

**Всеукраїнська
науково-практична конференція
студентів та магістрантів**

**СУЧАСНІ
ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ
ТА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ
КОМП'ЮТЕРНИХ СИСТЕМ**



Збірник тез доповідей

Міністерство освіти і науки, молоді та спорту України
Кіровоградський національний технічний університет
Національний технічний університет “Харківський політехнічний інститут”
Національний авіаційний університет
Тернопільський національний технічний університет імені Івана Пулюя
Запорізький національний університет
Харківський національний університет імені В.Н. Каразіна
Тернопільський національний економічний університет
Студентське наукове товариство Кіровоградського національного технічного університету
Наукове товариство студентів та аспірантів Запорізького національного університету
Студентське наукове товариство Тернопільського національного економічного університету
Студентське наукове товариство Сумського національного аграрного університету
Наукове студентське товариство Київського національного економічного університету
Студентське наукове товариство Харківського національного університету імені В.Н. Каразіна

Наукове видання

**СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА
ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ КОМП'ЮТЕРНИХ СИСТЕМ**
Збірник тез доповідей Всеукраїнської науково-практичної
конференції студентів та магістрантів
27-29 березня 2013 року

**Всеукраїнська науково-практична конференція
студентів та магістрантів**

**“СУЧАСНІ ІНФОРМАЦІЙНІ
ТЕХНОЛОГІЇ ТА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ
КОМП'ЮТЕРНИХ СИСТЕМ”**

27-29 березня 2013 року

Тези доповідей надруковано у авторській редакції.

Відповідальний за випуск: Доренський О.П.

Збірник тез доповідей

Видавництво «КОД»
Свідоцтво Державного комітету інформаційної політики ДК № 995 від 24.07.2002
25009, м. Кіровоград, вул. 50 років Жовтня, 7а, тел./факс (0522) 322-326

Підп. до друку 28.03.2013. Формат 60×90/16. Гарнітура Times New Roman.
Умовн. друк. арк. 13,00. Папір типографський №1. Друк офсетний.
Зам. № 405 Тираж 150 прим.

Кіровоград
«КОД»
2013

С91 Сучасні інформаційні технології та програмне забезпечення комп’ютерних систем: збірник тез доповідей Всеукраїнської науково-практичної конференції студентів та магістрантів, 27-29 березня 2013 року, м. Кіровоград. — Кіровоград: “КОД”, 2013. — 208 с.

Рекомендовано до друку Науково-технічною радою Кіровоградського національного технічного університету (протокол № 3 від 28 березня 2013 року)

Збірник містить матеріали Всеукраїнської науково-практичної конференції студентів та магістрантів “Сучасні інформаційні технології та програмне забезпечення комп’ютерних систем”, яка відбулась 27-29 березня 2013 року у Кіровоградському національному технічному університеті. У доповідях розглянуто наукові, технічні, технологічні й практичні проблеми сучасних інформаційних технологій та комп’ютерних систем, теорії розробки програмного забезпечення, програмного забезпечення комп’ютерних систем і мереж, захисту інформації в інформаційно-телекомунікаційних системах, програмного та інформаційного забезпечення автоматизованих систем керування, сучасних ІТ-технологій підготовки фахівців з програмування.

УДК 004
ББК 32.97
С91

Відповідальний за випуск: Дібринський О.П.

Матеріали збірника публікуються у авторській редакції.
Відповідальність за зміст несуть автори.

Адреса оргкомітету конференції

Кіровоградський національний технічний університет
просп. Університетський, 8, м. Кіровоград, 25006
Тел.: (0522) 55-10-49, (0522) 39-04-49
E-mail: conf_kir@ukr.net. Web-сайт: www.conference.ho.ua

© Автори, 2013
© Кіровоградський національний
технічний університет, 2013

ЗМІСТ

СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА КОМП’ЮТЕРНІ СИСТЕМИ	8
<i>Бігун М.Б.</i> Автоматизована комп’ютерна система збору та аналізу прогнозу погоди	8
<i>Близнюк М.В.</i> Розробка інформаційно-графічного забезпечення методів розв’язання оптимізаційних задач	9
<i>Бондарчук А.П.</i> Перспективи переходу к когнитивным технологиям	11
<i>Брушніцька А.С.</i> Алгоритми розпізнавання й аналізу поведінки споживачів рекламної продукції для комп’ютерної системи відеоспостереження.....	13
<i>Головатюк О.Ю.</i> Програмна система екологічного моделювання, спроектована з використанням об’єктно-орієнтованої технології	15
<i>Ветрогон О.М., Шпинковська М.І.</i> Проектування комп’ютерної мережі гуртожитку університету	17
<i>Алісова О.А.</i> Алгоритм розв’язання задачі управління запасами фармацевтичного підприємства	19
<i>Долженко А.А.</i> Використання GPU в паралельних обчисленнях на прикладі триангуляції Делоне	21
<i>Вовк О.В.</i> Розробка додатків в MS Access	23
<i>Верховський О.С.</i> Програмне забезпечення системи генерації складних двомірних матричних штрих-кодів типу QR	24
<i>Ігумин А.А.</i> Оценка вычислительной сложности моделей статической фрагментации задач.....	25
<i>Волохов Є.Ю.</i> Програмне забезпечення автоматів самообслуговування на базі сенсорних терміналів платіжної системи QIWI	26
<i>Врублевський Д.В.</i> Програмне забезпечення GPS навігатора на основі чипу серії SiRF Atlas V	27
<i>Десятник А.В.</i> Програмне забезпечення системи автоматичної перевірки ліцензійних угод програмних продуктів	28
<i>Демішонкова А.О.</i> Огляд та дослідження основних видів нейронних мереж для розпізнавання образів.....	29
<i>Гарбуз І.Є.</i> Розробка програмного забезпечення системи автоматизації збору заявок торгових агентів з використанням смартфонів	32
<i>Кислий Д.І.</i> Онтологічне моделювання для навчання студентів – філологів в системі понять лінгвістики	33
<i>Жак О.С.</i> Програмне забезпечення моніторингу використання Інтернет-трафіку у локальній мережі	35
<i>Кікоть В.М.</i> Оглядовий аналіз інформаційної системи конкурсного відбору кадрів	36
<i>Ковальчук С.А.</i> Програмне забезпечення розпізнавання графічних образів за допомогою нейронної мережі Хеммінга	37
<i>Котенко О.Ю.</i> Прогнозування основних показників фінансової діяльності підприємства «Гідроапаратура».....	38

<i>Кравчук О.В.</i> Автономна комп'ютерна система керування автомобілем	39
<i>Лісішин В.В.</i> Програмна реалізація системи розпізнавання зображень	41
<i>Кудря М.Ю.</i> Розробка інформаційної системи розкладу кафедри ВНЗ.....	42
<i>Могилевська Н.Ю., Гусев А.С.</i> Розробка геоінформаційної системи міста для торгових підприємств	44
<i>Наумова В.О., Рало О.М.</i> Розробка програмного забезпечення для медичних апаратно-комп'ютерних систем (МАКС)	46
<i>Кузьменко М.В.</i> Порівняльна характеристика багатопроцесорних архітектур.....	47
<i>Лактіонов О.В.</i> Розробка програмного забезпечення системи комп'ютерного зору для створення інтерактивних користувальницьких інтерфейсів.....	49
<i>Пайцький С.В.</i> Програмне забезпечення файлового менеджера смартфонів на базі мобільної ОС Android.....	51
<i>Обженський Д.А.</i> Програмне забезпечення системи моніторингу стану жорсткого диску з використанням технології SMART	51
<i>Панасюк О.М.</i> Програмне забезпечення системи автоматизованого керування електронним діловодством підприємства	52
<i>Пахомов О.В.</i> Автоматизація роботи бібліотечної системи	53
<i>Пшеничний І.М.</i> Програмне забезпечення інтелектуального дому за технологією Z-Wave	55
<i>Тагієв А.В.</i> Розробка програмного забезпечення системи стеження за автомобільним транспортом з використанням міток геокодування на базі ОС Android	56
<i>Хоткевич Е.В.</i> Расширение возможностей параллельного порта ПК.....	57
<i>Чернявський Р.В.</i> Розробка системи автоматизації роботи цеху на прикладі ПрАТ «Гідросила»	59
<i>Чужикова-Проскурнина О.Д.</i> Применение вероятностных устройств в измерительных системах.....	61
<i>Ярифа М.С.</i> Разработка нейронной модели оценки состояний маршрутизатора.....	63
<i>Шнуренко І.М.</i> Алгебраический метод демодуляции сложных сигналов.....	64
<i>Ятел О.В.</i> Розробка програмного забезпечення стиснення зображень за допомогою вейвлет-перетворень	66
ТЕОРІЯ РОЗРОБКИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ	68
<i>Кучерук В.Т.</i> Методика створення програмного забезпечення для систем управління підприємствами з використанням типових програмних компонентів	68
<i>Богатиренко А.С., Недолужко А.А.</i> Застосування метода статичного тестування для виявлення та усунення помилок ПЗ	70
<i>Командир А.А.</i> Технология MVC для разработки web-приложений	72
<i>Змеул О.М.</i> Дослідження методів забезпечення надійності програмного забезпечення	73
<i>Скакун П.П.</i> Розробка власної мови програмування та інтерпретатору до неї на основі мови програмування Racket	76
<i>Гуменюк С.С.</i> Програмне забезпечення верстата ЧПК обробки електроізоляційного картону	77
<i>Зінов'єв С.А.</i> Програмне забезпечення системи реінжинірингу та рефакторингу програмного коду до платформи .NET	78
<i>Кучеренко І.С.</i> Програмне забезпечення системи запобігання аналізу та модифікації програмних продуктів	79

<i>Сороколат С.Д.</i> Програмне забезпечення системи управління даними зовнішніх жорстких дисків з інтерфейсом USB 3.0.....	80
ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ КОМП'ЮТЕРНИХ СИСТЕМ І МЕРЕЖ	81
<i>Берчіян Д.А., Болтова Ю.В.</i> Проблеми моделювання при модернізації локальної обчислювальної мережі.....	81
<i>Бобрішиова Р.О.</i> Структура семантичного Web.....	82
<i>Богатиренко А.С.</i> Розробка інформаційної системи сучасного типу на прикладі будівельної організації.....	84
<i>Бондаренко Р.А.</i> Передача даних мережею за протоколом SSL	85
<i>Гаража В.О.</i> Створення архівів у файлової системі NTFS з розмежуванням доступу за допомогою алгоритму AES	87
<i>Давидов Д.О.</i> Програмне забезпечення системи формування фільтрів від фішингу в мережі Internet	89
<i>Джебко В.В.</i> Програмне забезпечення системи контролю та керування доступом з використанням смарт-карт за технологією RFID	90
<i>Кулик Д.І.</i> Масштабно-інваріантна поведінка процесу зростання комп'ютерних мереж.....	91
<i>Дерполок С.М.</i> Система моніторингу динаміки успішності студентів на основі мобільної платформи.....	92
<i>Івасишин Т.М., Михальчук Ю.П.</i> Проблемні питання використання автоматизованої системи «клієнт-банк» у розслідуванні кримінальних правопорушень	93
<i>Іванченко О.О.</i> Прогнозування футбольних матчів у режимі віддаленого доступу за допомогою засобів статистики та моніторингу баз даних	96
<i>Зубенко В.В.</i> Програмне забезпечення антивірусної перевірки HTTP-трафіку смартфонів на базі ОС Android	98
<i>Іщенко А.О.</i> Система аналізу динаміки успішності студентів в учбовому процесі.....	99
<i>Касян О.В.</i> Програмне забезпечення IRC-клієнту.....	101
<i>Катрухін О.С.</i> Програмна реалізація перешкодостійкого кодування для передачі даних комп'ютерною мережею	101
<i>Косенко О.О.</i> Автоматизація роботи відділу кадрів лікарні	103
<i>Коваленко І.І.</i> Проектування бази знань для підтримки прийняття рішень для управління обліком готової продукції на виробництві.....	104
<i>Малаховський В.Ю.</i> Програмні засоби поширення даних із застосуванням СМС повідомлень.....	105
<i>Мяснянкін К.А.</i> Програмне забезпечення як об'єкт авторських прав: проблеми правового захисту	107
<i>Миндра М.В.</i> Розробка програмного забезпечення системи налаштування маршрутизаторів локальної мережі з використанням методів оптимізації.....	110
<i>Молчанов І.С.</i> Програмне забезпечення обробки даних системи відеонагляду з використанням БД та технології KVM	111
<i>Недолужко А.А.</i> Розробка автоматизованої системи митного оформлення.....	112
<i>Осауленко К.І.</i> Програмне забезпечення антивірусного захисту файлових серверів....	113
<i>Орел А.В.</i> Застосування алгоритму Форчуна в сучасних САПР	114
<i>Печенюк С.В.</i> Дослідження мобільних операційних систем.....	115
<i>Пономар О.О.</i> Створення програмного забезпечення багатопотокової обробки цифрових зображень	116
<i>Попова Я.С.</i> Пристрій безпроводної передачі даних між ПК.....	117

<i>Прачѐв А.А., Троцький С.А.</i> Распараллеливание потока данных в MPLS сетях для повышения эффективности передачи данных	119
<i>Прокопов О.О.</i> Розробка програмного забезпечення системи керування роботою клієнтської частини аукціону.....	121
<i>Салтан В.С.</i> Розробка програмного забезпечення розрахунків показників QoS в мережах наступного покоління	123
<i>Семенов Ф.О.</i> Розробка програмного забезпечення методу виявлення аномалій телекомунікаційного трафіку на основі спектрально-часового аналізу.....	124
<i>Сербін Р.С.</i> Програмне забезпечення моніторингу локальної мережі та відстежування дій користувачів	126
<i>Суворов О.О.</i> Використання мультисерверної архітектури в сучасних СУБД.....	126
<i>Сурін В.В.</i> Розробка програмного забезпечення системи керування роботою адміністративної частини аукціону	128
<i>Троцький С.А., Прачѐв А.А.</i> Построение универсальной информационной системы с повышенной надежностью.....	129
<i>Цимбал К.С.</i> Розробка програмного забезпечення системи відеоспостереження на базі бездротових мереж	131
<i>Шевкун Б.О.</i> Програмне забезпечення браузеру для перегляду веб-сайтів.....	132
<i>Шпурік В.В.</i> Програмне забезпечення системи обміну миттєвими повідомленнями у мережі Інтернет.....	133
<i>Шевченко Д.Г.</i> Дослідження перспектив використання мови програмування Google Blockly	133

ЗАХИСТ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

<i>Землянко В.В.</i> Захист інформаційних мереж в Україні	136
<i>Гладишев Д.В.</i> Розробка програмного забезпечення захисту конфіденційної інформації у мережі методом стеганографії	137
<i>Козекін Ю.М.</i> Порівняльний аналіз методів екстраполяції для приховування даних в просторовій області нерухомих зображень методом Куттера-Джордана-Боссена	139
<i>Бубенкова В.С.</i> Способи обмеження просочування інформації по радіоканалу	140
<i>Войтищен Л.І.</i> Законмірності хвильових процесів в ближній зоні елементарних випромінювачів електричного та магнітного полів.....	142
<i>Гажур Д.М.</i> Програмна модель генератора m-последовності	145
<i>Годла А.С.</i> Усовершенствование распределенной модели использования ресурсов в условиях информационной безопасности	147
<i>Головатюк О.Ю.</i> Розробка програмного забезпечення реалізації прихованих цифрових водяних знаків з використанням методів псевдоголографії.....	149
<i>Гончарова Ю.В.</i> Про колізії у визначеннях, наданих у Законах України щодо інформаційно-комунікаційних мереж та безпеки інформації	152
<i>Деркач О.І.</i> Фізична природа прямих акустоелектричних перетворювань.....	154
<i>Дзюбенко С.О.</i> Розробка програмного забезпечення для статистичного стегоаналізу графічних файлів	155
<i>Єсіна М.В.</i> Алгоритм Кессак – новий стандарт гешування даних.....	157
<i>Зазимко А.В.</i> Розробка програмного забезпечення статистичного аналізу та фільтрації даних зі змінних носіїв.....	159
<i>Захарчук Н.В.</i> Ідентифікація радіовипромінювань.....	160
<i>Косенко О.О.</i> Дослідження ансамблевих, кореляційних і структурних властивостей складних дискретних сигналів	162

<i>Кудрина А.Г.</i> Технология линейного целочисленного декодирования псевдослучайных кодов	164
<i>Мартинюк В.М.</i> Ефективність методів захисту програм, як інтелектуальної власності	166
<i>Молдавський П.С.</i> Розробка програмного забезпечення вбудовування прихованих маркерів у файли для відстежування їх поширення по комп’ютерній мережі	168
<i>Пулеко К.І.</i> Застосування методу кластеризованих ранжировок при експертній оцінці рішень в галузі інформаційної безпеки	169
<i>Сальников М.С.</i> Оцінка багатовимірних функцій розподілу ймовірностей	170
<i>Суворов О.О.</i> Формування складних дискретних сигналів для стеганографічного захисту інформації.....	171
<i>Старіцин М.В.</i> Програмне забезпечення системи управління файлами в ОС Windows на основі технології EFS.....	172
<i>Таратайко Д.В.</i> Технологія застосування електронного цифрового підпису на державному підприємстві “Укрзалізниця”	173
<i>Тімохін С.С.</i> Кодування інформації точками на еліптичній кривій	175
<i>Ускова А.І.</i> Використання методів кліпуючих перетворень мовних сигналів у комп’ютерних мережах	177
<i>Хамидуллина Е.Д.</i> Прогнозирование и оценка потерь, связанных с угрозами информационных систем	178
<i>Хейдер О.В.</i> Розробка програмного забезпечення ЕЦП для автентифікації користувачів у системах дистанційного навчання та тестування.....	181

ПРОГРАМНЕ ТА ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ АВТОМАТИЗОВАНИХ СИСТЕМ КЕРУВАННЯ.....

<i>Власюк Е.Р., Март Б.А., Покотило А.А., Ступак Б.В.</i> Методы оценки состояния элементов корпоративной ИТ-инфраструктуры	183
<i>Бойко Д.И.</i> Автоматизация управления распределенными вычислительными процессами при использовании библиотеки имитационных моделей.....	185
<i>Буравченко К.О.</i> Автоматизована інформаційна система керування водопостачанням об’єкта.....	187
<i>Гостищев Є.А.</i> Розробка програмного забезпечення макромови для керування робототехнічним комплексом і спряження з контролером керування	188
<i>Погонієв В.А.</i> Сучасні напрямки використання мікроконтролерів та процесорів архітектури ARM	189
<i>Тарасенко А.О.</i> Програмне забезпечення системи побудови зображення TV-тюнера цифрового телебачення стандарту DVB-T2	190
<i>Усенко Д.В.</i> Розробка програмного забезпечення системи дистанційного голосового керування робототехнічним комплексом.....	191

СУЧАСНІ ІТ-ТЕХНОЛОГІЇ ПІДГОТОВКИ ФАХІВЦІВ З ПРОГРАМУВАННЯ.....

<i>Бондаренко І.С.</i> Програмна модель роботи підсистеми Win API 32 ОС Windows	193
<i>Мартыненко Н.М.</i> Онлайн-экзамен оценки знаний по курсу: «Язык программирования JavaScript»	194
<i>Гнезділов С.М.</i> Дослідження ефективності впровадження у навчальний процес емуляторів пристроїв і систем.....	196

Організаційний комітет конференції.....	199
Учасники конференції.....	200

СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА КОМП'ЮТЕРНІ СИСТЕМИ

УДК 004.89:551.509

М.Б. Бігун

Науковий керівник – Бабчук С.М., канд. техн. наук, доцент
Івано-Франківський національний технічний університет нафти і газу

Автоматизована комп'ютерна система збору та аналізу прогнозу погоди

В багатьох галузях народного господарства для досягнення максимального економічного ефекту необхідно планувати заходи з врахуванням прогнозу погоди на наступний період часу. Достовірна інформація про погоду необхідна в авіації, судноплаванні, рибальстві, будівництві, енергетиці, сільському господарстві [1-3]. Відсутність точного прогнозу погоди в авіації і мореплаванні може призвести до тяжких наслідків і навіть до загибелі людей. Більша частина жителів та підприємств планети використовує для отримання інформації про прогноз погоди джерела в мережі Internet. На даний момент в мережі Internet налічується понад півтори сотні сайтів які надають інформацію про прогноз погоди. Проте, головною проблемою є недостовірність такої інформації.

Метою даної роботи є розробка комп'ютерної системи, яка б автоматизовано проводила збір, аналіз, узагальнення наявної в мережі Internet інформації про прогноз погоди та формувала б найбільш достовірні дані про неї.

Проведені дослідження дають підстави вважати, що для реалізації даного завдання необхідно зчитувати інформацію, не менш ніж з 5 сайтів, які в рейтингу «Прогноз погоди» займають перші місця. В подальшому треба обчислити середнє арифметичне значення показників з 5 вибраних джерел.

Встановлено 5 погодних сервісів, які відповідають наступним критеріям:

- висока ймовірність точного прогнозування;
- пошук за назвою міста;
- weather API;
- надання сервісом XML-формату;
- період прогнозу від 3-х днів;
- безкоштовне надання інформації.

Кожен з обраних сервісів має свій власний стандарт подання даних, що ускладнює розрахування середнього прогнозу погоди. Оскільки сервіси надають результати прогнозу погоди в форматі XML, то було прийнято рішення конвертувати дані до власної форми:

- місто (назва міста);
- стан погоди (сонячно, хмарно, дощ);
- температура (поточна температура);
- вологість;

- швидкість вітру;
- напрямок вітру;
- мінімальна і максимальна температура на 3 дні.

З метою вирішення поставленої задачі розроблено алгоритм роботи програми.

Для зручності роботи з даними та правильної їх організації в Visual Studio 2010 створено класи-об'єкти:

- CurrentWeather;
- WeatherOnTheDay;
- ForecastWeatherItem.

Щоб перевірити ефективність створеної системи та працездатність розробленого програмного забезпечення проведені безпосередні спостереження за погодою та також порівняльні дослідження в які було залучено такі сервіси:

- Google Weather API;
- www.gismeteo.ua
- World Weather Online;
- Yahoo Weather API;
- Wunderground.com.

Проведений аналіз результатів досліджень дає підстави зробити висновок, що точність розробленої системи є більшою ніж у тих, що були використані для діагностики.

Автоматизована комп'ютерна система збору та аналізу прогнозу погоди забезпечує легке отримання результатів прогнозу погоди з різних сервісів, проведення їх аналізу та узагальнення, що збільшує ймовірність надання користувачу системи достовірних даних щодо погодних умов.

Список літератури

1. Баклі Б. Погода: Енциклопедичний путівник / Б. Баклі, Е.Д. Хопкінс, Р. Уайтекер. – К.: Махаон-Україна, 2007. – 304 с.
2. Пфейфер Ф. Погода интересует всех. – М.: Гидрометеорологическое издательство, 1966. – 124 с.
3. Погосян Х. П. Какая погода будет завтра? / Х.П. Погосян, И.Г. Ситников. – М.: Воениздат МО СССР, 1967. – 274 с.

УДК 004.42

М.В. Близнюк

Науковий керівник – Ляшенко О.А., канд. техн. наук, доцент
Український державний хіміко-технологічний університет

Розробка інформаційно-графічного забезпечення методів розв'язання оптимізаційних задач

Проблема пошуку максимуму чи мінімуму функцій при заданих обмеженнях (умовна оптимізація) чи без обмежень (безумовна оптимізація) є досить актуальною в наш час, адже спеціалісти різних напрямків часто стикаються з необхідністю розв'язання оптимізаційних задач. Вони є необхідними в економіці та банківській справі, в техніці, в соціології.

На сьогоднішній день є чимало варіантів програмного забезпечення спрямованих на вирішення певних оптимізаційних задач з певної області досліджень.

Але виникає необхідність самостійно створювати програмний модуль для вирішення задачі поставленої безпосередньо перед виконавцем.

При викладанні таких предметів як «Системи штучного інтелекту», «Чисельні методи» та інших виникає необхідність реалізації та візуалізації методів оптимізації.

Для вирішення певної задачі оптимізації можливим є використання MATLAB, MathCAD. Кожен з цих пакетів має можливість розв’язувати поставлені перед ними задачі шляхом завдання певної функції та зображення кінцевого графічного розв’язку. Наприклад, MATLAB дає змогу використовувати функцію `fminbnd`, а в MathCAD рішення визначається за допомогою функцій – `Maximize`, `Minimize`. На жаль, жоден з подібних пакетів не надає користувачеві відомостей щодо проміжних обчислень на кожному кроці вирішення задачі, на кожній ітерації.

З огляду на таку ситуацію, виникла необхідність створити програмне забезпечення, що дає змогу продемонструвати роботу деяких методів оптимізації графічно. Тож розробка інформаційно-графічної системи даного типу є наразі досить актуальною.

Було створено програмне забезпечення для деяких методів оптимізації. Розробка виконувалась в середовищі програмування Microsoft Visual Studio 2010 з використанням мови програмування C++ [1].

Для роботи було обрано функцію двох змінних – функцію Розенброка. Вона є тестовою функцією для локальних методів оптимізації. Функція задається програмно, а користувачеві надається можливість змінювати необхідні параметри для розв’язання задачі.

Завдяки подібному модулю є можливість реалізувати вирішення задачі наступними методами:

- метод сканування (метод повного перебору) – є одномірним, багатоекстремальним з неопуклою цільовою функцією;
- метод Бокса – є прямим методом умовної оптимізації;
- метод Нелдера-Міда (метод деформованого багатокутника) – є багатомірним, багатоекстремальним з неопуклою цільовою функцією методом безумовної оптимізації нульового порядку.

Для побудови графічної частини було побудовано лінії рівня (ізолінії) для обраної функції.

Метод сканування або метод повного перебору полягає у послідовному перегляді значень параметра оптимізації по всій поверхні функції та знаходженні такої точки, в якій параметр оптимізації має оптимальне значення. Точність методу визначається кроком квадратичної решітки, у вузлах якої знаходяться значення цільової функції. Тому користувачеві надано можливість змінювати крок решітки [2].

Метод Нелдера-Міда – метод безумовної оптимізації функції від декількох змінних. Тут розглядається регулярний симплекс, який у двомірному просторі є правильним трикутником. При використанні цього методу необхідно вказувати довжину ребра симплексу, коефіцієнти стягнення, розтягнення, відображення та редукції. Відповідно кожен з них впливає на формування кінцевого результату обчислення [3].

Метод Бокса є модифікацією методу деформованого багатогранника і призначений для вирішення задач нелінійного програмування з обмеженнями-нерівностями. Для мінімізації функції будують комплекси. При побудові комплексу вказується необхідний крок решітки [4].

Для розв’язання поставленої задачі користувачеві необхідно задавати не лише параметри кожного з методів, а й вказувати координати початкової точки, точність та швидкість побудови ліній на графіку.

Окрім графічної реалізації методу, користувач отримує й інформацію щодо результатів розв’язання як загального, так і проміжних. Користувачеві надається інформація про значення функції на кожній ітерації. Наявність такого пункту дає змогу спостерігати за точністю розрахунків під час вирішення задачі.

Також для зручності роботи користувача було створено інформаційну довідку щодо кожного з використаних методів, яка дозволяє проглянути необхідні для вирішення задачі теоретичні відомості.

Такого типу розробки є досить цікавими для викладачів вищих навчальних закладів. Маючи в своєму арсеналі подібні програми є можливість надавати студентам не лише теоретичні відомості про методи оптимізації функції, а й практично показувати поетапний процес знаходження оптимального обраної функції. Також програма дає можливість студентів проглянути результати вирішення задачі самостійно.

Список літератури

1. Шилдт Г. Искусство программирования на С++ [Текст]/Г.Шилдт–СПб.:БХВ-Петербург,2005. – 496с.
2. Трифонов А. Г. Постановка задачи оптимизации и численные методы ее решения [Электронный ресурс] // MATLAB&Toolboxes. – Электрон. книга. – 2012. – Режим доступа: http://matlab.exponenta.ru/optimiz/book_2/index.php – Заголовок з екрана.
3. Лутманов С. В. Курс лекций по методам оптимизации [Текст] / С. В. Лутманов. – Ижевск: НИЦ «Регулярная и хаотическая динамика», 2001. – 368 с.
4. Губарь Ю.В. Введение в математическое моделирование [Электронный ресурс] // М.:Интуит.РУ. - Электрон. книга. – 2007. – Режим доступа: <http://www.intuit.ru.department/mathematics/mathprog/12/4.html#sect5> – Заголовок з екрана.

УДК 34.01:004.9

А.П. Бондарчук

Государственный университет информационно-коммуникационных технологий

Перспективы перехода к когнитивным технологиям

Статистика показывает, что почти 20% капитальных затрат оператор беспроводной связи отдает за услуги проектирования сети и установки оборудования. 25% доходов оператора связи идут на затраты по эксплуатации и обслуживанию сети, обучение персонала, контроля и мониторинга состояния. В последнее время такие всемирно известные компании-гиганты как Nokia-Siemens, Motorola, Alcatel-Lucent, Samsung, Huawei, Docomo и другие, занялись разработкой современной сети поддержки. Функциями сети являются построение и эксплуатация современной беспроводной сети связи, которая будет предоставлять максимальное количество услуг высокого качества при уменьшенных капитальных затратах на проектирование, построение и содержание сети, а также обеспечивать ряд других инновационных идей. Технологии, которые смогут обеспечить данные требования, называются когнитивными.

Когнитивные технологии "имитирующие" умственную деятельность человека. Они, как правило, базируются на моделях с нечеткой логикой (fuzzy logic) и на нейронных сетях (neural networks). Цели, которые ставятся при создании когнитивных систем, могут быть представлены следующими примерами: получение новых знаний, принятие решений в сложных ситуациях и интеллектуальная обработка данных.

Отношения между когнитивными системами и инфокоммуникационными сетями можно рассматривать с разных точек зрения. Во-первых, для функционирования

когнитивной системы любого рода необходим обмен информацией, который обеспечивается инфокоммуникационными сетями. Во-вторых, в инфокоммуникационных сетях могут использоваться когнитивные системы и технологии, позволяющие радикально улучшить показатели эффективности процессов обмена информацией [1]. Название такой когнитивной системы - Self-organizing network (SON). Название было закреплено в рекомендации 3GPP TS 32.500, которая гласит: «Управление электросвязью; самоорганизующаяся сеть; концепции и требования».

Система SON устраняет процессы, занимающие много времени, а именно: ручные процессы при эксплуатации сетей, повышает эксплуатационную эффективность и позволяет операторам внедрять новые технологии и расширять сети быстрее, чем до этого.

Решения SON повышают эффективность эксплуатации существующих сетей за счет их автоматической конфигурации процессов хендовера, балансировки нагрузки мобильного трафика и минимизации необходимости в выездных тестированиях. Кроме того, за счет компенсирующих функций и самовосстановления минимизируются перерывы в работе сети для конечных пользователей. Стимулом для внедрения SON является поддержка конфигурации по принципу "plug & play", т.е. "присоединил и работает", не нужно вызвать специалистов для установки программного обеспечения и его настройки работы в сети. Сеть LTE более всего нуждается в SON, поскольку сеть LTE с одной стороны проще своих предшественников, а с другой - ее узлы гораздо функциональнее и сложнее.

Система SON автоматически сконфигурирована, подключена и полностью готова к использованию. Автоматическая конфигурация полностью избавит от расходов на локальные настройки, а автоматическое распознавание соседнего узла значительно снизит затраты на оптимизацию.

К основным возможностям SON можно отнести самоконфигурацию, самооптимизацию и самостоятельное устранение проблем.

Процесс самоконфигурации - это процесс, при котором только что развернутые новые узлы (eNB) автоматически, в процессе установки, конфигурируются путем получения необходимой для работы базовой конфигурации, т.е. происходит автоматическое подключение и ввод в эксплуатацию.

Функция Automatic Neighbour Relationship Setup (ANR) - автоматизация отношений между соседями обеспечивает взаимодействие как базовых элементов сети, так и взаимодействия сетей 2G, 3G или LTE.

Мобильная сеть будущего будет состоять из большого количества базовых станций, которые будут только частично под контролем оператора, а функция самоконфигурации обеспечит сеть гибкостью.

Процесс самооптимизации определен как процесс, во время которого оборудование пользователя и базовая станция проводят измерения, результаты которых используются для автонастройки сети. Функция самостоятельного устранения проблем или "самоочищения" обеспечивает автоматическое детектирование, локализацию большинства ошибок и выполнение механизмов "самоочищения", которые автоматически исправляют некоторые виды ошибок. Например, в случае перегрева системы, может быть снижена ее выходная мощность или произведен возврат на предыдущую версию программного обеспечения.

Самозащита компонентов предусматривает защиту и от вторжений, и от повреждения данных.

Приспособленность - способность компонентов системы приспосабливаться к меняющимся условиям окружающей среды.

Самодиагностика - механизмы для выполнения системных автономных проверок и сравнение результатов с эталонным значением.

Самовосстановления - методы для изменения конфигурации и эксплуатационных параметров системы в целом с целью компенсации неудачи. При самовосстановлении главное внимание уделяется выявлению и диагностике проблем и исправлению сбоя в работе, преимущественно силами соседних базовых станций eNB (evolved Node Base station).

В соответствии с расположением алгоритмов оптимизации, SON можно разделить на три класса: централизованные, распределенные и гибридные.

Когнитивные радиосети (Cognitive Radio Networks - CRN) - парадигма управления сети, целью которой является повышение уровня автоматизации и гибкости сети. CRN позволит результативно и эффективно функционировать мобильным сетям будущего. CRN считается преемником SON [3].

Можно сделать вывод, что концепция самоорганизующихся сетей, введенная альянсом NGMN (Next generation mobile network) в 2007 году и ее преемник - когнитивная система, являются ключевыми факторами для упрощения эксплуатации и технического обслуживания в следующем поколении мобильных сетей.

Разработка данных технологий направлена на:

- сокращение эксплуатационных расходов за счет снижения уровня вмешательства человека в строительство и эксплуатацию сети;
- сокращение капитальных затрат за счет оптимизации использования имеющихся ресурсов;
- увеличение прибыли за счет уменьшения количества ошибок, вносимых человеком.

Список літератури

1. Комашинский В.И., Соколов Н.А. Когнитивные системы и телекоммуникационные сети. Вестник связи, №10, 2011.
2. Gopalakrishnan T.R., Nair, Abhijith N., Sooda K. Transformation of Networks through Cognitive Approaches. - JRI (Journal of Research & Industry), Vol. 1, Issue 1, December 2008.
3. Seppo Hamalainen, Henning Sanneck, Cinzia Sartori. LTE self-organising networks (SON): network management automation for operational efficiency.-John Wiley&Sons,Ltd, 2011 - 428 pp.

УДК 0004.65:65

А.С. Брушніцька

Науковий керівник – Саченко А.О., д-р техн. наук, професор
Тернопільський національний економічний університет

Алгоритми розпізнавання й аналізу поведінки споживачів рекламної продукції для комп’ютерної системи відеоспостереження

Багато сучасних технологій людино-комп’ютерної взаємодії базуються на обробці зображення обличчя. За обличчям можна не тільки ідентифікувати людину, але й розпізнати реакцію на той чи інший зовнішній чинник. Оскільки людські емоції впливають на прийняття рішень, то відслідковування реакції та поведінки, а також їх аналіз, набули значної важливості, зокрема у сфері маркетингових досліджень.

Метою даної роботи є розробка системи розпізнавання реакції споживачів на рекламну продукцію, яка включає наступні етапи: сегментацію за рухом, виявлення та відслідковування облич та аналіз реакції споживача. На ринку вже існують системи, які реалізують деякі з вище згаданих процедур для відеоспостереження за рухомими об’єктами. Наприклад, FaceReader, eMotion Software, MMER_FEASy, FaceSecurity та Neoface, яка дозволяє використовувати систему для аналізу особи покупця, щоб визначити приблизний вік, стать, а також факт повторного відвідування магазинів в рамках торгової мережі. Нажаль не всі системи є повнофункціональними, достовірність їхньої роботи не є достатньою, що зумовлює необхідність пошуку нових підходів до розпізнавання та аналізу.

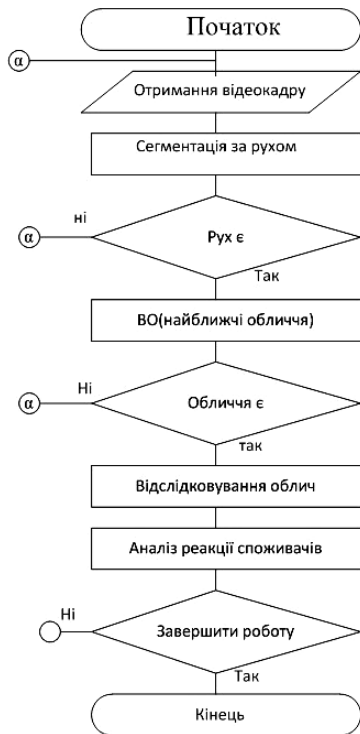


Рисунок 1 – Алгоритм системи розпізнавання реакції споживачів на рекламну продукцію

Ціллю сегментації за рухом є виявлення тих ділянок відеозображення, де присутні рухомі об’єкти. У роботі використано метод віднімання фону, який характеризується високою швидкодією. Суть його полягає у попиксельному відніманні поточного зображення від опорного фонового, створеного як середнє зображення на протязі певного часу при ініціалізації.

Наступним кроком є виявлення облич (ВО), ціллю якого є знаходження координат облич на динамічному зображенні, а також максимальне відкидання фонових ділянок. З цією метою використано методи виявлення облич на основі комбінованого каскаду неймережових класифікаторів (ККНК) [1], який складається із каскаду слабких класифікаторів для виявлення облич-кандидатів і згорткової нейронної мережі для верифікації об’єктів типу “обличчя”. Для даної системи прийнято обмеження, що до уваги береться найближче, тобто найбільше за розміром, зображення обличчя.

Відслідковування облич - це аналіз кадрів у відеопотоці для оцінки та прогнозування параметрів руху виявленого об’єкту. Для цього використано фільтр Калмана та метод співставлення з шаблоном [2]. Калібрування фільтру виконується кожен раз, коли виявлено нове обличчя, щоб він вловив “історію” траєкторії руху обличчя. Для уточнення координат центру обличчя, раз в декілька кадрів виконується локалізація в

області інтересу методом співставлення з шаблоном, так як він простий в реалізації і швидкий. Коефіцієнт кореляції знаходиться за наступною формулою:

$$R_{\text{corr}}(x, y) = \sum_{x', y'} [T(x', y') \cdot I(x + x', y + y')]^2$$

де T – шаблон, I – область інтересу вхідного зображення, Z – нормалізація, (x, y) – координати розміщення пікселя.

Останім етапом є аналіз поведінки споживачів, коли знаходиться маркетингова статистика, зокрема ті люди, які пройшли повз рекламний продукт, поділяються на наступні категорії:

- Дуже зацікавлені – повернулися до продукту;
- Зацікавлені – провели час більший за пороговий;
- Мало зацікавлені - провели час нижчий за пороговий.

Для виявлення людей першої категорії зображення виявлених облич заноситься в базу даних, і кожне нове виявлене обличчя порівнюється з наявними в базі за допомогою методу співставлення з шаблоном. Якщо в базі вже є таке зображення обличчя, то людина відноситься до першої категорії.

Для наступних двох категорій пороговий час визначається експериментально.

Отже, в даній роботі показано структуру та проаналізовано основні процедури системи розпізнавання реакції споживачів на рекламну продукцію. Подальші дослідження включають експериментальну оцінку запропонованого підходу на тестовій вибірці і порівняння показників достовірності і швидкодії із відомими рішеннями.

Список літератури

1. Paliy I. Face Detection on Grayscale and Color Images Using Combined Cascade of Classifiers / Y. Kurylyak, I. Paliy, A. Sachenko, A. Chohra, K. Madani // Computing. – 2009.–Vol. 8, Issue 1.–P. 61-71.
2. Bar-Shalom Y., Li R., Kirubarajan T. Estimation with Applications to Tracking and Navigation. // New York: John Wiley & Sons, 2001. – P. 308–317.
3. Welch G., Bishop G. An Introduction to the Kalman Filter. // University of North Carolina at Chapel Hill, <http://www.cs.unc.edu/welch/kalman/>, pages 1–11, 2006.

УДК 519.876.5

О.Ю. Головатюк

Науковий керівник – Лєвошко О.Л., ст. викладач
Кіровоградський національний технічний університет

Програмна система екологічного моделювання, спроектована з використанням об’єктно-орієнтованої технології

Моделювання широко застосовується для вирішення багатьох актуальних задач екології. Поведінку організмів в живій природі важко адекватно описати засобами математики, але моделі допомагають встановити деякі закономірності і загальні тенденції розвитку окремих популяцій та співтовариств. Вони допомагають виділити суть або об’єднати й виразити, за допомогою декількох параметрів, важливі розрізнені властивості великої кількості унікальних спостережень, що полегшує аналіз розглянутого процесу або проблеми. За допомогою них може бути описане кожне унікальне явище, і відносні властивості таких явищ стають більш зрозумілими [1].

Модель може служити зразком «ідеального об’єкта» або ідеалізованої поведінки, при порівнянні з якою можна оцінювати і вимірювати реальні об’єкти і процеси.

Метою розробленої програмної системи є забезпечення інтерактивного моделювання життєдіяльності океану. Воно складається з океану, який включає

встановлене користувачем число здобичі, хижаків і перешкод. Основні напрямки моделювання описані нижче:

- здобич і хижаки пересуваються;
- перешкоди статичні і не пересуваються, вони перешкоджають руху інших об'єктів в океані;
- моделювання забезпечує залежний механізм для росту і зменшення числа здобичі і хижаків;
- здобич і хижаки розмножуються випадковим чином, чисельність кожного з них може зростати;
- здобич гине, коли її з'їдає хижак;
- хижак гине, якщо не харчується протягом певного інтервалу часу.

Об'єктно-орієнтована технологія є однією з парадигм програмування, яка розглядає програму як множину об'єктів, що взаємодіють між собою. Основу ООП складають три основні концепції: інкапсуляція, успадкування та поліморфізм. Перевагою ООП є більш краща модульність програмного забезпечення [2]. Відповідно до парадигми об'єктно-орієнтованого програмування, кожний об'єкт здатний отримувати повідомлення, обробляти дані, та надсилати повідомлення іншим об'єктам.

Океан складається з двовимірного масиву комірок. Комірка – це абстрактний об'єкт, який зазвичай порожній. Його підкласи представляють різні види об'єктів, які зустрічаються в океані. Океан в моделі – це сукупність усіх комірок. Здобич, хижак та перешкода є видами комірки.

Здобич може рухатися. Вона розмножується у випадку, коли її час для розмноження досягнув нуля і вона перемістилася. Хижак рухається і їсть сусідню здобич. Якщо в сусідній комірці немає здобичі, він буде рухатися до порожньої комірки. Хижак розмножується у випадку, коли його час для розмноження досяг нуля і він перемістився. Хижак вмирає, якщо він не поїсть протягом певного часу. Перешкода не може рухатися.

Результат роботи програми показаний на рисунку 1.

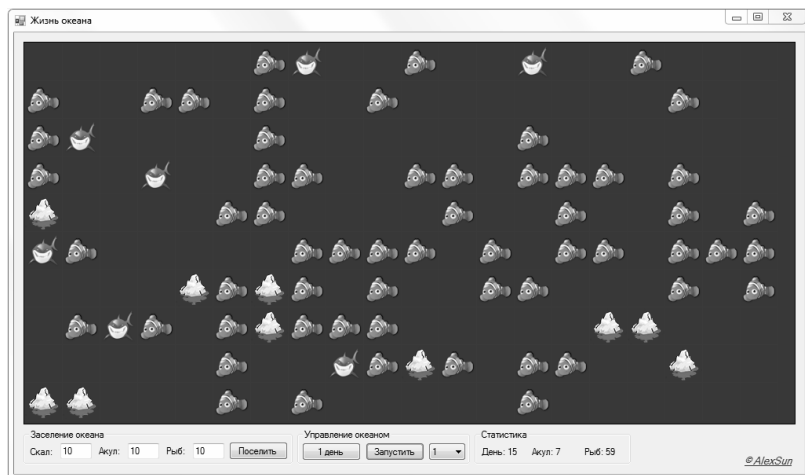


Рисунок 1 – Результат моделювання

Використання програмних систем істотно розширяє межі моделювання екологічних процесів. Вони надають можливість всебічної реалізації складних

математичних моделей, які не допускають аналітичного дослідження. Моделі дійсно можуть пролити світло на реальний світ, недосконалими імітаціями якого вони являються.

Список літератури

1. Имитационное моделирование – Википедия [Электронный ресурс] // Режим доступа: http://ru.wikipedia.org/wiki/Имитационное_моделирование.
2. Вайнер Р. С++ изнутри / Р. Вайнер, Л. Пинсон; пер. с англ. под ред. И. В. Хижняка. – Киев: НПИФ ДиаСофт, 1993. – 299 с.

УДК 004.77

О.М. Ветрогон, М.І. Шпинковська

Науковий керівник – Шпинковський О.А., канд. техн. наук, доцент
Одеський національний політехнічний університет

Проектування комп'ютерної мережі гуртожитку університету

В студентському гуртожитку Одеського національного політехнічного університету склалася наступна ситуація з комп'ютерним забезпеченням:

- у певному замкнутому просторі (кімнати або блоці кімнат) є чимала кількість комп'ютерів, працюючих окремо від всієї решти комп'ютерів поверху (гуртожитку) і які не мають нагоди гнучко обмінюватися з іншими комп'ютерами інформацією;
- неможливе створення загальнодоступної бази даних, накопичення інформації при існуючих об'ємах і різних методах обробки і зберігання інформації.
- існуючі локальні обчислювальні мережі об'єднують в собі невелику кількість комп'ютерів і працюють тільки над конкретними і вузькими задачами.
- накопичене програмне і інформаційне забезпечення не використовується в повному обсязі і не має загального стандарту зберігання даних.

При тому, що є можливість підключення до глобальної обчислювальної мережі Internet, необхідно здійснити підключення до інформаційного каналу не однієї групи, а всіх користувачів за допомогою об'єднання в глобальні групи.

Для вирішення даної проблеми пропонується створити єдину інформаційну мережу підприємства, яка повинна виконувати наступні функції:

- створення єдиного інформаційного простору, здатного охопити всіх користувачів і надати їм інформацію, створену в різному програмному забезпеченні для її обробки, а також здійснювати розпаралелювання і жорсткий контроль даного процесу;
- підвищення достовірності інформації надійності її зберігання шляхом створення стійкої до збоїв і втрати інформації обчислювальної системи, та створення архівів даних які можна використовувати надалі;
- забезпечення ефективної системи накопичення, зберігання і пошуку технологічної, техніко-економічної і фінансово-економічної поточної інформації та вже виконаної (архівна інформація) за допомогою створення глобальної бази даних;
- обробки документів і побудови на базі цього діючої системи аналізу, прогнозування і оцінки обстановки з метою ухвалення оптимального рішення і вироблення глобальних звітів;

- забезпечення прозорого доступу до інформації авторизованому користувачу відповідно до його прав і привілеїв.

Пропонується створення єдиного інформаційного простору, шляхом розгляду і вибору кращого з існуючих способів або їх комбінації.

Проектування мережі складається з чотирьох етапів: системного, логічного, технічного проектування. Розглянуто переваги та недоліки основних методів проектування: спадного, висхідного та зустрічного.

Спадне проектування полягає в тім, що проектування походить від складних елементів до простих елементів. Тобто від системи в цілому, до її під системам і так далі до елементної бази. Висхідне проектування полягає в тому, що проектування походить від простих елементів до складних елементів. Зустрічне проектування це комбінація перших двох.

Так як гуртожиток № 7 є самою високою будівлею, на ньому буде розміщено бездротову точку доступу та файловий сервер усіх гуртожитків. Моделювання роботи мережі гуртожитку виконано у пакеті OLAN. Проведено моделювання завантаження комутаторів, серверів та визначено час транзакцій у мілісекундах на відповідних сегментах (поверхах та окремих кімнатах) будівлі. Результат моделювання підтвердив працеспроможність спроектованої системи. Проведено економічне обґрунтування та обрано відповідне апаратне забезпечення системи.

Таблиця 1 - Результати моделювання працеспроможності окремих комутаторів

Комутатор	Завантаження комутатора, *100%	Час транзакції, ms
Switch2	0.15	329.16
Switch3	0.14	329.16
Switch4	0.14	329.16
Switch5	0.15	329.16
Switch6	0.13	329.16
Switch Hostel 7	0.17	329.16

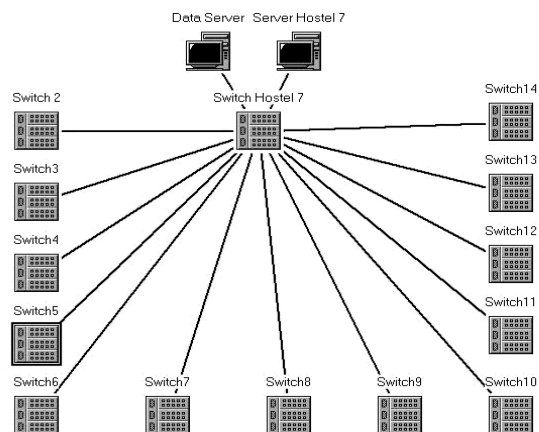


Рисунок 1— Схема з’єднання основного мережевого обладнання гуртожитку

Мережа, що спроектована, має гарний запас по навантаженню для можливого подальшого розширення. Результати розрахунків використовуються для проектування комп’ютерних мереж інших гуртожитків та будівель університету.

Список літератури

1. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 3-е изд. / В.Г.Олифер, Н.А.Олифер. – СПб: Питер, 2006. – 958 с.: ил.

УДК 658.7

О.А. Алісова

Науковий керівник – Сізова Н.Д., д-р. фіз.-мат. наук, професор
Харківський національний університет будівництва та архітектури

Алгоритм розв’язання задачі управління запасами фармацевтичного підприємства

Запас як явище в роботі логістичних систем і ланцюгів поставчань є товарно-матеріальними цінностями, що чекає споживання [1]. Задача управління запасами виникає тоді, коли необхідно створити запас матеріальних ресурсів або предметів споживання з метою задоволення попиту на заданому інтервалі часу (скінченному або нескінченному) [2]. Основна проблема, що виникає при розв’язанні задачі управління запасами, полягає в створенні ефективної і надійної системи управління рівнем наявних запасів [3].

Для того, щоб запас міг забезпечувати наявну потребу, необхідна реалізація процесу управління запасами. Під управлінням запасами розуміється діяльність, направлена на забезпечення необхідного рівня запасу. Процес управління запасами вимагає наявності алгоритму управління запасами. Процедура розробки такого алгоритму включає декілька етапів (рис. 1):

- 1) визначення об’єму потреби у запасі;
- 2) визначення складу статей витрат, пов’язаних із створенням і підтримкою запасу;
- 3) розрахунок оптимального розміру замовлення, що поповнює запас;
- 4) узгодження умов поповнення запасу;
- 5) проектування алгоритму управління запасами [4].

Процедура розробки алгоритму є одним з етапів процесу управління запасами. Вона включає питання, які розв’язуються на різних рівнях організаційної структури управління підприємством. На операційному рівні після завершення розробки алгоритму управління запасами потрібна розробка і відладка програмного забезпечення для підтримки ухвалення рішень відповідно до алгоритму. Експлуатація розробленого алгоритму може завершитися введенням нового алгоритму ухвалення рішень по управлінню запасами.

В роботі подається алгоритм управління запасами для фармацевтичного підприємства «Альфа». Це дозволило знизити рівень витрат на замовлення і збереження запасів лікарських засобів з урахуванням ризиків відсутності товару або його надлишок і підвищити ефективність організації збуту продукції МПП «Альфа».

Для вирішення оптимізаційної задачі управління запасами аптечного підприємства «Альфа» використане програмне середовище MS Excel, за допомогою

якого визначаються оптимальні параметри при різних вхідних даних моделі.



Рисунок 1 – Процедура розробки алгоритму управління запасами у ланцюзі поставок

Наведемо результати деяких розрахунків з використанням розробленого алгоритму. Для аптечного підприємства «Альфа» розрахунок річних витрат на замовлення і зберігання таких препаратів, як алпростан, амаріл та амлодипін вартістю 10, 50 та 1000 грн. відповідно, дозволив визначити річні витрати на замовлення

$$D = A \times (C / F); \quad (1)$$

річні витрати на зберігання

$$E = B \times (F / 2); \quad (2)$$

сумарні річні витрати

$$S = D + E, \quad (3)$$

де А – витрати на замовлення кожної партії ліків; В – витрати на збереження одиниці товару; С – річний продаж товару, F – розмір однієї закупівельної партії.

Встановлено, що при різних частоті і розмірі замовлень річні сумарні витрати змінюються різнонаправлено, існує по кожному з трьох представлених препаратів однакова потреба в кількості ліків у рік. Крім того, виявлено, що потреба в дешевих препаратах значно вище в кількісному виразі, ніж більш дорогих. Розрахунки показали також, що для товарів, вартість яких невисока, витрати на замовлення вагоміші, чим витрати на зберігання.

На рис.2 представлена діаграма витрат для одного із видів ліків.



Рисунок 2 – Витрати на замовлення та збереження одного з ліків алпростану

Список літератури

1. Гурч Л. М. Логістика : Навч. посіб. для студ. вищ. навч. закл. — К. : ДП «Видавничий дім «Персонал», 2008. — 560 с. : іл. — Біб-ліогр.: с. 369–378; 547–548.
2. Горелик В.А., Ушаков М.А. Исследование операций. -М.: Машиностроение, 2007. – 352 с.
3. Глушик М.М., Телесницька Н.М. Дослідження операцій. – Львів: «Новий світ-2000», 2009. – 368 с.
4. Стерлігова А.Н. Управління запасами у ланцюгах постачання: Підручник. – М.: ИНФРА-М, 2008. – 430 с.

УДК 004.92

А.А. Долженко

Науковий керівник – Дбрєнський О.П., викладач
Кіровоградський національний технічний університет

Використання GPU в паралельних обчисленнях на прикладі триангуляції Делоне

Інформаційні технології з комп’ютерної графіки динамічно розвиваються у напрямку візуалізації тривимірних зображень у режимі реального часу [1]. Її засоби допомагають вирішувати широке коло завдань інтерактивного проектування, автоматизованого навчання, контролю технологічних параметрів, теоретичних і прикладних досліджень. При цьому необхідно оброблювати величезні масиви інформації та виконувати розрахунки, які потребують затрат великої кількості ресурсів комп’ютерних систем. Тож, потужність центрального процесора й об’єму оперативної пам’яті є недостатньою. Саме тому для формування зображень використовують графічні процесори (GPU – від англ. Graphics Processing Unit), які стали одним із ключових компонентів обчислювальних систем [1].

GPU-обчислення представлені спільним використанням CPU та GPU в гетерогенній моделі обчислень. Завдяки цій моделі програмування розробники можуть змінити програми і перенаправити обробку вимогливих до ресурсів блоків програм на GPU. Інша частина програми виконується на центральному процесорі. Основною відмінністю GPU від CPU є кількість обчислювальних ядер. Структури CPU та GPU зображено на рисунку 1.

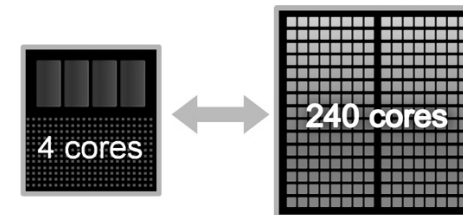


Рисунок 1 – Структури CPU та GPU

Одним з лідерів ринку GPU-обчислень є компанія NVIDIA, яка створила власну програмно-апаратну платформу під назвою CUDA [3]. Фактично CUDA дозволяє включати в текст

програми, написаної за допомогою мови C, спеціальні функції, які виконуються на графічному процесорі. CUDA дає розробникові можливість на власний розсуд організувати доступ до набору інструкцій графічного пристроювача і керувати його пам’яттю, організувати на ньому складні паралельні обчислення. Саме завдяки цим можливостям CUDA перетворюється в потужну програмовану платформу з відкритою архітектурою.

Науково-дослідна робота є продовженням дослідження [2] алгоритмів триангуляції Делоне [5] та має на меті розробку програмно-апаратного комплексу реального часу, призначеного для побудови високодеталізованих моделей реального світу і їх коректного відображення.

Триангуляція Делоне та її застосування наведено у літературі [5, 6]. Графічні приклади триангуляції та триангуляції Делоне зображено на рис. 2.

В роботі [2] досліджено ітеративний алгоритм “Видаляй та будуй”, у результаті чого встановлено, що, завдяки обмеженням архітектури центрального процесора використання вказаного алгоритму є досить обмеженим і може спричинити досить

повільну роботу системи при великому масиві точок. Отже, для розв’язку задачі, що постала, застосовано графічний процесор.

Дослідження проведено на основі відеоадаптера GTX560.

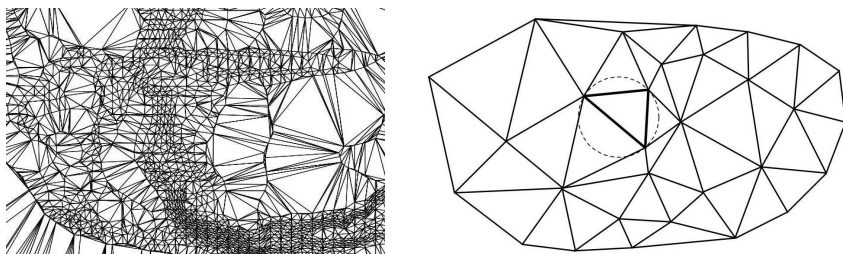


Рисунок 2 – Приклад триангуляції (ліворуч) та триангуляції Делоне (праворуч)

Особливості структури GPU дозволяють виконувати паралельну обробку ділянок площини, що дозволяє пришвидшити роботу програмного забезпечення приблизно в 3-4 рази. На процесорі GF114 [4] програма показала 4-кратну швидкість обробки графічних масивів даних (об’ємних об’єктів). Але, безсумнівно, основним призначенням відеокарт є побудова високоякісного тривимірного зображення (пряме відношення до якого має триангуляція [2]). І сучасні GPU забезпечують рішення графічних задач. На рисунку 3 зображено результати роботи алгоритму триангуляції з використанням центрального процесора (ліворуч) та графічного (праворуч) процесора.

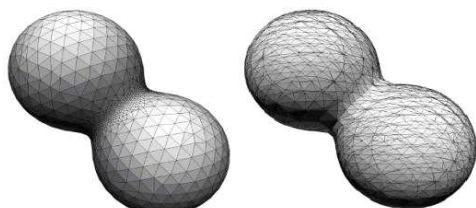


Рисунок 3 – Порівняння результатів роботи алгоритму Делоне

Звичайно, деталізація 3D-об’єкта, що знаходиться праворуч, є набагато більшою. Разом з цим, кількість відображених на екрані кадрів становить 60 FPS, що є достатньою нормою для створення, наприклад, анімації.

В результаті дослідження зроблено висновок, що GPU є найбільш перспективною технологією паралельних обчислень, яка досить активно інтегрується в сучасних наукових розробках. Використання графічного процесора для розв’язку задачі триангуляції Делоне, що постала у дослідженні [2], є цілком виправданим рішенням. Також є доцільним застосування гетерогенної моделі обчислень в задачах побудови детального зображення.

Список літератури

1. Романюк О.Н. Класифікація графічних відеоадаптерів / Романюк О.Н., Довгалюк Р.Ю., Олійник С.В. // Наукові праці ДонНТУ: Інформатика, кібернетика та обчислювальна техніка. – Вип. 14 (188). – 2011. – С. 211-215.
2. Долженко А.А. Побудова високодеталізованих тривимірних об’єктів на основі триангуляції / А.А. Долженко, О.П. Доренський // Актуальні задачі сучасних технологій – Тернопіль.: Видавництво ТНТУ ім. Івана Пулюя, 2012. – С. 182-183.
3. NVIDIA [Електронний ресурс] – Режим доступу: www.nvidia.com/object/cuda_home_new.html.
4. NVIDIA [Електронний ресурс] – Режим доступу: www.nvidia.ru/object/product-geforce-gtx-560-ru.html.
5. Фукс А.Л. Предварительная обработка набора точек при построении триангуляции Делоне / А.Л. Фукс // Геоинформатика. – Вип. 1. – 1998. – С. 48-60.
6. Скворцов А.В. Триангуляция Делоне и её применение / А.В. Скворцов – Томск: Изд-во Том. ун-та, 2002. – 128 с.

УДК 004.65

О.В. Вовк

Науковий керівник – Єсін В.І., канд. техн. наук, доцент
Харківський національний університет імені В.Н. Каразіна

Розробка додатків в MS Access

В умовах сучасного розвитку інформаційних технологій, при зростаючому обсязі інформації, що циркулює на підприємстві, необхідні механізми, що служать для її зберігання, обробки та аналізу. Одним з таких механізмів є організація зберігання інформації в базах даних. Використання цього механізму надає можливість оперативного доступу до даних, дозволяє автоматизувати зберігання та обробку інформації, підвищує ефективність прийняття управлінських рішень.

Бази даних складають в даний час основу комп’ютерного забезпечення інформаційних процесів, входять практично в усі сфери людської діяльності. Процеси обробки інформації мають загальну природу і спираються на опис фрагментів реальності, виражене у вигляді сукупності взаємопов’язаних даних. Бази даних є ефективним засобом представлення структур даних і маніпулювання ними. Концепція баз даних припускає використання інтегрованих засобів зберігання інформації, що дозволяють забезпечити централізоване управління даними і обслуговування ними багатьох користувачів. При цьому БД повинна підтримуватися в середовищі ЕОМ єдиним програмним забезпеченням, званим системою управління базами даних.

В даний час серед розробників бази даних (БД) великою популярністю користується реляційна СУБД Access, що входить до складу пакета Microsoft Office. Дружній інтерфейс і простота настройки, ефективні засоби створення таблиць, форм, запитів, інтеграція з іншими додатками пакета, засоби організації роботи з базами даних і захист інформації - ось далеко не повний перелік переваг цього додатка.

