отриманих результатів у програмі використовується відома діаграма Вольперта-Смітта. Відображення цієї діаграми на комплексну площину вхідних (вихідних) імітансів дозволяє швидко отримувати інформацію про критичні точки та запас стійкості чотириполюсника, про максимальні та мінімальні можливі значення імітансів чотириполюсника,

про відповідність вхідних (вихідних) імітансів чотириполюсника імітансам навантаження тощо.

Рис. 1. Загальний вигляд інтерфейсу програми

Програмою передбачено як введення відомих імітансих параметрів чотириполюсників, так і розрахунок імітансних та хвилевих параметрів за допомогою розроблених методів через експериментально отримані значення комплексних навантажень чи коефіцієнтів відбиття. Також передбачено розрахунок координат критичних точок діаграми та відповідних їм навантажень. Можливе введення масиву частотних значень імітансних параметрів з текстового файлу та побудова на їх основі частотних залежностей. При русі курсору по діаграмі, на екран динамічно виводяться значення дійсної та уявної складових вхідного імітансу чотириполюсника у даній точці. При натисненні ж клавіші мишки - виводяться розраховані значення навантажень для даної точки.

УДК 004.738.5

ФОРМАЛЬНІ МОДЕЛІ СИСТЕМИ КЕРУВАННЯ КОНТЕНТОМ

В.А. Висоцька, асистент, Л.В. Чирун, к.т.н., доцент
Національний університет «Львівська політехніка»
victana@bk.ru

Формальна модель системи керування контентом $S = \langle X, C, Y \rangle$ - це множини величин, що описують процес функціонування системи і утворюють такі підмножини: вхідні дані $x_i \in X$, $i = \overline{1, n_X}$; контент $c_i \in C$, $i = \overline{1, n_C}$; вихідні дані $y_j \in Y$, $j = \overline{1, n_Y}$. Процес функціонування S описується функцією $\vec{y}(t) = f\left(\vec{x}, \vec{c}, \vec{v}, \vec{h}, t\right)$. Системи керування контетном класифікують за способом роботи.

Генерація сторінок за запитом – $S_Q = \langle X, C, Q, R, Edit, Y \rangle$, де $X = \{x_1, x_2, \ldots, x_{n_X}\}$ – множина вхідної інформації; $C = \{c_1, c_2, \ldots, c_{n_C}\}$ – множина контенту; $Y = \{y_1, y_2, \ldots, y_{n_Y}\}$ – множина сформованих сторінок; $Q = \{q_1, q_2, \ldots, q_{n_Q}\}$ – множина запитів; R – функція формування та подання сторінки; $Edit$ – функція редагування та модифікації контета. Система працює на основі зв'язки «Модуль редагування → База даних → Модуль представлення». Модуль представлення генерує сторінку із змістом при запиті на нього, на основі інформації з бази даних. Інформація в базі даних змінюється за допомогою модуля редагування. Сторінки наново створюються сервером при кожному запиті, а це

створює навантаження на системні ресурси. Процес редагування та модифікації контенту описується функцією $\vec{c}(x_i,t)=Edit(\vec{c},x_i,t)$. Процес формування сторінок описується функцією $\vec{y}(t+\Delta t)=R(\vec{q},\vec{c},t,\Delta t)$, тобто

$$y_i=\left\{\bigcup c_j \middle| (\forall c_j\in C_x)\wedge(\exists x_i\in C_x),\ j=\overline{1,m},i=\overline{1,n}\right\}.$$

Генерація сторінок при редагуванні – $S_E=\langle C,Edit,Y\rangle$, де $C=\{c_1,c_2,\ldots,c_{n_C}\}$ – множина контенту; $Y=\{y_1,y_2,\ldots,y_{n_Y}\}$– множина статичних сторінок; $Edit$ – функція редагування та модифікації контета. Система при внесенні змін до змісту сайту створює набір статичних сторінок. При такому способі не враховується інтерактивність між відвідувачем і вмістом сайту. Процес формування сторінок описується функцією $Edit$ вигляду: $\vec{y}(t)=Edit(\vec{c},t)$.

Змішаний тип – $S_M=\langle X,C,Q,R,Edit,Caching,Y\rangle$, де $X=\{x_1,x_2,\ldots,x_{n_X}\}$– множина вхідної інформації; $C=\{c_1,c_2,\ldots,c_{n_C}\}$ – множина контенту; $Y=\{y_1,y_2,\ldots,y_{n_Y}\}$– множина сформованих сторінок; $Q=\{q_1,q_2,\ldots,q_{n_Q}\}$– множина запитів; R – функція формування та подання сторінки; $Edit$ – функція редагування та модифікації контета, $Caching$ – функція формування кешу сторінок. Система реалізовується шляхом кешування — модуль представлення генерує сторінку один раз, надалі вона в декілька разів швидше підвантажується з кешу. Процес формування кешу сторінок $Cache=Caching(\vec{y},t,\Delta t)$, тобто $Cache=\left\{\bigcup y_i \middle| y_i\in Y,t+\Delta t,i=\overline{1,n}\right\}$.

УДК 621.394

АНАЛІЗ МЕТОДІВ ОЦІНКИ ЯКОСТІ ПЕРЕДАЧІ МОВНИХ СИГНАЛІВ У ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

Р.П. Шевчук, к.т.н., В.Й. Бегман, студент
Тернопільський національний економічний університет
rsh@tneu.edu.ua

Сучасний етап розвитку телекомунікаційних систем характеризується стрімким ростом технологій передачі мовних сигналів, ключовою проблемою в яких є якість передачі мовних сигналів. На сучасному рівні розв’язання цієї проблеми використовують три підходи: 1) апаратний контроль фізичних параметрів каналів зв’язку; 2) програмне тестування протоколів зв’язку; 3) експертне оцінювання якості прийнятої мовної інформації. Для кожного з підходів розроблено методи оцінки якості передачі мовних сигналів телекомунікаційними системами. У даній роботі проводиться аналіз відомих методів оцінки якості передачі мовних сигналів з метою визначення їх недоліків та перспективних шляхів розвитку.

Всі методи оцінки якості мовних сигналів умовно діляться на суб'єктивні і об'єктивні. Щоб оцінити якість передачі мовного сигналу згідно суб’єктивних методів, потрібно здійснити багато експериментів з різними дикторами і абонентами, а потім усереднити результати вимірювань. Існуючі методи (ГОСТ № 8031-56, ICPIF, MOS) ґрунтуються на залученні людини-експерта для оцінювання розбірливості мови на виході каналу, при якій за шкалу

приймається усереднена оцінка розбірливості мови (Mean Opinion Score, MOS).

Аналіз показує, що існуючі суб'єктивні методи оцінки якості передачі мовних сигналів мають цілий ряд недоліків, до яких в першу чергу слід віднести їхню суб'єктивність, недостатню достовірність та надзвичайно високу вартість.

Для оцінки якості мовного сигналу об'єктивними методами (PESQ, PESQM, ICPIF, E–модель) створені автоматизовані системи контролю якості передачі мовних сигналів. Існуючі методи є високоточними і простими у використанні тільки для оцінки якості послуг телефонії або передачі/приймання мовних сигналів, чого недостатньо, оскільки набір послуг сучасних телекомунікаційних систем є значно ширшим і з року в рік зростає. Перевага даних методів – висока точність при відомих параметрах мережі або з'єднання, але серед недоліків необхідно виділити наступне: методи застосовуються для вимірювання тільки якості мовних сигналів, володіють значною алгоритмічною складністю і недостатньою достовірністю результатів при зміні параметрів мережі.

Проведений у роботі аналіз методів оцінки якості передачі мовних сигналів у телекомунікаційних системах показав, що використання суб'єктивних методів є достатньо дорогим, тому на регулярній основі його можуть дозволити собі лише декілька великих телекомунікаційних компаній у всьому світі. Перед іншими компаніями постає проблема вибору одного з об'єктивних методів, в яких виконується автоматизована оцінка якості мовних сигналів.

Для усунення наведених вище недоліків, методів оцінки якості передачі мовних сигналів, перспективними є дослідження в напрямках: 1) оцінювання якості каналів передачі мовних сигналів; 2) розпізнавання мови; 3) розробки методик та алгоритмів автоматизованої оцінки якості передачі мовних сигналів.

УДК 621.3

ОДНОРІДНА СТРУКТУРА У СКЛАДІ КЛАСИФІКАТОРА СИГНАЛІВ

А.В. Кожем'яко к.т.н., Ю.О. Панасюк студент,
А.В. Лілевський студент
Вінницький національний технічний університет
gotmog666@inbox.ru

Розвиток фотограмметрії в Україні, як і в усьому світі, визначається стрімким зростанням можливостей обчислювальних машин та комп'ютерних технологій. В даний час у всьму світі ведеться активна розробка та дослідне використання цифрових знімаючих приладів, що використовуються для потреб фотограмметрії та картографії. Одним з них є скануюча аерокамера (аеросканер) 3-DAS-1, що розроблений ДНВП „Геосистема".

Основною конструктивною особливістю 3-DAS-1 є наявність трьох скануючих камер (переднього огляду , надірної та заднього огляду) зі своїми об'єктивами та трьохканальними (кольоровими) лінійними ПЗЗ сенсорами у фокальній площині кожного об'єктиву.

У процесі аерофотозйомки виникає проблема своєчасного встановлення присутності завад, а саме - хмар і їх тіней, та повідомлення оператору про необхідність корегування траєкторії польоту. Адже завчасне повідомлення про заваду значно економить час виконання аерофотографічних зйомок у великих масштабах та їх вартість.

Для розв'язання цієї задачі пропонується спроектувати класифікатор сигналів і встановити його на аерофотосканер.

В основу роботи класифікатора сигналів покладено метод розпізнавання, за дискримінантними функціями. З іншого боку відомо, що використання концепції різницевих зрізів, дозволяє спростити структуру і розширити функціональні можливості класифікатора та відмовитись від накопичення дискримінантних функцій.

Класифікатор має однорідну структуру, яка містить m рядків по n комірок у кожному рядку, тобто має вигляд матриці комірок розмірністю mxn. Так як при використанні концепції різницевих зрізів виконується обробка матриці даних по стовпцях, тому і комірки однорідної структури мають переважно вертикальні інформаційні зв'язки. Зв'язки по рядках є керуючими і необхідні для просування (транспозиції) нульових елементів матриці в кінець рядка. Особливістю даної однорідної структури є те, що кожен рядок її містить вихід ознаки нуля даного рядка. Це дає можливість виключити нульовий рядок з подальшої обробки.

Комірка однорідної структури містить мультиплексор, арифметично-логічний елемент, мініматор, два регістри, комутатор, мультиплексор, блок налаштування, до якого входять D-тригер, q-вхідний елемент АБО-НІ, де q - розрядність даних, та елемент затримки.

Реалізація даного класифікатора сигналів планується на елементній базі ПЛІС, а саме схемах сімейства FLEX фірми "Altera".

Готовий пристрій буде монтуватися збоку на корпусі скануючого модуля аерофотокамери під захисною кришкою поряд із блоком живлення.

УДК 621.397

МЕТОД КОРИГУВАННЯ НЕЛІНІЙНОСТІ АЦП

Г.Г. Бортник, к.т.н., доцент
М.Л. Мінов, аспірант
Вінницкий національный техничний університет
minov@bk.ru

Аналого-цифрові перетворювачі (АЦП) знаходять широке використання у сучасних комп'ютерних системах. Використання перетворювачів аналог-код призводить іноді до втрат цифрової інформації. Для відновлення її використовують різні методи коригування.

Можна відмітити, що у n-розрядних АЦП, передатна характеристика має деяку нелінійність, а вхідні напруги змінюються у діапазоні від 0 до U_{FS} та вихідний цифровий код становить $0,1,2,...,N-1$, де $N = 2^n$.

Припустимо, що значення $N_{вих}$ дорівнює k, тоді для АЦП значення вихідного коду $N_{к.вих}$ буде визначатись за формулою:

$$N_{к.вих} = f(n, N_0, N_1, N_2, ..., N_n). \qquad (1)$$

Метод коригування базується на інтерполяційній методиці, яка дає змогу покращити відношення сигнал/шум в АЦП. Коли вихідний сигнал з АЦП $N_{вих}$ буде дорівнювати k, сигнал після цифрової корекції $N_{к.вих}$ буде складати:

$$N_{к.вих} = \frac{1}{2}\frac{n}{M_{FS}}\left(N_n + N_{n+1}\right), \qquad (2)$$

де M_{FS} - повномасштабний код.

Можна відмітити, що цифровий вихідний код $N_{вих}$ поданий в n–розрядній формі, але сигнал після коригування $N_{к.вих}$ отримано у $n+q$–розрядній формі, де $q>0$. Іншими словами відкорегованний сигнал більший на q додаткових розрядів.

На рисунку 1 наведено структуру АЦП з коригуванням нелінійності.

Рис. 1. Структура АЦП з коригуванням не лінійності

Вхідний сигнал $U_{вх}$ поступає на аналоговий ключ (АК), після чого кодується за допомогою АЦП. Отриманий цифровий код $N_{вих}$, поступає до блоку цифрової корекції та до високоточного цифро-аналогового перетворювача (ЦАП). Із ЦАП цифровий код надходить до аналогового ключа (АК) та до ЦПС. У блоці цифрової корекції здійснюється корекція нелінійності АЦП.

Такий метод дозволяє знизити нелінійність аналого-цифрового перетворювача, що в свою чергу збільшує вільний від паразитних складових динамічний діапазон.

УДК 681.32

ТЕХНОЛОГИИ КОНСТРУИРОВАНИЯ МОДЕЛЕЙ MNK-КЛАССА

Т.Н. Боровская, к.т.н., доцент, Е.П. Хомин, аспирант
Винницкий национальный технический университет
taisaborovska@gmail.com

Современные технические системы как объекты оперативного и стратегического управления невозможно рассматривать без учёта их окружения – потребителей и других производителей. Предложена и реализована концепция систем «M производителей, N продуктов, K потребителей», коротко: MNK систем. Формально, MNK система – три системы взаимосвязанных нелинейных разностных уравнений, описывающих поведение каждого производителя, продукта, потребителя. Для того чтобы исследовать, оптимизировать и прогнозировать поведение некоторого предприятия (= бизнес-единицы), моделируем поведение полной системы в режиме «один на фоне всех». В этом режиме задаются среднестатические параметры поведения всех элементов, а для выбранного элемента организуется поиск оптимальных управлений с учётом неопределённостей. Такая модель не может быть создана в рамках традиционных технологий (модели-аппроксимации) и догм «адекватности».

Разработанная модель MNK системы базируется на воспроизведении механизмов (подобных законам физики) поведения элементов, а не аппроксимации статистики (предложено Форрестером). Модель MNK системы разбивается в систему редуцированных (агрегированных без потери информации и упрощённых – с потерей информации) моделей. Вначале создаются редуцированные модели классов «M производителей, 1 агрегированный продукт», «1 производитель, N продуктов», «M производителей, N

продуктов», «L продуктов линейки, K потребителей» и т.д. Каждая последующая модель строится как расширение предыдущей, причём, предыдущие модели остаются в системе моделей – для контроля и аварийной замены более сложной модели, для разработки новых версий. На базе обобщения практического опыта сформирована и реализована концепция метамодели – пары {«множество состояний системы моделей», «нечёткий оператор преобразования состояния системы моделей»}.

Для современных летательных аппаратов, ядерных реакторов характерно создание имитационной модели задолго до создания реального объекта. В авиации, кроме чисто компьютерных моделей широко используют тренажёры: для обучения пилотов: дёшево, эффективно и безопасно. Известные имитаторы производственных систем пока находятся на уровне компьютерных игр. Эти факты выходят за пределы традиционной парадигмы моделирования – догмы «адекватности»: реальный объект должен быть адекватным модели-эталону. Новый подход к моделированию меняет содержание термина «модель- предиктор»: от «что будет, если оставить всё по-прежнему», к «что будет, если использовать другой алгоритм управления системой». Наши технологии позволили это сделать:

УДК 621.391

МЕТОД ПІДВИЩЕННЯ ТОЧНОСТІ ОЦІНЮВАННЯ СКЛАДОВИХ ДЖИТЕРУ В ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ

Г.Г. Бортник, к.т.н., доцент,
М.В. Васильківський, Л.Ф. Мінов
Вінницький національний технічний університет
vmvvin@gmail.com

Використання нових стандартів високошвидкісної передачі даних передбачає підвищення вимог до якості роботи телекомунікаційних мереж. В сучасних мережах зв'язку основним параметром якості роботи є джитер цифрового сигналу.

Для повного дослідження причин виникнення джитеру необхідно комплексно дослідити параметри джитеру у розрізі випадкової та детермінованої складових. Існуючі методи аналізу параметрів джитеру не дають можливості виконувати оцінювання складових джитеру. Тому існує необхідність розробки методу комплексного аналізу складових джитеру, що в свою чергу дозволить підвищити вірогідність результатів практичної діагностики джитеру, направлених на підвищення якості функціонування телекомунікаційних мереж.

У роботі запропоновано метод підвищення точності оцінювання параметрів складових джитеру за допомогою відновлення пропущених значень помилок часових інтервалів (ПЧІ).

Значення загального джитеру J_{TJ} визначається як сума всіх його компонентів згідно виразу:

$$J_{TJ}(i) = J_{DCD}(i) + J_{ISI}(i) + J_{PJ}(i) + J_{RJ}(i) + J_{BUJ}(i), \quad (1)$$

де $J_{DCD}(i)$, $J_{ISI}(i)$, $J_{PJ}(i)$, $J_{RJ}(i)$, $J_{BUJ}(i)$ - параметри джитеру, що спричинені відповідно спотворенням коефіцієнта заповнення імпульсної послідовності, міжсимвольною інтерференцією, періодичними змінами положень фронтів імпульсів, шумовими процесами, перехресними впливами між сусідніми лініями передачі.

Густину розподілення ймовірностей загального джитеру $J_{TJ}(i)$ визначимо як згортку густин ймовірностей всіх його компонентів:

$$f_{TJ}(J) = f_{DCD}(J) \otimes f_{ISI}(J) \otimes f_{PJ}(J) \otimes f_{RJ}(J) \otimes f_{BUJ}(J). \quad (2)$$

Для комплексного аналізу періодичного джитеру, випадкового джитеру та обмеженого некорельованого джитеру використовують спектральну методологію, яка базується на дискретному перетворенні Фур'є. Існуючий метод спектрального аналізу базується на заповненні пропущених значень послідовності ПЧІ методом інтерполяції по найближчим відомим значенням. В результаті інтерпольовані значення ПЧІ ігноруються. Використання інтерполяції невідомих значень послідовності помилок часових інтервалів за найближчими відомими значеннями спотворює спектр ПЧІ у смузі нижніх частот з подавленням амплітуд високочастотних складових. Такі спотворення спектра призводять до погіршення точності оцінювання періодичного, випадкового та обмеженого некорельованого джитерів при використанні спектральної методики аналізу.

Запропонований метод спектрального аналізу, що базується на заповненні пропущених значень послідовності ПЧІ, забезпечує вищу точність у порівнянні з існуючим. Даний метод підвищує точність оцінювання параметрів джитеру в телекомунікаційних системах, що підтверджено комп'ютерним моделюванням процедури оцінювання основних параметрів джитеру.

УДК 004.8

НЕЙРОМЕРЕЖНИЙ КЛАСИФІКАТОР НА БАЗІ ПЕРСЕПТРОНА

Т.Б. Мартинюк, к.т.н., доцент,
І.В. Бондарчук, студент,
Є.В. Дубінін, студент
Вінницький національний технічний університет
inka2lot@rambler.ru

Найбільш простим за структурою вважається класифікатор сигналів на базі багатошарового персептрона. Але в цьому випадку його необхідно доповнити вихідним шаром, який виконує визначення максимального значення дискримінантних функцій g_i, сформованих у прихованому шарі класифікатора у вигляді

$$g_i = \sum_{j=1}^{n} w_{ij} \cdot x_j ,$$

де x_j – j-й компонент вхідного вектора; w_{ij} – відповідний елемент матриці ваг **W** або ваговий коефіцієнт входження j-го компонента x_j до складу i-ї дискримінантної функції g_i.

Таким чином, вихідний шар можна організувати у вигляді відомої нейромережі, наприклад, MAXNET з властивостями визначення максимуму серед її вхідних даних, що дозволить сформувати вихідний вектор **Y** належності вхідного образу до певного i-го класу ($i=\overline{1,m}$). При цьому одиничне значення приймає i-й елемент y_i вихідного вектора.

У даній роботі пропонується варіант реалізації вихідного шару нейромережного класифікатора на базі персептрона. Принцип роботи блока класифікації в якості вихідного шару базується на відомому методі визначення

максимального числа серед масиву чисел у процесі одночасного зменшення всіх числових величин з фіксуванням моменту обнулення і місцезнаходження останнього числа. Структура такого блока класифікації містить m комірок, базовими вузлами яких є лічильник для запису значення дискримінантної функції g_i та RS-тригер для формування значення і-го елемента y_i вихідного вектора, $y_i \in \{0,1\}$.

Працює даний блок за таким принципом. На початку роботи всі RS-тригери встановлено в одиничний сигнал. Вміст усіх лічильників одночасно зменшується на одиницю з надходженням кожного тактового імпульсу. Якщо першим обнулиться і-й лічильник, то на R-вхід відповідного RS-тригера подається одиничний сигнал, який встановлює його у нульовий стан. На прямому виході цього RS-тригера формується нульовий сигнал, який відображає обнулення вмісту даного лічильника. Аналогічним чином відбувається обнулення решти лічильників.

При обнуленні останнього лічильника на R-вхід відповідного RS-тригера подається нульовий сигнал, який не змінює стану цього RS-тригера. Отриманий на прямому виході RS-тригера одиничний сигнал відображає належність вхідних сигналів до відповідного класу за максимумом дискримінантних функцій.

Таким чином, час спрацювання запропонованого блока класифікації залежить від значення максимальної дискримінантної функції, а не від їх кількості.

УДК 681.3; 004.93

КОМП'ЮТЕРНЕ МОДЕЛЮВАННЯ НЕЙРОМЕРЕЖЕВОЇ ІНТЕЛЕКТУАЛЬНОЇ СИСТЕМИ ДЛЯ ЗАДАЧ ПРОГНОЗУВАННЯ СКЛАДОВИХ ХАРАКТЕРИСТИК ПРОФІЛЮ ЛАЗЕРНОГО ПРОМЕНЯ

А.А. Яровий, к.т.н., доцент,
Р.С. Власюк, магістрант, О.В. Крейчі, магістрант
Вінницький національний технічний університет

Лазер як високотехнологічний пристрій вимагає постійного моніторингу роботи. Для якісного використання лазеру необхідно забезпечувати велику точність його роботи. При аналізі його роботи враховується велика кількість даних, починаючи від типу лазеру, потужності лазерного промення (ЛП) і закінчуючи зовнішніми впливами. ЛП, проходячи через атмосферу, піддається величезній кількості зовнішніх впливів. Сумарна вага впливів може призвести до відносно незначного відхилення енергетичного центру лазеру від його очікуваного положення. Через це виникає необхідність прогнозування поведінки ЛП, щоб мати можливість передбачити положення енергетичного центру ЛП хоча б на крок вперед, а в майбутньому і на більш тривалий період.

Тому актуальною є задача побудови інтелектуальних систем для задач профілювання лазерних променів, статистичної обробки та аналізу в реальному часі їх основних параметрів (що можуть бути представлені як часові ряди) при проходженні у зовнішньому середовищі, а також прогнозування відповідних параметрів профілю ЛП.

Попереднє моделювання прогнозування поведінки енергетичного центру ЛП було здійснене за допомогою пакету аналітичних засобів обробки та аналізу данних Deductor 5.2 компанії BaseGroup Labs. В якості інтелектуального засобу обробки данних було використанно нейронні мережі (НМ). Початковими данними було 500 наборів координат енергетичного центру реальних плямових зображень ЛП. На основі проведеного комп'ютерного моделювання та отриманих результатів експериментів було обрано структуру багатошарового персептрона 50-25-12-2, так як вона дозволила отримати більш точний прогноз вихідних координат. В якості алгоритму навчання НМ був використаний алгоритм зворотного розповсюдження помилки. Допустима помилка розпізнавання – 5%.

В результаті НМ було коректно спрогнозовано 98,03% наборів координат енергетичних центрів з навчальної вибірки та 80,67% - тестової. На рис. 1 зображено одну з діаграм відношення, що надає можливість візуально оцінити характер зміни координат енергетичного центру ЛП, та як спрогнозована система відтворює цей характер.

Рисунок 1 – Діаграма відношення

УДК 004.773.5

СИСТЕМА ПЕРЕДАЧІ ПОТОКОВИХ ДАНИХ В КОМП'ЮТЕРНИХ МЕРЕЖАХ

О.Л. Зозовський[1], студент; І.Р. Арсенюк[2], к.т.н., доцент
Вінницький національний технічний університет
[1]alezozov@mail.ru, [2]IgRosArs@gmail.com

Сучасні комп'ютерні мережі дозволяють передавати значні обсяги інформації в тому числі потокової, що дозволяє за допомогою технічних засобів вести контроль та спостерігати за різноманітними процесами.

Дана робота присвячена розробці, трьохрівневої системи передачі, прийому та оброблення аудіо-відео даних.

Перший рівень представлений клієнтом (наприклад, комп'ютером, оснащеним відеокамерою та мікрофоном), який передає дані із певних пристроїв у мережу на наступний серверний рівень системи, який виступає в ролі автомату прийому, оброблення, моніторингу та наступної передачі отриманої інформацію третьому рівню системи, який отримує інформацію і також може бути представлений, наприклад, персональним комп'ютером, підключеним до мережі, мобільним телефоном, КПК чи робототехнічною системою.

Розроблена система є частиною більш глобального проекту з розробки робототехнічної операційної системи, оснащеної машинним зором та штучним інтелектом, в ній і проводиться обмін потоковими даними між роботами по мережі.

Розробка виконувалась з врахуванням багатьох факторів: якості зв'язку, швидкодії, кросплатформеності,

легкості керування та в розрахунку на динамічне розширення усіх трьох рівнів системи. Остання властивість означає можливість оперативного підключення великої кількості будь-яких елементів системи, які можуть вводитись для підвищення швидкодії.

Проект є кросплатформеним і може працювати на багатьох сучасних операційних системах. Існує можливість налаштування сервісу якості даних, а отримане клієнтом відеозображення, може бути масштабоване в зручному для користувача розмірі. Для перегляду аудіо-відео даних потрібні: інтернет-браузер, підключення до мережі та підтримка java-аплетів. При цьому потреба у наявності будь-яких аудіо- та відео- кодеків відсутня. Клієнт може швидко перемикатись на різні „канали” за аналогією телебачення (оскільки одночасно може бути багато трансляцій), поява чи відключення яких динамічно відображається у вікні браузера. Окрім цього перший рівень системи може відсилати текстові повідомлення, які також миттєво будуть відображатись як коментарі до трансляцій.

Таким чином одним із місць застосування програмного комплексу може бути дистанційна освіта (перегляд занять в аудиторіях, конференцій тощо) або інтернет-телебачення.

Система пройшла ряд випробувань у локальній мережі, з калібруванням та налагодженням програмного продукту і показала задовільні результати функціонування. Планується її подальше розширення, вдосконалення та обов’язкове застосування у практичній діяльності.

УДК 004.4

МОДЕЛІ КОМП'ЮТЕРНИХ СИСТЕМ НА БАЗІ КОНЦЕПЦІЇ «РОЗПОДІЛ ВИРОБНИЦТВА»

І.С. Колесник к.т.н., І.І. Михайлова
Вінницький національний технічний університет
M-ineska@yandex.ru

Комп'ютерні системи розвиваються дуже стрімко як нові засоби, що вирішують старі, нові і породжені самими комп'ютерними системами завдання. Сьогодні моделі комп'ютерних систем - інструмент дослідження, проектування, а також і моделі-предиктори для вбудовування в складні системи управління. Виникає проблема створення раціональних технологій конструювання робочих моделей комп'ютерних систем.

У даній роботі будується робоча модель комп'ютерної системи, що виробляє інформаційні «продукти» і послуги. Розглядається система «виробничих» елементів (це можуть бути сервери, комп'ютери користувачів, мікро-контролери). Обрана базова модель - система класу «N виробників, M продуктів, K споживачів». Базове управління в системі розподілене, кожен елемент має «власні цілі», виходячи з яких, формує власні - локальні управління.

Головні програмні модулі: «динаміка елемента», «локальне керування», «динаміка попиту» були розробленими на основі обробки великого обсягу «розсіяних знань». Параметризація структур дозволяє настроювати модель на конкретну комп'ютерну систему.

В модулі «генератор випадкових подій» саме невизначеність диктує методологію і технологію побудови

математичних моделей комп’ютерних систем, а ефективність процесів функціонування та розвитку комп’ютерних систем істотно буде залежати від ефективності імітаційних моделей, які використовуються для тактичного і стратегічного управління.

Невизначеність у прийнятті рішень може трактуватися як результат невизначеності вхідних даних для прийняття рішень, неадекватності математичних моделей процесів. Невизначеність у прийнятті рішень є одним з методів "боротьби" з невизначеністю зовнішнього оточення. Суть такого підходу в тому, щоб в умовах невизначеності робити випадкові експерименти, а потім за їх результатами коригувати ймовірності певних рішень. Це відповідає механізмам навчання в природних соціальних мережах, на цьому базується метод випадкового пошуку. Відомо, що для нормального функціонування адаптивних систем управління потрібні невеликі обурення. На розробленій моделі виявлено існування оптимального рівня збурень для елементів системи.

Сьогодні все більше поширення отримує підхід «математизація задач динаміки і оптимізації». Раціонально сконструйовані програмні модулі можуть розглядатися як оператори, а структури вхідних та вихідних даних як математичні об'єкти.