Для організації ефективної роботи користувача, за допомогою програми MS Access, можна створити цілісний додаток, в якому всі компоненти бази даних будуть згруповані за функціональним призначенням. При цьому можна забезпечити зручний графічний інтерфейс користувача. Додаток дає можливість користувачеві працювати з базою даних, витрачаючи при цьому менше зусиль.

При створенні програми користувача головну роль відіграють форми, так як саме вони є основним діалоговим засобом роботи користувача з базою даних. У форми можуть включатися процедури обробки подій, які дозволяють управляти процесом введення, перегляду і коректування даних. Такі процедури зберігаються в модулі форми.

Форми створюються для наступних цілей:

- введення і перегляду взаємопов’язаних даних бази на екрані в зручному вигляді, відповідному звичному для користувача документу;
- управління ходом виконання програми;
- виведення повідомлень;
- друк інформації.

Додатковим елементом програми користувача є організація виклику головної кнопкової форми при відкритті бази даних, що дозволяє користувачеві відразу ж почати роботу в середовищі додатку.

Розробка додатків в Access включає наступну послідовність етапів:

- збір інформації про потреби підприємства;

- вибір архітектури додатку;
- реалізація СУБД і бізнес-логіки додатка;
- оптимізація продуктивності БД;
- тестування та налагодження;
- розгортання додатки.

За допомогою MS Access можна створювати додатки, які повністю будуть відповідати вашим потребам по управлінню даними. Одне з найбільш потужних засобів Access - різні Майстри (засоби розробки об'єктів), які використовуються для створення таблиць, запитів, різних типів форм і звітів, просто вибравши потрібні опції. Щоб повністю автоматизувати роботу додатку, можна легко зв'язати дані з формами та звітами за допомогою макросів Access.

Список літератури

1. Д.Крэнке. Теория и практика построения баз данных. 8-е издание. – СПб.: Питер, 2003. – 800 с.
2. Ролланд Ф.Д. Основные концепции базы данных. – М.: Вильямс, 2002. – 256 с.
3. Гурвиц Г.А.. Разработка приложений на реальном примере. – СПб.: БХВ-Петербург, 2010. – 496 с.

УДК 004.4

О.С. Верховський

Науковий керівник – Минайленко Р.М., канд. техн. наук, ст. викладач
Кіровоградський національний технічний університет

Програмне забезпечення системи генерації складних двомірних матричних штрих-кодів типу QR

QR-код (англ. quick response – швидкий відгук) – матричний код (двовимірний штрихкод), розроблений і представлений японською компанією «Denso-Wave» в 1994 році. Основне достоїнство QR-коду – це легке розпізнавання скануючим устаткуванням (у тому числі й фотокамерою мобільного телефону), що дає можливість використання в торгівлі, виробництві, логістиці. QR-коди найбільше поширені в Японії, країні, де штрих-коди користувалися такою великою популярністю, що обсяг інформації, зашифрованої в кодї, незабаром перестав улаштовувати індустрію. Японці почали експериментувати з новими способами кодування невеликих обсягів інформації в графічній картинці.

Максимальна кількість символів, які містяться в один QR-код:

- цифри – 7189;
- цифри й букви (включаючи кирилицю) – 4296;
- двійковий код – 2953 байт;
- ієрогліфи – 1817.

У цей час QR-код широко розповсюджений у країнах Азії (особливо в Японії), поступово розвивається у Європі й Північній Америці. Найбільше визнання він одержав серед користувачів мобільного зв'язку – установивши програму-розпізнавач, абонент може моментально заносити у свій телефон текстову інформацію, додавати контакти в адресну книгу, переходити по web-посиланнях, відправляти SMS-повідомлення й т.п.

Таким чином, виходячи з вищеперерахованого, розробка програмного забезпечення системи генерації складних двомірних матричних штрих-кодів типу QR, є актуальною задачею.

Список літератури

1. Романов Д. Двухмерные штрих-коды [Электронный ресурс]. – Режим доступа: <http://www.ibs.ua/spravka/181/>.
2. Трукин Д. Двухмерный (2D) штрих-код – Структура [Электронный ресурс]. – Режим доступа: <http://www.barcoding.ru/resources/statii-obzory/dvukhmernyi-shtrikh-kod-struktura.html>.
3. Еремин Е. А. Язык трехмерного моделирования VRML и его образовательные возможности [Электронный ресурс]. – Режим доступа: <http://inf.1september.ru/article.php?ID=200800200>.
4. Коренберг В. М. Интерактивные системы. Человеко-машинный интерфейс, основанный на распознавании жестов / Коренберг В. // Научные труды XVII международной конференции молодых ученых по приоритетным направлениям развития науки и техники. – Екатеринбург: УГТУ–УПИ, 2010. – С. 27–34.
5. Кручинин А. Спецификация Aztec Code (без Small Aztec) [Электронный ресурс]. – Режим доступа : <http://recog.ru/blog/standarts/6.html>.
6. Лонгрейс Э. Двумерное штриховое кодирование. Штрих-код Aztec [Электронный ресурс]. – Режим доступа : <http://www.biprint.ru/index.php?area=text&parent=10>.

УДК 004.75

А.А. Игумин

Научный руководитель – Шматков С.И., доктор техн. наук
Харьковский национальный университет им В.Н. Каразина

Оценка вычислительной сложности моделей статической фрагментации задач

Быстрое расширение областей применения распределенных вычислительных сетей (РВС) приводит к постоянному роду требований к их эффективности, в первую очередь к производительности, времени выполнения задач, величине доставки сообщений, достоверности обработки информации. Вычислительную сложность метода/модели статической или временной фрагментации задач определим как суммарное количество «условных» операций, используемых при решении задачи фрагментации.

В данной работе выполнено моделирование оценки вычислительной сложности статической фрагментации. Программа написана на языке высокого уровня программирования C++ в среде Visual Studio.

Исходные данные: kfr – число фрагментов; n – вершины; k – ярусы; s – степень полиномов.

Оценка сложности $Q1(k)$ синтеза для k -го яруса $SL(k)$ полного множества полиномов:

$$Q1(k) = \sum_{s=1}^{n(k)-1} n^s(k)$$

Оценка сложности $QT(k)$ синтеза редуцированных формальных полиномов k -го яруса Si -графа:

$$QT(k) = \frac{n(k)!}{s!(n(k)-s)!};$$

Оценка сложности $QR(k)$ формирования k -го яруса множества покрытий $R(k)$:

$$QR(k) = \sum_{s=1}^{n(k)-1} C_{n(k)}^s * \sum_{i=s+1}^{n(k)} C_{n(k)}^s;$$

Оценка сложности QM(k) выбора для k-го яруса покрытия с минимальным количеством обменов сообщениями:

$$QM(k) = \sum_{s=1}^{n(k)-1} \sum_{f=1}^{k_f} n(f, s);$$

```

C:\WINDOWS.1\system32\cmd.exe
Enter k 3
Enter kfr chislo fragmentov 2
Enter steepni s 5
Enter kol-vo vershyn n 4

k = 1
Q1 = 137256
QT = 21
QR = 35231
QM = 84

k = 2
Q1 = 1.11125e+009
QT = 252
QR = 3.69936e+006
QM = 180

k = 3
Q1 = 2.52407e+013
QT = 399.317
QR = 3.17614e+007
QM = 312
Для продолжения нажмите любую клавишу . . .
    
```

Рисунок 1 – Приклад роботи програми

Список литературы

1. Воеводин В.В., Воеводин Вл. В. Параллельные вычисления. – СПб.: БХВ-Петербург, 2002. – 608 с.
2. Поляков Г.А., Шматков С. И., Толстолужская Е. Г., Толстолужский Д. А. – Харьков: Синтез и анализ параллельных процессов в адаптивных времяпараметризованных системах. - 2012. - 554с.
3. www.parallel.ru

УДК 004.4

Є.Ю. Волохов

Науковий керівник – Дреєва Г.М., асистент
 Кіровоградський національний технічний університет

Програмне забезпечення автоматів самообслуговування на базі сенсорних терміналів платіжної системи QIWI

Програмне забезпечення для автоматів самообслуговування (АСО) – обов'язкова складова комплексного програмно-апаратного рішення, призначеного для прийому платежів через систему ОСМП.

Програмне забезпечення встановлюється на АСО і являє собою додаток, що зв'язує АСО із платіжною системою. Додаток складається із двох модулів:

– Модуль прийому платежів надає користувачеві можливість оплатити різні види послуг за допомогою зручного й інтуїтивно зрозумілого інтерфейсу.

– Адміністративний модуль дозволяє провести настроювання АСО, здійснювати подальше сервісне обслуговування, а так само виконує функції моніторингу.

Для максимальної зручності організована можливість віддаленого керування й моніторингу АСО в режимі реального часу. Для цього існує ряд додатків:

– Програма для моніторингу автоматів самообслуговування за допомогою ПК “QIWI Монітор”.

– Програма для моніторингу автоматів самообслуговування за допомогою мобільного телефону “QIWI Монітор Мобайл (Java)”.

– Програма для моніторингу автоматів самообслуговування за допомогою КПК і смартфонів “QIWI Монітор Мобайл (PDA)”.

– Програма для моніторингу автоматів самообслуговування за допомогою apple iphone.

– Моніторинг автоматів самообслуговування за допомогою особистого кабінету агента ОСМП.

Таким чином, виходячи з вищеперерахованого, розробка програмного забезпечення автоматів самообслуговування на базі сенсорних терміналів платіжної системи QIWI, є актуальною задачею.

Список литературы

1. Техническое описание автомата по приему платежей ОСМП-УЛИЦА ТО 5151-001-71320257-2006-07.
2. Техническое описание автомата по приему платежей ОСМП-2 С ЛАЙТ-БОКСОМ.
3. Инструкция по установке и настройке программного обеспечения для автомата по приему платежей.
4. Техническое описание автомата по приему платежей ОСМП-2 ТО 5151-001-71320257-2006-02.
5. Попов В.И. Основы сотовой связи стандарта GSM – М.: ЭкоТрендз, 2005 – 296с.

УДК 004.4

Д.В. Врублевський

Науковий керівник – Сидоренко В.В., ст. викладач
 Кіровоградський національний технічний університет

Програмне забезпечення GPS навігатора на основі чипу серії SiRF Atlas V

Винахід супутникових систем навігації по своїй значимості можна зрівняти з винаходом мобільного зв'язку, супутникових телебачення й телефонії. Людина, що хоч один раз у житті виявлялася в незнайомій місцевості, удалині від доріг і інших орієнтирів, по достоїнству оцінить цей найбільший винахід 20 століття.

Сьогодні GPS-навігація стає надзвичайно популярною серед аматорів пішого, гірського, водного й лижного туризму, мисливців і рибалок, велосипедистів і багатьох інших аматорів активного відпочинку. Тому, кому потрібно знати, де він перебуває, звідки прийшов, як йому добратися до потрібного місця, з якою швидкістю він рухається й коли добереться до мети – можна порадити скористатися перевагами, надаваними GPS.

Навігація, у сучасному своєму виді, заснована на таких дисциплінах, як астрономія, картографія, геодезія. Робота штурмана вимагає безлічі спеціальних знань, навичок роботи з навігаційними приладами, картами, довідниками. Недарма на судні штурман є другою людиною після капітана. Помилки штурмана нерідко приводять до трагічних наслідків.

Основні завдання, розв'язувані навігацією – вибір безпечного і найкоротшого шляху, визначення місця, швидкості й напрямку руху, оцінка точності цих визначень. З усіма цими завданнями з легкістю впорасться грамотний користувач супутникового навігатора, не обтяжений тим величезним обсягом знань, необхідних професійному штурманові в його роботі.

Таким чином, виходячи з вищеперахованого, розробка програмного забезпечення GPS навігатора на основі чипу серії SiRF Atlas V є актуальною задачею.

Список літератури

1. Пер Энге GPS добрался до метра// В МИРЕ НАУКИ № 6 2007 с35-43
2. GPS: Все, что Вы хотели знать, но боялись спросить. Неофициальное пособие по глобальной системе местопределения, М.: «Бук Пресс» -2006. 352 с.

УДК 004.622

А.В. Десятник

Науковий керівник – Помазан Л.В., канд. техн. наук, доцент
Кіровоградський національний технічний університет

Програмне забезпечення системи автоматичної перевірки ліцензійних угод програмних продуктів

Рівень використання в Україні неліцензійного, «піратського», програмного забезпечення становить близько 90%, повідомила прес-служба Державного комітету зв'язків й інформатизації України. В Україні щорічно реалізується програмного забезпечення на суму близько 120-140 мільйонів доларів, з них легального - тільки на суму від 25 до 35 мільйонів доларів. Втрати бюджету від недоотриманих податків становлять близько 30 мільйонів доларів у рік.

Відмітні ознаки ліцензійного програмного забезпечення – це оплата за використання програмного продукту протягом застереженого періоду часу. На підтвердження внесення оплати правовласник підписує з користувачем угоду, яка фактично і є ліцензією (ліцензійною угодою).

Як правило, визначення наявності ліцензій на програмне забезпечення, установлене на підприємстві, здійснюється на підставі надання компанією документів, які можуть це підтвердити. До них ставляться бухгалтерські документи, що підтверджують придбання ПЗ (рахунок-фактура, платіжне доручення, накладна про одержання програм, податкова накладна), підписана ліцензійна угода із правовласником, голографічні наклейки, ліцензійні диски, з яких здійснювалася установка. Крім того органи, що перевіряють, можуть захотіти подивитись сертифікат компанії, у якій купувалося ПЗ. Він служить підтвердженням легального уведення ліцензійного програмного забезпечення на територію України.

Масова перевірка встановленого ПЗ на підприємстві та формування звітів потребує спеціалізованого ПЗ, яке буде дозволяти проводити перевірки в полу автоматичному режимі зосереджуючись на інших питаннях.

Таким чином, виходячи з вищеперахованого, розробка програмного забезпечення системи автоматичної перевірки ліцензійних угод програмних продуктів є актуальною задачею.

Призначення системи – автоматична перевірка ліцензійних угод програмних продуктів. Тобто в нас є флешка та ПК який необхідно перевірити. Необхідно вставити флешку до ПК який необхідно перевірити, та через декілька хвилин отримати детальний звіт о ліцензіях які використовуються на цьому ПК. Інспектор з питань інтелектуальної власності має право проводити огляд документів та прав на використання програм. Область застосування ПЗ – формування звіту ліцензій на ПК у короткій проміжок часу. Програма працює в автоматичному режимі, втручання користувача мінімальні.

УДК 004.8

А.О. Демішонкова

Науковий керівник – Мелешко Є.В., канд. техн. наук, доцент
Кіровоградський національний технічний університет

Огляд та дослідження основних видів нейронних мереж для розпізнавання образів

Розпізнавання необхідної інформації-важливий аспект у сучасному використанні ЕОМ. Для реалізації даного завдання людство вигадало таке поняття, як нейронна мережа. Штучні нейронні мережі (ШНМ) – математичні моделі, а також їхня програмна та апаратна реалізація, побудовані за принципом функціонування біологічних нейронних мереж – мереж нервових клітин живого організму. Системи, архітектура і принцип дії базується на аналогії з мозком живих істот. Ключовим елементом цих систем виступає штучний нейрон як імітаційна модель нервової клітини мозку – біологічного нейрона. Цей термін виник при вивченні процесів, які відбуваються в мозку, та при спробі змодельовати ці процеси. Першою такою спробою були нейронні мережі Маккалока і Піттса. Як наслідок, після розробки алгоритмів навчання, отримані моделі стали використовуватися в практичних цілях: в задачах прогнозування, для розпізнавання образів, в задачах керування та інших [4].

Актуальними на сьогоднішній день є задачі використання нейромережевих методів для розпізнавання тексту, зображень, людських облич тощо. Перспектива їх використання досить яскрава в світлі вирішення нетрадиційних проблем і є ключем до цілої технології.

Мета даної роботи – огляд та дослідження нейромережевих методів для розпізнавання графічних образів.

Загальні принципи розпізнавання тексту. Алгоритм розпізнавання тексту наступний: на вхід системи розпізнавання надходить растрове зображення сторінки. Для роботи алгоритмів розпізнавання бажано, щоб поступаюче на вхід зображення мало прийнятну якість. Тому перед застосуванням алгоритмів розпізнавання проводиться його попередня обробка, спрямована на поліпшення якості зображення [1].

Робота простого класифікатора здійснюється в два кроки. Спочатку по вхідному зображенню обчислюються ознаки. Значення кожної ознаки є функцією від яскравостей деякої підмножини пікселів зображення. У результаті виходить вектор значень ознак, що надходить на вхід нейронної мережі. Кожен вихід мережі відповідає

одній з букв алфавіту, а одержуване на виході значення розглядається як рівень приналежності літери нечіткій множині [2].

Завданням алгоритму комбінування є узагальнення інформації, що надходить у вигляді вхідних нечітких множин та обчислення на їх основі вихідної нечіткої підмножини множини розпізнаваних символів. Результатом роботи класифікатора є нечітка множина, отримана в результаті комбінування на самому верхньому рівні.

На останньому етапі приймається рішення про найбільш правдоподібний варіант прочитання слова. Для цього використовуються рівні можливості прочитання окремих літер, між літерної сегментації та частоти сполучень літер.

Застосування таких методів дає можливість виконати процедури навчання нейронної мережі на прикладі друкованих символів, виконавши розпізнавання символів, і на основі отриманих даних вибрати оптимальний метод.

Нейронні мережі для розпізнавання зображень. Для розпізнавання окремих зображень використовують наступні види нейронних мереж:

- багатощарові нейронні мережі. Архітектура багатощарової нейронної мережі (БНМ) складається з послідовно з'єднаних шарів, де нейрон кожного шару своїми входами пов'язаний з усіма нейронами попереднього шару, а виходами - наступного. НМ з двома вирішувальними шарами може з будь-якою точністю апроксимувати будь-яку багатовимірну функцію. НМ з одним вирішувальним шаром здатна формувати лінійні розділяючі поверхні, що сильно звужує коло завдань, що вирішуються, зокрема така мережа не зможе вирішити завдання типу "виключаюче або". НМ з нелінійною функцією активації та двома вирішувальними шарами дозволяє формувати будь-які опуклі області в просторі рішень, а з трьома вирішувальними шарами - області будь-якої складності, в тому числі і неопуклості. При цьому МНС не втрачає своєї узагальнюючої здатності. Навчаються МНС за допомогою алгоритму зворотного поширення помилки, що є методом градієнтного спуску в просторі ваг з метою мінімізації сумарної помилки мережі. При цьому помилки (точніше величини корекції ваг) поширюються в зворотному напрямку від входів до виходів, крізь ваги, що з'єднують нейрони;

- нейронні мережі високого порядку (НМВП) відрізняються від БНМ тим, що у них тільки один шар, але на входи нейронів надходять так само терми високого порядку, що є добутком двох або більше компонентів вхідного вектора [1]. Такі мережі так само можуть формувати складні розділяючі поверхні. Особливістю такої мережі полягає в тому, що для навчання деякому класу достатньо продемонструвати його образ без варіацій масштабів та поворотів – після вивчення мережа буде розпізнавати відомі класи з масштабом та поворотом. Така мережа не є повнозв'язною, швидко навчається та працює в порівнянні з БНМ;

- НМ Хопфілда (НМХ) буває одношарова і повношарова (зв'язки нейронів на самих себе відсутні), її виходи пов'язані з входами. На відміну від БНМ, НМХ є релаксаційною - тобто будучи встановленою в початковий стан, функціонує до тих пір, поки не досягне стабільного стану, який і буде її вихідним значенням. НМХ застосовуються в якості асоціативної пам'яті і для розв'язання оптимізаційних задач. У першому випадку НМХ навчається без вчителя (наприклад, за правилом Хебба), у другому випадку ваги між нейронами спочатку кодують вирішуване завдання. Таким чином НМХ з початкового стану сходиться до найближчого локального мінімуму енергії мережі, стан нейронів в якому і буде відновленим образом для задач розпізнавання, і рішенням - для оптимізаційних задач. Для пошуку глобального мінімуму стосовно оптимізаційних задач використовують стохастичні модифікації НМХ [1]. Застосування даної мережі відмічається хорошим результатом відновлення трьохвимірної форми (також для зображень облич) і високою швидкістю;

- самоорганізуючі нейронні мережі Кохонена (СНМК) забезпечують топологічне упорядкування вхідного простору образів. Вони дозволяють топологічно безперервно відобразити вхідний n -мірний простір в вихідний m -мірний, $m \ll n$. Вхідний образ проєктується на деяку позицію в мережі, кодованих як положення активованого вузла. На відміну від більшості інших методів класифікації і кластеризації, топологічне упорядкування класів зберігає на виході подобу у вхідних образах [2], що є особливо корисним при класифікації даних, що мають велику кількість класів. Мережі такого типу складаються з одного шару (не рахуючи вхідного), який так само може бути організований в n -мірну сітку, в залежності від розмірності вихідного простору. Кожен нейрон зв'язаний з усіма вхідними нейронами. Налаштування ваг мережі здійснюється методом конкурентного навчання, в процесі якого змінюються тільки ваги нейрона-переможця, що має максимальну активність. Для даної мережі характерна висока швидкість навчання;

- когнітрон [3] своєю архітектурою схожий на будову зорової кори, має ієрархічну багатощарову організацію, в якій нейрони між шарами пов'язані тільки локально. Навчається дана мережа без вчителя. Кожен шар мозку реалізує різні рівні узагальнення; вхідний шар чутливий до простих образів, таких, як лінії, і їх орієнтації в певних областях візуальної області, в той час як реакція інших шарів є більш складною, абстрактною і незалежною від позиції образу. Аналогічні функції реалізовані в когнітроні шляхом моделювання організації зорової кори. Когнітрон є потужним засобом розпізнавання зображень, але потребує високих обчислювальних затрат, які на сьогодні недосяжні[3].

Висновки. Загалом до переваг розглянутих нейронних мереж можна віднести надійне розпізнавання зображень, швидке навчання та високу швидкість. Проте при застосуванні цих методів до зображень тривимірних об'єктів виникають труднощі, пов'язані з просторовими поворотами і зміною умов освітленості [5].

Зображення для різних кутів повороту об'єкта суттєво різняться, частина інформації на зображенні втрачається, виникає нова, специфічна для даного кута. Такі обмеження зазвичай долаються шляхом пред'явлення всіляких варіацій зображення (різні повороти і освітленість) при навчанні, але побудова такого навчального набору - важке завдання, і найчастіше такі набори недоступні.

Як показує світовий досвід, ці проблеми не можуть бути повністю вирішені вибором вихідного представлення даних. Отже необхідно, щоб система самостійно витягала характеристики, інваріантні до змін всередині класу і максимально репрезентативні по відношенню до міжкласових змін. Таке завдання в загальному вигляді для систем розпізнавання осіб ще не вирішене, але існують методи, які показують можливості вирішення окремих аспектів [1] (інваріантність до освітлення, синтез повернутих в просторі зображень осіб на основі навчання). Вказана вище проблема і є головним недоліком використання існуючих нейронних мереж для розпізнавання образів, і потребує подальшого вивчення та вирішення у майбутньому.

Список літератури

1. Головкин В.А. Нейроинтеллект: Теория и применения. Книга 1. Организация и обучение нейронных сетей с прямыми и обратными связями – Брест:БПИ, 1999, – 260 с.
2. Головкин В.А. Нейроинтеллект: Теория и применения. Книга 2. Самоорганизация, отказоустойчивость и применение нейронных сетей – Брест:БПИ, 1999, - 228 с.
3. Уоссермен Ф. Нейрокомпьютерная техника: Теория и практика, 1992 – 184 с.
4. Интернет-ресурс «Вікіпедія» (www.wiki.com).
5. Брилок Д.В., Старовойтов В.В. Распознавание человека по изображению лица нейросетевыми методами. – Минск, 2002. – 54 с.

УДК 004.738.5

І.С. Гарбуз

Науковий керівник – Коваленко О.В., канд. техн. наук, ст. викладач
 Кіровоградський національний технічний університет

Розробка програмного забезпечення системи автоматизації збору заявок торгових агентів з використанням смартфонів

Бізнес стає усе більш складним і вимагає при ухваленні рішення урахування великої кількості різноманітної інформації [1-2]. Торговельний агент уже не може утримати в голові всі особливості бізнес-процесів при роботі із все зростаючою кількістю покупців, кожний з яких тепер вимагає індивідуального підходу.

Через це агентові доводиться возити із собою величезна кількість паперів з різноманітною інформацією, що дозволяє йому виступати перед покупцем у ролі експерта у своїй області, підтримувати імідж професіонала, що допомагає діставати максимальний прибуток своїм клієнтам.

У багато численних статтях теоретики від маркетингу переконливо показують, що тільки орієнтація на споживача може служити ефективним інструментом для збільшення прибутків компанії. І практика доводить, що підприємства, які роблять ставку на безпосередню роботу із клієнтом, домагаються явних конкурентних переваг перед фірмами, що ігнорують такий підхід.

Однак, реалізація клієнт - орієнтованого підходу в бізнесі досить складне й ресурсомістке завдання, тому без автоматизації цього процесу неможливо отримати необхідний ефект.

Однак, організація роботи торговельних представників досить складне й трудомістке завдання. Виникають складності організації й підтримки ефективної роботи команди торговельних представників. Чим жорсткіше конкуренція, тим більше інформації потрібно агентові для прийняття правильних рішень і виконання своїх обов'язків. А, отже, тим більше ймовірність помилок, що ведуть до конкретних фінансових втрат і тем вище вимоги торговельних компаній до рівня представників.

Мета й завдання дослідження. Ціль роботи складається в розробці програмного забезпечення, яке призначено для автоматизації збору заявок торгових агентів з використанням смартфонів.

Об'єктом дослідження є процес автоматизації збору заявок торгових агентів з використанням смартфонів.

Предметом дослідження є методи й алгоритми автоматизації збору заявок.

Методи дослідження. Для рішення поставлених задач у роботі використовувалася теорія клієнт-серверної взаємодії протоколу TCP/IP, алгоритми обробки та зберігання даних на мобільній платформі[3], алгоритми синхронізації та обміну даними.

Наукова новизна отриманих результатів. У процесі рішення завдань, обумовлених цілями дослідження, отримані наступні результати:

– Вперше розроблено вітчизняний продукт системи автоматизації збору заявок торгових агентів з використанням смартфонів на основі мобільної операційної системи Android 4.1;

– Розроблено клієнт-серверну методику взаємодії серверного ПЗ з клієнтським ПЗ на основі SQL запитів та алгоритмів автоматизації.

– Запропоновано вдосконалені методи стиску даних торговельного агента.

Практична цінність отриманих результатів полягає в тому, що використовуючи смартфон, торговельні агенти можуть здійснювати двухсторонній мобільний обмін даними, тобто одержувати й відправляти інформацію в центральну облікову систему, не відвідуючи офіс, з використанням бездротової технології передачі даних GPRS або 3G.

Систему можуть використовувати: торгові агенти, експедитори підприємств-виробників, приватні підприємці; працівники фірм, що мають власні магазини або торговельні точки, що дозволяє автоматизувати торговельну діяльність представників підприємства.

Достовірність наукових результатів підтверджена теоретичними викладеннями, даними комп'ютерного моделювання, коректними дослідженнями параметрів на функціонуючій обчислювальній мережі, а також відповідністю отриманих результатів окремим результатам, наведеним у науковій літературі.

Список літератури

1. Компьютерные системы передачи данных. 6-е издание, Вильям Столлингс; 928 стр., 2002.
2. Цифровая связь. Теоретические основы и практическое применение, 2-е издание, Бернард Скляр; 1104 стр. 2007.
3. Java 2. Библиотека профессионала, том 2. Тонкости программирования, 8-е издание, Кей С. Хорстманн, Гари Корнелл; 992 стр.; 2012.

УДК 81'33:004.652

Д.І. Кислий

Науковий керівник – Кеберле Н.Г., канд. техн. наук, доцент
 Запорізький національний університет

Онтологічне моделювання для навчання студентів – філологів в системі понять лінгвістики

Онтології широко використовуються для узгодженого розуміння термінів складної предметної області між групами людей [1]. Онтологічний інжиніринг розвиває основні положення інженерії знань – науки про моделі і методи добування, структуризації та формалізації знань.

Онтології дозволяють представити поняття в такому вигляді, що вони стають придатними для машинної обробки. На формальному рівні онтологія [2] – система, що складається з наборів понять і тверджень про ці поняття, на основі яких можна будувати класи, об'єкти, відношення, функції і теорії. Практично всі моделі онтології містять певні концепти (поняття, класи), властивості концептів (атрибути, ролі), відносини між концептами (залежності, функції) та додаткові обмеження, які визначаються аксіомами.

Онтологічні системи будуються на основі наступних принципів: формалізації, тобто опису об'єктивних елементів дійсності в єдиних, акуратно визначених термінах; використання обмеженої кількості базових термінів (сутностей), на основі яких конструюються всі інші поняття; принципу повноти і логічної несуперечності.

Серед областей використання онтологій особливо виділяється область навчання за допомогою онтологій. Побудована онтологія слугує не тільки довідником залежності між концептами предметної області для експертів, але й засобом ознайомлення з предметною областю. Наявність засобів пошуку й візуалізації концептів та їх ієрархії (редактори онтологій Protégé, TopBraid Composer, та браузері онтологій, наприклад, KSMSA) дозволяють використовувати інноваційне навчання для складних предметних областей, наприклад, побудова фрагмента онтології з подальшим (напівавтоматичним) порівнянням з еталонним фрагментом як засіб перевірки знань.

В якості ілюстрації застосування онтологічного моделювання для навчання була обрана предметна область «Лінгвістика». Необхідно зазначити, що наразі існують загальновідомі ресурси, присвячені цій предметній області, серед яких – енциклопедія Wikipedia має окремий портал для предметної області «Лінгвістика»¹, та власну систему категорій, цікавих для тих, хто вивчає лінгвістику. Однак, перелік категорій не є повним, не відображає спектра питань та розділів, є людино-орієнтовним, тобто, відповідає найбільш частим запитам користувачів та вже створеним статтям у Wikipedia, а не структурі лінгвістики як науки.

Нами було проведено власний онтологічний інжиніринг предметної області «Лінгвістика», з’ясовано основні її концепти, побудовані онтології окремих підрозділів лінгвістики, та зв’язки між цими онтологіями. В роботі використовувалися підручники з різних розділів лінгвістики. Для подання онтологій використовувався редактор онтологій Protege 4.1, та формальні мови RDF, RDFS, OWL.

Основними типами зв’язку між концептами виявилися відношення ієрархії `rdfs:subClassOf` та еквівалентності `owl:equivalentClass` (див. рис. 1, а). Для визначення концептів на загальноприйнятній мові використовуються коментарі, наприклад, `rdfs:comment`. Для визначення властивостей, притаманних предметній області, використовуються `owl:ObjectProperty` та `owl:DataProperty`. Обмеження на взаємодію концептів та властивостей подається у вигляді аксіом (див. рис. 1, б).

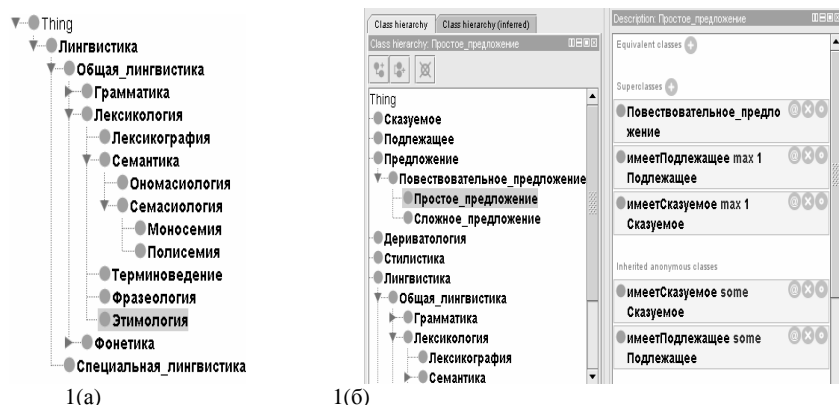


Рисунок 1 – (а) таксономія до рівня «Семантика»; (б) обмеження на взаємодію концептів: у концепта «Простое предложение» властивість «имеетПодлежащее» обмежена тільки екземплярами концепту «Подлежащее» та вимагає лише одного такого екземпляру.

¹ Портал:Лингвистика. <http://ru.wikipedia.org/wiki/Портал:Лингвистика>

Таким чином, головними факторами, що підкреслюють значущість даної роботи є: системність – онтологія представляє цілісний погляд на предметну область; узгодженість – матеріал, представлений в єдиній формі, найбільш краще сприймається та відтворюється; наочність – побудова онтологічної моделі дозволить відтворити складні різноманітні логічні зв’язки між поняттями, визначеними провідними фахівцями з лінгвістики.

В рамках навчального процесу онтологічний підхід забезпечить можливість організації ефективного розподіленого доступу та автоматизованого пошуку до навчальних ресурсів шляхом створення єдиної бази знань, яка буде включати в себе компоненти багатьох навчальних дисциплін. Також використання онтологій для навчання лінгвістиці дозволить протягом всього терміну навчання розбирати та уніфікувати її фрагменти, цілісно та наочно, в зв’язку з іншими фрагментами.

Список літератури

1. Uschold M. Ontologies: Principles, Methods and applications /M. Uschold, M. Gruninger // Knowledge Engineering Review. — 1996. — Vol. 11, № 2. — P. 93-136.
2. Онтологии и тезаурусы : учеб. пособ. / В.Д. Соловьев, Б.В. Добров, В.В. Иванов и др. – Казань ; Москва, 2006. – 173 с.
3. Noy N. Ontology Development 101: A Guide to Creating Your First Ontology [Електронний ресурс] / N. Noy, D. L. McGuinness // Stanford Knowledge Systems Laboratory Technical Report KSL-01-05 and Stanford Medical Informatics Technical Report SMI-2001-0880. — 2001. // Режим доступу: http://protege.stanford.edu/publications/ontology_development/ontology101.html

УДК 004.738.5

О.С. Жак

Науковий керівник – Приходькіна А.І., ст. викладач
Кіровоградський національний технічний університет

Програмне забезпечення моніторингу використання Інтернет-трафіку у локальній мережі

Інформатизація нашого суспільства збільшується з кожним роком. Повсюдно в школах починають викладати інформатику, в інститутах реферати приймаються тільки в друкованому виді, на роботі від службовців усе частіше вимагають знання ПК, та й у побуті комп’ютер уже перестав бути просто дорогою іграшкою.

Стає гостра потреба у системах моніторингу використання Інтернет-трафіку. Яка реалізована у вигляді проксі-сервера. Проксі-сервер це програма в комп’ютерних мережах, що дозволяє клієнтам виконувати непрямі (через посередництво проксі-сервера) запити до мережних сервісів. Спочатку клієнт з’єднується з проксі-сервером і запитує який-небудь ресурс (наприклад, e-mail), розташований на іншому сервері. Потім проксі-сервер або підключається до вказаного сервера і отримує ресурс у нього, або повертає ресурс з власного кешу (у випадках, якщо проксі має свій кеш).

У деяких випадках запит клієнта або відповідь сервера може бути змінена проксі-сервером в певних цілях. Також проксі-сервер дозволяє захищати клієнтський комп’ютер від деяких мережних атак і допомагає зберігати анонімність клієнта.

Таким чином, виходячи з вищеперерахованого, розробка програмного забезпечення моніторингу використання Інтернет-трафіку у локальній мережі є актуальною задачею. Основне призначення системи – моніторинг використання Інтернет-трафіку у локальній мережі, виконаного у вигляді проксі-сервера.

В.М. Кікоть

Науковий керівник – Сидоренко В.В., ст. викладач
Кіровоградський національний технічний університет

Оглядовий аналіз інформаційної системи конкурсного відбору кадрів

Робота будь-якої організації неминуче пов'язана з необхідністю комплектування штату. Задача підбору персоналу є ключовою, адже від якості відібраних кадрів залежить ефективність роботи організації, та використання ресурсів. Для будь-якої організації відбір і навчання працівників, які не підходять для виконання дорученої їм роботи є, як мінімум, нерациональним використанням часу та коштів. Отже, інформаційна система призначена для реалізації конкурсного відбору кадрів є досить актуальною задачею.

Основною задачею інформаційної системи конкурсного відбору кадрів є скорочення часу пошуку працівників за вакансіями підприємства, що відповідно призводить до спрощення роботи працівників відділу кадрів. Дана система дозволяє підприємству через Internet оголосити конкурс на наявні вакантні посади, збирати і зберігати відомості про учасників конкурсу у вигляді заповнюваних ними анкет.

Адміністратор системи має можливість вносити в базу даних нові вакансії, видаляти непотрібні вакансії, а також редагувати список надісланих анкет, відбираючи найбільш перспективні для діяльності підприємства.

Інформаційна система конкурсного відбору кадрів має клієнт-серверну архітектуру. Клієнтська частина представляє собою анкету, в яку користувач повинен ввести основну інформацію про себе: ПІБ, рівень освіти, спеціальність, досвід роботи за фахом, адресу. Приклад заповненої анкети зображений на рисунку 1.

Рисунок 1 – Заповнена анкета кандидата

Після заповнення користувачем анкети створюється запит SQL, який передається серверу. Запити передаються у вигляді рядків. При отриманні запиту основну роботу виконує серверна частина. Клієнту висилаються тільки дані, отримані в результаті отримання запиту. Це призводить до зниження навантаження, що дозволяє підвищити безпеку при роботі з даними. Перед посилкою запиту необхідна ресстрація на сервері.

Інформаційна система була розроблена на базі програмного забезпечення MySQL та мережі Internet, що дозволяє створити велику базу даних. Вибір таких проектних рішень також дає можливість легко організувати багатокористувацьку роботу, та робить систему зручною у використанні.

Список літератури

1. Асбари С. Корпоративные решения на базе Linux. / Асбари С. – К.: БХВ-Петербург, 2002. – 486 с.
2. Максим Кузнецов. MySQL 5. / Максим Кузнецов, Игорь Симдянов. – К.:БХВ-Петербург,2010.–392 с.

С.А. Ковальчук

Науковий керівник – Дреєв О.М., викладач
Кіровоградський національний технічний університет

Програмне забезпечення розпізнавання графічних образів за допомогою нейронної мережі Хеммінга

Розпізнавання образів – один з найважливіших розділів кібернетики. Він вивчає ідентифікацію предметів, сигналів, процесів і всього того, що характеризується певним набором ознак. Наприклад, всі людські особи або автомобільні номери, хоч і розрізняються між собою, мають схожі ознаки. Так, у першому випадку це один ніс, два ока, один рот і все інше, розташоване за певними правилами, на основі яких і виявляється особа. У той же час, кожна людина має свої унікальні риси, які використовуються для його впізнання.

Класичним прикладом можна назвати вміння більшості сучасних цифрових фотокамер знаходити обличчя в кадрі. Але одна справа відрізнити особу від табуретки й зовсім інша – виділити одну людину з безлічі інших. Незважаючи на те, що люди дуже легко розпізнають один одного по вигляду, реалізувати подібну систему – завдання не із простих. Треба було чимало часу й фінансових витрат, перш чим удалося створити діючі моделі. Споконвічно такі розробки велися за замовленням спецслужб. Тепер же навіть недорогі ноутбуки часто оснащуються спеціальним програмним забезпеченням, що дозволяє використовувати убудовані веб-камери для розпізнавання вигляду власника (правда, потрібно відзначити, що якість роботи подібних простих рішень не можна назвати занадто високим). Основне достоїнство систем оптичного розпізнавання полягає в тому, що інші засоби доступу, начебто магнітних карток, можуть бути украдені, загублені або підроблені, у той час як особа людини завжди при ній й підробити її куди суцужніше. До того ж процес може відбуватися на великому видаленні. На сьогоднішній день системи розпізнавання образів використовуються повсюдно, у справі автоматизації, ресстрації, ідентифікації й забезпечення безпеки.

Отже, розробка програмного забезпечення розпізнавання графічних образів за допомогою нейронної мережі Хеммінга є актуальною задачею.

Список літератури

1. Дэвид А. Форсайт, Джин Понс. Компьютерное зрение. Современный подход = Computer Vision: A Modern Approach. – М.: «Вильямс», 2004. – С. 928.
2. В. П. Сочивко, “Распознавание образов при помощи вычислительных машин”, Итоги науки. Сер. Теор. вероятн. Мат. стат. Теор. кибернет. 1964, ВИНТИ, М., 1966, 55–99.
3. В.Н. Вапник, А.Я. Червоненкис. Теория распознавания образов М.: Наука, 1974. – 416 с.
4. Вишневский А., Кокорева О., Чекмарев А. Microsoft Windows Server 2003. Русская версия. – С.-Пб.: БХВ-Петербург, 2003 – 1120 с

УДК 681.3.068

О.Ю. Котенко

Науковий керівник – Сізова Н.Д., д-р фіз.-мат. наук, професор
Харківський національний університет будівництва та архітектури

Прогнозування основних показників фінансової діяльності підприємства «Гідроапаратура»

В умовах ринку в економічному аналізі провідне місце займають фінансові показники. Фінансовий стан – найважливіша характеристика економічної діяльності підприємства, що відображає конкурентоспроможність підприємства, його потенціал в діловому співробітництві, оцінює в якій мірі гарантовані економічні інтереси самого підприємства та його партнерів за фінансовими та іншими відносинами.

Без аналізу фінансового стану сьогодні стає неможливим функціонування будь-якого суб'єкта економічної діяльності, включаючи й тих, що з певних причин не переслідують мету максимізації прибутків [1-3].

В даній роботі розглядаються питання фінансового стану конкретного підприємства АТ «Гідроапаратура» з урахуванням складу і структури експлуатаційних витрат і прогнозування його показників на майбутні періоди.

Для цього розглянуто структуру експлуатаційних витрат по АТ «Гідроапаратура» за досліджуваній період, вивчалася методологія фінансового стану підприємства, розглядалася його динаміка за 2006-2010 роки, проведено аналіз фінансової стійкості підприємства, аналіз ліквідності балансу, аналіз фінансових коефіцієнтів, аналіз рентабельності та ділової активності, вироблення рекомендацій щодо вдосконалення комерційної діяльності підприємства.

Прогнозування фінансового стану підприємства АТ «Гідроапаратура» виконувалося з використанням трендових моделей, це дозволило зробити відповідні висновки і рекомендації.

З використанням програмного середовища EXCEL апроксимація даних по фінансових показниках за декілька попередніх років дозволили обрати апроксимуючі функції (лінії тренда), одержати відповідне рівняння, використати вбудовані функції EXCEL, що дозволило на майбутні періоди одержати числові характеристики відносно фінансових показників.

Прогноз виявив наступне: об'єми реалізації продукції на протязі зазначеного періоду зазнали значних коливань: стрімке зростання показників валового прибутку у 2007 році в порівнянні з 2006 змінили тенденції стрімкого зниження, що, в першу

чергу, було спричинене несприятливими тенденціями на ринку машинобудування у зв'язку із світовою фінансовою кризою [4].

Підприємство АТ "Гідроапаратура" має недостатню фінансову стійкість. Про це свідчить ряд показників. Зокрема, коефіцієнт абсолютної ліквідності вказує на те, що підприємство в змозі негайно погасити лише 9% поточної заборгованості при нормативі 20-80%. Коефіцієнту миттєвої ліквідності також має низьке значення, вдвічі менше нормативного. Лише значення коефіцієнту поточної ліквідності знаходиться в межах норми, навіть перевищує її.

Станом на 2007 рік показники фінансової діяльності підприємства були досить високими, проте у зв'язку зі світовою економічною кризою вони значно погіршились у 2008-2009 роках. Зокрема зменшується рентабельність капіталу та продукції через зменшення чистого прибутку підприємства та попит на його продукцію. Щодо показників ділової активності підприємства, то вони також мають негативну тенденцію, швидкість оборотності капіталу зменшилась у декілька разів.

Для прогнозування фінансового стану підприємства АТ «Гідроапаратура» було використано також апарат нечіткої логіки [5].

Побудована нечітка модель показала достатньо високу точність, що обумовлює її успішне застосування в практиці фінансового стану підприємств і використовувати її для визначення адекватності, достовірності і порівняння результатів, одержаних різними підходами.

Список літератури

1. Азаренкова Г.М., Журавель Т.М., Михайленко Р.М. Фінанси підприємств: Навч. посіб. для самостійного вивчення дисципліни. – К.: Знання-Прес, 2009. – 299 с.
2. Фінанси підприємств: Підручник / А.М. Поддєрьогін, М.Д. Білик, Л.Д. Буряк та ін.; Кер. кол. авт. і наук. ред. проф. А.М. Поддєрьогін. – 5-те вид., перероб. та допов. – К.: КНЕУ, 2005. – 546 с.
3. Іванілов О.С. Економіка підприємства: Підручник. – К.: Центр учбової літератури, 2009. – 728 с.
4. Котенко О.Ю. Економічний аналіз фінансового стану підприємства. – Сборник трудов XIV Международной научно-практической конференции аспирантов и студентов «Проблемы развития финансовой системы Украины в условиях глобализации», 21-23 марта 2012, г. Симферополь/ Центр глобализации. – Симферополь: Таврич. нац. унив. имени В.И. Вернадского, 2012.– С.98-99.
5. Котенко О.Ю. Оцінка фінансового стану підприємства на основі нечіткої моделі // Збірник тез доповідей Всеукр. студ. науково-практичного семінару «Сучасні інформаційні технології та програмне забезпечення комп'ютерних систем». – Кіровоград: Вид-во «КОД», 2012. – С. 55 – 57.

УДК 004.89:629.33

О.В. Кравчук

Науковий керівник – Бабчук С.М., канд. техн. наук, доцент
Івано-Франківський національний технічний університет нафти і газу

Автономна комп'ютерна система керування автомобілем

За останнє десятиліття сфера використання комп'ютерних систем значно розширилась. Вказаний процес викликаний появою нової елементної бази, яка дозволила створювати високошвидкісні, компактні та відносно дешеві комп'ютерні системи. Це в свою чергу сприяє зближенню даних систем з технікою зв'язку та об'єктами керування [1].

В даний час в автомобілебудуванні комп'ютерні технології набувають все більшого поширення. Сьогодні автомобільна промисловість розробляє системи, що дозволяють машинам спілкуватися, самостійно планувати маршрут і не завдавати шкоди екології. Передача даних між автомобілями, як правило, направлена на забезпечення руху автомобілів на дорогах. Іншою метою таких розробок є розширення інформації яка надається водію про ситуацію на дорозі, незалежно від відстані й видимості.

Провідні автомобільні компанії світу активно ведуть роботу над створенням "безпілотного авомобіля", який обладнаний системою автоматичного управління та може пересуватися без участі людини. В якості автономної системи, він здатен сканувати навколишнє середовище та орієнтуватись в ньому. Людина може обрати місце призначення, але не є обов'язковим механічне керування транспортом. Такі автомобілі обладнуються відеокамерами, лазерними далекомірами, системою GPS-навігації, оптичними та звуковими давачами. Прогресивні комп'ютерні системи управління за результатами аналізу отриманої інформації повинні забезпечити рух автомобіля за вказаним маршрутом.

В даний час такі роботи ведуться з використанням трьох технологій: GPS, бездротових мереж та комп'ютерних систем для обробки інформації.

Для того щоб забезпечити подальший розвиток та конкурентоздатність автомобілів українських виробників необхідне проведення розробки технологій "безпілотного авомобіля" і в Україні [2].

Метою роботи є створення моделі автономної комп'ютерної системи керування автомобілем на базі мікропроцесору ATmega8 та фотодатчиків.

В результаті проведених досліджень, розроблена автономна комп'ютерна система керування мініавтомобілем на основі мікроконтролера Atmel Atmega8-16PU та фотодатчиків. Обладнаний такою системою автомобіль здатен рухатись, притримуючись дорожньої розмітки та оминати перешкоди.

Для написання програмного забезпечення та подальшого його компілювання до мікропроцесору Atmega-8 використано програмний пакет CodeVision AVR. Це інтегроване середовище розробки було створено спеціально для мікроконтролерів сімейства Atmel AVR. Також великою перевагою даного інтегрованого середовища розробки є використання Сі-подібної мови програмування для AVR та можливість асемблерних вставок [3].

Створено алгоритм реагування системи на сигнали давачів.

Після проведення багатьох експериментів зі змінами положення фотодавачів, різною напругою було сформовано остаточний варіант програмного забезпечення.

Для тестування розробленої системи за основу ходової частини робота використано машинку на радіокеруванні після внесення в неї певних структурних змін.

Тестування проводилося на спеціальній трасі білого кольору з нанесеною чорним розміткою. Також, з метою перевірки роботи фронтальних давачів на шляху руху моделі "безпілотного авомобіля" були розкладені предмети різного розміру і форми.

В цілому результати тестування програмного забезпечення та безпосереднього тестування мінімоделі "безпілотного авомобіля" дають підстави сказати, що створена комп'ютерна система здатна автономно керувати системою керування і двигуном, тримати автомобіль в межах дороги, а також у випадку виникнення перешкод під час руху обминати їх.

Для ще кращої роботи системи можна використати лазерні далекоміри замість фотодавачів. В такому випадку значно розшириться "поле видимості" комп'ютерної системи.

Розроблена в цій роботі комп'ютерна система може стати базою для реалізації проекту "безпілотного авомобіля". Вдосконаливши цю систему та об'єднавши її з існуючими методами позиціонування в автомобілі можна створити високоінтелектуальну автономну комп'ютерну систему керування автомобілем.

Список літератури

1. Бабчук С. М. Контроль вмісту кадмію в посуді комп'ютерною системою [Текст] / С. М. Бабчук, Л. Р. Бабчук // Восточно-європейский журнал передовых технологий. – 2012. – № 6/2(60). – С. 14-17.
2. Кривоконь О.Г. Стратегія та перспективи розвитку легкового автомобілебудування в Україні [Текст] / О.Г. Кривоконь, А.І. Бондаренко // Автомобільний транспорт. – 2012. – № 30. – С. 23-28.
3. Лебедев М.Б. CodeVisionAVR. Пособие для начинающих: монографія [Текст]. – М.: Додэка-XXI, 2008. – 592 с.

УДК 004.738.5

В.В. Лісшин

Науковий керівник – Кудінович Д.С., викладач
Олександрійський політехнічний коледж

Програмна реалізація системи розпізнавання зображень

Завдання виділення образу людини у природній або штучній обстановці завжди перебувала в ряду найбільш пріоритетних завдань для дослідників, що працюють в області систем машинного зору та штучного інтелекту. Тим не менш, безліч досліджень, що проводяться в провідних наукових центрах всього світу протягом кількох десятиліть, до недавніх часів так і не привело до створення реально працюючих систем комп'ютерного зору, здатних виявляти людину в будь-яких умовах [1].

Серйозною проблемою, що стоїть перед системами комп'ютерного зору, є велика мінливість візуальних образів, що пов'язана зі змінами освітленості, масштабів, ракурсів спостереження. Однак найбільш складним завданням комп'ютерного зору є проблема усунення неоднозначності, що виникає при проектуванні тривимірних об'єктів реального світу на плоскі зображення. Колір і яскравість окремих пікселів на зображенні також залежить від великої кількості важко прогнозованих факторів.

Повне використання інформації, що міститься в зображенні, вимагає аналізу кожного пікселя на приналежність його об'єкту або фону з урахуванням можливої зміни характеру об'єктів. Такий аналіз обґрунтовано потребує високих витрат ресурсів та продуктивності комп'ютера.

На сьогоднішній день основні алгоритми вирішення задачі розпізнавання образів входять до складу програмних шаблонів OpenCV – це бібліотека комп'ютерного зору з відкритим вихідним кодом, розроблена компанією Intel на мовах програмування C++, Java. Включає в себе велику кількість алгоритмів комп'ютерного розпізнавання зображень в режимі реального часу. Бібліотека OpenCV може бути використана безкоштовно, як в освітніх цілях, так і в комерційних проектах [2].

Програмна реалізація розпізнавання зображень на основі OpenCV включає в себе алгоритми: розпізнавання об'єктів та тексту, фільтрацію початкового зображення, виявлення подібності форми об'єктів, стеження за переміщенням об'єктів, розпізнавання рухів, жестів і т.д [3].

На першому етапі алгоритми бібліотеки виділяють із загального зображення обличчя, потім відбувається нормалізація зображення. До нормалізації зображення відносяться наступні дії:

- зміна роздільної здатності зображення до 100 * 100 пікселів;
- перетворення кольорів до 256 відтінків сірого;
- зміна сумарної яскравості зображення до деякого середнього значення.

Теорія тематики розпізнавання облич досить складна, адже базується на поєднанні великих об’ємів математичних понять, формул, залежностей, серед яких найбільш кращим по співвідношенню показників ефективності розпізнавання в залежності від швидкості роботи є алгоритм Віюлі-Джонса [3]. Реалізація алгоритму має вкрай низьку ймовірність помилкового виявлення особи. Алгоритм добре працює та розпізнає риси обличчя під невеликим кутом, приблизно до 30 градусів. Але, в стандартній реалізації алгоритму, при куті нахилу більше 30 градусів відсоток розпізнавання різко падає, що не дозволяє детектувати повернуте обличчя людини під довільним кутом.

Тому саме дозволена зміна стандартної реалізації алгоритмів відкритої бібліотеки OpenCV здатні вирішити проблему програмної модифікації коду, для підвищення ефективності процесів розпізнавання та ідентифікації об’єктів.

Список літератури

1. А. С. Потапов «Распознавание образов и машинное восприятие» / А. С. Потапов – «Политехника», 2007. – 552 с.
2. Bradski G.R. «Learning OpenCV» / Bradski G.R., Kaehler A. - O'Reilly Media, Inc, 2008. - 556 с.
3. Laganière R. «OpenCV 2 Computer Vision Application Programming Cookbook» / Laganière R. - Packt Publishing, 2011. – 298 с.

УДК 004.738.5

М.Ю. Кудря

Науковий керівник – Сидоренко В.В., ст. викладач
Кіровоградський національний технічний університет

Розробка інформаційної системи розкладу кафедри ВНЗ

Будь-яка кафедра навчального ВУЗу має свій розклад занять. Підбір предметів та викладачів, які будуть вести предмети зазвичай займає багато часу та зусиль. Завданням даної роботи було побудувати автоматизовану інформаційну систему кафедри "Програмного забезпечення" Кіровоградського національного технічного університету. Втім, дану систему, при необхідності можна використовувати не тільки для однієї кафедри, але і для всього ВУЗу в цілому, також може бути застосована в будь-якому іншому навчальному закладі.

Дана інформаційна система дозволяє легко складати розклад предметів для груп на будь-який актуальний період для існуючих груп на кафедрі або ВУЗі. Головною відмінною особливістю при цьому є те що інтерфейс користувача доступний з будь-якого місця, де існує Інтернет, що дозволить студентам, викладачам та іншим зацікавленим особам дізнатися актуальний розклад в будь-який час. При необхідності також можна налаштувати експорт даних у форматі електронних

календарів для синхронізації з локальними календарями користувачів в мобільних і інших електронних пристроях. Приклад заповненої таблиці розкладу зображена на рисунку 1.

Добавить элемент расписания

Группы	Понедельник 2013-02-11	Вторник 2013-02-12	Среда 2013-02-13	Четверг 2013-02-14	Пятница 2013-02-15	Суббота 2013-02-16	Воскресенье 2013-02-17
КИ-10-1		1 пара Численные методы Гермак Ауд. 501 Практика Ред					
		2 пара АФП Левашко Елена Львова Ауд. 500 Лекция Ред	3 пара Программирование Мелешко Елизавета Владислава Ауд. 500 Лекция Ред	1 пара Численные методы Петренко Владимир Ильич Ауд. 500 Лекция Ред	1 пара Системное программирование Коваленко Александр Владимирович Ауд. 500 Лекция Ред		
	3 пара СУБД Сидоренко Валентина Владимировна Ауд. 500 Лекция Ред			2 пара СУБД Сидоренко Валентина Владимировна Ауд. 505 Практика Ред	2 пара АФП Мелешко Елизавета Владислава Ауд. 508 Практика Ред		

Рисунок 1 – Кінцевий результат таблиці

Програмний код написаний для інтерпретатора PHP з використанням об’єктно-орієнтованого фреймворку CodeIgniter з принципами об’єктно-орієнтованої моделі "Модель-подання-контролер", що представляє собою схему використання декількох шаблонів проектування, за допомогою яких модель даних програми, користувальницький інтерфейс і взаємодія з користувачем розділені на три окремі компоненти так, що модифікація одного з компонентів надає мінімальний вплив на інші. Дана схема проектування часто використовується для побудови архітектурного каркаса, коли переходять від теорії до реалізації в конкретній предметній області.

Саме моделлю є SQL-запити в БД MySQL. При необхідності розширення даного програмного продукту, написання додаткових модулів (наприклад, можливість авторизації користувачів, експорт даних в інші формати (SQL, PDF) та інше), зв’язок з іншими БД, зміна дизайну інтерфейсу і т.д. програмний код легко і швидко може бути модифікований якраз за рахунок подання "Модель-подання-контролер".

Результатом даної роботи є те, що за допомогою подібного інструментарію можна розробляти серйозні БД на мільйони записів в таблицях. Даний конкретний приклад легко адаптується під системи вокзалів та інших організацій де необхідно використовувати тижневий розклад, також при необхідності пишуться додаткові модулі, які допомагають розширити функціональність системи.

Список літератури

1. Кузнецов С. Д. Основы баз данных. - 2-ге вид. - М.: Интернет-университет информационных технологий; БИНОМ. Лаборатория знаний, 2007. - 484 с.
2. В. Васвані. MySQL: використання та адміністрування = MySQL Database Usage & Administration. - М.: «Пітер», 2011. – 368 с.
3. Кузнецов Максим, Сімдянов Ігор. MySQL на прикладах. - СПб.: «БХВ-Петербург», 2008. – С. 952.

УДК 330.46:519.86

Н.Ю. Могилевська, А.С. ГусєвНауковий керівник – Кучма Ю.В., канд. техн. наук, доцент
Східноукраїнський національний університет ім. В. Даля

Розробка геоінформаційної системи міста для торгових підприємств

Сучасні ГІС пропонують все більше і більше можливостей для відображення просторової інформації. Абревіатура ГІС розшифровується буквально як географічна інформаційна система або геоінформаційна система. ГІС це набір апаратних і програмних інструментів, що використовуються для введення, зберігання, маніпулювання, аналізу і відображення просторової інформації [1].

Управління бізнесу передбачає збір і обробку величезної кількості даних про продаж, клієнтів, запасах, демографічних відомостях, списків розсилки і багато іншого. Основна частина цих даних пов'язана з географічним місцем розташування, і тому їх можна відображати на електронних картах і працювати з ними у діалоговому режимі. У сьогоденному економічному кліматі компанії стурбовані тим, як скоротити витрати і збільшити продажі для того, щоб підвищити прибутковість. ГІС містить дані та інструменти, які допоможуть бізнесу у вирішенні цих завдань. Функції просторового аналізу дозволяють, наприклад, за допомогою ГІС вирішити, де слід відкрити новий магазин, аптеку або відділення банку, ґрунтуючись на нових демографічних даних та планах розвитку міста. Ви можете відразу отримати потрібну інформацію про об'єкт, клацнувши по ньому на електронній карті. У будь-який момент Ви можете оновити інформацію, прив'язану до карти, і внесені зміни автоматично проступлять на карті. І для користування ГІС не потрібно спеціальної підготовки. Комерційні фірми намагаються використовувати ГІС для вибору місця розташування нових супермаркетів, для управління поставками і т.і. [2].

Цілком очевидно, що в сучасних умовах ГІС є доладним способом зберігати інформацію про території, які знаходяться під юрисдикцією організації.

Нами було покладено початок створенню в місті Луганську ГІС для бізнесу. Першим завданням, яке Ми взялися вирішувати це створення «ГІС-Схід Луганська». Ця частина міста була обрана нами в якості полігону. Мета проекту: апробація ГІС-технології на конкретній ділянці території міста.

Геоінформаційна система орієнтована на аналіз просторової інформації та моделювання різних бізнес-рішень на основі статистичних даних.

Першим кроком до створення повноцінної геоінформаційної системи є розробка інтерактивних карт. Викладаємо основні етапи її розв'язання.

1. Збір картографічних даних. На даному етапі відбувається збір картографічної інформації. В якості вихідних даних можуть бути використані різні карти, супутникові знімки, плани розглянутої місцевості.

2. Обробка та аналіз картографічних даних. На цьому етапі вся картографічна інформація приводиться до вигляду, придатного для подальшого використання, проводиться розпізнавання будівель, доріг та інших важливих об'єктів, з подальшою їх класифікацією, на основі реальних даних (рисунк 1).

3. Створення інформаційної бази даних. На цьому етапі проектується і створюється база даних, яка буде використовуватися для обробки запитів і виведення статистичної інформації. База даних буде містити всі раніше розпізнані об'єкти.

4. Побудова алгоритмів обробки даних. На цьому етапі створюються різні алгоритми для обробки даних: отримання різного виду статистичної інформації, знаходження оптимального маршруту, обробка користувача запитів і т. і.



Рисунок 1 – Приклад роботи алгоритму

5. Підготовка системи для кінцевого користувача. На даному етапі відбувається переоформлення карти для додавання їй більш естетичного вигляду. На карту наносяться різні умовні позначення, створюється додаткова анімація, можливе створення тривимірного представлення.

На даний момент розроблено програмне забезпечення, яке дозволяє обробляти адміністративні карти міста та розпізнавати на них будинки. Використана технологія java-апплетів, що дозволяє запускати її як веб-додаток безпосередньо в браузері, незалежно від операційної системи, на якій вона буде використовуватися. Розроблений алгоритм розпізнавання на мапі побудований на основі алгоритму заливки, який використовує принцип чотирьохзв'язності пікселів.

Також проектується основна база даних по будівлях міста. Вона буде містити інформацію про житлові будинки та торгові об'єкти міста Луганська.

На поточному етапі перед нами стоїть завдання розробки алгоритмів обробки картографічних і статистичних даних. Планується реалізація ряду математичних методів і алгоритмів для оцінки економічно значущих показників. Так вже розроблені моделі для прогнозу обороту торговельного підприємства [3,4].

Узагальнюючи все вищесказане про ГІС в бізнесі, можна виділити наступне: ГІС допомагає приймати більш обґрунтовані рішення. Однак геоінформаційна система - це не інструмент для видачі рішень, а засіб, що допомагає прискорити і підвищити ефективність процедури прийняття рішень. Вона забезпечує відповіді на запити і функції аналізу просторових даних, подання результатів аналізу в наочному і зручному для сприйняття вигляді.