УДК 62.50:658

МОДЕЛЬ КОМП'ЮТЕРНОЇ СИСТЕМИ НА БАЗІ КОНЦЕПЦІЇ «МАСОВЕ ОБСЛУГОВУВАННЯ»

І.С. Колесник к.т.н., І.І. Михайлова
Вінницький національний технічний університет
M-ineska@yandex.ru

Сьогодні існує велика кількість робіт з тематики управління комп'ютерними системами. Поставлена мета звести різноманітність структур, функцій і специфіки комп'ютерних систем до деякої узагальненої моделі, що параметризується, дозволяє за рахунок налаштування параметрів отримувати адекватні моделі відомих комп’ютерних систем. У даній роботі розглядається побудова такої моделі на базі концепції масового обслуговування. Таку модель гарантовано можливо створити, в середовищі математичних пакетів, якщо використовувати нові інформаційні технології - математизацію завдань оптимізації і моделювання динаміки, різні методи агрегації складних багатовимірних систем.

Процес розробки узагальненої моделі СМО включає розробку моделі невизначеностей, структури даних стану, оператора перетворення. Оператор перетворення стану імітує операції обробки завдань і управління з включенням ситуацій відмов і збоїв.

Розглядаються невизначеності кількості і об'ємів завдань, що поступають на черговому інтервалі обслуговування. У моделі передбачена можливість задавати вигляд і параметри розподілів вірогідності, також імітуються тренди.

Структура стану даних повинна відображати стан

комп’ютерної системи і в загальному випадку є ієрархічною векторною для матриці.Видимий вектор, складений з трьох скалярів і двох матриць.

У базовій моделі відображені наступні пріоритети обслуговування: абсолютний, об'єм завдання, час в черзі, реальний і комплексний час – зважена сума пріоритетів. Структура програмного модуля допускає необмежене поповнення набору пріоритетів.

Оператор переходу між станами складається з функціональних модулів, що імітують логіку процесу обробки вхідних завдань. На малюнку представлений текст модуля «оператор переходу. Модульна структура спрощує його модифікацію.

Програма розрахована на дослідника, аналітика, конструктора моделей. В одній з версій виводяться одночасно процеси для декількох пріоритетів обслуговування. На рис.1 представлений приклад процесу обслуговування задач в черзі з відносним пріорітетом.

Рисунок 1 – Приклад процесу обслуговування задач в черзі з відносним пріорітетом

Отримана робоча і працююча імітаційна модель СМО з довільними дисциплінами обслуговування. Зрештою з моделлю можна оперувати як з простим різницевим рівнянням, проте всі необхідні аспекти поведінки об'єкту упаковані в моделі без втрати адекватності і точності.

УДК 004.896:004.853

КОНЦЕПТУАЛЬНАЯ МОДЕЛЬ СИСТЕМЫ УПРАВЛЕНИЯ МОБИЛЬНЫМ РОБОТОМ

К.К. Кадомский[1], А.А. Каргин[2]
Донецкий национальный университет
[1]kadomsky@ukr.net, [2]kargin@dongu.donetsk.ua

В рамках современной парадигмы естественного интерфейса (natural user interface, NUI) рассматриваются способы эффективного взаимодействия технических программно-аппаратных систем с человеком, в том числе взаимодействия робототехнической системы с оператором (human-robot interaction, HRI). Актуальной является задача интеллектуализации интерфейса робота на основе адаптации и обучения.

В докладе предложена концептуальная модель самообучающейся системы управления (СУ) мобильным роботом на основе жестов. Данная модель является результатом синтеза следующих подходов: теории когнитивных агентов, теории адаптивного резонанса (adaptive resonance theory, ART) и нейроподобных растущих сетей (н-РС). Существуют готовые когнитивные агенты, способные реализовать элементарные функции СУ, т.е. набор предопределенных реакций на простейшие жесты. Ставится задача повышения качества поведения агента в сложных, динамических и нестандартных ситуациях посредством его самообучения. Предлагается применить обобщающие возможности сетей ART и н-РС для выявления и структуризации высокоуровневых знаний в процессе функционирования агента. Основой представления этих знаний является система понятий, т.е.

обобщенных категорий ситуаций, каждой из которых поставлен в соответствие некоторый прототип. Используется нечеткое описание ситуаций на основе признаков; внутреннее представление ситуации либо категории есть набор выпуклых унимодальных нечетких множеств. Поэтому модель может использоваться для обобщения как сенсорного опыта, так и информационных единиц представления знаний нижнего уровня, т.е. прототипов ситуаций, связанных с мотивами, поведениями и эффекторами. В табл. 1 дан простейший пример обобщения для случая 2х нечетких признаков.

Таблица 1. Пример обобщения прототипов

Параметры функции принадлежности	Прототип ситуации					
	Признак 1 (ф-я принадл.)			Признак 2 (ф-я принадл.)		
	Центр	Высота	Концентрированность	Центр	Высота	Концентрированность
Мотив1	0.5	1.0	0.9	0.5	1.0	0.9
Мотив2	0.6	0.8	0.8	0.2	0.2	0.4
Результат	0.54	0.8	0.89	0.45	0.2	0.76

В результате обучения формируются: а) прототипы категорий; б) подмножества признаков, специфичных для каждой категории; в) терм-множества, используемые для определения категорий; г) иерархические связи между категориями. Обучение предлагается реализовать с помощью усовершенствованной модели сети ART, которая кодирует нечеткие категории паттернами активации в ассоциативном слое. Подученные коды категорий служат входными данными для н-РС. Каждая простая категория кодируется единственным элементом ассоциативного слоя обобщенной сети ART, а каждая сложная категория - единственным элементом н-РС. Таким образом, формируется система понятий, организованная по принципам семантической сети, причем проблема пластичности, характерная для н-РС, решена уже на уровне простых понятий.

УДК 621.3

АНАЛИЗ СПИСКА СОЕДИНЕНИЙ СИНТЕЗИРУЕМЫХ HDL – МОДЕЛЕЙ ЦИФРОВЫХ СИСТЕМ

А.Л. Карасёв, ассистент, С.П. Дементьев, студент
Харьковский национальный университет радиоэлектроники
unownn@rambler.ru

Маршрут проектирования современных систем на кристалле обязательно включает в себя выполнение этапа синтеза, а именно переход от RTL описания модели цифрового устройства (на языках описания аппаратуры) к модели, состоящей из внутренних библиотечных элементов системы проектирования. Задача поиска по заданным параметрам (шаблонам) в синтезированном списке соединений является основной при формировании оптимального списка соединений (под оптимальностью понимается удовлетворение требованиям к синтезу, представление результатов синтеза на заданном уровне абстракции и т.д.). Многие из существующих систем проектирования в той или иной мере используют распознавание (поиск) элементов или групп элементов заданным параметрам в списке соединений. Недостаток используемых методов состоит в том, что поиск происходит в последовательном режиме, что сильно замедляет реализацию алгоритмов поиска. Поиск эффективных методов решения данной задачи является актуальной задачей. Вместо последовательного метода предлагается метод параллельного обхода списка соединений с привлечением понятия атрибутов.

Основные положения метода:

Информация о схеме представляется в виде, подобном реляционной базе данных – в виде подмножеств и связей между ними.

Атрибут – способ представления дополнительной информации на линии схемы, то есть это признак, описывающий особенности этой линии: порт, выход триггера, выход комбинационного элемента.

Распространение атрибутов по схеме – это распространение свойств некоторой линии на её приёмников через библиотечные элементы. Прохождение атрибута через библиотечный элемент регулируется определёнными правилами.

Шаблон поиска задаётся в терминах: тип целевого объекта и условия, в которых он должен находиться.

Поиск кандидатов, удовлетворяющих шаблону, происходит путём выбора из заранее сформированных подмножеств определённого типа целевого элемента и анализа условий, в которых он существует.

Необходимо подчеркнуть, что фаза распространения атрибутов выполняется один раз. Метод позволяет на схеме, представленной в виде базы данных после фазы распространения атрибутов находить кандидатов для любого числа шаблонов без повторного распространения атрибутов. Такой подход гарантирует существенное уменьшение суммарного времени на поиск. С помощью данного метода решаются следующие задачи: определение глобальных сигналов синхронизации, асинхронных управляющих сигналов (сброс/установка), определение и анализ доменов синхронизации, проверка правил проектирования, проверка правил тестопригодного проектирования, поиск циклов с обратными связями.

УДК 004.942

ПРОГРАМНІ ЗАСОБИ ФОРМУВАННЯ ПЕРЕДАВАЛЬНОЇ ФУНКЦІЇ ЦИФРОВИХ ФІЛЬТРІВ З ГІПЕРКОМПЛЕКСНИМИ КОЕФІЦІЄНТАМИ

А.М. Царенко, магістрант
Національний технічний університет України
“Київський політехнічний інститут”
next_step@ukr.net

Зважаючи на поширеність цифрових фільтрів в сучасній техніці, в останні роки ведеться значна кількість досліджень, метою яких є покращення їхніх характеристик. Одним з можливих рішень є використання гіперкомплексних числових систем для представлення коефіцієнтів передавальних функцій цифрових фільтрів.

В даній роботі виконана побудова прототипів передавальних функції фільтрів першого порядку з комплексними, подвійними, дуальними, триплексними і квадриплексними коефіцієнтами та фільтрів різних порядків з дійсними коефіцієнтами на мові програмування C++. Проведено порівняння результатів роботи фільтрів з гіперкомплексними та дійсними коефіцієнтами.

Основними блоками цифрового фільтру є суматори, помножувачі та блоки затримки, а також блок формування результату фільтрації. Ці блоки повинні оперувати гіперкомплексними числами різних вимірностей, для кожного випадку – своїми, а також дійсними числами.

Розроблені прототипи фільтрів з гіперкомплексними коефіцієнтами складаються з класу GKNumb, що представляє собою гіперкомплексне число необхідної вимірності. В ньому реалізовані функції ініціалізації та

виводу компонент гіперкомплексного числа. Клас Gfilter реалізує сам фільтр з коефіцієнтами. Він містить методи Fill(), gcomplex_mult(GKNumb A, GKNumb B, GKNumb &res), complex_mult(double a1, double a2, double b1, double b2, double &res1, double &res2), complex_add_sub(bool sign, double a1, double a2, double b1, double b2, double &res1, double &res2), gcomplex_add_sub(bool sign, GKNumb A, GKNumb B, GKNumb &res), Simulate().

Функція Fill(), так само як і конструктор прототипу, присвоює відповідним змінним введені користувачем значення коефіцієнтів передавальної функції, числа відліків вхідного сигналу та самі відліки вхідного сигналу.

Функції gcomplex_mult, complex_mult, complex_add_sub, gcomplex_add_sub реалізують арифметичні операції.

Метод Simulate() моделює роботу фільтра відповідно до його структури. Ця функція об’єднує блоки множення, додавання, затримки, виконує всі операції по формуванню результату і, крім кінцевого результату фільтрації, видає результати на проміжних точках структури фільтра.

Прототип фільтру з дійсними складається з з функцій Fill(), mult(double A, double B, double &res), add_sub(bool sign, double A, double B, double &res), Simulate(), які виконують подібні операції до функцій, що реалізують фільтр з гіперкомплексними коефіцієнтами.

Розробка даних модулів є першим наближенням до побудови універсального модуля, що буде здатний автоматично вибирати гіперкомплексну числову систему, яка підходить для представлення коефіцієнтів передавальної функції цифрового фільтра, і будувати відповідну передавальну функцію по відомій передавальній функції з дійсними коефіцієнтами.

6. ВІДМОВОСТІЙКІ КОМП’ЮТЕРНІ СИСТЕМИ ТА КОМПОНЕНТИ

УДК 004.054; 004.056.55

ДИАГНОСТИЧЕСКАЯ ИНФРАСТРУКТУРА С ИНТЕЛЛЕКТУАЛЬНЫМИ СВОЙСТВАМИ В РЕКОНФИГУРИРУЕМЫХ МУЛЬТИПРОЦЕССОРНЫХ СИСТЕМАХ

Л.В. Дербунович[1], д.т.н., профессор,
Я.Ю. Королева[1], аспирант,
М.А. Бережная[2], к.т.н., доцент
[1]Национальный технический университет "Харьковский политехнический институт"
[2]Харьковский национальный университет радиоэлектроники
vano815@rambler.ru

Современные информационные и субмикронные технологии позволяют создавать экономичные параллельные отказоустойчивые мультипроцессорные системы управления (МПСУ) и обработки данных с реконфигурируемыми структурами, производительность которых сравнима с производительностью мощных суперкомпьютеров типа n-Cube, Cray и им подобных, но со стоимостью в десятки и сотни раз меньшей. Широкое использование сетей (NOC – Network on Chip) и систем (SOC – System on Chip) на одном кристалле, ПЛИС, интеллектуально защищенных интегральных модулей (IP-cores) определяет возможность реализации новой концептуальной модели диагностической инфраструктуры с интеллектуальными свойствами (ДИ-ИС) для тестового, функционального диагностирования МПСУ и восстановления работоспособности путем реконфигурации структуры мультипроцессорной системы.

Предтечей процедуры реконфигурации и восстановления работоспособности является идентификация состояния МПСУ, обнаружение и локализация неисправных модулей (НМ). В концептуальной модели ДИ-ИС предложено интегрировать процедуры и встроенные средства тестового диагностирования (ТД) МПСУ в онлайновом режиме в процессе нормального функционирования системы, что позволяет расширить класс обнаруживаемых дефектов и глубину локализации НМ, осуществлять реконфигурацию системы, поддерживать производительность и отказоустойчивость МПСУ в пределах допустимых технических и технологических норм.

Определены и обоснованы основные задачи ДИ-ИС, а именно: 1) управление процедурами тестового диагностирования параллельно функционирующих процессорных модулей (ПМ); 2) диспетчеризация загрузки ПМ с целью определения периода и продолжительности ТД, потребляемой энергии с учетом допустимого уровня деградации производительности системы; 3) обработка результатов ТД, принятие решения о реконфигурации системы и восстановления работоспособности. Управление процессами оптимизации производительностью МПСУ, процедурами ТД и реконфигурации осуществляется двумя диагностическими модулями, которые представляют собой двухленточные автоматы с магазинной памятью (МП-автоматы) с входной и выходной лентами, магазинной памятью тестовых последовательностей, модуля управления и принятия решений. Показано применение концептуальной модели и архитектур ДИ-ИС при создании МПСУ ростовыми установками для выращивания крупногабаритных монокристаллов в опытном производстве Института сцинтилляционных материалов НАН Украины г. Харьков.

УДК 004.054; 004.056.55

СИНТЕЗ САМОПРОВЕРЯЕМЫХ МОДУЛЕЙ ЗАЩИТЫ ДАННЫХ С ИСПОЛЬЗОВАНИЕМ САМОДВОЙСТВЕННЫХ ФУНКЦИЙ

Л.В. Дербунович[1], д.т.н., профессор,
Д.Г. Караман[2], аспирант
Национальный технический университет
"Харьковский политехнический институт"
[1]derbunovich@gmail.com
[2]karaman.dmitry@gmail.com

Практика применения устройств защиты информации показывает их чувствительность к сбоям и ошибкам, возникающим в процессе их функционирования, а также уязвимость к новому классу атак, основанных на искусственном вызове сбоев при функционировании устройства, существенно упрощает взлом атакуемого устройства.

Описанные проблемы решаются применением различных средств встроенного контроля, реализующих методы функционального диагностирования (ФД) исправности устройств.

Наиболее эффективным методом ФД является использование самопроверяемых цифровых устройств, в которых одновременно проверяется исправность функциональной части и средств контроля устройства.

Для обеспечения свойства самопроверяемости предложено использовать самодвойственные функции (СФ).

Функция называется самодвойственной, если она обладает следующим свойством:

$$f(x_1, x_2, ..., x_n) = \overline{f}(\overline{x}_1, \overline{x}_2, ..., \overline{x}_n)$$

где $x_1, x_2, ..., x_n$ и $\overline{x}_1, \overline{x}_2, ..., \overline{x}_n$ – поразрядно взаимно инверсные входные наборы. Это свойство СФ положено в основу системы встроенного функционального контроля аппаратной реализации самопроверяемого подстановочного блока алгоритма шифрования Rijndael (рис. 1).

Рис. 1. Структурная схема самопроверяемого подстановочного блока.

Проведено исследование возможности применения СФ для синтеза самопроверяемых схем дискретных устройств, которые могут использоваться при разработке криптографических модулей с встроенным самоконтролем.

Показано, что самопроверяемые схемы, построенные на базе самодвойственных функций, позволяют эффективно использовать международный стандарт проектирования IEEE1149.1÷4 (граничное сканирование) и IEEE P1500 (встроенное самотестирование) и своевременно обнаруживать одиночные константные неисправности на входах и внутренних соединениях схемы. Предложенные самопроверяемые схемы подстановочных блоков обладают минимальной аппаратной и временной избыточностью среди аналогичных решений.

УДК 681.3.06

ОБНАРУЖЕНИЕ И ИСПРАВЛЕНИЕ ОШИБОК В ПЕРЕСТАНОВКАХ

А.А. Борисенко, д.т.н., профессор,
А.Е. Горячев, аспирант, Е.Л. Онанченко, к.т.н., доцент
Сумский государственный университет
electron@sumdu.edu.ua

Перестановки нашли широкое применение для решения задач комбинаторной оптимизации, при помехоустойчивой передаче данных и защите их от несанкционированного доступа. В процессе передачи перестановок между узлами использующего их устройства, либо между различными устройствами, возможно возникновение ошибок в перестановке, что является недопустимым, так как может привести к потере данных.

Перестановки обладают помехоустойчивостью, которая обеспечивается их структурной избыточностью. Одним из способов обнаружения ошибок, использующих структурную избыточность перестановок, является метод контроля суммы элементов перестановки. Сумма всех элементов перестановки порядка n вычисляется с помощью следующей формулы:

$$P = n\,(n - 1) + \ldots + 2 + + 1 = n\cdot(n+1)/2, \qquad (1)$$

Если сумма элементов проверяемой перестановки не равна P, значит перестановка содержит ошибку. В этом случае исправить ошибку можно с помощью повторной передачи всей перестановки.

Рассматриваемый метод позволяет выявлять не все возможные ошибки. Это объясняется тем, что помимо случаев, когда одна перестановка переходит в другую

(например, 12345 → 12354), не выявляются ошибки при переходах вида 12345 → 13344, так как в обоих случаях сумма элементов на выходе равна P.

Достоинством метода является хорошее быстродействие, сохраняющееся при проверке перестановок высокого порядка.

Наиболее простым способом исправления однократных ошибок в перестановках, не требующим повторной передачи, является добавление контрольной суммы по модулю 2 к каждому из элементов перестановки. Данный метод вносит наименьшую избыточность (1 бит на элемент).

При возникновении однократной ошибки в перестановке, один из её элементов перейдёт либо в другой элемент, либо в запрещённый элемент. Данная ошибка может быть обнаружена проверкой контрольных сумм всех элементов. Для исправления ошибки необходимо определить, какой из элементов отсутствует в полученной перестановке, и заменить им ошибочный элемент. Найти отсутствующий элемент можно с помощью контрольной суммы элементов перестановки. Эта сумма, как было замечено ранее, является постоянной величиной для всех перестановок одного порядка и определяется по формуле (1). Путём вычитания из контрольной суммы значений всех правильно принятых элементов перестановки, можно получить верное значение элемента перестановки, содержащего ошибку. Данным значением заменяется значение ошибочного элемента перестановки.

Следует отметить, что с помощью метода суммы по модулю 2 невозможно обнаруживать ошибки в одном элементе кратности 2. Для обнаружения таких ошибок можно комбинировать данный метод с другими методами обнаружения ошибок.

УДК 681.188

ПРИНЦИПЫ ПОСТРОЕНИЯ ДЕШИФРАТОРОВ РАВНОВЕСНЫХ КОДОВ

А.А. Борисенко, д.т.н, профессор,
Д.В. Гутенко, аспирант
Сумский государственный университет
Wista07@mail.ru

Равновесные коды широко применяются для передачи данных, и поэтому синтез дешифратора для работы с равновесными комбинациями был бы полезен при разработке устройств передачи данных. Поскольку часть кодовых комбинаций не поступает на вход дешифратора, то она может быть использована для минимизации дешифратора.

Так как при поступлении какой-либо комбинации с *k*-единицами на вход такого дешифратора, на выходе соответствующему входной комбинации будет единица, а на входах, соответствующих всем остальным равновесным комбинациям нули, то для функции *F*, характеризующей значения на каком-либо выходе дешифратора, будет иметь единичное значение для одной комбинации с *k*-единицами n-разрядного набора, для всех остальных C_n^k-1 возможных комбинаций с *k*-единицами, значение функции будет принимать нулевое значение. Так как предполагается, что на вход дешифратора поступают только комбинации, содержащие *k*-единиц, то для всех других комбинаций n-разрядного кода (содержащих больше или меньше единиц чем *k*), значение функции *F* неопределенно. Это свойство может быть использовано для минимизации функции *F*.

Оценка Квайна для простого одноступенчатого дешифратора, достаточного для работы с равновесным кодом k из n равна

$$C_1 = n \cdot C_n^k.$$

Для найденного дешифратора равновесных кодов оценка Квайна:

$$C_2 = \begin{cases} k \cdot C_n^k, k \le \dfrac{n}{2}, \\ (n - k) \cdot C_n^k, k > \dfrac{n}{2}. \end{cases}$$

При сравнении оценки Квайна простого одноступенчатого дешифратора с дешифратором равновесного кода *k* из *n* получим соотношение:

$$\frac{C_1}{C_2} = \begin{cases} \dfrac{n}{k}, k \le \dfrac{n}{2}, \\ \dfrac{n}{(n-k)}, k > \dfrac{n}{2}. \end{cases}$$

Благодаря минимизации функций для каждого выхода дешифратора, полученный дешифратор будет характеризоваться уменьшением аппаратурных затрат более чем в 2 раза по сравнению с простым одноступенчатым дешифратором, но для его корректной работы необходимо поступление только равновесных комбинаций, соответствующей равновесному коду, для работы с которыми данный дешифратор предназначен. При поступлении на вход комбинации, несоответствующей равновесному коду, данный дешифратор сработает некорректно.

УДК 621.38

ОЦЕНКА ПОМЕХОУСТОЙЧИВОСТИ МАТРИЧНЫХ БИНОМИАЛЬНЫХ КОНЕЧНЫХ АВТОМАТОВ

А.А. Борисенко, д.т.н., профессор,
В.В. Петров, аспирант, С.Ю. Булатов, студент
Сумской государственный университет
electron@sumdu.edu.ua

Цифровые автоматы широко используются в различных прикладных цифровых системах и устройствах, особенно при проектировании систем на кристаллах.

Существует несколько способов кодирования состояний конечного автомата: OHE, Gray, Compact, Johnson, Sequential. Согласно исследованию OHE применительно к ПЛИС с архитектурой FPGA дает возможность строить конечные автоматы, которые в общем случае требуют меньших ресурсов и отличаются более высокими скоростными показателями, чем аналогичные конечные автоматы с двоичным кодированием состояний.

Суть метода OHE состоит в применении 1 из n кодирования состояний автомата.

Код OHE является схожим с матричного биномиальным кодом с параметром $k = 1$. Отличие матричного биномиального кода состоит в том, что он содержит комбинацию со всеми нулями. Пример комбинаций матричного код с параметрами $n = 3$, $k = 1$ 000, 100, 010, 001.

Достоинство матричных биномиальных автоматов состоит в высоком быстродействии и помехоустойчивости, которая проявляется в содержании естественной избыточности. Вторым немаловажным достоинствам

является простота устройства контроля таких автоматов. Разработанные устройства контроля позволяют детектировать запрещенные состояния в течение того же такта, в котором они возникли.

Интересной задачей является оценка помехоустойчивости матричных биномиальных автоматов.

Для оценки автомата применена модель, в которой абсолютно надежное цифровое устройство выбирает выходные символы в момент t из ансамбля X. Однако выходные символы выбираются из некоторого ансамбля E, причем выбор происходит без задержек. В результате имеется модель, в которой реализован канал связи с шумом и нулевой задержкой

Для оценки помехоустойчивости автоматов применена методика, согласно которой любая из M разрешенных кодовых комбинаций из общего числа $N > M$ может перейти в класс правильных комбинаций, класс из $N - M$ запрещенных комбинаций с обнаруживаемыми ошибками и класс из $M - 1$ разрешенных комбинаций с не обнаруживаемыми ошибками. Соответственно вероятности переходов кодовых слов Z+V+I =1, где Z, V и I представляют собой вероятности переходов кодовых слов в запрещенные, разрешенные, ошибочные слова и в самих себя.

Для равновероятного появления состояний автомата, вероятность не обнаруживаемой ошибка равна:

$$V = \frac{1}{n+1}\left(\left((n-1)p_{10} \cdot p_{01} \cdot p_{00}^{n-2} + p_{10} \cdot p_{00}^{n-1}\right)n + p_{10} \cdot p_{00}^{n-1} \cdot n\right),$$

где n - разрядность автомата; p_{10}, p_{01}, p_{00} вероятности переходов соответственно $1 \to 0$, $0 \to 1$, $0 \to 0$.

Таким образом, проведена оценка помехоустойчивости матричных биномиальных автоматов с параметром $k = 1$ по критерию вероятности не обнаруживаемой ошибки.

УДК 004.387:621.3.087.92

ПЕРЕТВОРЕННЯ «АНАЛОГ – РОБОЧИЙ КОД – ЦИФРОВИЙ ЕКВІВАЛЕНТ» В АЦП, ЩО САМОКАЛІБРУЮТЬСЯ, З ВАГОВОЮ НАДЛИШКОВІСТЮ

О.Д. Азаров[1], д.т.н., професор, О.В. Кадук[2], асистент, А.Г. Бас[3], студент
Вінницький національний технічний університет
[1]azarov1@vstu.vinnica.ua
[2]k67alex@yahoo.com
[3]artem_bus@inbox.ru

Аналого-цифрові перетворювачі відносяться до класу перетворювачів форми інформації (ПФІ), що широко застосовуються в різних галузях людської діяльності, а саме: багатоканальних системах збору даних, апаратурі для контролю систем теле- і радіомовлення, для сейсморозвідки та ін. Використання вагової надлишковості та самокалібрування дозволяє створювати високоточні відмовостійкі АЦП, побудовані на неточних елементах. До того ж, такий підхід дає можливість значно скоротити час перетворення і підвищити швидкодію за рахунок компенсації динамічних похибок першого і другого роду.

Водночас, у АЦП з ваговою надлишковістю по суті використовуються три системи числення (СЧ): базова СЧ із ваговою надлишковістю (СЧВН), робоча СЧВН і зовнішня СЧ, що переважно є двійковою. При цьому виникає задача перетворення робочого коду в його цифровий еквівалент ($N_P \to K_{BX}$). Так, узагальнена операторна схема АЦ-перетворення з ваговою надлишковістю може бути представлена таким чином:

$$A_{BX} \to A_K \to N_P \to K_{ВИХ}(A_K),$$

де A_{BX} – це вхідний аналоговий сигнал; A_K – компенсуючий аналоговий сигнал, $N_P \in \{a_{n_\alpha-1},...,a_1,a_0\}$ – робочий код; $K_{ВИХ}(A_K)$ – цифровий еквівалент компенсуючого аналогового сигналу. Структурну схему обчислювального перетворювача порозрядного наближення $N_P \to K_{BX}$ показано на рис. 1. Тут ОП – блок оперативної пам'яті, ЦК – керований цифровий комутатор, БК – блок керування, См – нагромаджувальний суматор, РгР – регістр результату.

Рис. 1. Пристрій обчислення $K_{ВИХ}$ для АЦП порозрядного наближення з ваговою надлишковістю

Обчислення $K_{ВИХ}$ у вище наведеному перетворювачі не зменшує швидкодію АЦП, оскільки здійснюється одночасно і послідовно такт за тактом з порозрядним АЦ-врівноваженням.

Варто відзначити, що реалізація вказаного перетворення $N_P \to K_{BX}$ здійснюється з використанням відомих обчислювальних вузлів, що працюють у двійковій системі числення. Це не вимагає побудови оригінальної елементної бази і дозволяє застосовувати серійні цифрові мікросхеми.

УДК 004.387:621.3.087.92

ПЕРЕТВОРЕННЯ «ЦИФРОВИЙ ЕКВІВАЛЕНТ – РОБОЧИЙ КОД – АНАЛОГ» В ЦАП, ЩО САМОКАЛІБРУЮТЬСЯ, З ВАГОВОЮ НАДЛИШКОВІСТЮ

О.Д. Азаров[1], д.т.н., професор,
О.В. Дудник[2], магістрант, А.О. Росощук, студент
Вінницький національний технічний університет
1azarov1@vstu.vinnica.ua
2dudniksasha@mail.ru

Застосування багаторозрядних ЦАП паралельної структури в інформаційно-вимірювальних системах, багатоканальних системах збору даних, системах управління та інше вимагає дотримання їх метрологічних характеристик протягом всього циклу експлуатації, а також при роботі у складних умовах. При цьому у вказаних пристроях можуть виникати параметричні відмови. Для нівелювання впливу параметричних відмов на характеристики перетворювача використовується процедура цифрового самокалібрування, що можлива при побудові ЦАП на основі систем числення з ваговою надлишковістю (СЧВН).

Разом з цим, у ЦАП із ваговою надлишковістю фактично використовуються три системи числення (СЧ): базова СЧВН, робоча СЧВН і зовнішня СЧ, що переважно є двійковою. Також слід зазначити, що таке ЦА-перетворення є специфічним і дещо відрізняється від аналогічної процедури для двійкової СЧ. Відмінністю, при цьому, є наявність проміжного перетворення цифрового

еквіваленту (ЦЕ), що зображується класичним двійковим кодом в робочий код.

Узагальнена операторна схема ЦА-перетворення виглядає, як $K_{BX} \to N_P \to A_{ВИХ}$, де $A_{ВИХ}$ – це вихідний аналоговий сигнал, K_{BX} – ЦЕ вхідного двійкового коду. Узагальнену структурну схему обчислювального перетворювача порозрядного наближення $K_{BX} \to N_P$ для ЦАП із ваговою надлишковістю показано на рис. 1. Тут ЦСП – цифрова схема порівняння, Рг – регістр, ЦК – цифровий комутатор, БК – блок керування, См – нагромаджувальний суматор, РгР – регістр результату.

Рис. 1. Пристрій формування робочого коду N_P у ЦАП із ваговою надлишковістю

Перетворення K_{BX} у N_P здійснюється послідовно за n_α тактів, де n_α – розрядність α-ЦАП. На початковому етапі, по команді БК K_{BX} подається в регістр Рг. Далі по команді БК і за допомогою ЦК з пам'яті вибирається код ваги розряду $K(Q_i)$. На См відбувається віднімання значення $K(Q_i)$ від K_{BX}, що знаходиться в Рг. На основі аналізу результату операції віднімання на ЦСП у РгР формуються розрядні коефіцієнти N_P – a_i, а в Рг відбувається запис значення результату операції віднімання.

УДК 681.3

ВИСОКОТОЧНІ ФУНКЦІОНАЛЬНІ ГЕНЕРАТОРИ АНАЛОГОВИХ СИГНАЛІВ НА ОСНОВІ ЦАП З ВАГОВОЮ НАДЛИШКОВІСТЮ

О.Д. Азаров[1], д.т.н., професор,
В.В. Рибак[2], аспірант
Вінницький національний технічний університет
[1]azarov@vstu.vinnica.ua, [2]vovarybak@gmail.com

Застосування комп'ютерів у різних галузях людської діяльності вимагає постійного вдосконалення, поліпшення характеристик існуючих та розробки нових типів аналого-цифрових та цифроаналогових перетворювачів (АЦП та ЦАП). До недоліків відомих обчислювальних перетворювачів можна віднести складність пристроїв і, як наслідок, збільшені апаратні витрати при їх схемотехнічній реалізації. При цьому, у випадку застосування додаткових аналогових і аналого-цифрових вузлів на точність роботи пристрою істотно впливають похибки елементної бази. Проте у теперішній час розроблено багато різних способів підвищення точності та лінійності перетворювачів та генераторів. Вони можуть бути розділені на два напрямки. Перша група методів підвищення точності АЦП ґрунтується на застосуванні прецизійних технологій виготовлення аналогових вузлів, що вимагає більших матеріальних витрат і не завжди гарантує часову й метрологічну стабільність. Другий напрямок – це методи підвищення точності АЦП, що базуються на введенні надлишковості на різних рівнях проектування пристроїв: функціонально-

алгоритмічному, інформаційному й структурно-схемотехнічному.

В високоточному функціональному генераторі аналогових сигналів на базі ЦАП із ваговою надлишковістю пропонуємо використати систему числення на базі чисел Фібоначі, що дозволить компенсувати похибки завдяки надлишковості, яка наявна у даній системі числення. Ваги розрядів відповідного ЦАП будуть обчислюватися за рекурентною формулою $F_1 = 1, \quad F_2 = 1, \quad F_{n+1} = F_n + F_{n-1} \quad n \in N$. Але, в реальному ЦАП ваги розрядів відрізняються від ідеальних $Q_i = Q_{i\,эä} + \Delta Q_i$, де допустима похибка обчислюється за формулою $\partial Q_{Ä} = \frac{\Delta Q_i}{\Delta Q_i}$. І, в результаті внесених похибок згенерований лінійний сигнал виглядає так, як зображено на рисунку. Для усунення розривів спочатку знаходяться граничні кодові комбінації, а потім, в залежності від типу розриву вносяться корективи по одному із двох алгоритмів:

- ігноруємо деякий набір кодових комбінацій
- переводимо генератор в режим роботи із забороною ввімкнення старшого розряду.

В результаті вищеописаного цифрового калібрування отримуємо лінійний сигнал без розривів та зміщень. Це дозволяє значно підвищити лінійність функціонального сигналу генератора на основі ЦАП із ваговою надлишковістю.

УДК 681.3:621.375

МОДЕЛІ АЧХ І ФЧХ ДВОТАКТНИХ ПІДСИЛЮВАЧІВ СТРУМУ НА ОСНОВІ СХЕМ ЗАМІЩЕННЯ ТРАНЗИСТОРІВ У ФОРМАТІ SPICE

О.Д. Азаров, д.т.н., професор, В.А. Гарнага, аспірант, М.Ю. Теплицький, студент
Вінницький національний технічний університет
misha_pirate@ukr.net

Проектування аналогових інтегральних схем в значній мірі базується на комп'ютерному моделюванні, при цьому для розрахунків схем використовуються чисельні методи. Це пов'язано із тим, що системи аналітичних рівнянь, якими можуть описуватися аналогові схеми є досить складними. Водночас для використання пакетів схемотехнічного моделювання таких як MicroCap, OrCAD та інших потрібна деталізована бібліотека елементів у форматі SPICE, яка містить схеми заміщення відповідних компонентів. Для цього необхідна наявність адекватних математичних моделей компонентів, а також відповідних схем заміщення, зокрема, малосигнальних. Водночас слід відзначити, що при моделюванні активних компонентів (діодів, транзисторів і т. ін.) і побудові їх малосигнальних математичних моделей засобами схемотехнічного аналізу, рекомендується введення в схеми заміщення керованих генераторів сигналів (КГС) (струм-струм IofI, струм-напруга UofI, напруга-напруга UofU, напруга-струм IofU), що дозволяє отримати точніші результати моделювання.

Додатково необхідно зазначити, що аналіз схем заміщення із такими генераторами сигналів у літературі

розглянуто недостатньо, а їх використання має свою специфіку і вимагає особливих правил вибору конфігурації схеми.

Рисунок 1 – Малосигнальна схема заміщення для транзисторного каскаду загальна база із КГС

Побудова математичних моделей електронних схем базується на використанні схем заміщення окремих компонентів. При цьому для побудови АЧХ і ФЧХ потрібні так звані П- або Т-подібні малосигнальні схеми заміщення транзисторів. Вони можуть бути отримані зі схем заміщення для великого сигналу з використанням частини елементів останніх, а також заміною p-n переходів еквівалентними резисторами. Автори пропонують універсальний підхід до побудови малосигнальних схем заміщення – уведення в них керованих генераторів струму (КГС). При коректному виборі точок підключення давачів таких генераторів, автоматично враховуються внутрішні зворотні зв’язки транзисторів і відповідно відсутня потреба в коригуванні параметрів фізичних моделей.

УДК 681.32

АЦП ПОРОЗРЯДНОГО НАБЛИЖЕННЯ З АНТИГЛІЧЕВИМ КОДУВАННЯМ

О.Д. Азаров, д.т.н., професор, О.Г. Муращенко
Вінницький національний технічний університет
oleksandr.g.m@gmail.com

Традиційно в техніці багаторозрядного (n ≥ 12 двійкових розрядів) аналого-цифрового і цифро-аналогового перетворення існують дві основні задачі. Перша – це зменшення відносної похибки перетворення, тобто підвищення точності. Друга – це зменшення часу перетворення, тобто підвищення швидкодії.

Тривалість аналого-цифрового перетворення $T_{пер}$ складається з суми тривалості тактів врівноваження, причому значення t_T тривалості такту для двійкового ЦАП повинна бути такою, щоб похибка усталеного компенсуючого сигналу $A_к(t)$ на кожному такті була мінімальною і не перевищувала половини молодшого кванту $A_к(t) \leq 0{,}5Q_0$. Якщо перехідний процес, за яким змінюються у часі ваги розрядів, що перемикаються, відповідає схемній функції I порядку, то відносна похибка усталення дорівнює $\delta Q = e^{-t_T/\tau}$. Звідси $t_T = -\tau \cdot \ln \delta Q$. Для певних кількостей розрядів існують певні значення t_T і $T_{пер}$, зменшення яких може призвести до появи зон розривів, які неможливо компенсувати в умовах відсутності вагової надлишковості. Водночас у випадку застосування систем числення з ваговою надлишковістю можна компенсувати значні похибки усталення ваг розрядів і таким чином звести на останньому такті врівноваження динамічну похибку так, щоб виконувалась умова $A_к(t) \leq 0{,}5Q_0$. В свою чергу

можливість компенсації похибки дозволяє скоротити t_T і в результаті значно зменшити загальний час перетворення. Наприклад у випадку класичного 6-ти розрядного перетворення при $\alpha = 2$ мінімальна тривалість $t_T = 4{,}18\tau$, а час перетворення $T_{пер} = 25{,}08\tau$. Якщо $\alpha = \sqrt{2} \approx 1{,}414$, то тривалість такту можна зменшити до $t_T = 0{,}97\tau$. При цьому порівняно з двійковою СЧ еквівалентне число розрядів збільшиться до $n_\alpha = 12$ і відповідно до цього збільшиться і число тактів врівноваження. Незважаючи на це загальний час одного перетворення не перевищить $T_{пер} = 11{,}64\tau$. Таким чином протягом часу для класичного випадку встигне реалізуватись два прискорених перетворення, а отже для $\alpha = \sqrt{2}$ маємо вдвічі більшу швидкодію.

Отже використання вагової надлишковості дозволяє істотно зменшити динамічні похибки і водночас значно зменшити загальний час перетворення. В той же час застосування систем числення з ваговою надлишковістю дозволяє здійснювати антиглічеве кодування у ході порозрядного аналого-цифрового перетворення. У свою чергу відсутність глічів дозволяє додатково підвищити швидкодію АЦП із ваговою надлишковістю, що працюють за прискореними алгоритмами. Слід відзначити, що «природним» антиглічевим алгоритмом порозрядного аналого-цифрового перетворення є алгоритм «тільки вмикання». Проте реалізація такого алгоритму вимагає системи числення з ваговою надлишковістю із знакорозрядними коефіцієнтами $\{\bar{1}, 1\}$. Це, в свою чергу, можна реалізувати тільки при застосуванні двох ЦАП протилежної полярності, що збільшує кількість аналогового обладнання.

У ході дослідження доведено, що антиглічевий алгоритм можна реалізувати, використовуючи систему числення з ваговою надлишковістю з розрядними коефіцієнтами $\{0, 1\}$.

УДК 681.3:621.375

КОМПЕНСАЦІЯ ДИНАМІЧНИХ ПОХИБОК ПРИ ПРИСКОРЕНОМУ ПОРОЗРЯДНОМУ АНАЛОГО-ЦИФРОВОМУ ПЕРЕТВОРЕННІ З ВАГОВОЮ НАДЛИШКОВІСТЮ

О. Д. Азаров д.т.н., професор,
М. Ю. Шабатура, магістрант
Вінницький національний технічний університет
smydev@gmail.com

Одним з перспективних напрямків розвитку АЦП порозрядного наближення є їхня побудова з використанням надлишкових позиційних систем числення (НПСЧ).

У НПСЧ використовується недвійкова основа системи числення $1<\alpha<2$, а ваги розрядів представляються у вигляді $Q_i = q.a^i$, де q – вага молодшого розряду.

Будь-яке дійсне число може бути представлене в НПСЧ у вигляді суми ваг розрядів:

$$X = \sum_{i=0}^{N} a_i \cdot q \cdot \alpha^i ,$$

де a∈(0;1) - двійковий і-ий біт N- розрядного результату перетворення. У НПСЧ існує декілька кодових еквівалентів для представлення числа, на відміну від двійкової при якій число представляється одним кодовим еквівалентом.

До НПСЧ відноситься так званий код "золотої пропорції" з основою $\alpha = \left(\sqrt{5}+1\right)/2 \approx 1{,}618$. "Золота пропорція" є границею відношень двох сусідніх чисел ряду Фібоначчі :

$$\alpha = \lim_{i\to\infty} \frac{F_i + 1}{F_i} .$$

Основна перевага НПСЧ, реалізована при аналого-цифровому перетворенні полягає у відсутності "розривів" у перетворювальній характеристиці, викликаних відхиленнями реальних ваг розрядів від їхніх розрахункових значень. Для двійкових АЦП ці відхилення не повинні перевищувати половини молодшого розряду. Для АЦП на основі "золотої пропорції" відносна похибка ваг розряду за рахунок технологічних, температурних, часових факторів може досягати до 23,6%, що не приведе до пропусків кодів. Отже, є можливість, знаючи точні значення реальних ваг розрядів, що беруть участь у перетворенні, одержати точне значення вхідного аналогового сигналу.

В АЦП на основі НПСЧ поява помилок типу "невмикання" розряду компенсується на наступних тактах перетворення за рахунок включення групи більш молодших розрядів.

До складу динамічних характеристик аналого-цифрового перетворення входять, зокрема, динамічні похибки першого і другого роду. Динамічна похибка першого роду $\Delta Ад^{I}$ обумовлена інерційністю аналогових і цифрових вузлів тракту аналого-цифрового врівноваження, динамічна похибка другого роду $\Delta Ад^{II}$ – зміна рівня вхідного аналогового сигналу $A_{вх}$ за час врівноваження. Дослідження зазначених похибок може здійснюватися: за допомогою спеціальної вимірювальної апаратури, або за допомогою комп'ютерного моделювання.

УДК 681.513

МЕТОД КОМПЕНСАЦИИ ПОМЕХ В АДАПТИВНЫХ АНТЕННЫХ РЕШЕТКАХ

В.М. Кичак д.т.н., професор, И.Ю. Кравцов магистр
Винницкий национальный технический университет

Вопросы построения адаптивных антенных решеток (ААР) для пространственно-временной обработки сигналов являются актуальными при функционировании радиосредств различного назначения. Это связано с постоянно возрастающей плотностью размещения радиосредств и повышениям интенсивности их использования.

Целью данного доклада является анализ исследования метода компенсации помех на основе нахождения минимума среднеквадратичной ошибки с использованием коэффициента предельного подавления для одной из функциональных схем адаптивных антенных решеток и подтверждение предположения о симметричности и равенстве соответственных весовых коэффициентов.

Коэффициент предельного подавления определяется как отношение мощности сигнала помехи на выходе к значению мощности в нерегулируемом канале.

$$K_{пред} = \frac{\sigma_{\varepsilon}^{2}}{\sigma_{0}^{2}}.$$

При этом предположим, что полезный сигнал отсутствует и на вход поступает только сигнал помехи. Набор весовых коэффициентов, обеспечивающих максимально возможное подавление, называется оптимальным $W_{оптим}$, а коэффициент подавления при этом предельным.

Рассматривался случай линейного симметричного и эквидистантного распределения элементов ААР. В результате были получены аналитические выражения коэффициента предельного подавления и значения оптимальных весовых коэффициентов:

$$K_{пред} = 1 - \frac{2\rho(\tau) - 2\rho^2(\tau)\rho(2\tau)}{1 - \rho^2(2\tau) - \hat{\rho}^2(2\tau)} -$$

$$- \frac{4\rho(\tau)\hat{\rho}(\tau)\hat{\rho}(2\tau) + 2\hat{\rho}^2(\tau) + 2\hat{\rho}^2(\tau)\rho(2\tau)}{1 - \rho^2(2\tau) - \hat{\rho}^2(2\tau)} = 1 - \frac{2k^2(\tau)}{1 + k(2\tau)};$$

$$W_{1opt} = \frac{\rho(\tau) - \rho(\tau)\rho(2\tau) - \hat{\rho}(\tau)\hat{\rho}(2\tau)}{1 - \rho^2(2\tau) - \hat{\rho}^2(2\tau)} = \frac{k(\tau)}{1 + k(2\tau)} \cos\omega_0\tau;$$

$$W_{2opt} = \frac{-\hat{\rho}(\tau) + \rho(\tau)\hat{\rho}(2\tau) - \hat{\rho}(\tau)\rho(2\tau)}{1 - \rho^2(2\tau) - \hat{\rho}^2(2\tau)} = -\frac{k(\tau)}{1 - k(2\tau)} \sin\omega_0\tau;$$

$$W_{3opt} = \frac{\rho(\tau) - \rho(\tau)\rho(2\tau) - \hat{\rho}(\tau)\hat{\rho}(2\tau)}{1 - \rho^2(2\tau) - \hat{\rho}^2(2\tau)} = \frac{k(\tau)}{1 + k(2\tau)} \cos\omega_0\tau;$$

$$W_{4opt} = \frac{\hat{\rho}(\tau) - \rho(\tau)\hat{\rho}(2\tau) - \hat{\rho}(\tau)\rho(2\tau)}{1 - \rho^2(2\tau) - \hat{\rho}^2(2\tau)} = \frac{k(\tau)}{1 - k(2\tau)} \sin\omega_0\tau.$$

Анализирую выражения приходим к выводу, что предположение симметричности и равенстве соответственных весовых коэффициентов верно при подавлении помеховых сигналов, носящих как детерменированний, так и случайный характер. Проведенная оценка характера изменения коэффициента предельного подавления от величины τ, с использованием огибающей вида $k(\tau) = e^{-\alpha\tau^2}$, показала, что с увеличением τ увеличивается коэффициент предельного подавления. Величина τ задавалась в периодах несущей частоты.

УДК 681.322

ПІДВИЩЕННЯ ЗАВАДОСТІЙКОСТІ МІКРОПРОЦЕСОРНИХ СИСТЕМ

Ю.О. Гунченко[1], к.т.н., О.В. Банзак[2], к.т.н.
[1]Одеський національний університет ім. І.І. Мечникова
[2]Одеська національна академія зв'язку ім. О.С. Попова
_ua@mail.ru

Сучасні системи управляння складними системами будуються, за звичай, з використанням мікропроцесорної (МП) техніки.

Однак, за рахунок програмного управляння, у таких системах є суттєвий недолік – значно менша завадостійкість. Цей недолік не дозволяє широко використовувати мікропроцесорні системи (МПС) для управління відповідальними системами, для яких нормується високий показник відмовостійкості, навіть при наявності високого рівня перешкод.

На сьогодення відомо кілька методів підвищення завадостійкості МПС, всі з яких приводять до скидання (реініціалізації) системи. Основні з цих методів наступні:

- реініціалізація МП системи при включені напруги живлення (скидання по включенню, POR);
- реініціалізація МП системи при заданому знижені напруги живлення (скидання по зниженню напруги живлення, BOR);
- реініціалізація МП системи при несанкціонованому зациклюванні програми (скидання по тайм-ауту, WDT).

Зазвичай, всі ці методи використовуються водночас, що дозволяє майже стовідсотково запобігти "зависанню"

МП системи. Всі ці методи приводять до скидання процесору, реініціалізації всієї системи і продовження її роботи з початку.

Для додаткового підвищення завадостійкості МПС пропонується введення нових елементів (рис.1).

Рис. 1. Функціональна схема завадостійкої МПС

Регістр RG1, призначений для запам'ятовування стану відповідальних виходів N по додатковому сигналу з МП. Регістр RG1, призначений для зчитування стану регістра RG1 по додатковому сигналу з МП.

При включені живлення, система POR виробляє сигнал скидання, якій діє одночасно на МПС та RG1. При цьому система реініціалізується і починає роботу. При сигналах WDR, або BOR скидається тільки МПС, стан RG1 не змінюється. Після реініціалізації, МПС зчитує стан RG1, за допомогою додаткового регістру RG2. Таким чином, після WDR або BOR – МПС реалізує алгоритм управління із врахуванням поточного стану виходів.

Наведена схема й метод її роботи дозволив значно підвищити надійність, завадостійкість системи управління, навіть при наявності високого рівня перешкод.

УДК 681.32

ФОРМИРОВАНИЕ КВАЗИРАВНОВЕСНЫХ КОДОВ НА ОСНОВЕ ДВОИЧНЫХ БИНОМИАЛЬНЫХ ЧИСЕЛ

И.А. Кулик, к.т.н., доцент, Е.М. Скордина, аспирант
Сумский государственный университет
kulik@pe.sumdu.edu.ua

Квазиравновесные коды могут эффективно использоваться в адаптивных системах передачи информации, системах сжатия и комбинаторной оптимизации, поскольку обладают такими свойствами как, возможность адаптации к уровню помех, простотой обнаружения ошибок, бо́льшей мощностью по сравнению с равновесными кодами при той же длине кодовых комбинаций. Кроме того, квазиравновесные комбинации представляют интерес и как отдельный тип комбинаторных конфигураций – сочетаний длины n с переменным числом k единиц. Но генерирование квазиравновесных кодов, также как и равновесных, представляет достаточно сложную задачу, поэтому разработка алгоритмов формирования квазиравновесных комбинаций, отличающихся высокой скоростью преобразований и невысокими аппаратно-программными затратами является актуальной задачей.

Для получения регулярных (нетабличных) методов формирования квазиравновесных кодов предлагается использовать двоичные биномиальные числа. Кроме того, в этом случае появляется возможность генерирования квазиравновесных кодов как в систематическом (лексикографическом), так и в случайном порядке.

Поскольку количество N двоичных биномиальных чисел $X_j = \left(x_1 x_2 ... x_i ... x_r\right)$ с параметрами n и k составляет:

$$N = C_n^k,$$

то при рассмотрении известной формулы сложения для чисел сочетаний:

$$C_n^k = C_{n-1}^{k-1} + C_{n-1}^k$$

можно предположить, что структура биномиальных чисел лежит в основе кодовых комбинаций длины $n-1$ разрядов, содержащих k и $k-1$ двоичных единиц, т.е. квазиравновесных комбинаций с параметрами n, k и $k-1$, где $j = \overline{0, C_n^k - 1}$.

Таким образом, на основе двоичных биномиальных чисел X_j возможно взаимно-однозначное отображение:

$$\varphi_{\hat{e}\partial} : X\left[n, k\right] \to Y\left[n-1, k, k-1\right]$$

множества X биномиальных чисел $X_j = \left(x_1 x_2 ... x_i ... x_r\right)$ с параметрами n и k на множество $Y\left[n-1, k, k-1\right]$ квазиравновесных комбинаций Y_j длины $\left(n-1\right)$ разрядов, содержащих k и $\left(k-1\right)$ двоичных единиц.

Разработанные алгоритмы, реализующие кодовые отображения $\varphi_{\hat{e}\partial}$ и $\varphi_{\hat{e}\partial}^{-1}$, содержат достаточно простые операции поразрядного сравнения и конкатенации групп разрядов биномиальных чисел и квазиравновесных комбинаций, вследствие чего они обладают высокой скоростью работы и небольшим объемом аппаратно-программных затрат при практической реализации.

УДК 519.718

К ПРОБЛЕМЕ РАСЧЕТА НАДЕЖНОСТИ ОТКАЗОУСТОЙЧИВЫХ МНОГОПРОЦЕССОРНЫХ СИСТЕМ

А.М. Романкевич, А.В. Шурига
Национальный технический университет Украины "Киевский политехнический институт"
romankev@scs.ntu-kpi.kiev.ua

В последние десятилетия имеет место рост использования многопроцессорных систем, особенно в сфере управления сложными объектами и системах критического управления. Одновременно к таким системам растут требования к надежности, что обеспечивается такой организацией работы системы, при которой она остается работоспособной при отказе определенного множества ее компонентов.

Сложный процесс проектирования многопроцессорных систем не всегда может гарантировать изначально заданный уровень отказоустойчивости. Для повышения степени отказоустойчивости в структуру системы вносятся изменения, в связи с чем возникает необходимость расчета надежности уже спроектированной системы для проверки соответствия требованиям.

Достаточно распространенными методами повышения отказоустойчивости являются дублирование и реконфигурирование. Дублирование неэффективно использует ресурсы системы и поэтому в последнее время вытеснено реконфигурированием. При этом по ходу эксплуатации системы на некоторые процессоры возлагается выполнение функций вышедших из строя

процессоров, и это усложняет расчет надежности системы. Действительно, отказоустойчивые многопроцессорные системы управления сложными объектами могут состоять из многих подсистем, каждая из которых имеет свои процессоры (со своей производительностью и интенсивностью отказов) и свою степень отказоустойчивости.

В докладе делается сравнительный анализ аналитического метода расчета надежности с использованием биномиального разложения и метода расчета при помощи модели поведения системы в потоке отказов. На основе проделанного авторами обзора доступных им работ по расчету надежности делается вывод, что аналитический метод целесообразно использовать в k-out-of-n системах, то есть системах, которые остаются работоспособными при выходе из строя k процессоров из n. При более сложной зависимости работоспособности системы от вышедших со строя процессоров, а именно при сохранении работоспособности системы также на некотором множестве (k+1) и более отказов процессоров, метод расчета отказоустойчивости с использованием структурной модели является более эффективным.

УДК 519.95

ЗАВАДОСТІЙКІСТЬ СИСТЕМИ ПЕРЕДАВАННЯ З ПРОСТОРОВО-ЧАСОВИМ КОДУВАННЯМ

М.О. Іщенко, к.т.н. ст. викладач,
О.Д. Персин, магістрант, М.Ю. Балута, магістрант
Одеська національна академія зв'язку ім. О.С. Попова
dima_ischenko@rambler.ru dragall@mail.ru

Основна увага за останні роки приділяється методам, які базуються на передачі інформації до абонента через декілька рознесених у просторі передавальних антен, причому сигнали різних антен піддаються спеціальному кодуванню. Такі просторово-часові коди дають виграш по завадостійкості в каналах із завмираннями як за рахунок кодування, так і за рахунок рознесення каналів передачі. Перший зразок такої технології у формі методу «просторово-часового кодування» був запропонований колективом авторів V. Tarokh, N. Seshadri на чолі з R. Calderbank і продовжений у роботах S. Alamouti. Ними запропонована значна кількість просторово-часових кодів. Разом з тим, не було проведено системний аналіз та порівняння характеристик просторово-часових кодів спільно з багатопозиційними сигналами.

Авторами проведено дослідження завадостійкості системи передавання з просторово-часовим кодуванням на основі відомих блокових кодів *S. Alamouti* (з використанням двох передавальних і однієї, двох, трьох і чотирьох приймальних антен) зі спільним використанням багатопозиційних сигналів ФМ-4, ФМ-8 та ФМ-16. Дослідження завадостійкості системи передавання проводилось на основі комп'ютерної моделі в середовищі MATLAB 7.5. На основі отриманих результатів завадостійкості визначено необхідне відношення сигнал/шум при ймовірності помилки на виході декодера Аламоуті $p_{доп}=10^{-5}$, що дало змогу проаналізувати додатковий енергетичний виграш.

УДК 681.32

СТРУКТУРНА І АЛГОРИТМІЧНА ОРГАНІЗАЦІЯ ШВИДКОДІЮЧИХ АЦП ПОРОЗРЯДНОГО ВРІВНОВАЖЕННЯ І ЦАП З ВАГОВОЮ НАДЛИШКОВІСТЮ

Л.В. Крупельницький, к.т.н., О.О. Решетнік, аспірант
Вінницький національний технічний університет
de_gratnik@rambler.ru

Структурна схема АЦП порозрядного врівноваження з ваговою надлишковістю і змінною тривалістю тактів врівноваження має деякі відмінності від схеми звичайного АЦП з ваговою надлишковістю. Такий АЦП, як на базі НПСЧ {0, 1}, повинен містити схему порівняння (СП) з регульованою чутливістю та спеціальний цифровий блок, тактовий генератор імпульсів регульованої тривалості (ТГІРТ або просто ТГ) для завдання різної тривалості тактів врівноваження.

Порозрядний АЦП на основі СЧВН {1, 0} працює за класичним алгоритмом порозрядного врівноваження. Проте прискорене порозрядне аналого-цифрове перетворення в системі {1, 0} неможливе без використання форсуючих сигналів. Форсуючі сигнали генеруються спеціальним блоком або формуються на кожному такті врівноваження за рахунок використання молодших розрядів ЦАП.

Порозрядний АЦП на основі СЧВН {1, -1} працює за алгоритмом порозрядного врівноваження «тільки вмикання». Прискорене порозрядне аналого-цифрове перетворення в системі {1, -1} можливе з форсуючими сигналами так і без них. Форсуючі сигнали генеруються

спеціальним блоком або формуються на кожному такті врівноваження за рахунок використання молодших розрядів ЦАП.

ЦАП із ваговою надлишковістю можна виготовляти у вигляді цілісного пристрою, а можна використати запропонований підхід щодо використання для цього звичайних двійкових ЦАП. При побудові надлишкового ЦАП на базі двійкових за методом „гребінки” можна використовувати загальний РПН (регістр послідовного наближення) або окремі РПН для кожного з ЦАП, проте це потребує додаткового блоку керування.

За допомогою запропонованого методу побудови надлишкових ЦАП можна тримати такі системи числення з ваговою надлишковістю:

{1; 1; 2; 2; 4; 4; 8; 8, …}
{1; 1,5; 2; 3; 4; 6; 8; 12, …}
{1; 1,414; 2; 2,828; 4; 5,656; 8; 11,312, …}
{1; 1,259; 1,585; 2; 2,518; 3,17; 4, …}
{1; 1,681; 2,826; 4,750; 8; 13,448; 22,608;, …}

Доведено, що використання прогресуючого набору тривалостей тактів порозрядного врівноваження з ваговою надлишковістю дозволяє зменшити час перетворення порівняно з пристроями на основі двійкової системи числення.

Побудова порозрядного АЦП з ваговою надлишковістю з прогресуючим набором тривалостей тактів врівноваження не вимагає створення спеціальної елементної бази. Такі АЦП можна будувати на сучасній елементній базі.

УДК 681.326

ПОИСК ОШИБОК ПРОЕКТИРОВАНИЯ В HDL– МОДЕЛЯХ ЦИФРОВЫХ УСТРОЙСТВ

С. Альмадхоун, аспирант,
Е.Е. Сыревич, к.т.н., доцент,
А.С. Шкиль, к.т.н., доцент
Харьковский национальный университет радиоэлектроники
unownn@rambler.ru

Полный цикл диагностирования (верификации) модели цифрового устройства (ЦУ), на языках описания аппаратуры (HDL) включает в себя следующие этапы: описание модели на языках описания аппаратуры, компилирование внутренней модели, генерацию тестов, построение списка ошибок проектирования, получение эталонов, алгоритмы обработки диагностической информации и, собственно, методы поиска дефектов.

HDL-модели обладают свойством двойственности. С одной стороны, они формально выглядят и ведут себя как код на языках программирования, а с другой стороны, обладают рядом принципиальных отличий, присущих аппаратуре (сигналы, параллелизм, синтезируемость). Поэтому подход к диагностированию таких моделей должен быть комбинированным. Определим модель ошибки проектирования (дефекта), как ошибку в любом операторном выражении не являющуюся синтаксической

В качестве модели объекта диагностирования используется представление описания устройства на HDL в виде двух графов. Информационный I-граф описывает поток данных и их преобразование. Управляющий C-граф

соответствует цепочке условий, при выполнении которых выполняется тот или иной оператор. Учитывая, что операторы HDL (примитивы), не содержат внутри себя ошибок, то их тестирование состоит в определении типа примитива путем подачи специальных различающих последовательностей (РПС). Для декомпозиции исходного графа используются контрольные точки (КТ) которые позволяли «разбить» путь активизации и определить границы подграфов при поиске ошибок проектирования.