Список літератури

1. Турпалов В.Е. Геоинформационные системы в экономике: Учебно-методическое пособие. – Нижний Новгород: НФ ГУ-ВШЭ, 2007. – 118 с.
2. Stas Sushkov, Stas's Geomarketing Blog. <http://stasgeomarketing.wordpress.com/>.
3. Кучма І.В., Кучма Ю.В. До питання про вибір місця розташування торгового підприємства // Вісник Східноукраїнського нац. універс. імені Володимира Даля. – 2009. - №12(142). – С. 187-191.
4. Кучма І.В., Кучма Ю.В. Прогноз обороту торгового підприємства на основі моделей виявлених переваг // Матеріали І-ї Всеукраїнської науково-практичної конференції студентів, аспірантів та молодих вчених «Актуальні питання теорії та практики менеджменту» 17-19 березня 2010 року. Присвячується 90-річчю СХУ ім.В.Даля –Луганськ: ТОВ «Віртуальна реальність», 2010. – С.352-353.

В.О. Наумова, О.М. РалоНауковий керівник – Стервєсдов М. Г., канд. техн. наук, доцент
Харківський національний університет ім. В.Н. Каразіна

Розробка програмного забезпечення для медичних апаратно-комп'ютерних систем (МАКС)

Важливим різновидом спеціалізованих медичних інформаційних систем є медичні апаратно-комп'ютерні системи (МАКС). В даний час одним з напрямків інформатизації медицини є комп'ютеризація медичної апаратури. Використання в медичній практиці комп'ютера в поєднанні з вимірювальною та управляючою технікою дозволило створити нові ефективні засоби для забезпечення автоматизованого збору інформації про стан хворого, її обробки в реальному масштабі часу та управління станом пацієнта. Цей процес привів до створення медичних апаратно-комп'ютерних систем, які підняли на якісно новий рівень інструментальні методи досліджень та інтенсивну терапію.

Типовими представниками МАКС є медичні системи моніторингу за станом хворих; системи комп'ютерного аналізу даних томографії, ультразвукової діагностики, ЕЕГ, ЕКГ, радіографії; системи автоматизованого аналізу даних мікробіологічних та вірусологічних досліджень, аналізу клітин та тканин людини.

Системи такого класу дозволяють підвищити якість профілактичної та лікувально-діагностичної роботи, особливо в умовах масового обслуговування, коли бракує кваліфікованих спеціалістів та часу.

Для підтримки таких МАКС потрібне спеціалізоване програмне забезпечення, можливості якого загострені під швидкісну та одночасну обробку великої кількості біометричних даних. При розробці ПЗ такого рівня головною проблемою постає оптимізація роботи з пам'яттю, що може якісно відобразитися на роботі як математичних методах обробки медико-біологічної інформації, так і на швидкості алгоритмів програми. Такий підхід формує розуміння необхідності створення багатомодульного програмного забезпечення, що реалізовуватиме різні рівні функціонування. Таких модулів можна виділити велику кількість залежно від масштабу системи взагалі, але базовими є:

1. модуль підготовки дослідження
2. модуль проведення дослідження
3. модуль перегляду та редагування результатів дослідження
4. модуль аналізу
5. модуль візуалізації та підготовки звітності
6. модуль роботи з архівом результатів

ПЗ систем з різними правами доступу користувача припускає наявність бази даних користувачів, а також інформацію для їх ідентифікування та притягнення до відповідальності. Необхідність різноманітності рівней доступу до інформації обумовлено ще й важливістю збереження інформації не тільки самих користувачів, а й об'єктів та суб'єктів досліджень, тобто пацієнтів та їх особистих даних, бо неправомірне використання останніх може призвести до суттєвих юридичних наслідків.

Крім цього, окремо від алгоритмічного апарату при розробці ПЗ слід приділяти особливу увагу способам та засобам синхронізації отриманих даних з обчислювальною системою. В залежності від концептуальної реалізації системи в загалом синхронізація може значним чином відрізнятися одна від одної.

Зваживши усі вище перелічені властивості розробки програмного забезпечення для МАКС можна зробити висновок, що розробка таких програмних продуктів залежить від реалізації системи в загалом та включає велику кількість питань стосовно

захисту інформації, отриманої в процесі проведення досліджень та збереження конфіденційності цих даних протягом кожного етапу взаємодії з ними.

Список літератури

1. МАКС - Теоретичні відомості [Електронний ресурс] // Режим доступу: http://intranet.tdmu.edu.ua/data/kafedra/internal/informatika/classes_stud.htm
2. Ж. Бланшет, М. Саммерфилд Qt 4: Программирование GUI на C++. — М.: «КУДИЦ-ПРЕСС», 2007. — С. 648.

М.В. КузьменкоНауковий керівник – Сидоренко В.В., ст. викладач
Кіровоградський національний технічний університет

Порівняльна характеристика багатопроцесорних архітектур

Часто буває, що відносно великі накладні витрати, пов'язані з обробкою переривань, незрідка роблять доцільним включення в систему додаткових процесорів. Одним з аргументів на користь створення багатопроцесорних обчислювальних систем є підвищення надійності обчислювальної системи за допомогою багатократного резервування. Якщо один з процесорів багатопроцесорної системи відмовляє, система може перерозподілити завантаження між тими, що залишилися. Для комп'ютерів перших поколінь підвищення надійності в такий спосіб часто виявлялося доцільним, особливо в додатках, що вимагали цілодобової доступності.

Іншим аргументом на користь включення в систему додаткових процесорів є той факт, що алгоритми, які використовують для вирішення багатьох прикладних завдань, незрідка піддаються “розпаралелюванню”: розділенню роботи між декількома більш менш незалежно працюючими процесорами. Залежно від алгоритму рівень досяжного паралелізму може сильно розрізнятися. Відношення продуктивності системи до кількості процесорів і продуктивності однопроцесорної машини називають “коефіцієнтом масштабування”. Для різних завдань, алгоритмів, ОС і апаратної архітектури цей коефіцієнт різний, але завжди менше одиниці і завжди зменшується в міру збільшення кількості процесорів.

Порядок доступу до пам'яті в SPARC. Сучасні процесори надають можливість управляти порядком доступу команд до пам'яті. Наприклад, біля мікропроцесорів SPARCvQ визначено три режими роботи з пам'яттю, які перемикаються бітми в статусному регістрі процесора: вільний доступ до пам'яті (RMO), частково впорядкований доступ (PSO) і повністю впорядкований доступ (TSO).

Кожен наступний режим підвищує упевненість програміста в тому, що його програма прочитає з пам'яті саме те, що туди записав інший процесор, але одночасно наводить і до падіння продуктивності. Найбільший програш забезпечує реалізація режиму TSO, коли ми просто вимикаємо і динамічне переупорядкування команд, і кешування даних.

Іншим вузьким місцем багатопроцесорних систем є системна шина. Системи шинної архітектури прості в проектуванні і реалізації, до них легко підключати нові пристрої, тому така архітектура набула широкого поширення. Проте, особливо в багатопроцесорних системах, шина часто є одним з основних обмежувачів

продуктивності. Підвищення пропускної спроможності шини частенько можливо, але наводить до підвищення загальної вартості системи.

Втім, при великій кількості вузлів проблеми виникають і біля систем з настільки високошвидкісною шиною, як FinePape. Крім того, у міру зростання фізичних розмірів системи, стає необхідно брати до уваги фізичну швидкість передачі сигналів – як сигналів самої магістралі, так і запитів до арбітра шини і його відповідей. Тому шинна топологія з'єднань при багатьох десятках і сотнях вузлів виявляється недопустима, і застосовуються складніші топології.

Системи NUMA-Q. Багатопроцесорні сервери IBM NUMA-Q складаються з окремих процесорних модулів, кожен з яких має власну оперативну пам'ять і чотири процесори x86. Модулі сполучені високошвидкісними каналами IQ-Link з центральним комутатором. Заміна загальної шини на зіркоподібну топологію з центральним комутатором дозволяє вирішити проблеми арбітражу доступу до шини, зокрема, усунути затримки при запиті до арбітра шини і чеканні його відповіді пристрою, який подає запит.

При більшому числі модулів застосовується гіперкубічна топологія, коли кожен вузол зазвичай також містить декілька процесорів і власну оперативну пам'ять.

Завдяки множинності доріг, маршрутизатори можуть вибирати для кожного повідомлення найменш завантажену в даний момент дорогу або обходити вузли, що відмовили.

Масивно-паралельні системи Cray/SGI Origin. Вузли суперкомп'ютерів сімейства Cray/SGI Origin сполучені в гіперкуб каналами з пропускною спроможністю 1 Гбайт/с. Адаптери з'єднань забезпечують не просто обмін даними, а прозорий доступ процесорів кожного з вузлів до оперативної пам'яті інших вузлів і забезпечення когерентності процесорних кешів.

Відмінність в швидкості доступу до локальної пам'яті процесорного модуля і інших модулів є проблемою і при невдалому розподілі завантаження між модулями приведе до значного зниження продуктивності системи. Відомо два основних рішення цієї проблеми:

1. COMA (Cache Only Memory Architecture) – архітектура пам'яті, при якій робота з нею відбувається як з кешем. Система переносить сторінки пам'яті, з якою даний процесорний модуль працює частіше за інших, в його локальну пам'ять.

2. CC-NUMA (Cache-Coherent Non-Uniform Memory Access). У цій архітектурі адаптери між модульних з'єднань забезпечуються власною кеш-пам'ятю, яка використовується при зверненні до ОЗУ інших модулів. Основна діяльність центрального комутатора і каналів зв'язку полягає в підтримці когерентності цих кешів.

Зрозуміло, що ці архітектури не вирішують в корені проблеми неоднорідності доступу: для обох можливо побудувати таку послідовність міжпроцесорних взаємодій, яка “проміє” всі кеші і перезавантажить міжмодульні зв'язки, а в разі COMA приведе до постійного перекачування сторінок пам'яті між модулями. Те ж саме справедливо і для симетричних багатопроцесорних систем із загальною шиною.

Можна лише підкреслити, що масштабованість багатопроцесорних систем визначається в першу чергу природою завдання і рівнем паралелізму, закладеним у використаний для вирішення цього завдання алгоритм. Різні типи багатопроцесорних систем і різні топології міжпроцесорних з'єднань придатні і оптимальні для різних завдань.

Список літератури

1. Жаркова А.И. Многопроцессорные системы. – М.: 2004 – 173 с.
2. Богданов А.В. Архитектура и топологии многопроцессорных вычислительных систем. Уч. изд. Интернет-Университет Информационных Технологий: 2005. – 176 стр.

УДК 004.4

О.В. Лактіонов

Науковий керівник – Мелешко Є.В., канд. техн. наук, доцент
Кіровоградський національний технічний університет

Розробка програмного забезпечення системи комп'ютерного зору для створення інтерактивних користувальницьких інтерфейсів

У цей час завдання оцифрування й зберігання великих обсягів візуальної інформації мають закінчені технічні рішення, що цілком задовольняють вимогам користувачів, у той час як в області розробки методів рішення завдань пошуку й семантичної класифікації зображень ситуація виявляється прямо протилежною. Відзначимо, що до останнього часу найбільше часто використовувався пошук візуальної інформації, що опирається на індексування текстових описів, асоційованих із зображенням (наприклад, пошук картинок на Яндекс і Google). При очевидній необхідності організації доступу до колекції зображень за допомогою пошуку за текстовою інформацією, асоційованою із зображеннями, даний підхід представляється недостатнім. Дійсно, існуюча неоднозначність при встановленні відповідності між візуальним змістом і текстовим описом знижує показники точності й повноти пошуку, а цілому ряді випадків виявляється досить важким або взагалі неможливим скласти словесний опис зображення (наприклад, абстрактні картини).

На початку 80-х років для подолання недоліків пошукових систем на основі тексту були початі розробки методів пошуку зображень за змістом (у закордонній літературі для позначення даного підходу використовується абревіатура CBIR – Content-based image retrieval). В CBIR-системах зображення індексуються по їхньому візуальному вмісті (за кольором, текстурою, формою й т.д.).

Аналіз сучасних тенденцій розвитку систем пошуку зображень показує, що найбільш популярним виявляється підхід, заснований на використанні тих або інших алгоритмів аналізу зображень. Наприклад, одним з останніх нововведень Google стало введення нових типів зображень, які Google автоматично класифікує. На сучасний момент дана пошукова система розпізнає наступні типи зображень: портрети, фотографії, гравюри, олівцеві рисунки й схеми, «кліпарт». У квітні 2009 року запущений пошук схожих зображень Google Similar Images: на першому етапі використовується традиційний спосіб пошуку по текстовому запиті, а потім як запит використовується одне зі знайдених зображень і здійснюється пошук по візуальній подібності. У пошуковій системі Яндекс наприкінці 2008 року став можливий пошук портретів, а раніше був запущений пошук картинок по переважному кольору, пошук фотографій і механізм виявлення дублікатів.

У цей час відомі демо-версії систем пошуку зображень за змістом (MFIRS, CIRES, Tiltomo, INRIA, Retrievr і ін.). Проведений аналіз якості пошуку в перерахованих системах показує, що якість пошуку в них істотно нижче в порівнянні із системами пошуку зображень по текстових анотаціях. Так, з 20-ти перших знайдених зображень запиту відповідає не більше 16% зображень (при пошуку по текстових анотаціях у системі Яндекс аналогічний показник рівняється 51%).

Слід зазначити, що завдання пошуку зображень за змістом по своїй постановці формально близька до завдання розпізнавання образів, однак по своїй суті ці завдання не є ідентичними. У завданні розпізнавання образів основною метою є віднесення вхідного зображення до одного із заздалегідь відомих класів, у той час як у завданні пошуку зображень за змістом споконвічно явної вимоги до ідентифікації класу вхідного зображення не ставиться, але потрібно знайти зображення, що володіють візуальною подібністю із запитом.

Аналіз базових принципів, використовуваних у сучасних CBIR-системах, показує, що в більшості з розглянутих систем пошуку зображень за змістом пошук ведеться за ознаками, що витягається із усього зображення (глобальні ознаки). Крім того, при пошуку зображень користувач найчастіше цікавиться цілком конкретним об'єктом, що є присутнім на зображенні, і, відповідно, результатом пошуку повинні бути зображення, що містять шуканий об'єкт.

У той же час у науковій літературі описані результати дослідження механізмів сприйняття людиною зображень, згідно яким увага людини в процесі аналізу зображень концентрується не на всьому зображенні, а на деяких цілком конкретних областях зображення. При цьому вибір області (або декількох областей), що привертає увагу людини, більшою мірою обумовлений властивостями даної області, але в меншому ступені високорівневими когнітивними процесами (модель висхідної уваги).

Мета й завдання дослідження. Ціль роботи складається в розробці програмного забезпечення, яке призначено для системи комп'ютерного зору для створення інтерактивних користувальницьких інтерфейсів.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

1. Аналіз сучасного стану проблеми пошуку зображень за змістом й огляд інформаційних ознак зображень, використовуваних в CBIR-системах.
2. Аналіз критеріїв якості сегментації й виділення критеріїв, які доцільно використовувати для оцінки якості алгоритмів сегментації зображень.
3. Аналіз відомих моделей висхідної візуальної уваги й дослідження ступеня суб'єктивності уваги людини.
4. Розробка алгоритму автоматичного знаходження об'єкту на зображенні, що привертає увагу людини.
5. Розробка методів пошуку зображень із використанням інформації про об'єкт і проведення експериментальної перевірки їхньої працездатності.
6. Розробка на основі запропонованих методів пошуку зображень прототипу CBIR-системи.

Об'єктом дослідження є процес створення системи комп'ютерного зору.

Предметом дослідження є системи комп'ютерного зору для створення інтерактивних користувальницьких інтерфейсів.

Список літератури

1. Фершильд М.Д. Модели цветового восприятия, Рочестерский технологический институт, Манселловская научная лаборатория по цвету, 2006.
2. Pass G., Zabih R. Histogram refinement for content-based image retrieval // IEEE Workshop on Applications of Computer Vision, 1996, pp. 96-102.
3. Ma W.Y., Zhang H. Benchmarking of image feature for content-based retrieval // In IEEE 32nd Asilomar Conference on Signals, Systems, Computers, 1998, v. 1, pp. 253-257.
4. Deng Y., Manjunath B. S., Kenney Ch., Moore M. S., Shin H. An efficient color representation for image retrieval // IEEE Transactions on image processing, 2001, v. 10, no. 1, pp. 140-147.
5. Стандарт MPEG-7 [Электронный ресурс]: Дескриптор доминантного цвета. – Режим доступа: http://book.itep.ru/2/25/mpeg_7.htm, 27.03.2009.

УДК 004.63

С.В. Паїцький

Науковий керівник – Помазан Л.В., канд. техн. наук, доцент
Кіровоградський національний технічний університет

Програмне забезпечення файлового менеджера смартфонів на базі мобільної ОС Android

В даний час ринок мобільних пристроїв зростає в геометричній прогресії. Швидко розвиваються мобільні операційні системи. Крім цього такі ОС як Windows (версія 8) повністю інтегруються в мобільні платформи.

Android це операційна система і платформа для мобільних телефонів та планшетних комп'ютерів, створена компанією Google на базі ядра Linux. Підтримується альянсом Open Handset Alliance (ОНА).

У сумі станом на 2013 продано вже понад 300 млн Android-пристроїв, випущених 42 виробниками, їх розповсюджували у мережах 215 операторів зв'язку.

Загальне число моделей пристроїв на базі платформи Android досягло 510. Всього було продано більш ніж 400 млн Android-пристроїв. Каталог Android Market подолав позначку в 200 тисяч програм.

Всього з Android Market встановлено близько 4.5 мільярдів копій програм. За даними Google у 2013 році, активовано 700 мільйонів "Андроїдів". Найпоширенішою задачею у ОС Android є виконувати найчастіші операції з файлами.

Проаналізувавши ринок програмного забезпечення під операційну систему Android було встановлено що існує вкрай мало реалізацій спеціалізованих файлових менеджерів. Таким чином, виходячи з вищеперахованого, розробка програмного забезпечення файлового менеджера смартфонів на базі мобільної ОС Android, є актуальною задачею.

Призначення системи – виконувати найчастіші операції з файлами у смартфоні: створення, відкриття/програвання/запуск/перегляд, редагування, переміщення, перейменування, копіювання, вилучення, зміну атрибутів та властивостей, пошук файлів та призначення прав. Область застосування – ОС Android.

УДК 004.4

Д.А. Обженський

Науковий керівник – Минайленко Р.М., канд. техн. наук, ст. викладач
Кіровоградський національний технічний університет

Програмне забезпечення системи моніторингу стану жорсткого диску з використанням технології SMART

Сучасний жорсткий диск – унікальний компонент комп'ютера. Він унікальний тим, що зберігає в собі службову інформацію, вивчаючи яку, можна оцінити «здоров'я» диска. Ця інформація містить у собі історію зміни безлічі параметрів, що відслідковуються вінчестером у процесі функціонування. Більше жоден компонент

системного блоку не надає власникові статистику своєї роботи. Укупі з тим, що HDD є одним із самих ненадійних компонентів комп'ютера, така статистика може бути досить корисною й допомогти його власникові уникнути нервування й втрати грошей і часу.

Інформація про стан диска доступна завдяки комплексу технологій, названих загальним ім'ям S.M.A.R.T. (Self-Monitoring, Analysis and Reporting Technology, тобто технологія самомоніторингу, аналізу й звіту). Цей комплекс досить великий, але розглянемо ті його аспекти, які дозволяють подивитися на атрибути S.M.A.R.T., і зрозуміти, що діється з диском.

Відзначу, що нижчезазначене відноситься до дисків з інтерфейсами SATA і PATA. У дисків SAS, SCSI і інших серверних дисків теж є S.M.A.R.T., але його подання сильно відрізняється від SATA/PATA. Та й моніторить серверні диски звичайно не людина, а RAID-контролер, тому в даній дипломній роботі ми їх розглядати не будемо.

Таким чином розробка програмного забезпечення системи моніторингу стану жорсткого диску з використанням технології SMART є актуальною задачею.

Список літератури

1. Фигурнов В. Э. IBM PC для пользователя. М.: ИНФРА-М. 2002.
2. Архитектура ПК, комплектующие, мультимедиа. – Рудометов Е., Рудометов В. – Питер, 2000.
3. Аладьев В. З. Компьютерная хрестоматия. Справочное руководство. – М.: Росс. энциклопедия, 2003.
4. Ушаков Н. Н. Технология элементов вычислительных машин. – М.: Высшая школа, 2001.

УДК 004.91

О.М. Панасюк

Науковий керівник – Приходькіна А.І., ст. викладач
Кіровоградський національний технічний університет

Програмне забезпечення системи автоматизованого керування електронним діловодством підприємства

Автоматизований електронне діловодство це людино-машинна система, у якій за допомогою технічних засобів забезпечується збір, накопичення, обробка інформації, формулювання оптимальної стратегії керування певними компонентами й видача результатів людині або групі людей, що приймають рішення по керуванню.

Завдання накопичення, обробки й розповсюдження (обміну) інформації стояла перед людством на всіх етапах його розвитку. Протягом довгого часу основними інструментами для її рішення були мозок, мова й слух людини.

Перша кардинальна зміна відбулася із приходом писемності, а потім винаходом друкарства. Оскільки в епоху друкарства основним носієм інформації став папір, то технологію накопичення й поширення інформації природно називати “паперовою інформатикою”. Положення в корені змінилося з появою електронних обчислювальних машин.

Одним з перших прикладів подібного системного застосування ЕОМ у світовій практиці були так звані адміністративні системи обробки даних: автоматизація банківських операцій, бухгалтерського обліку, резервування й оформлення квитків і т.п.

Вирішальне значення для ефективності систем подібного роду має та обставина, що вони опираються на автоматизовані бази, що документують. Це означає, що в пам'яті ЕОМ постійно зберігається інформація, потрібна для рішення тих завдань, на які розрахована система. Вона й становить уміст інформаційної бази відповідної системи.

Зберігання інформації в пам'яті ЕОМ надає цій інформації принципово нову якість динамічності, тобто здатності до швидкої перебудови й безпосередньому її використанню в розв'язуванні на ЕОМ завданнях. Обладнання автоматичного друку, якими постачені сучасні ЕОМ, дозволяють якщо буде потреба швидко представити будь-яку вибірку із цієї інформації.

Таким чином, виходячи з вищеперерахованого, розробка програмного забезпечення системи автоматизованого керування електронним діловодством підприємства, є актуальною задачею.

Призначення системи – автоматизоване керування електронним діловодством підприємства. З захищеним обміном даних між керівником підприємства та підлеглими по захищеному каналу передачі даних. Область застосування – автоматизація керування електронним діловодством підприємств та установ. Необхідне керівникам, директорам та ін.

УДК 004.738.5

О.В. Пахомов

Науковий керівник – Сидоренко В.В., ст. викладач
Кіровоградський національний технічний університет

Автоматизація роботи бібліотечної системи

Не зважаючи на те, що на сьогоднішній день глобальна мережа інтернет стала основним джерелом інформації, важливу роль продовжують відігравати і традиційні бібліотеки. Це зумовлено тим, що далеко не всі документи переведено в цифровий вигляд, а доступ до деякої літератури, що наявна в мережі, може бути обмеженим.

Бібліотека – культурно-просвітницька і науково-допоміжна організація, яка організовує використання суспільством творів друку. Бібліотеки систематично займаються збором, зберіганням, пропагандою і видачею читачам творів друку, а також інформаційно-бібліографічною роботою.

Автоматизація бібліотеки може рухатись в двох напрямках: інформаційна підтримка традиційних видів діяльності бібліотеки, таких як комплектування фондів, ведення каталогу, пошук, видача літератури читачам; створення повнотекстової електронної бібліотеки шляхом переведення в цифровий вигляд всього бібліотечного фонду. Кожен із напрямків значно спрощує процес експлуатації реальної бібліотеки. Перший напрямок автоматизації дає можливість прискорити виконання деяких стандартних операцій, що виконуються бібліотеками, зробити їх виконання значно зручнішим. Другий напрямок фактично перетворює реальну бібліотеку на віртуальну, оскільки у читачів з'являється можливість відвідувати бібліотеку сидячи в себе вдома за комп'ютером. Але цей напрямок потребує значних ресурсів: часу, для переведення книг в електронний вигляд, апаратних ресурсів, для збереження оцифрованої інформації та інших.

Отже, питання автоматизації роботи бібліотечної системи є актуальним.

За допомогою такої інформаційної системи можна вирішувати наступні задачі:

- реєструвати нових абонентів бібліотеки;
 - вести облік вже зареєстрованих абонентів;
 - формувати звітну інформацію про відвідування бібліотеки та про книговидачу;
 - здійснювати контроль за вчасним поверненням книжок та інших друкованих видань в бібліотеку;
 - вести облік всіх наявних в бібліотеці книжок та друкованих видань;
 - здійснювати збір звітної інформації бібліотек-філій, що підпорядковуються центральній бібліотеці (відвідування, книговидача).
- Система включає в себе наступні об’єкти:
- книга - об’єкт, що має такі характеристики: інвентарний номер, назву, авторів, рік видання, назву видавництва, кількість сторінок, код бібліотечно-бібліографічної класифікації (ББК).
 - книжковий фонд – сукупність всіх книжок зареєстрованих у певній бібліотеці;
 - фонд періодичних видань – аналог книжкового фонду для періодичних видань (газет та журналів). На кожне періодичне видання заводиться реєстраційна картка, яка містить наступну інформацію: індекс періодичного видання, дату виходу, назву та номер видання;
 - абонент характеризується номером, що присвоюється йому під час реєстрації і однозначно ідентифікує його, ПІБ, датою народження, адресою і контактним номером телефону, датою реєстрації. Також фіксуються паспортні дані (серія та номер паспорту), освіта та професія абонента.
 - бібліотека-філія – це звичайна, зазвичай невелика, бібліотека, яка розташована на території певної територіально-адміністративної одиниці (наприклад району) і підпорядковується центральній бібліотеці даного району.

Зміст вихідної інформації буде залежати від того, що саме цікавить користувача. Наприклад, за допомогою запитів користувач може відшукати в книжковому фонді потрібну йому книжку або отримати звіт, що міститиме дані про книговидачу та кількість зареєстрованих абонентів певної бібліотеки-філії.

Є декілька шляхів удосконалення даної системи. Так, наприклад, можна реалізувати дану систему як клієнт-серверну, об’єднавши в мережу центральну бібліотеку, яка виступатиме сервером, та бібліотеки-філії, які будуть клієнтами. Це значна оптимізація, оскільки бібліотеки-філії отримають доступ до інформації, яка може знадобитися їм в процесі їх функціонування. Також, такий підхід значною мірою удосконалив механізм подачі звітів бібліотеками-філіями. Але для такої оптимізації потрібно забезпечити доступ до мережі інтернет кожної з бібліотек-філій, а оскільки зазвичай вони знаходяться в невеликих селищах, які не мають доступу до мережі інтернет, то реалізація такого удосконалення системи в повній мірі неможлива.

Список літератури

1. Жаркова Л.С. Методика організації роботи бібліотеки в сфері соціально-культурної діяльності: научно-практичне посібник /Л.С. Жаркова – М.: Литера, 2009. – 111 с.
2. Олефир С.В. Організація роботи бібліотеки освітнього закладу в умовах модернізації освіти: навчальне посібник / С.В. Олефир. – М.: Литера, 2010. – 198 с.

УДК 004.4

І.М. Пшеничний

Науковий керівник – Дреєва Г.М., асистент
Кіровоградський національний технічний університет

Програмне забезпечення інтелектуального дому за технологією Z-Wave

Інтелектуальний будинок – це інтелектуальна система управління, що поєднує в єдиний комплекс все устаткування, що вирішує різні завдання в сфері забезпечення безпеки, життєзабезпечення, розваг і зв’язку. Будь-яка система інтелектуального будинку складається з датчиків, через які надходить інформація, і виконавчих пристроїв.

Одне з головних переваг інтелектуальних будинків – це комфорт, що вони забезпечують своїм мешканцям. Управління освітленням будинку й прибудинкової інфраструктури дозволяє створювати різні варіанти світлових сцен, будь-які комбінації, залежно від часу доби й настрою, одним натисканням на кнопку. Система клімат-контроль дає можливість у той саме час у різних кімнатах відтворити умови різних кліматичних зон. Для цього всього лише потрібно задати необхідну температуру на сенсорній керуючій панелі. Вся побутова техніка, наявна в будинку, може перетворитися в турботливих помічників – кава в кавоварці буде готова до моменту пробудження, мікрохвильова піч ввімкнеться по таймері, а система мультимедіа дозволить господарці не відриватися від перегляду фільму, що дивиться вся родина у вітальні, коли вона відправиться на кухню для готування обіду, або сама зменшить гучність на музичному центрі, коли задзвонить телефон. Хазяїн будинку зможе управляти їм навіть віддалено, давши команду системі за телефоном. У результаті, наприклад, у вогкий день до його повернення з роботи буде готові гаряча

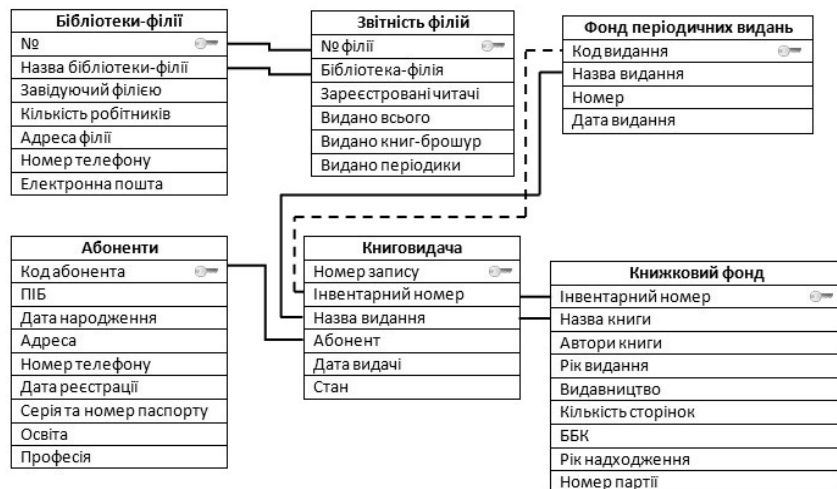


Рисунок 1 – Інформаційно-логічна модель системи

Вхідною інформацією для бази даних системи буде інформація про абонентів, що реєструються в бібліотеці, про всі наявні в бібліотеці книги та періодичні видання, про бібліотеки-філії та про реєстрацію видачі певної книги чи видання абоненту. Також, звітність бібліотек-філій.

ванна й закип'ячений чайник, а приглушене світло й присмна музика зроблять повернення затишним і радісним, навіть якщо будинок порожній.

Таким чином, виходячи з вищеперахованого, розробка програмного забезпечення інтелектуального дому за технологією Z-Wave, є актуальною задачею

Список літератури

1. Кашкаров П. Электронные схемы для "умного дома". Серия: В помощь радиолюбителю – М.: НТ ПРЕСС, 2007.
2. Роберт К. Элспенитер, Тоби Дж. Велт. Умный Дом строим сами. М.: КУДИЦ-Образ, 2005. – 384 с.
3. Гололобов В.Н. "Умный дом" своими руками. – М.: NT Press Москва, 2007. – 417 с.
4. Архипов В. Системы для «интеллектуального» здания. – "СтройМаркет". – № 45. – 1999.

УДК 004.738.2

А.В. Тагієв

Науковий керівник – Коваленко О.В., канд. техн. наук, ст. викладач
Кіровоградський національний технічний університет

Розробка програмного забезпечення системи стеження за автомобільним транспортом з використанням міток геокодування на базі ОС Android

В даний час у всьому світі намічається значне зростання інтересу до систем, що забезпечує автоматизацію контролю за переміщенням автотранспорту [1-3]. Будучи на початковому етапі прерогативою спецслужб і невеликого числа комерційних організацій, що займаються транспортуванням особливо цінних вантажів, в даний час, завдяки вдосконаленню технологій і зниження цін, ці системи стають доступні й економічно ефективні для використання в самих різних галузях, включаючи комерційні вантажоперевезення, громадський транспорт і цілі пересічного споживача.

Останнім часом широкого поширення у всьому світі набули системи і комплекси технічних засобів визначення місцеположення рухомих об'єктів. Ці системи використовуються на морі, суші і в повітрі для стеження за об'єктами, визначення їх місця розташування, коректування маршруту і т.д. Існує гостра проблема актуальна для державних правоохоронних органів, приватних структур безпеки і диспетчерських служб підприємств різних форм власності – визначення місця розташування автомашин, інших транспортних засобів, цінних вантажів зловмисниками, тобто вторгнення в особисте життя, спробу незаконного отримання інформації конфіденційного характеру або державної таємниці. Завдання щодо запобігання подібній ситуації доводиться вирішувати в процесі управління і контролю переміщення рухомих об'єктів, забезпечення безпеки автомашин, супроводження транспортних засобів, цінних вантажів і т.д.

Таким чином, виходячи з вищеперахованого, розробка програмного забезпечення системи стеження за автомобільним транспортом, є актуальною задачею.

Метою роботи є розробка програмного забезпечення системи стеження за автомобільним транспортом з використанням міток геокодування на базі ОС Android.

Об'єктом дослідження є процес стеження за автомобільним транспортом з використанням міток геокодування на базі ОС Android.

Предметом дослідження є методи й алгоритми забезпечення системи стеження за автомобільним транспортом.

Для рішення поставлених задач у роботі використовувалася теорія системи глобального позиціонування, обробки геокоординатних даних, формування шляху слідування автотранспорту.

Наукова новизна отриманих результатів:

- На основі існуючих моделей пошуку автомобільного транспорту, запропоновано методику системи стеження за автомобільним транспортом з використанням Інтернет протоколів прикладного рівня POP3 та SMTP;
- Запропоновано використовувати нові підходи обробки міток геокодування;
- Вперше розроблено вітчизняний продукт системи стеження за автомобільним транспортом на мобільній операційній платформі Android версії 4.2.

Список літератури

1. Андрианов В.И. Автомобильные охранные системы – Санкт-Петербург: ВHV Арлит, 2000. –272 с.
2. С.А.Золотарева, И.В. Шишигина Справочное пособие: Охранные устройства для автомобилей. Под общей редакцией О.В.Колесниченко. – Санкт-Петербург, ВHV Арлит. – 1997.
3. В.И.Андрианов, В.А.Бородин, А.В.Соколов. Справочное пособие: Устройства для защиты объектов и информации. Под общей редакцией С.А.Золотарева. – Санкт-Петербург, ВHV Арлит. – 1996.

УДК 004.324

Е.В. Хоткевич

Научный руководитель – Силкин М.Ю., канд. физ.-мат. наук, доцент
Харьковский национальный университет им. В.Н. Каразина

Расширение возможностей параллельного порта ПК

Параллельный порт принято использовать как интерфейс для подключения принтера к ПК. Данный порт может, однако, использоваться и для других приложений, связанных с сопряжением ПК с внешними устройствами [1]. В работе исследованы средства и предложены решения, позволяющие использовать параллельный порт для автоматизации экспериментов и управления производственными процессами.

Интерфейс параллельного порта обеспечивает 12 линий вывода данных и 4 линии ввода данных в ПК. Линии вывода сгруппированы в два регистра: регистр данных (Data) и регистр управления (Control). Ввод данных идет через третий регистр, называемый регистром состояния (State).

Разработанная в ходе исследований плата (Рис. 1) предназначена для изучения и наглядной демонстрации обмена информацией через параллельный порт ПК. Плата предусматривает подключение всевозможных пользовательских устройств. В частности, возможно дальнейшее расширение ее функциональных возможностей за счет увеличения числа управляемых 8-битовых регистров чтения-записи. Плата снабжена светодиодами для индикации логического состояния каждого входа и выхода.

Дальнейшее наращивание возможностей экспериментальной платы может быть достигнуто за счет использования микросхем средней степени интеграции, таких,

наприклад, як мікросхема програмуемого периферійного інтерфейса 82C55A (Рис. 2). Мікросхема має 4 зовнішні двонаправлених 8-бітових реєстри з трьома станами. Один із реєстрів (D0-D7) використовується як вхідний і підключається к шині даних. Три інших реєстри (PA, PB, PC) використовуються для вводу/виводу даних плати розширення. Вони можуть незалежно бути налаштовані як на ввід інформації (читання), так і на вивід (запис). Налаштування режимів реєстрів PA, PB, PC проводиться шляхом запису через реєстр D0-D7 управляючого слова во внутрішній реєстр управління PD мікросхеми.

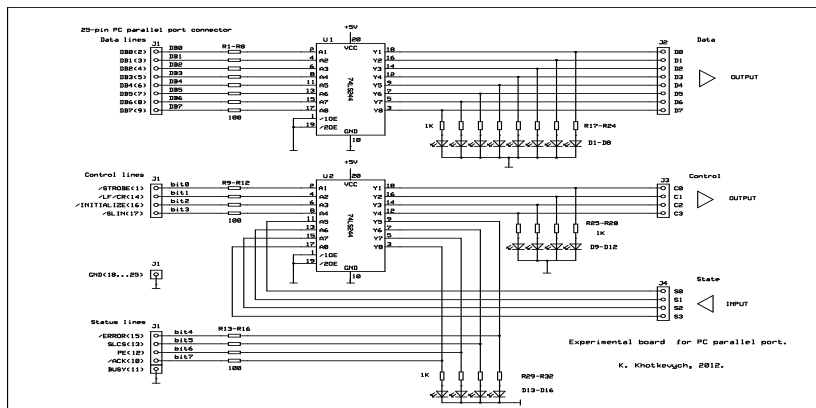


Рисунок 1 – Експериментальна плата для підключення к ПК, забезпечуюча ввід-вивід інформації

Алгоритм запису: Требуємі дані спочатку записуються реєстр Data, а стан ліній A0, A1 – в реєстр Control. Далі лінія /WR (реєстр Control) встановлюється в 0, буфери U3 відкриваються, і дані записуються в вибраний реєстр 82C55A. Нарешті повертаємо сигнал /WR в 1.

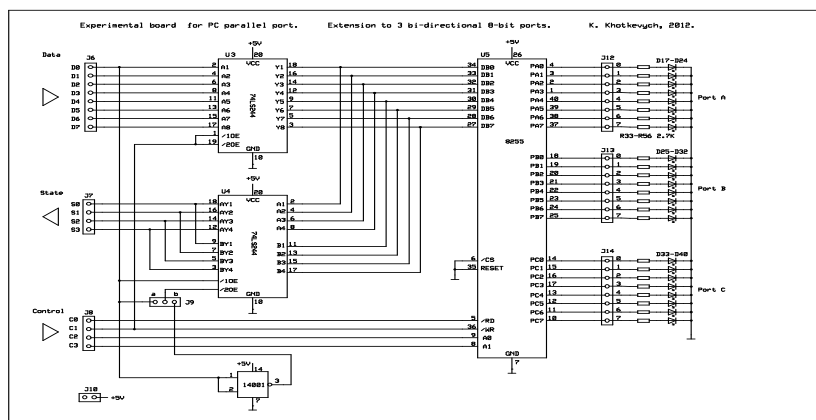


Рисунок 2 – Експериментальна плата, забезпечуюча додавання 3-х двонаправлених 8-бітових реєстрів обміну інформацією

Алгоритм читання: Читання даних із вибраного при допомозі A0, A1 реєстра 82C55A відбувається в два етапи через реєстр State. Спочатку нульовий біт реєстра Data встановлюється в 0, і при подачі 0 на /RD, на 4 біта State поступають 4 молодших біта з шини даних. Вони читаються програмою із State. Після цього /RD повертаємо в 1. Далі нульовий біт Data встановлюється в 1, і при подачі 0 на /RD на State виводяться для читання 4 старших біта з шини даних. Після читання із State /RD знову встановлюємо в 1. Таким чином, всі 8 біт з шини даних прочтені через 4-бітний реєстр State (за 2 операції читання).

При розробці програм управління обміном через паралельний порт використовуються підпрограми Output і Input бібліотеки inport32.dll, що дозволяють безпосередньо звертатися к реєстрам паралельного порта. Підпрограми обслуговують обмін з реєстрами 82C55A і наочно ілюструють принципи формування управляючих сигналів. В демонстраційних програмах застосовуються ActiveX керування фірми National Instruments, які зазвичай включені в склад Windows XP Professional. При їх відсутності знадобиться файл swui.ocx.

Таким чином, в рамках поточної роботи було досліджено обмін інформацією через паралельний порт ПК, створено і випробовано пристрій для розширення можливостей паралельного порта, що працює під управлінням оригінального програмного забезпечення, розробленого в межах даного проекту. Отримані електронні схеми і ПО можна, в першу чергу, розглядати як навчальний посібник, а також використовувати для управління виробничими процесами і автоматизації експериментів.

Список літератури

1. Ан П. Спряження ПК з зовнішніми пристроями: Пер. с англ. – М.: ДМК Пресс, 2001. – 320 с.

УДК 004.738.5

Р.В. Чернявський

Науковий керівник – Сидоренко В.В., ст. викладач
Кіровоградський національний технічний університет

Розробка системи автоматизації роботи цеху на прикладі ПрАТ «Гідросила»

З розвитком інформаційних технологій стає дедалі доцільніше їх використання в нашому житті. Зараз інформаційні технології впроваджуються на багатьох підприємствах, організаціях та різних органах влади. Розроблені концепції впровадження інформаційних технологій в наукові заклади, фабрики, тощо.

Основними конкурентними перевагами підприємств, що використовують інформаційні технології є:

- оперативність отримання інформації, особливо при міжнародних операціях;
- зниження невиробничих витрат (торгових витрат, витрат на рекламу, витрат, пов'язаних з сервісним обслуговуванням та інформаційною підтримкою споживачів);
- скорочення циклу виробництва та продажу, оскільки зникає потреба повторного підтвердження інформації і знижується вірогідність помилок при введенні інформації, або її передачі;

- значно знижуються затрати, пов'язані з обміном інформацією, за рахунку використання більш дешевих засобів телекомунікації;

- більша відкритість компаній для споживачів;

- можливість звертання користувача до великих масивів інформації у вигляді баз даних і до інформаційної продукції широкої номенклатури;

Автоматизована система виробничого призначення (автоматизована виробнича система) здійснює збирання інформації з об'єкта керування, передає, перетворює й обробляє її, формує керуючі команди та виконує їх на керованому об'єкті, тобто ті функції, які піддаються автоматизації. Людина визначає цілі та критерії керування й коригує їх, коли змінюються умови, зокрема, виконує функції нагляду за роботою автоматизованих пристроїв, а в разі потреби змінює програму їхньої роботи (завдання) і приймає загальні рішення щодо керування в змінених або складних ситуаціях.

Усвідомлення важливості розподілу обчислень в автоматизованих розрахунках виникло тоді, коли було помічено, що в багатьох прикладних програмах використовуються аналогічні обчислення, а індивідуальні фактори, які впроваджуються в прикладні програми для допомоги конкретному користувачу, вносять незначні відмінності. Крім того, мало місце значне дублювання дій і процедур під час розробки, реалізації та тестування цих обчислювальних функцій.

Із зростанням кількості прикладних програм для надання персоналізованої оперативної підтримки, а також із збільшенням кількості інформаційних систем зростав обсяг обчислювального дублювання, що стало значною мірою гальмівним чинником: для індивідуальної оперативної підтримки необхідно виконувати досить багато персоналізованих версій однієї й тієї самої прикладної програми, причому кожна версія підлягає багаторазовій модифікації упродовж періоду її експлуатації, з тим щоб вона відповідно реагувала на зміни в можливостях, знаннях, позиції і побажаннях користувача. Більше того, дубльована версія часто виявлялась менш ефективною, викликала взаємну несумісність програм і меншу продуктивність обчислень.

Виходом із такої ситуації стала концепція утворення єдиної централізовано керованої бази моделей.

У цьому напрямку було одержано ряд результатів:

1) більш високий рівень модульності, досягнутий завдяки стандартизації інтерфейсів, дозволив поліпшити можливості знаходження надмірностей;

2) системи управління базами даних були використані для контролю та управління інтерфейсами моделей;

3) за допомогою засобів системного аналізу і мов специфікацій були здійснені спроби описати обчислення таким способом, який був би прийнятним для широкого діапазону користувачів (від кінцевих користувачів до розробників системи);

4) деякі системні описи були автоматизовані та включені в програмне забезпечення за допомогою діалогу користувач—система, параметризованих алгоритмів та інтерфейсів типу меню.

Впровадження інформаційної системи відкриває нові можливості для ефективного вирішення основних задач також для автоматизації роботи цеху. Експлуатація системи дозволяє підприємству реалізувати програми ресурсозбереження шляхом зниження експлуатаційних витрат на утримання систем зв'язку, зниження енергоспоживання, уникнути пікових навантажень, збільшити продуктивність праці, поліпшити якість послуг, робіт що виконуються і підвищити кваліфікацію працівників підприємства, чи окремого цеху.

Усе це визначає актуальність застосування інформаційних технологій в умовах розвитку ринкових відносин, координації наукової і практичної діяльності в області сучасних інформаційних технологій.

Як свідчить світовий досвід, лідерство в конкурентній боротьбі здобуває сьогодні та фірма, яка оперативніше реагує на потреби клієнтів і надає послуги за прийнятною ціною і якістю. В умовах переходу до ринкових відносин інформаційний центр набуває першочергового значення, будучи невід'ємним елементом ефективної системи управління.

Раціональна методологія використання інформаційної технології дозволить досягти більшої гнучкості, підтримувати загальні стандарти, здійснити сумісність інформаційних локальних продуктів та знизити дублювання діяльності.

Таким чином, використання інформаційних технологій вказує на те, що підприємство, яке їх використовує у майбутньому буде перспективним та впевнено буде крокувати шляхом прогресу.

Список літератури

1. Горшкова Л.А., Горбунова М.В. Основы управления организацией: Практикум. М.: КНОРУС, 2006.
2. Золотогоров В.Г. Организация производства и управление предприятием: Учеб. пособие. М.: Интерпрессервис, 2005.
3. Новицкий Н.И. Организация производства на предприятиях: Учеб. пособие. М.: Финансы и статистика, 2004.
4. Поршнева А.Г.: Управление организацией: Учебник / Под ред. З.П. Румянцевой и Н.А. Саломатина. М.: ИНФРАМ, 2005.

УДК 681.2:004.31

О.Д. Чужикова-Проскурнина

Научный руководитель – Сапожников Н.Е., д-р техн. наук, профессор
Севастопольский национальный университет ядерной энергии и промышленности

Применение вероятностных устройств в измерительных системах

Принцип представления значения любого параметра сигнала вероятностью не нов [1]. С развитием цифровой вычислительной техники и методов имитационного моделирования стал широко использоваться метод статистических испытаний, основная идея которого - связь между вероятностными характеристиками случайных процессов и величинами, являющимися решениями задач математического анализа.

В общем виде суть стохастического или вероятностного преобразования [2] заключается в том, что любому значению преобразуемой величины можно привести в соответствие некоторую вероятность. В наиболее простом случае, значение преобразуемой величины либо всегда положительно, либо всегда отрицательно, а сам процесс преобразования выполняется в соответствии с правилом (1).

$$y_{ij} = \begin{cases} 1 & \text{при } x_i > R(t_{ij}) \\ 0 & \text{при } x_i \leq R(t_{ij}) \end{cases} \quad (1)$$

где x_i - i -е значение параметра преобразуемого сигнала $X(t)$;

$R(t_{ij})$ - j -е значение вспомогательного случайного сигнала $R(t)$, изменяющегося в интервале изменения $X(t)$;

$i = \overline{1, N}$ - число циклов преобразования сигнала $X(t)$;

$j = \overline{1, K}$ - количество статистических испытаний каждого значения x_i внутри временного интервала $\Delta t_i = t_{i+1} - t_i$;

y_{ij} - значение вероятностного отображения параметра сигнала x_i из ряда $Y_i(t) = \{y_{i1}; y_{i2}; \dots; y_{ij}; \dots; y_{iK}\}$.

Особый интерес представляет случай, когда вспомогательный случайный сигнал подчиняется равномерному закону распределения, тогда оценку математического ожидания можно вычислить по формуле (2).

$$x_i^* = \{M[Y_i(t)]\}^* = \frac{1}{K} \sum_{j=1}^K y_{ij}, \quad (2)$$

где K – количество статистических испытаний.

Таким образом, при однолинейном однополярном преобразовании параметра сигнала в вероятность, для получения исходного значения следует подсчитать количество единиц в вероятностном отображении и отнести его к количеству статистических испытаний (количеству членов вероятностного отображения).

Вероятностное представление данных является непозиционной системой исчисления. Именно эта особенность позволяет на порядки уменьшить аппаратный объем вероятностных устройств, т.к. важен не порядок следования единиц в записи, а их количество.

Выполнение вероятностного умножения [3] выполняется по формуле (3).

$$(x_1 \cdot x_2)^* = \frac{1}{K} \sum_{j=1}^K (y_{1j} \& y_{2j}), \quad (3)$$

где K – количество статистических испытаний при выполнении операции;

y_{1j} и y_{2j} – j -ые члены вероятностных отображений первого и второго операнда соответственно.

Выполнение вероятностного сложения [4] выполняется по формуле (4).

$$(x_1 + x_2)^* = \frac{1}{K} \sum_{j=1}^K (y_{1j} \vee y_{2j}), \quad (4)$$

Из формул (3) и (4) видно, что арифметические операции можно легко реализовать аппаратно. Операция вероятностного умножения реализуется на одном конъюнкторе, на входы которого одновременно подаются вероятностные отображения операндов. Операция вероятностного сложения может быть реализована на дизъюнкторе, однако второй операнд подается с задержкой относительно первого, чтобы получить сумму единиц, содержащихся в вероятностном отображении каждого из операндов. Если же операнды поступают последовательно, то операцию сложения можно выполнить на двоичном счетчике.

В качестве преимуществ вероятностной формы представления данных можно выделить следующее:

- уменьшение аппаратного объема устройств и, следовательно, их линейных размеров и потребляемого питания;
- уменьшение себестоимости устройств, за счет снижения аппаратных затрат;
- устойчивость при возникновении помех.

Однако существуют и недостатки, такие как:

- ограниченный диапазон измеряемых величин;
- работа только с положительными или только с отрицательными числами;
- зависимость точности вычислений, от выбранного диапазона и количества статистических испытаний.

Учитывая недостатки вероятностного представления данных, можно сделать вывод, что создание универсальных вероятностных устройств является сложной трудоемкой задачей, но оно идеально подходит для применения измерительных систем.

Диапазон измерения заранее ограниченный диапазоном сигналов с датчиков, что позволяет создать точные вероятностные устройства и использовать все преимущества такого представления данных.

Список литературы

1. Гладкий В.С. Вероятностные вычислительные модели. – М.: Наука, 1973. – с. 300.
2. Сапожников Н.Е. О вероятностном преобразовании информации // Приборостроение.- Вып.34, 1983. – с.31-38.
3. Сапожников Н.Е., Сапожникова А.В. Анализ и моделирование работы вероятностных умножителей // Вестник СевГТУ, Информатика, электроника, связь.- №10, 1998. – с.15-20.
4. Сапожников Н.Е. Сравнительная оценка методов суммирования вероятностно преобразованных сигналов // Вестник СевГТУ, Механика, энергетика, экология.- №6, 1997. – с.89-95.

УДК 004.7

М.С. Ярифа

Научный руководитель – Шматков С.И., д-р техн. наук
Харьковский национальный университет им. В.Н. Каразина

Разработка нейронной модели оценки состояний маршрутизатора

Современный этап развития человечества характеризуется революционными преобразованиями в области создания, обработки и передачи информации. Одним из важнейших ресурсов мира становится интеллект. Его эффективное использование – главная задача инфокоммуникационной отрасли мировой экономики. Темпы развития глобальных телекоммуникаций должны быть опережающими по отношению к темпам потребностей людей в целом. Таким образом, для обеспечения требуемого качества обслуживания необходимо не только иметь информацию о состоянии информационно-вычислительной сети, но и уметь его прогнозировать.

В данной работе проведен теоретический анализ модели состояний вычислительной сети на примере маршрутизатора, а так же практическая разработка нейронной модели оценки состояний маршрутизатора.

На сегодняшний день информация о состоянии сети представлена определенным набором параметров, текущее состояние сети определяется взаимным влиянием этих параметров между собой. В качестве примера были проанализированы 4 состояния маршрутизатора (не загружен, загружен, критическая загрузка, потери), которые зависят от таких параметров как загруженность процессора, памяти, используемой под таблицу маршрутизации, средней загруженности входного и выходного буферов. Для сбора статической информации о состоянии сети проведен натурный эксперимент на базе оборудования Cisco.

Проблема оценки состояний маршрутизатора в настоящее время изучена недостаточно. Единого подхода к градации состояний пока не существует.

Задача оценки состояний маршрутизатора имеет ряд особенностей, а именно:

- большое число параметров сети;

- сильная взаимосвязь между параметрами;
- большое число внешних факторов;
- высокая динамика.

Все эти факторы усложняют задачу оценки состояний маршрутизатора.

В области теории распознавания и классификации хорошо себя зарекомендовало применение искусственных нейронных сетей. Именно поэтому был выбран данный подход.

Список литературы

1. Бодянский Е.В. Искусственные нейронные сети: архитектуры, обучение и применение \ Е.В. Бодянский, О.Г. Руденко. – Харьков: ТЕЛТЕХ, 2004. – 372 с.
2. Кизим Н.А. Нейронные сети: теория и практика применения\Н.А. Кизим, Е.Н. Ястремская, В.Ф. Сенчуков. – Х.: ИД «ИНЖЭК», 2006. – 240 с.
3. Высочина О.С. Диссертация «Методы и модели классификации и прогнозирования состояний информационно-вычислительных систем на базе модифицированных вероятностных нейронных сетей»\О.С. Высочина. – 161 с.

УДК 621.376.9

І.М. Шнуренко

Науковий керівник – Рассомахін С.Г., канд. техн. наук, доцент
Харківський національний університет ім. В.Н. Каразіна

Алгебраический метод демодуляции сложных сигналов

Традиционно используемые цифровые методы демодуляции сложных сигналов основаны на нахождении спектральных коэффициентов при помощи быстрого дискретного преобразования Фурье (БДПФ) [3]. Достоинством таких алгоритмов является наличие развитой элементной базы, обеспечивающей аппаратную поддержку вычислений. К недостаткам метода следует отнести:

- повышенную вычислительную сложность, так как приходится находить множество ненужных (внеполосных) коэффициентов квадратурного гармонического разложения;

- трудности, связанные с обеспечением совпадения шкалы частот БДПФ с истинными значениями несущих частот в случае полигармонических структур сигналов.

Указанных недостатков лишен предлагаемый ниже алгебраический метод демодуляции. Принцип алгебраической демодуляции основан построении и решении системы линейных алгебраических уравнений (СЛАУ) для каждого канального символа радиосигнала. Зная структуру сигнала, можно составить уравнения в каждый момент времени передачи канального символа, в котором, коэффициентами при неизвестных будут служить значения модулирующих функций в соответствующие моменты времени, а вектор правых частей – измерения сигнала.

Пусть исходный сигнал описывается формулой:

$$s(t) = \sum_{i=0}^{N-1} (r_i \cdot \sin(2\pi f_1 \cdot t) + q_i \cdot \sin(2\pi f_2 \cdot t)) \quad (1)$$

где $s(t)$ - модулированный сигнал, r_i, q_i - значения двух битовых последовательностей, N - длина информационных последовательностей, f_1, f_2 - модулирующие частоты, выбраны так, что две синусные составляющие сигнала не влияют друг на друга. Для такой групповой структуры на каждом интервале T - периода сигнала строится СЛАУ из двух уравнений:

$$\begin{aligned} a_{11} \cdot x_1 + a_{12} \cdot x_2 &= b_1 \\ a_{21} \cdot x_1 + a_{22} \cdot x_2 &= b_2 \end{aligned} \quad (2)$$

где $a_{11} = \sin(2\pi f_1 \cdot t_1), a_{12} = \sin(2\pi f_2 \cdot t_1), a_{21} = \sin(2\pi f_1 \cdot t_2), a_{22} = \sin(2\pi f_2 \cdot t_2)$ - коэффициенты при искомым неизвестных в моменты времени t_1, t_2 на интервале одного канального символа сигнала, а $b_1 = s(t_1), b_2 = s(t_2)$ - величины измерения сигнала в моменты времени t_1, t_2 . В векторной записи СЛАУ имеет вид:

$$A \cdot X = B. \quad (3)$$

Таким образом, составив и решив СЛАУ из N уравнений, возможно однозначно идентифицировать каждое r_i и q_i значения входящей последовательности. Решение одной СЛАУ на интервале одного канального символа осуществляет групповую демодуляцию сразу двух составляющих общего сигнала.

Существует так же перспективная возможность снижения реальных существующих помех в канале. При взятии не одного измерения на каждом интервале канального символа, а нескольких, количество уравнений превысит количество неизвестных. Таким образом, решение уже переопределенной СЛАУ будет псевдорешением, минимизирующим величину помехи. Матрица коэффициентов будет не квадратной, поэтому для нахождения решения СЛАУ, правая и левая часть домножается на транспонированную матрицу коэффициентов A .

Преимущества такого метода демодуляции:

- высокая технологичность алгоритма с точки зрения программной реализации;
- невысокая вычислительная сложность;
- возможность переопределения СЛАУ для повышения помехозащищенности и устойчивости решения.

Внедрение алгебраических способов демодуляции сигналов способствует упрощению и удешевлению аппаратной реализации телекоммуникационного оборудования.

Список літератури

1. Теория электрической связи. / Под ред. Д. Д. Кловского. – М.: Радио и связь, 1999. – 204 с.
2. Макаров С. Б., Цикин И. А. Передача дискретных сообщений по радиоканалам с ограниченной полосой пропускания. – М.: Радио и связь, 1988. – 304 с.
3. Волощук Ю. І. Сигнали та процеси у радіотехніці. – т. 1, 2. – Х.: Компанія СМІТ, 2003. – 444, 580 с.
4. Долгов В. И., Рассомахин С. Г., Лисицкая И. В., Линник Н. Ф., Ткаченко С. А. Многоосновное кодирование в каналах связи с ограниченной полосой пропускания // Збірник наукових праць. – Х., ОНДІ ЗС, 2007. – Вип. 1(6). – С. 137 – 154.
5. Кузниченко В. С., Рассомахин С. Г. Цифровая демодуляция OFDM сигналов в условиях частичной неопределенности параметров // Системи управління, навігації та зв'язку. – 2011. – Вип. 4(20). – С. 283 – 288.

УДК 004.4

О.В. ЯтелНауковий керівник – Смірнов О.А., канд. техн. наук, доцент
Кіровоградський національний технічний університет

Розробка програмного забезпечення стиснення зображень за допомогою вейвлет-перетворень

При розгляді зображення як єдиної структури (а не як сукупності окремих рядків і стовпців), представляється можливим виявити додаткові закономірності й закласти їх у структуру нероздільного вейвлет-фільтру. У результаті підвищується якість обробки – знижується потужність помилки відновленого сигналу, збільшується вірогідність виявлення конкретного примітива в зашумленому сигналі й т.п.

Непогані результати обробки зображень виходять при спільному використанні методів вейвлет-перетворень і стандартних методів обробки зображень. Наприклад, для синтезу двовимірного вейвлет-фільтру в роботі використовується нове параметричне подання амплітудно-частотної характеристики (АЧХ) фільтру й рішення стандартного фазового завдання (розрахунок фазочастотної характеристики, використовуючи значення амплітудно-частотної характеристики). У цей час теорії й практичної реалізації методів обробки зображень присвячено багато робіт. Найбільш відомими в даній області є роботи Прэтта У., Ярославського Л.П., Зубарева Ю.Б., Дворковича В.П. і Дворковича А.В.

Вище відзначалося, що оптимізація вейвлет-функції під часові й частотні властивості оброблюваного зображення дозволяє підняти загальну якість обробки. Серед публікацій, що мають справу з оптимізованим вибором що аналізує вейвлет-фільтру, розглянуті роботи Ваттерлі (Vetterli M.), Моулін (Moulin P.), Claypoole R., Baraniuk R., Charith G., Abhayaratne K., Jones E., Runkle P., Новикова Л.А. У роботі [8] представлені два алгоритми адаптивного вейвлет-стиску, засновані на ліфтинг-схемі: оператор передбачення коректується або на кожному масштабі, або на кожному кроці в схемі ліфтинга в заданих межах. За аналогією з [8], у роботі [7] розроблений критерій оптимальної інтерполяції в схемі ліфтинга для операторів передбачення й корекції (причому передбачення здійснюється на кожному кроці ліфтинга). Додатковий інтерес представляє робота Новикова Л.А. [4], у якій проведений взаємозв'язок погодженої фільтрації й оптимального вейвлет-перетворення й наведена процедура синтезу вейвлетів з урахуванням апріорної інформації про форму сигналу й кореляційної функції шуму.

Другий основний напрямок оптимізованого вейвлет-перетворення пов'язане з вибором і збереженням тільки вибраних коефіцієнтів багаторівневого вейвлет-розкладання; адаптація здійснюється на другому етапі – на етапі вибору коефіцієнтів вейвлет-розкладу. Ключовими поняттями тут є "оптимізація дерева нулів" і алгоритм SPIHT. Серед публікацій, що стосуються оптимального вибору коефіцієнтів вейвлет-розкладання, розглянуті роботи Чобану М.К., Черникова А.В., Шапіро (Shapiro J.M.) [5-7].

У напрямку оптимізованих вейвлет-перетворень виділяється цикл робіт Лабунця В.Г., присвячений реалізації три-адичних вейвлет-перетворень для обробки кольорових зображень (одна з робіт – [6]). Реалізація будь-яких із

представлених вище алгоритмів цифрової обробки неможлива без використання загальних методів цифрової обробки сигналів. Значний внесок у розробку теорії й алгоритмів цифрової обробки сигналів внесли закордонні вчені: Найквіст Х., Гоулд Б., Рейдер Ч., Рабінер Л., Оппенгейм А., Боярин Р. і ін. Велике значення мали також роботи вітчизняних учених: Котельникова В.А., Ципкіна Я.З., Трахтмана А.М., Ланне А.А., Карташева В.Г., Гольденберга Л.М., Матюшкина Б.Д., Поляка М.Н., Витязева В.В., Брюханова Ю.А.