Особенностью верификации HDL-модели является отсутствие эталонного HDL-кода, поэтому вычислить эталонные значения сигналов во всех КТ без привлечения внешних источников информации невозможно. Исходя из этого, определим два типа КТ, используемых при поиске места ошибки проектирования в HDL-коде в условиях отсутствия исчерпывающей (полной) спецификации. КТ первого рода – сигналы (переменные) модели, которые наблюдаемы, и эталонные значения которых известны из спецификации. КТ второго рода – сигналы (переменные) модели, значения в которых наблюдаемы, но до начала диагностического эксперимента эти значения неизвестны.

Таким образом, общая методика диагностирования HDL-модели состоит из следующих шагов.

1. Составление модели на основе I–графа и C– графа , «разрыв» обратных связей в этой модели.

2. Определение класса ошибок проектирования, составление РПС для этих ошибок и тестирование модели путем подачи РПС и сравнение с имеющимися эталонами.

3. Сужение области подозреваемых дефектов на основе структурного метода для многовыходовых моделей.

4. Применение структурного метода поиска для подграфов только с контрольными точками первого рода.

5. Применение метода обратного прослеживания в подграфах ограниченных КТ первого рода.

УДК 519.711

ОБ ОПТИМИЗАЦИИ ВЫЧИСЛЕНИЯ РЕБЕРНЫХ ФУНКЦИЙ В GL-МОДЕЛЯХ

В.А. Романкевич, К.В. Морозов
Национальный технический университет Украины
«Киевский политехнический институт»
romankev@scs.ntu-kpi.kiev.ua

В настоящее время, в связи с широким распространением сложных многопроцессорных реконфигурируемых отказоустойчивых систем, при их проектировании часто возникает необходимость расчета их надежности. Один из методов расчета надежности основывается на статистическом моделировании поведения системы в потоке отказов. Для этих целей удобно использовать разработанную на кафедре Специализированных компьютерных систем Национального технического университета Украины «КПИ» модель поведения отказоустойчивых многопроцессорных систем (ОМС) в потоке отказов, названную графо-логической моделью, или GL-моделью. Модель принимает на вход векторы состояния системы (векторы, в которых 0 − процессор отказал, 1 − он работоспособен) и дает на выходе ответ, работоспособна ли система. Очевидно, что точность расчета надежности зависит от количества векторов, участвующих в моделировании. Оптимизация вычислений в модели позволяет сократить время обработки одного вектора, что дает возможность увеличить количество участвующих в моделировании векторов и тем самым повысить точность расчета.

Модель строится как неориентированный граф с некоторыми булевыми функциями на ребрах. Функции зависят от вектора состояния и определяют, присутствует ли ребро в модели в данном состоянии. Связность графа модели и определяет работоспособность системы. Известно несколько моделей; в работе за основу взята модель, которая теряет минимальное количество ребер, при появлении «лишних» отказов.

Ранее были предложены методы минимизации системы реберных функций. Однако, рассматривая всю систему функций в целом, можно значительно сократить сложность вычислений.

В докладе предлагается метод построения оптимизированной GL-модели для базовой K(m,n), то есть устойчивой к не более, чем m отказам, системы. Основная идея заключается в сведении процедуры вычисления значений реберных функций модели к расчету выходных значений некоторой специально построенной комбинационной схемы из элементов И и ИЛИ, в которой выходы не являются независимыми.

УДК 621.391+004.73

МЕТОДЫ И СРЕДСТВА ФОРМИРОВАНИЯ ОСТАТКОВ В МНОГОКАНАЛЬНЫХ ПОМЕХОУСТОЙЧИВЫХ КОДЕКАХ

Э.В. Фауре, к.т.н., Р.О. Бивзюк
Черкасский государственный технологический университет
emmil@km.ru

Вследствие возникновения ошибок при передаче данных по каналам связи, большинство современных систем передачи информации использует помехоустойчивое кодирование. Вид и параметры кодирования зависят от типа ошибок, их интенсивности, а также от требуемой величины повышения достоверности передаваемых данных. Вместе с тем, большинство видов помехоустойчивого кодирования основано на вычислении контрольной суммы (остатка от деления на некоторый кодовый многочлен) в конечном поле.

В настоящее время из-за постоянно возрастающей скорости передачи информации, а также из-за интеграции большого количества потоков с различными требованиями по достоверности в единый информационный поток актуальными являются вопросы повышения эффективности функционирования устройств формирования контрольной суммы в кодере и синдрома ошибок в декодере. Одним из наиболее важных вопросов является сокращение объема используемого оборудования в многоканальных помехоустойчивых кодеках при сохранении их быстродействия.

В работе проводится подробный системный анализ современных методов и средств формирования остатков в многоканальных помехоустойчивых кодеках, указываются их недостатки.

Показано, что техническим результатом работы устройства формирования остатков в многоканальных системах является получение остатка (вычета по модулю некоторого полинома) из поступающих бит за битом блоков данных от N различных каналов:

$$R_i(x) = \left|A_i(x)\right|_{G_{n_i}(x)} = \left|\sum_{j=0}^{T_i-1} a_{ij}x^j\right|_{G_{n_i}(x)},$$

где $A_i(x)$ – делимое i-го канала (последовательность символов блока данных в полиномиальной форме); $G_{n_i}(x)$ – кодовый полином i-го канала; n_i – порядок кодового полинома i-го канала; T_i – число бит в информационной части блока данных i-го канала.

Сущность предлагаемых методов и устройств формирования остатков в многоканальных помехоустойчивых кодеках заключается в выделении в структуре устройств вычисления остатка комбинационной части и памяти. Данный подход позволяет использовать единственную комбинационную структуру для всех каналов (подканалов) и запоминающее устройство для хранения индивидуальных для каждого из каналов (подканалов) результатов промежуточных вычислений.

В устройстве предусмотрена возможность использования кодовых полиномов различных степеней для каждого из каналов.

Таким образом, предложенные методы и средства формирования остатков расширяют техническую базу проектирования многоканальных систем связи с использованием помехоустойчивого кодирования.

УДК 621.3

САМОКАЛІБРОВАНИЙ ЦИКЛІЧНИЙ АЦП ІЗ ВАГОВОЮ НАДЛИШКОВІСТЮ

С.М. Захарченко, к.т.н, доцент, О.В. Бойко, аспірант
Вінницький національний технічний університет
zahar@vstu.vinnica.ua

Аналого-цифрові перетворювачі широко використо-вуються в різноманітних пристроях та системах. Питання покращення метрологічних характеристик АЦП, і особливо точності, не втрачають актуальності. Частково дана може бути вирішена за рахунок покращення технології, однак цей підхід, призводить до погіршення температурних параметрів, зменшує надійність пристроїв. Інший шлях покращення точнісних характеристик АЦП – застосування методів самокалібрування. При використанні двійкової системи числення калібрування здійснюється в цифро-аналоговій формі, що передбачає застосування додаткових коригуючих ЦАП і зменшує швидкодію перетворювача. Для уникнення зазначених недоліків використовують надлишкові позиційні системи числення, що дозволяє виконати калібрування виключно в цифровій формі і таким чином уникнути головних недоліків цифро-аналогового калібрування. Також використання інформаційної надлишковості у вигляді надлишкової позиційної системи числення дає змогу не тільки спростити процедуру калібрування та зменшити вимоги до точності розрядів, а й суттєво підвищити швидкодію перетворювачів.

Одним із видів АЦП із накопиченням заряду є алгоритмічний (циклічний) АЦП, які вирізняються

простою структурою, низькою потужністю споживання і малими фізичними розмірами на кристалі. Крім того, дані АЦП є розрядно-незалежними, тобто збільшення розрядної сітки перетворювача не веде за собою збільшення або ускладнення апаратного забезпечення. В основі роботи даного виду перетворювачів лежить алгоритм МакЧарльза, який дозволяє будувати АЦП, результуючий код якого отримується послідовно розряд за розрядом. Даний алгоритм функціонує використовуючи співвідношення $U_{i+1} = 2 \cdot U_i + B_i \cdot U_{on}$ для отримання кожного розряду і представляє ідеальний процес перетворення, тому на практиці реалізують неідеальний алгоритм, який можна описати наступним рівнянням:

$$U_{i+1} = (2 + \Delta_1) \cdot U_i + (1 + \Delta_2) \cdot B_i \cdot U_{on}, \qquad (1)$$

де Δ_1 – похибка, яка впливає на лінійність перетворювача, Δ_2 – похибка, яка впливає на коефіцієнт нахилу характеристики перетворення.

Оскільки для побудови АЦП пропонується застосовувати надлишкову позиційну систему, то можливе калібрування ваг розрядів зі значними відхиленнями, що істотно знижує вимоги до ряду аналогових вузлів перетворювачів.

Основна ідея запропонованого цифрового самокалібрування полягає в тому, що ми калібруємо не розряд, а похибку. У базову структуру циклічного АЦП введено додаткові блоки – генератор калібрувальних сигналів (ГКС) і додатковий малорозрядний калібрувальний АЦП

ГКС генерує певний сигнал, який буде оброблятись за допомогою і звичайного алгоритмічного АЦП, і калібрувального АЦП, після декількох циклів результати цих перетворювачів порівнюються і вносяться відповідні поправки.

УДК 621.391

ЦИФРОВІ ФІЛЬТРИ НА ПЛІС В СИСТЕМАХ ПЕРЕДАЧІ СИГНАЛІВ

[1]І.Д. Прокопов к.т.н., доцент, [2]О.І. Прокопов, студент
[1]Вінницький національний технічний університет
[2]Київський національний університет ім. Т.Г.Шевченка
alexprokopov@mail.ru

Цифрові методи дають можливість збільшити якісні характеристики систем передачі сигналів. Для реалізації таких систем з використанням ПЛІС-технології потрібно розробити ефективні методи по скороченню кількості обчислювальних операцій і логічних елементів структури. Скоротити кількість обчислювальних операцій можливо за рахунок використання метода половинного ділення частоти, який дає можливість за рахунок децимації (проріджування) і послідовного зсуву спектра по частоті виконувати спектральний аналіз одним фільтром нижніх частот.

Використовуючи цей метод, а також властивості коефіцієнтів фільтра і позицій однакових їх значень імпульсної характеристики можливо побудувати структури багатоканальних фільтрів з скороченою кількістю обчислювальних операцій і меншою кількістю вентилів ПЛІС- схеми.

Цифровий нерекурсивний фільтр має симетричну імпульсну характеристику, що дає можливість групувати його коефіцієнти і отримати залежність вихідного сигналу $y(n)$ від вхідного $x(n)$ у вигляді:

$$y(n)=\sum_{k=2l}^{\frac{M}{2}} h_k(x_{n-k}+x_{n-2M+k})+...+\sum_{k=2l+1}^{\frac{M}{2}} h_k(x_{n-k}+x_{n-2M+k})+...$$

$$+\ h_M x_{n-M}\ , \qquad (1)$$

де l=0,1,2,3… .

Враховуючи, що кожний другий відлік є парним відліком, а у виразі (1) згруповані пари значення добутків коефіцієнтів:

$$\sum_{k=2+1}^{\frac{M}{2}} h_k(x_{n-k}+x_{n-2M+k})+...+h_M x_{n-M}(\pm 1)^M\ , \qquad (2)$$

Вираз суми $h_M x_{n-M}(\pm 1)^M$ може мати від'ємне (для високочастотних складових і $(-1)^M h^M x_{n-M}$), чи додатне значення (для низькочастотних складових і $(+1)^M h_M x_n$).

Було проведено моделювання багатоканального цифрового фільтра 256 порядку згідно виразів (1) і (2) у програмному пакеті Quartus. Для реалізації фільтра після моделювання вибрана ПЛІС фірми Altera EP1K50QC208-2 класу ACEX EP1K50, з кількістю 50 тисяч елементів. В результаті моделювання були визначенні основні характеристики фільтра 256 порядку. Частота зрізу фільтра приблизно 2.5% від частоти дискретизації, частотний діапазон від долі герц до 100 кГц. Затухання в смузі непрозорості 55 ± 1 дВ. Нерівномірність затухання на смузі пропускання не більша за 1 ± 0.05 дВ. Фільтр працює в режимі децимації вихідного сигналу в 16 разів.

Запропонована реалізація цифрового фільтра за ПЛІС-технологією дозволяє оптимізувати структуру багатоканального фільтра і створити високошвидкісні апаратні реалізації систем цифрового звукозапису, компресії, та передачі мовних сигналів.

УДК 519.725; 519.816; 519.712.6

ПРОТОКОЛ АРГУМЕНТА ДЛЯ СЛОВА КОДА ГОППЫ И ОШИБКИ ОГРАНИЧЕННОГО ВЕСА

В.Е. Федюкович
Интропро, г. Киев
vf@unity.net

Проверка справедливости утверждений о секретах является важным инструментом обеспечения безопасности данных в условиях взаимного недоверия взаимодействующих субъектов. Классическим примером является проверка корректности бюллетеня системы электронного демократического голосования, так, что содержание бюллетеня остается недоступным проверяющей стороне. Проверки такого вида также используются в системах электронных монет и проверяемых схемах разделения секрета. Некоторые схемы электронной подписи были получены путем преобразования интерактивных протоколов, позволяющих выполнить проверку утверждения о знании секретного ключа подписи. Протоколы такого вида являются основой Direct Anonymous Attestation (IBM, Intel, HP) и U-Prove (Credentica, Microsoft).

Значительный практический интерес представляют протоколы аргумента, допускающие только ничтожную вероятность ошибки корректности, а также предусматривающие ответы доказывающей стороны, полученные как значения линейных полиномов. Так, например, протокол Шнорра позволяет доказывающей стороне показать знание некоторого секрета, который является индексом (логарифмом) в конечной группе.

В этой работе рассматривается протокол, позволяющий проверить справедливость утверждения о том, что вес ошибки в искаженном кодовом слове кода Гоппы не превышает заданного порога, причем кодовое слово и полином Гоппы доступны проверяющей стороне только в виде экземпляров привязки. В процессе этой проверки проверяющая сторона не получает какой-либо информации о структуре кода (определяемой полиномом Гоппы), кодовом слове и весе ошибки, за исключением результата проверки. Проверяющая сторона также не может убедить какую-либо третью сторону в справедливости проверенного утверждения. Получена верхняя оценка вероятности ошибочного решения, приведен моделирующий алгоритм. Предложенный протокол является аргументом в предположении о вычислительной сложности задачи поиска логарифма в используемой группе. Проверяется утверждение о знании доказывающей стороной корней полинома, из которых ранее были получены экземпляры привязки. Используется схема запрос-ответ, которая может рассматриваться как расширение протокола Шнорра. В отличие от протокола Шнорра, проверяемое утверждение представлено несколько более сложным полиномом. Для создания элементов привязки используется схема Педерсена, которая допускает использование произвольных групп со сложной задачей поиска логарифма, таких как мультипликативная группа классов вычетов и группа точек на эллиптической кривой.

Также были получены протоколы аргумента для проверки справедливости утверждений о верхней границе мощности разности множеств, о строках, и для классических задач распознавания изоморфизма графов и цикла Гамильтона; найден и исправлен нежелательный сценарий в протоколе DAA.

УДК 681.3.06

ВИБІР ОПТИМАЛЬНОЇ КОНФІГУРАЦІЇ ВІДМОВОСТІЙКОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ

Л.Ю. Юрчук, к.т.н., доцент, С.В. Жульжик, студент
Національний технічний університет України «КПІ»
admin@julik.org.ua

В умовах ринкової економіки особливого змісту набуває підвищення якості та економічної ефективності функціонування виробу, пристрою чи системи. Особливо актуальним з економічної точки зору є дослідження надійності складних і великих комп'ютерних систем, якими є, наприклад, ієрархічні розгалужені системи (ІРС).

Розглянемо систему управління з обчислювальними вузлами двох типів – керуючі комп'ютери (КК) та вузли вводу/виводу (ВВВ), які взаємодіють в комунікаційному середовищі, побудованому на комутаторах (Км), підключення до яких вимагає мережевих адаптерів (МА).

В роботі будемо вважати заданими наступні параметри:

1. Кількість обчислювальних вузлів (ОВ) кожного типу в системі: КК – N і ВВВ – M. Мінімальна необхідна кількість робочих ОВ, при якому система зберігає свою роботоздатність, $N1$, $M1$ $\left(N1 \le N,\ M1 \le M\right)$.

2. Гранично допустима кратність резервування МА в ОВ – r. Обмеження часу реакції системи – T^*.

3. Імовірність безвідмовної роботи МА, КК, ВВВ, комутаторів – відповідно $p_{МА}$, $p_{КК}$, $p_{ВВВ}$, $p_{Км}$. Рівень необхідної надійності системи вцілому – $p^*_{СПД}$ (P^*).

4. Вартість елементів системи: $ВКК$, $ВПВВ$ – вартість КК та пристроїв вводу-виводу відповідно; $ВКм$ – вартість комутатора; $ВМА$ – вартість мережевого адаптера.

5. Параметри інформаційних потоків та параметри продуктивності вузлів і мережевого обладнання.

При нижній оцінці надійності вважатимемо, що в системі повинно бути, принаймні $K1$ справних комутаторів, що забезпечують зв'язок між $N1$ справними із N вузлами першої групи (КК) і $M1$ справними з M вузлами другої групи (ВВВ), причому для кожного із вказаних зв'язків МА, розташовані у відповідних вузлах, мають бути справні.

При верхній оцінці вважатимемо, що кожен справний вузол першої і другої групи має бути підключений хоч би до одного із справних комутаторів через справні МА.

Методика вибору раціонального варіанту конфігурації системи, що забезпечує максимальний рівень надійності при заданих обмеженнях на час реакції і вартість (пряма задача) містить два етапи: *1)* вибір мінімальної конфігурації системи, що задовольняє обмеженню за часом реакції; *2)* підвищення надійності вибраної на першому етапі конфігурації системи (резервування).

При виборі конфігурації, що забезпечує мінімальний час реакції при заданих обмеженнях на надійність і вартість (зворотня задача) процес вибору конфігурації наступний: *1)* пошук конфігурації з максимальною кількістю комунікаційного устаткування, що задовольняє обмеженню на вартість системи; *2)* визначення числа основних і резервних комутаторів, при якому забезпечується задане обмеження надійності системи; *3)* оцінка часу реакції знайденої конфігурації.

Таким чином розглянута, пов'язана із завданням вибору, модель оцінки надійності досліджуваної системи управління та описана методика вибору раціонального варіанту конфігурації системи, що забезпечує мінімальний час реакції (максимальний рівень надійності) при заданих обмеженнях на надійність і вартість.

УДК 681.3

СПЕЦІАЛІЗОВАНИЙ ПРОЦЕСОР ДЛЯ УЩІЛЬНЕННЯ ДАНИХ

Л.А. Савицька, асистент
Вінницький національний технічний університет

Практика показує, що повторне застосування відомих алгоритмів ущільнення до даних, які вже ущільнені, не тільки не приводить до збільшення степеня ущільнення, а в деяких випадках і зменшує її. Тому актуальною задачею є розробка алгоритму ущільнення, що забезпечував би збільшення степеня ущільнення за рахунок багаторазового його застосування до ущільнених даних. У доповіді розглядається саме такий алгоритм і спеціалізований процесор, що його реалізує.

У процесі ущільнення інформації блок цифрових даних будь-якої довжини розглядається як надвелике ціле додатне число, що представляється набором із трьох невеликих чисел. Таке представлення чисел, називається лінійною формою Фібоначчі або *q*-представленням Фібоначчі.

Нехай T_i - блок даних, призначених для ущільнення, n - розрядність цього блоку, m - кількість блоків даних; $\varphi_1(n)$ і $\varphi_1(n-1)$ - числа Фібоначчі; K_i - код Фібоначчі блоку даних; M_i* - *q*-представлення блоку даних; M_i - блок ущільнених даних. Тоді маємо такі множини, що описують операційний автомат.

1. Множина вхідних слів **D**={T_i, n,m, $\varphi_1(n), \varphi_1(n-1)$}.
2. Множина вихідних слів **R**={M_i }.

3. Множина внутрішніх слів **S**={n,m, $\varphi_1(n), \varphi_1(n-1)$, К$_i$, М$_i$*, }.
4. Множина мікрооперацій **Y**={y_l}, l=1,…,L, яка визначається алгоритмом ущільнення.
5. Множина логічних умов **X**={x_1}.

Згідно з канонічним методом структурного синтезу автоматів кожному математичному елементу абстрактного опису автомата ставиться у відповідність структурний елемент.

З огляду на це, маємо узагальнену структуру спеціалізованого процесора для ущільнення даних, що наведена на рис. 1

Рис.1 - Структурна схема спеціалізованого процесора для ущільнення даних

Тут блок вхідних даних Т$_i$ зберігається у блоці пам'яті 1. Для зберігання блоку ущільнених даних М$_i$ призначений блок пам'яті 2. Блок перетворення кодів реалізує перетворення двійкового коду блоку вхідних даних у код Фібоначчі. Формування q-представлення блоку вхідних даних на основі коду Фібоначчі здійснюється у блоці додавання q-представлень. Остаточний результат ущільнення формується у блоці мінімізації q-представлення.

УДК 681.3:621.375

ДВОТАКТНІ ПІДСИЛЮВАЧІ ПОСТІЙНОГО СТРУМУ ДЛЯ БАГАТОРОЗРЯДНИХ АЦП І ЦАП ІЗ ВАГОВОЮ НАДЛИШКОВІСТЮ, ЩО САМОКАЛІБРУЮТЬСЯ

О.Д. Азаров, д.т.н., професор, В.А. Гарнага, аспірант
Вінницький національний технічний університет
w0lfman@ramber.ru

Значна кількість сучасних підсилювачів постійного струму застосовують переважно одноканальну асиметричну структуру з диференційним підсилювальним каскадом на вході і двотактним вихідним каскадом, який передбачає принцип підсилення і перетворення напруг. Перевагами такого підходу є функціональна універсальність цих схем, що дозволяє використовувати їх у різних пристроях (операційні підсилювачі, буферні пристрої, пристрої вибірки-зберігання аналогових сигналів, компаратори і т. д.). Проте підсилювачі на базі диференційного каскаду з одноканальною структурою, хоча і використовуються досить давно, проте мають певні недоліки: низька швидкість наростання вихідного сигналу, значний коефіцієнт нелінійних спотворень, особливо, при збільшенні частоти вхідного сигналу, асиметричність вихідного сигналу при роботі з прямокутним двополярним вхідним імпульсом.

Особливо слід відзначити, що надзвичайно високі вимоги висуваються до підсилювачів постійного струму (ППС), які застосовуються у багаторозрядних АЦП і ЦАП, що входять до складу високоточних інформаційно-

вимірювальних систем, а також гібридних обчислювальних систем, оскільки, від точності опрацювання вхідного сигналу підсилювачем залежить підсумкова точність результатів перетворень. Таким чином, проектуючи схеми ППС, необхідно використовувати схемні рішення, які б могли відповідати таким вимогам: висока лінійність статичної передатної характеристики, коефіцієнт підсилення по струму на рівні (10^4-10^6), низький коефіцієнт нелінійних спотворень при максимальній смузі пропускання, мінімальні струми зміщення нуля.

Водночас використання методів самокалібрування дозволяє зменшити похибки складових АЦП і ЦАП із ваговою надлишковістю проте не усі. Так можна виділити три групи похибок:

– кориговані;
– не кориговані;
– частково кориговані.

При цьому до коригованих похибок відносяться похибка масштабу та зміщення нуля і вони відносно легко зменшуються за допомогою самокалібрування. Для зменшення ж інтегральної лінійності необхідно використовувати значні апаратні витрати і тому застосування такого підходу для АЦП із розрядністю 16-18 розрядів є проблематичним. Саме тому цю похибку відносять до похибок, що не коригуються. Для її зменшення потрібно використовувати високо лінійні аналогові вузли.

Водночас використання аналогових вузлів на базі запропонованих двотактних симетричних ППС дозволяє суттєво зменшити похибку інтегральної лінійності, а також підвищити й інші статичні та динамічні характеристики.

УДК 681.32

СУЧАСНІ ВИСОКОПРОДУКТИВНІ АЦП ПОРОЗРЯДНОГО ВРІВНОВАЖЕННЯ

О.О. Решетнік, аспірант
Вінницький національний технічний університет
de_gratnik@rambler.ru

Нажаль провідне положення на ринку АЦП мають лише закордонні компанії. Лідерами в цій царині є такі фірми: Analog Devices, Texas Instruments, Intersil, National Semiconductors, Linear Technologies, Maxim. На сучасному рику АЦП є величезна кількість пристроїв. АЦП виробляє близько двадцяти компаній, але безсумнівними лідерами є лише перелічені вище. Інші компанії є аутсайдерами і виробляють пристрої низької продуктивності для обробки звуку.

Сучасні АЦП використовують в таких галузях: системи збору та обробки даних, прецизійні вимірювальні системи, аудіосистеми та телефонія, швидкодіючі системи збору даних.

На рисунку наведено граничні параметри різних типів АЦП по точності та частоті дискретизації. З рисунка видно, що можна підібрати різні типи АЦП з однаковими параметрами, проте вибір типу АЦП залежить від галузі застосування. Порозрядні АЦП (SAR) займають проміжне положення серед інших типів АЦП. Вони забезпечують високу швидкодію та точність (частота дискретизації 10 МГц при роздільній здатності 16 біт). Порозрядні АЦП найчастіше використовуються в багатоканальних системах збору і обробки даних. Такі АЦП не мають затримки, характерної для конвеєрних АЦП (pipeline), що дозволяє

використовувати їх в багатоканальному режимі або при кодуванні неперіодичних процесів в режимі одиничних вимірювань.

В сучасних перетворювачах використовуються ЦАП на основі комутованих конденсаторів, такі матриці на відміну від резистивних не вимагають лазерного припасування ваг розрядів. Варто зазначити, що в порозрядних АЦП легко реалізувати режим само тестування та самокалібрування.

Переважна більшість сучасних АЦП порозрядного врівноваження будується на основі двійкової системи числення, що накладає фундаментальні обмеження на такі пристрої. Водночас побудова АЦП порозрядного наближення з використанням систем числення з ваговою надлишковістю дозволяє значно покращити точність та швидкодію таких пристроїв, без значного збільшення апаратних затрат та зміни алгоритму врівноваження. Наявність вагової надлишковості в розрядній сітці АЦП дозволяє використовувати спеціалізовані алгоритми самокалібрування та самокоригування та методи прискорення аналлого-цифрового перетворення.

УДК 681.3:621.375

СХЕМНА ОРГАНІЗАЦІЯ ВХІДНОГО КОМПЛЕМЕНТАРНОГО КАСКАДУ ДВОТАКТНОГО СИМЕТРИЧНОГО ПІДСИЛЮВАЧА ПОСТІЙНОГО СТРУМУ

С.В. Богомолов, аспірант
Вінницький національний технічний університет
bogomolovsergiy@rambler.ru

Визначальним компонентом аналогової схемотехніки є підсилювачі постійного струму, які у свою чергу є основою операційних підсилювачів, що використовуються в системах автоматики, вимірювання та приладобудування.

Водночас деякі фірми (Analog Devices, National Semiconductor, Texas Instruments), ще у 70-х роках почали будувати двотактні симетричні підсилювачі струму. Проте ці пристрої були недосконалі, оскільки мали обмежену кількість (1÷2) підсилювальних каскадів, низьку лінійність і малий коефіцієнт передачі. Однією з причин цього було те, що у вказаних схемах складно задавати потрібний режим по постійному струму проміжних каскадів підсилення.

Значна кількість сучасних підсилювачів постійного струму застосовують переважно одноканальну асиметричну структуру з диференційним підсилювальним каскадом на вході, однотактний проміжний підсилювальний каскад та двотактний симетричний каскад на виході. Цей підхід зорієнтовано переважно на підсилення і перетворення напруг. Перевагами такого підходу є функціональна універсальність цих схем. Проте

підсилювачі на базі диференційного каскаду з одноканальною структурою мають певні недоліки: низьку швидкість наростання вихідного сигналу, значний коефіцієнт нелінійних спотворень, особливо, при збільшенні частоти вхідного сигналу, асиметричність вихідного сигналу при роботі з прямокутним двополярним вхідним імпульсом.

Розвиток мікроелектронних технологій і можливість виготовлення на одному кристалі комплементарних біполярних транзисторів стимулювали розробників до проектування нових структур і схем та застосування двоканальних симетричних структур, що орієнтовані на принцип підсилення струмів і потенційно мають вищу швидкодію. Проте для побудови таких підсилювачів необхідно вирішити проблему завдання режиму по постійному струму підсилювальних каскадів, що ускладнює задачу побудови багатокаскадних підсилювачів з високим коефіцієнтом підсилення по струму, високою лінійністю та обмежує сферу їх застосування. До того ж потрібно вжити заходів щодо симетрування коефіцієнтів передачі вхідного комплементарного каскаду по парафазних виходах.

Запропоновано метод схемної реалізації вхідного комплементарного каскаду двотактного симетричного підсилювача постійного струму на біполярних транзисторах різної провідності з виходами по емітерах із подальшим каскодуванням, а також із виходами по емітерах і по колекторах. Наводяться аналітичні співвідношення для коефіцієнтів передачі по струму вхідного комплементарного каскаду з парафазними виходами та в каналах підсилення верхнього і нижнього ярусів двотактних симетричних підсилювачів постійного струму, а також загального коефіцієнту передачі по струму для малосигнальної зони та зони великого сигналу.

7. ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ОСВІТІ, ЕКОЛОГІЇ ТА ЕКОНОМІЦІ

УДК 519.711

СИНТЕЗ МАТЕМАТИЧНИХ МОДЕЛЕЙ РІВНІВ СИНЕРГЕТИЧНОЇ УНІВЕРСИТЕТСЬКОЇ СИСТЕМИ

Б.І. Мокін, д.т.н., професор, А.В. Писклярова, к.т.н.
Вінницький національний технічний університет
panna@vstu.vinnica.ua

Синергетична університетська система представлена п'ятьма рівнями: академічні групи, кафедри, органи управління і забезпечення факультетів, інститутів та університету в цілому. Математичні моделі академічних груп та кафедр можуть бути подані в такому вигляді

$$\vec{\hat{X}}(t) = \vec{F}_{\Gamma}(\vec{\hat{\mathrm{U}}}, \vec{\hat{\mathrm{V}}}, \mathrm{t}),\ \vec{\hat{Y}}(t) = \vec{F}_{K}(\vec{\hat{\mathrm{Q}}}, \vec{\hat{\mathrm{Z}}}, \mathrm{t}),\ \vec{H}(t) = \vec{f}_{\phi}(\vec{\Lambda}, \vec{\Gamma}, t),$$

$$\vec{\Omega}(t) = \vec{f}_{ін}(\vec{\theta}, \vec{\Psi}, t),$$

де $\vec{\hat{X}}(t)$, $\vec{\hat{Y}}(t)$, $\vec{H}(t)$, $\vec{\Omega}(t)$ – вектори реакції кожного з перших чотирьох рівнів, $\vec{\hat{U}}(t)$, $\vec{\hat{Q}}(t)$, $\vec{\Lambda}(t)$, $\vec{\theta}(t)$ – вектори управління; $\vec{\hat{V}}(t)$, $\vec{\hat{Z}}(t)$, $\vec{\Gamma}(t)$, $\vec{\Psi}(t)$ – вектори завад.

Частина проекцій вихідних векторів $\vec{\hat{X}}(t)$, $\vec{\hat{Y}}(t)$ співпадає з частиною векторів управління $\vec{\hat{U}}(t)$, $\vec{\hat{Q}}(t)$, а інша частина має самостійне значення, адресоване до об'єктів інших рівнів ієрархії системи:

$$\vec{\hat{U}}(t) = \begin{Vmatrix} \vec{\hat{U}}_1(t) \\ \vec{\hat{U}}_2(t) \end{Vmatrix},\ \vec{\hat{Q}}(t) = \begin{Vmatrix} \vec{\hat{Q}}_1(t) \\ \vec{\hat{Q}}_2(t) \end{Vmatrix},\ \vec{\hat{X}}(t) = \begin{Vmatrix} \vec{\hat{X}}_1(t) \\ \vec{\hat{X}}_2(t) \end{Vmatrix},\ \vec{\hat{Y}}(t) = \begin{Vmatrix} \vec{\hat{Y}}_1(t) \\ \vec{\hat{Y}}_2(t) \end{Vmatrix}.$$

Тоді справедливими будуть тотожності

$$\vec{\hat{U}}_1 = \vec{\hat{Y}}_1,\ \vec{\hat{Q}}_1 = \vec{\hat{X}}_1.$$

Вихідні вектори академічної групи $\vec{\hat{X}}_2(t)$ і кафедри $\vec{\hat{Y}}_2(t)$ можна представити у вигляді

$$\vec{X}_2(t)=\begin{Vmatrix}\vec{X}_{21}(t)\\ \vec{X}_{22}(t)\\ \vec{X}_{23}(t)\end{Vmatrix},\vec{Y}_2(t)=\begin{Vmatrix}\vec{Y}_{21}(t)\\ \vec{Y}_{22}(t)\\ \vec{Y}_{23}(t)\end{Vmatrix},$$

де $\vec{X}_{21}(t)$, $\vec{X}_{22}(t)$, $\vec{X}_{23}(t)$, ($\vec{Y}_{21}(t)$, $\vec{Y}_{22}(t)$, $\vec{Y}_{23}(t)$) – вихідні вектори академічних груп та кафедр, які поступають на вхід органів управління факультетів, інститутів та інших структурних блоків університету.

Складові $\vec{\Lambda}_1(t)$ та $\vec{\theta}_1(t)$ вихідних векторів факультету і інституту можна представити у вигляді

$$\vec{\Lambda}_1(t)=\begin{Vmatrix}\vec{\Lambda}_1^*(t)\\ \vec{X}_{21}(t)\\ \vec{Y}_{22}(t)\end{Vmatrix},\quad \vec{\theta}_1(t)=\begin{Vmatrix}\vec{\theta}_1^*(t)\\ \vec{Y}_{21}(t)\\ \vec{X}_{22}(t)\end{Vmatrix},$$

де $\vec{\Lambda}_1^*(t)$, $\vec{\theta}_1^*(t)$ – це складові вихідних векторів інших структурних блоків університету, що поступають на входи даного факультету і даного інституту для участі в формуванні складових $\vec{\Lambda}_1(t)$, $\vec{\theta}_1(t)$ вихідних векторів $\vec{\Lambda}(t)$ та $\vec{\theta}(t)$.

Побудовані узагальнені математичні моделі академічних груп, кафедр, факультетів і інститутів університету за умови, що університет розглядається як синергетична багатозв’язна ієрархічна логіко-динамічна стохастична система.

УДК 681.32

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ДОКУМЕНТУВАННЯ ЖИТТЄДІЯЛЬНОСТІ

А.А. Тимченко, д.т.н., професор
Черкаський державний технологічний університет
tymchenko@uch.net

Розглядаються питання документування в першу чергу процесів людської життєдіяльності. В основу розгляду покладені особливості документування результатів діяльності в галузі культури.

Вступ. Коротка історична довідка.

В доповіді показано, що людина з давніх-давен залишає результати своєї діяльності (інколи чистолюбивої) в першу чергу матеріальному світі (середовищі) – піраміди, храми, споруди культу та ін. Відповідно до можна виділити 3 види культурної діяльності людства – *образи, письменність, науки.* Результати відтворення відповідно в культурних надбаннях людства – *музеї, бібліотеки, наукові зібрання.*.

З появою засобів обчислювальної техніки (ЗОТ) якісно змінилась картина (і відповідно змістилась в інформаційне середовище). А по мірі розвитку можливостей ЗОТ «образне мислення» штучного інтелекту надає людству сьогодні практично необмежені можливості використання інформаційних технологій.

Постановка задачі та основні напрями використання.

Як відомо, людство живе в 3-х світах: *світі природи, світі техніки – другої природи, соціально-економічному – світі собі подібних.* Відповідно до законів кожного із

«світів» відбуваються відповідно і процеси документування людської життєдіяльності.

Закони фізики, хімії, біології та інших наук дозволяють документувати результати їх пізнання. Наприклад, так звані «життєві цикли» як розуміння змін в природі дозволяють виділити результати можливих перетворень окремих видів (метелик-гусінь, багатолітні рослини та ін.).

Відповідно життєві цикли в техніці (наукові дослідження, проектування, виробничі процеси виготовлення продукції та різноманітні сфери використання) дозволяють упорядковувати інформаційно-матеріальні перетворення об'єктів нової техніки (ОНТ) та їх поколінь.

Документування процесів життєдіяльності як окремої людини, так і їх об'єднань носить достатньо різноплановий характер: це і документування в органах РАЦС (реєстраційних актів цивільних станів), документи діяльності установ, організацій, підприємств (процеси навчання, трудової діяльності, пенсійні заклади, РАЦС, архіви та ін.)

Цілі інформаційні потоки (якщо не більше) супроводжують людську діяльність, даючи можливість відповідним наукам «оглянутися назад», осмислити сьогодні, та по мірі можливостей заглянути в майбутнє. А засоби масової інформації дають можливість масово розтиражувати і довести до свідомості кожного із нас.

Заключення. Основні висновки.

Можливо, звернувши увагу на діяльність *обслуговуючих систем* більш змістовніше і ефективніше потрібно уважніше подивитись на *системи, що обслуговуються*. Тобто, нашу з вами діяльність в сферах інформаційних технологій. Це повинно стати об'єктом наукових досліджень з метою оптимальних результатів.

УДК 621.38

ЗАСТОСУВАННЯ ТЕХНОЛОГІЇ «ELECTRONICS WORKBENCH» У ВИВЧЕННІ ДИСЦИПЛІН РАДІОЕЛЕКТРОННОГО ПРОФІЛЮ

Б.І. Медведенко, к.т.н., професор
Національний авіаційний університет
medvedenkoboris@gmail.com

Реформування вищої освіти спрямоване на перехід від отримання студентами потрібного набору знань (заучування) до навчання методам і принципам використання знань для вирішення практичних та творчих завдань.

Наявність комп`ютерних класів, стовідсотковий доступ студентів до ПК, а також досконале програмне забезпечення «Electronics Workbench» (EWB), зокрема версія «Multisim 10.0», дозволяють суттєво покращити організацію навчального процесу підготовки фахівців радіоелектронного профілю з метою вирішення згаданої задачі.

Виділимо такі основні напрями:

1. Розробка, формування електронних копій та передача студентам підручників, навчальних посібників, повного комплекту навчально-методичного забезпечення.

2. Викладення лекційного матеріалу відбувається традиційно, але до 30% часу виділяється для демонстрації динамічних віртуальних процесів перетворення електричних інформаційних сигналів у електронних пристроях, які створюються шляхом моделювання в середовищі «Multisim 10.0». Демонстрація роботи функціональних вузулів дає можливість проілюструвати

вплив компонентів схеми на вихідні сигнали, підкреслити і помилки, скоригувати форму вихідних сигналів та ін.

3. Впровадження EWB суттєво вплинуло на організацію та проведення лабораторних робіт. Традиційні дослідження електронних пристроїв доповнюються «монтажем», налагодженням та дослідженням моделей аналогічних пристроїв в середовищі « Multisim 10.0».

4. Курсове проектування передбачає виконання за індивідуальним завданням розрахунку, формування в середовищі EWB, налагодження та дослідження типових функціональних вузлів радіоелектронної апаратури. На захист курсової роботи подаються діючі віртуальні моделі спроектованих вузлів та працююча модель всього мікроелектронного пристрою обробки інформації.

5. Самостійна робота студентів при використанні комп`ютерної технології піднімається на якісно вищий рівень. Це забезпечується підготовкою в цифровому форматі базових підручників, навчальних посібників повного систематизованого навчально-методичного комплекту, а також необмеженим об`ємом інформації в мережі Internet. Моделювання радіоелектронних пристроїв в середовищі EWB сприяє формуванню уміння та навичок використання ЕОМ для вирішення завдань професійної діяльності.

Створення та дослідження віртуальних пристроїв суттєво змінює ставлення студентів до навчання. З`являються елементи гри, коли студенти одержують задоволення від того, що вміють «змонтувати» віртуальну схему, усунути помилки і добитись функціювання електронного пристрою.

Використання технології EWB дозволяє поліпшити керованість пізнавальною діяльністю, сприґяє інтенсивній самостійній роботі студентів, а відтак - формуванню конкурентоздатного фахівця.

УДК 37.046

ТРЕБОВАНИЯ К СОВРЕМЕННЫМ ЭЛЕКТРОННЫМ УЧЕБНЫМ МАТЕРИАЛАМ И РАСЧЁТ ТРУДОЗАТРАТ НА ИХ РАЗРАБОТКУ

В.Н. Анохин[1], к.т.н., с.н.с.,
В.В. Огурцов[2], к.е.н.
Харківський національний економічний університет
[1]viktoranohin@online.ua, [2]vitaliy.ogurtsov@hneu.net

К электронным учебным материалам, как элементам образовательных ресурсов можно предъявить следующие категории требований: доступность; рациональность; адаптивность; интерактивность; пригодность.

Возможные на сегодня форматы электронных учебных материалов (ЭУМ) можно разделить на пять типов: 1) простой текстовый документ с рисунками, 2) гипертекст, 3) двумерные мультимедийные материалы (2D Мультимедиа), 4) гипермедиаматериалы (гипермедиа – гипертекст, в состав которого входит структурированная мультимедийная информация разных типов), 5) трёхмерные мультимедийные материалы (3D Мультимедиа). Каждый из ЭУМ указанных форматов может быть разной степени сложности и эффективности, в зависимости не только от характера изучаемого материала, но и от уровня соответствия современным требований к ЭУМ. В связи с этим ЭУМ может: а) не иметь дополнительных возможностей(начальный уровень) или обладать набором дополнительных качеств, б) адаптивностью навигации и методики изложения(2,3,4,5), в) адаптивностью уровня сложности(2,3,4,5), г)начальной интерактивностью (контентно - зависимая навигация, обратная связь на воздействие), (3,4,5), д) средней интерактивностью (условные переходы по результату), (3,4,5), е) высокой интерактивностью

(моделирование учащимися объектов и процессов с мультимедийной обратной связью), (3,4,5), ж) виртуальной реальностью(5). С повышением уровня эффективности ЭУМ растут творческие и технологические затраты на его создание, требуется освоение и применение специализированных программ для ЭУМ, объектно-ориентированного программирования, трёхмерного проектирования и т.д. Для определения трудозатрат на создание электронных учебных материалов {конспектов лекций, практикумов, средств тренинга (ролевых игр), средств контроля (тестов, ролевых игр с оцениванием)} предлагается следующая методика.

В качестве базового применяется формат 1 (для лекций и практикумов это текстовый документ с рисунками в формате файлов doc, pdf, ppt в количестве страниц или слайдов, приведённых к условно-типографским листам (УТЛ); для ролевых игр это текстовый документ с описанием алгоритма ролевой игры, разделённого на сцены (слайды), приведённые к УТЛ; для тестов это текстовый документ, приведённый к УТЛ. Для остальных форматов применяется коэффициент по отношению к базовому. Создание дополнительных качеств учебного материала по сравнению с начальным уровнем учитывается в процентах к трудозатратам начального уровня. В данной методике сохранено приведение учебных материалов к УТЛ для совместимости с имеющейся практикой определения трудозатрат в учебно-методической работе. Коэффициенты для второго формата - 1,2, для третьего – 2, для четвёртого - 2,25. Добавочные проценты: б) и в) 25%, г)25% для всего ЭУМ или в пропорции, д) 35% для всего ЭУМ или в пропорции. Данные получены эмпирическим путём. Затраты на разработку моделирующих модулей для (г) определяются отдельно. Трудозатраты в часах на один УТЛ для формата 1 обычно определены в каждом ВУЗе. Определение коэффициента для формата 5 требует дополнительных исследований.

УДК 004.896

СИСТЕМА АВТОМАТИЧНОЇ ГЕНЕРАЦІЇ ТЕСТОВИХ ЗАВДАНЬ

А.М. Мельник[1], Р.М. Пасічник[2], к.ф-м.н., доцент
Тернопільський національний економічний університет
[1]melnyk.andriy@gmail.com, [2]roman.pasichnyk@gmail.com

В сучасних умовах багато уваги приділяється автоматизованим системам контролю знань, і особливе місце тут займають системи тестування. Багато досліджень присвячено питанням валідності і надійності тестів, питання формування самого банку завдань у більшості випадків залишається виключно прерогативою викладача. Зважаючи на велику трудоємкість та значні інтелектуальні затрат на створення завдань, яка супроводжується питаннями педагогічної цінності сформованих тестів, а також захисту від вгадування без залучення набутих знань - виникає актуальна задача автоматизації процесу створення самих тестових завдань.

Серед відомих методів автоматичної генерації тестових завдань необхідно відзначити – метод на основі параметризованих тестів, метод на основі семантичних мереж, генерація тестових завдань з використанням понятійно-тезисної моделі. Основними недоліками даних підходів є створення завдань з низькою педагогічною цінністю, не проводиться аналіз їх складності, а також значні затрати на підготовку вхідної інформації. Тут виникає задача розробки методу, який би вирішував дані проблеми.

Для розв’язання цієї задачі пропонується система семантичних класів, яка базується на пізнавальній функції природної мови і направлена на розв’язання проблем. Щоб професійно представити сутність проблеми необхідний понятійний апарат. Розв’язання проблем здійснюється за допомогою методів. Обґрунтований вибір методу можна здійснити на основі опису його ефективності, тобто доцільності використання методу в певних умовах. Формальний опис методу допускає його неоднозначне трактування, а його повний опис породжує значну надлишковість. Тому для забезпечення вірного використання методу використовують приклади його конкретної реалізації.

Відомо, що речення (лінгвістичні твердження) можна розглядати, як сукупність компонент, пов’язаних відповідними зв’язками, їх зручно представляти за допомогою деревовидних інформаційних структур.

Наприклад, для семантичного класу метод отримаємо наступну інформаційну структуру:

$$Sm_i = \{[IE_{i,j}, Cp_{i,j}, CS_{i,j}, \Pr n_IE_{i,j}, Op_Dsc]\},$$

де Sm_i - схема методу, $IE_{i,j}$ - ідентифікатор елемента дерева, $Cp_{i,j}$ - ідентифікатор обов’язковості елемента, $\Pr n_IE_{i,j}$ - посилання на батьківський елемент, Op_Dsc - лінгвістичний опис операцій.

Генерація тестових завдань відбувається шляхом маніпулювання елементами структури методів керуючись певними правилами (узгодженість зв’язків, рівнів представлення, відповідність батьківських елементів).

Запропонована методика дозволяє генерувати тестові завдання складної структури, а обґрунтована структура семантичних класів дозволяє уникати неправильних класифікаційних відношень в процесі формалізації навчального матеріалу.

УДК 004.42

ПРОГРАМА ДЛЯ ПЕРЕВІРКИ ТЕКСТІВ НА ПЛАГІАТ

В.В. Войтко, к.т.н., доцент, С.В. Бевз, к.т.н., доцент, О.В. Гавенко, магістрант
Вінницький національний технічний університет
sm@vstu.vinnica.ua

Основними критеріями оцінки ефективності роботи програм перевірки текстів на плагіат є швидкодія та універсальність підходів до ідентифікації масивів текстової інформації.

Метою роботи є підвищення швидкодії та забезпечення універсальних характеристик методів пошуку плагіату. Під об'єктом дослідження розуміємо методи аналізу текстових масивів даних. Предметом дослідження є методи та алгоритми пошуку плагіату в текстових файлах. Основними завданнями роботи вбачаємо розробку принципів, методів та алгоритмів пошуку плагіату та їх реалізацію у комп'ютерній програмі.

Розроблена комп'ютерна програма для перевірки текстів на плагіат реалізована засобами мови програмування C#. У ній реалізовані два методи пошуку плагіату, а саме: метод ідентифікації повного співпадання речень, та метод аналізу кількості співпадання слів. Метод пошуку повного співпадання речень дозволяє забезпечити високу швидкодію пошукової системи. Метод співпадання слів орієнтований на аналіз модифікованих текстових документів, що забезпечує універсальні характеристики використання програми пошуку плагіату. Крім того програмно реалізована можливість комбінованого

виконання запропонованих методів аналізу текстових даних.

Результатом роботи програми є визначення коефіцієнту наявності плагіату в роботі та виділення у досліджених текстах речень, у яких був виявлений плагіат.

Підвищення швидкодії роботи програми забезпечується реалізацією методу ієрархічного конвертуванню вхідної інформації. Вхідний файл розглядається як сукупність речень, а самі речення визначаються сукупністю слів як елементарних символьних елементів текстових документів. За етапом конвертування вхідної інформації слідує етап фільтрації, який дозволяє відфільтрувати неінформативні дані. Програмно реалізовано два режими символьної фільтрації: фільтрація речень та фільтрація слів. Відфільтровуються речення, які містять менше, ніж 30% українських букв, або якщо кількість символів, які у них входять менше 30. Відфільтровуються слова, які містять менше чотирьох букв. Етап фільтрації дозволяє суттєво зменшити обсяг змістовної інформації при збереженні достовірності результату оцінювання. Також підвищення швидкодії роботи програми забезпечується введенням принципу пріоритетності у процес порівняння вхідного файлу з наявними файлами робочої бази даних. Тобто вхідний файл почергово порівнюється з файлами у порядку спадання відсоткового коефіцієнту співпадання, визначеного на етапах попереднього аналізу документів.

Забезпечення універсальних характеристик роботи програми здійснюється шляхом введення методу порівняння слів за коренем у базові алгоритми запропонованих методів пошуку плагіату, що дозволяє суттєво зменшити вплив зумисної модифікації текстів у процесі ідентифікації символьної інформації.

УДК 004.89

ОПРАЦЮВАННЯ ЗНАНЬ В ІНТЕЛЛЕКТУАЛЬНІЙ ІНФОРМАЦІЙНІЙ СИСТЕМІ КЕРОВАНІЙ МОДЕЛЯМИ

Є.В.Буров, к.т.н, доцент
Національний університет “Львівська політехніка”
eugene_burov@yahoo.com

Вузьким місцем у процесі зростання продуктивності інформаційних систем усе більше встають інтелектуальні функції та операції які традиційно виконує людина. Значна частина таких операцій є шаблонними і передбачають виконання визначених дій у визначених ситуаціях. Одним з шляхів вирішення цієї проблеми є делегування операцій аналізу та прийняття рішення у простих рутинних ситуаціях самій системі.

Значна частина робіт в галузі представлення знань у системах штучного інтелекту зосередилася на вивченні представлення декларативних знань. Зокрема, були запропоновані онтології як декларативні формальні моделі предметної області.

Перевагами декларативних систем подання знань є можливість створення цілісної формальної моделі предметної області. Водночас, декларативні системи подання знань мають і ряд суттєвих недоліків, зокрема велику складність.

Альтернативою до декларативного підходу до представлення знань є методологія проектування інтелектуальних систем, що базується на схемах. Головні відмінності такого підходу від використання онтологій полягають в тому, що схема описує фрагмент світу і, як правило, призначена для вирішення певної задачі.

В основу для побудови інформаційних систем керованих моделями доцільно покласти комбінацію обох – декларативного та схемного підходів.

Запропонована система моделювання складається з таких компонент. База фактів містить факти про об'єкти та події зовнішнього світу. Онтологія містить модель предметної області подану як таксономія класів. Моделі визначають які задач вирішуються в кожен момент у системі і як вони вирішуються. Система реагує на визначене коло подій зовнішнього світу та опрацьовує їх створюючи нові або модифікуючи існучі факти.

База знань BdKn це кортеж, що містить базу фактів BdFc, онтологію On, мережу моделей (схем) NMd: $BdKn = (BdFc, On, NMd)$.

База фактів BdFc – це множина фактів про об”єкти та події зовнішнього світу та відношення між ними. Кожен факт та зв”язок є семантично- інтерпретованим, тобто його тип визначено в онтології On: $BdFc = (M(Fc), M(LnFc))$, $\forall Fc_i : Type(Fc_i) \in On$, $\forall LnFc_i : Type(LnFc_i) \in On$

Моделі утворюють мережу що містить множину моделей M(Md) та множину їх зв”язків M(LnMd): $NMd = (M(Md), M(LnMd))$

На відміну від класів онтології, моделі не утворюють чіткої ієрархії, і формують динамічну мережу. Кожна модель може бути в одному з двох станів - активному або пасивному. Активна модель – це модель ініціалізована інформацією з певного контексту. Моделі переходять в активний стан на вимогу інших моделей, або при настанні певних подій. Якщо потреба в моделі відпала, то вона переходить у пасивний стан.

Запропонований підхід до опрацювання знань в інтелектуальній інформаційній системі дозволить створювати системи, які порівняно з існуючими, швидше реагують на зміни вимог та бізнес-середовища.

УДК 004.852

ІГРОВА МОДЕЛЬ З АРБІТРОМ КОЛЕКТИВНИХ РІШЕНЬ В УМОВАХ НЕВИЗНАЧЕНОСТІ

П. О. Кравець, к.т.н., доцент
Національний університет «Львівська політехніка»
krpo@i.ua

Багатоагентна стохастична гра є зручною моделлю колективного прийняття рішень в умовах невизначеності, оскільки дозволяє дослідити процеси конкуренції, кооперації, координації, самоорганізації, навчання та адаптивної поведінки гравців.

Відомі методи ігрового вибору варіантів рішень в основному базуються на відсутності обміну інформацією між гравцями, що спрощує математичний аналіз їх збіжності до станів колективної оптимальності. Врахування обміну інформації між гравцями дозволяє вивчати проблеми кооперативного вироблення та прийняття рішень за рахунок укладання договорів та переговорів.

Метою роботи є побудова методу колективного прийняття рішень в умовах невизначеності з використанням арбітра для координації стратегій гравців.

Гра в умовах невизначеності задається кортежем $\Gamma_{\xi} = (I, \{U^i\}_{\forall i \in I}, \{\xi^i(U\}_{\forall i \in I})$, де $I \neq \varnothing$ – множина гравців, які взаємодіють з середовищем за допомогою скінченного набору чистих статегій $U^i = (u^i(1), ..., u^i(N_i))$, $N_i \geq 2$, вибір яких $u_n^i = u^i$ здійснюється у дискретні моменти часу $n = 1,\ 2,\ ...$ випадково і незалежно на основі векторів змішаних стратегій $p_n^i \in S^{N_i}$, де S^{N_i} – N_i-вимірний

одиничний симплекс. Значення комбінованої стратегії $u_n = u \in U = \underset{i \in I}{\times} U^i$ є колективним рішенням гравців, за яке кожен з них отримує випадковий програш $\xi_n^i(u_n)$.

Допустимо, що математичні сподівання програшів $M\{\xi_n^i(u)\} = v^i(u) = const$ не відомі та мають обмежений другий момент $\sup\limits_n M\{[\xi_n^i(u)]^2\} = \sigma_i^2(u) < \infty$.

Нехай у системі колективного прийняття рішень присутній арбітр, який діючи згідно узагальненого розподілу $q_n \in S^N$, $N = \coprod\limits_{i \in I} N_i$, рекомендує гравцям обрати для реалізації дії, які утворюють комбінований варіант $a_n = (a_n^1, ..., a_n^L) \in U$, де $L = |I|$ – кількість гравців. Гравець з номером i отримує інформацію тільки про компоненту a_n^i комбінованого варіанту $a \in U$. Цей сигнал сприймається гравцем як необов'язкова пропозиція виконати дію a_n^i.

Кожен гравець таємно і незалежно вибирає у момент часу n дійсний варіант дії u_n^i, за що отримує поточний програш:

$$\zeta_n^i(u_n, a_n^i) = \lambda \xi_n^i(u_n) + (1-\lambda)\Delta_n^i(u_n^i, a_n^i), \qquad (1)$$

де $\Delta_n^i(u_n^i, a_n^i)$ – штраф за відмову від запропонованого арбітром рішення a_n^i; $\lambda \in [0,1]$ – ваговий коефіцієнт.

Ефективність поточних ходів гри оцінюється функціями середніх програшів гравців:

$$\mathrm{Z}_n^i = \frac{1}{n}\sum_{t=1}^{n} \zeta_t^i \quad \forall i \in I. \qquad (2)$$

Метою кожного гравця є мінімізація функції середніх програшів (2):

$$\overline{\lim_{n\to\infty}} Z_n^i \to \min \ \ \forall i \in I. \qquad (3)$$

Асимптотичні розв'язки задачі (3) будемо шукати у множині точок корельованої рівноваги, яка визначається об'єднаним розподілом стратегій гравців $q_n \in S^N$, коли кожен агент не має мотивацій, щоб відхилитися від домовленостей в односторонньому порядку.

Формування послідовностей $\{u_n^i\}$ з потрібними властивостями виконаємо на основі рекурентного методу:

$$p_{n+1}^i = \pi_{\varepsilon_{n+1}}^{N_i} \left\{ p_n^i - \gamma_n R\left(\zeta_n^i, p_n^i, u_n^i\right) \right\} \ \forall i \in I \,, \tag{4}$$

де $\pi_{\varepsilon_{n+1}}^{N_i}$ – проектор на одиничний ε-симплекс $S_{\varepsilon_{n+1}}^{N_i} \subseteq S^{N_i}$; $\varepsilon_n > 0$, $\gamma_n > 0$ – монотонно спадні послідовності величин; $R\left(\zeta_n^i, p_n^i, u_n^i\right)$ – вектор, що визначає середній напрямок на оптимальний розв'язок стохастичної гри. При $R\left(\zeta_n^i, p_n^i, u_n^i\right) = \zeta_n^i / (e^{\mathrm{T}}(u_n^i) p_n^i)$ з (4) отримуємо градієнтний метод стохастичної апроксимації.

Змішана стратегія арбітра визначається поточними стратегіями гравців:

$$q_n = \left(\prod_{i \in I} p_n^i(u_i) \middle| u_i \in u, \forall u \in U \right), \tag{5}$$

що дозволяє знаходити рівноважні за Нешем розв'язки гри.

Вибір чистих стратегії арбітра та гравців може здійснюватись детерміновано або випадково. Детерміно-вана процедура базується на визначенні аргумента максимального значення розподілу стратегій. При випадковому виборі чисті стратегії арбітра визначаються з імовірностями q_n (5), а чисті стратегії гравців – з імовірностями p_n^i $\forall i \in I$ (4).

Стохастична гра повторюється у моменти часу $n := n+1$ до виконання умови точності $\left\| p_{n+1}^i - p_n^i \right\| < \varepsilon \ \forall i \in I$ або до досягнення заданої кількості кроків $n = n_{\max}$.

УДК 519.21:681.142

ИНТЕЛЛЕКТУАЛЬНЫЕ ВЕБ-АГЕНТЫ ДЛЯ ПОИСКА И ПУБЛИКАЦИИ ИНФОРМАЦИИ

П.А. Помилуйко, м.н.с.
Международный научно-учебный центр информационных технологий и систем

В работе рассматривается проблематика структуризации, поиска и размещения информации в сети Интернет. Предлагается комплексное решение поставленной задачи – построение информационной системы, используя современные технологии и интеллектуальное управление.

Большинство реализованных поисковых систем в Интернете находятся на зачаточном уровне развития и являются не конкурентоспособными, поскольку их эксплуатация трудна и экономически не выгодна. Поисковая система в ответ на нечеткий запрос выдает адреса страниц и дальнейший поиск информации пользователь ведет уже, перейдя по одному из предложенных вариантов. Выбирая нужные ему ссылки, пользователь уточняет область интересов своего поиска и доходит до конечного результата. Если необходимой информации не оказалось или она не удовлетворяет требованиям пользователя, он возвращается в поисковую систему, выбирает новую страницу, и снова проходит путь по ссылкам. На этот процесс уходит не только много времени и действий, но также и потраченные нервы.

Лицам, ведущим предпринимательскую деятельность на Украине, необходимо потратить немало времени и средств для реализации технологически современного веб-сайта, который еще нужно продвинуть, чтобы донести информацию к целевой аудитории. Поэтому вопрос о конструировании многофункциональной информационной системы, которая

поможет упорядочить и структурировать информацию в Интернете является актуальным.