У процесі рішення поставлених завдань, найчастіше проблема зводилася до чисто математичних завдань. Їхні рішення виконане за допомогою різних підручників і статей.

Ціль роботи складається в розробці програмного забезпечення, яке призначено для стиснення зображень за допомогою вейвлет-перетворень.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

- розробка алгоритму параметризації одномірних вейвлет-функцій;
- розробка алгоритму параметризації двовимірних нероздільних вейвлет-функцій;
- синтез двовимірних нероздільних вейвлет-фільтрів із заданою частотною вибірковістю;
- розробка критерію оптимізації одномірних вейвлет-фільтрів для стиску сигналів;
- дослідження впливу частотних характеристик одномірних вейвлет-фільтрів на якість відновлення сигналів після стиску;
- розрахунок одномірних оптимізованих вейвлет-фільтрів;
- розробка критерію оптимізації двовимірних нероздільних вейвлет-фільтрів для стиску зображень;
- розрахунок двовимірних оптимізованих вейвлет-фільтрів для стиску зображень.

Об'єктом дослідження є процес стиснення зображень.

Предметом дослідження є методи стиснення зображень за допомогою вейвлет-перетворень.

Достовірність наукових результатів підтверджена теоретичними викладеннями, даними комп'ютерного моделювання, коректними дослідженнями параметрів на функціонуючій обчислювальній мережі, а також відповідністю отриманих результатів окремим результатам, наведеним у науковій літературі.

Список літератури

1. Добеши И. Десять лекций по вейвлетам. Москва-Ижевск: НИЦ "Регулярная и хаотичная динамика", 2004. – 464 с.
2. Чуй К. Введение в вейвлет. Пер. с англ. М.: Мир, 2001. – 412 с.
3. Уэлстид С. Фракталы и вейвлеты для сжатия изображения в действии. М.: Триумф, 2003.-230 с.
4. Блатер К. Вейвлет-анализ. Основы теории. М.: Техносфера, 2004. – 280 с.
5. Короновский А., Храмов А. Непрерывный вейвлетный анализ и его приложения. М.: Физматлит., 2003. – 176 с.
6. Дремин И.М., Иванов О.В., Нечитайло В.А. Вейвлеты и их использование // УФН-2001. Т. 171, №5. С. 465-561.
7. Астафьева Н.М. Вейвлет-анализ: основы теории и примеры применения // УФН. 1996. Т. 166, № 11. С. 1145-1170.
8. Малоземов В.Н., Машарский С.М. Обобщенные вейвлетные базисы связанные с дискретным перетворением Вилленкина-крестенсона // Алгебра и анализ. 2001. Т. 13, №1. С. 111-157.

ТЕОРІЯ РОЗРОБКИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

УДК 004.416.6

В.Т. Кучерук

Науковий керівник – Андреев А.М., канд. пед. наук, доцент
Запорізький національний університет

Методика створення програмного забезпечення для систем управління підприємствами з використанням типових програмних компонентів

Розробка та впровадження складних програмних комплексів для підприємств вимагає залучення значних ресурсів як розробника так і самого підприємства, тому вартість таких рішень для промислового підприємства середнього розміру починається від декількох десятків тисяч доларів в нижньому ціновому діапазоні і практично не має верхньої цінової межі. Виникає питання чи є шляхи її зменшення з боку розробників системи. Вартість сукупного володіння програмною системою складається з вартості створення, вартості впровадження та вартості супроводу. Причому досить поширеною помилкою при виборі ПЗ є облік вартості тільки самої системи.

В даний час методи і засоби зменшення трудомісткості розробки і супроводу ПЗ розроблені досить глибоко. Це такі методи програмної інженерії, спрямовані на створення складних систем, як розробка відкритих систем [1], розробка принципів оптимального розбиття систем на модулі [2], методи об'єктно-орієнтованого аналізу і проектування систем [3]. Зараз для розробки ПЗ різного призначення широко застосовується повторне використання програмних об'єктів і програмних компонентів [4], пропонувані виробниками засобів прискореної розробки додатків (rapid application development RAD). Використання CASE-засобів [5] також дозволяє значно скоротити трудомісткість проектування і супроводу систем.

Здавалося б, до вищесказаного вже нічого додати, і при використанні перерахованих методів і засобів вартість створення і супроводу ПЗ буде мінімальною. Однак це не так. Одразу хоч зауважити, що "срібної кулі" за висловом Ф. Брукса [6], що дозволяє розробляти легко супроводжувані, дешеві програмні системи, ще не створено, і пропонуваній підхід вимагає подальших досліджень, проте, він вже застосовувався в тій чи іншій мірі при розробці.

Таким чином, надання програмісту готової структури ПЗ, побудованої на основі об'єктивних досліджень конкретної предметної області, і методичних рекомендацій щодо створення ПЗ на основі такої структури може значно зменшити трудомісткість створення і, що важливо, супроводу системи і вберегти від дорогих логічних помилок при створенні програмних модулів.

Така структура була розроблена, а методика створення ПЗ на основі модулів, побудованих по даній структурі, названих типовими програмними компонентами (ТПК) (рис.1).

Термін "типовий програмний компонент" визначається як набір програмних об'єктів, що враховують особливості предметної області, невіддільних один від одного в рамках виконання певного класу завдань, що мають уніфікований інтерфейс, що дозволяє ТПК взаємодіяти між собою без додаткового координуючого коду та мають можливість зміни своїх властивостей без внесення змін в програмний код.

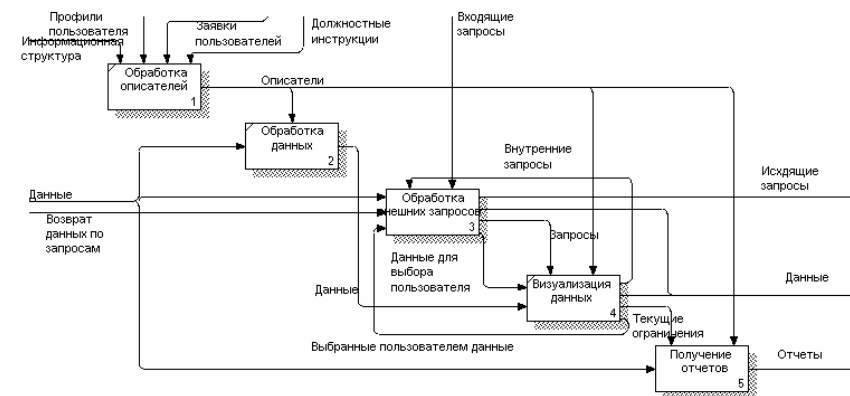


Рисунок 1 – Функціональна схема ТПК

Для створення ПЗ на основі ТПК пропонуються наступні кроки:

1. Створення ТПК - найбільш трудомісткий і дорогий етап, який повинен бути виконаний кваліфікованим програмістом.
2. Аналіз предметної області для подальшого створення модулів системи на основі ТПК. Цей етап виконується аналітиком системи і не включає в себе безпосереднього програмування.
3. Модулей системи на основі ТПК і профілів користувачів. Цей етап виконується програмістами середньої кваліфікації і включає основний обсяг робіт по створенню системи.
4. Налаштування ПО здійснюється відділом впровадження і, надалі, відділом супроводу безпосередньо на підприємстві.

Зaproпонована методика дозволяє скоротити витрати на створення і супровід ПЗ АСУП шляхом скорочення розмірів програмного коду вимагає подальшого супроводу, підвищення його гнучкості, що дозволяє здійснювати основну адаптацію до мінливих умов експлуатації силами самого підприємства без залучення розробника. Знижуються вимоги до кваліфікації програмістів, підвищується надійність системи за рахунок використання багаторазово протестованих компонентів.

Список літератури:

1. Липа В.В., Філіна О.М. Мобільність програм і даних у відкритих інформаційних системах. -М.: Наукова книга, 1997. – 368 с.
2. Маміконов А.Г. Методи розробки автоматизованих систем управління. -М.: Енергія, 1973. - 336 с.
3. Буч Г. Об'єктно-орієнтований аналіз та проектування з прикладами додатків на C++: Пер. з англ. - М.: СПб.: Видавництво Біном, Невський діалект, 1999. – 560 с.
4. Zubek J. Повторне використання об'єктів в системах вкоренитися розробки додатків // COMPUTERWEEKLY. - 1998. - № 7. - С. 24-28
5. Трофімов С.А. CASE-технології: практична робота в Rational Rose. -М: ЗАТ Видавництво БІНОМ, 2001 р. -272 с.
6. Брукс Ф. Міфічна людина-місяць або як створюються програмні системи. - Пер. з англ. - СПб.: Символ-Плюс, 1999. - 304 с.
7. Бюрер К. Від ремесла до науки: пошук основних принципів розробки ПЗ.

УДК 004.05

А.С. Богатиренко, А.А. Недолужко
 Науковий керівник – Дбрєнський О.П., викладач
Кіровоградський національний технічний університет

Застосування метода статичного тестування для виявлення та усунення помилок ПЗ

Тестування – невід'ємна складова процесу програмної інженерії, один з методів подальшого вдосконалення якості розроблених програмних засобів за допомогою усунення дефектів, що залишилися не виявленими іншими видами перевірок.

Тестування можна розглядати як процес семантичного налагодження (перевірки) програми, яка полягає у виконанні послідовності різних наборів контрольних тестів, для яких заздалегідь відомий результат. Тобто тестування передбачає виконання програми і отримання конкретних результатів виконання тестів.

Упродовж свого розвитку проблематика тестування розвивалася паралельно у декількох напрямках, зокрема:

- дослідження та розроблення методів тестування й критеріїв адекватності тестування (відповідно до методів);
- визначення кількісних метрик тестування та критеріїв його завершення;
- створення програмних інструментів підтримки тестування;
- формування моделей оцінювання процесу тестування та його вдосконалення.

Статичні методи використовуються при проведенні інспекцій і розгляді специфікацій компонентів без їхнього виконання.

Техніка статичного аналізу полягає в методичному перегляді (або огляді) і аналізі структури програм, а також у доведенні їхньої правильності вручну. Статичний аналіз направлений на аналіз документів, розроблених на всіх процесах життєвого циклу (ЖЦ) і полягає в інспекції вхідного коду і наскрізного контролю програми.

Інспекція ПЗ – це статична перевірка відповідності програми заданим специфікаціями, проводиться шляхом аналізу різних представлень результатів проектування (документації, вимог, специфікацій, схем або коду програм) на процесах ЖЦ. Перегляди й інспекції результатів проектування і відповідності їх вимогам замовника забезпечують більш високу якість розроблюваного ПЗ.

При інспекції програм розглядаються документи робочого проектування на процесах ЖЦ разом з незалежними експертами й учасниками розробки ПЗ. На початковому процесі проектування інспекція припускає перевірку повноти, цілісності, однозначності, несуперечності і сумісності документів з вимогами до програмної системи. На процесі реалізації системи під інспекцією розуміють аналіз текстів програм на дотримання вимог стандартів і прийнятих керівних документів технології програмування.

Ефективність такої перевірки полягає в тому, що залучені експерти намагаються подивитися на проблему «з боку» і піддають її всебічному критичному аналізу.

Ці прийоми дозволяють на більш ранніх процесах проектування знайти помилки або недоробки шляхом багаторазового перегляду вхідного опису програми. Символьне тестування застосовується для перевірки окремих ділянок програми на вхідних символьних значеннях.

Крім того, розробляється безліч нових засобів автоматизації символьного виконання програм. Наприклад, автоматизований засіб статичного контролю для

мовно-орієнтованої розробки, інструменти автоматизації доведення коректності й автоматизований апарат мереж Петрі.

Масове виробництво і повсюдна доступність 64-бітових процесорів привели розробників додатків до необхідності розробки 64-бітових версій своїх програм. Адже для того, щоб користувачі могли отримати реальні переваги від використання нових процесорів, додатки повинні бути перекомпілювати для підтримки 64-бітної архітектури. Основні проблеми при переносі коду виявляються в додатках, розроблених з використанням низькорівневих мов програмування типу С або С++. Усі високорівневі конструкції та бібліотеки С++ в кінцевому підсумку реалізовані з використанням низькорівневих типів даних, таких як покажчик, машинне слово і т.п. Оскільки при зміні архітектури ці типи даних змінюються, то і поведінка програм також може змінитися.

Для того щоб б впевненим у коректності програми на новій платформі, необхідно вручну виконати перегляд коду і переконатися в його коректності. Тому виникає завдання пошуку в вихідному коді програми тих місць, які при перенесенні з 32-бітної на 64-бітову архітектуру можуть працювати неправильно. Тестують команди за послідовністю їх розташування в тексті програми. Під час статичного тестування тестують не всі можливі шляхи в графі програми, тому частина помилок може залишитися виявленою; програмний код взагалі не виконується — його тестують тільки шляхом логічного аналізу.

Для статичного тестування використовують такий інструментальний засіб, як компілятор. Виявивши, наприклад, синтаксичну помилку або неправильну операцію, він видає відповідне повідомлення. Компонувальник теж може видавати корисні повідомлення, зокрема імена змінних та інших об'єктів, що повторюються, посилання на неоголошені змінні та функції.

Статичний аналіз програми спеціалісти-тестувальники виконують неавтоматизовано. Вони читають вихідний код програми, обговорюють його і знаходять, як правило, досить багато помилок. Робота вичитування програмного коду досить рутинна, але необхідна.

Існують статичні аналізатори коду (як, наприклад, Gimpel Software PC-lint і Parasoft C++ test) призначені для комплексного забезпечення якості коду і містять кілька сотень аналізованих правил. У них також є деякі з правил, які аналізують коректність 64-бітних додатків. Однак, оскільки це аналізатори коду загального призначення, то їх використання для забезпечення якості 64-бітних додатків не завжди зручно. Це пояснюється, насамперед, тим, що вони не призначені саме для цієї мети. Іншим серйозним недоліком є їх зорієнтованість на модель даних, яка використовується в Unix-системах (LP64). У той час як модель даних, яка використовується в Windows-системах (LLP64), істотно відрізняється від неї. Тому застосування цих статичних аналізаторів для перевірки 64-бітних Windows-додатків можливо тільки після неочевидного додаткового налаштування.

Список літератури

1. Андон Ф.И., Коваль Г.И., Коротун Т.М., Лаврищева Е.М. Суслов В.Ю. Основы инженерии качества программных систем. Киев: Академперіодика.– Второе изд., 2007. – 680 с.
2. Weyuker E.J., Ostrand T.J. Theories of program testing and the application of revealing subdomains. IEEE Trans.Soft.Eng. – 1980. – V. 6, – № 3, – P. 236–246.
3. Лаврищева Е.М., Коротун Т.М. Построение процесса тестирования программных систем. Проблемы программирования.–2002.– №1-2.– С. 272-281.
4. Бабенко Л.П., Лаврищева Е.М. Основы программной инженерии. Киев: Знание, 2001. – 269 с.

А.Я. Командир

Научный руководитель – Толстолужская Е.Г., канд. техн. наук, доцент
Харьковский национальный университет им. В.Н. Каразина

Технология MVC для разработки web-приложений

В настоящий момент набирает всё большую популярность разработка web-приложений. Для стандартизации и повышения качества разработки была введена модель MVC — схема использования шаблонов проектирования, с помощью которых модель данных приложения, пользовательский интерфейс и взаимодействие с пользователем разделены на три отдельных компонента так, что изменение одного из компонентов оказывает минимальное воздействие на остальные. Данная схема проектирования часто используется для построения архитектурного каркаса, когда переходят от теории к реализации в конкретной предметной области.

Модель — содержит бизнес-логику приложения и включает методы выборки, обработки (например, правила валидации) и предоставления конкретных данных. Модель не должна напрямую взаимодействовать с пользователем. Все переменные, относящиеся к запросу пользователя должны обрабатываться в контроллере. Модель не должна генерировать HTML или другой код отображения, который может изменяться в зависимости от нужд пользователя. Такой код должен обрабатываться в видах.

Одна и та же модель, например: модель аутентификации пользователей может использоваться как в пользовательской, так и в административной части приложения.

Вид — используется для задания внешнего отображения данных, полученных из контроллера и модели.

Виды содержат HTML-разметку и небольшие вставки кода для обхода, форматирования и отображения данных. Не должны напрямую обращаться к базе данных. Не должны работать с данными, полученными из запроса пользователя. Может напрямую обращаться к свойствам и методам контроллера или моделей, для получения готовых к выводу данных.

Контроллер — связующее звено, соединяющее модели, виды и другие компоненты в рабочее приложение. Контроллер отвечает за обработку запросов пользователя. Контроллер не должен содержать SQL-запросов. Контроллер не должен содержать HTML и другой разметки.

Цикл от обращения браузера к определенному url-адресу (рис. 1) до момента отображения страницы для пользователя:

- пользователь вводит url(или переходит по ссылке), и браузер(через web-сервер) обращается к контроллеру;
- контроллер обращается к модели;
- модель обращается к БД (для получения необходимой для вывода информации);
- информация из БД передается в модель;
- из модели данных передаются в контроллер;
- контроллер выносит эту информацию в вид;
- вид выводится в браузер с помощью контроллера.

Браузер может обращаться только к контроллеру, так как контроллер является частью url-адреса. Пользователь не может обратиться к чему бы то ни было, кроме контроллера. Человек не может через адресную строку обращаться к видам или моделям. Он взаимодействует только с контроллером.

В связи с этим можно говорить о контроллере как о своеобразном “распределительном центре” (менеджере). Контроллер обрабатывает запросы пользователя, контроллер обращается к модели, контроллер же является посредником для вывода вида в браузер.

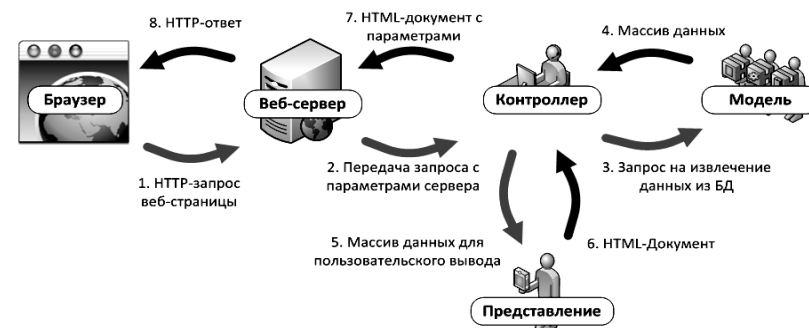


Рисунок 1 – Схема работы MVC для web-приложения

В рамках концепции MVC принято, что с базой должны работать только модели. Вывод: причины использовать MVC модель для разработки web-приложения:

- Типизированность. Каждый разработчик, который понимает MVC, быстро разберётся в чужом проекте (построенном по принципу MVC), и сможет продуктивно продолжить работу.
- Возможность повторного использования. Модель составляется так, чтобы предусмотреть многократное использование с минимальными изменениями или вообще без них.
- Расширяемость. Модель имеет четко определенное поле для работы, если требуется изменить вид или функциональность.

Список литературы

1. Интернет-ресурс: www.ozon.ru/context/detail/id/3771474/
2. Интернет-ресурс: www.rsdn.ru/article/patterns/generic-mvc.xml
3. Стивен Сандерсон ASP.NET MVC Framework с примерами на C# для профессионалов. — М.: Вильямс, 2009.
4. Интернет-ресурс: www.ibm.com/developerworks/ru/library/wi-embed/index.html?ca=dre-ru

О.М. Змеул

Науковий керівник – Доренський О.П., викладач
Кіровоградський національний технічний університет

Дослідження методів забезпечення надійності програмного забезпечення

Стрімкий розвиток інформаційних технологій (ІТ), комп’ютерної техніки, програмного забезпечення (ПЗ) та, як наслідок, технологій розробки програмних продуктів, розширення спектра використання автоматизованих систем у сучасному

світі зумовлюють паралельний розвиток усіх складових процесу побудови й впровадження ПЗ [1]. Підвищення складності та багатокomпонентність сучасного ПЗ вимагають спеціалізованого підходу під час його розробки й експлуатації. Будь-яке програмне забезпечення повинне досягати високого рівня надійності, що дозволяє йому ставати ефективним інструментом нових технологій. Будь-який збій ПЗ може мати серйозні наслідки та втрати (матеріальні та нематеріальні збитки), що є неприпустимим. Тому задача забезпечення надійності ПЗ, що розробляється, є актуальною та однією з основних для розробників та користувачів програмних продуктів.

За умови досягнення високої надійності, ПЗ стає ефективним та конкурентоспроможним. Саме від показника надійності похідними будуть інші, не менш важливі показники – якість, живучість, безпека, готовність [2].

Метою роботи є дослідження методів забезпечення надійності програмного забезпечення з метою уникнення збоїв в роботі ПЗ.

В багатьох дослідженнях поняття надійності програмного забезпечення (ПЗ) виділяють окремо [3], тому, що при застосуванні понять надійності до програмних засобів варто враховувати особливості і відмінності цих об'єктів від традиційних технічних систем, для яких спочатку розроблялася теорія надійності. Принципова відмінність програм від техніки, та технічних систем зокрема, полягає в тому, що програма не зношується з плином часу, а навпаки, виявляються помилки, які не були знайдені раніше, ПЗ з часом вдосконалюється і покращується. Водночас підвищуються і вимоги до надійності та витривалості програм, виникає потреба у скороченні затрат на тестування та, відповідно, у прогнозуванні надійності розроблюваного програмного забезпечення [2].

Аналіз [1-5] показав, що дослідження методів забезпечення надійності програмного забезпечення є актуальною задачею.

Визначальне значення для забезпечення надійності програм мають методи контролю і забезпечення надійності програм [5]. Для її підвищення і захисту інформації програмно-алгоритмічними методами ефективно застосовувати часову, інформаційну та програмну надлишковість.

Метод часової надлишковості полягає у використанні певної частини апаратних засобів і продуктивності комп'ютера для контролю виконання програм і відновлення обчислювального процесу (ОП). Передбачається певний резерв продуктивності, необхідний для контролю й підвищення надійності функціонування ПЗ. Резерв часу використовують для контролю і виявлення спотворень, їх діагностування і прийняття рішень щодо відновлення ОП або інформації, реалізації операцій відновлення.

Для застосування інформаційної надлишковості необхідно дублювати накопичені початкові й проміжні дані. Цей метод використовують для забезпечення достовірності даних, які потребують значного часу для відновлення чи найбільше впливають на нормальне функціонування програмного забезпечення.

Метод програмної надлишковості забезпечує контроль і достовірність найважливіших рішень з оброблення інформації та керування. При ньому застосовують кілька варіантів програм, що відрізняються методами розв'язання певного завдання або програмною реалізацією одного й того самого методу. Це дає змогу виключати спотворення результатів, зумовлених програмними помилками чи збоями ЕОМ.

Часто введенням надлишковості для забезпечення надійності ПЗ нехтують, що знижує показники надійності програм, що розробляють [5].

Щодо процесу експлуатації, то контроль надійності функціонування ПЗ проводять трьома етапами, відповідно до яких він і має назви.

– профілактичний контроль, за якого здійснюють у неробочому режимі системи керування або оброблення інформації під час проведення регламентних профілактичних робіт;

– передпусковий контроль, який проводять під час підготовки до ввімкнення нормального робочого режиму функціонування ПЗ;

– оперативний контроль, що здійснюють у процесі розв'язання системою основних функціональних завдань у нормальному режимі роботи.

Після завершення випробувань і передавання ПЗ замовнику його експлуатують і тиражують впродовж певного часу. На цьому етапі можливі спотворення програм у процесі їх зберігання та регулярної експлуатації. Крім того, з огляду на зміну вхідних даних, може виникнути необхідність внесення змін у програму. Тому навіть одне незначне низькоякісне коректування може спричинити істотне зниження напрацювання на відмову. Щоб зберегти і поліпшити показники надійності ПЗ під час його тривалої експлуатації, необхідно чітко регламентувати впровадження програм. Зміни в ПЗ вводять групами, що формують чергову версію ПЗ зі зміненими характеристиками.

Серед версій ПЗ виокремлюють еталонні і користувальницькі. Еталонну версію допрацьовують і модернізують основні розробники ПЗ або спеціалісти з експлуатації. Вони мають скоректовану технічну документацію, що відповідає програмам, і точний перелік усіх змін, введених у дану версію порівняно з попередньою. Розробка кожної наступної еталонної версії вимагає випробування і перевірки на працездатність.

Користувальницькі версії (або версії конкретної системи [5]) формують за інструкціями і правилами, що є в експлуатаційній документації еталонних версій. Зміни в них обмежені й стосуються окремих компонентів ПЗ. Щоб перевірити, чи коректно їх виконують, додають методики перевірки та правила розроблення контролюючих тестів.

Загальними способами забезпечення і підвищення надійності ПЗ є:

- розроблення і вибір алгоритмів функціонування ПЗ, нечутливих до порушень обчислювального процесу (використання алгоритмічної надлишковості);
- удосконалення технології програмування;
- контроль і тестування програм з наступною їх корекцією;
- резервування програм та інші методи введення структурної надлишковості.

Отже, в роботі досліджено методи забезпечення надійності програмного забезпечення, запропоновано й обґрунтовано застосування часової, інформаційної й програмної надлишковості. Зважаючи на стрімкий розвиток ІТ-технологій, комп'ютерної техніки і програмного забезпечення, є перспективними подальші дослідження, зокрема у напрямку забезпечення надійності ПЗ мобільних систем.

Список літератури

1. Змеул О.М. Дослідження помилок програмного забезпечення / О.М. Змеул, О.П. Доренський // Актуальні задачі сучасних технологій: збірник тез доповідей Міжнародної науково-технічної конференції молодих учених та студентів, 19–20 грудня 2012 р., м. Тернопіль – Тернопіль: Вид-во ТНТУ ім. Івана Пулюя, 2012. – С. 187-188.
2. Чабанюк Я.М. Побудова і дослідження моделі надійності програмного забезпечення з індексом величини проекту / Я.М. Чабанюк, В.С. Яковина, Д.В. Федасюк і ін. // Інженерія програмного забезпечення. – Вип. 1. – 2010. – С. 1-6.
3. Половко А.М. Основи теорії надійності / А.М. Половко, С.В. Гуров – СПб.: БХВ-Петербург, 2006. – 704 с.
4. Яковин В. Огляд основних підходів до аналізу надійності програмного забезпечення / В. Яковина, В. Смирнов // Комп'ютерні науки та інформаційні технології – Вип. 719. – 2011. – С. 278-282.
5. Локазюк В.М. Надійність, контроль, діагностика і модернізація ПК: Посібник / В.М. Локазюк, Ю.Г. Савченко. – К.: Видавничий центр “Академія”, 2004. – 376 с.

П.П. Скакун

Науковий керівник – Мелешко Є.В., канд. техн. наук, доцент
Кіровоградський національний технічний університет

Розробка власної мови програмування та інтерпретатору до неї на основі мови програмування Racket

Метою роботи є розробка нескладної мови програмування та інтерпретатора до неї на основі мови програмування Racket.

Як відомо, існує безліч мов програмування, які відрізняються одна від одної різними аспектами, такими як:

- Типізація.
- Парадигма.
- Структура.
- Семантика.

Реалізація мови програмування є нелегким, проте досить цікавим процесом, який допомагає вивчити особливості та можливості мов програмування.

Для реалізації власної мови програмування було обрано мову програмування Racket, яка є вдосконаленням нащадком мови програмування Scheme – діалекту мови програмування Lisp. Racket є функціональною та мета-мовою програмування з динамічною типізацією, що надає усе необхідне для реалізації власної мови програмування.

Перед реалізацією необхідно визначитись з можливостями нової мови:

- Типи даних: ціле число, булевий тип, рядковий тип та ін.
- Логічні оператори.
- Умовні оператори.
- Функції. Виклик функцій. Рекурсивний виклик функцій.
- Локальна область визначення. Замикання.
- Обробка синтаксичних помилок.
- Обробка помилок типізації.
- Функціональні особливості:
 - a) функції вищого порядку;
 - b) каррирування (або карринг, англ. currying);
 - c) анонімні функції.

Використовувати нову мову програмування можна буде безпосередньо у середовищі виконання мови програмування Racket, застосовуючи зарезервованій синтаксис, який інтерпретатор буде розглядати як дерево виразів. Загальна структура використання власної мови програмування наведена на рисунку 1:

Об'єктом дослідження є процес створення синтаксису нової мови та інтерпретації виразів на цій мові.

Предмет дослідження – аспекти мов програмування та їх загальна структура.

Наукова новизна отриманих результатів полягає у наступному:

1. Розроблена нова мова програмування, відкрита для вдосконалення.

2. Розроблений інтерпретатор для нової мови програмування.

Загальна структура

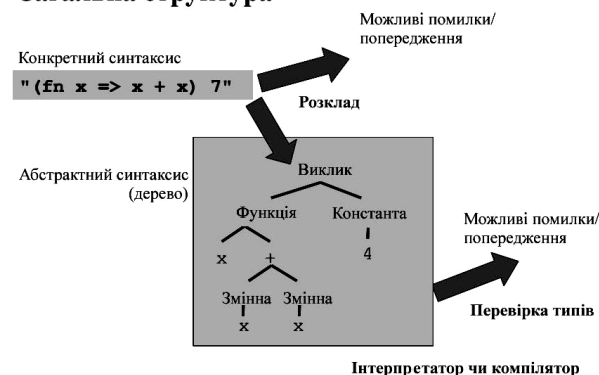


Рисунок 1 – Загальна структура використання власної мови програмування

Практична значимість роботи:

– На прикладі нової функціональної мови програмування розкрито принципи реалізації мов програмування, їх інтерпретації, а також загальної функціональності необхідної функціональній мові програмування.

– Вихідний код визначення виразів відповідних синтаксису мови та інтерпретація дають поняття про основні можливості функціональних мов програмування, що дає простір для порівняння їх з імперативними мовами програмування.

Список літератури

1. Racket Documentation - <http://docs.racket-lang.org/>.
2. Washington University course “Programming languages” by Dan Grossman (2013).

С.С. Гуменюк

Науковий керівник – Собінов О.Г., асистент
Кіровоградський національний технічний університет

Програмне забезпечення верстата ЧПК обробки електроізоляційного картону

Електрокартон електротехнічний – це один з найбільш популярних ізоляційних матеріалів. Найбільше поширення електрокартон одержав у сфері створення ізоляції для електроприладів і пристроїв (від зварювальних агрегатів до ізоляції електричних стендів) а також як матеріал для лекал. Основне призначення електрокартону (електроізоляційний картон) – це виготовлення елементів електроізоляції. Але на практиці сфера його застосування набагато ширша. Завдяки високій зносостійкості

електрокартон придбав величезну популярність у підприємств швейного виробництва й став звичним матеріалом для виготовлення лекал.

Найбільш часто електрокартон (картон електроізоляційний) застосовується разом із супутніми електротехнічними матеріалами: лаком ГФ 95, трансформаторним маслом, електробумагою і багатьма іншими.

Із всіх марок електрокартону (пресшпану), що виготовляються згідно зі стандартом ДСТ 4194 від 1983 року, найбільше поширення одержав електроізоляційний картон марок ЕВ, А, Б. Картон електротехнічний (електрокартон) марки ЕВ застосовується в різних галузях промисловості для електроізоляції при роботі в повітряних середовищах при температурі до 90 градусів Цельсія. Картон електроізоляційний марки Б (електротехнічний картон) використовується для деталей електроізоляції в трансформаторах, в апаратах, а також в іншому електроустаткуванні з масляним заповненням при робочій температурі до 150 °С. Картон електроізоляційний марки А (пресшпан) застосовується як електроізоляційний матеріал для різних агрегатів, трансформаторів і приладів, що працюють при напрузі до 750 кВольт.

Таким чином, розробка програмного забезпечення верстата ЧПК обробки електроізоляційного картону є актуальною задачею.

Список літератури

1. Сосонкин В. Л., Мартинов Г. М. Системы числового программного управления. Учебное пособие для вузов. Изд. Логос, 2005. – 296 с.
2. В. Л. Сосонкин, Г. М. Мартинов Программирование систем числового программного управления. Изд. Логос, Университетская книга, 2008. – 344 с.
3. Босинзон М. А. Современные системы ЧПК и их эксплуатация. Учебник для нач. проф. образования Изд. Academia, 2009.

УДК 004.4

Є.А. Зінов'єв

Науковий керівник – Собінов О.Г., асистент
Кіровоградський національний технічний університет

Програмне забезпечення системи реінжинірингу та рефакторингу програмного коду до платформи .NET

Багато підприємств за роки свого існування накопичують потужну власну розрахункову базу, адаптовану під специфічні умови й вимоги конкретного підприємства. Як правило, такі розрахункові бази засновані на стандартних розрахункових методиках, але з використанням власних практичних знань і досліджень у сфері діяльності підприємства. Найчастіше, власні розрахункові методики – це не що інше, як база знань, що забезпечує нормальне функціонування підприємства й, відповідно, своєчасний випуск нової продукції.

На жаль, деякі підприємства можуть із упевненістю сказати, що їхні розрахункові бази втримуються в належному виді й зручні для повсякденного використання. От основні критерії, по яких можна встановити незадовільний стан розрахункових методик підприємства:

- розрахунок не автоматизований, тобто є тільки на папері;

- розрахунок автоматизований частково, тобто є програма, але на певному етапі розрахунку потрібне втручання людини, наприклад для уведення значень із діаграм або таблиць;

- програма застаріла настільки, що її неможливо запустити на сучасному комп'ютері;

- програма має незручний інтерфейс;

- програма не дозволяє зберегти вихідні дані для повторного використання й/або результати розрахунку в електронному виді;

- програма вимагає доробки, але через відсутність кваліфікованого фахівця їй користуються "як є";

- неможливість або труднощі наступності досвіду роботи із програмою молодими фахівцями.

Таким чином, виходячи з вищеперерахованого, розробка програмного забезпечення системи реінжинірингу та рефакторингу програмного коду до платформи .NET, є актуальною задачею.

Список літератури

1. Фаулер М., Бек К., Брант Д., Робертс Д., Апдайк У. Рефакторинг: улучшение существующего кода = Refactoring: Improving the Design of Existing Code (2000). – Спб: Символ-Плюс, 2009. – 432 с.
2. Скотт В. Эмблер, Прамоджумар Дж. Садаладж. Рефакторинг баз данных: эволюционное проектирование. – М.: «Вильямс», 2007. – 368 с.
3. Джошуа Кериевски Рефакторинг с использованием шаблонов. – Вильямс, 2008. – 400 с.

УДК 004.4

І.С. Кучеренко

Науковий керівник – Коноплицька О.К., асистент
Кіровоградський національний технічний університет

Програмне забезпечення системи запобігання аналізу та модифікації програмних продуктів

Система запобігання аналізу та модифікації програмних продуктів базується на використанні обфускації. Обфускація (від англ. to obfuscate – спантеличувати, заплутувати) – це приведення коду, що виконується, або вихідного тексту програми до виду, що зберігає її функціональність, але утрудняє розуміння, аналіз алгоритмів роботи, а також модифікацію при декомпіляції.

Мета обфускації:

- Продемонструвати неочевидні можливості мови й кваліфікацію програміста (якщо заплутування виробляється не інструментальними засобами, а вручну).

- Оптимізувати програму для зменшення розміру коду й прискорення роботи.

- Ускладнити декомпіляцію/налагодження й вивчення шкідливих програм, щоб запобігти виявленню їхньої шкідливої функціональності.

- Утруднити декомпіляцію пропрітарних програм, щоб запобігти зворотній розробці або обхід систем перевірки ліцензій і DRM.

- Порушити авторські права програмістів і сховати авторство.

У пошуковій оптимізації обфускація javascript-файлів використовувалася для заплутування пошукових ботів при декомпіляції коду, нерідко в облудних цілях. На сьогоднішній день це неактуально.

Отже, розробка програмного забезпечення системи запобігання аналізу та модифікації програмних продуктів є актуальною задачею.

Список літератури

1. Альфред В. Ахо, Моника С. Лам, Рави Сети, Джеффри Д. Ульман. Компиляторы: принципы, технологии, инструментарий. – М.: Вильямс, 2008. – С. 719-760.
2. Barak B., Goldreich O., Impagliazzo R., Rudich S., Sahai A., Vadhani S., Yang K. On the (Im)possibility of obfuscating programs // Lecture Notes in Computer Science, v. 2139, 2001, p. 1-18.
3. Лифшиц Ю. М. Запутывание (обфускация) программ. Обзор. – СПб.: СПб.отд.Мат.инст. им.В.А.Стеклова РАН, 2004. <http://logic.pdmi.ras.ru/~yura/of/survey1.pdf>.

УДК 004.4

С.Д. Сороколат

Науковий керівник – Приходькіна А.І., ст. викладач
Кіровоградський національний технічний університет

Програмне забезпечення системи управління даними зовнішніх жорстких дисків з інтерфейсом USB 3.0

Допомогти користувачеві зберегти, а головне – легко перенести великі обсяги контенту, покликані сучасні переносні жорсткі диски з використанням USB 3.0.

Інтерфейс USB 3.0 стає все актуальнішим з кожним днем. Допомагають йому в цьому програмні системи та мультимедійні файли, розміри яких постійно збільшуються. Якщо торкнутися питання мультимедійних даних, то знімки, як правило, займають ще більше місця, не говорячи вже про все більше поширення RAW-формату. Не відстає й відеоконтент: наприклад, на початку квітня на українському ринку з'явився перший Quad-HD Ultra High Definition-телевізор з розрешенням 3840 x 2160 крапок. Допомогти користувачеві зберегти, а головне – легко перенести великі обсяги мультимедійного контенту покликані сучасні переносні жорсткі диски USB 3.0.

Крім цього, як правило, зовнішні жорсткі диски інтерфейсу USB 3.0 доволі часто використовуються як сховища даних, або резервні копії актуальних даних.

Але при цьому гостро стає проблема збереження даних на зовнішніх жорстких дисках інтерфейсу USB 3.0, зокрема збереження конфіденційних даних.

Проведені дослідження показали, що одним з найбільш перспективних напрямків управління даними з ціллю збереження конфіденційності інформації на зовнішніх носіях, зокрема на зовнішніх жорстких дисках інтерфейсу USB 3.0, є використання потокових шифрів.

Таким чином, розробка програмного забезпечення системи управління даними зовнішніх жорстких дисків з інтерфейсом USB 3.0 є актуальною задачею.

Список літератури

1. Коржик В.И., Кушнир Д.В. Теоретические основы информационной безопасности телекоммуникационных систем: учебное пособие / СПбГУТ. – СПб, 2000.
2. Жельников В. Криптография от папируса до компьютера. – М.: АБФ, 1996.
3. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. – М.: Радио и связь, 1999.
4. Коржик В.И., Кушнир Д.В., Морозов К.Г. Основы защиты информации в компьютерных системах: методические указания к лабораторным работам / СПбГУТ. – СПб, 1999.

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ КОМП'ЮТЕРНИХ СИСТЕМ І МЕРЕЖ

УДК 621.391

Д.А. Берчіян, Ю.В. Болтова

Науковий керівник – Клименко А.М., канд. техн. наук, доцент
Національний технічний університет «Харківський політехнічний інститут»

Проблеми моделювання при модернізації локальної обчислювальної мережі

Модернізація існуючих локальних обчислювальних мереж (ЛОМ) потребує врахування багатьох взаємозалежних факторів і для зменшення вартісних і часових витрат може бути проведена з використання комплексу моделей.

В докладі розглянуте питання модернізації локальної обчислювальної мережі. Основними завданнями розробленої ЛОМ є організація інформаційного обміну даними між робочими станціями, організація доступу користувачів до ресурсів ЛОМ: баз даних, файлового сервера, мережевих принтерів, взаємодія системних додатків в різних вузлах, і доступ до них співробітників, а також забезпечення належного рівня захисту інформації, що не допускає її спотворення, або витоку.

Для модернізації ЛОМ використовують особливий клас математичних моделей – імітаційні. При імітаційному моделюванні мережі не потрібне дороге устаткування – його робота імітується програмами, що достатньо точно відтворюють всі основні особливості і параметри такого устаткування. Результатом роботи імітаційної моделі є зібрані, в ході спостереження, за перебігом подій статистичні дані про найбільш важливі характеристики мережі: часах реакції, коефіцієнтах використання каналів і вузлів, вірогідності втрат пакетів і т.д.

Існують спеціальні, орієнтовані на моделювання обчислювальних мереж програмні системи, в яких процес створення моделі спрощений. Такі програмні системи самі генерують модель мережі на основі вихідних даних про: її топологію, використовуваних протоколів, інтенсивність потоків запитів між комп'ютерами мережі, протяжність ліній зв'язку, типи використовуваного устаткування і додатків.

На основі проведених досліджень запропонована власна система імітаційних моделей, що враховує недоліки досліджених готових програмних продуктів з імітаційного моделювання ЛОМ. Запропонована система виконує збір даних про роботу мережі; забезпечує детальне моделювання мережі; проводить швидку оцінку продуктивності мережі (виявлення недоліків та вразливих місць ЛОМ).

Список літератури

1. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы.–СПб.:Питер, 2002.–672 с.
2. Кобелев Н.Б. Введение в общую теорию имитационного моделирования. – М.: ООО Принт-сервис, 2007.– 268 с.
3. Нардожев В.И., Нардожев И.В. Модели и алгоритмы информационно-вычислительной системы компьютерного тестирования. Монография. – М.: Прометей, 2000. – 148 с.
4. Рыжиков Ю.И. Имитационное моделирование. Теория и технологии. – СПб.: КОРОНА принт; М.: Альтекс-А, 2004. – 384 с.

Р.О. БобрішоваНауковий керівник – Колодочкіна А.В., асистент
Кіровоградський національний технічний університет

Структура семантичного Web

За 10 років свого існування Web настільки розвинувся, що близький до стану "переповнення", як це не парадоксально звучить. Дві основні причини породжують дві основні проблеми Internet. Перша причина - зростання обсягів інформаційного наповнення, породжений популярністю і дешевизною Web-технологій, а друга - формат подання інформації в Мережі, який орієнтований переважно на людей і лише в деяких випадках допускає автоматичну обробку програмними агентами.

В результаті, по-перше, виникає проблема знаходження необхідної користувачеві інформації в будь-якому вигляді - обсяги Web-простору не дозволяють оперативно оновлювати бази даних інформаційно-пошукових систем, а по-друге в автоматизованому режимі практично неможливо виділити сенс інформаційних повідомлень, наприклад, за назвою якої-небудь конкретної статті, представленої в Internet, можна знайти сотні посилань на цю статтю, в масиві яких сама стаття втрачається.

Тому подальший розвиток Internet багато вчених пов'язують з концепцією Семантичного Web (Semantic Web), яка багато в чому завдяки уніфікації обміну даними ймовірно дасть можливість інтегрувати в Internet навіть об'єкти реального світу. Концепцію Семантичного Web висунув Тім Бернерс-Лі, один з основоположників World-Wide Web і голова WWW-консорціуму на міжнародній конференції XML-2000, що пройшла в 2000 році у Вашингтоні.

Основна ідея цього проекту полягає в організації такого подання даних в мережі, щоб допускалася не тільки їх візуалізація, але і їх ефективна автоматична обробка програмами різних виробників. Шляхом таких радикальних перетворень концепції вже традиційного Web передбачається перетворення його в систему семантичного рівня. За задумом творців Семантичний Web повинен забезпечити "розуміння" інформації комп'ютерами, виділення ними найбільш придатних за тими чи іншими критеріями даних, і вже після цього - надання інформації користувачам.

При автоматичній обробці інформації в рамках Семантичного Web взаємодіють один з одним сервіси на основі аналізу смислових зв'язків між об'єктами і поняттями, що зберігаються в Мережі повинні відбирати лише ту інформацію, яка буде реальною корисною користувачам.

За визначенням консорціуму W3C Семантичний Web являє собою розширення існуючої мережі Internet, в якому інформація подається в чіткому та певному смисловому значенні, що дає можливість людям і комп'ютерам працювати з більш високим ступенем взаєморозуміння і узгодженості. Семантичний Web передбачає поєднання різноманітних видів інформації в єдину структуру, де кожному смисловому елементу даних буде відповідати спеціальний синтаксичний блок (тег). Теги повинні складати єдину ієрархічну структуру, на основі якої і повинен функціонувати Семантичний Web. За словами Бернерса-Лі, в рамках проекту "Семантичний Web" розробляються мови для вираження інформації у формі, доступній для машинної

обробки, на яких можна буде описувати як дані, так і принципи трактування цих даних. Це має призвести до того, що правила висновків, існуючі в якій-небудь одній системі подання знань, будуть передаватися по мережі іншим подібним системам. У процесі реалізації концепції Семантичного Web отримали широкий розвиток синтаксичні методи представлення інформації мовними засобами XML і його доповнень, призначених для опису типових властивостей елементів XML-документів, їх структури та семантики: рекомендації W3C, що регламентують DTD (Document Type Definition), XML Schema, XQuery (мова запитів до баз XML-даних) і т.д. Інша гілка Семантичного Web пов'язана з напрямками, близькими до галузі штучного інтелекту, і названа онтологічним підходом. Цей підхід включає в себе засоби анування документів, якими могли б скористатися комп'ютерні програми - Web-сервіси та агенти при обробці складних запитів користувачів.

Отже, Семантичний Web можна представити як симбіоз двох напрямів, перше з яких охоплює мови представлення даних. На сьогоднішній день основними такими мовами є XML (eXtensible Markup Language) і RDF (Resource Description Framework). Існує також ряд інших форматів, але XML і RDF надають більше можливостей, тому вони володіють статусом рекомендацій W3C.

Друге, концептуальний напрям несе в собі теоретичне уявлення про моделі предметних областей. Такі моделі предметних областей в термінології Семантичного Web називаються онтологіями. 10 лютого 2004 консорціумом W3C була затверджена й опублікована специфікація мови мережових онтологій OWL (Web Ontology Language). Таким чином, дві гілки Семантичного Web використовують три ключові мови (відповідно, технології):

- Специфікація XML, що дозволяє визначити синтаксис і структуру документів;
- Механізм опису ресурсів RDF, що забезпечує модель кодування для значень, визначених в онтології;
- Мова онтологій OWL, що дозволяє визначити поняття і відносини між ними.

Семантичний Web використовує також й інші мови, технології та концепції, зокрема, універсальні ідентифікатори ресурсів, цифрові підписи, системи логічного висновку і т.д.

Вже сьогодні практично всі відомі компанії рівня IBM, Adobe або Sun Microsystems, активно використовують технологію Семантичного Web у своїх продуктах для вирішення завдань управління даними.

Компанія Microsoft інвестує сотні мільйонів доларів в проект взаємодіючих мережових ресурсів. NET, який відображає їх уявлення про найближче майбутнє Internet. Створювана система дозволяє проводити автоматизований обмін мережевими ресурсами між окремими програмами, додатками, базами даних, користувачами, ґрунтуючись на XML, як на ключовій технології.

Нещодавно в рамках ідеології Семантичного Web була розроблена в School of Electronics & Computer Science (ECS) Університету Саутгемптона була розроблена система mSpace. Програмне забезпечення цієї системи являє собою набір потужних інструментів, що дозволяють збирати дані з різних джерел і організувати інформацію по категоріях і дають змогу користувачеві вільно орієнтуватися в ній.

Розробники наводять наступний приклад. Наприклад, якщо в Google набрати "класична музика", то пошукова система видасть посилання на сайти, які хоч трохи стосуються класичної музики. Якщо ж шукати "класичну музику" на mSpace, то буде

виданий список композицій, які можна тут же завантажити. Інший приклад - по запиті "Гаррі Поттер" користувач отримає не просто набір посилань, а відсортований звіт, в якому частина посилань буде лежати в графі "фільми", інша частина - у колонці "книги", а третя - в колонці "рецензії". Семантичний Web надасть користувачеві можливість вибирати, в якому напрямку досліджувати інформацію, а не просто видавати саме релевантне за загальним алгоритмом.

Список літератури

1. Смирнов А.В., Пашкин М.П., Шилов Н.Г., Левашова Т.В. Онтологии в системах искусственного интеллекта: способы построения и организации (часть 1) // "Новости искусственного интеллекта". – № 1 (49). – 2002.
2. Порівняння ефективності методів індивідуального аналізу даних [Електронний ресурс] / Режим доступу: <http://www.osp.ru/text/print/article/2053324.html>
3. Вираз семантики даних [Електронний ресурс] / Режим доступу: http://citforum.ru/internet/xml/rdf_xml.

УДК 004.738.5

А.С. Богатиренко

Науковий керівник – Сидоренко В.В., ст. викладач
Кіровоградський національний технічний університет

Розробка інформаційної системи сучасного типу на прикладі будівельної організації

Оскільки інтеграція інформаційних систем у всі сфери життя збільшується з кожним днем, то актуально стає розробка подібних баз даних. При цьому розробник повинен враховувати те, що найбільш прості БД можуть бути схильні до надмірності, але при цьому не можна і захоплюватися діленням БД на багато складених таблиць. Також сучасні засоби дружнього інтерфейсу дозволяють розробити інтуїтивно зрозумілі застосування, що є одним з основних вимог замовника. При створенні БД необхідно взяти до уваги область, для якої розробляється база даних.

Якщо вибирати систему управління баз даних (СУБД), то це є складним багатопараметричним завдання і є одним з важливих етапів при розробці додатків баз даних. Обраний програмний продукт повинен задовольняти як поточним, так і майбутнім потребам підприємства, при цьому слід враховувати фінансові витрати на придбання необхідного обладнання, самої системи, розробку необхідного програмного забезпечення на її основі, а також навчання персоналу. Крім того, необхідно переконатися, що нова СУБД здатна принести підприємству реальні вигоди.

Відповідно до завдання слід було створити автоматизовану систему «Маркет будівельних матеріалів», яку найзручніше можна організувати за допомогою баз даних.

База даних повинна вирішувати наступні завдання: облік товару, видача даних, про постачальників і товари, найменування товарів, характеристики, ціни. Реалізувати запити впорядкування по полях: товари, постачальники, ціна. Здійснювати пошук відомостей про фірму-постачальника якогось товару. Робити підрахунок вартості і кількості товару, що залишився в магазині, а також видавати звіт про відсутні товари.

Створена інформаційна система «Маркет будівельних матеріалів» надає наступні можливості для користувачів: занесення нової інформації про товари на складі; оформлення заявки на закупівлю; здійснення продажу товару; отримання інформації про співробітників які працюють на складі (ПІБ, адреса, телефон, посада);

отримання інформації про будь-які операції, які були виконані з товаром. Головна сторінка цієї інформаційної системи зображена на рисунку 1.

За допомогою даної бази даних була зроблена спроба створити оптимальне управління організацією. Вона забезпечує цілісність збережених даних, перешкоджає їх втрати та спотворення. Забезпечує швидкий пошук необхідної інформації, наочність (тому що всі дані представлені в зручному вигляді для користувача). Дозволяє користувачеві вносити зміни (додавати, видаляти непотрібну інформацію).

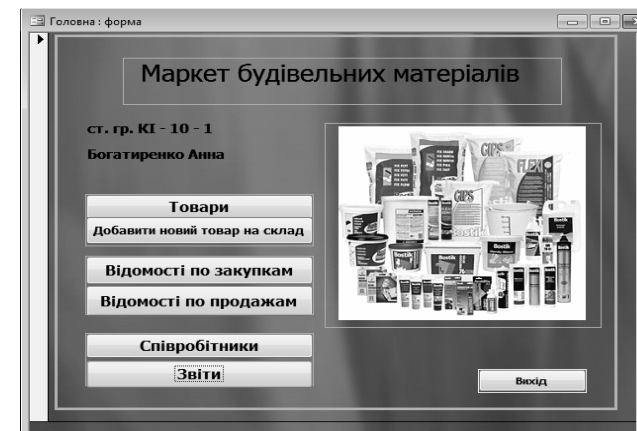


Рисунок 1 – Головна форма будівельної організації

Створена база даних має бути корисна при роботі на будь-якому складі або магазині, що спеціалізується на продажу будівельних матеріалів.

Список літератури

1. Голицина О. Л. Базы данных / Голицина О. Л., Максимов Н. В., Попов И. И. – М.: Форум, 2003. – 352 с.
2. Рудаков А.В. Технология разработки программных продуктов – М.: Академия, 2005. – 208 с.
3. Благодатских В. А. Стандартизация разработки программных средств: Учеб. пособие/ Благодатских В. А., В. А. Волнин, К. Ф. Поскакалов; Под ред. О. С. Разумова. – М.: Финансы и статистика, 2003. – 288 с.

УДК 004.42:004.057.4

Р.А. Бондаренко

Науковий керівник – Дорєнський О.П., викладач
Кіровоградський національний технічний університет

Передача даних мережею за протоколом SSL

Сьогодні Інтернет використовується не тільки для роботи й дозволяти, але й як зручний засіб для укладання угод, у тому числі й фінансових. За допомогою сервісів всесвітньої мережі можливо здійснювати продаж й купувати товарів і послуг, переказувати кошти, тобто здійснювати транзакції такі ж, як і у банківській системі.

Але для того, щоб убезпечитись та бути впевненим у тому, що після здійснення оплати, гроші надійдуть саме до вказаного одержувача, необхідне застосування SSL-

сертифіката. Це є гарантією того, що всі дані, які передаються глобальною мережею, перебувають під захистом, а що є важливим та актуальним.

SSL-сертифікат дозволяє переконатися будь-якому користувачеві у тому, що він належить конкретній організації, а передані дані є захищеними. Визначити такий сайт можна за піктограмою замка. Під час входу на такий ресурс, сервер і браузер клієнта обмінюються ключами. Захищене з’єднання завжди здійснюється за протоколом https, тому вся інформація передається в зашифрованому й розшифровуються за допомогою спеціального ключа.

Таким чином, розробка програмного забезпечення системи передачі даних у мережі за протоколом SSL, є актуальною задачею.

Для програмної реалізації системи запропоновано функціональну схему, що наведена на рисунку 1.

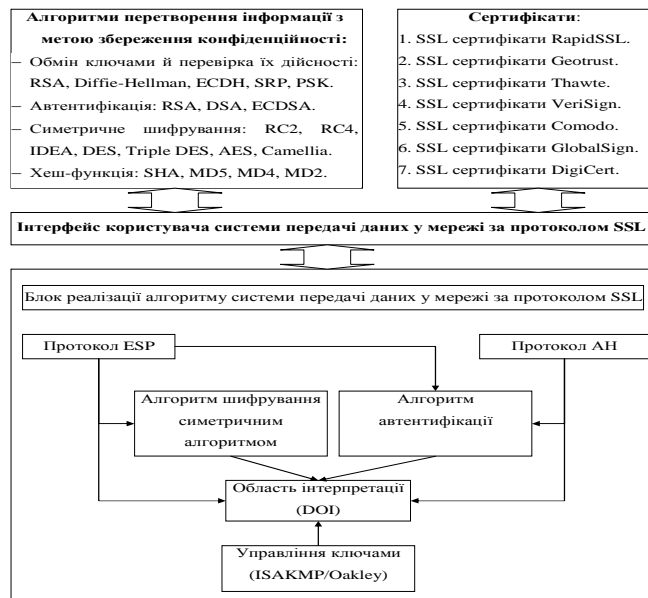


Рисунок 1 – Функціональна схема системи передачі даних у мережі за протоколом SSL

Функціональні блоки розробленого програмне забезпечення системи передачі даних у мережі за протоколом SSL реалізовано на основі наступних алгоритмів: RSA, Diffie-Hellman, ECDH, SRP, PSK для обміну ключами й перевірки їхньої дійсності; RSA, DSA, ECDSA для автентифікації; RC2, RC4, IDEA, DES, Triple DES або AES, Camellia для симетричного перетворення інформації з метою збереження конфіденційності; SHA, MD5, MD4 і MD2 для хеш-функцій.

Для здійснення SSL-з’єднання необхідно, щоб сервер мав інстальований цифровий сертифікат – файл, що унікально ідентифікує користувача і сервер. Це – свого роду електронний паспорт, що проводить автентифікацію сервера до того, як встановлюється сеанс SSL-з’єднання. Цифровий сертифікат незалежно підписується й засвідчується третьою стороною, що гарантує його достовірність. У ролі такої третьої сторони виступають центри сертифікації, наприклад, компанія “Thawte”.

Запропоноване ПЗ для встановлення захищеної сесії забезпечує перевірку, щоб доменне ім’я в сертифікаті відповідало тому домену, від якого йде запит на захищене з’єднання; сертифікат не був прострочений; сертифікації, що підписала сертифікат домену, входив до числа довірених Web-браузера.

Список літератури

1. Балакирский В.Б. Безопасность электронных платежей. Защита информации – Конфидент, № 5, 1996.
2. Бернет С., Пэйн С. Криптография. Официальное руководство RSA Security. М.: Бином-пресс, 2002.
3. Бруно Л. Certificate Authorities: Кому Вы доверяете? Data Communications (Russian edition). № 3, 1998.
4. Галатенко В.А. Информационная безопасность. Обзор основных положений. Jet Info. № 1-3, 1996.
5. Галатенко В.А. Стандарты в области безопасности распределенных систем. Jet Info, № 5, 1999.
6. Галатенко В.А. Основы информационной безопасности. – М.: ИНТУИТ.РУ – “Интернет-университет информационных технологий”, 2003.

УДК 004.056.55

В.О. Гаража

Науковий керівник – Доренський О.П., викладач
Кіровоградський національний технічний університет

Створення архівів у файлової системі NTFS з розмежуванням доступу за допомогою алгоритму AES

Програми для стиснення даних почали розроблятися одночасно зі створенням перших персональних комп’ютерів, адже ще тоді постійно відчувалася недостача вільного місця на жорстких дисках. Як правило, користувачі стискають текстові документи, рідше – фотографії і відеодані, тому що в останньому випадку виграш у вільному місці виявляється зовсім невеликим. Процес створення архіву називають архівацією або упакованням, а зворотній процес – розпакуванням або екстракцією [1].

Проте під час перенесення архівів портативними носіями або передачі їх мережею гостро постає питання безпеки заархівованої інформації. Тому задача забезпечення розмежування доступу до архівів є актуальною.

Метою роботи є розробка програмного забезпечення створення архівів у файлової системі NTFS з розмежуванням доступу.

Аналіз [2-5] показав, що серед найпоширеніших алгоритмів шифрування оптимальними з погляду специфіки їх роботи, рівня захисту та простоти імплементації є алгоритми AES та RSA. Водночас, симетричний алгоритм AES, наприклад, відповідно до дослідження [4], має значно кращу часову характеристику: якщо 1 Мб даних асиметричний RSA шифрує за 7,5 сек., то AES – за 0,51 сек. Тобто програмна реалізація криптографічних перетворень над даними на основі алгоритму AES є більш ніж в 10 разів швидша ніж при використанні RSA. Таким чином, алгоритм AES можна вважати доцільним для програмної реалізації з метою подальшого впровадження і використання, що є актуальною задачею. Також слід відзначити, що Rijndael стандарту AES – це швидкий і компактний алгоритм з простою математичною структурою, завдяки чому він є простим для аналізу під час оцінювання рівня захисту.

Отже, можна впевнено зробити висновок, що для розробки програмного забезпечення створення архівів у файлової системі NTFS з розмежуванням доступу є доцільним застосування саме алгоритму AES, відомого ще під назвою Rijndael [3].

Розробку ПЗ створення архівів у файлової системі NTFS з розмежуванням доступу за допомогою AES пропонується здійснити відповідно до розробленої структурної схеми, яку наведено на рисунку 1.

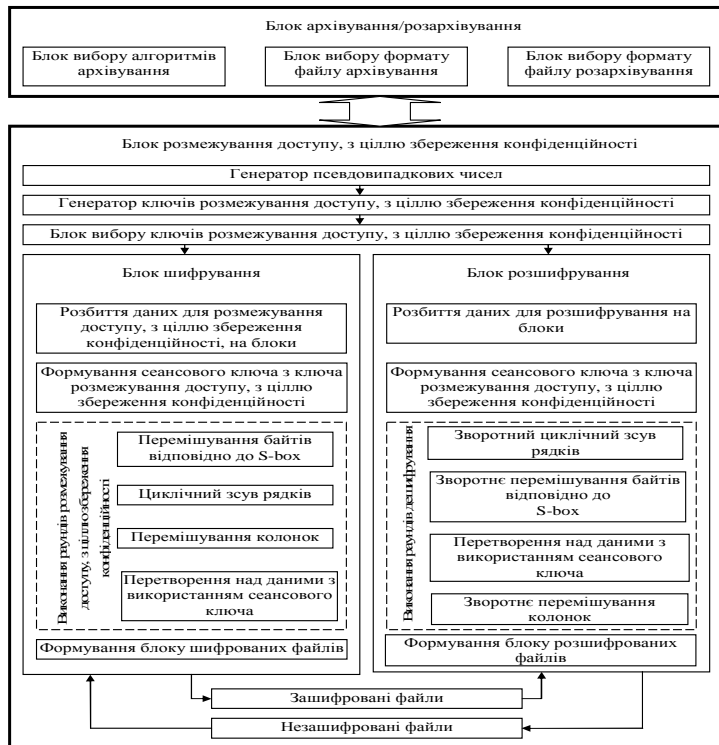


Рисунок 1 – Структурна схема ПЗ архівування у файлової системі NTFS з розмежуванням доступу за допомогою AES

У роботі [6] досліджено особливості програмної реалізації алгоритму AES. Слід відзначити, що AES є нетрадиційним блоковим шифром, оскільки не використовує мережу Фейштеля для криптоперетворень [7]. Він оперує 128-бітними блоками даних і довжиною ключа розрядністю 128, 192 або 256. Вхідні, проміжні і вихідні результати перетворень, що виконуються в рамках алгоритму, називають станами (state) [8], які можна представити матрицею $4 \times N_b$ (N_b – кількість 32-бітних слів вхідного блоку), елементами якої є чотири рядки по N_b байт в порядку $S_{00}, S_{10}, S_{20}, S_{30}, S_{01}, S_{11}, S_{21}, S_{31}$ і т.д. Ключ шифрування, як і масив State [7], представляється прямокутним масивом (матрицею) з чотирма рядками.

До основних особливостей AES, який специфікує алгоритм Rijndael [5, 7], та його програмної реалізації можна віднести те, що він є симетричним блоковим шифром, який працює з блоковими даними довжиною 128 біт та використовує ключі 128, 192 і 256 біт (версії AES-128, AES-192, AES-256) [7]. Дослідження [5] показали, що однією з особливостей програмної реалізації і важливою перевагою з погляду криптостійкості, впровадженні й практичного застосування зазначеного алгоритму є

також те, що він може працювати і з іншими довжинами блоків даних та ключів. Хоча така можливість не входить до стандарту [3], проте вона може бути ефективно застосована на практиці.

Особливості програмної реалізації AES також впливають з особливостей самого алгоритма. Серед них, зокрема, слід відзначити нову архітектуру “Квадрат”, що забезпечує надшвидке “розсіювання” та “перемішування” інформації, при чому за один раунд перетворенню підлягає весь вхідний блок [5]. Крім того в алгоритмі застосовується байт-орієнтована структура, що під час програмної реалізації процесу шифрування забезпечує розробку на 8-розрядних мікроконтролерах. Варто відзначити одну з найважливіших особливостей AES: ефективна апаратна та програмна реалізація на різноманітних платформах. Зокрема важливим для програмної реалізації AES є те, що у структурі алгоритму закладена можливість паралельного виконання операцій, що на багатопроцесорних ЕОМ дозволить збільшити швидкість шифрування у кілька разів.

Список літератури

1. Тарасов О.В. Обзор та порівняльний аналіз методів стиснення інформації / О.В. Тарасов, Є.В. Оношко // Системи обробки інформації. – 2011. – Вип. 7 (97) – С. 64-67.
2. Бурачок Р.А. Використання симетричних алгоритмів шифрування при передаванні мультимедійних даних / Р.А. Бурачок, П.О. Гуськов, Р.І. Бак // Радіоелектроніка та телекомунікації. – 2012. – № 738. – С. 156-160.
3. Баричев С.Г. Стандарт AES. Алгоритм Rijdael / Баричев С.Г., Гончаров В.В., Серов Р.Е. // Основы современной криптографии. – М.: “ГЛ-Телеком”, 2002. – 247 с.
4. Дудикевич В. Б. Розробка клієнт-орієнтованих засобів шифрування абонентських даних в мобільному зв’язку / В.Б. Дудикевич, Ю.Л. Пархучь // Інформаційна безпека. 2011.–№1(5).–С. 83-87.
5. Фисун С.Н. Методика шифрования данных с использованием программно-методического комплекса VisualAES / С.Н. Фисун, А.И. Копылов // Радіоелектроніка і комп’ютерні системи. – 2012. – № 5 (57). – С. 83-85.
6. Гаража В.О. Особливості програмної реалізації алгоритму AES / В.О. Гаража, О.П. Доренський // Актуальні задачі сучасних технологій: збірник тез доповідей Міжнародної науково-технічної конференції молодих учених та студентів, 19–20 грудня 2012 р., м. Тернопіль – Тернопіль: Вид-во ТНТУ ім. Івана Пулюя, 2012. – С. 184-185.
7. Основы зашиту информации: Навч. посібник. / [Смірнов О.А., Віхрова Л.Г., Осадчий С.І. та ін.]. – Кіровоград: РВЛ КНТУ, 2011. – 322 с.
8. Панасенко С.П. Алгоритмы шифрования. Спец. справочник / С.П. Панасенко. – СПб.: БХП Петербург, 2009. – 576 с.

УДК 004.4

Д.О. Давидов

Науковий керівник – Сидоренко В.В., ст. викладач
Кіровоградський національний технічний університет

Програмне забезпечення системи формування фільтрів від фішингу в мережі Internet

Найбільш розвинутою формою шахрайства в Інтернеті, безсумнівно, є фішинг. Зловмисники використовують перехоплювачі клавіатури, поштові повідомлення, складені за всіма правилами соціальної інженерії, спеціально розроблені сайти й інші засоби.

Усе більше винахідливими стають атакуючі, усе вище рівень їхньої підготовленості. Фішинг (phishing) – вид інтернет-шахрайства, що полягає в

розсиланні електронних повідомлень із метою крадіжки конфіденційної інформації (як правило, фінансового характеру).

Фішинг-повідомлення складаються таким чином, щоб максимально походити на інформаційні листи від банківських структур або компаній з відомими брендами. Листи містять посилання на свідомо помилковий веб-ресурс, спеціально підготовлений зловмисниками і є копією сайту організації, від імені якої відправлений лист.

На даному фальшивому сайті користувачеві пропонується ввести, наприклад, номер своєї кредитної карти й іншу конфіденційну інформацію.

Отже, розробка програмного забезпечення системи формування фільтрів від фішингу в мережі Internet є актуальною задачею, яка потребує розв'язку.

Список літератури

1. Гайкович В., Першин А., Безопасность электронных банковских систем. – Москва.: Единая Европа, 2002.
2. Галатенко В., Информационная безопасность, «Открытые системы». – М.: Азбука-Книга, 2005.

УДК 004.4

В.В. Джебко

Науковий керівник – Сидоренко В.В., ст. викладач
Кіровоградський національний технічний університет

Програмне забезпечення системи контролю та керування доступом з використанням смарт-карт за технологією RFID

Принцип комплексного «інтелектуального» управління всіма життєво важливими функціями житлових і промислових об'єктів, практична реалізація якого стала можливою завдяки застосуванню інтегрованих слабкострумових систем, знаходить сьогодні все більшу популярність.

Особливе значення при цьому мають спеціальні програмно-апаратні комплекси, призначені для забезпечення безпеки, і, насамперед, – системи контролю й управління доступом, або, скорочено СКУД.

Що являють собою системи контролю доступу? Загалом їх можна охарактеризувати як призначені для здійснення контролю й управління доступом як безпосередньо на об'єкт у цілому, так і на його окремі ділянки, комплекси, що поєднують у своєму складі організаційно-адміністративні заходи й великий перелік програмно-технічних засобів.

Крім властиво управління доступом з метою попередження проникнення на об'єкт небажаних осіб, функція системи контролю доступу може полягати також у спостереженні за обслуговуваним персоналом, включаючи пересування в межах території об'єкта, моніторинг періоду перебування на робочому місці, раціональність використання робочого часу й т.д. Установка систем контролю доступу й у житлових приміщеннях не менш затребувана, чим на господарських об'єктах, просто домашні системи, як правило, відрізняються більшою простотою й меншою кількістю інтегрованих у їхній склад функціональних елементів.

Таким чином, виходячи з вищеперерахованого, розробка програмного забезпечення системи контролю та керування доступом з використанням смарт-карт за технологією RFID є актуальною задачею.

Список літератури

1. Автоматизированная Система Контроля Доступа SmartMonitor Plus V1.1.0/ Руководство пользователя. Минск.
2. О системах контроля доступа. М.: ТЕХИНВЕСТ – 2004 <http://www.sistema-dostupa.ru>
3. Системы управления доступом. М.: ТЕХИНВЕСТ – 2004 <http://www.sistema-dostupa.ru>
4. Требования разработки и внедрения СКД. М.: ТЕХИНВЕСТ – 2004 <http://www.sistema-dostupa.ru>
5. ПЗ для систем контроля доступа. М.: ТЕХИНВЕСТ – 2004 <http://www.sistema-dostupa.ru>

УДК 004.725.4

Д.І. Кулик

Науковий керівник – Павлик С.І., канд. фіз.-мат. наук, доцент
Запорізька державна інженерна академія

Масштабно-інваріантна поведінка процесу зростання комп'ютерних мереж

Еволюція складних мереж та розповсюдження сигналів нею останнім часом обґрунтовано привертає велику увагу з точки зору можливого застосування до аналізу усесвітньої павутини (World Wide Web), яка трактується як розподілена система, що надає доступ до зв'язаних між собою документів, розташованих на різних комп'ютерах, підключених до Інтернету [1]. Крім того, такі складні мережі описують різні системи, що зустрічаються в природі і суспільстві. За традицією ці системи моделюються як випадкові графи з відносно примітивною і жорсткою структурою. Але ці моделі не завжди демонструють топологічні і структурні властивості, що відображуються в реальних прикладах мереж. Це пов'язано з певною обчислювальною складністю при їх комп'ютерному моделюванні. Основна проблема - виявити закономірності в поведінці складної мережі при зміні її масштабу. Для цього існує розвинений теоретичний підхід, пов'язаний з масштабно-інваріантними властивостями складних систем (так званий скейлінг).

Вживання концепції скейлінга для моделювання поведінки випадкових мереж вже обговорювалася в ранній роботі [2]. Проте, складність моделювання випадкових систем заставляє шукати простіші моделі, на основі аналізу яких можна відповісти на низку запитань, які виникають в реальній поведінці, наприклад, усесвітньої павутини. Для цієї мети ми використовуємо модель ZRP (zero-range process) [3] разом із спробою інкорпорувати в неї концепцію скейлінга. Основні особливості використання моделі ZRP в нашому завданні полягають в наступному. Уявимо собі одновимірний ланцюжок з певним числом вузлів L , у вузлах якого може знаходитися довільне число частинок $h(x, t)$, де x - номер вузла від початку, t - час. На перший вузол частинка заходить з вірогідністю p , з останнього вузла вирушає з вірогідністю q . Між вузлами частинки здійснюють переходи з вірогідністю $u(h)$. Завдання полягає в обчисленні

$W(L, t) = \sqrt{q} h(x, t) - \mathfrak{h}(x, t) c^2 c$, де $\mathfrak{h}(x, t) c = e^{-h(x, t)/L}$, сумування - по вузлах

x . Ґрунтуючись на даних математичного моделювання і на аналогії з масштабно-інваріантними законами в теорії фазових переходів, раніше (див. [4-5]) запропоновано

вираз $W(L, t) = L^a f(t/L^z)$, де функція $f(x)$ визначається наступними асимптотичними виразами: $f(x \gg 1) \approx const \cdot x^{-b}$, $b = a/z$. Завдання дослідження – є обчислення таких скейлінгових показників. Для цього було проведено стохастичне моделювання з використанням оригінальної комп’ютерної програми на C++.

Звичайно, змінюючи параметри можна отримати незлічену безліч результатів. Тому необхідно виділити такі області в параметричному просторі, в яких система демонструє скейлінгову поведінку. На жаль, це досягне лише методом перебору, який вельми скрутний хоч би тому, що окремий чисельний розрахунок займає досить-таки тривалий час. Але ми виявили, що більшість результатів підтверджує масштабно-інваріантну поведінку для функції $W(L, t)$. Більш цього, при деяких параметрах спостерігається спадання цієї функції із часом. Але звичайна поведінка у більшості чисельних розрахунків - зростання із степеневим законом, яке переходить до насичення. Як приклад, приведемо результати для наступних значень параметрів. Отже, задаємо вірогідність: $u(h) = \sin(p^h/2H)$, $p=0.5$, $q=0.53$, де H – максимально можливе число частин в вузлі. В такому випадку $W(L, t)$ на початковому етапі зростає з часом як $t^{0.64}$, потім виходить на насичення $L^{0.34}$. Схожі закономірності було отримано і при іншому виборі параметрів. У всіх випадках було підтверджено скейлінгову поведінку середньоквадратичного відхилення заповнення сайтів.

Складаючи прогноз для розвитку усесвітньої павутини, необхідно брати до уваги, що мережа може зростати нескінченно, але середньоквадратичне відхилення заповнення сайтів зростатиме в часі, хоча потім виходить на насичення.

Список літератури

1. Barabasi A.L. The Structure and Dynamics of Networks / Barabasi A.L., Newman M., Watts D.J. - Princeton University Press, 2006. – 624 p
2. Barabasi A.L. Emergence of scaling in random networks / A.L. Barabasi, Réka Albert // Science. - 1999. - Vol. 286. - №. 5439. - P509-512.
3. Evans M. R. and Hanney T. Nonequilibrium statistical mechanics of the zero-range process and related models / M. R. Evans, T. Hanney // Journal of Physics A: Mathematical and General. - 2005.-Vol. 38.-№19.- R.195.
4. Barabasi A.L. Fractal Concepts in Surface Growth / A.L. Barabasi, H.E. Stanley. - Cambridge : Cambridge University Press, 1995. – 405 p
5. Family F. Scaling of the active zone in the Eden process on percolation networks and the ballistic deposition model / F. Family, T. Vicsek // Journal of Physics A: Mathematical and Theoretical. –1985.–V.18, № 2.–P. 75-81.

УДК 004.738.5

С.М. Дерполюк

Науковий керівник – Сидоренко В.В., д-р техн. наук, професор
Кіровоградський національний технічний університет

Система моніторингу динаміки успішності студентів на основі мобільної платформи

Традиційна система моніторингу динаміки успішності, що існує в Україні, потребує особливих методів вирішення цієї проблем, з точки зору комп’ютеризації. Системи моніторингу динаміки успішності можуть сприяти створенню нової культури організації в навчальних закладах, зробивши роботу викладацького та обслуговуючого

персоналу більш легкою, цікавою і значимою [2].

Моніторинг динаміки успішності – високотехнологічний і прогресивний підхід до суттєвого підвищення ефективності роботи навчальної частини. Система управління базами даних надає повний контроль над процесом визначення даних, їх обробкою та використанням, також істотно полегшує обробку великих об’ємів інформації, які зберігаються в багаточисленних таблицях.

На даний час розроблено багато автоматизованих систем управління навчальним процесом серед яких:

1. Інформаційно-аналітична система керування вищим навчальним закладом «Університет», розроблена в Херсонському державному педагогічному університеті.
2. Автоматизована система керування вищим навчальним закладом АСК «ВНЗ», розроблена Науково-дослідним інститутом Прикладних інформаційних технологій Кібернетичного центру Національної академії наук України.
3. «ВНЗ АЛЬМА-МАТЕР» товариства з обмеженою відповідальністю «Direct IT».
4. Комп’ютерна система «Деканат», розроблена приватним підприємством «Політек-софт»[1].

Недоліком розглянутих систем є їх надмірна складність в управлінні та введенні даних. Також вони не відображають динаміку успішності студента та відсутність підтримки мобільних платформ. В роботі на основі огляду існуючих систем здійснюється постановка вимог і основних задач, які повинна вирішувати система аналізу динаміки успішності студентів в учбовому процесі.

В розробленій системі вирішуються поставлені задачі. Основною перевагою системи є доступ до бази даних з пристрою на мобільній платформі. Це дозволить користувачу отримувати потрібну інформацію в будь-якому місці.

Список літератури

1. Кузьма К.Т. Аналіз автоматизованих систем управління вищим закладом освіти [Електронний ресурс]: збірник наукових праць, том 12 / Актуальні проблеми автоматизації та інформаційних технологій // Дніпропетровський національний університет ім. Олеся Гончара, 2008. Режим доступу до журн. : www.nbu.gov.ua/portal/natural/Akpa/2008_12/12.pdf
2. <http://uk.wikipedia.org/>

УДК 343.1:342.534.2+006.424(477)

Т.М. Івасишин, Ю.П. Михальчук

Національна академія Служби безпеки України

Проблемні питання використання автоматизованої системи «клієнт-банк» у розслідуванні кримінальних правопорушень

Стрімкий розвиток та використання інформаційно-комунікаційних технологій має вирішальне значення для переходу від індустріального до постіндустріального, інформаційного суспільства, відкриваючого широкі можливості для прогресивного розвитку людини, суспільства, держави та міжнародного суспільства в цілому, розповсюдження процесів демократизації.

Ефективність діяльності з розслідування злочинів залежить від багатьох чинників. Особи, які її здійснюють, стикаються з широким колом проблем різного

характеру: правового, організаційного, технічного, професійного та ін. Серед обставин, що можуть негативно вплинути на всебічність, повноту й об'єктивність розслідування кримінальної справи, є використання особливостей автоматизованої системи «клієнт-банк» у розслідуванні кримінальних правопорушень.

Одним із класичних визначень автоматизованих систем «клієнт-банк» можна вважати таке: «клієнт-банк» – це система дистанційного банківського обслуговування поточних рахунків клієнтів, яка функціонує з використанням спеціального програмного забезпечення.

Слід зауважити, що автоматизована система «клієнт-банк» є лише частиною (підсистемою) того програмного забезпечення, яке використовує будь-який банк у своїй діяльності – АБС (автоматизована банківська система). На сьогодні банки України використовують кілька десятків різних АБС, як власного виробництва, так і відомих іноземних фірм (R-style, Scrooge, Rs-bank, Б2 та інших). До всіх із них без винятку входить підсистема дистанційного банківського обслуговування «клієнт-банк». Ще в 1995 році Національний банк України видав спеціальну Постанову й Уточнення до неї, де вперше виклав обов'язкові вимоги до всіх систем «клієнт-банк», які можуть застосовуватися в банківських установах України [1]. У загальному вигляді вони були викладені в главі 11 «Інструкції про безготівкові розрахунки в Україні в національній валюті» [2]. Зазначені нормативні акти чітко визначають процес взаємодії клієнтів зі своїм банком за допомогою автоматизованих систем дистанційного керування розрахунковим рахунком.

За структурою й основним призначенням для користувача характеристики системи «клієнт-банк» можна поділити на два великих типи. Перший вимагає установки на комп'ютері клієнта спеціального програмного забезпечення, з допомогою якого створюються різного роду платіжні та інші документи, які потім зашифровуються й передаються в банк по каналах зв'язку (модем, Інтернет). У цьому випадку процес роботи з документами не вимагає з боку клієнта постійного й безпосереднього з'єднання з банком. Таке з'єднання необхідне лише на час прийому і передачі інформації (платіжних документів, виписок про стан рахунку, заявок на купівлю валюти й тому подібне). Такі клієнт-банки називають оф-лайновими.

На противагу оф-лайновим «клієнт-банкам» в останні кілька років, із розвитком інтернет-технологій, набули розвитку й он-лайн «клієнт-банки». Під час роботи з ними необхідне постійне з'єднання із сервером банку й найчастіше взаємодія між користувачем системи клієнт-банк і самим банком відбувається через веб-сайт банку. За своїми функціональними можливостями обидва типи «клієнт-банків» нині практично ідентичні.

Знання того, до якого типу належить «клієнт-банк» у кожному конкретному випадку, дуже важливо, оскільки від цього залежить і той об'єм інформації про роботу конкретного клієнта, яку можна витребувати в банківській установі.

У практичній діяльності інколи необхідно визначити сам факт здійснення тих або інших фінансових операцій за допомогою системи «клієнт-банк», а також коли, хто і звідки їх провадив.

У разі використання системи «клієнт-банк» у протиправних цілях документи, що надаються в банк, можуть бути підробленими. Найчастіше з цією метою оформляється договір на приватного підприємця, який працює без печатки. Характерною ознакою також є оформлення всіх документів і відкриття рахунку за генеральним дорученням. При створенні групи фірм із метою відмивання коштів вони можуть реєструватися протягом короткого проміжку часу за однією юридичною адресою. Це відображено в документах, що зберігаються в банку.

Розглянемо питання технології роботи системи «клієнт-банк» із погляду того об'єму інформації, який може допомогти ідентифікувати справжніх осіб, що працюють із системою.

Насамперед зауважимо, що окрім згаданих вище юридичний документів, у банківській установі залишається вся інформація про рух коштів на рахунках клієнтів. За необхідності банк за рішенням суду в рамках розслідування тієї або іншої кримінальної справи зобов'язаний офіційно надати цю інформацію в повному обсязі. До цієї інформації належить весь обсяг даних, який міститься в стандартних платіжних дорученнях, заявках на купівлю-продаж валюти і так далі.

За потреби ґрунтовного вивчення ситуації необхідно витребувати в банківській установі також додаткову інформацію. У зв'язку з цим важливо врахувати використання виду клієнт-банк (оф-лайн або он-лайн).

Так, наприклад, якщо особа, яку шукають користувалася модемним зв'язком при передачі інформації в банк, то необхідно отримати інформацію про те, в який час (із точністю до секунд) і на які номери телефонів банку здійснювалися дзвінки. Якщо для з'єднання використовувався Інтернет, то на відповідних серверах зв'язку банку зафіксовані IP-адреси, з яких ініціювалися сеанси зв'язку. За цією інформацією інколи можна встановити місце перебування осіб у момент їх роботи в системі «клієнт-банк», а також їх інтернет-провайдерів. Особливу цінність має сукупність такої інформації. Це інколи дає змогу виявити приховані моменти взаємозв'язків між розрізненими організаціями (якщо, наприклад, зв'язок від різних організацій ініціювався з тих самих телефонних номерів або IP-адрес).

При взаємодії з банком, у якому перебував на обслуговуванні підозрюваний, слідчому або оперативному співробітнику потрібно передусім скласти перелік питань, відповіді на яких необхідно отримати в процесі взаємодії з працівниками банку. Досить часто вони, посилаючись на необхідність збереження банківської таємниці, вельми неохоче йдуть на особисті контакти. Тому попередній перелік питань украй необхідний, оскільки дає змогу включити їх у постанову суду на проведення вилучення відповідних документів. Необхідно мати на увазі, що поряд зі співробітниками розрахунково-касових відділів банку, з клієнтами, котрі працюють із системою «клієнт-банк» безпосередньо співпрацюють і співробітники комп'ютерних відділів (відділів автоматизації) банку. Саме вони інколи виїжджають безпосередньо до клієнта для встановлення необхідного програмного забезпечення, дають консультації по телефону і тому подібне. Особливо часто таке відбувається, якщо банківська установа використовує оф-лайновий тип системи «клієнт-банк».

Якщо є можливість, то досить цінну інформацію можуть дати також і деякі співробітники організації, яка працювала із системою «клієнт-банк». Тут необхідно акцентувати увагу на їхній кількості і персональному складі. Зазвичай в організаціях до системи «клієнт-банк» мають доступ перші особи організації, а також деякі співробітники, котрі мають справу з бухгалтерією підприємства. Важливу інформацію можуть дати й технічні фахівці, котрі відповідають за комп'ютерне забезпечення і зв'язок. Необхідно врахувати, що інколи всю бухгалтерську інформацію зберігають у зашифрованому вигляді, недоступному для явного перегляду. Деякі бухгалтерські облікові системи, включаючи і «клієнт-банк», можуть фізично розміщуватися на змінних носіях, що дає змогу в разі потреби швидко переміщати їх в інші місця зберігання. За наявності інших ознак цей факт може вказувати на здійснення з їх допомогою протизаконних операцій.

Таким чином, автоматизована система віддаленого банківського обслуговування системи «клієнт-банк», незважаючи на все різноманіття можливих варіантів її реалізації та сучасний характер послуг, що надаються, несе в собі потенційні

можливості для знеособлення клієнтів, котрі, послугуючись нею, здійснюють фінансові операції. У зв'язку з цим необхідно враховувати особливості її функціонування та наявність потенційних можливостей здійснення з її допомогою незаконних дій.

Стосовно завдання доказування факту злочину та вини особи, яка вчинила комп'ютерний злочин, криміналістичному аналізу підлягає сукупність різноманітних об'єктів, що пов'язані з цим злочинним проявом, встановлення і аналіз яких дає можливість отримати дані щодо особи злочинця, мети, мотивів і способу його злочинних дій, обстановки й механізму вчинення злочину й слідів як наслідків злочинних дій, розміру завданої шкоди та інших обставин вчиненого, котрі підлягають доказуванню. Здійснення такого аналізу дає змогу визначення напрямів розслідування та формування системи доказів у справі.

Список літератури

1. Постанова Національного банку України № 106 від 12 травня 1995 року й Уточнення до неї № 24-313/17 від 9 лютого 1996 року.
2. Інструкція про безготівкові розрахунки в Україні в національній валюті, затверджена Постановою НБУ № 22 від 21 січня 2004 року.

УДК 004.519.226.5

О.О. Іванченко

Науковий керівник – Якименко Н.М., канд. фіз.-мат. наук, доцент
Кіровоградський національний технічний університет

Прогнозування футбольних матчів у режимі віддаленого доступу за допомогою засобів статистики та моніторингу баз даних

Одним із ключових завдань удосконалення інформаційних комунікацій є завдання дослідження (моніторингу) та аналізу деякої інформації. Для реалізації поставленої задачі використовуються мережні бази даних, що знаходяться на певному сервері і містять великі об'єми інформації. Використання таких баз дозволяє легко, а головне швидко поповнювати обсяги даних на дисковому просторі серверу, які можна одразу використовувати в режимі віддаленого доступу. Головною перевагою використання саме мережних баз даних є висока швидкість роботи з ними. Іншою задачею є розробка зрозумілого та зручного інтерфейсу користувача, який може легко та без зусиль отримати необхідну йому інформацію, не застосувавши при цьому введення специфічних команд або термінів[4]. Глобалізація Інтернету серед населення сприяє тому, що кінцевий програмний продукт матиме вигляд Інтернет-сайту зі зрозумілим оформленням, з яким буде легко працювати.

Метою роботи є створення мережної бази даних спортивних результатів, автоматизація аналізу статистичної інформації.

У відповідності метою роботи було сформульовано основні наукові задачі:

- вибрати та обґрунтувати технологію обробки даних;
- вибрати та обґрунтувати методику аналізу статистичної інформації;
- розробити програмне забезпечення моніторингу мережної бази даних спортивних результатів з аналізом статистичної інформації.

Наукове значення роботи полягає у вдосконаленні процесу аналізу статистичної інформації. Було отримано такі наукові результати:

- вперше в Україні була автоматизована методика аналізу статистичної інформації за допомогою засобів статистики, що виводить результати через інтерактивну мережу;
- вперше реалізовано можливість аналітичного прогнозування статистичної інформації без урахування людського фактору.

Поставлені задачі розв'язуються за допомогою моделі нормальних помилок, непараметричної оцінки точності прогнозу і довірчої границі для нього з використанням кваліметричного методу. Кваліметрія - наукова дисципліна, в рамках якої вивчаються методологія і проблематика комплексної, кількісної оцінки якості об'єктів будь-якої природи. В даному випадку проводиться рейтингова оцінка двох футбольних клубів, що беруть участь у матчі[9].

Моніторинг мережної бази даних може бути реалізований як на сервері безпосередньо, так і в режимі віддаленого доступу. Інформація, для перегляду якої користувач відправив запит, виводиться у вигляді сторінки веб-сайту. Прогнозування відбувається наступним чином:

– після завершення моніторингу бази даних[5] система отримує певні числові значення (вагові коефіцієнти);

– розраховується відносний рейтинг команд[7].

Для розрахунку необхідно виконувати ряд дій[8,9]:

1. Розрахувати відносну вагу показника для кожної команди. Для цього треба використати формулу (1) для показників-стимуляторів і формулу (2) для показників-дестимуляторів:

$$Brel_i = \frac{B_i}{\sum_{j=1}^2 B_j} \quad (1),$$

де B – вихідне значення показника, i – команда, Brel – відносне значення показника.

$$Brel_i = 1 - \frac{B_i}{\sum_{j=1}^2 B_j} \quad (2),$$

2. Розрахувати рейтинг команд за формулою (3).

$$Ra_i = Mrel_i^T \cdot W \quad (3),$$

де W – матриця вагових коефіцієнтів, Mrel – матриця, що містить відносні значення показників Brel для кожної команди, i – команда, Ra - рейтинг команди.

3. Для зручності порівняння нормується рейтинг команд на одиницю за формулою (4).

$$Rrel_i = \frac{Ra_i}{\sum_{j=1}^2 Ra_j} \quad (4),$$

де Ra - абсолютний рейтинг команди, i – команда, Rrel – рейтинг команди, нормований на одиницю.

Для інтерпретації отриманого рейтингу команд необхідно ввести так звану лінгвістичну інтервальну шкалу. У кваліметрії шкала вимірювань є засобом

адекватного зіставлення і визначення чисельних значень окремих властивостей і якостей відмінності об'єктів. У даній моделі використовується п'ятирівнева лінгвістична шкала, наведена в таблиці 1.

Таблиця 1 – Рівні шкали виведення результатів

Результат	Рейтинг команди
Перемога	$X > 75\%$
Перемога нічия	$55\% < X \leq 75\%$
Нічия	$45\% \leq X < 55\%$
Поразка нічия	$25\% \leq X < 45\%$
Поразка	$X < 25\%$

Дане програмне забезпечення має простий, дружній та зручний інтерфейс користувача, що забезпечує легкість у освоєнні роботи програмного продукту, зручність у використанні, і не потребує особливих спеціальних знань.

При створенні програмного забезпечення було використано об'єктно-орієнтований підхід, що відповідає сучасним тенденціям у галузі розробки комерційних програмних систем та було досліджено методи обробки та аналізу даних, в результаті чого було обрано найменш громіздкий, швидкодіючий та ефективний процес аналізу та прогнозування даних і процес моніторингу мережної БД із застосуванням архітектури «клієнт-сервер».

Список літератури

1. Джейсон Ленгсторф «PHP и jQuery для профессионалов» – Вильямс, 2011. - 334 с.
2. Давид Фланаган «JavaScript: Подробное руководство» – Вильямс, 2008. - 982 с.
3. Дейв Крейн, Эрик Паскарелло, Даррен Джеймс «Аjax в действии» – Диалектика, 2006. - 640 с.
4. Келли Мэрдок «JavaScript. Наглядный курс создания динамических Web-страниц» – Директ, 2004.-288 с.
5. П. Дюбуа «MySQL» – Вильямс, 2004- 1056 с.
6. Дронов С.В. «Многомерный статистический анализ» –Изд-во Алт. гос. унив., 2003. – 213 с.
7. Вуколов Э.А. «Основы статистического анализа» –ФОРУМ, 2008, 464 с.
8. Костин А.В. «Квалиметрический анализ и рейтинг» –ФОРУМ, 2010, 169 с.
9. Полозов А. А. «Статистика и спорт» –Институт физической культуры, 2007, 207 с.

УДК 004.772

В.В. Зубенко

Науковий керівник – Помазан Л.В., канд. техн. наук, доцент
Кіровоградський національний технічний університет

Програмне забезпечення антивірусної перевірки НТТР-трафіку смартфонів на базі ОС Android

В сучасному світі комп'ютерні віруси заважають користувачам по усьому світу, і більш 20 років антивірусні експерти борються з ними. За цей час антивірусні програми пройшли шлях від аматорських до комерційних пакетів, що приносять своїм авторам мільйони доларів.

В теперішні часи загроза атаки комп'ютерним вірусом мобільної платформи складає 95% в перші часи роботи з Інтернет контентом. Характерною рисою сьогодення є не тільки величезний збиток, який наносять вірусні атаки, але і ріст числа самих шкідливих кодів. Відзначу, що в 2013 році ріст популярності

комп'ютерних шкідників придбав просто підричний характер. Особливо під ОС Android. Це операційна система і платформа для мобільних телефонів та планшетних комп'ютерів, створена компанією Google на базі ядра Linux. Підтримується альянсом Open Handset Alliance (ОНА).

На жаль, конкуренція між антивірусними компаніями призвела до того, що розвиток йде в бік збільшення кількості вірусів, а не в бік покращення їх детектування (ідеал це 100%-е детектування) і алгоритмів лікування файлів, що заражені.

На даний момент немає надійної антивірусної перевірки НТТР-трафіку смартфонів на базі ОС Android. Яким буде антивірус для смартфонів, які технології будуть використовуватися в антивірусі для смартфонів - на даний момент немає відповіді на ці питання.

Таким чином, виходячи з вищеперахованого, розробка програмного забезпечення антивірусної перевірки НТТР-трафіку смартфонів на базі ОС Android, є актуальною задачею.

Призначення системи – захист смартфонів від шкідливого ПЗ методом антивірусної перевірки НТТР-трафіку. Більшість існуючих типів вірусів під ОС Андроїд передаються через НТТР-трафік при з'єднанні з глобальною мережею Інтернет.

Область використання та застосування системи – захист мобільних платформ, забезпечення гарантованої стійкості при роботі з Інтернет контентом.

УДК 004.738.5

А.О. Іщенко

Науковий керівник – Сидоренко В.В., д-р техн. наук, професор
Кіровоградський національний технічний університет

Система аналізу динаміки успішності студентів в учбовому процесі

У наш час стрімкого розвитку інформаційних технологій потоки інформації, що циркулюють у світі, – величезні і мають тенденцію до збільшення. Тому, в будь-якій організації, виникає проблема керування даними, яке б забезпечило найбільш ефективну роботу. Не є виключенням і навчальні заклади.

Майже всі освітні установи використовують автоматизовані системи управління. Всі останні управлінські завдання вирішуються шляхом складання зведеної і аналітичної звітності в офісних електронних документах (MS Excel, MS Word). Багато з них самотужки намагаються вирішити проблему управління навчальним процесом і зараз, для багатьох освітян, увійшли в звичку комп'ютерні програми які можуть зробити розклад занять, розподіл аудиторного фонду навчального закладу або розрахувати навантаження викладачів. Але відсутність єдиного системного підходу зменшує позитивні ефекти та переваги кожної з цих розробок. Негативно впливає і той факт, що програми від різних розробників не можуть здійснювати ефективний обмін даними між собою.

Метою роботи є огляд існуючих систем на основі якого здійснюється постановка вимог і основних задач, які повинна вирішувати система аналізу динаміки успішності студентів в учбовому процесі.

На даний час розроблено багато автоматизованих систем управління навчальним процесом серед яких:

1. Автоматизована система керування вищим навчальним закладом АСК «ВНЗ», розроблена Науково-дослідним інститутом Прикладних інформаційних технологій Кібернетичного центру Національної академії наук України.

2. Комп'ютерна система «Деканат» ПП «Політек-софт».

3. «ВНЗ АЛЬМА-МАТЕР» ТОВ «Direct IT».

4. Інформаційно-аналітична система керування вищим навчальним закладом «Університет», розроблена в Херсонському державному педагогічному університеті.

Найбільш ефективним є програмне забезпечення, розроблене співробітниками підприємства «Політек-СОФТ», яке охоплює майже всі аспекти діяльності навчального закладу. Серед усіх пакетів, які пропонує «Політек-Софт», найбільш функціональними, з точки зору автоматизації сфер діяльності ВНЗ, є пакети «Деканат» та «Колоквіум».

Система «ДЕКАНАТ» призначений для автоматизації планування та обліку навчального процесу в закладах освіти (технікумах, коледжах, училищах, інститутах та університетах). Пакет дозволяє створити та підтримувати базу даних, в якій формується та реструктується така інформація:

- структура навчального процесу закладу (спеціальності, групи, підгрупи, потоки, предмети, кількість годин з предметів за різними видами занять, навчальні плани та, при необхідності, факультети, кафедри, циклові комісії);

- дані щодо всіх викладачів закладу та їхнього планового навантаження, розклад;

- щоденні дані про фактичну роботу кожного викладача з кожного предмету;

- великий обсяг даних щодо всіх студентів закладу та їхньої успішності за весь період навчання;

- дані про наявні корпуси та аудиторії навчального закладу, їхнього заповнення, розклад занять.

На даний момент система «ДЕКАНАТ» отримала підтримку кредитно-модульної системи, що робить її однією з найкращих на ринку програмного забезпечення для ВНЗ в Україні.

Проте недоліком оглянутих систем є те, що вони не відображають динаміку успішності студента. А також їх надмірна складність в управлінні та введенні даних.

Основними вимогами до систем аналізу динаміки успішності студентів в учбовому процесі є:

- зберігання наступних даних: інформацію про студента; інформація про оцінки за: лабораторні роботи, практичні заняття, індивідуальні завдання та інше; інформація про відвідування занять; рубіжний контроль.

- виведення наступних даних: оцінки студента по всім предметам та його рубежі; статистика пропусків занять студента; інформація про студента; розклад занять на семестр.

Отже, при повноцінному використанні комп'ютерних засобів можливе значне підвищення якості навчального процесу та контролю над ним. В роботі були розглянуті існуючі систем обліку і аналізу успішності студентів в учбовому процесі та поставлені вимоги до системи аналізу динаміки успішності студентів. На основі даного аналізу була розроблена система аналізу динаміки успішності студентів в учбовому процесі.

Список літератури

1. Про Національну програму інформатизації. Закон України від 04.02.98// Відомості Верховної Ради України. – 1998. – № 27 – 28. – С.181.
2. Про Державну національну програму «Освіта» (Україна XXI століття). Постанова Кабінету Міністрів України від 03.11.93. – 1993. – № 896.
3. Кузьма К.Т. Аналіз автоматизованих систем управління вищим закладом освіти [Електронний ресурс]: збірник наукових праць, том 12 / Актуальні проблеми автоматизації та інформаційних технологій // Дніпропетровський національний університет ім. Олеся Гончара, 2008. Режим доступу до журн. : www.nbu.gov.ua/portal/natural/Akpa/2008_12/12.pdf

УДК 004.4

О.В. Касян

Науковий керівник – Константинова Л.В., асистент
Кіровоградський національний технічний університет

Програмне забезпечення IRC-клієнту

IRC (Internet Relay Chat) – це одна із самих популярних у світі інтерактивних служб. Без сумніву, WEB гарний, коли треба знайти яку небудь інформацію й електронну пошту набагато швидше й зручніше звичайної пошти, але коли ти хочеш спілкування, IRC – саме те, що треба. Використовуючи IRC-клієнт (програму) ви можете обмінюватися текстовими повідомленнями з людьми з будь-якої точки миру. Найпоширеніші програми-клієнти це mIRC, Pirc, MS Chat і Virc для Windows і Homer або IRCle для Macintosh. У принципі, не має значення, яку із програм ви використовуєте, всі вони з'єднуються з одними IRC-мережами (або серверами). Коли ви ввійшли в таку мережу, ви можете спілкуватися з іншими її учасниками, друкуючи повідомлення, які негайно передаються вашому співрозмовникові.

IRC одержав міжнародну популярність під час війни в Перській затоці в 1991 році, коли останні новини передавалися через Інтернет, і величезна кількість IRC-користувачів збиралася на одному каналі, що б послухати ці повідомлення. Подібним же чином IRC використовувався під час подій у вересні 1993 року в Москві. IRC-користувачі з Москви давали на канали живі репортажі про нестабільну ситуацію того часу. Як і в житті, не всі люди, що спілкуються на IRC говорять про те, що дійсно цікаво, але можна познайомитися й із цікавим співрозмовником і багато з людей розвили тривалу й міцну дружбу через IRC. Трапляється навіть, що відносини, початі на IRC, приводять до шлюбу. Тож, IRC є великим засобом для спілкування людей із всіх кінців світу. Ви можете бути ввевненим, що зустрінете безліч цікавих людей і знайдете не одну кампанію ваших однодумців у тих або інших питаннях.

Отже, розробка програмного забезпечення IRC-клієнту є актуальною задачею.

Список літератури

1. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 2-е изд. / В.Г. Олифер, Н.А. Олифер. – СПб. Питер, 2004. – 864 с.
2. Глушаков С.В., Ломотько Д.В., Сурядный А.С. Работа в сети Internet/ 2-е изд., доп. и перераб./ Худож. - оформитель А.С. Юхтман. – Харьков: Фолио, 2003. -399 с.
3. В. Холмогоров Компьютерная сеть своими руками. Самоучитель. СПб.: Питер. 2004. - 171 с.

УДК 004.42:004.056.5

О.С. Катрухін

Науковий керівник – Дбрєнський О.П., викладач
Кіровоградський національний технічний університет

Програмна реалізація перешкодостійкого кодування для передачі даних комп'ютерною мережею

Інтенсивний перехід, що почався в кінці минулого тисячоріччя, до систем обробки й передачі інформації цифрового формату на сьогодні стає усе більше масштабним і характеризується досить швидким і значним підвищенням вимог до вірогідності цифрових даних. Безсумнівно, провідну роль у забезпеченні високого рівня

надійності і якості передачі дискретної інформації грають сучасні методи завадостійкого кодування. Застосування завадостійкого кодування в системах передачі даних комп'ютерною мережею дозволяє одержати енергетичний вигравш кодування. У цей час у теорії кодування відомо всього кілька методів кодування/декодування, що забезпечують роботу пропускну здатності каналу. Однак останнє десятиліття однозначно показало, що дані методи усе ще мають досить велику обчислювальну складність, що утрудняє їхнє практичне застосування у високошвидкісних системах передачі даних. У зв'язку із цим виникає завдання пошуку більш простих і, відповідно, більш надійних і дешевих для практичної реалізації методів кодування/декодування. Це завдання, з огляду на постійний ріст швидкостей обміну даних, з кожним роком стають актуальнішим.

Таким чином, програмна реалізація перешкодостійкого кодування для передачі даних мережею є актуальною задачею, яка потребує нагального розв'язку.

За результатами дослідження розроблено структурну схему перешкодостійкого кодування для передачі даних комп'ютерною мережею, яку наведено на рисунку 1.

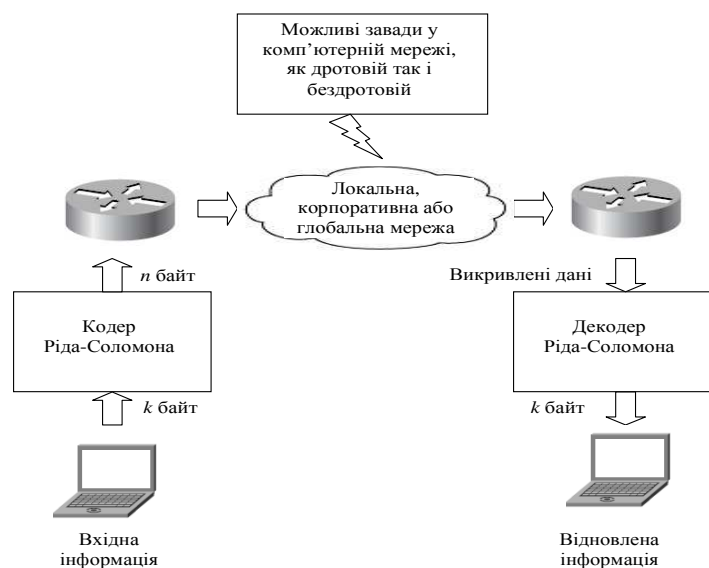


Рисунок 1 – Структурна схема перешкодостійкого кодування для передачі даних комп'ютерною мережею

Для програмної реалізації перешкодостійкого кодування під час передачі даних комп'ютерною мережею найбільш повно, на думку автора, відповідає простий і одночасно дуже ефективний метод Раїда-Соломона. Алгоритм Раїда-Соломона є ітеративними процедурами, при цьому вони мають властивість строгого росту правдоподібності своїх рішень протягом усього процесу виправлення помилок у перекрученому шумами повідомленні. Код Раїда-Соломона може бути визнаний основним методом декодування для багатьох сучасних високошвидкісних систем передачі даних із гранично можливими рівнями енергетичного вигравшу й дуже високою швидкодією.

Запропонована реалізація системи перешкодостійкого кодування на основі алгоритма Раїда-Соломона є ефективною у застосуванні для забезпечення передачі даних комп'ютерною мережею та має практичну цінність.

Список літератури

1. Слободзян В.І. Дослідження особливостей завадостійкого кодування на основі циклічних кодів / В.І. Слободзян, А.М. Слівінський // Вимірювальна та обчислювальна техніка в технологічних процесах. – 2010. – № 2. – С. 104-111.
2. Кулик А.Я. Забезпечення завадостійкого передавання інформації у проблемно-орієнтованих розподілених комп'ютерних системах / А.Я. Кулик // Вісник КНУ імені Михайла Остроградського: Електронні апарати, комп'ютернатехніката інформаційно-вимірювальнітехнології. – 2011. – Вип. 1 (66), ч. 1. – С. 47-51.
3. Кривогубченко С.Г. Особливості використання завадозахищених кодів для закриття інформації при передаванні колективними лініями зв'язку / С.Г. Кривогубченко, М.М. Компанець, А.Я. Кулик // Збірник наукових праць Донецького державного технічного університету. – Сер. “Електротехніка і енергетика”. – 2000. – Вип. 17. – С. 65 – 69.

УДК 004.056.55

О.О. Косенко

Науковий керівник – Сидоренко В.В., ст. викладач
Кіровоградський національний технічний університет

Автоматизація роботи відділу кадрів лікарні

Використання баз даних і інформаційних систем стає невід'ємною частиною ділової діяльності сучасної людини і функціонування процвітаючих організацій. У зв'язку з цим велику актуальність набуває освоєння принципів побудови і ефективного використання відповідних технологій і програмних продуктів: систем управління базами даних, CASE-систем автоматизації проектування та інших.

В основі рішення багатьох задач лежить обробка інформації. Для полегшення обробки інформації створюються інформаційні системи (ІС).

В кожній області діяльності створюються власні БД: в соціальному забезпеченні – для отримання пенсії, в медицині – по диспансерному обліку, по пільговим лікам.

Так, для відділу кадрів розроблена програма «Автоматизація роботи відділу кадрів обласної лікарні» спеціально для роботи з особистими даними працівників. База даних, яка є в закладах, дозволяє працівникам кадрових служб накопичену інформацію по працівникам зберігати оптимально, шукати, а також використовувати при оформленні різноманітних статичних даних, підготовці звітів, при вирішенні задач по питанням підвищення кваліфікації, сертифікації.

Для Кіровоградської обласної лікарні було вирішено створити базу даних «Кадри», в якій буде зберігатися інформація в декількох таблицях. При встановленні між ними зв'язків можна створювати запити даних з цих зв'язаних таблиць.

Облік трудових ресурсів та управління ними - необхідна складова у загальному плануванні ресурсів будь-якої організації.

З мірою росту організації для забезпечення оперативної обробки документації по особистому складу і ефективної роботи з персоналом виникає необхідність в засобах автоматизації. Використання комп'ютерних технологій дає можливість швидко отримувати будь-які форми звітності, гнучко змінювати вихідні звітні форми в відповідності з змінами в законодавстві та потребами самої організації.

Впровадження програм на великих підприємствах дозволяє значно поліпшити умови праці працівників відділу кадрів, планових і розрахункових підрозділів. Користувачі можуть самостійно готувати різноманітні звіти по персоналу підприємства, формувати списки на основі довільно сформованого звіту.

Програма дозволяє підготувати до друку та роздрукувати велику кількість документів, необхідних при роботі з кадрами, тим самим, заощаджуючи робочий час співробітника. Дана програма має зручний інтерфейс, невеликі вимоги до апаратного забезпечення.

Створена база даних є досить простою та легкою до подальшої модифікації, вдосконалення та налаштування під інші види діяльності.

Отже, можна відзначити такі основні позитивні риси як:

– всі дані зберігаються в електронному вигляді внаслідок чого вони можуть ефективно використовуватися;

– виключається будь-яке дублювання даних;

– значно економить час.

В подальшому БД може розширяться і вдосконалюватися з метою збільшення функціональності цієї програми. Також ця БД може використовуватися не тільки в лікарнях, а і в будь-яких інших структурах, які потребують автоматизації роботи відділу кадрів.

Список літератури

1. Горев А., Макашарипов С., Ахаян Р. Эффективная работа с СУБД. – 445 с.
2. Хомоненко А.Д., Цыганков В.М., Мальцев М.Г. Базы данных: Учебник для высших учебных заведений. – 2004. –736 с.
3. Кренке Д.. Теория и практика построения баз данных . - 2005. – 800 с.

УДК 004.056

І.І. Коваленко

Науковий керівник – Савеленко О.К., викладач

Кіровоградський національний технічний університет

Проектування бази знань для підтримки прийняття рішень для управління обліком готової продукції на виробництві

Метою роботи є освоєння основних понять, методів та моделей, що дозволяють створювати основані на знаннях інтелектуальні системи підтримки прийняття рішень на підприємстві. В роботі використані розробки (бібліотеки), що дозволяють автоматизувати побудову блоків підтримки прийняття рішень інтелектуальних систем. В роботі також наведено опис програмних засобів, що реалізують розглянуті методи та моделі.

Сучасний світ вимагає швидкого і точного прийняття рішення щодо того чи іншого завдання і особливо це актуально у виробництві, де важливо швидко й правильно прийняти рішення, бо від цього залежатиме прибуток даного підприємства. Для цього використовують автоматизовані системи підтримки прийняття рішень, які, в першу чергу, радять користувачу даної системи найбільш оптимальне на їх погляд рішення, а саме рішення вже приймається користувач. Автоматизація управління

випуску готової продукції на виробництві також удосконалюється і вона вже значно спростила роботу працівників підприємств.

Управління випуском готової продукції є досить трудомістким і складним процесом та саме від нього залежить ефективна робота усього підприємства. Логістичний процес на підприємстві досить складний, оскільки вимагає узгодженості функцій вироблення нової продукції по замовленням клієнтів.

Для проектування бази знань для підтримки прийняття рішень при управлінні випуском готової продукції на виробництві було обрано задачу оброблення замовлення клієнта по певній продукції. Замовлення продукції безперечно є однією з найважливіших задач, так як у разі відсутності певної продукції інші задачі, пов’язані з транспортуванням, зберіганням чи обслуговуванням клієнтів, будуть недоречними, бо немає що реалізувати. Обробленням замовлення продукції займається комірник.

Під час розв’язання задачі здійснюється управління такими об’єктами: складом а також безпосередньо самим підприємством тому, що з кожним замовленням потрібно приймати рішення щодо подальшого випуску продукції.

У ході виконання цієї роботи було досліджено та вивчено предметну область, пов’язану з управлінням обліку готової продукції. В результаті було спроектовано базу знань для підтримки прийняття рішень при управлінні обліком готової продукції, а саме щодо прийняття рішення про оброблення замовлення клієнта комірником в програмному середовищі MATLAB, за допомогою бібліотеки SNTOOLBOX.

У ході дослідження було обґрунтовано необхідність проектування бази знань для підтримки прийняття рішень в управлінні обліком готової продукції на виробництві.

Система може бути в подальшому застосована працівниками складів різних підприємств. Використання автоматизованої системи має такі переваги: зручність у використанні; простота; швидкість оброблення інформації.

Список літератури

1. Субботін С.О. Подання й обробка знань у системах штучного інтелекту та підтримки рішень: Навч. посібник. – Запорізький національний технічний університет, 2008. – 341с.
2. Иглин С.П. Математические расчеты на базе MATLAB. – СПб.: БХВ-Петербург, 2005. – 640 с.

УДК 004.738.2

В.Ю. Малаховський

Науковий керівник – Сидоренко В.В., д-р техн. наук, професор

Кіровоградський національний технічний університет

Програмні засоби поширення даних із застосуванням СМС повідомлень

Дотримання вимоги мобільності поширення даних серед їх користувачів, а також живе оновлення таких даних вимагають розробки та забезпечення спеціальних програмних засобів. Такі засоби виконують функцію розповсюдження інформації, яка формується на сервері і може бути відображеною на різноманітних засобах обміну інформації (наприклад мобільних телефонах). Мобільних телефон сьогодні є найбільш поширеним засобом зв’язку, який забезпечує безперервний зв’язок та передачу даних.

Метою публікації є розробка програмного засобу поширення даних, що працює на сервері і обслуговує відповідну базу даних.

Аналіз показав, що серед серез існуючих систем [1,2] існує багато недоліків, як наприклад складність у обслуговуванні, складність у застосуванні, неможливість коригування системи для окремих випадків, та низька надійність таких систем.

За існуючих сьогодні можливостей зв'язку між сервером та мобільним телефоном, постає питання про розробку прикладного програмного забезпечення для поширення текстових повідомлень. Така програма повинна працювати на сервері, налаштовуватись у відповідності до потреб поширювача даних.

Запропоноване програмне рішення працює на базі ОС Linux. Вона включає наступні програмні модулі: драйвери модему; консольні утиліти; графічну оболонку.

Драйвери модему були взяті з джерела [3]. Згадані драйвери забезпечують можливість: звертатись до телефонної книги, здійснювати дзвінки, працювати з календарем и надсилати СМС повідомлення. Для вирішення проблеми дослідження використовується остання перелічена можливість вищезазначених драйверів.

Консольні утиліти включають в себе засоби для роботи з драйверами модему використовуючи консоль.

Графічна оболонка візуалізує вікно налаштувань, що дозволяє внести зміни у режим роботи програмного продукту що розробляється (рисунок 1).



Рисунок 1 – Зовнішній вигляд вікна налаштувань

Для роботи програмного засобу, попередньо формується база даних. Розроблена програма у заданий час звертається до БД, здійснює цілеспрямований вибір даних за заданими ознаками, та відправляє сформований звіт отримувачу інформації. Дана система зв'язку передбачає отримання повідомлення про доставку СМС користувачеві. Використання програми передбачає можливість зворотнього зв'язку користувача з системою, що зберігає оригінальний текст повідомлення.

Також дану систему можна використати не тільки для повідомлення графіку успішності, також може бути використана для відображення пропусків, якщо систему інтегрувати з системою

перепусток, або студентських квитків, у такому повідомлення буде надходити адресатові у разі проході студента через вхідну систему безпеки ВНЗ.

Висновки. У публікації висвітлюється послідовність розробки програмного засобу поширення даних із застосуванням СМС повідомлень, що відображає графік успішності студентів у ВНЗ.

Список літератури

1. <http://www.net-school.ru/sms.php>
2. Кузьма К.Т. Аналіз автоматизованих систем управління вищим закладом освіти [Електронний ресурс]: збірник наукових праць, том 12 / Актуальні проблеми автоматизації та інформаційних технологій // Дніпропетровський національний університет ім. Олеся Гончара, 2008. Режим доступу до журн. : www.nbu.gov.ua/portal/natural/Akpa/2008_12/12.pdf
3. <http://gnokii.org>
4. <http://www.schoolsms.ru>
5. <http://www.pisof.ru/smschool/>

УДК: 347.78:004.4

К.А. Мяснянкін

Науковий керівник – Ткалич М.О., канд. юрид. наук, доцент
Запорізький національний університет

Програмне забезпечення як об'єкт авторських прав: проблеми правового захисту

Останнє десятиріччя характеризується різким підвищенням інтенсивності інноваційних процесів у світі, перетворенням технологічних інновацій на головний чинник економічного зростання й соціального розвитку. Інноваційні процеси в економіці й суспільстві тісно переплетені з функціонуванням інституту інтелектуальної власності. Значна частина інновацій є практичним використанням прав на об'єкти інтелектуальної власності, створені й придбані суб'єктом господарювання. Багато нововведень базується на охороноздатних результатах інтелектуальної діяльності, що модифікуються в утилітарних цілях.

В інформаційному суспільстві головним інструментом у діяльності широкого кола спеціалістів розумової праці є комп'ютери, а головним елементом у процесі успішної співпраці людини і комп'ютера є програмне забезпечення, яке дозволяє оперативно обробляти інформацію та обмінюватися нею. За умов активної комп'ютеризації та інформатизації суспільства розвиток комп'ютерних технологій та програмного забезпечення, безумовно, повинен бути одним з основних напрямків інноваційної діяльності.

Питання захисту об'єктів авторського права ґрунтовно опрацьовані в юридичній науці, проте саме питання визначення правової природи комп'ютерних програм і виникнення авторських прав на них, їх передавання досліджені не достатньо. Це пов'язано, з одного боку, з відносною новизною самого об'єкта, а з другого, з тим, що нормотворча діяльність і теоретичні дослідження не встигають за швидким виникненням та розвитком принципово нових відносин.

Такими вимогами до результатів інтелектуальної власності, які відповідають властивостям інновацій, на погляд, таких вчених, Ю. Є. Атаманова, В. І. Березанська, С. П. Гаврилов та ін., є:

- а) наявність новизни;
- б) суттєве підвищення якісних характеристик товару;
- в) промислова придатність;
- г) економічна доцільність реалізації інновацій;
- ґ) формальна визначеність та документальна оформленість результатів досліджень чи інноваційних об'єктів;

д) наявність у складі інновацій об'єктів інтелектуальної власності, виключні права на які підтверджуються правостановлюючими документами [1, с. 273].

У цьому аспекті визначення сутності комп'ютерних програм настановується на дискусійне питання щодо віднесення їх до об'єктів авторського права чи об'єктів промислової власності.

Відповідно до положень Бернської конвенції про охорону літературних і художніх творів, до якої Україна приєдналася і з 25 жовтня 1995 р. стала її членом, а також згідно з п. 4 ст. 433 Цивільного кодексу України та п. 5 ст. 15 Закону України «Про авторське право та суміжні права» - комп'ютерні програми охороняються як літературні твори. Хоча в США, наприклад, на комп'ютерні програми видають патенти.

Україна багато в чому увібрала у своє законодавство норми права колишнього СРСР, формальною перешкодою на шляху охорони комп'ютерних програм нормами патентного права стало Роз'яснення № 4 Держкомітету у справах винаходів і відкриттів від 13 листопада 1975 р. «Про визнання винаходами об'єктів обчислювальної техніки, які характеризуються математичним забезпеченням ЕОМ», яким передбачалося, що «не

приймаються до розгляду заявки на видачу авторського свідоцтва і патенту на винахід, якщо об'єкт, що заявляється, представляє собою математичне рішення задачі, зокрема, алгоритми, програму для ЕОМ» [2, с. 163].

Згідно із законодавством України комп'ютерна програма - набір інструкцій у вигляді слів, цифр, кодів, схем, символів чи в будь-якому іншому вигляді, виражених у формі, придатній для зчитування комп'ютером, які приводять його в дію для досягнення певної мети або результату. За правовим режимом комп'ютерні програми належать до літературних творів. Правова охорона поширюється на всі види комп'ютерних програм, у тому числі на операційні системи і програмні комплекси, що можуть бути виражені будь-якою мовою і в будь-якій формі, включаючи вихідний текст і об'єктний код. До об'єктів авторського права не належать ідеї та принципи, які лежать в основі програм, ідеї і принципи організації інтерфейсу й алгоритму, мови програмування.

Іншими словами авторським правом захищається текст (код) програми, а не функції, які вона виконує, охороняється лише форма вираження. Це означає, що при захисті комп'ютерної програми має значення код, а не ідея, концепція, принципи. Авторським правом охороняються як оприлюднені програми, так і неоприлюднені.

Авторське право поширюється як на цілу програму, так і на її частину, якщо вона може використовуватися самостійно, наприклад, модуль, бібліотека.

Охорона авторським правом є найбільш сприятливою формою захисту комп'ютерних програм. Забезпечити охорону з використанням механізмів авторського права можна відносно швидко, легко й недорого. Сам факт їх створення в об'єктивній формі є підставою виникнення авторського права на дані об'єкти. Термін дії авторського права значний і, як правило, перевищує економічний і технічний термін використання програмного забезпечення.

Авторське право захищає саму програму у формі вихідного тексту або об'єктного коду, а зміст (як ідея, процес, засіб) - авторським правом не охороняється. Отже, охороняється авторське вираження ідеї в конкретній матеріальній формі.

Як ми згадували раніше, остаточне міжнародне законодавче закріплення за комп'ютерними програмами режиму об'єкта авторського права відбулося в 1991 році, згідно з Директивою Європейського Союзу «Про правову охорону комп'ютерних програм». Відповідно до Угоди про торговельні аспекти прав інтелектуальної власності СОТ 1995 року, «комп'ютерні програми у вихідному або об'єктному коді охороняються подібно до охорони, що надається літературним творам за Бернською конвенцією». Практично таку ж міжнародну норму закріпив Договір ВОІВ щодо авторського права, відповідно до якого «комп'ютерні програми охороняються як літературні твори в розумінні статті 2 Бернської конвенції».

У країнах СНД, у тому числі й в Україні, підтверджене міжнародне трактування комп'ютерних програм як літературних творів. Відповідно до нього, комп'ютерні програми охороняються, як літературні твори, і така охорона поширюється на всі види програм, у тому числі на прикладні програми й операційні системи, виражені будь-якою мовою і в будь-якій формі, включаючи вихідний текст й об'єктний код.

У той же час необхідно відзначити, що, незважаючи на те, що авторське право і спеціальне законодавство забезпечують основний обсяг охорони комп'ютерних програм, у деяких випадках цього недостатньо. Тому існує можливість захисту комп'ютерних програм шляхом використання засобів патентної охорони, хоча при одержанні патентів на винаходи, пов'язані з програмним забезпеченням і алгоритмами, виникає ряд проблем.

В Україні комп'ютерна програма охороняється лише авторським правом і її не можна «запатентувати», тобто отримати патент на винахід або корисну модель. Шлях даного процесу в нашій країні іноді називають «український феномен» комп'ютерного піратства [3, с.72]. Мається на увазі те, що за досить короткий час своєї незалежності Україна змогла вийти на перші місця в світі за обсягом контрафактного програмного забезпечення [4, с. 78].

Що цікаво, українські пірати змогли не лише розповсюдитись в межах країни, а й продовжили свою експансію в держави Східної, пізніше — Західної Європи [5, с. 19].

Комп'ютерне піратство в Україні набуло настільки значних меж, що світова спільнота почала працювати над блокуванням такої діяльності. Найбільш гучним прикладом піратства стало викрадення в компанії Microsoft частини початкового коду операційної системи Windows, котра лише готувалася до презентації на ринку. А це означало, що нову операційну систему можна було придбати на ринку ще до її офіційного виходу. І це не була альфа- чи бета-версія, це була повноцінна операційна система [6, с. 51].

Україна проголосила, що бере на себе зобов'язання дотримуватись міжнародних норм, підтвердивши це вступом у 1995 році до Світової організації інтелектуальної власності. Є Україна і однією із учасниць Бернської конвенції про охорону літературних і художніх творів. Україна — учасниця Всесвітньої конвенції про авторське право. Було підписано також двосторонні договори між США та Україною про зобов'язання дотримуватись світових стандартів у вказаній сфері. Але, як відомо, вони не були виконані, що призвело до застосування щодо України жорстких санкцій з боку США.

Можна згадати і Угоду про партнерство та співробітництво між Європейським співтовариством і Україною. Все вище наведене говорить про те, що така ситуація в Україні з піратством досить активно підтримувалась лобістами, що захищали свій нелегальний бізнес. Але були й такі сили, які вважали сусідство з Індією, країнами Південної Америки у рейтингу охорони авторських прав на програмне забезпечення неприпустимим, тому і продовжували боротьбу.

Для того щоб отримати патент на спосіб (процес) у галузі інформаційних технологій, потрібно описати направлені на досягнення технічного результату спосіб як дію або сукупність дій, які виконуються стосовно матеріального об'єкта за допомогою як мінімум одного продукту.