Впервые на Украине запущен сервис для быстрого конструирования профессиональных веб-сайтов, который поможет избавиться от многих сложностей и упростить работу пользователей. Система представляет собой комплекс программных, лингвистических и логико-математических средств для реализации основной задачи: осуществление поддержки деятельности человека, публикации и поиска информации в режиме продвинутого диалога. Применение современных технологий позволило полностью контролировать процесс разработки веб-сайтов, что позволило существенно сократить время и затраты, связанные с этим процессом.

Целями создания системы «БУД» было желание избавить клиента от необходимости думать о сложных технических деталях и сократить время работы над веб-сайтом до минимума. В результате, было предоставлено современное удобное решение, как для пользователей, так и достойная альтернатива для разработчиков. Специализированная информационная система, где все основные процессы автоматизированы, изначально спроектирована под специфику сети Интернет и построена на платформе современного программного обеспечения. Она предназначена для обеспечения взаимодействия между пользователями и удовлетворения информационных потребностей в сфере товаров и услуг.

Большой объем товарных предложений, развитые средства поиска и просмотра необходимой информации, гибкие возможности администрирования, современные средства сбора статистики, эргономичный интерфейс с интерактивной помощью, интегрированная CRM-система, бесплатный доступ не только с ПК, но и с любого мобильного устройства делают ее мощным средством маркетинга для каждого участника рынка. Система рассчитана как на конечного потребителя услуг, так и на крупного производителя или другого субъекта предпринимательства.

УДК 004.031.42:37

АДАПТИВНІ КОМП'ЮТЕРНІ СИСТЕМИ В НАВЧАННІ

Д.Ю. Явтушкевич, магістрант
Національний технічний університету України «Київський політехнічний інститут»

Адаптивні системи в навчанні націлені на збільшення ефективності навчання з допомогою електронних засобів.

Сучасні технології дозволяють зберігати великі об'єми інформації малими витратами, використовувати значно більші можливості при відтворенні порівняно з паперовим форматом та взаємодіяти з користувачем під час прочитання документу. Це робить електронну освіту привабливою і актуальною, про що свідчать незліченні публікації про дистанційне навчання, потребу, користь та особливості складання електронних підручників, використання мультимедіа в навчанні та впровадження державними установами використання електронних читачів.

Застосування адаптивних систем є рішенням проблеми різного рівня підготовки тих хто навчається та допомагає врахувати їх індивідуальні особливості: під час роботи такої системи матеріал витягається з бази знань компонується за певними правилами і передається користувачу вже в підготовленому вигляді. Механізм компоновки використовує як мінімум одне з джерел інформації про користувача, це може бути дані про психологічні типи користувачів, досвід роботи користувача з системою, результати оцінки знань користувача при початку роботи з системою тестуванням.

Крім того статистику роботи користувачів з системою можуть використовувати автори навчальних курсів для розуміння того, як саме краще сформувати матеріал.

Адаптивні системи є результатом розвитку технологій штучного інтелекту у освіті (AI-CAI), що з'явилися у 1970-х роках. Технологія штучного інтелекту у освіті у 80-х переросла в інтелектуальні навчаючі системи (ITS), потім у кінці 90-х на адаптивні і інтелектуальні освітні системи на основі Інтернет (AIWBES). Кожний етап приносив досвід роботи з досліджуваними системами, він описаний у наукових статтях та тезах конференцій і доступний в Інтернеті.

Сучасний варіант адаптивної системи використовує базу знань та модель користувача. База знань має містити в собі фрагменти матеріалу і метадані які описують кожний фрагмент і зв'язки з іншими фрагментами. Широко використовуються стереотипна або оверлейна модель користувача. Під час роботи за оверлейною моделлю визначається рівень знань користувача по окремим темам, при роботі за стереотипною моделлю користувач асоціюється з однією з заздалегідь занесених груп. Результат роботи адаптивних систем можна згрупувати у такі категорії: адаптація інтерфейсу – більше стосується індивідуальних особливостей користувача (наприклад покращення роботи з системою при вадах зору); адаптація вмісту – компонування матеріалу розділу з фрагментів ґрунтуючись на рівні знань користувача; адаптація порядку подачі матеріалу – визначення оптимального для сприйняття порядку тем, розділів. В подальших дослідженнях варто приділити увагу адаптації вмісту на окремій сторінці, опису результатів застосування педагогічних методів під час використання цих систем та дослідження негативних наслідків впровадження систем.

УДК 681.32

НОВИЙ ПІДХІД ЩОДО АВТОМАТИЗАЦІЇ ОПТИМІЗАЦІЇ ВПЛИВУ ПРОТИПАВОДКОВИХ СПОРУД НА ВОДНІ ОБ'ЄКТИ

В.Б. Мокін[1], д.т.н., професор, Л.М. Скорина[2], асистент
Вінницький національний технічний університет
[1]vbmokin@gmail.com, [2]gavrishko@gmail.com

За останні роки зросла кількість та інтенсивність руйнівних паводків на річках України. З метою попередження шкідливої дії вод і ліквідації її наслідків є актуальною розробка нового підходу щодо моделювання та оптимізації впливу гідротехнічних споруд на водні об'єкти.

Для регулювання та оптимального управління паводковим стоком пропонується розробляти геоінформаційну модель, яка містить атрибутивні та просторові характеристики паводкорегулюючих споруд та дані про водні об'єкти басейну.

Комплексне поєднання геоінформаційних моделей гідрографічної мережі басейну та системи гідротехнічних споруд забезпечується через модель зв'язків та відношень, що дозволяє відстежити взаємовпливи та динаміку зміни їх характеристик.

В основі вибору оптимальної конструкції гідротехнічної споруди покладено метод факторного аналізу. Підхід щодо оптимізації впливу протипаводкових споруд на водні об'єкти полягає у підборі параметрів гідротехнічних споруд з мінімальною вартістю будівництва й найменшими витратами на реконструкцію з урахуванням їх комплексного впливу на водні об'єкти у період паводків.

Дана розробка дозволяє своєчасно виявити незадовільний стан гідротехнічних споруд та забезпечити вчасне втручання фахівців з раціональним вкладенням коштів для підтримання усього комплексу водних об’єктів басейну в належному стані.

Для практичної реалізації підходу можна використати геоінформаційні системи, створені на основі технології просторово-орієнтованого представлення даних колективом науково-дослідної лабораторії екологічних досліджень та екологічного моніторингу Вінницького національного технічного університету для басейнів великих та середніх річок України: Південний Буг, Дністер, Сіверський Донець, Прип’ять, Тиса (рис. 1), Кальміус.

Рис. 1 – ГІС басейну р. Тиса з гідротехнічними спорудами

Реалізація нового підходу дасть змогу забезпечити безпечні умови проживання населення, відновити сприятливий гідрологічний стан водних об’єктів, поліпшити умови пропуску паводків, мінімізувати збитки від шкідливої дії вод та можливі затрати на відновлення існуючих та будівництво нових протипаводкових споруд.

УДК 681.32

НОВИЙ ПІДХІД ДО ІДЕНТИФІКАЦІЇ ТА ФОРМАЛІЗАЦІЇ ГЕОІНФОРМАЦІЙНОЇ МОДЕЛІ ТРАНСПОРТНОЇ МЕРЕЖІ НА ОСНОВІ ГІС-МОДЕЛЕЙ ЇЇ ЕЛЕМЕНТІВ

В.Б. Мокін[1], д.т.н., професор, В.Г. Сторчак[2], аспірант
Вінницький національний технічний університет
[1]vbmokin@gmail.com, [2]storchak@rambler.ru

Проблема завантаженості доріг великою кількістю транспорту робить актуальним різні методи та технології оптимального управління транспортними потоками.

Існує багато моделей, методів та технологій моделювання та оптимізації параметрів транспортних мереж (ТМ), але вони не дозволяють гнучко та швидко враховувати нові фактори та взаємовплив одних факторів на інші. Наприклад, необхідність врахування нових об’єктів транспортної інфраструктури або погіршення умов пересування (стан доріг, «пробки» тощо) транспортних засобів вимагає значного часу на ідентифікацію та оптимізацію раніше побудованої моделі цієї мережі. Прискорити розв’язання цієї задачі можна, попередньо побудувавши інформаційні моделі елементів ТМ та процесів, які впливають на зміну параметрів транспортних потоків у місті. Ці моделі повинні враховувати як статичні та динамічні параметри елементів, так і співвідношення, що описують зміну цих параметрів під впливом інших елементів ТМ.

Визначивши типові елементи транспортної мережі та об’єкти транспортної інфраструктури міста, потрібно ідентифікувати їх атрибутивні і просторові параметри та

зв’язки між ними. Враховуючи просторову розподіленість елементів транспортної мережі, атрибутивні і просторові параметри та зв’язки між ними найкраще формалізувати у вигляді геоінформаційної моделі (ГІС-моделі). ГІС-модель узагальненої транспортної мережі у вигляді певних з‘єднань її просторових елементів, яке відповідає топологічній будові елементів, тобто їх розташуванню у просторі один відносно іншого, описує основні параметри мережі. Атрибутивні параметри елементів містяться в базі даних ГІС у вигляді числових або текстових даних про кожен елемент.

На основі цих даних потрібно сформувати набір правил (атрибутивних та топологічних відношень), які дозволять встановити чіткі зв’язки між елементами мережі. Набір топологічних відношень можливо автоматично отримати з набору геопросторових даних (карта), а атрибутивні відношення визначаються на основі даних, отриманих із технічної документації, правил, ДСТУ тощо.

Після ідентифікації ГІС-моделей елементів ТМ слід відібрати лише ті елементи, які є найбільш важливими для розв’язання тієї чи іншої задачі оптимізації ТМ, і на основі ГІС-моделей цих елементів побудувати узагальнену ГІС-модель усієї ТМ.

Таким чином, запропоновано новий підхід до ідентифікації та формалізації геоінформаційної моделі транспортної мережі на основі ГІС-моделей її елементів, який на відміну від існуючих дозволяє гнучко та оперативно враховувати чи не враховувати ті чи інші елементи транспортної мережі з урахуванням їх параметрів, розташування, просторових топологічних відношень, правил обробки даних та взаємовпливу з іншими елементами транспортної мережі.

УДК 504.06+004.9

АВТОМАТИЗАЦІЯ ПЕРЕВІРКИ ІНФОРМАЦІЙНОЇ ПОВНОТИ ТА НЕСУПЕРЕЧЛИВОСТІ В ГЕОІНФОРМАЦІЙНИХ СИСТЕМАХ ЕКОЛОГІЧНОГО МОНІТОРИНГУ ТА УПРАВЛІННЯ

В.Б. Мокін[1], д.т.н., професор
Д.Ю. Кульомін[2], студент
Вінницький національний технічний університет
[1]vbmokin@gmail.com, [2]duk@krovatka.su

Як відомо, при роботі з картографічною інформацією часто мають місце суперечливості у представленні просторових об’єктів. На даний момент існують автоматизовані засоби, які дозволяють знайти та виправити подібні помилки. Але це стосується тільки топографічних суперечливостей, а отже виникає необхідність розробки методів ідентифікації «логічних» помилок (приклад: річка не може розміщуватись на дамбі; для дамби, яка розташована на річці шириною 150 метрів, матеріалом не може бути дерево).

Отже, актуальною є розробка моделі зв’язків між просторовими об’єктами, визначення принципів і методів ідентифікації суперечливих зв’язків між об’єктами та можливості їх виправлення для відомих ГІС-пакетів програм. Важливим є забезпечення можливості автоматизованого введення та перевірки повноти і достовірності інформації, наприклад, про гідротехнічні споруди та стан водних об’єктів. При цьому слід оперувати, головним чином, атрибутивною інформацією та відомостям щодо топології просторових об’єктів ГІС басейнів річок України.

Задача виправлення топологічних суперечностей на даний момент є автоматизованою (такі універсальні продукти як ГІС «Панорама» та «ArcGIS» дозволяють це зробити). Натомість задача розв'язання логічних суперечностей є не вирішеною, а отже потребує детального вивчення, оскільки пошук та виправлення помилок такого роду є досить трудомісткою і рутиною роботою.

Авторами запропоновано новий підхід щодо автоматизації пошуку на основі ідентифікації моделі зв'язку між картографічними об'єктами, з урахуванням інформації баз даних, за рахунок перехресної перевірки коректності цих моделей для підвищення коректності даних у ГІС.

УДК 681.51+519.6+556.013

НОВИЙ ПІДХІД ДО МОДЕЛЮВАННЯ ЯКОСТІ ВОДИ У РІЧКОВИХ СИСТЕМАХ З ВИКОРИСТАННЯМ ЗАСОБІВ ПАРАЛЕЛЬНИХ ОБЧИСЛЕНЬ

В.Б. Мокін, д.т.н., професор, В.Ю. Булига, студент, К.Ю. Вознесенський, студент
Вінницький національний технічний університет
vbulyga@gmail.com

На сьогоднішній день надзвичайно актуальною є проблема чистої води, що відповідала б різноманітним вимогам водокористування. І тому актуальним є дослідження нових шляхів поліпшення стану природних вод.

Зазвичай при вимірюванні показників якості води вимірюють фонову концентрацію вище місця скиду забруднюючих речовин, в місці безпосереднього скиду і далі за течією в місці, де знаходиться створ спостереження. Тому виникає проблема визначення показників якості води між точкою скиду та створом, що на практиці реалізувати доволі складно та вимагає великих матеріальних затрат.

Для даної задачі зазвичай використовують таку математичну модель:

$$x_0 \cdot e^{-kT1} + U_1 \cdot e^{-k(T_1-\tau_1)} = x_1$$

$$x_0 \cdot e^{-kT1} + U_1 \cdot e^{-k(T_1-\tau_1)} + U_2 \cdot e^{-k(T_2-\tau_2)} = x_2$$

В реальних умовах для визначення точних показників якості води в конкретній річці потрібно розглядати річкову систему загалом, тобто разом з її притоками, які, в свою чергу, містять власні джерела забруднення.

В такому випадку математична модель ускладнюється і тому відповідно значно ускладнюється її реалізація.

Рис. 1 – Схема ділянки річки із двома входами – скидами стічних вод

В такому випадку математична модель ускладнюється і тому відповідно значно ускладнюється її реалізація.

Прискорити виконання розрахунків заданої математичної моделі дозволяє застосування паралельних обчислень за допомогою кластерів. Кластер — це декілька незалежних обчислювальних машин, що використовуються спільно і працюють як одна система для вирішення тих чи інших задач, наприклад, для підвищення продуктивності, забезпечення надійності, спрощення адміністрування, тощо.

Обчислювальний кластер потрібен для збільшення швидкості обрахунків за допомогою паралельних обчислень. Обчислювальний кластер, як і будь-яка система паралельних обчислень, є ефективним, коли обчислювальна задача, яку необхідно вирішити, принципово не може бути вирішена за допомогою комп'ютерів широкого вжитку (наприклад, персональних комп'ютерів) або вирішення задачі за допомогою поширених систем вимагає тривалого часу.

Основна ідея підходу полягає в тому, що якість води у річці змінюється внаслідок, головним чином, впливу вод її приток та скидів стічних і зворотних вод. А якість води на виході приток, у свою чергу, змінюється внаслідок впливу вод приток цієї притоки та скидів стічних і зворотних вод у неї ж. Отже, пропонується моделювати якість вод спочатку у притоках річки, а потім – у головній річці. Далі результат моделювання слід порівнювати з експериментальними даними. Якщо дані не збігаються, тоді –

проводити перерахування спочатку якості води у головній річці, а потім – у її притоках. Таким чином, можна паралельно обчислювати на різних комп'ютерах моделі для різних приток однієї річки. І окремо, на іншому комп'ютері – моделювати якість води у головній річці. Все це дозволяє значно пришвидшити усі розрахунки та розв'язувати дуже складні задачі моделювання та прогнозування якості вод у розгалуженій річковій системі за умов невизначеності або розмитості багатьох вхідних даних, програвати різні сценарії зміни стану вод та їх реакцію на різні природні та антропогенні впливи, що сприятиме виробленню науково обґрунтованих оптимальних управлінських рішень.

Рис. 2 – Річкова система з притоками та джерелами скиду забруднюючих речовин

Проведено випробування даного підходу на комп'ютерному кластері Вінницького національного технічного університету (10 машин по 2Гб оперативної пам'яті з Celeron Dual-Core 1.6 Ггц і жорсткими дисками по 250Гб, маршрутизатор зі швидкістю портів 1Гбіт) для тестового прикладу річкової системи. Випробування продемонстрували високу швидкість розрахунків та перспективу даного підходу.

Таким чином, запропоновано новий підхід до моделювання якості води у річкових системах, який відрізняється від існуючих можливістю паралелізації та прискорення розрахунків з використанням комп'ютерного кластеру. Працездатність підходу підтверджена тестовими випробуваннями.

УДК 681.32

ВИКОРИСТАННЯ ГІС-ТЕХНОЛОГІЙ ДЛЯ АНАЛІЗУ ПОТЕНЦІАЛУ ЗМЕНШЕННЯ ВИКИДІВ ПРОМИСЛОВОСТІ УКРАЇНИ ЗА РАХУНОК ПРОЕКТІВ СПІЛЬНОГО ВПРОВАДЖЕННЯ

В.Б. Мокін, д.т.н., професор,
Н.В. Гончар, студент
Вінницький національний технічний університет

Як відомо, зобов'язання з обмеження та скорочення викидів парникових газів (двоокис вуглецю, метан, закис азоту або фторвмісні гази) визначені у Кіотському протоколі, який було узгоджено на третій сесії Конференції Сторін Рамкової конвенції ООН про зміну клімату (грудень 1997 р., Кіото, Японія). Нині тенденція до зростання забруднення атмосферного повітря відновилась (Рисунок 1). Водночас, Кіотський протокол відкрив багато можливостей для скорочення викидів парникових газів, зокрема – проекти спільного впровадження (ПСВ), спрямовані на скорочення або поглинання викликаних діяльністю людини викидів парникових газів.

Для визначення потенціалу зменшення викидів промисловості України (або окремих її регіонів) за рахунок ПСВ пропонується підхід, який полягає в аналізі підприємств-джерел викидів у розрізі складових технологічного циклу виробництва, який дозволяє виявити ті складові, де доцільно застосування типових ПСВ (котельні, системи енергопостачання, звалища відходів тощо), нанесенні їх на карту ГІС та визначенні потенціалу розробки та видів оптимальних ПСВ для них. Запропонований підхід дозволить

прискорити впровадження ПСВ в Україні, і, через це, зменшить викиди парникових газів у повітря країни.

Рисунок 1 – Карта викидів забруднюючих речовин в атмосферу від стаціонарних джерел України з місцями впровадження ПСВ та розробниками ПСВ (за даними офіційного сайту Мінприроди України)

Запропонований підхід доцільно реалізовувати за таким алгоритмом:

1. Визначити типові види ПСВ, які доцільно застосовувати у виробництвах тих чи інших галузей та у тих чи інших регіонах.

2. Зібрати інформацію та побудувати карту стаціонарних джерел викидів з деталізацією по населених пунктах.

3. На основі аналізу видів галузей, етапів виробництва та викидів підприємств оцінити потенціал ПСВ для них.

4. Побудувати карту потенціалу розробки ПСВ та місць вже розроблених проектів та визначити пріоритетні напрямки розробки ПСВ.

На рисунку 1 наведена подібна карта у розрізі областей України.

УДК 004.652

ПРО ФОРМАЛІЗАЦІЮ ДАНИХ ЕКОЛОГІЧНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

М.П. Боцула, к.т.н., доцент
Вінницький національний технічний університет
botsual@gmail.com

Якщо проаналізувати всю різноманітність даних екологічного контролю, які збираються у існуючих інформаційних системах (ІС), то стає очевидним, що існує декілька спільних аспектів, які дозволять сумістити ці дані і визначити основу для побудови певної узагальненої структури. Така структура даних є базисом побудови екологічних ІС різного призначення, які будуть прозоро сумісні між собою. Якщо виходити з того, що головною інформацією в екологічних ІС є дані результатів вимірювань (РВ) показників стану навколишнього середовища, то можна запропонувати чітку реляційну структуру для їх представлення. Саме ці дані є основою екологічного контролю.

Основними загальними ознаками всіх даних РВ є належність їх до певної географічної координати, час вимірювання і показник, який досліджувався. Тобто можна стверджувати, що РВ однозначно характеризується трьома складовими: просторовою, часовою ознаками та об’єктом, стан якого представлений значенням РВ.

З врахуванням того, що кожний факт отримання РВ супроводжується певною документацією, умовами відбору та іншими атрибутами, які відіграють суттєву роль при аналізі даних, то до характеристик РВ необхідно включити ознаку, що

забезпечує зв'язок з такими даними, її будемо називати "додатковою".

Таким чином сукупність РВ та наведених ознак можна розглядати як "атомарну" одиницю інформації системи.

Кожна складова такої атомарної одиниці в свою чергу характеризується безліччю ознак, які можна поділити на певну визначену кількість категорій. Причому ці ознаки можуть бути різними для різних систем, мати власний набір характеристик та пов’язаних даних. Однак їх роль "зовнішня", вони несуть таку довідникову інформацію, за якою виконуються вибірки і аналіз даних. Як показує практика "зовнішня" інформація є особливою для кожної окремої екологічної ІС, є мінливою з часом, і фактично має динамічну структуру.

З врахуванням цього у найпростішому випадку виникає потреба у створенні загального ієрархічного переліку категорій ознак і самих ознак які можуть бути використані для уточнення характеристик складових РВ. Але при цьому врахування всіх необхідних зв’язків потребує реалізації занадто складної структури даних.

Частково, в межах можливостей реалізації, використання ієрархічного переліку категорій ознак реалізований в існуючих екологічних ІС. Але як показала практика, кожна з них має ряд суттєвих недоліків, які приводять до неможливості масштабування, розвитку і інтеграції цих систем.

Для уникнення таких недоліків пропонується будувати ІС на основі реляційної моделі даних для "атомарної" інформації, та об’єктно-орієнтовної моделі або документно-орієнтовної моделі для "зовнішньої" інформації.

Така реалізація надасть можливості інтеграції даних екологічних ІС, можливості уніфікованих підходів до аналізу і обробки даних, можливості зручного масштабування і кластерізації ІС.

УДК 631.514

СТВОРЕННЯ ІНФОРМАЦІЙНИХ РЕСУРСІВ ЕКОЛОГІЧНОГО МОНІТОРИНГУ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ WEB 2.0

Г.В. Горячев, к.т.н., доцент
Вінницький національний технічний університет
gorgeorg@vstu.vinnica.ua

У сучасних умовах збільшується інтерес людства до стану навколишнього середовища. Тому виникає необхідність глобалізованого накопичення даних про стан навколишнього середовища для створення систем комп'ютерного екологічного моніторингу на основі Web-сервісів. Найбільш масовим, динамічним і функціональним інформаційним ресурсом є всесвітня мережа Internet. Нечисленні існуючі інформаційні ресурси Internet екологічного моніторингу України в основному не містять динамічно оновлюваної інформації про екологічний стан навколишнього середовища. Ведучі ж розробки систем моніторингу, засновані на інформаційно-вимірювальних системах охоплюють територіально лише окремі підприємства, населені пункти або райони з-за їх високої вартості і низької надійності. У той же час, в Україні не існує єдиного інформаційного ресурсу національного масштабу, який об'єднав би всі доступні джерела даних про стан навколишнього середовища (наприклад, дані екологічної інспекції, санепідемстанції, басейнових управлінь водних ресурсів, гідрометеорологічної обсерваторії, МНС, підприємств).

Пропонується новий підхід до створення інформаційних ресурсів екологічного моніторингу на основі технологій Web 2.0. Основні принципи технології Web 2.0 – інтерактивність (наповнення ресурсу формується не тільки розробниками, а і

користувачами), синдикація (повне або часткове використання у якості джерел інформації інших сервісів Internet), соціалізація (використання технологій, що дозволяють створювати спільноти користувачів або професійні спільноти).

Запропонований підхід для створення інформаційного ресурсу передбачає накопичення даних моніторингу завдяки наданню необхідних функціональних і інформаційних сервісів зацікавленим особам і підприємствам у мережі Internet. Завдяки такому підходу стає можливим централізоване накопичення та обробка інформації різних суб'єктів моніторингу. За адресами http://ond86.eco-pro.org.ua/ і http://mns.eco-pro.org.ua/ знаходяться приклади реалізації інформаційних Web-ресурсів для моделювання поширення забруднюючих (рис. 1) за методикою ОНД-86 і небезпечних хімічних речовин за методикою МНС. Зазначені ресурси дозволяють забезпечити основні принципи технології Web 2.0, що дає можливість глобалізувати екологічний моніторинг в Україні.

Рис. 1. – Розрахунок приземних концентрацій забруднюючих речовин від викидів стаціонарних джерел (ТЕЦ5, м. Київ) та побудова тематичної карти забруднення

УДК 369.54

ПРОГНОЗУВАННЯ ОБСЯГІВ ВИПЛАТ СТРАХОВИХ КОМПАНІЙ

Р.М. Пасічник, к.ф.-м.н., доцент,
А.В. Ковбасістий, студент
Тернопільський національний економічний університет
roman.pasichnyk@gmail.com

Жорстка конкуренція на страховому ринку приводить до наявності в портфелях страхових компаній ризиків із високою відповідальністю. Для їх мінімізації використовується процедура перестрахування. З метою забезпечення економічної ефективності рішення про ініціювання або призупинення перестрахування послуг раціонально приймати на основі прогнозних оцінок значень показників сум платежів та виплат по відповідних страхових послугах.

Класичні методи прогнозування передбачають побудову точкових прогнозів, які не враховують ступеня невизначеності майбутніх значень. Використання апарату нечітких функцій для підвищення надійності такого роду прогнозів недостатньо досліджені. Проведенню такого дослідження присвячена дана робота.

Найпростіша прогнозна оцінка може бути побудована на основі усереднених оцінок за річний період. Прогнозована на наступний рік усереднена нестача обсягів страхувальних фондів PFS для виплати прогнозованих відшкодувань PVD по певному виді страхових послуг vs приведе до ініціювання перестрахування

$$\mathrm{PVD}_{\mathrm{vs}} \geq \mathrm{PFS}_{\mathrm{vs}}.$$

Перекриття прогнозованими страхувальними фондами прогнозів обсягів страхувальних виплат приведе до призупинення перестрахування по відповідних видах послуг на наступний річний плановий період

$$PVD_{vs,m} < PFS_{vs,m}.$$

Такі емпіричні оцінки не враховують динаміки показників діяльності компанії на протязі року. Її врахування дозволить проводити перестрахування по окремих місяцях року і за рахунок цього економити витрати на виплату відшкодувань.

Для прогнозування обсягів виплат та поступлень використано апарат нечітких функцій. Найімовірніше прогнозне значення будується на основі методу Тріга-Ліча, а побудова мінімально та максимально можливих значень здійснюється згідно допоміжних співвідношень. Верхня $(PPVD_U, PPFS_U)$ та нижня $(PPVD_B, PPFS_B)$ межі прогнозного коридору для обсягів необхідних страхових відшкодувань та фонду страхових виплат вважаються пропорційними усередненому граничному приросту значень прогнозованої величини. Ці прирости будуються згідно методу Холта. Наприклад

$$PPVD_U_{vs,m} = PPVD_T_{vs,m} + \Delta_U \cdot ZSV_{vs,m},$$

де коефіцієнти пропорційності Δ_U, Δ_B визначаються початковими значеннями $\Delta^0{}_U, \Delta^0{}_B$ та динамічно коригуються. Зокрема, якщо поточне значення спостережених величин більше прогнозованої верхньої межі, то збільшуємо коефіцієнти пропорційності цієї межі. Проведені чисельні експерименти із модельними та реальними даними підтвердили ефективність запропонованої методики.

УДК 681.51

АЛГОРИТМ УПРАВЛІННЯ ІННОВАЦІЙНОЮ МОДЕЛЛЮ ВИРОБНИЧОГО КОМПЛЕКСУ

Є.Н. Федорчук, к.т.н., доцент,
Н.М. Ткаченко, асистент
Національний університет «Львівська політехніка»
ntkachenko@ukr.net

Законом України від 22 жовтня 2008 р. затверджена Загальноцільова економічна програма розвитку промисловості до 2017 року. Метою програми є створення передумов для досягнення промисловістю якісно нового рівня розвитку, посилення промислового потенціалу держави, забезпечення його конкурентоспроможності. Це передбачає активізацію трансформаційно-інвестиційної діяльності з позитивним впливом на її обсяги і структуру виробництва, прискорення інтеграції промислового комплексу у світове виробництво. Програма передбачає інноваційні перетворення в структурі промисловості і має забезпечити умови для виходу на якісно новий її рівень по масштабності, конкурентоспроможності, інновативності і екологічній безпеці.

За напрямком інноваційних перетворень структури вітчизняних підприємств розроблена модель вітчизняного виробничого комплексу. В цій моделі всі фази з’єднані між собою, вихідні дані однієї фази можуть бути вхідними для іншої/інших фаз. На кожній фазі присутні певні технологічні процеси, сукупність яких створюють фазу. Технологічні процеси мають характеристики – їх показники. Для забезпечення заданої якості продукції, що виготовляється, такі характеристики/показники необхідно

контролювати. Крім перевірки на відповідність показників технологічних процесів для кожного підприємства-складника задається наперед і контролюється часовий період, на протязі якого підприємство повинно виконати свою роботу. У випадку невиконання підприємством заданих наперед якісних і часових показників на підприємство накладається санкція. Якщо невиконання заданих параметрів продовжується, підприємство, яке порушує режим забезпечення якості, виключається і замінюється іншим, з аналогічними можливостями.

Розроблена інноваційна структура містить у своєму складі підприємства, що виконують функції, які раніше були відсутні, і виникли у зв'язку зі зміною середовища функціонування підприємства. Така структура є достатньо складною і потребує відповідного управління.

Для управління такою структурою необхідно задавати наперед показник технологічних процесів, що відбуваються на кожному підприємстві, і отримувати від підприємств-складників підтвердження їх виконання, а також для кожного підприємства здійснюється перевірка терміну виконання роботи на відповідність заданому.

Україна традиційно володіє потужнім промисловим потенціалом. Зміна середовища функціонування вимагає реорганізації структури промислового підприємства. Для забезпечення випуску конкурентоспроможної (якісної) продукції реорганізація структури має враховувати вимоги міжнародних стандартів якості ISO серії 9000.