Таким чином, автор комп'ютерної програми повинен розуміти, що якщо він у своїй програмі виклав якийсь алгоритм розв'язання задачі, то саме цей алгоритм не буде охоронятися. Іншими словами, авторським правом захищається текст (код) програми, а не функції, які вона виконує. Для усунення цього недоліку авторського права останнім часом усе частіше й частіше в Україну подаються заявки на отримання патенту на винахід (корисну модель) із метою охорони й захисту алгоритму (способу) роботи комп'ютерної програми щодо розв'язання конкретної задачі.

Патент на винахід дозволяє захистити змістовий бік ПЗ, патентна охорона поширюється на сутність, утілену в алгоритмі, яка є основною ідеєю програми.

Крім того, патент дає виключне право власності на саму ідею (якщо вона відображена в істотних ознаках формули винаходу) і запобігає її несанкціонованому використанню.

На цей час захист комп'ютерних програм як об'єктів авторського права здійснюється не в повному обсязі, що призводить до неправомірного їх використання та становить серйозну перешкоду на шляху розвитку цивілізованого ринку інформаційних технологій у нашій країні, стримує міжнародне співробітництво, спричиняє економічні витрати держави, є незаконним із погляду порушення авторського права й завдає величезної шкоди виробникам комп'ютерних програм.

Як ми знаємо програмне забезпечення є продуктом технічної творчості. І, враховуючи те, що більшість програм (крім ігор, звісно) є по своїй суті засобами виробництва, то регулювання охорони авторських прав на них за допомогою патенту є досить слушним. Можна зробити узагальнення щодо охорони комп'ютерних програм нормами авторського права. В першу чергу потрібно наголосити на недосконалому саме цього інституту в охороні прав на комп'ютерні програми. Вбачається доцільним запозичення досвіду зарубіжних країн, які використовують комплексний механізм охорони з окремими елементами патентного права. Також логічним було б доповнити Закон України «Про авторське право і суміжні права» спеціальним розділом про охорону комп'ютерних програм, де викласти значення термінів, що стосуються їх охорони, законодавчо закріпити право на державну реєстрацію комп'ютерних програм і процедуру його здійснення. Важливо додати положення про те, що закон не застосовується до мов програмування, синтаксису, алгоритмів комп'ютерних програм, які використовуються при їх створенні. А також слід закріпити права законного

користувача на виготовлення копії комп'ютерної програми. Внесення зазначених змін до законодавства дозволить зменшити в Україні використання недієздатної програмного забезпечення, що сприятиме розвитку комп'ютерної індустрії та підвищенню темпів зростання економіки України.

Список літератури

1. Атаманова Ю. Є. Господарсько-правове забезпечення інноваційної політики держави [Текст] : монографія / Ю. Є. Атаманова. - Х. : ФІНН, 2008. - 424 с.
2. Дмитришин В. С. Інтелектуальна власність на програмне забезпечення в Україні [Текст] / В. С. Дмитришин, В. І. Березанська. - К. : Вірлен, 2005. - 304 с.
3. Богатова Л. Соглашения в области охраны авторских прав // Интеллектуальная собственность. — 1997. — № 7-8. — С. 58-8
4. Смирнова Г. П., Мигунов А. И., Поткин А. С. Проблемы правовой защиты программного обеспечения ЭВМ // НТИ, Сер. 1, Орг. и методика информ. работы. — 1991. — № 7/8. — С. 75-78.
5. Ботуз С. Социально-экономический аспект информационных технологий // Интеллектуальная собственность. — 1996. — № 3-4. — С. 10-19.
5. Терещенко Л. Глобальная сеть: пробелы в праве // Российская юстиция. — 2000. — № 8. — С. 35-52.

УДК 004.738.5

М.В. Миндра

Науковий керівник – Коваленко О.В., канд. техн. наук, ст. викладач
Кіровоградський національний технічний університет

Розробка програмного забезпечення системи налаштування маршрутизаторів локальної мережі з використанням методів оптимізації

Будь-яка складна обчислювальна мережа вимагає додаткових спеціальних засобів управління [1] крім тих, які є в стандартних мережевих операційних системах. Це пов'язано з великою кількістю різноманітного комунікаційного устаткування [2-3], робота якого критична для виконання мережею своїх основних функцій. Розподілений характер великої корпоративної мережі унеможливило підтримання її роботи без централізованої системи управління, яка в автоматичному режимі збирає інформацію про стан кожного концентратора, комутатора, маршрутизатора та надає цю інформацію оператору мережі. Зазвичай система управління працює в автоматизованому режимі, виконуючи найбільш прості дії по управлінню мережею автоматично, а складні рішення надаючи приймати людині на основі підготовленої системою інформації.

Система управління повинна бути інтегрованою. Це означає, що функції управління різнорідними пристроями повинні служити спільної мети обслуговування кінцевих користувачів мережі із заданою якістю.

Мета й завдання дослідження. Ціль – розробка системи налаштування маршрутизаторів локальної мережі з використанням методів оптимізації.

Об'єкт дослідження є процес налаштування маршрутизаторів локальної мережі з використанням методів оптимізації

Предмет дослідження – методи й алгоритми налаштування маршрутизаторів у локальній мережі.

Методами дослідження є методи і алгоритми клієнт-серверної взаємодії, оптимізації передачі даних, сканування локальної мережі.

Наукова новизна отриманих результатів. У процесі рішення завдань, обумовлених цілями дослідження, отримані наступні результати:

– На основі існуючих методів оптимізації роботи маршрутизаторів, запропоновано нову методику аналізу роботи маршрутизатора з подальшим формуванням скрипту корегування;

– Запропоновано нові методи налаштування маршрутизаторів з використанням протоколу передачі гіпертекстових документів;

– Вперше розроблено вітчизняний продукт системи налаштування маршрутизаторів локальної мережі з використанням методів оптимізації торгової мари D-link.

Практична цінність отриманих результатів полягає в тому, що розроблені алгоритми і програмне забезпечення дозволяють успішно вирішувати завдання налаштування маршрутизаторів локальної мережі з використанням методів оптимізації. Захищати ЛМ від програмних помилок маршрутизаторів та хакерських атак.

Достовірність наукових результатів підтверджена теоретичними викладеннями, даними комп'ютерного моделювання, коректними дослідженнями параметрів на функціонуючій обчислювальній мережі, а також відповідністю отриманих результатів окремим результатам, наведеним у науковій літературі.

Список літератури

1. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCENT/CCNA ICND1 640-822. ISBN 978-5-8459-1807-9, серия Cisco Press, 2013, , Издательство Вильямс, –С 720.
2. Димарцио Д.Ф. Маршрутизаторы Cisco. Пособие для самостоятельного изучения. –СПб: Символ-Плюс, 2003.
3. Кэтрин Пакет, Дайана Тир. Создание масштабируемых сетей Cisco. Серия Cisco Press, 2004, Издательство Вильямс, – С. 792.

УДК 004.4

І.С. Молчанов

Науковий керівник – Сидоренко В.В., ст. викладач
Кіровоградський національний технічний університет

Програмне забезпечення обробки даних системи відеонагляду з використанням БД та технології KVM

В умовах кризи, рівень криміналітету України значно виріс, що саме по собі говорить про необхідність убезпечити своє житло або офіс всіма можливими для цього засобами, у тому числі й відеоспостереженням. Системи відеоспостереження дійсно є ефективним методом захисту від незваних гостей. Комп'ютерна система відеоспостереження в будинку, квартирі або офісі надасть безліч переваг. Наприклад, огляд прилеглої території дозволить побачити, хто до вас прийшов. Якщо відеодомофон охоплює тільки тог, хто безпосередньо перед ним, то камери відеоспостереження допоможуть побачити інше.

У випадку проникнення в будинок або офіс під час відсутності хазяїна, записи з камер відеоспостереження, зафіксовані на відеореєстратор, пришивдшать упіймання злочинця правоохоронними органами. Досить часто, з метою психологічного ефекту,

по периметру встановлюють муляжі камер, але дане лякання може подіяти тільки на недосвідчених ведмежатників. Іноді, відеореєстратори встановлюють у сейфах або важкодоступних місцях, щоб зберегти запис від тих, кому це не вигідно. Вся інформація зберігається на жорстких дисках. Відеоспостереження в будинку або квартирі забезпечує не тільки додаткову охорону під час відсутності хазяїна, але й додаткову впевненість у домашньому персоналі, при наявності таких. Наприклад, якщо ви найняли нянюку для дитини, то за допомогою системи відеоспостереження через інтернет, ви завжди зможете в реальному часі подивитися, що зараз відбувається в будинку і як, найнята на роботу людина виконує свої обов'язки.

Таким чином, виходячи з вищеперахованого, розробка програмного забезпечення обробки даних системи відеонагляду з використанням БД та технології KVM, є актуальною задачею.

Список літератури

1. Гольдштейн Б.С. Сигнализация в сетях связи. Том 1. М.: Радио и зв'язок, 1998.
2. Гольдштейн Б.С. Протоколы сети доступа. Том 2. М.: Радио и зв'язок, 1999.
3. Гольдштейн Б.С., Ехриель И.М., Рерле Р.Д. Интеллектуальные сети. М.: Радио и зв'язок, 2000.
4. Кульгин М. Технологии корпоративных сетей. Изд. «Питер», 1999.
5. Демьяовски В. – CCTV. Библия охранного телевидения. М.: ООО «ИСС», 2002, – 352 с.

УДК 004.738.5

А.А. Недолужко

Науковий керівник – Сидоренко В.В., ст. викладач
Кіровоградський національний технічний університет

Розробка автоматизованої системи митного оформлення

Автоматизована система митного оформлення розроблена і призначена для автоматизованого оформлення митних документів у структурних підрозділах митного органу, зайнятих у процесі митного оформлення вантажів.

Програма дає змогу вирішувати такі завдання:

- автоматизована підтримка технології митного оформлення, прийнятої в митному органі й основаної на нормативних документах Держмитслужби України і митного органу;
- введення і форматно-логічний контроль електронних копій документів, необхідних для митного оформлення та перевірка вантажної митної декларації (ВМД) згідно з критеріями ризику;
- ведення бази даних митного органу — основного сховища інформації про митне оформлення (електронні копії ВМД, інші документи, задіяні в процесі митного оформлення, дані про проходження технологічних етапів митного оформлення тощо);
- обмін інформацією з іншими підрозділами митного органу із застосуванням криптографічного захисту інформації;
- формування інформації з метою подальшого введення її до центральної бази даних Єдиної автоматизованої інформаційної системи (ЦБД ЄАІС) ДМСУ.

Співробітник митної служби України повинен заповнити необхідну інформацію про вантаж: код товару, код відправника та одержувача, дату відправлення та прибуття товару, загальну суму за рахунком та валюту, вид транспорту на кордоні та

в межах країни, вагу брутто на нетто, а також код своєї печатки. Приклад заповнення електронної декларації зображений на рисунку 1.

Рисунок 1 – Заповнена електронна декларація

Дана база даних була зроблена для зберігання, пошуку та використання інформації. Така організація даних дозволяє зменшити надмірність даних, що зберігаються, спрощує їх введення і організацію запитів і звітів. Всі таблиці даних зв'язані, що дає змогу швидко перейти на потрібну інформацію. При появі нових виробничих завдань розробник може в найкоротші терміни реалізувати їх у базі даних, шляхом додавання рядків, стовпців і цілих таблиць.

В подальшому планується розширення і вдосконалення даної бази даних з метою збільшення функціональності цієї бази.

Список літератури

1. Голицина О. Л. Базы данных / Голицина О. Л., Максимов Н. В., Попов И. И. – М.: Форум, 2003, -352 с.
2. Рудаков А. В. Технология разработки программных продуктов / Рудаков А.В.–М.: Академия, 2005.–208 с.
3. Благодатских В. А. Стандартизация разработки программных средств: Учеб. Пособие/ Благодатски В.А., В.А. Волнин, К.Ф. Посакалов; Под ред. О. С. Разумова. – М.: Финансы и статистика, 2003. - 288с.

УДК 004.4

К.І. Осауленко

Науковий керівник – Дресва Г.М., асистент
Кіровоградський національний технічний університет

Програмне забезпечення антивірусного захисту файлових серверів

У міру підвищення доступності інтернету й локальних мереж у багатьох користувачів виникає бажання або необхідність обмінюватися файлами з іншими людьми. У принципі, це можна зробити й за допомогою "загального доступу", використовуючи убудовані можливості операційної системи. Однак через інтернет це небезпечно й вимагає установки VPN, а в локальній мережі – не дозволяє лімітувати швидкість завантаження й ваш комп'ютер може бути майже паралізований при активній скачці великих файлів. Щоб уникнути всіх цих проблем варто поставити файловий сервер, або, як його ще називають FTP-сервер, що дозволить гнучко управляти обсягами трафіку, централізовано маніпулювати списками доступних файлів і користувачів, а також використовувати для завантаження файлів програми з дозавантаженням після обриву (наприклад, ReGet).

Але при роботі з файловими серверами, особливо гостро постає питання безпеки. У цьому аспекті, у рамках виконання дипломного проектування розглянемо антивірусний захист файлових серверів.

Таким чином, система, яка розробляється у ході виконання дипломного проектування, призначена для захисту файлових серверів від комп'ютерних вірусів. Способи протидії комп'ютерним вірусам можна розділити на кілька груп: профілактика вірусного зараження й зменшення передбачуваного збитку від такого зараження; методика використання антивірусних програм, у тому числі знешкодження й видалення відомого вірусу; способи виявлення й видалення невідомого вірусу.

Таким чином, виходячи з вищеперахованого, розробка програмного забезпечення антивірусного захисту файлових серверів є актуальною задачею.

Список літератури

1. Леонтьев В.П. Новейшая энциклопедия персонального компьютера 2003. – М.: ОЛМА-ПРЕСС, 2003.–920 с.
2. Соколов А. Методы информационной защиты объектов и компьютерных сетей.–Из-во Полигон, 2000.–272 с.
3. Тайли Э. Безопасность персонального компьютера. Из-во ПОПУРРИ. 1997. – 480 с.
4. Купер С. Антивирусные программы. Обзор – //Windows IT Pro, 2004, №2.
5. Голубев С. Обзор популярных антивирусных программ – //Upgrade, 2004, №6.

УДК 004.738.5

А.В. Орел

Науковий керівник – Савеленко О.К., викладач
Кіровоградський національний технічний університет

Застосування алгоритму Форчуна в сучасних САПР

Алгоритм Форчуна – алгоритм планарного замітання, який використовується для побудови діаграм Вороного, і дає можливість розв'язати задачу за час $O(N^2 \log(N))$. Ключовим моментом алгоритму є можливість знаходження всіх подій, що надходять, ефективним способом. Замість того, щоб будувати діаграму Вороного за допомогою планарного замітання в своїй загальній формі, розраховують викривлену, але топологічно еквівалентну версію діаграми. Остаточна діаграма має таку ж структуру, як і діаграма Вороного, але з гранями, що є параболічними дугами. На основі такої діаграми легко згенерувати правильну діаграму Вороного з прямими відрізками.

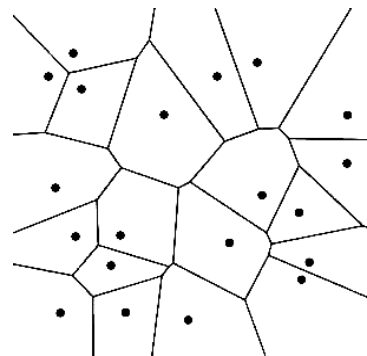


Рисунок 1 – Діаграма Вороного

Діаграма Вороного - це особливий вид розбиття метричного простору що визначається відстанями до заданої дискретної множини ізольованих точок цього простору. Діаграми Вороного використовуються у різноманітних областях науки та техніки.

У САПР діаграми Вороного(а, відповідно, і алгоритм Форчуна) можуть бути застосовані у таких областях:

- Побудова графа обмежень у системах перевірки, виправлення та стиснення топології НВІС(Надвеликих Інтегральних Схем);
- Побудова графа планування в системі глобального трасування;
- Перетворення звичайного розведення друкованих плат у полігональне;
- Обчислення критичних зон;
- Двовимірне стиснення топології тощо.

Список літератури

1. Evanthia Papadopoulou Critical area computation via Voronoi diagrams / Evanthia Papadopoulou, D.T. Lee // IEEE transactions on computer-aided design of integrated circuits and systems. – 1999. - №4. – С.463-474
2. Малинаускас К.К. Разработка математического и программного обеспечения систем топологического проектирования СБИС с использованием диаграмм Вороного: автореф. дис. на здобуття наук. ступеня канд. фіз.-мат. наук : / К.К. Малинаускас. – Москва, 2007. – 23 с.
3. Муров М.Ю. Метод преобразования обычной разводки печатных плат в полигональную / М.Ю.Муров // Технология и конструирование в электронной аппаратуре. – 2010. - №4. – С. 29-31

УДК 004.451

С.В. Печенюк

Науковий керівник – Доренський О.П., викладач
Кіровоградський національний технічний університет

Дослідження мобільних операційних систем

Наявність операційної системи (ОС) – головна особливість, що відрізняє смартфон від звичайного мобільного телефону. У комунікаторів ОС є за визначенням. При виборі конкретної моделі смартфона або комунікатора операційна система часто стає визначальним чинником [1]. Тому дослідження характеристик, властивостей, переваг і недоліків сучасних мобільних ОС є актуальною задачею, розв'язок якої має практичну цінність.

Метою роботи є дослідження мобільних операційних систем, виявлення їх основних переваг і недоліків з погляду програміста та користувача.

На сьогоднішній день досить популярною і поширеною є операційна система Android – одна з нових ОС, заснована на базі операційної системи Linux і розробляється “Open Handset Alliance” за підтримки “Google”. Вихідний код знаходиться у відкритому доступі, завдяки чому будь-який розробник може створити свою версію цієї мобільної ОС. Розробникам додатків висунуто невелику кількість обмежень, завдяки чому існує безліч як платних, так і безкоштовних додатків, які можна зручно завантажити з Android Market [1]. Сучасні смартфони HTC Desire, Samsung Galaxy Gio, Motorola Droid Razr, Samsung Galaxy S3 і HTC Wilfire працюють на ОС Android. До її переваг можна віднести гнучкість, відкриті вихідні коди, наявність великої кількості програм, висока швидкодія, зручна взаємодія з сервісами від “Google”, багатозадачність. У той же час слід відзначити наступні виявлені недоліки: безліч актуальних версій (для багатьох пристроїв нова версія входить занадто пізно або не з'являється зовсім, тому розробникам доводиться розробляти додатки, орієнтуючись на попередні версії); високий ризик хакерських атак через відкритість коду.

Операційна система IOS (до 24 червня 2010 року – iPhone OS) – мобільна операційна система, що розробляється і випускається американською компанією “Apple”. Була розроблена у 2007 році спочатку для iPhone і iPod Touch, пізніше – для таких пристроїв, як IPAD і Apple TV. На відміну від Windows Phone і Google Android,

вказана ОС випускається виключно для пристроїв, вироблених фірмою “Apple”. Серед важливих переваг IOS слід відзначити її зручність користування, якісну службу підтримки, регулярні оновлення, що усувають багато проблем в роботі, можливість купити в App Store безліч різних програм. У той же час дослідження дало можливість виявити суттєві недоліки: заблокований характер ОС, відсутність багатозадачності та вбудованого редактора документів [2].

Windows Phone – мобільна операційна система, розроблена “Microsoft”, яка є наступником Windows Mobile, хоча і несумісна з нею, з повністю новим інтерфейсом і з інтеграцією сервісів Microsoft. Дослідження цієї ОС дають підстави вказати на ряд її переваг: схожість з настільною версією, зручна синхронізація, у комплекті наявні офісні програми, багатозадачність. Слід відзначити і недоліки, які полягають у високих вимогах до обладнання, наявність на сьогоднішній день великої кількості вірусів, нестабільність в роботі.

В роботі досліджено три найпоширеніші і найпопулярніші на сьогоднішній день мобільні операційні системи від “Google”, “Microsoft” та “Apple”, проаналізовано їх характеристики, властивості, системні вимоги, виявлено та обґрунтовано їх основні переваги і суттєві недоліки з погляду програміста та користувача.

Список літератури

1. Разработка приложений для Android С. Хашими, С. Коматинени, Д. Маклин. Санкт-Петербург, 2011. – 372с.
2. Разработка приложений для iPhone, iPad и iPod touch с использованием iOS SDK.-М.:Диалектика-Вильямс, 2011.-264 с.
3. <http://streamport.ru>
4. <http://msdn.microsoft.com>
5. <http://biz.liga.net/all/all/stati/2049193-mobilnyy-obzor-operatsionnye-sistemy.htm>

УДК 004.738.5

О.О. Пономар

Науковий керівник – Якименко Н.М., канд. фіз.-мат. наук, доцент
Кіровоградський національний технічний університет

Створення програмного забезпечення багатопотокової обробки цифрових зображень

На сьогодні дуже стрімко розвивається багатопроцесорна архітектура. Одним з видів багатопроцесорності є багатоядерність. Багатоядерний процесор складається з двох і більше «обчислювальних ядер» на одному кристалі. Він має один корпус і встановлюється в один роз'єм на системній платі комп'ютера, але операційна система сприймає кожне його обчислювальне ядро як окремий процесор з повним набором обчислювальних ресурсів. Всі сучасні комп'ютери мають процесори, як мінімум, з двома ядрами. Основні виробники процесорів Intel і AMD - визнали подальше збільшення числа ядер процесорів як один з пріоритетних напрямків збільшення продуктивності.[1] Не дивлячись на те, що багатоядерні процесори давно ввійшли в наше життя, далеко не всі програми вміють коректно взаємодіяти з декількома ядрами, а також грамотно використовувати і оптимізувати доступні системні ресурси.

Одним з аргументів на користь включення в систему додаткових процесорів є той факт, що алгоритми, використовувані для вирішення багатьох прикладних завдань, піддаються розпаралелюванню, тобто розподіленню роботи між декількома більш-менш незалежно працюючими процесорами. Розпаралелювання розрахунків – найкращий метод

прискорення обробки зображень. Методи обробки зображень добре піддаються розпаралелюванню. Всі вони пов'язані з виконанням одного й того ж алгоритму над файлом зображення. Так як алгоритм змінюватися не може і розірвати його на паралельні процеси теж неможливо, розпаралелення приходить на роботу з файлом. Існують такі способи розпаралелювання алгоритмів обробки зображень:

- Кожне ядро працюватиме з повною копією зображення;
- Зображення розрізається на горизонтальні смуги, що не перетинаються. Їх кількість рівна кількості ядер. Кожне ядро отримує свою смугу для обробки;
- Зображення розрізається на горизонтальні смуги, що перетинають сусідні смуги на задану кількість пікселів. Кожне ядро отримує свою смугу, таким чином дані на границі смуги дублюються на двох ядрах. Це дає можливість перевірити правильність виконання алгоритму різними ядрами.

Рішення багатьох проблем науки і практики приводить до необхідності відбору корисної інформації із різного роду зображень. Такі задачі виникають в різних областях: в медицині, радіо-, тепло і гідролокації, дослідженні Космосу та Землі, телебаченні та іншому. Основними задачами обробки зображень є:

- Фільтрація і покращення візуального сприйняття.
- Відновлення відсутніх ділянок.
- Виявлення об'єктів та їх ідентифікація,
- Оцінка геометричних трансформацій.
- Оцінка параметрів зображення.
- Стиснення зображення.[2]

На програмах, оптимізованих під паралельне виконання, спостерігається приріст продуктивності на багатоядерних процесорах. Метою проекту є визначення продуктивності обробки зображень в багатопотоковому режимі на одноядерних та багатоядерних процесорах.

Список літератури

1. Вільна енциклопедія Вікіпедія [Електронний ресурс] Режим доступу: http://uk.wikipedia.org/wiki/Багатоядерний_процесор
2. Крашенинников В.Р. Основы теории обработки изображений: Учебное пособие. / Крашенинников В.Р. – Ульяновск: УлГТУ, 2003. – 150 с.

УДК 004.738.2

Я.С. Попова

Науковий керівник – Стервєдов М.Г., канд. техн. наук, доцент
Харківський національний університет імені В.Н. Каразіна

Пристрій безпроводної передачі даних між ПК

Передача даних по радіоканалу в багатьох випадках надійніша та безпечніша, ніж передача по комутованих або орендованих каналах. У ситуаціях, коли відсутня розвинена інфраструктура зв'язку, використання радіозасобів для передачі даних часто є єдино розумним варіантом організації зв'язку. Величезну практичну цінність радіоканали мають там, де необхідна передача невеликих обсягів інформації.

Було розроблено пристрій для передачі даних по безпроводному каналу для виконання лабораторних робіт. Тому не було завданням оптимізації деяких технологічних параметрів, таких як створення зовнішнього корпусу для зручного використання або захист самого пристрою від зовнішніх механічних пошкоджень, так

як основним предметом роботи було розгляд пристрої як системи, яка сумісна з усіма типами персональних комп'ютерів. Такий підхід надає можливість краще вивчити електронні пристрої і дає поштовх для подальшого розроблення подібних пристроїв або модернізації цього.

Кожен пристрій обладнано передавачем і приймачем, тому може бути використано в двох напрямках, що дозволить забезпечувати повноцінний двонаправлений зв'язок між персональними комп'ютерами.

Безпосередньо пристрій можна розділити логічно на три основних функціональних частин: конектор RS-232 з інтерфейсною схемою MAX232, мікроконтролер і трансивер (передавач і приймач). Причому при взаємодії пристроїв між собою вони мають можливість працювати одночасно за схемою, яка представлена на рисунку 1.



Рисунок 1 – Взаємодія пристроїв між собою

У загальних рисах роботу пристрою можна описати таким чином: дані надходять з персонального комп'ютера на послідовний СОМ-порт за допомогою спеціальної заздалегідь встановленої програми, далі вони переходять на перетворювач рівнів RS-232 в рівні транзисторно-транзисторної логіки. Після перетворення двійковий код поступає на мікроконтролер, який їх відправляє на інтегровану схему передавача і далі в антену. При роботі на прийом пристрій працює по реверсивній схемі. В результаті обміну інформація виявляється на тому чи іншому персональному комп'ютері.

При роботі з модулями пристрою було вирішено встановити їх по схемі трикутника, що зменшило проблему перешкоди передавання інформації. Працює так - якщо інформація, передана з модуля В, не може дійти до модуля А напряму, то модуль В пересилає дані модулю С, а той в свою чергу модулю А і таким чином обминає перешкоди.

В ході розробки пристрою було використано стандартну плату для мікроконтролерів низької потужності AVR CMOS 8-бітних, мікроконтролер ATmega16,

передавач AM Hybrid Transmitter AM-RT4-XXX, приймач Radio Receiver telecontrolli RR10-XXX.

Пристрій був запрограмований на мові С в програмі Codevision. Суть програми полягає в тому, щоб зчитувати дані з послідовного порту RS-232, далі побігово розбити їх і передати на один з виходів мікроконтролера. Враховуючи очікування і затримки, програма виконує реверсивні операції в режимі прийому, тобто прочитує дані з входу контролера, далі зберігає їх (збирає біти в байти) в окрему змінну і передає на послідовний порт RS-232.

У підсумку було отримано пристрій для бездротової передачі даних між ПК. Предметом дослідження були апаратно-програмні засоби з системним підходом для надійного обміну інформацією. З точки зору актуальності пристрій цікаво як зв'язок між персональними комп'ютерами усередині однієї локальної мережі, коли з'єднання через Інтернет відсутнє або воно занадто небезпечно для передачі цінної інформації. Безпека передачі даних забезпечується кодуванням інформації і низьким рівнем побічних випромінювань передавача. При таких умови легше здійснити безпеку передачі і зберегти 3 основні властивості інформації: конфіденційність, доступність і цілісність.

Список літератури:

1. Ю.А.Шпак. Программирование на языке С для AVR и PIC микроконтроллеров, т. 1-2, Корона-Век, МК-Пресс,2011.
2. В. Трапперт. Измерение, управление и регулирование с помощью AVR-микроконтроллеров,2006.

УДК 004.75

А.А. Прачёв, С.А. Троцкий

Научный руководитель – Полторак В.П., канд. техн. наук, доцент
 Национальный технический университет Украины
 «Киевский политехнический институт»

Распараллеливание потока данных в MPLS сетях для повышения эффективности передачи данных

В сетях MPLS передача информации происходит в один поток. Возникает потенциально возможно возникновение эффекта «бутылочного горлышка».

Для решения этой проблемы предлагается концепция организации сети в несколько потоков. Речь идет о нахождении двух и более оптимальных маршрутов. Для этого обратимся к теории графов, где в качестве вершин будут выступать маршрутизаторы, а в качестве графов - линии связи.

Проанализированы три типа организации распараллеливания.

Первый тип организации MPLS сети (рисунок 1) наиболее простой: строятся два или более не пересекающихся друг с другом маршрута. Таким образом максимально разгружаются промежуточные маршрутизаторы. Этот вариант хорошо подходит для случаев, когда многие маршрутизаторы и линии связи простаивают.

Второй тип (рисунок 2) допускает пересечения маршрутов на маршрутизаторах, но исключает передачу трафика разных маршрутов по одним линиям связи.

Этот вариант модели применим для сетей, в которых между достаточно быстрыми маршрутизаторами находятся относительно медленные линии связи. Т.е. маршрутизаторы не будут выступать узким местом в сети.

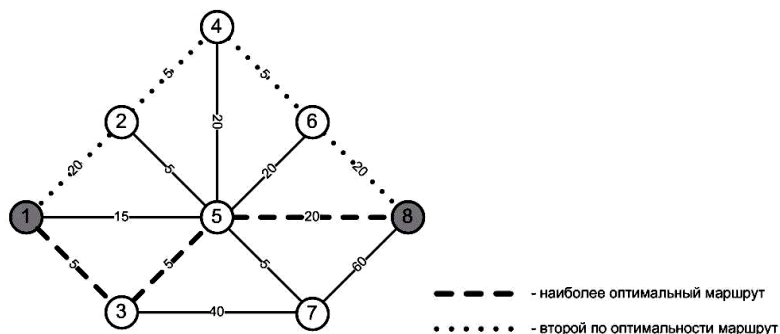


Рисунок 1 - Пример построения MPLS сети с распараллеливанием трафика с полностью изолированными оптимальными маршрутами

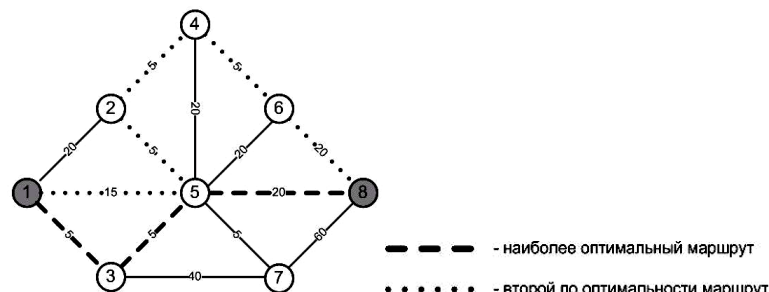


Рисунок 2 – Пример построения MPLS сети с распараллеливанием трафика с возможным пересечением оптимальных маршрутов на маршрутизаторах, но не совпадающими линиями связи

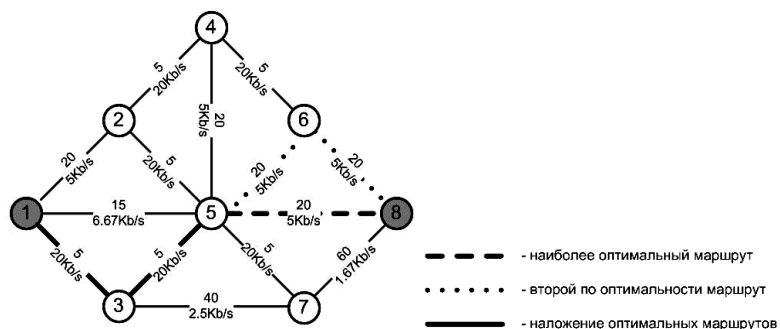


Рисунок 3 – Пример построения MPLS сети с распараллеливанием трафика с возможным пересечением оптимальных маршрутов и на маршрутизаторах, и на линиях связи

В третьем варианте (рисунок 3) не исключается возможность пересечения разных маршрутов на линиях связи, но проводится анализ по алгоритму:

- 1) пересекаются ли оптимальные маршруты на одной и той же вершине графа;
- 2) совпадают ли у оптимальных маршрутов графы, исходящие из данной вершины графа;
- 3) фиксируем количество маршрутов пытающихся пройти по совпадающему графу (для $X > 2$, где X – количество параллельных маршрутов);
- 4) достаточно ли пропускной способности для передачи увеличенного от двух, до X раз трафика и останавливаемся на максимально допустимом значении без потери скорости передачи относительно самого скоростного из «предыдущих» участков сети.

Список литературы

1. E. Rosen, Y. Rekhter, RFC-2547. BGP/MPLS VPNs. March 1999.
2. J. Malcolm, RFC-2702, Requirements for Traffic Engineering Over MPLS. September 1999.
3. A. Malis, RFC-2917, A Core MPLS IP VPN Architecture, September 2000.
4. E. Rosen. RFC-3031, Multiprotocol Label Switching Architecture, January 2001
5. В.Олифер, Н. Олифер, Сети на основе MPLS. Журнал сетевых решений LAN, январь 2002, стр. 58-63.
6. Д.Гринфильд, Глобальная служба MPLS: опережая время. Журнал сетевых решений LAN, март 2002, С.32-38.

УДК 004.738.5

О.О. Прокопов

Науковий керівник – Сидоренко В.В., д-р техн. наук, професор
Кіровоградський національний технічний університет

Розробка програмного забезпечення системи керування роботою клієнтської частини аукціону

Аукціон (ціновка; нім. Auktion, від лат. auctio — збільшення) — аукціон, що відбувається у мережі інтернет, учасники якого дистанційовані один від одного. На продаж можуть бути виставлені будь-які товари та послуги, від побутової техніки до ідей, проектів тощо. Перевагою Інтернет аукціону є легкий доступ до участі у ньому усіх користувачів.[1]

На основі досліджень і аналізу особливостей роботи клієнтської частини в мережі Інтернет.

Показано такі недоліки існуючих систем як одноманітність та те що вони являються вузькопрофільними. Тобто всі існуючі системи працюють за одним типом аукціонів задалегідь Англійським.

Метою роботи є створити систему яка б могла підтримувати декілька типів аукціонів в одній системі а також поліпшити умови управління системою для користувача. Тобто розробити легкий зрозумілий інтерфейс системи.

Аукціонний торг — це публічна (відкрита і загальнодоступна) послідовна реалізація товарних лотів тому з покупців, хто першим запропонував найвищу ціну. При цьому є три типи ведення аукціону: англійський; голландський і американський, або затемнений (рис. 1).

Так звані англійські аукциони проводиться в такому порядку:

- Аукціон веде в присутності організатора найманий ним ліцитатор. Аукціон починається з оголошення ліцитатором найменування, основних характеристик і початкової ціни предмета торгів і кроку аукціону.

Крок аукціону встановлюється організатором (не менше 5 % від стартової ціни) і залишається сталим протягом торгів. Учасникам аукціону видаються пронумеровані квитки, що їх вони піднімають після оголошення ліцитатором чергової ціни в разі, якщо готові купити предмет торгів за цією ціною.

Кожну наступну ціну ліцитатор признає збільшенням поточної ціни на крок аукціону. Після оголошення чергової ціни ліцитатор називає номер квитка учасника аукціону, який першим підняв квиток. Потім ліцитатор повідомляє наступну ціну згідно з кроком аукціону.

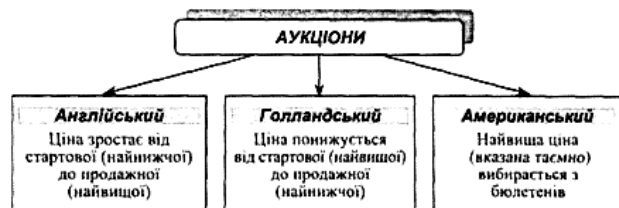


Рисунок 1 - Типи аукціонів

При відсутності учасників аукціону, готових купити предмет торгів за названою ліцитатором ціною, останній повторює цю ціну три рази.

- Аукціон завершується, якщо після трикратного оголошення чергової ціни жоден з учасників аукціону не підняв квиток. Переможцем аукціону визнається учасник, номер квитка якого був названий аукціоністом останнім.

Технологія проведення так званих голландських аукціонів аналогічна проведенню англійських аукціонів, однак вони розпочинаються з оголошення спочатку явно завищеної стартової ціни, що поступово знижується до тієї, за якою один з учасників торгу не висловить згоду купити товар.

При проведенні так званих американських аукціонів переможцем визнається особа, що запропонувала найвищу ціну за предмет торгів, яка зазначається у запечатаних конвертах. Визначення переможця відбувається на відкритому засіданні аукціонної комісії. Перед розкриттям конвертів комісія перевіряє цілісність конвертів, що фіксується в протоколі про результати торгів. Ціна повинна бути зазначена числом і прописом. У разі якщо числом і прописом зазначені різні ціни, комісія бере до уваги ціну, зазначену прописом. Пропозиції, що містять ціну нижче стартової, не розглядаються.

Дослідження показують, що найчастіше користувачі купують в онлайні предмети повсякденного попиту: одяг і дрібну побутову техніку. При цьому ефект пошуку online, покупки offline (ROPO-ефект) характерний для всіх категорій товарів

Віртуальна торгівля все ще не встигає за реальною. Хоча багато хто використовує Інтернет для збору відгуків про товар, порівняння цін, отримання консультацій та порад, покупки частіше здійснюються живцем. Тим не менш, частка online-продажів росте. Наприклад, компанія Google замовила дослідження про те, хто і що купує сьогодні в RUnetі, а учасники ринку online-продажів висловили свої поправки до отриманих результатів.

Список літератури

1. Висоцька В.А. Інтелектуальна система генерування профільних Web-сайтів / В.А. Висоцька, В.М. Дорош // Інформаційні системи та мережі. – 2012. – № 699. – С. 31-41.
2. Скоробагатів Д. Що таке веб-сайт [Електронний ресурс] / Дмитро Скоробагатів // Режим доступу: http://xbv.ua/web/Chsho_take_veb-sajt.
3. Ланде Д.В. Основи моделювання та оцінювання електронних інформаційних потоків: монографія / Ланде Д.В., Фурашев В.М., Брайчевский В.М. – К.: ТОВ “Інжиніринг”, 2006. – 348 с.

УДК 004.4

В.С. Салтан

Науковий керівник – Смірнов О.А., канд. техн. наук, доцент
Кіровоградський національний технічний університет

Розробка програмного забезпечення розрахунків показників QoS в мережах наступного покоління

Відповідно до принципів побудови мереж наступного покоління (Next Generation Network – NGN), заснованих на документах МСЕ-т, як технологічна база побудови транспортного рівня NGN передбачається технологія IP. Модель такої IP-орієнтованої мультисервісної мережі, що враховує особливості сучасної мережної інфраструктури, може бути представлена двома основними рівнями: рівнем послуг і транспортним рівнем.

У рамках розвитку NGN як єдиної мережі загального користування вирішуються завдання двох типів:

- короткострокові – стирання існуючої різниці в транспортуванні мови й даних, надання нових можливостей в області розвитку послуг, порівняльна простота реалізації при менших витратах щодо існуючих мереж;

- довгострокові – побудова простій і ефективний єдиної мережі для всіх видів додатків, здешевлення мережних компонентів, активний розвиток нових видів послуг.

Питання побудови мультисервісних мереж активно досліджуються в роботах вітчизняних (Б.С. Гольдштейн, А.Е. Кучерявий, А.Н. Назаров, Н.А. Соколов, С.Н. Степанов, М.А. Шнепс-Шнеппе, Г.М. Яновский) і закордонних (U. Black, J. Davidson, S. Fisher, J.M. Garcia, D. McDysan, D. Minoli, F.A. Tobagi) авторів.

У даній роботі ставляться й вирішуються завдання, пов'язані з розробкою моделей оцінок показників якості обслуговування в NGN з урахуванням особливостей трафіку таких мереж. У ряді публікацій (M. Crovella, W. Leland, S. Molnar, K. Park, M. Taqqu, W. Willinger) показано, що трафік IP-мереж може описуватися з використанням самоподібних процесів. Теоретичні дослідження самоподібних процесів у СМО розглядаються в роботах М.Н. Неймана (1998), Б.С. Цыбакова (1999), В.С. Зборовского (2000), О.И. Шелухина (2003).

Однак питання дослідження якості обслуговування (Quality of Service, QoS) в IP-орієнтованих мультисервісних мережах з урахуванням властивостей самоподоби трафіку залишаються відкритими, що й визначає актуальність роботи.

Метою роботи є розробка моделей розрахунку показників якості в мережах NGN з урахуванням особливостей трафіку IP-орієнтованих мультисервісних мереж і впливу кінцевих пристроїв.

Для досягнення поставленої мети в роботі вирішуються наступні завдання:

- аналіз трафіку різних додатків в IP-орієнтованих мультисервісних мережах з урахуванням властивостей самоподоби;
- розробка моделей розрахунку значень основних показників наскрізного QoS для різних додатків;
- оцінка впливу кінцевих пристроїв на показники QoS для мовного пакетного трафіку;
- дослідження взаємного впливу трафіку різних додатків у мультисервісних мережах з позицій забезпечення якості обслуговування.

Об’єктом дослідження є процес забезпечення QoS в мережах наступного покоління. Предмет дослідження – методи й алгоритми розрахунків показників QoS в мережах наступного покоління.

Проведені дослідження базуються на теорії ймовірностей, теорії масового обслуговування, теорії фрактальних процесів і методах імітаційного моделювання.

Список літератури

1. McDysan. “QoS and Traffic Management in IP and ATM Networks”. McGraw-Hill.2000.
2. Е.А. Кучерявий. Управление трафиком и качество обслуживания в Интернет. СПб, Наука и Техника. 2004.
3. Р. Кох, ГГ. Яновский. “Эволюция и конвергенция в электросвязи”. М., Радио и связь. 2001.
4. МСЕ-т Recommendation Y.1541. “Network Performance Objectives for IP-Based Services”. May 2002.
5. Лагутин В.С. Оценка характеристик пропускной способности мультисервисных пакетных сетей при реализации технологии разделения типов нагрузки. “Электросвязь”, №3, 2003.
6. Gunnar Ronneberg and Olav Lysne. “An OPNET-based Simulation Model of SCI-nodes”.
7. Debasis Mitra, K. G. Ramakrishnan, “Techniques for traffic engineering of multiservice, multipriority networks”. BLTJ. - 2001. - Vol.1.- №1.
8. Лихтциндер Б.Я., Попов П.М. Инжиниринг трафіку в мультисервісних сетях. «Электросвязь», №7, 2005.

УДК 004.4

Ф.О. Семенов

Науковий керівник – Якименко Н.М., канд. фіз.-мат. наук, доцент
Кіровоградський національний технічний університет

Розробка програмного забезпечення методу виявлення аномалій телекомунікаційного трафіку на основі спектрально-часового аналізу

Активне використання на сучасний час розподілених комп’ютерних систем та мереж приводить до необхідності приділяти увагу питанням безпеки.

Особливе місце в реалізації політики безпеки організації займають системи виявлення вторгнень (подій з безпекою) (СВВ), які можуть як виконувати функцію зворотного зв’язку, контролюючи ефективність компонентів системи безпеки, тобто бути, як доповненням до існуючого комплексу засобів захисту, так і являти собою самостійний продукт.

Впровадження багатьох СВВ, як і комплексних систем безпеки, стримує ряд факторів, таких як одноразові капіталовкладення, необхідність компетентної установки, настроювання, підтримки й т.д. У таких компаніях, як правило, функція спостереження за роботою мережі покладається на адміністратора. У такому випадку результат залежить від людського фактора, що включає досвід, інтуїцію, відповідальність, працездатність і т.п. Слід зазначити, що практично в кожній компанії, що має в розпорядженні розподілену мережу, установлені засоби збору статистичних даних про завантаження інтерфейсів мережного встаткування. Таким чином, закономірним кроком до автоматизації процесу виявлення позаштатних ситуацій, є впровадження доступного й, можна сказати, універсального засобу, що аналізує інтенсивності потоків даних у пошуку незвичайних і підозрілих подій або тенденцій, яке можна віднести до підкласу СВВ.

При цьому може використовуватися як сигнатурний метод, так і метод описової статистики. Математично обґрунтованими видами аналізу часових рядів є дослідження

сигналу на основі часових, спектральних і спектрально-часових алгоритмів, які інтенсивно розвиваються останнє з невеликим десятиліттям.

Аналіз у часовій області ґрунтується на методах математичної статистики і його можливості досить великі. Але слід зазначити, що досліджуваному телекомунікаційному сигналу властиво «виражене коливальне поводження» через його особливості його формування. Хоча в методах часового аналізу існують підходи для опису такого роду сигналів, найбільш підходящими для дослідження коливального процесу є методи спектрального й спектрально-часового аналізу. Частотні подання є більше інформативними й дозволяють розширити можливості існуючих систем виявлення аномалій, але вимагають більших розмірностей для подання результатів і мають більшу обчислювальну складність алгоритмів, що стримує їхнє застосування й розвиток у прикладних завданнях. Отже, є актуальною розробка методу виявлення аномалій в інтенсивностях потоків даних на основі алгоритмів аналізу частотних складових, оптимізованих по обчислювальному навантаженню.

Метою роботи є розробка підвищуючого безпеку функціонування мережі методу виявлення аномалій у даних про завантаження інтерфейсів телекомунікаційного встаткування, на основі аналізу частотних характеристик; оптимізація по обчислювальному навантаженню формуючих метод зсувних спектральних і спектрально-часових алгоритмів з одержанням математичних моделей оптимізації й дослідження особливостей і обмежень використання частотного подання в розглянутому додатку.

Завдання досліджень включають: дослідження спектральних і спектрально-часових алгоритмів аналізу й подання часових рядів, у тому числі визначення особливостей і обмежень їхнього використання в області застосування; дослідження алгоритмів спектрального розкладання, у тому числі з урахуванням зрушень аналізованої послідовності, із пропозицією математичної моделі оптимізації обчислень; дослідження формування областей впливу й вірогідності картини вейвлет-коефіцієнтів при реалізації алгоритмів спектрально-часового аналізу.

Пропозиція математичної моделі оптимізації алгоритмів спектрально-часового розкладання, у тому числі з урахуванням зрушень аналізованої послідовності й області вірогідності коефіцієнтів розкладання.

Пропозиція способу зменшення області невірогідності за рахунок введення в аналіз так званого довірчого простору вейвлет-коефіцієнтів.

Формування теоретичної й практичної бази для методу виявлення аномалій у результаті дослідження впливу особливостей сигналу на вейвлет-коефіцієнти.

Розробка методу виявлення аномалій у даних про завантаження інтерфейсів мережного встаткування на основі аналізу частотних характеристик.

Об’єктом дослідження є процес виявлення аномалій телекомунікаційного трафіку. Предмет дослідження – методи виявлення аномалій телекомунікаційного трафіку на основі спектрально-часового аналізу. Методи дослідження базуються на теорії ймовірностей і математичної статистики, теорії розпізнавання образів, теорії обчислювальних систем і мереж.

Список літератури

1. Будько М.Б., Будько М.Ю. Отслеживание изменений в структуре сети и решение задач повышения безопасности на основе анализа потоков данных // Научно-технический вестник Санкт-петербургского гос. ун-в. информац. технол., механики и оптики. №59. – СПб.: СПбГУ ИТМО. – 2009. – С. 78-82.
2. Будько М.Б. Определение источника широковещательного шторма на основе данных протокола SNMP // Сборник трудов конф. мол. ученых. № 6. Информац. технолог.–СПб.: СПбГУ ИТМО.–2009.–С.153-157
3. Будько М.Б., Будько М.Ю., Гирик А.В. Применение авторегрессионного интегрированного скользящего среднего в алгоритмах управления перегрузками протоколов передачи потоковых данных // Научно-технический вестник СПбГУ ИТМО. – 2007. – № 39. – С. 319-323.

УДК 004.4

Р.С. СербінНауковий керівник – Дреєв О.М., викладач
Кіровоградський національний технічний університет

Програмне забезпечення моніторингу локальної мережі та відстежування дій користувачів

Однією з важливих особливостей сучасних корпоративних мереж є їхній розмір, що найчастіше обчислюється тисячами, а й іноді й десятками тисяч комп’ютерів. При цьому діяльність користувачів може бути розподілена серед різних комп’ютерів, а та сама проблема часто вирішується групами користувачів. Важливим завданням є контроль роботи, як окремих користувачів, так і груп користувачів.

Основними цілями контролю є: забезпечення інформаційної безпеки, виявлення випадків некоректного, непрофесійного або нецільового використання ресурсів, оцінка характеристик функціонування корпоративної мережі й параметрів використання ресурсів. Основним завданням забезпечення інформаційної безпеки є «раннє виявлення» внутрішніх вторгнень, тобто виявлення дій користувачів, які можуть передувати внутрішнім вторгненням. Чим крупніша організація, тим актуальнішою є для неї проблема запобігання внутрішніх вторгнень, зокрема крадіжки інформації, тому що саме крадіжка є кінцевою метою більшості внутрішніх вторгнень. Зв’язано це з тим, що в великих організаціях утрудняється контроль над обігом інформації й істотно зростає ціна її витоку. Зазначені обставини визначають високий рівень заклопотаності даною проблемою з боку великого бізнесу й урядових організацій. Рішення даної проблеми полягає в застосуванні "твердої" політики інформаційної безпеки в організації й використанні засобів моніторингу дій користувачів.

Таким чином, розробка програмного забезпечення моніторингу локальної мережі та відстежування дій користувачів є актуальною задачею.

Список літератури

1. Cisco Systems, Inc. Internetworking Technology Handbook, 4-th Edition. /Indianapolis: CiscoPress, Sept. 2003.
2. Терентьев А.М. Информационная безопасность в крупных локальных сетях / Концепции, №1(9),2002,С. 25-30.
3. Сторожук Д.О. Увеличение безопасности работы в локальной сети при использовании систем мониторинга / Гусева А.И., Сторожук Д.О. //Безопасность информационных технологий.–2007, №1.–С. 46-50.

УДК 004.056.55

О.О. СуворовНауковий керівник – Сидоренко В.В., ст. викладач
Кіровоградський національний технічний університет

Використання мультисерверної архітектури в сучасних СУБД

В сучасних СУБД механізм організації взаємодії процесів типу «клієнт» та процесів типу «сервер». В основному даний механізм визначається структурою реалізації серверних процесів та часто називається архітектурою сервера баз даних. Спочатку існувала модель, коли керування даними (функція сервера) та взаємодія з користувачем були об’єднані в одній програмі. Далі функції керування даними були

виділені в самостійну групу – сервер, однак модель взаємодії користувача з сервером відповідала парадигмі «один до одного», тобто сервер виконував обробку запитів тільки одного користувача (клієнта), та для обслуговування декількох клієнтів потрібно було запустити еквівалентне число серверів. Для обслуговування великої кількості клієнтів на сервері повинна бути запущена велика кількість одночасно працюючих серверних процесів, а це різко підвищувало вимоги до ресурсів ЕОМ. Така модель є самою простою та історично вона з’явилась першою.

Проблеми, які притаманні моделі «один до одного», вирішуються в архітектурі «систем з відселеним сервером», який може обробляти запити від багатьох клієнтів. Сервер єдиний монополює керує даними та взаємодіє одночасно з багатьма клієнтами. Логічно клієнт зв’язаний з сервером окремим потоком, по якому передаються запити. Така архітектура отримала назву багатопоточна односерверна («multi-threaded»). Вона дозволяє значно зменшити навантаження на ОС, яке виникає при роботі великої кількості користувачів.

До недоліків даної моделі можна віднести, з причин того, що сервер може виконуватися тільки на одному процесорі, виникає неможливість використання і багатопроцесорних системах всіх процесорів. В деяких системах дана проблема вирішується введенням проміжного диспетчера. Така архітектура називається архітектурою віртуального сервера («Virtual Server»). В такій архітектурі клієнти підключаються не до реального сервера, а до проміжного, який називається диспетчером, який виконує тільки функцію розподілення запитів між серверами. В даному випадку немає обмежень на використання в багатопроцесорних системах. Основним недоліком такої моделі є те, що з’являється новий шар між сервером та клієнтом, що збільшує витрату ресурсів, навантажує систему.

Дана система працює нормально, якщо всі звернення матимуть однаковий пріоритет, але, наприклад, якщо потрібно обробити окремо, швидкий запит, скажімо з більш високим пріоритетом, то одразу починаються проблеми.

Сучасне рішення СУБД для багатопроцесорних платформ полягає в можливості запуску декількох серверів БД, в тому числі і на різних окремих процесорах. При цьому кожен з серверів повинен бути багатопоточним. Якщо ці дві вимоги виконанні, то кажуть, що реалізована таким чином багатопоточна архітектура з декількома серверами.

Дана модель ще називається просто мультисерверна. Ця архітектура зв’язана з питаннями розпаралелювання виконання одного користувацького запиту декількома процесами. Існує декілька варіантів розпаралелювання виконання запиту. Користувацький запит розбивається на ряд підзапитів, які можуть виконуватися паралельно, а результати їх виконання потім об’єднуються в загальний результат виконання запиту. Тоді для забезпечення оперативності виконання запитів їх підписи можуть бути направлені окремими серверними процесами, а потім отримані результати об’єднані в загальний результат.

В даному випадку серверні процеси не являються незалежними процесами. Ці серверні процеси прийнято називати потоками, та керування потоками великої кількості запитів користувачів потребує додаткових витрат від СУБД, однак при оперативній обробці інформації в сховищах даних такий підхід найбільш перспективний.

Список літератури

1. К. Дж. Дейт. Введение в системы баз данных. – 2006г., 1328 с.
2. Д. Кренке. Теория и практика построения баз данных. – 2005 г., 800 с.
3. Рэймонд Фрост, Джон Дей. Базы данных. Проектирование и разработка. – 2007, 592с.

В.В. Сурін

Науковий керівник – Сидоренко В.В., д-р техн. наук, професор
Кіровоградський національний технічний університет

Розробка програмного забезпечення системи керування роботою адміністративної частини аукціону

Аукціон (ціновка; нім. Auktion, від лат. auctio — збільшення) — аукціон, що відбувається у мережі інтернет, учасники якого дистанційовані один від одного. На продаж можуть бути виставлені будь-які товари та послуги, від побутової техніки до ідей, проектів тощо. Перевагою Інтернет аукціону є легкий доступ до участі у ньому усіх користувачів.[1]

На основі досліджень і аналізу особливостей роботи адміністративної частини в мережі Інтернет. Метою роботи є створення системи яка б дала змогу контролювати аукціон в якому використовується декілька типів систем одночасно.

Розробити досконалу систему роботи системи з базою даних (БД) — впорядкований набір логічно взаємопов'язаних даних, що використовуються спільно, та призначені для задоволення інформаційних потреб користувачів. У технічному розумінні включно й система керування БД.

Головним завданням БД є гарантоване збереження значних обсягів інформації (т.зв. записи даних) та надання доступу до неї користувачеві або ж прикладній програмі. Таким чином БД складається з двох частин: збереженої інформації та системи управління нею.

З метою забезпечення ефективності доступу записи даних організують як множину фактів (елемент даних).

Віртуальна торгівля все ще не встигає за реальною. Хоча багато хто використовує Інтернет для збору відгуків про товар, порівняння цін, отримання консультацій та порад, покупки частіше здійснюються живцем.

Тим не менш, частка online-продажів росте. Наприклад, компанія Google замовила дослідження про те, хто і що купує сьогодні в RUnetі, а учасники ринку online-продажів висловили свої поправки до отриманих результатів.

Список літератури

1. Висоцька В.А. Интеллектуальная система генерування профільних Web-сайтів / В.А. Висоцька, В.М. Дорош // Інформаційні системи та мережі. – 2012. – № 699. – С. 31-41.
2. Скоробагатів Д. Що таке веб-сайт [Електронний ресурс] / Дмитро Скоробагатів // Режим доступу: http://xbb.ua/web/Chsho_take_veb-sajt.
3. Ланде Д.В. Основи моделювання та оцінювання електронних інформаційних потоків: монографія. / Ланде Д.В., Фурашев В.М., Брайчевский В.М. – К.: ТОВ “Інжиніринг”, 2006. – 348 с.

С.А. Троцкий, А.А. Прачёв

Научный руководитель – Полторак В.П., канд. техн. наук, доцент
Национальный технический университет Украины
«Киевский политехнический институт»

Построение универсальной информационной системы с повышенной надежностью

«Корпоративные вычислительные сети» (КВС) – это разновидность информационно-телекоммуникационных систем (ИТС). Любая КВС состоит из управляющих и управляемых узлов. Базовые подходы к построению КВС даны в [1]. Существующие методы повышения надежности телекоммуникационных систем (ТС) в целом [2-3] основываются на резервировании элементов, но при этом не решается основной проблемы ненадежности – существования узлов, выход из строя которых, приводит к отказу всей системы (SPOF –Single Point of Failure). Гомогенное резервирование – подход к проектированию КВС, где узел представляет собой программный процесс, который выполняется в кластере и принадлежит множеству узлов информационного облака (ИО). В случае отказа одних узлов их функции передаются остальным. Каждый узел хранит данные, но при этом он делает копию этих данных на других узлах. Все данные равномерно распределены и обрабатываются параллельно. Базовая архитектура на языке UML, гомогенной системы, представлена на рисунке 1.

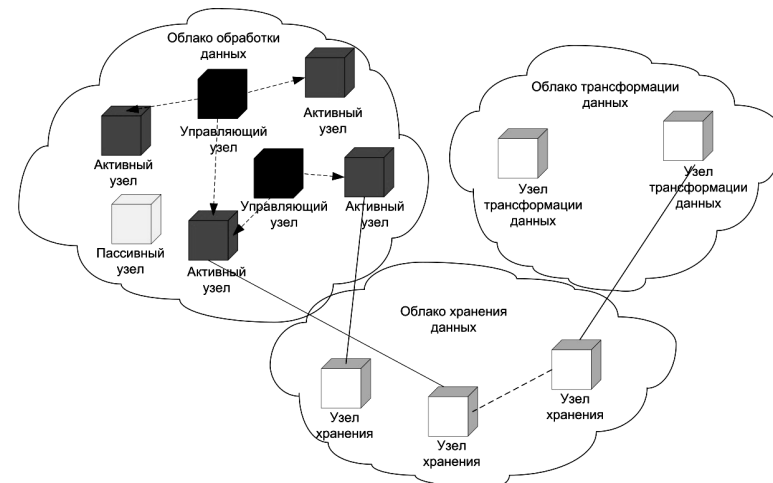


Рисунок 1 – Базовая модель гомогенной системы на языке UML

Облако обработки данных – информационное облако (ИО), входными параметрами которого является множество { алгоритм, данные }. Облако обработки данных (ООД) состоит из узлов, которые могут быть в одном из трех состояний <Активный узел, Пассивный узел, Управляющий узел>. Активный узел(active node) –

узел, который в текущий момент времени занят обработкой данных. *Пассивный узел(idle node)* – узел, который в текущий момент времени не занят обработкой данных, и не является *Управляющим узлом. Управляющий узел(master node)* - узел, который в текущий момент времени занят координацией *Активных узлов* и *Пассивных узлов. Облако хранения данных (ОХД)* – ИО хранения данных, которые состоят из *Узлов хранения. Узел хранения* – узел распределенной базы данных. *Облако трансформации данных (ОТД)* - ИО взаимодействия с внешними системами. *Узел трансформации данных* – узел главная задача, которого обеспечивать обмен данных между *Облаком хранения данных* и внешними системами. Система, на рисунку 1, может находиться в оном из (*КУОТД + КУОХД + КУООД*) состояний. Суммарная вероятность выхода из строя всей системы p_R вычисляется по следующей формуле (состояние $S_{КУОТД+КУОХД+КУООД-1}$):

$$p_R = 1 - (1 - p_{ООД} (КУООД)) * (1 - p_{ОХД} (КУОХД)) * (1 - p_{ОТД} (КУОТД))$$

$p_{ООД} (КУООД)$ - вероятность отказа ООД, которая является функцией от количества узлов ООД (КУООД);

$p_{ОХД} (КУОХД)$ - вероятность отказа ОХД, которая является функцией от количества узлов ОХД (КУОХД);

$p_{ОТД} (КУОТД)$ - вероятность отказа ОТД, которая является функцией от количества узлов ОТД (КУОТД).

Вероятность p_0 начального состояния S_0 (все узлы работоспособны) каждого ИО вычисляется по формуле:

$$p_0 = (1 + \frac{\lambda_1}{\mu_1} + \frac{\lambda_1 \lambda_2}{\mu_1 \mu_2} + \frac{\lambda_1 \lambda_2 \lambda_3}{\mu_1 \mu_2 \mu_3} + \frac{\lambda_1 \lambda_2 \lambda_3 \lambda_4}{\mu_1 \mu_2 \mu_3 \mu_4} + \dots + \frac{\lambda_1 \lambda_2 \lambda_3 \lambda_4 \dots \lambda_n}{\mu_1 \mu_2 \mu_3 \mu_4 \dots \mu_n})^{-1}$$

Расчет вероятности множества состояний $\{ S_1 \dots S_n \}$ любого ИО вычисляется согласно системе, где одно из уравнений – рекурсивная формула:

$$P_i = \begin{cases} \frac{(n-i+1)\lambda}{i\mu} P_{i-1}, & \text{для } i \neq 1 \\ n\lambda \left(\frac{1 - \left(\frac{\lambda}{\mu}\right)^n}{1 - \frac{\lambda}{\mu}} \right)^{-1}, & \text{для } i = 1 \end{cases}$$

Управляя лишь одним параметром в системе (количеством узлов информационного облака), задаются характеристики надёжности. Зависимость между надёжностью и количеством узлов – линейная в логарифмическом масштабе.

Список літератури

1. Forschungsberichte des Fachbereichs Informatik, Bericht Nr. 99-9 Federated Information Systems: Concepts, Terminology and Architectures
2. Богатырев В.А. Отказоустойчивые многомашинные вычислительные системы динамического распределения запросов при дублировании функциональных ресурсов / Изв. вузов. Приборостроение. 1996, № 4.
3. Дилон Б., Сингх И. Инженерные методы обеспечения надежности систем. М: Мир, 1984.
4. Шшмарев В.Ю. Надежность технических систем. – Москва. Издательский центр «Академия» 2010. с.149-152
5. Алиев Т.И. Основы моделирования дискретных систем. – Санкт-Петербург. ИТМО 2009. с182-189
6. Вентцель Е.С. Исследования операций: задачи, принципы, методология. – Москва 2006. С 137-138

УДК 004.4

К.С. Цимбал

Науковий керівник – Коваленко О.В., канд. техн. наук, ст. викладач
Кіровоградський національний технічний університет

Розробка програмного забезпечення системи відеоспостереження на базі бездротових мереж

Сучасні системи обробки візуальної інформації можуть містити в собі канали бездротової передачі даних. До таких систем, зокрема, відносяться охоронні комплекси відеоспостереження.

Більшість подібних систем побудовано на базі технології IEEE 802.11. Розвиток сучасних бездротових технологій дозволяє передавати по радіоканалу значні обсяги інформації на швидкостях, порівнянних з передачею по провідних каналах зв'язку. У той же час нескладно показати низьке використання пропускної здатності реальних бездротових каналів зв'язку. Технологічно вдосконалюється фізичний рівень: міняються способи модуляції, удосконалюються способи обробки сигналів і збільшуються бітова швидкість передачі й чутливість приймача.

Розвиток методів каналного кодування трохи відстає від розвитку методів кодування фізичного рівня. Більше того, при подальшому збільшенні швидкості передачі протокол керування доступом до середовища стає вузьким місцем всієї системи, не дозволяючи одержати відчутний приріст пропускної здатності навіть при застосуванні самих високоефективних технологій фізичного рівня. Приміром, максимальний теоретичний відсоток використання пропускної здатності каналу для стандарту IEEE 802.11n з бітовою швидкістю 108 Мбіт/с становить 51 %.

Підвищити даний показник можна, застосувавши принцип системного підходу до проектування системи обробки візуальної інформації. Найбільшу складність у цьому випадку представляє проектування каналного рівня. При проектуванні системи кодування каналного рівня необхідно вирішити завдання оптимального проектування на вибір методу кодування і його параметрів.

Проблемам керування передачею даних у бездротових мережах присвячена значна кількість досліджень. Серед найбільш відомих праць, присвячених цим проблемам, варто віднести роботи російських і закордонних учених: А.В. Віеля, В.М. Вишневого, А.І. Ляхова, А.П. Моше-Вікіна, В. Столлінгса, І.В. Шахновича.

Метою розробки є розробка програмного забезпечення, яке призначено для системи відеоспостереження на базі бездротових мереж.

Для досягнення поставленої мети вирішуються наступні завдання:

1. Розробка алгоритмів керування передачею відеозображень реального часу й дослідження їхньої ефективності.
2. Розробка й створення елементів керування системи бездротового відеоспостереження реального часу.
3. Аналіз і реалізація програмно-алгоритмічного забезпечення керування передачею даних для додавання можливості формування MAC-кадрів великої довжини по каналі спеціалізованого приймачепередатчика стандарту IEEE 802.15.4a (nanoNET). Об'єктом дослідження є процес відеоспостереження.

Предметом дослідження є система відеоспостереження на базі бездротових мереж.

Методи досліджень засновані на застосуванні теорії системного аналізу, теорії імовірності й випадкових процесів, статистичної теорії зв'язку, теорії завадостійкого кодування, обчислювальної математики й імітаційного моделювання.

Список літератури

1. Томас Конноли, Каролин Бегг. Проектирование, реализация и сопровождение. Теория и практика: Пер. с англ. М.: Изд. Вильямс, 2001.
2. Гончаров Р.В., Любимов М.Ф. Компьютеры и программы. – Ростов-на-Дону: РГЭА, 2004.– 206 с.
3. Попков А.И. Программное обеспечение.– М.: Радио и связь, 2006.– 389 с.
4. Сафронов И.К. Практикум по информатике.– СПб.: БХВ-петербург, 2006.– 432 с.

УДК 004.4

Б.О. Шевкун

Науковий керівник – Коноплицька О.К., асистент
Кіровоградський національний технічний університет

Програмне забезпечення браузера для перегляду веб-сайтів

Браузер являє собою програмний додаток, що здійснює пошук, доступ і перегляд веб-сторінок. Браузери переводять HTML код, що дозволяє читати текст, переглядати зображення, дивитися відео, грати в онлайн ігри й прослуховувати аудіо кліпи на веб-сайтах. Вони також інтерпретують гіперпосилання, які при натисканні відкривають інші веб-сторінки, дозволяючи «подорожувати» по інтернету. За допомогою додатків (наприклад: FTP клієнт FireFTP, плагін Mozilla Firefox), деякі інтернет-браузери можуть використовуватися для доступу до конфіденційної інформації на веб-серверах або файлових системах. Незважаючи на те, що всі браузери мають доступ в інтернет, різні браузери відкривають веб-сторінки по-різному. У цій продуктивності й полягає їхня конкуренція. Існують три основних фактори, при розробці інтернет-браузера:

1. Простота й набір функцій. Веб-браузер повинен зробити веб-серфінг простим і швидким. Це значить наявність оперативної системи закладок, панелі інструментів, що налаштовуються, і убудовану систему пошуку.
2. Швидкість і сумісність. Веб-браузери повинні швидко завантажуватися, бути сумісними з усіма основними операційними системами й переміщатися між сторінками протягом декількох секунд.
3. Безпека. З моменту створення Інтернету потрібний захист від атак, спрямованих на злом електронних даних. Функції безпеки, такі як параметри конфіденційності, блокувальники спливаючих вікон і шпигунських програм і допомога в збереженні особистої інформації, такий як логини й паролі.

Таким чином, розробка програмного забезпечення браузера для перегляду веб-сайтів є актуальною задачею.

Список літератури

1. Фаронов В. Delphi 2005. Разработка приложений для баз данных и Интернета, Изд.: Питер - 2006 г.
2. Топорков С. Альтернативные браузеры, Изд.: ДМК ПРЕСС - 2006 г.
3. Абрамян М. Э., Delphi 7. Карманный справочник с примерами, Изд.: КУДИЦ-ПРЕСС - 2006 г.
4. Гофман А., Хомоненко А., Гофман В. Delphi, Изд.: БХВ-Петербург - 2002

УДК 004.4

В.В. Шпурік

Науковий керівник – Дресев О.М., викладач
Кіровоградський національний технічний університет

Програмне забезпечення системи обміну миттєвими повідомленнями у мережі Інтернет

Миттєва передача повідомлень стала дуже популярним методом онлайн комунікації. Вона виявилася набагато зручнішою і швидшою ніж електронна пошта, тому що повідомлення між користувачами передаються в режимі реального часу, дозволяючи користувачам вільно розмовляти, до того ж такий тип зв'язку набагато дешевше телефонних дзвінків, оскільки використання основних функцій передачі повідомлень будь-якого месенджера стануть безкоштовним.

Для персональних користувачів месенджери – це відмінний спосіб залишатися на зв'язку із друзями, особливо, якщо ці користувачі живуть далеко друг від друга (у цьому випадку телефонні розмови можуть бути дорогим задоволенням, а електронна пошта – занадто офіційною). Для бізнес-користувачів такі комунікації можуть стати швидким способом підтримки контактів з колегами й менш нав'язливим, ніж телефонна розмова, під час якої у вашого колеги просто не буде часу обмірковувати свою відповідь.

Більшість месенджерів дозволить користувачам персоналізувати свою програму, шляхом додавання своїх фотографій або підключення веб-камер, що дозволяють іншим користувачам бачити, як вони виглядають. Для тих, хто соромиться камер, призначена функція використання анімованих роликів за участю користувача в якості аватара, відомих як WeeMees або Klonies, які можна створити онлайн.

Отже, розробка програмного забезпечення системи обміну миттєвими повідомленнями у мережі Інтернет є актуальною задачею

Список літератури

1. Олифер В. Г., Олифер Н. А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 3-е издание. С.-Пб.: "Питер", 2005 – 960 с.
2. Таненбаум Э. Компьютерные сети (3-е изд.). Пер. с англ. – С.-Пб.: "Питер", 2002 – 848 с.

УДК 004.738.5

Д.Г. Шевченко

Науковий керівник – Бісюк В.А., викладач
Кіровоградський національний технічний університет

Дослідження перспектив використання мови програмування Google Blockly

В даній роботі представлено нову візуальну мову програмування Google Blockly компанії Google, яка дозволяє створювати програми без введення яких-небудь символів або тексту, маніпулюючи тільки набором типових логічних блоків, з'єднання яких, нагадує складання пазла, дозволяє реалізовувати задану алгоритмічну функціональність. Технічно ця візуальна мова реалізована на JavaScript і дозволяє складати програми прямо в браузері, просто перетягуючи і компонуючи в логічні

ланцюжки блоки, після чого така програма може бути скомпільована в більш традиційну цільову мову, таку як JavaScript, Dart або Python. Код проекту поширюється під ліцензією Apache.

Ідеєю створення Blockly послужив схожий проект AppInventor, який спочатку розвивався для платформи Android [1]. При цьому сам AppInventor в свою чергу був натхненний мовою Scratch. Існує альтернативна розробка Scratch, яку принципово зробив відкритим Каліфорнійський університет в Берклі (University of California at Berkeley) - це Snap (також відомий як Build Your Own Blocks).

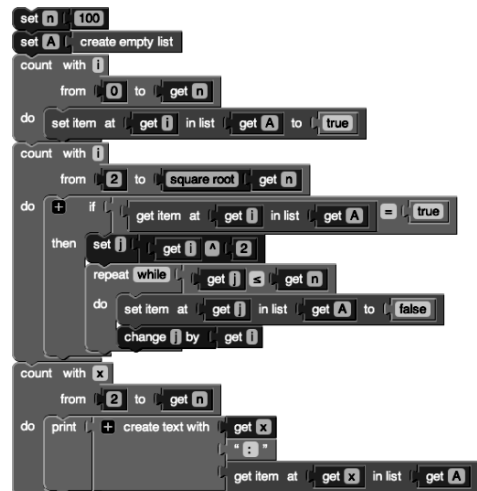


Рисунок 1 – Приклад програми, створеної в Google Blockly

Від інших мов візуального програмування, яких налічується близько сотні, Blockly відрізняється двома принциповими моментами. По-перше, це сильний акцент на візуальність складової розробки; за аналогією з високорівневими мовами запропоновано називати подібний тип мов "сильно-візуальними". Такий підхід затребуваний для нових сенсорних пристроїв, де введення традиційного тексту утруднений, крім того така форма програмування, як показує досвід, має набагато більш легкий поріг входження, зокрема програми на Google Blockly складають навіть діти.

Другий принциповий момент - це можливість крос-компіляції в традиційні мови програмування, що створює умови для реалізації самих різних підходів щодо подальшого розвитку проекту [2]. Наприклад, окремі частини програми можуть дуже швидко створюватися на Google Blockly, потім після компіляції, наприклад в Python, вихідний код такої програми може бути доопрацьований вже на Python, або навіть вставлений у вже готовий проект в цілях його розширення. В останньому випадку наводиться приклад створення на Google Blockly розширення до Gmail для забезпечення фільтрації листів. Google вважає, що це типовий випадок в сучасному програмуванні, наприклад при написанні якогось розширення до офісного пакету близько 90% коду реалізує "корисну логіку", а 10% - просто код сполучення цього розширення з API хост-програми. Google вважає, що в такому випадку дуже зручно швидко "зібрати" власне логіку додатку на Google Blockly, тоді як весь більш низькорівневий код роботи з API - дописати вже на Python або Dart.

Поточне тимчасове обмеження мови - вона не призначена для створення великих додатків. Поки область його застосування - невеликі сервісні скрипти, які містять складну логіку і багаторазово вкладені логічні і циклічні конструкції, які, на думку фахівців Google, простіше складати саме на Google Blockly. Окремо підкреслюється, що в наступних версіях цієї візуальної мови планується суттєво розширити її семантику, що по завіреннях Google зробить її можливості порівнянними з традиційними мовами програмування. Тому не слід розглядати цю мову лише як повчальну - в майбутньому планується створення повноцінної мультиплатформової мови програмування на його базі. Саме з причини майбутнього розширення цієї мови

прийнято рішення не використовувати підхід упаковки логіки у вже поширені умовно-символічні програмні схеми (data-flow metaphor languages), так як експерименти показали, що такий спосіб представлення важко піддається розширенню і застосований виключно до вузькоспеціалізованих областях програмування.

Розробка здійснюється безпосередньо в браузері, в процесі розробки програми її проміжні результати зберігаються і знову завантажуються у форматі XML. Google Blockly підтримує не тільки звичайні цикли і розгалуження, але і рекурсію. Найближчим часом планується реалізувати: елементи налагодження, підтримку мобільних пристроїв, роботу з курсором для кращої зручності роботи, генерацію коду для пристроїв на базі Arduino. Будуть додані найпростіші елементи подієво-орієнтованого програмування - виклик обробників при виникненні певних ситуацій або змін. У самий найближчий час планується суттєво поліпшити документацію, одночасно додавши безліч нових блоків, а також реалізувати можливість передачі параметрів в процедури і функції. Над логічними блоками (або відразу масивом з блоків) буде забезпечений набір візуальних операцій drag & drop, cut, copy і paste.

Нижче наведено експортований в JavaScript лістинг програми [3], яка була складена за допомогою Google Blockly (рисунок 1):

```

var n;
var A;
var i;
var x;
var j;
n = 100;
A = [];
for (i = 0; i <= n; i++) {
    A[i - 1] = true;
}
var i_end = Math.sqrt(n);
for (i = 2; i <= i_end; i++) {
    if (A[i - 1] == true) {
        j = Math.pow(i, 2);
        while (j <= n) {
            A[j - 1] = false;
            j = (j || 0) + i;
        }
    }
    for (x = 2; x <= n; x++) {
        window.alert([x, ': ', A[x - 1]].join(''));
    }
}

```

Один з розробників мови Ніл Фрейзер (Neil Fraser) так описує цілі створення мови [4]: "Ця концепція пройшла дуже довгий шлях, від Асемблера до Фортрана, потім до C++ та Python, і нарешті, це Blockly. Це спроба піднятися на ще більш високий рівень абстракції, щоб позбавити програмування кастовості і закритості, зробити його більш природним і доступним для якомога ширшого кола осіб". У висновку творці Blockly іронічно зауважують, що кожному розробнику важливо спочатку правильно окреслити сферу застосування цієї візуальної мови, і не "намагатися переписувати ядро Linux на цю нову і перспективну мову".

Отже, Google Blockly – це написаний на JavaScript Web-додаток, результат роботи якого – вихідний код додатка на JavaScript, Dart або Python. Такий підхід потрібен для нових сенсорних пристроїв, де введення традиційного тексту затруднене. З урахуванням найсерйозніших намірів по його розвитку зі сторони Google, ця мова має дуже цікаві перспективи на майбутнє.

Список літератури

1. Современное визуальное программирование: Google Blockly [Електронний ресурс] / Igor Савчук // Bloggerator's Litdybr Engine - 2013. – Режим доступу до журн.: <http://bloggerator.ru/page/sovremennoe-vizualnoe-programmirovanie-google-blockly-vpl>.
2. Компания Google представила новый визуальный язык программирования Blockly [Електронний ресурс] / Igor Савчук // OpenNET – 2012. Режим доступу до журн.: <http://www.opennet.ru/opennews/art.shtml?num=34087>.
3. Визуальный язык программирования Google Blockly [Електронний ресурс] / Анатолий Алізар // Хабрахабр – 2012. – Режим доступу до журн.: <http://habrahabr.ru/post/145067/>.
3. Google Blockly – A visual programming language [Електронний ресурс] // Storify – 2012. – Режим доступу до журн.: <http://storify.com/Eskills4Future/google-blockly-a-visual-programming-language>.

ЗАХИСТ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

УДК 004.056.53

В.В. ЗемлянкоНауковий керівник – Рассомахін С.Г., д-р техн. наук, професор
Харківський національний університет імені В.Н. Каразіна

Захист інформаційних мереж в Україні

Інформаційна безпека має велике значення для забезпечення життя важливих інтересів будь-якої держави. Створення розвиненого і захищеного середовища є неодмінною умовою розвитку суспільства та держави, в основі якого мають бути найновіші автоматизовані технічні засоби.

Останнім часом в Україні відбуваються якісні зміни у процесах управління на всіх рівнях, які зумовлені інтенсивним упровадженням новітніх інформаційних технологій. Швидке вдосконалення інформатизації, проникнення її в усі сфери життєво важливих інтересів зумовило, крім безперечних переваг появу низки стратегічних проблем. Посилюється небезпека несанкціонованого втручання в роботу комп'ютерних, інформаційних і телекомунікаційних систем.

На початку 2013 року в Україні хакерськими атаками були виведені з ладу сайти центральних органів влади. Для їх здійснення були залучені не лише транскордонні бот-мережі, але і рядові користувачі українського інтернету, яким організаторами атак було надано доступ до шкідливого програмного забезпечення та можливість приєднатись до атак через спеціально для цього створену веб-сторінку. Внаслідок таких атак було порушено функціонування близько 30-ти веб-сайтів державних органів і установ. Необхідно працювати над вдосконаленням системи інформаційного захисту. Розроблено Програму захисту державних інформаційних ресурсів. Цей документ дає можливість систематизувати заходи із захисту інформації та безпеки інформаційно-телекомунікаційних систем, врегулювати відносини між суб'єктами інформаційних відносин для підвищення рівня захисту електронних інформаційних ресурсів.

Впровадження в Україні електронного документообігу із застосуванням електронного цифрового підпису є одним із головних та пріоритетних завдань для розбудови сучасної системи державного управління. Така система сприятиме прозорості діяльності влади, підвищенню її ефективності і відповідає інтересам усього суспільства.

Впровадженню відповідну систему електронної взаємодії органів державної влади, головним організатором і координатором цих робіт визначено Державне агентство з питань науки, інновацій та інформатизації України.

Розроблено заходи із захисту державних інформаційних ресурсів, технічного і криптографічного захисту інформації на всіх етапах створення системи електронного документообігу.

Телекомунікаційною основою для системи електронного документообігу може стати спеціальна інформаційно-телекомунікаційна система, що розгорнута в межах Національної системи конфіденційного зв'язку. Забезпечується цілісність загальнодержавного електронного документообігу і захищеність інформаційного обміну.

У світі почалася «нова ера кібертероризму», що є наслідком глобального процесу інформатизації, та охоплює всі сфери життя. Люди дедалі більше усвідомлюють факт переміщення загроз у кіберпростір. Кібертероризм - це сукупність організованих несанкціонованих дій, спрямованих на порушення штатного режиму функціонування інформаційно-телекомунікаційних систем та порядку обробки інформаційних ресурсів. Це робиться з метою отримання несанкціонованого доступу або виведення таких систем з ладу.

Вирішення цих завдань потребує підвищення якості підготовки кадрів та відповідного законодавчого забезпечення, а також особливої уваги з боку держави для прискорення процесів створення осередків протидії кібертероризму в Україні.

Порядок надання користувачу інформації з вказаними місцем, часом, відповідальними посадовими особами, а також необхідними процедурами встановлює власник документів, масиву документів та інформаційних систем або вповноваженим ним особи відповідно до чинного законодавства, а також забезпечує умови доступу користувачів до інформації. Власник документів, масиву документів та інформаційних систем забезпечує рівень захисту інформації згідно з законодавством України.

Список літератури

1. Гайкович В, Першин О. Безпека електронних банківських систем. - М., 1999.
2. Карасик І. Програмні та апаратні засоби захисту інформації для персональних комп'ютерів // КомпьютерПресс. – № 3, – 1995
3. Петров В.А., Піскарьов С.А., Шейн А.В. Інформаційна безпека. Захист інформації від несанкціонованого доступу в автоматизованих системах. – М., 1998.

УДК 004.4

Д.В. ГладішевНауковий керівник – Смірнов О.А., канд. техн. наук, доцент
Кіровоградський національний технічний університет

Розробка програмного забезпечення захисту конфіденційної інформації у мережі методом стеганографії

Тема, обрана для дослідження, є актуальною у зв'язку з бурхливим розвитком комп'ютерних технологій і впровадження їх у повсякденне життя. Одна з основних проблем такого розвитку суспільства є проблема захисту інформації. Стеганографія вирішує такі гострі питання як: електронно-цифровий підпис, захист прав інтелектуальної власності й авторських прав, а також сховане зберігання й передача секретної (закритої) інформації з відкритих каналів передачі даних. Математичні аспекти цієї проблематики на сьогоднішній день розроблені недостатньо й дане дослідження деякою мірою заповнює цей пробіл.

Існує два принципово різних способи передачі по відкритому каналу зв'язку конфіденційної (секретної) інформації. Перший з них, відомий як шифрування, складається в заміні (по деякому алгоритму) символів переданої інформації іншими

символами, у результаті чого виходить шифртекст, що і спостерігається «супротивником» у каналі зв'язку. Наука, що вирішує відповідні проблеми забезпечення безпеки переданої таким способом конфіденційної інформації, називається криптографією.

Другий спосіб полягає в тому, щоб замаскувати передану секретну інформацію іншою, так званою, «шумовою» інформацією, що звичайно являє собою переданий по каналу зв'язку деякий відкритий текст. У цьому випадку секретні символи «вкрапляються» у відкритий текст, тобто деякі його знаки замінюються на «секретні» знаки. Такий, видозмінений відкритий текст, що несе в собі секретну інформацію, і спостерігається «супротивником». Відповідна наука про організацію й аналіз подібних процедур приховання інформації називається стеганографією.

Треба відзначити, що якщо криптографія, як математична наука, є в цей час досить просунутою, то цього не можна сказати про стеганографію. Тут на сьогодні досить добре розроблені відповідні технологічні аспекти; що ж стосується побудови й аналізу адекватних математичних моделей, то ці питання ще чекають свого кваліфікованого рішення, і сьогодні дослідження має своєю метою в певній мірі усунути наявний тут пробіл.

Криптографічний захист інформації не знімає проблему приховання конфіденційної інформації повністю, оскільки наявність шифрованого повідомлення вже саме по собі привертає увагу «супротивника», і він, заволодівши криптографічно захищеним файлом, відразу виявляє факт розміщення в ньому секретної інформації й може кинути всю сумарну міць своєї комп'ютерної бази на дешифрування схованих даних. Тому для передачі конфіденційної інформації широко використовують також і стеганографічні методи.

Термін «стеганографія» походить від двох грецьких слів – *steganos* (таємниця) і *graphy* (запис), тому її можна називати тайнописом. Хоча термін «стеганографія» з'явився тільки наприкінці XV століття, використовувати стеганографію почали кілька тисячоріч тому. Стеганографія – це наука про сховану передачу інформації шляхом збереження в таємниці самого факту передачі секретних даних. На відміну від криптографії, що приховує зміст секретного повідомлення, стеганографія приховує саму його наявність. Стеганографія не заміняє, а доповнює криптографію. Приховання повідомлення методами стеганографії значно знижує ймовірність виявлення самого факту передачі конфіденційного повідомлення, а якщо це повідомлення до того ж і зашифроване, то воно має ще один, додатковий, рівень захисту.

Стеганографія – це метод організації зв'язку. Завданням стеганографії є приховання самого факту існування секретних даних при їхній передачі, зберіганні або обробці. Інакше кажучи, під прихованням існування інформації мається на увазі не тільки неможливість виявлення в перехопленому повідомленні схованого повідомлення, але й взагалі унеможливити виникнення будь-яких підозр на цей рахунок. Загальною рисою стеганографічних методів є те, що приховуване повідомлення вбудовується в якийсь, не приваблюючий уваги, об'єкт (контейнер), що потім відкрито пересилається адресатові. На відміну від криптографії, де ворог точно може визначити, чи є повідомлення зашифрованим, методи стеганографії дозволяють вбудовувати секретні повідомлення в необразливі файли так, щоб не можна було запідозрити існування таємного послання.

На сьогоднішній день стеганографічна система, або стегосистема, може розглядатися як сукупність засобів і методів, які використовуються для формування схованого каналу передачі інформації. При побудові стеганографічної системи враховуються наступні положення. Супротивник має повне подання про стеганографічну систему. Єдиною інформацією, що невідома потенційному супротивникові, є ключ, за допомогою якого тільки його тримач може встановити факт присутності повідомлення і його зміст. Таким чином, вся таємність системи захисту

переданих повідомлень повинна втримуватися в ключі – фрагменті інформації, попередньо розділеному між адресатами.

Найбільш перспективним напрямком стеганографії на сьогоднішній день є цифрова стеганографія – напрямок комп'ютерної стеганографії, заснований на прихованні інформації в цифрових об'єктах, що споконвічно мають аналогову природу, тобто мультимедіа-об'єкти (зображення, відео, звуки). У зв'язку з розвитком апаратних засобів обчислювальної техніки й величезною кількістю каналів передачі інформації з'явилися нові стеганографічні методи, в основі яких лежать особливості подання інформації у файлах, обчислювальних мережах і т.п. Таким чином, поряд з добре вивченими математичними моделями криптографії, побудова математичних моделей стеганографії і їхній ймовірнісно-статистичний аналіз є актуальною проблематикою.

Метою роботи є побудова програмного забезпечення математичних моделей вбудовування секретної інформації при її зберіганні або передачі по відкритих каналах зв'язку й дослідження стійкості стеганосистеми залежно від кількості вбудовуваної інформації й особливостей самого процесу вбудовування.

У роботі використовуються методи математичного аналізу, теорії ймовірностей і математичної статистики, теорії цифрової обробки сигналів і зображень.

Достовірність наукових результатів підтверджена теоретичними викладеннями, даними комп'ютерного моделювання, коректними дослідженнями параметрів на функціонуючій обчислювальній мережі, а також відповідністю отриманих результатів окремим результатам, наведеним у науковій літературі.

Список літератури

1. Коначович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография.– К.: МК-пресс, 2006. – 288 с.
2. Быков С. Ф. Алгоритм сжатия JPEG с позиции компьютерной стеганографии. // Защита информации. Конфидент. – СПб.: 2000, № 3.
3. Грибунин В. Г., Оков И. Н., Туринцев И. В. Цифровая стеганография. – М.: Солон-пресс, 2002. – 272 с.
4. Schneier B (1996) Applied Cryptography. John Wiley and Sons, Indianapolis, IN
5. Dumitrescu, S., W. Xiaolin and Z. Wang, 2003. Detection of LSB steganography via sample pair analysis. In: LNCS, Vol. 2578, Springer-Verlag, New York, pp: 355–372.

УДК 621.391

Ю.М. Козекін

Науковий керівник – Семенов С.Г., канд. техн. наук, ст. наук. співроб., доцент
Національний технічний університет “Харківський політехнічний інститут”

Порівняльний аналіз методів екстраполяції для приховування даних в просторовій області нерухомих зображень методом Куттера-Джордана-Боссена

Побудова стеганографічного методу захисту інформації Куттера-Джордана-Боссена заснована на використанні методів екстраполяції (прогнозування) випадкових сигналів.

У доповіді проведено порівняльний аналіз методів екстраполяції та обґрунтовано їх подальше використання у стеганографічних алгоритмах.

Екстраполяція – це метод, при якому прогнозовані показники розраховуються як продовження динамічного ряду на майбутнє по виявленій закономірності розвитку. По суті, екстраполяція є перенесенням закономірностей і тенденцій минулого на майбутнє на основі взаємозв’язків показників одного ряду. Метод дозволяє знайти рівень ряду за його межами, у майбутньому. Екстраполяція ефективна для короткострокових прогнозів, якщо дані динамічного ряду виражені яскраво й стійко.

Куттер (М. Kutter), Джордан (F. Jordan) і Боссен (F. Bossen) запропонували алгоритм вбудовування в канал синього кольору зображення, що має RGB-кодування, оскільки до синього кольору ЗСЛ є найменш чутливою. Цей метод використовує низькорівневу властивість ЗСЛ – слабку чутливість до незначної зміни синього кольору зображення.

У роботі Куттера-Джордана-Боссена показано, що запропонований алгоритм стійкий до багатьох відомих видів атак: НЧ фільтрації зображення, його компресії відповідно до алгоритму JPEG, обрізанню країв.

Перед вилученням повідомлення повинні бути відомі:

- параметри контейнера;
- первинний ключ K_0^* ;
- кількість циклів обчислення координат (x, y) ξ^* ;
- кількість дублюючих вбудовувань одного біта τ^* ;
- розмірність (конфігурація) хреста σ — кількість пікселів зверху (знизу, зліва, справа) від оцінюваного пікселя.

Список літератури

1. Коначович Г.В., Пузыренко А.Ю. Компьютерная стеганография. Теория и практика. – К.: «МК-Пресс», 2006. – 288 с.
2. Кузнецов О.О., Кучук Г.А., Семенов С.Г. Методи обробки сигналів даних та зображень: навч. Посібник. Харків: НТУ "ХПІ", 2011. – 310 с.
3. Хорошко В.А. Чекатков А.А. Методы и средства защиты информации. — К.: Юниор, 2003. – 501с.
4. Хорошко В.А., Шелест М.Е. Введение в компьютерную стеганографию. – К.: НАУ, 2002. – 140 с.

УДК 621.3.12(043.3)

В.С. Бубенкова

Науковий керівник – Пєпа Ю.В., канд. техн. наук, доцент
Національний авіаційний університет

Способи обмеження просочування інформації по радіоканалу

Вступ. Як відомо, радіоканал є одним з технічних каналів витоку інформації, який відносять до небезпечних [1]. В наш час, коли цінність інформації стає все вищою, а власники інформації хочуть як найбільше знизити ризик її втрати, розглядати цю тему в край необхідно. В країнах Західної Європи питанням захисту електронної апаратури від перехоплення інформації за рахунок побічних електромагнітних випромінювань (ПЕМВ) [2] приділяють не менше уваги ніж в нашій країні. Тому ця проблема актуальна на сьогодні як для користувачів радіоапаратури, так і для її розробників.

Основна частина. Дуже зручним способом перехоплення інформації є перехоплення ПЕМВ. За допомогою чутливої радіоапаратури можливе приймання

радіосигналу, і після перетворення сигналу, навіть повне відтворення інформації, що оброблювалась, наприклад, комп’ютером.

Найбільш небезпечними з точки зору їх подальшого перехоплення є, так звані, потенційно інформативні випромінювання, що генеруються колами та ланцюгами живлення, по яким можуть передаватися інформативні сигнали:

- відеосигнал від відеокарти до монітору;
- сигнали від контролера клавіатури до порту вводу-виводу материнської плати;
- сигнали, що передаються до різних периферійних пристроїв.

Щоб захиститися від витоку інформації по ПЕМВ, необхідно допрацьовувати пристрої для зменшення інтенсивності випромінювання. Більш дієвий спосіб – це встановлення електромагнітного екрану для обчислювальних пристроїв чи навіть екранування приміщень, що відведені для роботи з обчислювальною технікою [3]. Але і цей спосіб має свої недоліки. Такі дії вимагають значних капітальних витрат та регулярний контроль за ефективністю екранування. Крім того, екранування вносить помітний дискомфорт в умови роботи персоналу, наприклад, відсутність мобільного зв’язку в приміщенні.

Ефективність екранування може забезпечити екран, виготовлений з одинарної мідної сітки з комірками 2,5 мм, чи з тонколистової оцинкованої сталі товщиною 0,51 мм. На рамі дверей потрібно забезпечити надійний електроконтакт по всьому периметру (це можна здійснити за рахунок нанесення шару фосфорної бронзи). Вікна потрібно затягнути одним або двома шарами мідної сітки з комірками не менше 50 мм. Обидва шари повинні мати якісний електроконтакт з стінками приміщення. Найголовніше – екран потрібно заземлити.

На сьогодні існують багатофункціональні радіомаскувальні покриття для різних видів радіоелектронної техніки, в основі яких радіопоглинаючим елементом є наноструктурні феромагнітні мікропровідники. Це тришаровий композит, що складається з металевого провідника діаметром 1-30 мк, наноструктурного перехідного шару завтовшки близько 5 нм і скляної ізоляції товщиною 2-30 мк. Завдяки різниці коефіцієнтів термічного розширення металу і скла, а також наявності наноструктурного перехідного шару, матеріал металевого провідника знаходиться під впливом гігантських механічних напруг (109 Па) і володіє унікальними електрофізичними характеристиками в НВЧ-діапазоні:

- унікальні масогабаритні характеристики: 1 км такого матеріалу важить 1 г;
- інертна скляна ізоляція, що дозволяє поєднувати наповнювач з будь-якою матрицею;

- можливість простими технологічними прийомами змінювати в широкому діапазоні електрофізичні властивості матеріалу: хімічний склад сплаву; діаметр металеві жили; товщину і хімічний склад скляної ізоляції; співвідношення діаметра металеві жили і товщини ізоляції та ін.;

- можливість отримати до 10 км матеріалу за одну технологічну операцію.

Використання такого матеріалу дозволяє: створювати різні маскувальні екрани; усувати небажаний електромагнітний фон; забезпечувати екологічну електромагнітну безпеку біологічних об’єктів; організовувати пасивний захист об’єктів та радіообладнання від несанкціонованого доступу до інформації через радіоканал.

Основні характеристики матеріалу:

- робочий діапазон довжин хвиль 0,2-15 см;
- коефіцієнт відбиття не гірше - 17 дБ;
- вага 1 м складає 2,1 кг;
- робочий діапазон температур - 60 °С +60 °С;
- екологічна чистота.

Екранування є засобом пасивного захисту від витоку по радіоканалу. У наш час існує безліч приладів, що забезпечують активний захист. Найбільш розповсюдженим способом є використання шумогенераторів, що працюють у діапазоні ПЕМВ. На ринку технічних засобів захисту можна знайти генератори радіошуму як стаціонарні, так і мобільні чи комп’ютерні, генератори для захисту від витоку через ПЕМВ, пристрої для блокування роботи радіопередавальних засобів. Головною умовою для вдалого захисту є те, що рівень шуму, що генерується генератором має бути вищим, ніж власний шум чи електромагнітний фон ПЕМВ.

Висновки. На ефективність захисту інформації від витоку суттєво впливає тип апаратури, що підлягає захисту та вид інформації, що оброблюється в них. Також слід зауважити, що необхідний постійний радіомоніторинг захищеного об’єкту. Як правило, заміна обладнання, його ремонт чи перестановка з одного місця в інше може суттєво змінити електромагнітний портрет навколо апаратури чи приміщення.

Список літератури

1. Баранов В.М. Защита информации в системах и средствах связи [учеб. пособ.] / В.М. Баранов, Г.В. Вальков, М.А. Еремеев и др. – СПб: ВИККА им. А.Ф. Можайского, 1994. – 113 с.
2. Василевский И.В. Способы и средства предотвращения утечки информации по техническим каналам / И.В. Василевский. – М.: НПЦ "Нелк", 1998. – 200 с.
3. Генне В.И. Защита информации от утечки через побочные электромагнитные излучения цифрового электромагнитного оборудования / В.И. Генне // Защита информации. – 1998. – № 2. – С.89-95.

УДК 681.2.083

Л.І. Войтишен

Науковий керівник – Крючкова Л.П., канд. техн. наук, доцент
Державний університет інформаційно-комунікаційних технологій

Закономірності хвильових процесів в ближній зоні елементарних випромінювачів електричного та магнітного полів

Ближні поля електромагнітних випромінювачів мають складну просторову структуру, досліджувати яку аналітично досить складно. У випадках, коли точно розрахувати амплітудні, фазові і поляризаційні характеристики електромагнітних полів (далі – ЕМП) неможливо, в якості первинних вимірювачів електричного поля зазвичай використовуються короткі дрові антенні, а в якості первинних вимірювачів магнітного поля – рамки. Розміри первинних вимірювачів поля мають надзвичайно важливе значення: з однієї сторони, вони повинні бути настільки малими, щоб спотворення електромагнітних полів за рахунок внесення їх в точку спостереження були в допустимо малих межах, а з іншої сторони, їх розміри повинні бути достатніми для забезпечення надійного приймання та вимірювання необхідних характеристик полів при обмеженій чутливості вимірювальних пристроїв та наявності завад. На практиці перша вимога є вирішальною, тому, як правило, довжина вібратора та діаметр рамки набагато менші за довжину хвилі, що відповідає теоретичній моделі елементарних випромінювачів – електричного (диполь Герца) і магнітного вібраторів. Аналіз фізичних закономірностей хвильових процесів в їх ближній зоні нажаль недостатньо повний, а самі критерії дальньої зони різняться у різних авторів.

Розглянемо класичне рішення задачі про випромінювання електричного диполя Герца довжиною l , збуджуваного струмом i , що змінюється за гармонічним законом $e^{i\omega t}$:

$$\dot{H}_\theta = \frac{il}{4\pi} \left(ik + \frac{1}{R} \right) \sin\theta e^{-ikR}; \quad (1)$$

$$\dot{E}_\theta = \frac{k}{\omega \epsilon_0} \frac{il}{4\pi} \left(ik + \frac{1}{R} - \frac{i}{kR^2} \right) \sin\theta e^{-ikR}; \quad (2)$$

$$\dot{E}_R = \frac{k}{\omega \epsilon_0} \frac{il}{4\pi} \left(\frac{1}{R^2} - \frac{i}{kR^3} \right) \cos\theta e^{-ikR}; \quad (3)$$

де $k = \frac{\omega}{V_\Phi} = \frac{2\pi}{\lambda}$.

Залежності компонент ЕМП від відстані, віднесеної до довжини хвилі, мають вигляд:

$$\dot{H}_\theta = \frac{il}{R^2} \sqrt{\frac{4\pi^2 R^2}{\lambda^2} + 1} \sin\theta e^{-i2\pi \frac{c}{V_\Phi} \frac{R}{\lambda}}; \quad (4)$$

$$\dot{E}_\theta = \frac{ilZ_0}{R^2} \sqrt{\frac{4\pi^2 R^2}{\lambda^2} + 1} \sin\theta e^{-i2\pi \frac{c}{V_\Phi} \frac{R}{\lambda}}; \quad (5)$$

$$\dot{E}_R = \frac{ilZ_0}{R^2} \sqrt{\frac{4\pi^2 R^2}{\lambda^2} + 1} \cos\theta e^{-i2\pi \frac{c}{V_\Phi} \frac{R}{\lambda}}; \quad (6)$$

c – швидкість світла у вакуумі, $Z_0 = 120 \pi$ – хвильовий опір вільного простору, Ом;

$$\frac{c}{V_\Phi} = 1 - \frac{1}{2\pi R} \arctg \frac{2\pi R}{\lambda}; \quad (7)$$

$$\frac{c}{V_\Phi} = 1 - \frac{1}{2\pi R} \arctg \left(\frac{2\pi R}{\lambda} - \frac{1}{2\pi R} \right); \quad (8)$$

$$\frac{c}{V_\Phi} = 1 + \frac{1}{2\pi R} \arctg \frac{1}{2\pi R}; \quad (9)$$

Розглянемо закономірності зміни амплітуд компонентів випромінювання диполя Герца, в залежності від відстані до точки спостереження.

З (4)...(6) бачимо, що можна виділити деякі нормовані множники,

$$\dot{E}_{\theta 0} = \dot{E}_{R0} = \frac{ilZ_0}{R^2}; \quad \dot{H}_{\Phi 0} = \frac{il}{R^2}, \quad (10)$$

що визначаються змінними параметрами – амплітудою струму, довжиною диполя та хвилі. Тоді нормовані до цих значень компоненти ЕМП випромінювання диполя Герца будуть описувати універсальні функціональні залежності їх від відстані, віднесеної до робочої довжини хвилі, та від кута θ :

$$\frac{|\dot{H}_\theta|}{\dot{H}_{\Phi 0}} = \sqrt{\frac{4\pi^2 R^2}{\lambda^2} + 1} \sin\theta; \quad (11)$$

$$\frac{|\dot{E}_\theta|}{\dot{E}_{\theta 0}} = \sqrt{\frac{4\pi^2 R^2}{\lambda^2} + 1} \sin\theta; \quad (12)$$

$$\frac{|\dot{E}_R|}{\dot{E}_{R0}} = \sqrt{\frac{4\pi^2 R^2}{\lambda^2} + 1} \cos\theta; \quad (13)$$

Дані залежності досить прості, тому немає необхідності виділяти в явному

вигляді складові, обернено пропорційальні першому, другому і третьому ступеню відстані, як це зазвичай робиться в класичній теорії диполя Герца.

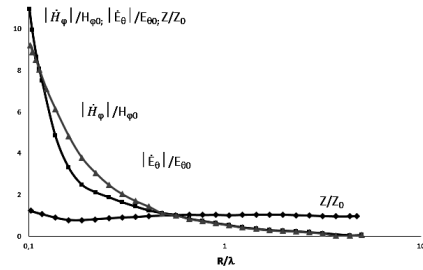


Рисунок 1 – Відносні амплітуди поперечних компонент електричного і магнітного полів у площині

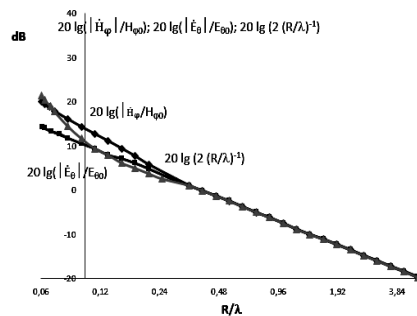


Рисунок 2 – залежність від відстані $\frac{R}{\lambda}$, яка нормована до хвильового опору вільного простору

На рис. 1 наведені відносні амплітуди поперечних компонент електричного і магнітного полів у площині, перпендикулярній диполлю, тобто при $\theta = 90^\circ$, в залежності від відстані R, віднесеної до довжини хвилі. Ці графіки відображають уніфіковані функціональні залежності відносних амплітуд компонент ЕМП у всіх зонах спостереження – ближньої, проміжної та дальньої і дозволяють аналізувати швидкість спаду амплітуд полів при збільшенні відстані до точки спостереження.

Залежність від відстані логарифмів відносних амплітуд E і H компонент ЕМП та функції $2\left(\frac{R}{\lambda}\right)^{-1}$ наведена на рис.2. Бачимо, що амплітуди двох компонент поля спадають пропорційно першій ступені відстані при $\frac{R}{\lambda} > 0,5$.

На практиці важливо визначити мінімальну відстань від диполя, починаючи з якої амплітуди полів зменшуються по закону $1/R$, характерному для дальньої зони.

Розглянемо фазові співвідношення між компонентами ЕМП на кінцевій відстані від диполя. Із теорії відомо, що в ближній зоні диполя Герца електрична і магнітна компоненти поля зрушені по фазі на мінус 90° . В дальній зоні ці компоненти синфазні. Із співвідношень (4)...(9) легко визначити відстань, на якій відбуваються відповідні зміни різниці фаз (рис.3).

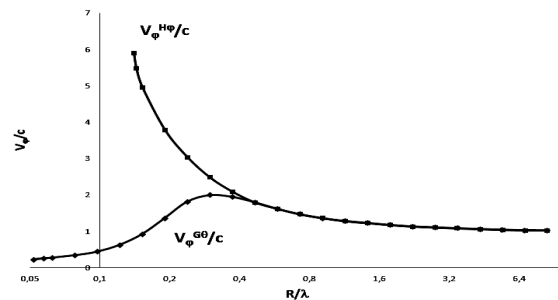


Рисунок 3 – Відносні значення фазових швидкостей компонент ЕМП в залежності від відстані в межах від 0,05 до 10 довжини хвилі

Зазначені фізичні закономірності зміни різниці фаз компонент електричного та магнітного полів в залежності від відстані до точки спостереження легко пояснюються аналізом змін фазових швидкостей цих компонент у просторі.

Із (7)...(8) видно, що фазові швидкості компонент ЕМП не залежать від довжини диполя, амплітуди збуджуючого струму та довжини робочої хвилі. Рівняння (7)...(9) задовольняють принцип електродинамічної подібності.

Розглянуті фізичні закономірності, згідно з принципом переставної двоїстості рівнянь Максвелла, справедливі і для магнітного вібратора при відповідній заміні компонент ЕМП.

Встановлені закономірності хвильових процесів в ближній зоні елементарних випромінювачів електричного та магнітного полів мають важливе значення для забезпечення технічного захисту інформації на об'єктах інформаційної діяльності.

Список літератури

1. Горобец Н.Н., Горобец Ю.Н., Цехмистро Р.И. Характеристики електромагнітних полів в ближній зоні коротких проволочних антен // Вестник Харківського національного університету. Радиофизика и електроника. –2000. – №. 467. – С.62- 66.

УДК 519.72

Д.М. Гажур

Науковий керівник – Рассомахін С.Г., д-р техн. наук, доцент
Харківський національний університет імені В.Н. Каразіна

Програмна модель генератора m-последовності

На сьогодні, для захисту інформації в зв'язку, часто використовують псевдовипадкові послідовності. Псевдовипадковий код насправді не є випадковим, це детермінований періодичний сигнал, відомий як передатчику, так і приймачу. Псевдовипадковий він тому, що має всі статичні властивості білого шуму і для стороннього користувача абсолютно випадковий.

M-последовність – це псевдовипадкова послідовність, або послідовність максимальної довжини. Формується вона за допомогою перемикальних схем на основі регістра зсуву зі зворотнім зв'язком. Схема має наступний вигляд:

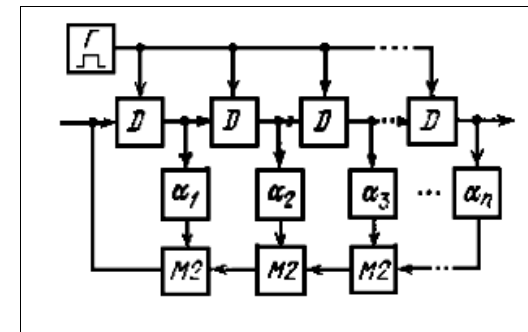


Рисунок 1 – Загальна схема регістра зсуву зі зворотнім зв'язком

До елементів схеми відносяться:

- елемент пам'яті D , який має один вхід і вихід;
- перемикач зворотного зв'язку (a_i);
- суматори по модулю 2 ($M2$).

Так як використовується система числення $p = 2$, а число розрядів регістру n , то число можливих різноманітних станів регістру дорівнює $p^n = 2^n$. Однак з усіх можливих станів регістру один заборонено, що являє собою n нулів, бо поява цієї комбінації приведе до створення нових послідовностей, що будуть теж дорівнювати нулю. Звідси число можливих станів регістру становить $L = 2^n - 1$.

Математично, регістр зсуву зі зворотнім зв'язком описуються за допомогою поліному $P(D)$ по степеням одиничної пам'яті D . При цьому для того, щоб забезпечити максимальну довжину послідовності, перш ніж закінчиться цикл регістра зсуву, цей поліном повинен бути незвідним та примітивним (бути дільником поліному $D^m + 1$ тільки при $m = 2^n - 1$ та не бути дільником при $m < L$). В якості прикладу можна привести поліном наступного вигляду:

$$P(D) = 1 \oplus D \oplus D^3, \quad (1)$$

де елемент з нульовою пам'яттю $D^0 = 1$. Коефіцієнти $\{a_i\}$, що відповідають поліному (1), дорівнюють $a_0 = 1, a_1 = 1, a_2 = 0, a_3 = 1$.



Рисунок 2 – Автокореляційна функція m-послідовності поліному 3го степеня

На основі цих знань, побудована програмна модель генератору m-послідовності, що дозволяє користувачу здійснити генерування псевдовипадкової послідовності, задавши для цього необхідні вхідні дані. Програмне забезпечення складається з трьох частин:

- введення вхідних параметрів генератора;
- відображення схеми створеного регістру та результату генерації;
- отримання автокореляційної та взаємнокореляційної функцій послідовності.

Задавши вхідні дані, а саме степінь поліному та послідовність відводів (поліном може мати декілька комбінацій, при яких його коефіцієнти $\{a_i\}$ будуть дорівнювати 1), на екран виводиться схема регістра та безпосередньо сама послідовність. Після цього, користувач має змогу дослідити результат генерації шляхом оцінки АКФ та ВКФ.

Програма здійснює роботу в двох режимах: автоматичному та ручному. В першому випадку відбувається генерація безпосередньо всієї послідовності, а в другому є можливість дослідити поведінку та стан регістру на кожній ітерації.

M-послідовності значно поступаються по автокореляційним властивостям послідовностям, що винайдені відносно нещодавно. Але завдяки своїй оптимальності, ефективності та простому алгоритму побудови, вони продовжують використовуватись в таких системах як CDMA чи GPS. Також, вони спричинили винайдення не менш відомих коду Голда і коду Касамі.

В подальшому, планується розробка програмного забезпечення моделювання каналу зв'язку, з метою демонстрації ефективності m-послідовності в умовах зашумленості за допомогою технології OFDM-QAM.

Список літератури

1. Формирование и свойства M-последовательностей: методическая разработка к лабораторной работе по дисциплине «Прием и обработка сложных сигналов» / сост. Н.П. Никитин. Екатеринбург : ГОУ ВПО УГТУ – УПИ, 2007.
2. Ширман Я. Д., Манжос В. Н. Теория и техника обработки радиолокационной информации на фоне помех. – М.: Радио и связь, 1981. – С. 138-146.

УДК 004.492.2

А.С. Годла

Научный руководитель – Губенко Н.Е., канд. техн. наук, доцент
Донецкий национальный технический университет

Усовершенствование распределенной модели использования ресурсов в условиях информационной безопасности

Информационная безопасность - защита информации и поддерживающей инфраструктуры от случайных и преднамеренных действий естественного или искусственного характера, которые наносят вред владельцам и пользователям информации. В настоящий момент существуют передовые международные практики, применяемые во многих странах, обеспечивающие достаточный режим информационной безопасности.

IT-контрмеры не совершенны, поэтому организации должны быть готовы к управлению рисками, а не только к попыткам их устранения (Alberts & Dorofee, 2002; McCumber, 2005; Peltier, 2005; Schneier, 2004; Whitman & Mattord, 2003).

Минимальным требованиям к режиму информационной безопасности соответствует базовый уровень информационной безопасности. Для создания повышенных требований для модели распределения и использования ресурсов важно придерживаться следующих этапов: определение стоимости ресурсов; подсчет вероятности угроз; выявление уязвимости ресурсов и оценка потенциального ущерба от последствий атак [1, с.17].

Сегодня на многих малых предприятиях вопрос управления рисками находится в самом низу пирамиды приоритетов. Опрос, проведенный в рамках Малого бизнес-саммита Америки в мае 2010 года показывает, что главным приоритетом в малом

бізнесе являються маркетинг і продажі. Менше всего частных предпринимателей волнует вопрос защиты от судебных исков. [2]

В условиях малого бизнеса идея политики в области развития безопасности может быть решена с помощью специальных инструментальных средств оценки и управления рисками. Использование этих программ может эффективно влиять на экономию средств, которые раньше предприниматель планировал расходовать на ликвидацию последствий атак на информационную собственность [3].

С точки зрения использования такого рода программ в сфере малого бизнеса наилучших результатов с меньшими материальными затратами можно достичь с помощью методик OCTAVE-S и CRAMM.

Методы OCTAVE основаны на практических критериях OCTAVE, которые являются стандартными подходами для оценки информационной безопасности. [5] Данная методика реализуется вручную, без использования программных средств.

В отличие от OCTAVE, CRAMM-CCTA Risk Analysis & Management реализуется с помощью специализированного программного обеспечения, которое можно настроить для различных отраслей (хозяйственной, гражданской обороны, финансовые услуги и т. д.).

Таким образом, анализ показывает, что для построения эффективной, комплексной системы информационной безопасности предполагается внести следующие изменения:

1. Определить сопротивление системы защиты распределенным атакам, то есть при формировании модели угроз нужно ориентироваться на модель распределенных атак;
2. Определить степень уязвимости объекта защиты, так как оценка рисков системы информационной безопасности каждого ценного ресурса определяется путем анализа не только угроз, но и уязвимостей, через которые может поступить угроза. Это можно осуществить путем проведения аудита информационной системы.

Немаловажно отметить, что использование ресурсов в модели распределения ресурсов может быть построено на основе E-NET модели распределения, доступа и использования ресурсов уровнями безопасности и групп (ENLG) Николая Тодорова Стоянова и Веселина Ценова Целкова. [6]

Принцип взаимодействия в модели заключается в том, что любая группа состоит из пользователей и ресурсов с максимальным уровнем доступа. Любой пользователь может взаимодействовать только с теми ресурсами, уровень которых ниже или равен уровню пользователя и одновременно принадлежат к одной группе.

Согласно этой модели, функциональными возможностями для пользователей являются:

- запрос доступа (идентификация);
- анализ прав пользователя (проверка авторизации);
- идентификация уровня безопасности;
- получения списка групп;
- выбор группы;
- получение списка ресурсов;
- выбор ресурса;
- использование ресурса;
- сохранение (log-file);
- выход из системы.

Таким образом, становится возможным уменьшение риска несанкционированного использования ресурсов компьютера в связи с проверкой доступа пользователей на корректность обращения к ресурсам.

Предлагаемые изменения направлены на улучшение распределенной модели использования ресурсов и уменьшение вероятности угрозы конфиденциальности, целостности и доступности данных, другими словами, становится возможным снижение риска несанкционированного использования ресурсов.

Список литературы

1. Петренко С. А. Управление информационными рисками. Экономически оправданная безопасность / Петренко С. А., Симонов С. В. - М.: Компания Айти; ДМК Пресс, 2004. - 384 с.
2. Townsend Stephen. Managing Risk: It's Not Just for Big Business, IS 8930 Information Security Administration, Summer 2010,7/14/2010.
3. Beachboard John. Issues in Informing Science and Information Technology Volume 5, 2008. Improving Information Security Risk Analysis Practices for Small- and Medium-Sized Enterprises: A Research Agenda. John Beachboard, Alma Cole, Mike Mellor, Steven Hernandez, Kregg Aytes, Idaho State University, Pocatello, Idaho USA; Nelson Massad, Florida Atlantic University, Florida USA.
4. Software Engineering Institute Carnegie Mellon [Электронный ресурс] // Режим доступа: <http://www.cert.org/octave/>.
5. Stoianov Nikolai Todorov , Tselkov Veselin Tsenov. E-net models for distribution, access and use of resources in security information systems [Электронный ресурс] // Режим доступа: <http://arxiv.org/abs/1011.3148>.

УДК 004.056

О.Ю. Головатюк

Науковий керівник – Мелешко Є.В., канд. техн. наук, доцент
Кіровоградський національний технічний університет

Розробка програмного забезпечення реалізації прихованих цифрових водяних знаків з використанням методів псевдоголографії

Все більшого значення в нашому світі, що швидко змінюється, набуває захист інформації. Давно існують два напрямки рішення цієї задачі: криптографія та стеганографія. Метою криптографії є приховування змісту повідомлень за допомогою їх шифрування. На відміну від цього, стеганографія приховує сам факт існування таємного повідомлення.

В даний час популярність досліджень в області стеганографії викликана двома причинами: обмеження на використання засобів криптографії в низці країн світу і поява проблеми захисту прав власності на інформацію, представлену в цифровому вигляді. Перша причина спричиняє за собою велику кількість досліджень приховання факту передачі інформації, друга – численні роботи в області цифрових водяних знаків [1].

Цифровий водяний знак (ЦВЗ) – спеціальна мітка, що непомітно вбудовується в зображення або іншу цифрову інформацію з метою контролювати її використання.

Метою даної роботи є розробка програмного забезпечення для приховування цифрових водяних знаків у зображеннях, використовуючи методи псевдоголографії.

Найважливіша властивість голографії полягає в тому, що якщо відламати шматочок голограми, то в ньому буде видно ціле зображення [2]. Застосування голографії для приховування цифрових водяних знаків у вигляді зображень надає можливість відновлення ЦВЗ меншої роздільної здатності з будь-якого шматочка їх

голограми. Також можливе відновлення контурів початкового ЦВЗ, якщо відсутня чи пошкоджена значна частина його голограми. Тобто стає можливим вилучення ЦВЗ з пошкодженого чи видозміненого зображення та встановлення його справжнього автора (чи власника).

Біт-реверсивна перестановка має вищенаведені голографічні властивості [3].

Суть методу полягає в наступному. Припустимо, є послідовність довжиною 2^L . Кожен елемент цієї послідовності має індекс від 0 до $2^L - 1$. У двійковому представленні індекс буде виглядати $(b_{L-1}b_{L-2}...b_0)_2$. Тоді реверс бітів цього індексу буде виглядати $(b_0b_1...b_{L-2}b_{L-1})_2$. Наприклад, дана послідовність символів А, В, С, D, E, F, G, H. Індексами цієї послідовності є числа: 0, 1, 2, 3, 4, 5, 6, 7; або в двійковому вигляді: 0b000, 0b001, 0b010, 0b011, 0b100, 0b101, 0b110, 0b111. Спочатку потрібно переставити біти кожного числа у зворотному порядку з урахуванням максимальної довжини двійкового числа ($L = 3$): 0b000, 0b100, 0b010, 0b110, 0b001, 0b101, 0b011, 0b111 (десяткові числа: 0, 4, 2, 6, 1, 5, 3, 7.) Потім елементи вихідної послідовності переставляються відповідно отриманим індексам: А, Е, С, G, В, F, D, H. Таким чином, вийшла перестановка послідовності в біт-реверсному порядку. Суміжні пари АЕ, СG, ВF, DH складаються з елементів, які розташовані в різних половинках вихідної послідовності. Щоб перетворити двомірне зображення, достатньо переставити біти в обох координатах кожного пікселя.

На рисунку 1а показаний цифровий водяний знак, на рисунку 1б його псевдоголограма. Квадратам кожних чотирьох пікселів відповідає один піксель кожної чверті початкового зображення в досить хаотичному порядку. Із цього можна зробити висновок, що при біт-реверсивній перестановці пікселів зображення, великі елементи зображення стають дрібними, а дрібні великими.

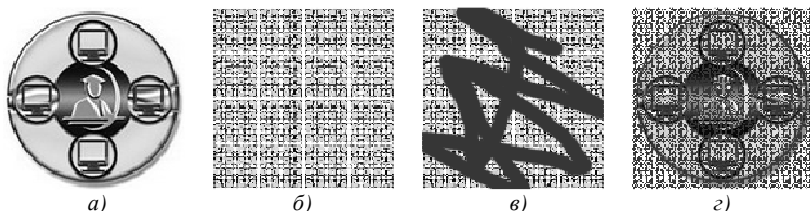


Рисунок 1 – відновлення пошкодженої псевдоголограми: а – ЦВЗ, б – його голограма, в – пошкоджена голограма, г – відновлений ЦВЗ із пошкодженої голограми

На рисунку 1 (в) показана голограма ЦВЗ з нанесеним низькочастотним шумом. Після відновлення початкового зображення, низькочастотний шум перетворився на високочастотний, однаково розподілений по всьому зображенню, але не зіпсував його пізнаваність.

Важливо, що біт-реверсивна перестановка може бути застосована тільки для послідовностей довжиною рівною степені двійки (4, 8, 16 і так далі). Також, при відновленні частини зображення воно повинно мати роздільну здатність рівну степені двійки і починатися з кратної їй позиції.

Псевдоголограму цифрового водяного знаку можна приховати в контейнер за допомогою одного з методів стеганографії – LSB методу (Least Significant Bit, найменший значущий біт).

Суть цього методу полягає в заміні останніх значущих бітів у контейнері на біти прихованого повідомлення. Різниця між порожнім і заповненим контейнерами повинна бути не відчутна для органів сприйняття людини [1].

В розробленій програмі реалізовано отримання псевдоголограми графічного ЦВЗ за допомогою біт-реверсивної перестановки пікселів та її приховування у зображенні з глибиною кольору 24 біти на піксель за допомогою методу LSB.

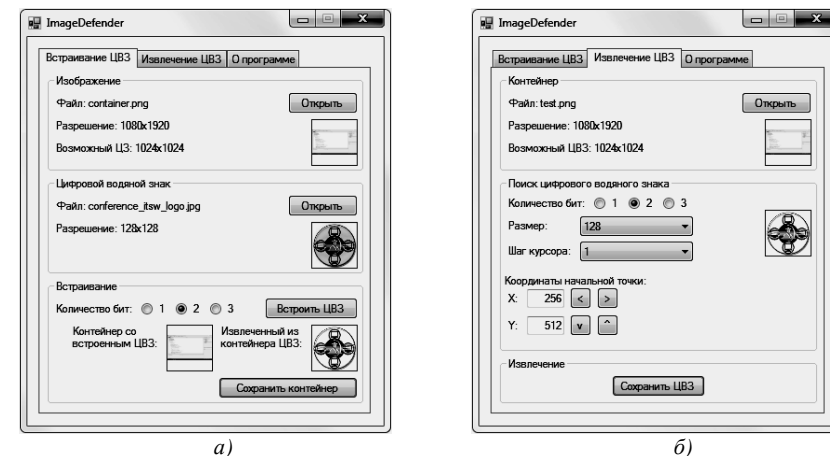


Рисунок 2 – інтерфейс програми: а – вбудовування ЦВЗ, б – вилучення ЦВЗ

Програма має інтуїтивно зрозумілий інтерфейс, показаний на рисунку 2, та проста у користуванні. Щоб сховати у зображенні цифровий водяний знак, потрібно відкрити контейнер, ЦВЗ та обрати кількість молодших біт (від 1 до 3), куди він буде прихований. Якщо роздільна здатність ЦВЗ не рівна степені двійки, виводиться пропозиція привести її до 2^N або використати його центральну частину. При натисненні на зменшені зображення, відкривається вікно для перегляду їх в оригінальному розмірі з можливістю зміни масштабу. При вбудовуванні ЦВЗ, він заміщується по всій площі зображення. Для вилучення цифрового водяного знаку потрібно відкрити зображення, обрати кількість задіяних молодших біт, вказати його розмір та початкові точки.

Основними результатами, отриманими у ході виконання даної науково-практичної роботи є:

- Досліджені та обґрунтовані переваги використання методів псевдоголографії в алгоритмах вбудовування прихованих цифрових водяних знаків.
- Реалізовано алгоритм, що створює псевдоголограму цифрового зображення за допомогою біт-реверсивної перестановки пікселів зображення.
- Реалізовано алгоритм вбудовування прихованого цифрового знаку у графічні файли LSB методом.
- Розроблено програмне забезпечення на мові програмування С#, що здійснює вбудовування у графічні файли прихованих цифрових водяних знаків з використанням методів псевдоголографії.