Формалізовано технологію побудови інноваційного виробничого комплексу. Визначено контрольовані показники, що забезпечують якість продукції, яка виготовляється. Розроблений алгоритм управління виробничим комплексом, структура якого базується на процесному підході у відповідності до вимог стандартів ISO серії 9000.

УДК 62.50

МОДЕЛИ ДЛЯ АНАЛИЗА РИСКОВ РАЗВИТИЯ

Г.Ю. Дерман, магистр, В.А. Северилов, к.т.н., доцент
Винницкий национальный технический университет
taisaborovska@gmail.com

Рассматриваются математические модели оптимальных процессов. Оптимальный процесс развития - результат решения вариационной задачи с интегральным критерием типа «накопленная суммарная прибыль за плановый период». Развитие: изменения производственных мощностей, номенклатуры, конструкций и технологий продуктов производства. Для процессов развития характерны многочисленные источники неопределённостей. Даже если частотные распределения для неопределённостей известны, получение частотных распределений для выходных параметров – тяжёлая проблема, поскольку производственная система - сложный нелинейный и нестационарный «преобразователь» случайных входов.

В работе ставятся в комплексе три цели: - анализ и построение моделей источников рисков; - разработка программных модулей - «инструментов» анализа рисков; - разработка программных модулей – средств управления рисками. Разработка базируется на программе оптимального развития производственной системы и модели децетрализованной системы «производители – продукты. Программа оптимального развития использует метод оптимального агрегирования для оптимального одношагового распределения обобщённых ресурсов «в пространстве» - между подсистемами и продуктами и метод принципа максимума для оптимального распределения ресурсов между

накоплением и развитием «во времени» - по шагам процесса развития.

Рациональная декомпозиционная структура модели, ориентация на воспроизведение механизмов развития, производства, спроса и управления, а не статистических зависимостей, позволяет легко уточнять и вводить новые механизмы – непосредственно в среде математического пакета, минуя этап «формул, набранных в текстовом редакторе формул» упрощает процедуру получения функций чувствительности.

Обусловленная рациональной декомпозиционной структурой вычислительная эффективность моделей позволяет легко получать виртуальную статистику на выборках в тысячи реализаций. Используемая технология построения моделей гарантирует для специалиста получение практических и теоретических результатов. Ниже приведен малый фрагмент – пример результата моделирования процесса развития с учётом неопределённостей и управления класса «горизонт прогнозирования».

УДК 681.3

ІНФОРМАЦІЙНА СИСТЕМА ДЛЯ ПІДБОРУ ТА ОЦІНЮВАННЯ ПЕРСОНАЛУ

Н.Р. Кондратенко, к.т.н., доцент,
С.В. Лужецький, аспірант
Вінницький національний технічний університет

Інформаційні технології широко впроваджуються в різні сфери людської діяльності і, зокрема, у сферу управління персоналом. Менеджери з персоналу будь-якої компанії або спеціалісти рекрутингової фірми активно використовують останні досягнення інформаційних технологій для пошуку кращих фахівців для своїх компаній і клієнтів.

У доповіді розглядається автоматизована інформаційна система, що інтегрує комп'ютери, відеокамери, смартфони і телефони та забезпечує комплексну автоматизацію багатьох процесів, які на цей час виконуються людиною. Структуру такої системи наведено рис.1.

Для пошуку кандидатів на існуючі вакансії використовуються такі можливості Інтернету:

- соціальні мережі. Чисельні соціальні мережі перетворюються в місця встановлення ділових контактів і рекрутингу. Співробітникам доцільно рекомендувати під час спілкування в мережі пропагувати переваги роботи в вашій компанії.

- відео-вакансії. Краще один раз побачити, ніж прочитати сотні слів. У багатьох західних компаніях корпоративні відео, що демонструють переваги роботи в тій чи іншій компанії, знаходяться на другому місці серед засобів інформування потенційних співробітників.

Рис. 1 – Структура інформаційної системи

- відео-резюме. Спеціалісти, що шукають роботу, розміщують свої резюме в вигляді відеороликів у соціальних мережах і на відеохостингах.

- WEB-резюме. Резюме в вигляді невеликого особистого сайту.

- корпоративні та особисті блоги співробітників.

Після створення бази кандидатів здійснюється їх оцінювання і відбір. Базою для оцінювання є результати тестування.

Розрізняють кваліфікаційне і психологічне тестування. Кваліфікаційне тестування дозволяє визначити професійний рівень кандидата. Психологічні тести спрямовані на оцінювання особистісних та індивідуальних особливостей кандидатів. Останнім часом набуває популярності віддалене тестування в режимі онлайн, яке дозволяє відсіяти тих осіб, які не відповідають посаді.

Дана інформаційна система забезпечує оперативність пошуку кандидатів та їх оцінювання і відбір, а також структуризацію потрібної інформації.

УДК 338.2

СУЧАСНИЙ АНАЛІЗ ДИНАМІКИ РОЗВИТКУ ЕКОНОМІЧНОЇ ДІЯЛЬНОСТІ ПІДПРИЄМСТВА ЗАСОБАМИ КОМП'ЮТЕРНОГО КОМПЛЕКСУ PROJECT EXPERT

О.М. Кузьміна[1], к.т.н., доцент, Л.М. Захарченко[2]
[1]Вінницький торговельно – економічний інститут КНТЕУ
[2]Вінницький національний технічний університет
[1]kuzmin_andrey@bk.ru

Економіку в цілому і її окремі компоненти (підприємства, фірми і т.п.) можна віднести до динамічних систем. Робота таких систем пов'язана з діями мінливого зовнішнього середовища і обробкою величезних об'ємів інформації. Ефективність застосування інформаційних систем для управління економічними об'єктами (підприємствами, банками, торговими організаціями, державними установами і так далі) залежить від широти обхвату і інтеграції на їх основі функцій управління, від здатності оперативно готувати управлінські рішення, адаптуватися до змін зовнішнього середовища і інформаційних потреб користувачів.

В сучасному світі економічна діяльність тісно зв'язана з комп'ютерною технікою та інформаційними технологіями. Діяльність підприємства залежить від інформованості і здатності ефективно використовувати інформаційні ресурси. Ці ресурси розглядаються спільно з автоматизованими інформаційними технологіями, які додають їм необхідну мобільність. Інформаційні технології забезпечують реалізацію інформаційних процесів та

призначені для зниження трудомісткості процесів використання інформаційних ресурсів, підвищення їх надійності і оперативності.

Сучасні процеси управління економічним об'єктом будуються на основі автоматизації інформаційних технологій. Для ефективного управління діяльністю економічного об’єкту інформаційні технології об'єднуються в єдину інтегровану систему. Це дозволяє розв’язувати широкий комплекс функціональних задач економічного об’єкту.

В сучасних умовах аналіз розвитку економічної діяльності підприємства неможливий без застосування автоматизованих інформаційних технологій та аналітичних систем. Ефективним розв’язанням цієї задачі є методи та засоби імітаційного моделювання. Імітаційні моделі дозволяють програвати різні варіанти розвитку економічного об'єкту, стану зовнішнього економічного оточення. Вони дають можливість перевірити різні ідеї, гіпотези і припущення щодо розвитку бізнесу, проаналізувати наслідки їх реалізації. Таким вимогам цілком відповідає комп’ютерна система підтримки - прийняття стратегічних рішень Project Expert. Система дозволяє моделювати діяльність підприємств різних розмірів – від невеликого приватного підприємства до холдингових структур. З її допомогою можна створювати проекти будь-якої складності – від розрахунку окупності нового обладнання до оцінки ефективності диверсифікованості діяльності підприємства. Система Project Expert є потужним інструментом, що дозволяє моделювати діяльність діючого чи нового підприємства, вивчати вплив навколишнього економічного середовища, розраховувати різні варіанти розвитку, здійснювати інвестиційне проектування і фінансове планування, створювати бізнес - плани. Так, система підтримки -

прийняття рішень Project Expert дозволяє вибрати оптимальний шлях розвитку, проаналізувати альтернативні стратегії, оцінити запас потужності бізнесу, оптимізувати закупівлі, витрати і продажі, спрогнозувати ефективність проекту для бюджету, а також вести контроль за реалізацією проектів. Система цільового управління, що використовує Project Expert , надає можливість вивчати і планувати інтегровані фінансові потоки для групи бізнес - моделей і оцінювати ефективність діяльності підприємства, що здійснює моделювання різних бізнес - моделей. Ці властивості роблять Project Expert унікальним засобом імітаційного моделювання для дослідження бізнес - моделі і застосування в якості основного аналітичного інструмента фінансового моделювання.

Пропонований погляд на аналіз динаміки розвитку економічної діяльності підприємства з використанням інструменту імітаційного моделювання та його взаємозв'язок з основними показниками управління дає можливість створювати аналітичні моделі розвитку. Зокрема, це можливість підійти впритул до розробки групи методик аналізу стратегічного розвитку економічних об’єктів.

УДК 519.21:681.142

МОДЕЛЬ РАСПРЕДЕЛЕНИЯ ПРИБЫЛИ МЕЖДУ ПАРТНЕРАМИ ВИРТУАЛЬНЫХ ПРЕДПРИЯТИЙ

Р.В. Резниченко
Международный научно-учебный центр информационных технологий и систем Национальной Академии наук Украины и Министерства образования и науки Украины
reznichenko.roma@mail.ru

Глобальная экономическая среда сегодня характеризуется драматическими изменениями под влиянием таких факторов, как сокращение жизненного цикла товаров, повышения уровня технологий, высокой конкурентоспособностью. В этой глобальной экономической среде, компания зависима от организационной эффективности, гибкости и быстроты реагирования на рыночные изменения. Однако все эти возможности вряд ли может представить одна компания. Виртуальные предприятия (ВП) позволяют объединять возможности нескольких организаций, которые обладают различными возможностями и таким образом создавать организацию, которая может представить общий потенциал.

Виртуальные предприятия (ВП) можно рассматривать как кооперативный альянс. На этапе создания виртуальных предприятий, необходимо рассмотреть распределение прибыли между партнерами в условиях неопределенности. Этот вопрос необходимо рассматривать как нечеткую игру сотрудничества. Поэтому актуальным вопросом является построение четких схем

распределения прибыли на основе нечетких значений Шепли.

ВП можно рассматривать как временный союз компаний. Он может быстро создаваться в целях продвижения конкретных возможностей рынка и расформировываться, когда рынок возможностей уже упущен. Эта бизнес-модель уже существует во многих проектно-ориентированных отраслях, таких, как строительство, консалтинг, коммерческое страхование и т.д., которая позволяет удовлетворять требования заказчика для нестандартных продуктов и услуг.

Классические ценности Шепли основываются на двух допущениях:

1. Игроки в полной мере участвуют в конкретной коалиции. Это означает, что степень участия каждого игрока в коалиции 1 или 0.

2. Игроки, в самом начале игры, точно знают, ожидаемую прибыль.

ВП можно рассматривать как кооперативный альянс компаний-участниц, которые обладают различными возможностями, и способны зарабатывать максимальную прибыль. Этот случай можно рассматривать как нечеткую игру сотрудничества $(I,\tilde{v})$. В математической модели нечетких значений Шепли представим коалицию, где любой партнер, скорее всего, примет участие в $\tilde{v}(K)$ что обозначает возможную прибыль коалиции $K,\tilde{v}(K-\{i\})$. Используя нечеткие функции принадлежности представляется возможным получить описания различных выплат коалиции.

УДК 004.94

ГЕОІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ПРОСТОРОВОГО АНАЛІЗУ ПРОЦЕСІВ ЕМІСІЇ ДІОКСИДУ ВУГЛЕЦЮ З ВРАХУВАННЯМ РОЗИ ВІТРІВ

М.Ю. Лесів, аспірант
Національний університет «Львівська політехніка»
myroslava.lesiv@gmail.com

Сучасні геоінформаційні системи, призначені для просторового аналізу емісій парникових газів, не враховують процеси атмосферної дифузії та вплив вітру. Тому задача, яку розв'язано в цій роботі, полягає в розробці математичних моделей та геоінформаційних технологій просторового аналізу процесів емісії вуглекислого газу в енергетичному секторі західних регіонів України з врахуванням рози вітрів.

Вуглекислий газ за своїми фізичними властивостями важчий за повітря, що й визначає його поведінку в атмосфері. Тобто молекули діоксиду вуглецю переміщуються в повітрі під впливом сили тяжіння і різниці концентрацій, а також – вітру.

При моделюванні були зроблені наступні припущення: емісії вуглекислого газу постійні на протязі року; має місце збереження маси (немає хімічних реакцій чи поглинань); основні метеорологічні умови, від яких залежить поширення вуглекислого газу, є постійними на протязі року.

У відповідність процесу розподілу маси вуглекислого газу на деякій відстані від джерела викиду у випадку вітряної погоди поставлено модель Гауса. Ця

модель враховує обидва процеси: переміщення у вітровому полі і розсіювання за рахунок атмосферної турбулентності. У випадку відсутності вітру вуглекислий газ поширюється в приземному шарі атмосфери рівномірно у всіх напрямках.

Оскільки на практиці потрібно враховувати вплив великої кількості джерел емісій діоксиду вуглецю та різні напрямки вітру, то для зручності оперування і підвищення ефективності обчислювального процесу отримано формули для переходу від системи координат цифрової карти до нової, з центром в точці джерела емісії та з віссю абсцис, спрямованою паралельно напрямку вітру.

Для здійснення числових експериментів використано дані про розу вітрів, а також цифрову карту Західної України з інформацією про емісії вуглекислого газу на рівні елементарних ділянок заданого розміру (2 км х 2 км).

На основі розробленого математичного апарату та геоінформаційних технологій засобами мови програмування MapBasic9 реалізовано додаткове меню на панелі інструментів ГІС, яке дає можливість формувати на цифровій карті елементарні ділянки кордону для аналізу, “вирізати” прикордонну смугу певної ширини та обчислювати емісії, що пройшли через кожну елементарну ділянку кордону.

Розроблені геоінформаційні технології просторового аналізу процесів емісії вуглекислого газу в енергетичному секторі з врахуванням рози вітрів дають можливість обчислювати масу вуглекислого газу, яка пройшла через кордон, на рівні елементарних ділянок.

УДК 681.3

ЗАДАЧА ОПТИМАЛЬНОГО РОЗПОДІЛУ ДЕКЛАРАЦІЙ З ПДВ МІЖ ІНСПЕКТОРАМИ В ІНФОРМАЦІЙНІЙ ТЕХНОЛОГІЇ АДМІНІСТРУВАННЯ ПОДАТКУ НА ДОДАНУ ВАРТІСТЬ

С.П. Дерлеменко, аспірант
Київський національний університет будівництва і архітектури
derlemenko_s@ukr.net

Впровадження сучасних інформаційних технологій в органах Державної податкової служби забезпечує ефективність, прозорість, швидкість та якість процесів адміністрування податків.

Адміністрування податку на додану вартість – один з пріоритетних напрямів роботи органів ДПС по наповненню бюджетів усіх рівнів.

Автоматизація адміністрування податку на додану вартість дозволить підвищити ефективність системи оподаткування за рахунок скорочення часу на опрацювання декларацій, зменшення кількості помилок в роботі працівників органів ДПС та приділення максимальної уваги платникам податків, у яких виявлено найбільшу ймовірність порушення податкового законодавства, а також які мають найбільший вплив на формування бюджету.

Оскільки кількість платників податків постійно зростає, а кількість інспекторів, що займаються адміністрування ПДВ не може зростати такими ж темпами,

постає питання оптимального відбору декларацій платників податків для опрацювання.

Для цього декларації розподіляються на групи (так звані «коридори») за алгоритмом, який враховує ризики (вірогідності порушення податкового законодавства), виявлені під час аналізу діяльності платника податків, та заявлені в декларації операції – сплату чи відшкодування податку на додану вартість.

Виходячи з кількості працівників підрозділів, що займаються опрацюванням декларацій, в автоматичному режимі обирається така кількість декларацій, час на опрацювання яких відповідатиме загальній кількості робочого часу інспекторів підрозділу.

Задачу розрахунку і розподілу декларацій між інспекторами можна представити як окремий випадок незбалансованої транспортної задачі, цільовою функцією якої є максимум сум добутків коефіцієнтів ефективності опрацювання платника інспектором (враховуючи досвід інспектора взагалі та його роботи з конкретним платником, податкову поведінку та фіскальну важливість платника, а також дати останньої повної документальної перевірки платника податків) (d_{ij}) та ознак, чи буде проводити інспектор перевірку платника (x_{ij}).

Обмеженням в задачі є кількість робочих годин, за які необхідно опрацювати податкові декларації з метою своєчасного відшкодування ПДВ.

В результаті розв’язання задачі отримаємо оптимальний розподіл декларацій між інспекторами, який використовується в інформаційній системі автоматизованого адміністрування ПДВ.

Впровадження інформаційної технології автоматизованого адміністрування ПДВ дозволить оптимізувати використання ресурсів органів ДПС та сприятиме своєчасному та в повній мірі наповненню бюджету.

УДК 004.8 + 681.518.25

ПРОГНОЗУВАННЯ СОЦІАЛЬНО-ЕКОНОМІЧНИХ ПРОЦЕСІВ НА ОСНОВІ ІНТЕРВАЛЬНИХ НЕЧІТКИХ МНОЖИН ТИПУ-2

О.В. Чеборака[1], асистент
О.А. Ткачук[2], аспірант
Вінницький національний технічний університет
[1]alch_666@yahoo.com, [2]otkachuk@gmail.com

Необхідність прогнозування соціально-економічних процесів зумовлена потребою у визначенні перспектив розвитку суспільства та виробленні найбільш оптимальних програм і планів економічного та соціального розвитку країни. При прийнятті управлінських рішень завжди доводиться працювати в умовах невизначеності даних, що ускладнює вибір найбільш оптимального рішення. Ефективним інструментом обробки невизначеностей є інтервальні нечіткі множини типу-2. Побудовані на основі них моделі дозволяють обчислювати не тільки точкові прогнози, а й інтервальні, які є більш інформативними, тому що вказують межі, в яких може знаходитись майбутнє значення об’єкта, що прогнозується.

Інтервальна нечітка модель типу-2 складається з таких компонентів: база правил, блок приведення до нечіткості, блок нечіткого логічного виведення, блок пониження типу та блок приведення до чіткості. На виході цієї моделі з’являються два значення: інтервальне та чітке, які виводяться блоками пониження типу та приведення до чіткості відповідно.

Для підвищення якості інтервального прогнозування використовується множина інтервальних нечітких моделей

типу-2, об’єднані в одне ціле – узагальнена інтервальна нечітка модель типу-2. При прогнозуванні процесів в умовах невизначеності даних основну увагу зосереджено на обчислення інтервальних прогнозів. Тому при побудові узагальненої інтервальної нечіткої моделі типу-2 використовуються критерії якості інтервального прогнозу: частка експериментальних значень, що не потрапили в прогнозний інтервал, та середньоквадратична ширина прогнозного інтервалу. Обчислення вихідного інтервального прогнозу узагальненої моделі здійснюється шляхом перетину інтервальних прогнозів часткових моделей. Якщо результат перетину існує, то він і є виходом узагальненої моделі. В іншому випадку виходом є результат об’єднання інтервальних прогнозів часткових моделей. За рахунок такої процедури вдається зменшити ширину прогнозного інтервалу. Побудова узагальненої моделі здійснюється на основі попередньо побудованих адекватних інтервальних нечітких моделей типу-2, які пройшли етап навчання. Необхідною умовою адекватності моделі є влучення усіх навчальних та тестових точок в прогнозний інтервал моделі.

На практиці було розв’язано задачу інтервального прогнозування індексу споживчих цін, який є основним показником інфляції. Вихідна вибірка даних містила 16 макроекономічних показників соціально-економічного розвитку України. На основі наявних даних побудовано узагальнену інтервальну нечітку модель типу-2, яка дозволила обчислити більш якісні інтервальні прогнози, ніж інтервальна нечітка модель типу-2.

8. ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В МЕДИЦИНІ

УДК 615.47:616-072.7

ІНФОРМАЦІЙНІ ОПТИКО-ЕЛЕКТРОННІ ТЕХНОЛОГІЇ ВИЗНАЧЕННЯ ФУНКЦІОНАЛЬНОГО СТАНУ ЛЮДИНИ-ОПЕРАТОРА

С.М. Злепко, д.т.н., професор,
С.В. Павлов, д.т.н., професор,
А.П. Моторний, аспірант
Вінницький національний технічний університет
smzlepko@ukr.net

Вступ. Функціональний стан – це характеристика рівня функціонування систем організму в певний період часу, що відображає особливості гомеостазу і процесу адаптації. Досягнення того або іншого рівня функціонування здійснюється завдяки діяльності механізмів регуляції.

Ключовою ланкою в структурі загального функціонального стану організму є стан центральної нервової системи (ЦНС), який розглядається як результат взаємодії неспецифічної генералізованної активності (джерелом якої є ретикулярна формація) і специфічної активності, що має ряд локальних джерел. Останні визначають рівень уваги й сприйняття, понятійного мислення, моторної активності, мотивації, а також емоцій.

Метод. Одним із методів визначення гемодинамічних показників для оцінювання функціонального стану людини є фотоплетизмографічний метод, який заснований на тому, що досліджувана тканина через спеціальний світловод і світлофільтри просвічується монохроматичним світлом, яке після розсіювання або відбиття потрапляє на фотоелектроперетворювач, викликаючи зміни фотоструму,

реєстровані гальванометром. Встановлено, що інтенсивність світла, відбитого або розсіяного шкірою, є функцією кількості крові, що міститься в ній. Оскільки коефіцієнт поглинання інфрачервоного світла кров'ю значно вищий, ніж тканиною, фотоплетизмографія реєструє лише зміни вмісту крові. При цьому розсіювання світла відбувається в основному за рахунок відбиття від поверхні еритроцитів.

При такому опроміненні, оптична відповідь може бути поділена на дві складові частини – пульсову та постійну частину. Пульсова складова безпосередньо відповідає за значення пульсувань. Деякі результати показували, що крім величини пульсувань до результату мала входити ще й дія ефекту переорієнтацій червоних кров’яних тілець (як функція від зміни швидкості кровотоку), хоча відносне значення цього ефекту в порівнянні з величиною зміни кількості крові невідома. Існуючі методи досліджень дозволяють одержувати характеристичні спектри життєво важливих компонентів – білків, амінокислот, гемоглобіну та інших.

В загальному випадку крім визначення складових параметрів фотоплетизмограми можливе одночасне визначення рівня сатурації крові киснем за рахунок введення в систему додаткових випромінювачів, що дозволяє розширити спектр інформаційних показників про поточний фізіологічний стан людини-оператора.

Таким чином, можна зробити висновок про можливість застосування даного методу для оцінки фізіологічного стану як однієї зі складових функціонального стану людини-оператора.

УДК 616.8-08

ОЦІНЮВАННЯ ЯКОСТІ РЕАБІЛІТАЦІЙНОГО ПРОЦЕСУ НЕВРОЛОГІЧНИХ ХВОРИХ В УМОВАХ САНАТОРІЮ

С.М. Злепко[1], д.т.н., професор, О.П. Азархов[2], здобувач, С.В. Костішин[1], аспірант
[1]Вінницький національний технічний університет
[2]ПП «Санаторій Металург», м. Маріуполь
smzlepko@ukr.net

Будемо розглядати реабілітацію неврологічних хворих в умовах санаторію як багатокомпонентний процес, направлений на досягнення максимальної якості медичної допомоги (ЯМД) пацієнтам.

Досягти оптимального рівня здоров'я можна тільки створивши цілісну систему або інформаційну технологію для управління лікувально-діагностичним процесом, яка передбачає етапи планування, мотивації і контролю, діагностування, реабілітації і послідовність розвитку згідно сучасних медичних стандартів. Використання медичних стандартів забезпечує новий підхід до управління ЯМД з орієнтацією на позитивний підсумковий результат на основі конкретних кількісних показників при її оцінці (Бреусова А.В. та інші, 2004 р.).

Багатокомпонентність реабілітаційного процесу неврологічних хворих в умовах санаторію передбачає наявність таких складових як лікувальна, організаційно-методична, інформаційна і наукова роботи. Лікувальна складова, яка відіграє провідну роль, передбачає обстеження і лікування хворих з метою виявлення особливостей їх адаптації на початковому етапі

санаторного лікування, профілактики виникнення негативних метеопатологічних і бальнеологічних реакцій і призначення, оцінювання і, при необхідності, корегування індивідуальної терапії деяких категорій пацієнтів тощо.

Як правило, пацієнти, що поступають на лікування до санаторію умовно розподіляються на дві групи. До першої відносяться хворі, які направляються до санаторію після отримання амбулаторно-поліклінічної допомоги за місцем проживання, не потребують постійної уваги лікаря-невропатолога і проходять класичну двухетапну реабілітацію. Друга група, менш чисельна, поступає в санаторій після лікування в стаціонарі, потребує постійного догляду з боку лікаря-невропатолога і потребує трьохетапної реабілітації з обов'язковим післясанаторним лікарняним контролем за місцем проживання.

Саме такий диференційований підхід і дозволяє у поєднанні з призначеними діагностичними, лабораторними і фізіотерапевтичними та іншими дослідженнями і процедурами успішно прогнозувати переносимість курортних факторів, визначати ступінь адаптації і можливі шляхи корекції функціонального стану пацієнтів, зміст та ефективність суто реабілітаційних заходів.

Таким чином, забезпечення оптимальної якості медичної допомоги на етапі санаторно-курортного лікування досягається, перш за все, збалансованою, багатофункціональною тактикою відновлювального лікування неврологічних хворих і, по-друге, застосуванням систем і технологій, що забезпечують інформаційну та інтелектуальну підтримку санаторно-курортного лікування в умовах невизначеності і дефіциту часу.

УДК 004.891: 614:612.843.215

ПОБУДОВА ПРОТОТИПУ ЕКСПЕРТНОЇ СИСТЕМИ ДОСЛІДЖЕННЯ НЕЙРОТОКСИКАЦІЇ ЛЮДИНИ МЕТОДОМ ЕЛЕКТРОРЕТИНОГРАФІЇ

Б.І. Яворський, д.т.н., с.н.с.,
Р.А. Ткачук, к.т.н., доцент
Тернопільський національний технічний університет імені Івана Пулюя
Kaf_BT@tu.edu.te.ua

Для виявлення, ідентифікації та визначення дози нейротоксикації організму людини наночастинками (НЧ) мають перспективу електрофізіологічні неінвазивні методи, зокрема, електроретинографія. Через використання реакції сітківки ока, яка є близькою до мозку і центральної нервової системи, на подразнення світлом, цей метод уможливлює оцінювання нейротоксикації людини в реальному часі, in vivo, ще в початковій стадії.

Існують міжнародні стандарти, в яких регламентовано методи відбору електроретиносигналу (ЕРС), його попереднього опрацювання, оцифрування, оптимального оброблення та реєстрації, а також оцінювання морфологічних параметрів (часових інтервалів, амплітуд тощо) отриманої електроретинограми (ЕРГ) та діагностування патологій зорового аналізатора. Проте, застосування ЕРГ-досліджень для виявлення НЧ, їх ідентифікації та дози в організмі людини з прогнозованою вірогідністю досліджені недостатньо.

У даній роботі наведено медико-технічні вимоги до побудови прототипу електроретинографічної експертної системи (ЕРГЕС) для підвищення ефективності досліджень нейротоксикацій.

Оскільки прототип експертної системи будується на початковому етапі її розробки, то на основі результатів ідентифікації ЕРГЕС для досліджень НЧ-нейротоксикації організму людини встановлено основні концептуальні засади її побудови. Отримані концепції формалізовано в рамках обгрунтованої математичної моделі ЕРС. Результати формалізації уможливили синтез структури ЕРГЕС та її реалізації апаратними та програмними засобами. При цьому обґрунтовано критерії та методи для:

- оптимального вибору енергетичних, просторово-часових та частотних характеристик подразнення ретини;
- побудови та керування параметрами та конструкції електродів для відбору ЕРС;
- оптимізації характеристик та параметрів відбору та оцифровки ЕРС;
- адаптивного оптимального оцінювання ЕРГ.

Побудовано електроретинографічну систему (ЕРГС) з автоматизованими та інтерактивними режимами й ознаками штучного інтелекту.

Для оптимального виділення сегментів ЕРГ застосовано адаптивний фільтр (Калмана). Його складність є меншою за складність фільтрів Колмогорова-Вінера чи Норса, а також фільтрів, отриманих апроксимацією їх характеристик ортогональними поліномами, гармонічними функціями, методом ковзного середнього тощо. Ця різниця особливо проявилася при підвищенні вимог до вірогідності виявлення та ідентифікації нейротоксикації організму, роздільної здатності та точності визначення його дози.

Отримано оцінки залежностей ймовірності відтворення ЕРГ у межах заданої точності від середньої повної дисперсії її спектральної густини потужності при заданих ймовірностях відтворення ЕРГ з більшою за порогове значення цієї потужності похибкою та уможливлено побудову бази знань про НЧ- токсиканти.

УДК 53.072.11:612.172.2

ОЦІНЮВАННЯ ФУНКЦІОНАЛЬНОГО СТАНУ ЛЮДИНИ ЗА ВАРІАБЕЛЬНІСТЮ СЕРЦЕВОГО РИТМУ

В.В. Фалендиш, Б.І. Яворський, д.т.н., с.н.с., М.В. Бачинський, к.т.н.
Тернопільський національний технічний університет імені Івана Пулюя
falendysh@gmail.com, kaf_bt@tu.edu.te.ua

Одним із засобів підвищення надійності оператора складних людино-машинних (ергатичних) систем є забезпечення неперервного автоматизованого контролю поточного функціонального стану його організму – безпосередньо, в процесі роботи, з допомогою ефективних методів та засобів. Для оцінювання загального функціонального стану людини широко застосовується аналіз серцевого ритму. Для цього розроблено низку програмно-апаратних комплексів в яких, проте, серцевий ритм вважається стаціонарним випадковим процесом. Це значною мірою ускладнює застосування таких комплексів для автоматизованого контролю функціонального стану оператора в режимі реального часу, оскільки під час виконання професійних обов’язків оператор перебуває під дією великої кількості подразників, що спричиняє нестаціонарність серцевого ритму.

Представлення серцевого ритму у вигляді періодично корельованої випадкової послідовності дало змогу отримувати якісні оцінки спектральної густини потужності серцевого ритму з дихальною нестаціонарністю

за допомогою фільтрового методу, чим отримано меншу дисперсію оцінок.

З допомогою фільтрового методу оцінювання спектральної густини потужності стаціонарних компонент (СГПСК) серцевого ритму побудовано їх оцінки для різних періодів корельованості серцевого ритму (періодів дихання).

а)

б)

Рисунок 1 – Оцінка спектральної густини потужності стаціонарних компонент варіабельності серцевого ритму з різними періодами корельованості фільтровим методом.

За побудованими оцінками СГПСК отримано достовірніші висновки про зміну функціонального стану людини оператора ергатичної системи в режимі реального часу при його засинанні, ніж при оцінках СГПСК, отриманих компонентним чи когерентним методами.

УДК 612.17:616-073.584

АНАЛИЗ НЕСТАБИЛЬНОСТИ ВРЕМЕННОГО РЯДА КАРДИОИНТЕРВАЛОВ С ТОЧКИ ЗРЕНИЯ САМООРГАНИЗОВАННОЙ КРИТИЧНОСТИ.

Н.Т. Абдуллаев, к.т.н., доцент,
О.А. Дышин, к.ф-м.н., с.н.с., А.Д. Джабиева, к.т.н.
Азербайджанская государственная нефтяная академия
a.namik46@mail.ru

При исследовании работы сердца по совокупности реальных процессов с явно выраженной нелинейностью, любые причинно-следственные отношения подлежат сомнению в качестве оценочных. В качестве физического параметра для исследования исходного системного процесса выбирается интервал времени между соседними динамическими структурами. Поскольку в ритме сердца закодирована вся информация об общем системном процессе, то можно предположить, что информация о структуре кардиоциклов и даже об амплитудных значениях биопотенциалов косвенно выражается величинами временных интервалов между соседними R-зубцами. Формируемый номерной ряд RR-интервалов представляет собой RR-интервалограмму, являющуюся, по своему содержанию, функцией времен сдвижек i-х RR-интервалов относительно наиболее вероятного значения RR-интервала. Подготовленная для анализа модифицированная форма RR-интервалогрмаммы представляет собой номерной ряд абсолютных отклонений i-х значений RR-интервалов от среднего выборочного в норме. Временной ряд биопотенциалов трансформируется в RR-интервалограмму как апериодическую последовательность кардиоциклов.

Поскольку для динамических процессов методы статистики не всегда эффективны, необходим поиск новых признаков, основанных на предположении, что сердечная деятельность – это детерминированный хаос. Последовательность кардиоинтервалов рассматривается как сложный динамический процесс с детерминированной хаотической составляющей. Переход от регулярных состояний данного процесса к хаосу через перемежаемость характеризуется проявлением феномена самоорганизованной критичности (слабого хаоса), приводящего к нестабильности системы и фликкер-шуму в частотной области. Явление перемежаемости (чередование длинных регулярных фаз и относительно коротких нерегулярных всплесков) тесно связано с фликкер-шумом, спектр мощности которого расходится на низких частотах по степенному закону. Число хаотических всплесков нарастает при увеличении внешнего параметра, а это означает, что перемежаемость представляет собой непрерывный переход от регулярного движения к хаотическому. С учетом степенного характера спектра мощности RR-интервалограммы было предложено использовать его в качестве диагностического признака, позволяющего различать такие катастрофические аритмии сердечно-сосудистой системы как фибрилляция желудочков, пароксизмальная тахикардия, пароксизмальная тахиаритмия и упорядочивать эти синдромы по характеру их приближения к состоянию слабого хаоса – предтечей чистого хаоса.

УДК 616.74

ПОДХОД К ОБРАБОТКЕ ЭЛЕКТРОМИОГРАФИЧЕСКИХ СИГНАЛОВ С ПОМОЩЬЮ АППАРАТА НЕЧЕТКИХ МНОЖЕСТВ

Н.Т. Абдуллаев[1], к.т.н., доцент,
А.С. Аббаскулиев[2], к.т.н., доцент,
К.Ш. Исмаилова[3], ассистент
Азербайджанская государственная нефтяная академия
[1]a.namik46@mail.ru, [2]abayso@list.ru,
[3]Is_kamalya@yahoo.com

Электромиография (ЭМГ) есть совокупность, возникающих в различных временных и пространственных взаимоотношениях, соответственным образом усиленных и записанных потенциалов действия (ПД) отдельных возбудимых элементов мышцы. Достаточно полное представление о состоянии мышцы и систем, непосредственно регулирующих ее деятельность, можно получить при сочетанном изучении ЭМГ произвольного усилия, состояния нервно-мышечной передачи, скорости проведения по двигательным нервам и изучении сократительных свойств мышц.

В используемых для анализа электромиограмм методах биоэлектрические сигналы рассматриваются как линейные стационарные, что не всегда позволяет дифференцировать состояние систем, отображающих происходящие в мышцах процессы.

Сбор, обработка и автоматизированный анализ физиологической информации о состоянии организма человека являются важнейшей составной частью многих диагностических методов современной медицины.

Компьютерные системы сбора и математической обработки электрофизиологических сигналов являются сложными аппаратно-программными комплексами, состоящими из множества программных компонентов, выполняющих функции регистрации биомедицинской информации, ее обработки и системного анализа, а также диагностические и сервисные операции.

Функциональные возможности подобных систем практически невозможно было расширить, так как они выполняют лишь те функции, которые были заложены на этапе проектирования. Однако современные требования, предъявляемые к данным системам, в значительной мере, связаны с необходимостью постоянного расширения и наращивания их функциональных свойств. Важными проблемами являются также универсализация биомедицинского программного обеспечения, под которой, прежде всего, понимается проблема использования закодированных состояний, связанных с конкретными нарушениями, и преодоление имеющихся препятствий на пути интеграции разнородных компьютерных медицинских систем.

В данной работе предлагается подход к обработке ЭМГ-сигналов, который совместим с поведенческими аспектами и неопределенностью в действиях лиц, принимающих решения. Работа, в основном, акцентирована на построение математической базы системы обработки ЭМГ-сигналов с помощью аппарата нечетких множеств.

УДК 004.925.5:621.391.25: 61

ЦВЕТОВОЕ КОДИРОВАНИЕ ИЗОБРАЖЕНИЙ В МЕДИЦИНЕ

Л.С. Годлевский[1], д.м.н., профессор
И.В. Хихловская[2], к.т.н., доцент
[1]Одесский государственный медицинский университет
[2]Одесская национальная академия связи им. А.С.Попова
godlevsky@odmu.edu.ua

Биомедицинские изображения, полученные в результате рентгеновских, маммографических или ультразвуковых исследований, характеризуются низкой контрастностью, искаженными яркостными характеристиками и высокой зашумленностью. Врач-диагност должен обнаруживать аномальные образования на осложнённом таким фоном изображении. При этих условиях он может не заметить мелкие детали или пропустить слабоконтрастную структуру. Повышение достоверности обнаружения объектов возможно за счёт цветового кодирования полутоновой шкалы. Выбор цветов следует оптимизировать по критерию максимизации минимального расстояния между ними в равноконтрастном пространстве, связанном с цветовыми ощущениями человека. Пороги контрастной чувствительности зрительной системы по яркости и цветности существенно различны. По яркости человек различает всего порядка 100…200 градаций, а на современном воспроизводящем устройстве (экране телевизора, мониторе) до 4000 цветов.

Задача отыскания оптимального набора цветов может рассматриваться как задача максимизации функционала, в качестве которого используется минимальное расстояние между точками, изображаемыми цвет в цветовом пространстве.

Задача нахождения *N* наборов оптимальных цветов решена для телевизионной системы, цветовое пространство которой определяется основными цветами x, y - координатами цветности в системе МКО 1931г. Поверхность, ограничивающая тело цветов, воспроизводимых телевизионной системой, определяется максимальными относительными значениями сигналов, которые не должны быть больше единичных. Для окрашивания шкалы в соответствии с моделью цветового пространства в виде равноконтрастного пространства МКО 1976 г. Получены оптимальные наборы цветов для *N*=2…16.

Проведённые эксперименты показали, что применение цветового кодирования эффективно тогда, когда анализируемые изображения малоподвижны, сохраняются светлотный образ исходного изображения и траектория изменения цветов в цветовом пространстве непрерывна. Рекомендуемое количество цветов не должно превышать 20 и на кодированном изображении следует вводить цветовой клин для сравнения с исходными градациями яркости.

УДК 159.942.2

ПІДХІД ДО КЛАСИФІКАЦІЇ ЕКСТРЕМАЛЬНИХ СТАНІВ ЛЮДИНИ

О.М. Роїк, д.т.н., профессор,
Н.А. Дудатьєва, аспірант
Вінницький національний технічний університет

Кінець XX початок XXI сторіччя характеризуються великою кількістю різних подій, які можна охарактеризувати як екстремальні для стану людини або надзвичайними з точки зору наслідків, в першу чергу, економічних, екологічних, техногенних тощо.

Достатньо велика кількість природних і техногенних катастроф, постійні повторення терористичних актів у різних точках світу, проведення спеціальних інформаційних операцій або війн, першочерговою метою яких є вплив на психологічний стан людини і його свідомість, вводять людину у стан, який можна охарактеризувати як екстремальний. Крім того, ритм сучасного життя, певні професії також сприяють перебуванню людини у цьому стані.

Людина, яка потрапила в надзвичайну ситуацію і, як наслідок, знаходиться у екстремальному стані, проходить декілька різних психологічних етапів, які в загальному випадку характеризуються погіршенням самопочуття, зменшенням рівня ефективності виконання робіт, депресивним станом тощо.

При наданні медичної допомоги людям, які перебувають у екстремальному стані, дуже важливо виявити залежність ’’надзвичайна ситуація – надзвичайний стан - наслідки’’ з метою підвищення ефективності

надання допомоги, а також оптимізації підбору медичного обладнання.

Оскільки екстремальний стан людини пов'язаний і визначається багатьма чинниками, що характеризують в першу чергу навколишнє середовище та його внутрішній стан, то підхід щодо класифікації ймовірних екстремальних станів людини пропонується будувати саме на залежності “екстремальна ситуація – екстремальний стан людини’’.

Під екстремальною або надзвичайною ситуацією в загальному випадку можна розуміти обстановку, яка склалася на певній території внаслідок техногенної аварії, стихійного лиха тощо, які можуть нанести втрати здоров’ю людини, її працездатності і навіть привести до людських жертв.

Виходячи з цього, доцільно представляти можливі екстремальні стани людини, враховуючи тип джерела виникнення цього стану, оскільки в подальшому це надасть можливість деталізувати необхідну для прийняття оптимального рішення ланку ’’причина – наслідок’’. За джерелом походження екстремальні стани можна розділити на такі групи: екстремальні стани техногенного характеру, екстремальні стани природного походження, екстремальні стани соціального характеру.

Наведений підхід щодо класифікації ймовірних екстремальних станів людини за своєю сутністю достатньо гнучкий, оскільки передбачає використання визначених залежностей і надає у разі необхідності можливості розширення за рахунок виникнення нових надзвичайних ситуацій і розширення відповідної множини або бази даних щодо ймовірних екстремальних станів людини та відповідних наслідків.

УДК 681.3.06

МЕТОД СЕГМЕНТАЦІЇ БІОЛОГІЧНИХ ОБ'ЄКТІВ УЛЬТРАЗВУКОВИХ ЗОБРАЖЕНЬ

Й.Й. Білинський, д.т.н., професор,
А.О. Мельничук, аспірант, Т.М. Крисак, аспірант
Вінницький національний технічний університет
Andreymelnichuk@rambler.ru

Незважаючи на велику кількість існуючих алгоритмів для сегментації зображень, переважна більшість їх є малоефективними при роботі з ультразвуковими зображеннями, оскільки з високою достовірністю не виділяють гомогенні структури, з урахуванням їх характеристик. Це означає, що для точного визначення геометричних параметрів сегментовані області повинні бути однотонними, мати нескладну форму контуру і не містити велику кількість «отворів». Досягти такого ефекту для ультразвукових зображень важко через наявність специфічного спекл-шуму та розмитість зображення досліджуваного об'єкта. Застосування загальних технік дає посічений контур, наявність псевдоотворів у зображеннях і високу розмитість. Тому розробка сучасних методів сегментації ультразвукових зображень залишається актуальною задачею розвитку діагностики біологічних об'єктів УЗУ зображень.

В доповіді запропонований метод сегментації ультразвукових зображень, який базується на використанні гістограм зображень і так званих локальних гістограм. Весь спектр відтворюваних рівнів яскравості ділиться на певну кількість частин залежно від складності зображення, котрі в подальшому використовуються для класифікації кожного

піксела окремо. Для класифікації пікселів використовується локальна статистика. Прямокутне ковзне вікно, розміром 7x7 чи 9x9 пікселів пересувається по зображенню з кроком в 1 піксел. В кожному положенні вікна аналізується гістограма іцнтенсивностей пікселів в межах вікна. В отриманій гістограмі аналізується ширина діапазону яскравостей, кількість піків, та піддіапазони з піками.

Кожна локальна гістограма, отримана в певному положенні ковзного вікна, в залежності від місця його розташування має характерні ознаки. Сукупність цих ознак дозволяє визначити, до якого типу об’єкту належить область, обмежена вікном. Приналежність кожного піксела до певного типу об’єкту визначається за загальним критерієм схожості.

Наступним кроком сегментації є коригування похибки. Для цього у межах ковзного вікна, визначається кількість пікселів кожного типу, центральний піксел класифікується як представник домінантної області у вікні.

Після класифікації усім пікселам, що не класифіковані, як контур присвоюється значення «0», іншим пікселам присвоюється значення «256». Далі отримане зображення з контурами і фоном додається до вхідного. Отриманий результат є зображенням з чітко визначеними контурними лініями навколо об’єктів.

Отримані результати показують сегментовані області УЗД зображення об’єктів, що мають нескладну форму, контурна лінія відносно проста, не містить розривів, загалом, на зображеннях об’єктів і на фоні відсутні випадкові «отвори».

УДК 681.7

ОПТИЧНІ ТЕХНОЛОГІЇ В КОНТЕКСТІ РЕАЛІЗАЦІЇ ІНТЕЛЕКТУАЛЬНИХ БІООКО-ПРОЦЕСОРНИХ ОПТИКО-ЕЛЕКТРОННИХ СИСТЕМ

С.В. Павлов, д.т.н., професор,
Р.В. Просоловский, аспірант,
Т.І. Козловська, аспірант
Вінницький національний технічний університет
psv@vstu.vinnica.ua

Вступ. Метою роботи є реалізація волоконно-оптичного сенсора для інтелектуальних біооко-процесорних оптико-електронних систем та приладів діагностування периферійного кровонаповнення, що дозволить підвищити інфоормативність, а також функціональні можливості біомедичних приладів та систем при експрес-діагностуванні стану периферійного кровообігу.

Технологія. Біомедичний оптоволоконний сенсор (рис. 1) для просторової діагностики біотканини представляє собою набір оптичних волокон, які поділяються на випромінюючі, що забезпечують передачу випромінювання від випромінювача до біотканини; та приймаючі – що забезпечують передачу відображеного інформативного випромінювання до фотоприймача.

Випромінюючі волокна у оптичному кабелі обираються таким чином, щоб забезпечити рівномірне освітлення досліджуваної частини біотканини.

Висновки. Реалізація такого сенсора дозволить більш ретельно визначати патології мікроциркуляції у різних ділянках, зокрема, щелепно-лицьовій області, в

хребетно-рухомих сегментах, нижніх кінцівок, передньої черевної стінки. Вивчення мікроциркуляторного русла за умов патології за допомогою запропонованого оптоволоконного сенсору дозволить визначати гемодинамічні показники до і після проведеного лікування.

Рис. 1. Функціональні вузли біомедичного оптоволоконного датчика для просторової діагностики біотканини:
а – схематичне зображення випромінювача; б – схематичне зображення фотоприймача; в – схематичне зображення сенсора

УДК 004.415.2:57.087.1+618.2-071.6

МЕТОД РОЗДІЛЕННЯ СУМІШІ ЦИКЛОСТАЦІОНАРНИХ БІОСИГНАЛІВ

Є.Б. Яворська, к.т.н.,
О.В. Гевко, к.м.н., доцент
Тернопільський національний технічний університет імені Івана Пулюя
kaf_bt@tu.edu.te.ua

Перинатальна смертність в Україні продовжує залишатись високою. Показник перинатальної смертності плоду в Україні вдвічі перевищує аналогічний показник в більшості Європейських країн. Однією з вагомих причин даної проблеми залишається відсутність адекватних ресурсів для забезпечення моніторингу стану плоду під час вагітності.

Дані літератури свідчать, що зниження перинатальної смертності може стати можливим завдяки інтенсивному спостереженню за станом плоду під час вагітності і в пологах за допомогою сучасних методів дослідження, які базуються на аналізі його серцевої діяльності.

Серед захворювань перинатального періоду перше місце займають хронічна внутріутробна гіпоксія плоду і асфіксія новонародженого. Ураження серцево-судинної системи зустрічається у 25% новонароджених, таких, що перенесли перинатальну гіпоксію.

Основні прояви гіпоксії плоду: порушення частоти серцевих скорочень, погіршення гучності серцевих тонів, поява аритмії, зниження інтенсивності руху плоду, тощо.

Діагностика гіпоксії плоду може бути тільки комплексною. Поширеним методом контролю за

функціональним станом плоду під час вагітності і в пологах є реєстрація його серцевої діяльності.

Одним із методів здійснення моніторного контролю серцебиття плоду є непряма електрокардіографія. Важливою проблемою при його застосуванні є важкість виділення електрокардіосигналу плоду (ЕКСП) від електрокардіосигналу матері (ЕКСМ).

Удосконалення методів та засобів математичного моделювання ЕКСП уможливлює підвищення ефективності алгоритмів виділення та обробки серцевих сигналів внутріутробного плоду.

Використано методи статистичної теорії вибору рішень та обчислювальні методи засобів математичного та програмного забезпечення пакету MATLAB для вирішення задачі тестування методу розділення суміші ЕКСП та ЕКСМ.

Побудовано комп'ютерну імітаційну модель суміші ЕКСП та ЕКСМ, яка враховує циклостаціонарні випадки, з подальшим використанням її для виділення та обробки серцевих сигналів внутріутробного плоду.

Згенеровано тестову суміш ЕКСП та ЕКСМ на базі моделі ЕКС, запропонованої Лосадою. Проведено розділення згенерованої суміші ЕКСП та ЕКСМ на базі стохастичного алгоритму самонавчання для максимізації взаємної інформації. Проаналізовано роботу даного алгоритму і визначено його недоліки, а також недоліки методу незалежних компонент для задачі виділення ЕКСП з суміші ЕКСМ.

Таким чином, результати отримані для тестової моделі вказують на можливість покращення алгоритму виділення ЕКСП з суміші ЕКСМ на базі апріорної інформації про ЕКСМ.

УДК 004.652.4+004.827

ІНФОРМАЦІЙНА МОДЕЛЬ ЛІКУВАЛЬНИХ СИСТЕМ ПРИЙНЯТТЯ РІШЕНЬ

Н.І. Мельникова[1],
Н.Б. Шаховська[2], к.т.н., доцент
[1]Інститут підприємництва та перспективних технологій
[2]Національний університет «Львівська політехніка»
[1]krapna@rambler.ru, [2]natalya233@gmail.com

Розвиток інформаційних технологій і сучасних комунікацій, поява в клініках великої кількості автоматизованих медичних пристроїв, систем для спостереження привели до нового та значного росту числа медичних інтелектуальних інформаційних систем (МІІС). Сьогодні МІІС трансформувалися у введення електронних медичних записів, що перетворені у пошукові медичні бази даних, забезпечені «інтелектуальними мережами», що не лише вдосконалює роботу лікаря, а сприяє дослідженню широкого спектра фармакологічної продукції. Медичні інформаційні технології з теоретичної й ексклюзивної площини сьогодні впритул наблизилися до медичної практики.

Аналізуючи стан сучасних світових інформаційних систем (ІС) в медицині, ми пропонуємо класифікацію їх основних напрямків: діагностичні, лікувальні, лікувально-діагностичні та інформативно-аналітичні системи.

На сьогодні практично не існує аналогів лікувальних експертних систем (ЕС), які давали б практичному лікарю – фахівцю структуровані терапевтичні схеми медикаментозного призначення для лікування різних патологій. Складність полягає в створенні інформаційної

моделі представлення знань даної предметної області, яка вимагає знань кваліфікованого експерта. Внаслідок цього була розроблена інформаційна модель лікувальних ІС. (Рис.1)

Рис.1 Інформаційна модель лікувальної ІС.

Системи діагностичного кодування стають в наш час більш універсальними, але детальний перелік ознак і симптомів, формати для реєстрації даних, а також організація записів визначаються індивідуально. Ще немає гнучких комп'ютерних методів машинного представлення медичних знань, а також формалізації прийняття рішень. Проте інтелектуальні програми підтримки прийняття рішень, що допомагають лікарям в задачах вибору варіанту лікування, на сьогодні є найменш висвітленою галуззю штучного інтелекту і створює підґрунтя для подальшого розпрацювання та вирішення цієї проблеми.

УДК 681.3.06

ПРОГРАМА ІМІТАТОР КОМП'ЮТЕРНОГО МОДЕЛЮВАННЯ ЗУБНИХ ПРОТЕЗІВ

Ю.П. Гульчак[1], к.т.н., доцент,
Е.Ю. Гульчак[2], студент
[1]Вінницький національний технічний університет
[2]Вінницький медичний коледж

Нові технології розвиваються з кожним днем. У стоматології комп'ютери застосовуються не лише для точної діагностики захворювання, але і для моделювання зубних протезів. Останнє досягнення в протезуванні зубів – імплантація, абсолютно немислима без комп'ютерного моделювання.

Програми, використовуючи дані комп'ютерної томографії зубів і щелеп, створюють ідеально точну модель майбутньої конструкції в тривимірній графіці з урахуванням всіх індивідуальних особливостей пацієнта. Комп'ютер, враховуючи їх, створює прозору об'ємну модель, і лікар на екрані дістає можливість побачити структуру щелепи, розташування нервів і судин, коріння зубів. А потім має можливість прямо на екрані провести віртуальну установку імплантатів, задаючи розмір, товщину, кут нахилу.

В стоматології починає впроваджуватись спеціальна програма CEREC inLab 3Dрозпізнає тривимірні зображення препарованих зубів, сусідніх зубів і антагоністів (протилежних зубів) і моделює системні пропозиціїпо їх реставрації з банку даних, який налічує декілька тисяч оптичних зліпків природних зубів.

Алгоритм коструювання зубного протеза формується лише в голові техніка чи стоматолога. Без досвіду роботи з 3D графікою їм складно відслідкувати всі його етапи на екрані монітора. Це займає багато часу і скорочує ефективність використання апарату CEREC. Л з набуттям досвіду роботи і розвитком просторової уяви стає легко і зрозуміло спілкуватися з програмою.

Запропоновано створити комп'ютерну навчальну програму з об'ємними моделями різних конструкцій і схемами їх побудов. Для відновлення вставки потрібно вибрати відповідну об'ємну фігуру (первинну форму у вигляді прямокутної призми) і змоделювати окремі її поверхні. Перш за все це жувальна поверхня, нижня основа вставки, її бічні поверхні, внутрішні грані основи, які межують з бічними стінками препарованої поржнини. Аналогічно для коронки і вініра: це циліндр і, відповідно, сплющений циліндр.

Програма повторює всі етапи побудови конструкції протеза і дає можливість розглянути в об'ємі, з усіх сторін, кожен елемент окремо і всю конструкцію повністю, як на препарованому зубі, так і поза ним. Поєднанняліній побудови із зоною препарування і з самою відновною конструкцією дозволяє швидко зрозуміти цілісну картину конструювання і передбачити кінцевий результат протезування.

Програма адаптована для використання як зубним техніком, так і стоматологом. Він може майбутню конструкцію в об'ємі, а вже потім, за допомогою того ж комп'ютера, це в реальну річ. У програмі розглядаються послідовності побудов окремо для різних моделей зубних протезів (молярів, премолярів, різців).

Окрема версія використовується в рекламних цілях і орієнтована на пацієнта та покращення взаєморозуміння лікаря та запитів пацієнта.

УДК 004.658.2+004.415.2

СТРУКТУРА ІНФОРМАЦІЙНОЇ СИСТЕМИ «МЕДИЧНИЙ ПАСПОРТ»

А.Г. Григорович, викладач
Дрогобицький державний педагогічний університет імені Івана Франка
a_grygorovych@mail.ru

Інформаційна система «Медичний паспорт» функціонально складається із двох частин: стаціонарної частини «Поліклініка» та мобільної частини «Дільничний терапевт» (рис. 1).

Стаціонарна частина системи «Медичний паспорт» (підсистема «Поліклініка») оперує із базою даних пацієнтів. Інформація із підсистеми «Поліклініка», яка стосується пацієнтів певної дільниці експортується у XML-документ (стрілка 1 на рис.2,а) для передачі мобільній частині. Інформація із підсистеми «Поліклініка» може бути проаналізована та у вигляді статистичних звітів надана користувачеві (стрілка 2 на рис.2,а). Дані із мобільної частини інформаційної системи, отримані з XML-документа, поповнюють базу даних (стрілка 3 на рис.2,а). Таким чином, підсистема «Поліклініка» реалізує сховище даних, інформація в якому може лише поповнюватися.

Мобільна частина інформаційної системи «Медичний паспорт» – інформаційна система «Дільничний терапевт» – оперує з даними про пацієнтів конкретної дільниці, представленими за допомогою XML-документу (оскільки це забезпечує найбільшу мобільність в оперуванні цими даними)

Рис.1. Функціональна схема інформаційної системи «Медичний паспорт»

Дільничний терапевт використовує XML-документ як електронний записник, що містить медичні паспорти пацієнтів: зчитує інформацію (стрілка 1 на рис. 2,б) та вносить нові записи (стрілка 2 на рис. 2,б).

а) ІС „Поліклініка” б) ІС „Дільничний терапевт”

Рис.2. Функціональна схема інформаційних систем «Поліклініка» і «Дільничний терапевт»

Розроблено алгоритми програмного модуля обміну даними між стаціонарною та мобільною частинами інформаційної системи «Медичний паспорт».

УДК 681.3.06

КЛАСТЕРИЗАЦИЯ МЕДИЦИНСКИХ СТАТИСТИЧЕСКИХ ДАННЫХ СРЕДСТВАМИ MICROSOFT ANALYSIS SERVER 2008

Д.В. Коломиец, ассистент кафедры
Одесский национальный университет
им. И.И. Мечникова
D.Kolomiyets@onu.odessa.ua

В процессе первичного анализа информации, когда о данных мало что известно, часто прибегают к решению задачи кластеризации исследуемых данных. Решение этой задачи помогает лучше понять природу возникновения событий, а также существенно сузить огромный объем информации до набора характерных групп или кластеров, обладающих схожими свойствами.

Основой для применения методов кластеризации будет база данных медицинского учреждения. В базе зафиксированы факты обращения пациентов с указанием даты, возраста, пола, код заболевания и признака диспансерного учета. Атрибут возраст позволяет отнести пациента к одной из возрастных групп: дети, подростки, взрослые или пенсионеры. Пол представлен двумя значениями: мужской и женский. Коду заболевания можно поставить в соответствие класс заболевания. Например, эссенциальная гипертензия, код I10, относится к классу заболеваний системы кровообращения.

Пакет Microsoft SQL Server 2008 Analysis Services (SSAS) содержит метод, позволяющий выполнять кластеризацию данных (Microsoft Clustering), а также просматривать полученные результаты в удобной форме. Метод базируется на двух основных алгоритмах

кластеризации: алгоритм k-средних (K-Means) и EM-алгоритме (Expectation Maximization). Оба алгоритма относятся к классу так называемых неиерархических алгоритмов, основанных на оптимизации некоторой целевой функции, определяющей оптимальное разбиение множества данных на группы. Алгоритм k-средних использует в качестве целевой функции сумму квадратов взвешенных отклонений координат объектов от центров кластеров. В EM-алгоритме вместо центров кластеров предполагается наличие функции плотности вероятности для каждого кластера с соответствующим значением математического ожидания и дисперсии. В смеси распределений ведется поиск их параметров (средние и стандартные отклонения) по принципу максимума правдоподобия.

Результатом применения описанного метода к исходному массиву данных является набор кластеров, анализ которых позволяет сделать определенные выводы. С одной стороны, можно убедиться в том, что болезни системы кровообращения больше свойственны людям пенсионного возраста, и наоборот, наличие соответствующего кластера дает основание считать, что травмам больше подвержены дети и подростки мужского пола. Таким образом, можно утверждать, что сформированная модель отражает естественные и логически объяснимые закономерности. Однако б*о*льший исследовательский интерес представляют кластеры, содержащие неочевидные, неожиданные закономерности, составляющие так называемые скрытые знания. Т.е. полученное разбиение может служить основой для применения других методов Data Mining, для того чтобы попытаться выяснить смысл, а также разобраться в причинах, вызвавших такое разбиение.

Наукове видання

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА КОМ'ЮТЕРНА ІНЖЕНЕРІЯ

Тези доповідей
Міжнародної науково-практичної конференції
м. Вінниця 19-21 травня 2010 року

(українською та російською мовами)

Матеріали подаються в авторській редакції

Оригінал-макет підготовлений оргкомітетом конференції

Підписано до друку 28.04.2010. Гарнітура Times New Roman
Формат 29,7×42¼. Папір офсетний.
Друк різографічний. Ум. друк. арк. 27,7.
Наклад 140 прим. Зам. № 2010-074.

Вінницький національний технічний університет
21021, м. Вінниця, Хмельницьке шосе, 95, ВНТУ, ГНК, к. 114.
Тел.: (0432) 59-85-32.
Свідоцтво суб'єкта видавничої справи
серія ДК № 3516 від 01.07.2009 р.

Віддруковано в Вінницькому національному технічному університеті,
комп'ютерному інформаційно-видавничому центрі.
21021, м. Вінниця, Хмельницьке шосе, 95, ВНТУ, ГНК, к. 114
Тел.: (0432) 59-81-59
Свідоцтво суб'єкта видавничої справи
серія ДК № 3516 від 01.07.2009 р.