Список літератури

1. Грибунин В.Г. Цифровая стеганография / Грибунин В.Г., Оков И.Н., Туринцев И.В. – М.: Солон-Пресс, 2009 – 272 с.
2. Голография – Википедия [Електронний ресурс] // Режим доступу: <http://ru.wikipedia.org/wiki/Голография>.
3. Голографические свойства бит-реверсивной перестановки [Електронний ресурс] / Сергей Шишинцев // Режим доступу: <http://habrahabr.ru/post/155471>.

УДК 340.5:65.012.8

Ю.В. Гончарова

Науковий керівник – Певнев В.Я., канд. техн. наук, доцент
Харківський національний університет імені В.Н. Каразіна

Про колізії у визначеннях, наданих у Законах України щодо інформаційно-комунікаційних мереж та безпеки інформації

Постановка проблеми. Українську правову базу досі навряд чи можна назвати досконалою: існує чимало прикладів двоякого трактування букви Закону, саме тому актуальним залишається поняття колізії. У підручнику з теорії держави та права надається таке визначення: «Юридична колізія - це обумовлений системою об’єктивних та суб’єктивних причин різновид протиріч у сфері права, сутність якого виявляється у наявності розбіжностей між приписами нормативно-правових актів чи нормативних та інтерпретаційних актів, що спрямовані на регулювання однотипних суспільних відносин чи роз’яснення правових норм.» [1, С.228], тобто відсутність можливості однозначного трактування та застосування. Авторами розглянуто питання існування колізій визначень, наданих у Законах України (ЗУ) стосовно інформаційної безпеки та загалом інформаційно-комунікаційних мереж.

Мета роботи: визначити колізії у визначеннях, наданих Законодавцем у ЗУ Верховної Ради України I-VII скликань, проаналізувати розбіжності, запропонувати можливі методи розв’язання проблеми виникнення колізій визначень.

Основний матеріал дослідження. Закон України надає перелік визначень, які застосовуються в межах вищезазначеного нормативно-правового акту. Але ці визначення є актуальним не тільки в межах цього документу, а й інших, які посилаються на нього чи роботах, які прямо або побічно мають відношення до Закону. Авторами розглянуто 35 ЗУ, у них знайдено 466 визначень, з яких 18 визначень є юридичною колізією. Декілька знайдених юридичних колізій надано у табл. 1.

Таблиця 1 – Деякі юридичні колізії у визначеннях, наданих у ЗУ

Поняття	Визначення
Інформація	- будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді (ч. 1 ст. 1 ЗУ «Про інформацію»; ч. 1 ст. 200 ЦК). - відомості, подані у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб (ст. 1 ЗУ «Про телекомунікації»); - відомості в будь-якій формі та вигляді, на будь-яких носіях (у тому числі листування, книги, помітки, ілюстрації (карти, діаграми, органіграми, малюнки, схеми тощо), фотографії, голограми, кіно-, відеофільми, мікрофільми, звукові записи, бази даних комп’ютерних систем або повне чи часткове відтворення їх елементів), пояснення осіб та будь-які інші публічно оголошені чи документовані відомості (ст. 1 ЗУ «Про обмеження монополізму та недопущення недобросовісної конкуренції у підприємницькій діяльності»; ст. 1 ЗУ «Про захист економічної конкуренції»).

Продовження таблиці 1

Конфіденційна інформація	Конфіденційна інформація – інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб’єктів владних повноважень (ч. 2 ст. 21 ЗУ «Про інформацію»); Конфіденційна інформація – інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб’єктів владних повноважень, та яка може поширюватися у визначеному ними порядку за їхнім бажанням відповідно до передбачених ними умов (ч.1 ст. 7 ЗУ «Про доступ до публічної інформації»).
--------------------------	--

Нажаль, існуючі Закони України не відобразили певною мірою поняття інформаційної безпеки: авторами знайдено лише одне визначення, надане у ЗУ «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки»: «Інформаційна безпека - стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації». Традиційно вважається, що поняття інформаційної безпеки є аналогом англomовного терміну “information security”, який за не обачністю перекладачів отримав значення «інформаційна безпека», хоча доцільніше було б перекласти це як «безпека інформації», що є дещо іншим поняттям. Тож авторами запропоновано вважати термін викладеним невірно, спираючись на [9, С.62], запропоновано ввести наступне визначення: «Інформаційна безпека – властивість системи протягом заданого відрізка часу протистояти несанкціонованому зняттю та модифікації інформації. До речі, в ЗУ «Про захист інформації в інформаційно-комунікаційних системах» немає навіть визначення інформаційної безпеки, не зважаючи на те, що це є необхідною (та іноді достатньою) умовою забезпечення захисту інформації.

Висновки. Нині авторами опрацьовано Закони України, прийняті Верховною Радою I-VII скликань, проте це тільки перші кроки у розгляданні недосконалості української нормативно-правової бази у питаннях інформації, систем інформації та інформаційної безпеки.

Список літератури

1. Зайчук О. В., Оніщенко Н. М.. Теорія держави і права. Академічний курс. – Підручник. Київ: Юрінком Інтер, 2006р.
2. ЗУ «Про державну таємницю» (Відомості Верховної Ради України (ВВР), 1994, N 16, ст.93);
3. ЗУ «Про доступ до публічної інформації» (Відомості Верховної Ради України (ВВР), 2011, № 32, ст. 314);
4. ЗУ «Про захист економічної конкуренції» (Відомості Верховної Ради України (ВВР), 2001, N 12, ст.64);
5. ЗУ «Про захист інформації в інформаційно-телекомунікаційних системах» (Відомості Верховної Ради України (ВВР), 1994, N 31, ст.286);
6. ЗУ «Про інформацію» (Відомості Верховної Ради України (ВВР), 1992, N 48, ст.650);
7. ЗУ «Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» (Відомості Верховної Ради України (ВВР), 2007, № 12, ст.102);
8. ЗУ «Про телекомунікації» (Відомості Верховної Ради України (ВВР), 2004, N 12, ст.155).
9. Певнев В.Я., Цуранов М.В. Математическая модель информационной безопасности. – Системи обробки інформації, випуск 3(84). 2010. – С. 62-64

О.І. ДеркачНауковий керівник – Крючкова Л.П., канд. техн. наук, доцент
Державний університет інформаційно-комунікаційних технологій

Фізична природа прямих акустоелектричних перетворювань

Під акустоелектричним перетворенням розуміють перетворення механічної енергії акустичного сигналу окремими пристроями в електричний сигнал, модульований за законом зміни акустичного сигналу. У свою чергу, електричні сигнали створюють електромагнітні поля, які можуть утворювати канали витоку інформації. Наведені електричні сигнали, незважаючи на свій низький рівень, можуть поширюватися по дротяних лініях за межі контрольованої зони та перехоплюватися засобами технічної розвідки.

Фізичною основою акустоелектричних перетворювань, в першу чергу, є зворотний ефект Фарадея, який полягає в тому, що при переміщенні провідника поперек силових ліній магнітного поля на його кінцях наводиться електрорушійна сила (у замкненому провіднику - тече струм). Зовнішнє магнітне поле існує завжди, отже, переміщення будь-якого провідника (вібрація, тремтіння), особливо обмотки з великою кількістю витків, неминуче викликає появу напруги або струму, відповідних акустичному (вібраційному) впливу. Тому всі моточні виробни (трансформатори, реле, котушки індуктивності, дроселі і т.д., які функціонують в складі вторинних технічних засобів, є джерелами акустоелектричних перетворювань. Крім того, під впливом акустичних сигналів виникає вібрація сердечників компонентів (це більш характерно для матеріалів з високим μ), що призводить (за рахунок хвиль стиску в матеріалі) до зміни їх магнітної проникності (зворотний магнітострикційний ефект, або ефект Велларі), і викликає появу сигналу в обмотці.

Другою причиною акустоелектричних перетворювань є різноманітні ємнісні ефекти. Якщо в конденсаторі, утвореному провідними елементами, одна обкладка рухається відносно іншої - змінюється ємність цього конденсатора, отже, змінюється напруга на його обкладках.

Третьою причиною акустоелектричних перетворювань, що досить часто зустрічається, є п'єзоефект. Значна кількість керамічних конденсаторів виконується з матеріалів типу ЦТС (цирконій-титанат свинцю). Такі матеріали завжди мають п'єзострикційний ефект, тобто, при докладанні до них механічного зусилля (вигин, зсув, стиснення і т.д.) на обкладках конденсатора генеруються електричні потенціали, пропорційні докладеним зусиллям (принцип дії п'єзоелектричного мікрофону).

Є ще ряд більш «тонких» ефектів, які спричиняють прямі акустоелектричні перетворення. Отже, в якості перетворювачів механічної енергії акустичного сигналу в електричні можуть виступати елементи технічних засобів, що мають різну природу і досить широкий спектр фізичних властивостей. І тільки вимірами можна довести, що в кожному конкретному випадку і при строго певних режимах роботи технічних засобів сигнал акустоелектричного перетворення не перевищує нормативних значень.

Список літератури

1. Г. А. Бузов, С. В. Калинин, А. В. Кондратьев, Защита от утечки информации по техническим каналам, учебное пособие – М.: «Горячая линия-Телеком» 2005 г., С.274-275.

Є.О. ДзюбенкоНауковий керівник – Мелешко Є.В., канд. техн. наук, доцент
Кіровоградський національний технічний університет

Розробка програмного забезпечення для статистичного стегааналізу графічних файлів

Метою даної роботи є розробка програмного забезпечення для статистичного стегааналізу графічних файлів.

Задача стегааналізу полягає в виявленні факту передачі прихованої інформації в аналізованому повідомленні. В деяких випадках під стегааналізом розуміють також вилучення прихованої інформації з повідомлення, яке містить її, і (якщо це можливо) подальшу дешифровку вилученої інформації.

Існують наступні методи стегааналізу графічних файлів:

- методи, призначені для виявлення даних, прихованих певним алгоритмом;
- методи «сліпого» розпізнавання;
- методи пасивного стегааналізу, які визначають наявність/відсутність прихованих даних в стегакодексі, або методи, що визначають алгоритм, за яким відбувалося вбудовування;
- методи активного стегааналізу, які визначають довжину вбудованого документа, його розташування, деякі параметри алгоритму вбудовування, а також вилучають приховану інформацію;
- сигнатурні методи, засновані на пошуку в стегаграмах так званих «відбитків пальців», - фрагментів коду, які залишають після своєї роботи стегаграфічні програми;
- ймовірнісні методи, які засновані на аналізі ймовірнісних показників, характерних для стегаповідомлень;
- методи, які аналізують зображення безпосередньо, тобто в просторовій формі представлення;
- методи, які аналізують частотні форми представлення зображення, тобто після переведення його до частотної форми за допомогою дискретного косинус-перетворення, або вейвлет-перетворення;
- методи, які використовують статистичні критерії згоди (напр., Хі-квадрат);
- методи, які використовують міру подібності цифрової сукупності;
- метод визначення JPEG-сумісності.

Розроблена програма використовує ймовірнісні методи стегааналізу. Програма зчитує значення бітів пікселів розглядаємого зображення та з отриманих даних будує графіки окремо для кожного кольору RGB формату.

Зображення з заповненим контейнером матиме графіки з горизонтальними відріzkами, інколи у вигляді східців.

На рисунках 1-2 наведені приклади стегааналізу пустого та заповненого контейнера, як видно з рисунків, у випадку заповненого контейнера на графіку з'являються горизонтальні відріzkи.

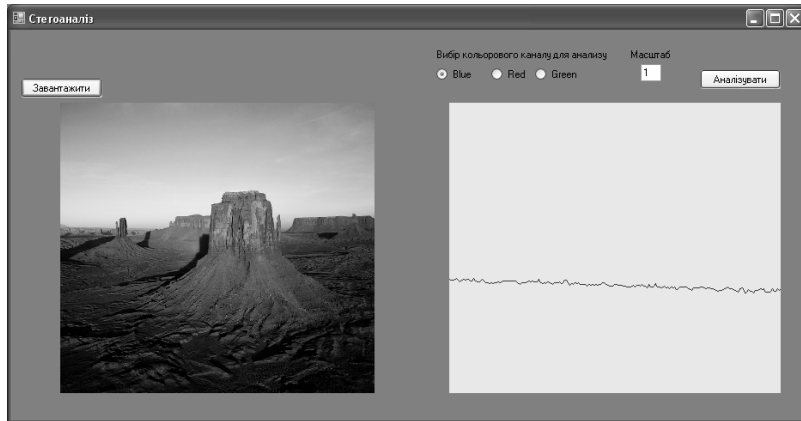


Рисунок 1 – Результати стегааналізу порожнього контейнера

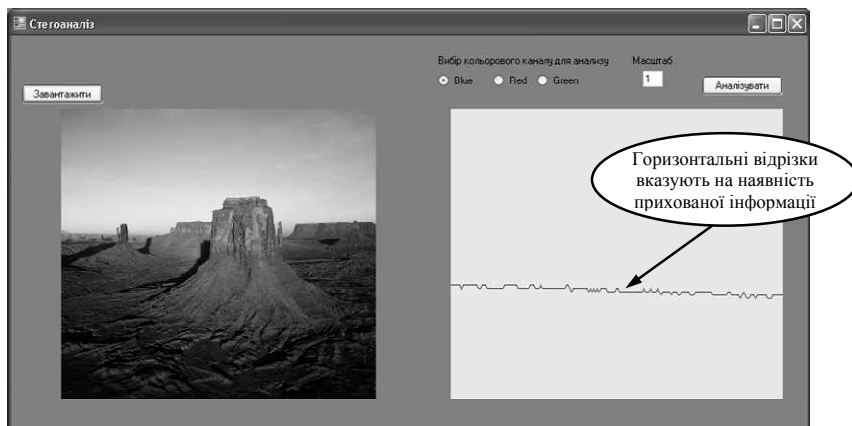


Рисунок 2 – Результати стегааналізу заповненого контейнера

Основні результати, отримані у ході виконання даної науково-практичної роботи:

- Проведено дослідження існуючих методів стегааналізу графічних файлів.
- Розроблено програму на мові програмування C#, що здійснює статистичний стегааналіз графічних файлів.

Список літератури

1. Коначович Г.Ф., Пузыренко А.Ю. "Компьютерная стеганография. Теория и практика".
2. Грибунин В. Г., Оков И.Н., Туринцев И.В. "Цифровая стеганография".

УДК 004.056.55

М.В. Єсіна

Науковий керівник – Горбенко І.Д., д-р техн. наук, професор
Харківський національний університет імені В.Н. Каразіна

Алгоритм Кессак – новий стандарт гешування даних

На початку 21 століття з’явилися підозри відносно стійкості алгоритму гешування SHA-1. Тому NIST США у листопаді 2007 року оголосив конкурс на проектування нового алгоритму гешування. Протягом наступного року від спеціалістів з багатьох країн було надіслано 56 кандидатів на роль перспективного стандарту. У 2009 році з алгоритмів-кандидатів конкурсу було обрано 14 алгоритмів, які брали участь у другому етапі проекту SHA-3. Потім кількість кандидатів була зменшена до п’яти (BLAKE, Grostl, JH, Kesscak, Skein), які стали фіналістами конкурсу SHA-3 [4].

При виборі фіналістів було відмічено, що жоден з 14-ти алгоритмів не був слабким з точки зору стійкості. Їх доводилось обирати за іншими критеріями (продуктивність, паралелізм і т.д.). Деякі алгоритми були відкинута через «надмірно високу» продуктивність. У результаті досліджень, NIST прийняв рішення, що в якості SHA-3 буде використовуватись алгоритм Кессак.

За словами спеціалістів NIST, алгоритм Кессак було обрано через простий та елегантний дизайн і дещо кращу, ніж у інших конкурентів, продуктивність та легкість реалізації на різних типах пристроїв. Алгоритм принципово відрізняється від SHA-2, а тому буде стійкий відносно атак, які реалізуються на SHA-2.

Автори алгоритму Кессак – Guido Bertoni, Joan Daemen, Michael Peeters і Gilles Van Assche.

Алгоритм Кессак належить до сімейства «sponge» функцій [3] які використовують побудову блоку перестановок, складається з 7-ох наборів перестановок. Його побудовано за принципом криптографічної губки.

Основною функцією стиснення алгоритму є функція $f()$, яка виконує перемішування внутрішнього стану алгоритму. Стан (позначимо його A) подається у вигляді двовимірного масиву 5×5 , елементами якого є 64-бітні слова, що ініціалізовані нульовими бітами (тобто розмір стану складає 1600 бітів). Функція $f()$ виконує 18 раундів, в кожному з яких виконуються наступні дії:

$$C[x] = A[x, 0] \oplus A[x, 1] \oplus A[x, 2] \oplus A[x, 3] \oplus A[x, 4], x = 0..4 \quad (1)$$

$$D[x] = C[x-1] \oplus (C[x+1] \ggg 1), x = 0..4; \quad (2)$$

$$A[x, y] = A[x, y] \oplus D[x], x = 0..4, y = 0..4; \quad (3)$$

$$B[y, 2x+3y] = A[x, y] \ggg r[x, y], x = 0..4, y = 0..4; \quad (4)$$

$$A[x, y] = B[x, y] \oplus (\sim B[x+1, y] \& B[x+2, y]), x = 0..4, y = 0..4, \quad (5)$$

де:

B – тимчасовий масив, аналогічний за структурою масиву стану;

C і D – тимчасові масиви, які містять по п’ять 64-бітних слів;

r – масив, який визначає кількість бітів обертання для кожного слова стану;

$\sim x$ – побітовий комплемент до x ;

операції з індексами масиву виконуються за модулем 5 [4].

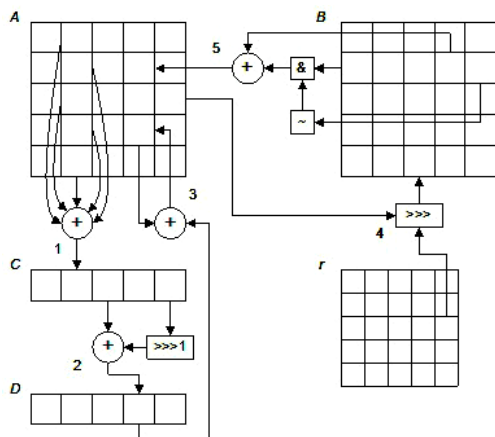


Рисунок 1 – Раунд алгоритму Кессак

Окрім наведених вище операцій, у кожному раунді також виконується накладання операцією XOR раундової константи на слово $A[0,0]$.

Перед виконанням функції стиснення на частину стану операцією XOR накладається блок даних, що гешуються. Це накладання в сукупності з функцією стиснення, що виконуються для кожного блоку вхідних даних, являють собою «поглинаючу» фазу криптографічної губки.

Варто зазначити, що функція $f()$ використовує лише операції, стійкі до атак, які використовують витoki даних побічними каналами.

Результуюче геш-значення обчислюється у процесі виконання «стискаючої» фази криптографічної губки, основу якої також складає описана вище функція $f()$. Можливі розміри геш-значень – 224, 256, 384 і 512 біт.

Алгоритм Кессак не допускає утворення двох ідентичних геш-значень, які можуть за основою відрізнятися один від одного фрагментами даних.

Оригінальний алгоритм Кессак має безліч параметрів, які можна налаштувати з метою забезпечення оптимального співвідношення криптостійкості та швидкодії для визначеного застосування алгоритму на визначеній платформі. Величини, що налаштовуються: розмір блока даних, розмір стану алгоритму, кількість раундів у функції $f()$ та інші.

Автори Кессак заснували ряд призив за досягнення в криптоаналізі даного алгоритму. У 2009 році з’явилося декілька робіт, присвячених криптоаналізу алгоритму Кессак (наприклад, [1-2]), проте, їх автори не виявили жодних уразливостей у даному алгоритмі. Таким чином, алгоритм Кессак вигідно відрізняється від інших кандидатів і має перспективи.

Список літератури

1. Aumasson J.-P., Khovratovich D. First Analysis of Keccak. [Електронний ресурс] // Режим доступу: <http://131002.net>.
2. Aumasson J.-P., Meier W. Zero-sum distinguishers for reduced Keccak-f and for the core functions of Luffa and Hamsi. [Електронний ресурс] // Режим доступу: <http://131002.net> – FHNW, Windisch, Switzerland.
3. Cryptographic sponge functions, January 2011 [Електронний ресурс] // Режим доступу: <http://sponge.noekeon.org/>.
4. [Електронний ресурс] // Режим доступу: <http://daily.sec.ru/publication.cfm?pid=30852>.

УДК 004.4

А.В. Зазимко

Науковий керівник – Мелешко Є.В., канд. техн. наук, доцент
Кіровоградський національний технічний університет

Розробка програмного забезпечення статистичного аналізу та фільтрації даних зі змінних носіїв

В останні роки в Україні намітився перехід від традиційної форми подання документів до їхнього електронного подання. Перехід до електронного документообігу з використанням змінних носіїв несе цілий ряд переваг, серед яких: істотне скорочення строків розробки й проходження документів у структурі підприємства, спрощення формування й пересилання пакетів документів між підприємствами, що, у свою чергу, припускає відчутну економічну вигоду. Не дуже давно були прийняті державний стандарт електронного цифрового підпису (ЕЦП) ДСТУ 4145-2002 і Закон «Про електронний цифровий підпис», що є вірним свідченням серйозних кроків у даному напрямку. Із прийняттям закону «Про електронний документ» електронні документи знайдуть свою юридичну чинність і зможуть замінити традиційні документи.

Крім правової бази, серйозним стримуючим фактором на шляху переходу до електронних документів (ЕД) є нерозв’язаність ряду серйозних питань, пов’язаних із забезпеченням збереження конфіденційності інформації в системах електронного документообігу з використанням змінних носіїв. Зокрема, перехід до ЕД припускає їхню передачу в електронному виді по різних каналах зв’язку, у тому числі з використанням змінних носіїв. З огляду на сучасний стан, а також перспективи розвитку систем зв’язку й телекомунікації, очевидним є широке використання для цих цілей відкритих каналів зв’язку й глобальних мереж. Збереження конфіденційності інформації при її передачі по відкритих каналах зв’язку може бути забезпечене методами як криптографічного, так і стеганографічного методу збереження конфіденційності інформації. При цьому варто помітити, що жоден із зазначених напрямків на поточному рівні розвитку не в змозі самостійно вирішити всі завдання, пов’язані із збереженням конфіденційності інформації в електронному документообігу. Крім того, рішення ряду специфічних завдань можливо тільки при спільному погодженому застосуванні методів криптографії й стеганографії.

Таким чином, актуальною проблемою є забезпечення збереження конфіденційності інформації в системах електронного документообігу з використанням змінних носіїв шляхом погодженого застосування методів криптографії й стеганографії.

Теоретичний аспект сформульованої проблеми складається у визначенні й обґрунтуванні можливих шляхів забезпечення збереження конфіденційності інформації при передачі електронних документів з використанням змінних носіїв та відкритих каналів зв’язку; пошуку механізмів забезпечення скритності найбільш значимої для підприємства частини документообігу від потенційних конкурентів; визначенні шляхів і способів протидії небезпечним для ІБ підприємства діям інсайдерів.

Практичний аспект проблеми полягає: у розробці механізмів забезпечення скритності електронного документообігу з використанням змінних носіїв від засобів конкурентної розвідки; розробці методів, алгоритмів і моделей програмних засобів, що дозволяють забезпечити безпеку електронних документів при їхній передачі з використанням змінних носіїв та по відкритих каналах зв’язку; розробці методів,

алгоритмів і моделей програмних засобів схованого маркування електронних документів при інформаційному обміні.

Об'єктом дослідження є процес виявлення несанкціонованого витоку конфіденційної інформації. Предметом дослідження – статистичний аналіз та фільтрація даних зі змінних носіїв.

Ціль роботи – підвищення ефективності методу збереження конфіденційності інформації в багатокористувальницьких розподілених системах електронного документообігу з використанням змінних носіїв на базі сучасних технологій схованого зв'язку.

Завдання дослідження: 1) Аналіз уразливостей і розробка класифікації стеганографічних атак на системи схованої передачі електронних документів з використанням змінних носіїв. 2) Оцінка ефективності сучасних стеганографічних методів і визначення границь їхньої застосовності, розробка методу й визначення критеріїв оцінки практичної стійкості стеганографічних методів збереження конфіденційності інформації. 3) Дослідження можливості побудови теоретично стійких стеганографічних методів і систем. 4) Розробка моделей, принципів і проектних рішень на базі методів криптографії й стеганографії для створення перспективних засобів збереження конфіденційності змісту електронних документів, що володіють високою теоретичною й практичною стійкістю, обґрунтування ефективності запропонованих рішень. 5) Розробка нових стеганографічних методів, орієнтованих на використання в розроблювальних системах методу збереження конфіденційності інформації, які б відповідали необхідним вимогам й мали високий рівень стійкості. 6) Розробка методів, алгоритмів, моделі й архітектури системи схованого маркування й перевірки маркування електронних документів у системах електронного документообігу з використанням змінних носіїв й баз даних.

Для рішення завдань використані методи теорії інформації й зв'язку, теорії ймовірностей і математичної статистики, методи обчислювальної математики, теорії ухвалення рішення, теорії інформаційної безпеки й розподілених систем.

Список літератури

1. Коначович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография. Теор. и практ.–К.:«МК-Пресс», 2006.–288 с.
2. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография. – М.: Солон-Пресс, 2002. – 272 с.
3. Хорошко В.А., Шелест М.Е. Введение в компьютерную стеганографию. – К., 2002. – 140 с.
4. Корольов В.Ю. Планивання досліджень методів стеганографії та стегоаналізу / В.Ю. Корольов, В.В. Поліновський, В.А. Герасименко, М.Л. Горінштейн // Вісник Хмельницького нац. ун-ту №4, 2011. – 187-196 с.
5. Корольов В. Ю. RS-стегоаналіз. Принципи роботи, недоліки та концепція метода його обходу / В. Ю. Корольов, В. В. Поліновський, В. А. Герасименко // Вісник Вінницького політехн. Ін-ту.–2010.–№6.–С.66-71.
6. Куц А.В. Использование алгоритмов стеганографии при проведении компьютерно-технической экспертизы / А.В. Куц // VI Вероссс. межвуз, конф. молодых ученых – СПб: СПбГУ ИТМО, 2009.

УДК 004.056:621.3(043.3)

Н.В. Захарчук

Науковий керівник – Пєпа Ю.В., канд. техн. наук, доцент
Національний авіаційний університет

Ідентифікація радіовипромінювань

Вступ. На сьогоднішній день невід'ємною частиною будь-якого підприємства чи банку є масове використання електронної апаратури, тому виникає проблема захисту інформації від зовнішнього впливу, адже будь-який пристрій при роботі створює електромагнітне поле випромінювання. В результаті створюються канали технічного витоку інформації [1], одним із самих небезпечних є радіоканал витоку

інформації, який широко застосовується шахрайськими або конкурентними фірмами чи організаціями для отримання конфіденційної та секретної інформації.

Основна частина. Знімання інформації з радіоканалу витоку інформації здійснюється, як правило, з використанням усіх досягнень сучасної мікроелектроніки [2]: радіозакладних пристроїв, приймачів, передавачів. Джерелами небезпечного сигналу є елементи, вузли і провідники технічних засобів забезпечення виробничої та трудової діяльності, а також радіо- і електронна апаратура. Крім того, кожне джерело небезпечного сигналу при деяких умовах може створити технічний канал витоку інформації і кожна електронна система, яка містить в собі сукупність елементів, вузлів і провідників, володіє деякою множиною технічних каналів витоку інформації.

Основними джерелами радіоканалу каналу витоку інформації є: перетворювачі фізичних величин; випромінювачі електромагнітних коливань; паразитні зв'язки й наведення на провідники й елементи.

Радіоканали витоку інформації утворюються за рахунок: мікрофонного ефекту; магнітного поля паразитної генерації; взаємного впливу; височастотного нав'язування по ланцюгах живлення і заземлення потужних радіотехнічних засобів; електромагнітного випромінювання; з волоконнооптичних систем зв'язку.

Для виявлення випромінюючих в ефір радіосигналів необхідно визначити можливий діапазон їх роботи, використані види модуляції і методи закриття. Це можливо за рахунок спектроаналізаторів з пам'яттю та приймачів скануючого типу.

Одним із новітніх видів радіозакладних пристроїв є радіозакладка заснована на застосуванні GSM технології. З повсякденним покращенням і здешевленням тарифів стільникового зв'язку виникла можливість використовувати мобільний телефон в якості радіозакладки. Побудова пристрою закладки та її реалізація дуже проста і є досить популярна. До роз'єму гарнітури стільникового телефону пристиковується виносний мікрофон, встановлюється режим автопідняття трубки мобільного телефону, встановлюється режим дисплея, клавіатура та ін.) і все це приховано встановлюється в контрольоване приміщення. В результаті ми маємо пристрій, який можемо активувати в будь-який момент з будь-якого телефону, в будь-якій точці Землі, і прослухати аудіо інформацію з контрольованого приміщення, так як радіосигнал телефону надійно «приховується» роботою великої кількості мобільних телефонів даного стандарту, а це істотно ускладнює завдання пошуку радіозакладних пристроїв за їх випромінюванням.

При використанні зловмисником радіозакладних пристроїв, виявлення їх можливе за фактом випромінювання (передачі перехопленої інформації). Це і визначає вимоги до діапазону роботи приймального пристрою, використовуваного для пошуку радіозакладних пристроїв.

При визначенні випромінювань радіозакладних пристроїв можна використовувати такі особливості їх радіовипромінювань, як:

- наявність досить потужних гармонік, що ресструються контролюючими приймачами (в сучасних радіозакладках послаблення радіовипромінювань гармонік не більше 50 дБ);

- випромінювання радіозакладок, як правило, проявляються у вільній, не зайнятій ділянці частотного діапазону;

- сигнал радіозакладки виділяється при зміні просторового положення приймальної (зондуючої) антени щодо інших сигналів (поляризація) [3];

- спектр випромінювання радіозакладки, працюючої без кодування, розширюється відповідно із збільшенням рівня звуку;

- якщо закладка працює без маскування сигналу, то в перехопленому сигналі прослуховується шум приміщення (або тестового сигналу);

- час роботи (випромінювання) радіозакладок збігається з часом інтенсивної роботи (обговорення) конфіденційних питань.

В якості приймальних пристроїв пошуку радіозакладок можуть бути використані: широкопasmові приймальні пристрої, супергетеродинні приймальні пристрої, програмно-апаратні комплекси [2].

Для визначення місця розташування радіозакладних пристроїв використовуються радіопеленгаторні пристрої [4] або спеціальні пристрої, що дозволяють визначити місце розташування закладки за величиною зсуву сигналу між тим, що випромінюється акустичним випромінювачем і прийнятим з ефіру радіосигналом від закладки.

Висновки. Для перекриття радіоканалу витоку інформації, який реалізується за допомогою GSM-закладки існує безліч програмних модулів та пристроїв. Прикладом може слугувати використання зашумлювачів GSM діапазону, індикаторів поля – для виявлення випромінювання, селективного частотоміру SEL SP-71/M. Також ефективним будуть портативний блокувач мобільних телефонів, а також більш сучасний метод – це використання комплексу постійного радіомоніторингу «Кассандра-М», який дозволяє на найвищому рівні виявити небезпечні прояви радіосигналів за допомогою цифрового аналізу спектрів сигналу. Наявність застосування комплексу «Кассандра-М» дозволяє виявити в ефірі найменший сплеск і проаналізувати його поведінку в конкретний момент часу, також він фіксує навіть дуже короткі моменти виходу в ефір.

Список літератури

1. Лунегов А.И. Технические средства и способы добытия и защиты информации / А.И. Лунегов, А.Л. Рыжов. – М.: ВНИИ «Стандарт», 1993. – 95 с.
2. Хорошко В.А. Методы и средства защиты информации/В.А.Хорошко, А.А.Чекатков.–К.:«Юниор»,2003.–421 с.
3. Пєпа Ю.В. Пошук радіозакладних пристроїв з використанням компонентної селекції електромагнітних сигналів / Ю.В. Пєпа, Н.В. Бородюк, С.С. Кириченко // Вісник інженерної академії України. – 2009. – Вип. 3-4. – С.112-115.
4. Вакин С.А. Основы радиопротиводействия и радиотехнической разведки / С.А. Вакин, Л.Н. Шустов. – М.: Советское радио, 1968. – 448 с.

УДК 004.056.55

О.О. Косенко

Науковий керівник – Смірнов О.А., канд. техн. наук, професор
Кіровоградський національний технічний університет

Дослідження ансамблевих, кореляційних і структурних властивостей складних дискретних сигналів

Перспективним напрямком сучасної теорії захисту інформації є стеганографічні системи, у яких забезпечується не тільки приховання інформаційного змісту переданих даних, але й ховається сам факт потайливої передачі повідомлень. Інакше кажучи, основним завданням методів стеганографічного захисту інформації є організація потайливого каналу передачі даних за допомогою вбудовування переданих інформаційних повідомлень в об'єкти (контейнери), що володіють високою природною надмірністю. Найбільш обґрунтований підхід до побудови стеганографічних систем

заснований на використанні сучасних методів цифрової обробки сигналів, кореляційного й спектрального аналізу.

У даній роботі досліджуються методи стеганографічного захисту інформації, засновані на використанні складних дискретних сигналів.

На даний момент існують методи приховання інформації в графічних файлах орієнтовані на формати файлів із втратою, приміром, JPEG. На відміну від LSB вони більше стійкі до геометричних перетворень. Це виходить за рахунок варіювання в широкому діапазоні якості зображення, що приводить до неможливості визначення джерела зображення.

Одним з таких методів є метод розширеного спектра, що полягає в тому, що спеціальна випадкова послідовність вбудовується в контейнер, потім, використовуючи погоджений фільтр, дана послідовність детектується. Даний метод дозволяє вбудовувати велику кількість повідомлень у контейнер, і вони не будуть створювати перешкоди один одному. Метод запозичений із широкопasmового зв'язку. Тому проведемо дослідження ансамблевих, кореляційних і структурних властивостей складних дискретних сигналів, які запозичені з теорії цифрового зв'язку.

Для побудови сучасних перешкодозахищених систем цифрового зв'язку використовуються методи теорії дискретних сигналів, кореляційного й спектрального аналізу.

Побудова перешкодозахищених та імітостійких систем цифрового зв'язку сполучена з рішенням завдання синтезу великих ансамблів слабкорельованих дискретних сигналів з необхідними структурними властивостями. З погляду ефективного використання частотно-часових і енергетичних ресурсів каналів зв'язку найбільш перспективними вважаються широкопasmові системи зі складними дискретними сигналами й прямим розширенням спектра.

Для передачі даних у широкопasmовій системі зв'язку інформаційний сигнал модулюється за допомогою його множення на розширювальний дискретний (кодовий) сигнал. Оскільки кодовий сигнал за своїми статистичними властивостями подібний до шуму, то отриманий розширений сигнал слабо відрізняється від шумів у каналі зв'язку, що й дозволяє здійснити сховану передачу. Показники перешкодозахищеності, що досягаються при цьому, імітостійкості та скритності радіоканалів керування безпосередньо пов'язані з кореляційними, ансамблевими й структурними властивостями використовуваних дискретних сигналів.

У даній роботі проводиться аналіз і порівняльні дослідження властивостей дискретних сигналів, синтезованими різними методами. Зокрема, досліджуються ансамблеві, кореляційні й структурні властивості складних дискретних сигналів, побудованих з використанням переборних методів синтезу в часовій і спектральній області, методи формування ансамблів сигналів на основі рішення систем рівнянь, які задають обмеження на бічні викиди функцій авто- і взаємної кореляції послідовностей і ін. Особлива увага приділена методам синтезу дискретних сигналів з так званими особливими властивостями, тобто сигналам, періодичні функції авто- і взаємної кореляції яких мають «східчастий» вид, а бічні повноти кореляційних функцій приймають кінцеве, заздалегідь задане число значень. Зокрема, досліджуються методи синтезу двійкових сигналів Голда, великі й малі безлічі послідовностей Касамі, недвійкові сигнали Френка, послідовності Лежандра, Пелі-Плоткіна, сигнали Баркера, синтезовані на основі m -послідовностей і для яких отримані аналітичні співвідношення для величин бічних викидів деяких функцій кореляції.

Проведені дослідження переборних методів синтезу дискретних сигналів показали, що величини бічних викидів функції кореляції формованих послідовностей визначаються статистичними методами. Строгий доказ й аналітичні співвідношення,

що описують кореляційні властивості, для таких сигналів відсутні. Дискретні сигнали з особливими кореляційними властивостями дозволяють забезпечити заданий рівень завадостійкості зв'язку. Бічні викиди функції кореляції таких сигналів приймають кінцеві задалегідь відомі значення, що дозволяє використовувати їх на різних етапах організації цифрового зв'язку, у тому числі для синхронізації каналів і в радіолокації. Однак, основним недоліком відомих методів синтезу дискретних сигналів з особливими властивостями є невелика потужність ансамблів формованих послідовностей. Найбільш важливими є методи, засновані на використанні алгебраїчних і структурних властивостей групових кодів. Так, у ході досліджень показано, що субортогональні дискретні сигнали, трьохрівневі сигнали Голда є частковим випадком n -рівневих дискретних послідовностей, утворених перетином циклічних орбіт групового двійкового коду й можуть бути аналітично формалізовані з використанням математичного апарата теорії кінцевих полів і, зокрема, теорії кілець багаточленів.

Таким чином, перспективним напрямком подальших досліджень є розробка методу синтезу великих ансамблів дискретних сигналів на основі перетину циклічних орбіт групового коду для забезпечення необхідних показників перешкодозахисності, імітостійкості й скритності в стеганографічних методах приховання інформації у нерухомих зображеннях орієнтованих на формати графічних файлів із втратою.

Список літератури

1. Коначович Г. Ф., Пузыренко А. Ю. Компьютерная стеганография. Теория и практика. – К.: «МК-Пресс»б 2006. – 288 с., ил.
2. J. Smith, B. Comiskey, Modulation and Information hiding in Image. // Information hiding: First Int. Workshop “InfoHiding’96”, Springer as Lecture Notes in Computing Science, vol 1174. 1996. – pp. 207-227.
3. Цифровые методы в космической связи. /Под ред. С. Голомба.- М.: Связь, 1969. – 272 с.
4. Скляр Б. Цифровая связь. Теоретические основы и практическое применение.–М.:Вильямс,2003.– 1104 с.
5. Горбенко И.Д., Стасев Ю.В. Анализ производных ортогональных систем сигналов // Радиотехника. – 1989. – № 9. – С. 16 – 18.

УДК 621.37:621.391

А.Г. Кудрина

Научный руководитель – Рассомахин С.Г., д-р техн. наук, доцент
Харьковский национальный университет имени В.Н. Каразина

Технология линейного целочисленного декодирования псевдослучайных кодов

Быстрое развитие телекоммуникационных систем повышает актуальность вопросов помехоустойчивости и эффективности при передаче информации. Чтобы достигнуть повышения данных параметров, необходимо объединять результаты, полученные в теории кодирования и в теории модуляции. На сегодняшний день вопросы про область, максимально приближенную к теоретическому пределу Шеннона, которая при этом обладает оптимальными параметрами одновременно по энергетическому и частотному критериям, остаются открытыми. Существенным порогом в развитии случайного кодирования является тот факт, что декодирование таких кодов имеет экспоненциальную сложность. Таким уровнем сложности обладает переборный метод, реализующий правило максимального правдоподобия. Иначе

нельзя гарантировать, что необходимый уровень достоверности данных будет достигнут. Таким образом, стоит задача разработки метода декодирования псевдослучайного кода в гауссовом канале, обладающего сложностью ниже экспоненциальной.

Подойти к решению возможно, применив вместо случайных кодов псевдослучайные коды. Такие коды генерируются с помощью детерминированных методов, которые уже имеют аналитическое описание и могут математически формализовать данную задачу декодирования в виде поиска экстремума целевого функционала. Формируется задача линейного программирования, алгоритм решения которой носит название симплекс-метод. Для генерации случайных чисел используется наиболее распространенный алгоритм - линейный конгруэнтный генератор (ЛКГ). Кодовое слово может быть представлено вектором $\vec{X} = \{x_0, x_1, \dots, x_{n-1}\}$ в n -мерном пространстве кода. По свойствам ЛКГ q -е число связано следующей зависимостью с порождающим числом x_0 , определяющим порядковый номер слова:

$$x_q = \text{mod} \left[a^q x_0 + \frac{a^q - 1}{a - 1} b, m \right], \quad q \in 1..(n-1), \quad (1)$$

где a, b, m – положительные целые константы, b и m – взаимно простые числа; величина $(a-1)$ кратна любому простому числу, которое меньше числа m и является его делителем. В условиях реального гауссова канала на выходе числа искажены случайной, нормально распределенной помехой. При декодировании требуется наиболее верно определить порождающее число передаваемого кодового слова. Вероятнее всего на выходе будут получены дробные числа и в процессе декодирования на них необходимо наложить условие целочисленности. Таким образом, для получения результата необходимо решить задачу линейного целочисленного декодирования. При линейности ограничений расчет всех евклидовых расстояний является нелинейной функцией, и её сложность растет практически по экспоненте с увеличением длины блока.

Подмножество множества возможных решений, включающее в себя все неотрицательные значения, является областью допустимых значений (ОДР). Способ округления полученных компонент до ближайшего целого может не только не дать оптимального решения, но и вывести за пределы ОДР. Правильные методы решения обеспечивают целенаправленное продвижение к искомой вершине оптимального решения по самому короткому пути. Одним из таких методов является решение сформированной симплекс-таблицы. Удобно использовать табличный алгоритм симплекс-метода, так как он легко программируется и хорошо визуализирует ход решения задачи. Для достижения целочисленности формируются дополнительные линейные ограничения (по методу отсечений Гомори), приводящие к увеличению размерности таблицы. Если требование целочисленности распространяется не на все переменные, а только на часть из них, то задача называется частично целочисленной. Способы построения ограничений Гомори различны для полностью и частично целочисленных задач, но они всегда имеют конечное число шагов, что обеспечивает решение поставленной задачи. После этого решается новая задача линейного целочисленного программирования, строится новое ограничение и т.д., пока не будет получен оптимальный план, удовлетворяющий условия целочисленности, либо не будет выявлена несовместимость поставленных условий. Применение данного метода снизит вычислительную сложность задачи. Основным результатом будет являться

получение метода, реализующего все преимущества случайного кодирования при обеспечении оптимальных значений энергетической и частотной эффективности.

Список літератури

1. Акулич И.Л. Математическое программирование в примерах и задачах / И.Л. Акулич. – М.: Высш. шк., 1986. – 319 с.
2. Данциг Дж. Линейное программирование. Его применения и обобщения – М.: Прогресс, 1966.
3. Схрейвер А. Теория линейного и целочисленного программирования. – М.: Мир, 1991.
4. Шевченко В.Н. Линейное и целочисленное линейное программирование / Уч. Пособие. – М.: Физматлит, 2002.
5. Шеннон К. Работы по теории информации и кибернетике / К. Шеннон. – М.: Изд. ИЛ. 1963. – 830 с.
6. Гасс С. Линейное программирование (методы и приложения). – М.: Физматгиз, 1961.

УДК 004.056.5(043.2)

В.М. Мартинюк

Науковий керівник – Павлов В.Г., канд. техн. наук, доцент
Національний авіаційний університет

Эффективность методов защиты программ, как интеллектуальной собственности

Проблемою неліцензійного використання програмного забезпечення (ПЗ) на сьогоднішній день стурбовані більшість його виробників. Кожен день відбуваються численні порушення ліцензійних угод шляхом відключення або злому захисних модулів у програмних продуктах. Це, в свою чергу, призводить до дуже великих збитків для більшості виробників програмного забезпечення, що робить його розробку майже збитковою та суттєво стримує розвиток цієї галузі інтелектуальної праці.

Автором поставлена мета: дослідити ефективність застосування різних засобів захисту програм від неліцензійного використання. При цьому об'єктами дослідження виступають засоби протидії злому програмного забезпечення.

Для цього вирішуються наступні завдання:

- доводитися актуальність вдосконалення механізмів захисту ПЗ;
- розглядаються різноманітні засоби злomu захисту ПЗ;
- здійснюється порівняльний аналіз методів захисту програмних продуктів;
- визначаються перспективні шляхи їх вдосконалення.

Актуальність дослідження визначається наступними чинниками:

- засвідченням права на інтелектуальну власність у законодавстві більшості країн;
- підвищенням ролі якісного програмного забезпечення у належному функціонуванні комп'ютерних інформаційних систем;
- збільшення складності та водночас вартості програмних продуктів;
- посиленням конкуренції на ринку серед виробників програмного забезпечення;
- зростанням кількості користувачів комп'ютерів та відповідно прикладних програм.

Проблема злomu програмного забезпечення породжує необхідність його захисту. Так як процес злomu кожен день еволюціонує, то методи захисту повинні розвиватися з ним, щоб забезпечити захищеність прав розробників ПЗ. Предметом дослідження

виступають методи захисту ПЗ, які існують на сьогоднішній день, та нові, які можуть бути розроблені.

Для аналізу систем безпеки ПЗ було проведено дослідження систем захисту ряду програм, які присутні сьогодні на ринку. Вони показали, що навіть звичайний користувач, який володіє тільки основами роботи за комп'ютером, при бажанні має можливість зламати (отримати додаткові привілеї) слабо захищений продукт, прочитавши деяку інформацію в весвітній мережі Інтернет. Для спеціаліста ж у відповідній галузі це взагалі не є суттєвою проблемою. Це доводить, що більшість виробників використовують в своєму ПЗ достатньо примітивні системи безпеки. Такий захист практично неефективний, але багато фахівців з розробки програмного забезпечення не надають цьому великого значення, внаслідок чого програми зламуються, а їх прибуток зменшується.

Великі компанії по розробці програм виграють лише за рахунок великого обсягу пропонованих програм, коли навіть 10-20% проданих ліцензій окупають витрати і дають не погану прибуток. На системи захисту свого програмного забезпечення вони витрачають не велику кількість ресурсів, тому як їх продукт, в більшості випадків, зламується через декілька днів після представлення програми на ринку спеціальними групами людей, які спеціалізуються на зломі найбільш відомих брендів та переслідують за мету зробити це як можна швидше. Це піднімає репутацію цих груп у своєму колі. Компанії, які випускають програмні продукти в порівняно невеликих обсягах, змушені приділяти питанням їх захисту від неліцензійного використання набагато більше уваги, щоб хоча б окупати свої витрати на їх розробку.

Серед засобів, які використовуються для злomu ПЗ виділяють такі найбільш часто вживані [1]:

- дизасемблер;
- відладчик;
- hex-редактор;
- інші не програмні засоби, які розробляються зломщиками з інженерними здібностями відповідно до об'єкту злomu.

Найбільшу увагу компаніям-розробникам ПЗ треба приділяти не тільки технічним аспектам захисту, а й дослідженню груп людей, які будуть користуватися цим продуктом, щоб мати уяву про свою майбутню долю ринку збуту та розрахувати ймовірність заробітку на ньому. Також досліджуються мотиви зломщиків, щоб уявити, на скільки далеко вони можуть зайти. Виділяють три головних мотивів, які спонукають їх проводити злом ПЗ:

- жарт;
- цікавість;
- прибуток.

Для захисту ПО використовуються різні методи. Основний акцент робиться на захисті програми від дослідження, при якому застосовуються відладчики та дизасемблери [2]. Якщо досліднику вдається вивчити структуру програми, то він може легко відключити механізм захисту або обійти його шляхом зміни програмного коду. Це і є злом, в результаті якого з'являються зламані версії програмних продуктів, начисто позбавлені якого-небудь захисту, або програмні "латки" - патчі, що відключають перевірку прав користувача при використанні ПЗ [3].

У доповіді розглядаються:

- методи і прийоми захисту програм від дослідження відладчиком;
- захист від дизасемблювання за допомогою статичного шифрування;
- застосування криптографічних алгоритмів динамічного шифрування, яке виконується безпосередньо під час виконання програми.

Кожен метод захисту має свої переваги і недоліки, а тому не є ідеальним. При його використанні слід враховувати не тільки суто програмно-технічні аспекти, а й економічні чинники. Впроваджувати ці технології слід з урахуванням необхідного рівня захисту, який повинен бути сумірним з вартістю програм, що захищаються. При цьому можна піти як по шляху застосування вже готових професійних рішень, так і за рахунок розробки власних алгоритмів перевірки прав на використання програм, що захищаються.

Список літератури

1. Касперски К. Техника и философия хакерских атак – записки мыща / Касперски К. – М.: СОЛОН-Пресс, 2004. – 272с.
2. Касперски К. Искусство дизассемблирования / Касперски К., Рокко Е. – СПб.: БХВ-Перепбург, 2008. – 896 с.
3. Панов А.С. Реверсинг и защита программ от взлома / Панов А.С. – СПб.: БХВ – Петербург, 2006. – 256 с.

УДК 004.7

П.С. Молдавський

Науковий керівник – Мелешко С.В., канд. техн. наук, доцент
Кіровоградський національний технічний університет

Розробка програмного забезпечення вбудовування прихованих маркерів у файли для відстежування їх поширення по комп'ютерній мережі

В останні десятиліття все більш важливим стає як поняття інформації, так і сама інформація. А з розвитком комп'ютерних технологій – цифрова інформація. Цифрові фотографії, відео- та аудіоматеріали, звичайна текстова інформація, відкритий програмний код, чи, власне, самі програмні засоби – для певних осіб або організацій можуть мати чимале значення, а тому і вартість, що може досягати дев'ятизначних сум, або навіть коштувати людського життя.

В зв'язку з тенденцією стрімкого розвитку комп'ютерних мереж – як локальних, так і глобальних, – все більшого значення набуває захист цифрових даних від несанкціонованого доступу, використання та поширення. Адже більшість інформації в наш час є продуктом діяльності людського розуму та інтелекту, і потребує захисту прав власності. Одним із способів захисту інформації від незаконного використання, тиражування та розповсюдження є обмеження її використання, коли доступ до неї може мати тільки певна кількість осіб, або й такий варіант, коли доступ надається всім, але не дозволяється копіювати її та використовувати у корисливих – часто комерційних, – цілях. Для запобігання випадків незаконного розповсюдження інформації з обмеженим доступом та виявлення правопорушників, досить доречно відстежувати її поширення.

Одним з методів відстежування є вбудовування у файли, що містять важливу інформацію, прихованих маркерів. За допомогою таких маркерів, в залежності від реалізації, можна здійснювати три способи захисту – окремо чи комплексно: 1) вбудовування певної зашифрованої інформації у файли; 2) приховування самого факту присутності вбудованої інформації; 3) локалізація поширення інформації.

Перший спосіб може забезпечити використання зашифрованої інформації тільки тими, хто має права доступу до неї. Другий спосіб приховує сам факт наявності певної

інформації та запобігає її виявленню і розшифруванню користувачами, що не мають прав доступу до неї. Третій же спосіб дозволяє відстежити шлях розповсюдження файлу в комп'ютерній мережі, та визначити, хто став джерелом, тобто початком його поширення.

Метою роботи є розробка програмного забезпечення вбудовування прихованих маркерів у файли для відстежування їх поширення по комп'ютерній мережі.

Методи дослідження базуються на теорії алгоритмів, теорії зв'язку і телетрафіку, використанні булевої алгебри та чисельних методів, а також математичного апарату теорії захисту інформації, зокрема основ криптографії та стеганографії.

Наукова новизна результатів, отриманих автором, полягає у наступному:

1. Розроблено вдосконалений метод шифрування даних та вбудовування їх у файли у вигляді прихованих маркерів.
2. Розроблено вдосконалений метод відстежування джерел та шляхів несанкціонованого поширення файлів по комп'ютерній мережі.
3. Розроблено вітчизняний продукт системи відстежування поширення інформації в комп'ютерних мережах на основі обміну даними за допомогою клієнт-серверних технологій та алгоритмів самомодифікації.

Практична значимість роботи забезпечується можливістю використання розробленого програмного забезпечення досить широким колом користувачів. Ними можуть бути як окремі особи, що бажають захистити продукт своєї інтелектуальної діяльності від несанкціонованого використання будь-ким, так і організації і установи, які піклуються про безпечність обміну важливою інформацією. Програмний продукт було вирішено будувати на основі нових програмних рішень – в середовищі Microsoft Visual Studio 2010-2012, з використанням технологій Microsoft .NET Framework, – що забезпечує сумісність та широку функціональність в сучасних ОС сімейства Windows.

Список літератури

1. Стеганография, цифровые водяные знаки и стеганоанализ: Монография / [А. В. Аграновский, А. В. Балакин, В. Г. Грибунин, С. А. Сапожников]. – М.: Вузовская книга, 2009. – 220 с.
2. Корнышев Ю.Н., Пшеничников А.П., Харкевич А.Д. Теория телетрафика: учебник для вузов. – М.: издательство «Радио и связь», 1996г, 272 с.
3. Василенко О.Н. Теоретико-числовые алгоритмы в криптографии. / Василенко О.Н. – М.: МЦНМО, 2003.–328 с.

УДК 004.051 (043.2)

К.І. Пулеко

Науковий керівник – Гнатюк С.О., канд. техн. наук, доцент
Національний авіаційний університет

Застосування методу кластеризованих ранжировок при експертній оцінці рішень в галузі інформаційної безпеки

У галузі інформаційної безпеки особам, що приймають рішення досить часто доводиться здійснювати вибір між тими чи іншими технічними і організаційними рішеннями, які мають приблизно однакові технічні і вартісні показники, або навпаки, різко відрізняються за технічними показниками чи вартістю. У цьому випадку математична задача оптимізації прийняття рішення стає векторною і

багатокритеріальною, при чому показники якості системи інформаційної безпеки можуть навіть суперечити один одному.

Одним із варіантів для вирішення такого класу задач може бути використання експертних методів оцінювання. Однак експертне оцінювання відноситься до класу задач, що погано формалізуються, і його застосування також має ряд труднощів, таких як підбір експертів та узгодження думок експертів.

На сьогоднішній день вже є розроблені ряд методик щодо підбору експертів, а у даній роботі пропонується один із варіантів узгодження думок експертів, що отримав назву методу кластеризованих ранжировок.

Метою застосування даного методу є підвищення ефективності обробки експертних рішень.

Суть методу кластеризованої ранжировки, полягає в узгодженні результуючої ранжировки з усіма ранжировками, що подані експертами. При цьому протиріччя між окремими початковими ранжировками переносяться у середину кластерів узгодженої ранжировки. У результаті цього узгоджені кластери відображають загальну думку експертів, точніше, те загальне, що міститься у початкових ранжировках.

Застосування методу кластеризованих ранжировок на практиці доводить свою ефективність, що підтверджує доцільність його використання і в інформаційній безпеці.

Список літератури

1. Горский В.Г., Орлов А.И., Гриценко А.А. Метод согласования кластеризованных ранжировок // Автоматика и телемеханика. 2000. №3. С. 159-167.
2. Орлов А.И. Экспертные оценки // Заводская лаборатория. 1996. Т.62. № 1. С.54-60.

УДК 004.738.5

М.С. Сальников

Науковий керівник – Розорінов Г.М., канд. техн. наук, доцент
Державний університет інформаційно-комунікаційних технологій

Оцінка багатовимірних функцій розподілу ймовірностей

Мовлення, з урахуванням таких його складових, як інформативність, емоціональний окрас, ефект присутності та автентичність являє собою універсальний інструмент спілкування у всіх сферах людської діяльності. Як наслідок, протягом останніх років спостерігається інтенсивна розробка методів та алгоритмів цифрової обробки мовленнєвих сигналів.

Основними напрямками досліджень у галузі цифрової обробки мовленнєвих сигналів є ідентифікація диктора, стискання мовленнєвих сигналів для передавання та зберігання, розпізнавання їх смислових елементів.

У докладі приведено результати досліджень мовленнєвих трактів зі спеціально сформованими характеристиками, на основі використання методів, моделей і алгоритмів, що забезпечують створення і функціонування мовленнєвого тракту на основі багатовимірного ймовірнісного аналізу випадкових процесів.

Для формалізації об'єктів дослідження було застосовано апарат теорії ймовірностей, математичної статистики та цифрової обробки сигналів. Для аналізу об'єктів було застосовано об'єктно-орієнтований аналіз.

На сьогоднішній день існує достатня кількість уніфікованих методів передавання мовленнєвої інформації, які відповідним чином забезпечені програмними і апаратними засобами, відповідають міжнародним та (або) державним стандартам, серійно виготовляються і знаходяться у користуванні широкого кола осіб. У той же час, поряд із зазначеними існують інші методи передавання мовленнєвої інформації, які орієнтовані на особливий порядок їх використання в межах певних груп користувачів.

Особливий порядок при цьому може полягати у спеціально сформованому обмеженні кола осіб, які беруть участь у передаванні і прийманні мовленнєвої інформації, наданні сеансам спілкування заздалегідь визначених реквізитів, підвищені вимог у частині надійності і якості передавання мовленнєвої інформації, тощо.

У процесі досліджень отримано такі наукові результати.

1. Запропоновані алгоритми оцінки багатовимірних функцій розподілу ймовірностей з усередненням за ансамблем реалізацій і за часом. Показано, що оцінки багатовимірних функцій розподілу ймовірностей - незмішені та повні.

2. На основі аналізу багатовимірних функцій розподілу ймовірностей запропонований критерій оцінки ступеня незалежності відліків довільних випадкових процесів, розроблена структурна схема пристрою для визначення незалежності відліків, виконані експерименти щодо оцінки ступеня незалежності відліків довільно розподілених випадкових процесів.

3. Розроблений порядок формування і реалізації основних технічних вимог для створення спеціалізованих мовленнєвих трактів, функціонування яких визначається нормативно-правовими актами.

Основні практичні результати полягають у наступному:

1. Розроблено оригінальний метод передавання і прийому мовленнєвої інформації, що дозволяє формувати спеціалізовані мовленнєві тракти під заздалегідь визначені умови їх функціонування в умовах обмеження кола користувачів.

2. У розробленні механізму втілення спеціальних функціональних вимог, для практичного використання багатовимірних функцій.

Список літератури

1. О.В. Брягин, А.К. Егоров, Г.Н. Розорінов. Об оценке многомерных функций распределения вероятностей речевых сигналов // Регистрация, зберігання і оброб. даних. – 2004.-Т.6, № 3.-С. 41-49.
2. М. Дж. Кенлалл, А. Стюарт. Многомерный статистический анализ и временные ряды. М. Наука.- 1976.- 736 с.

УДК 004.056.55

О.О. Суворов

Науковий керівник – Смірнов О.А., канд. техн. наук, професор
Кіровоградський національний технічний університет

Формування складних дискретних сигналів для стеганографічного захисту інформації

Перспективним напрямком сучасної теорії захисту інформації є стеганографічні системи, у яких забезпечується не тільки приховання інформаційного змісту переданих даних, але й ховається сам факт утаємниченої передачі повідомлень. Найбільш обґрунтований підхід до побудови стеганографічних систем заснований на використанні сучасних методів цифрової обробки сигналів, кореляційного й спектрального аналізу.

У даній роботі досліджуються методи стеганографічного захисту інформації, засновані на використанні складних дискретних сигналів і технології прямого розширення спектра. На прикладі вбудовування інформації в контейнер-зображення показано можливість організації каналу потайливої передачі даних (стеганоканала), досліджена ефективність стеганографічного перетворення з погляду забезпечуваної стійкості, пропускної здатності й величини внесених перекручувань у контейнер-зображення.

У результаті проведених досліджень показано, що використання в стеганографічних цілях прямого розширення спектра дискретних сигналів дозволяє здійснити потайливе вбудовування інформаційних повідомлень у нерушливі зображення. Завдання добування повідомлення на прийомній стороні стеганосистеми еквівалентні завданню виявлення інформації із суміші корисного сигналу й перешкоди в широкопasmовій системі зв'язку.

У ході досліджень виявлені наступні властивості стеганографічних систем з розширенням спектра дискретних сигналів: імовірність правильного добування убудованих даних залежить від величини внесених перекручувань, що у свою чергу залежить від забезпечуваної пропускної здатності стеганоканалу. Інакше кажучи, практична побудова стеганосистеми сполучена з пошуком компромісу між величиною внесених перекручувань, імовірністю правильного добування повідомлення на прийомній стороні й забезпечуваною пропускною здатністю. Крім того, у ході досліджень встановлено, що ймовірність правильного добування убудованих даних безпосередньо залежить від статистичних властивостей використовуваного контейнера-зображення.

Перспективним напрямком подальших досліджень, є використання більших ансамблів слабкорельєваних дискретних сигналів для побудови стеганосистем із прямим розширенням спектра. Це дозволить із однієї сторони без значного підвищення внесених перекручувань у контейнер-зображення істотно підвищити пропускну здатність стеганоканалу. З іншого боку, за рахунок адаптивного формування (вибору) дискретних сигналів за критерієм мінімізації коефіцієнта кореляції з контейнером зображення це дозволить істотно знизити ймовірність помилкового добування убудованих даних.

Список літератури

1. Коначович Г. Ф., Пузыренко А. Ю. Компьютерная стеганография. Теория и практика. – К.: «МК-Пресс», 2006. – 288 с.
2. Горбенко И.Д., Стасев Ю.В. Анализ производных ортогональных систем сигналов // Радиотехника. – 1989. – № 9. – С. 16 – 18.
3. Стасев Ю.В., Кузнецов А.А. та ін. Формирование больших ансамблей дискретных сигналов с использованием избыточных кодов // Збірник наукових праць ХУ ПС. –Харків:ХУПС.–2008.–№2(17). – С. 102-109.
4. Стасев Ю.В. Основы теории побудови сигналів. – Х.: ХВУ, 1999. – 87с.

УДК 004.4

М.В. Старіцин

Науковий керівник – Коноплицька О.К., асистент
Кіровоградський національний технічний університет

Програмне забезпечення системи управління файлами в ОС Windows на основі технології EFS

Encrypting File System (EFS) – Шифрована файлова система – це база технологія що дозволяє управляти файлами, які зберігаються на томах з файловою системою NTFS, з метою збереження конфіденційності. Файлова система EFS

інтегрована в NTFS, відрізняється простотою керування й стійкістю до атак. Користувачі можуть вибирати файли, якими потрібно управляти з метою збереження конфіденційності, але розшифровувати файли вручну перед використанням не потрібно – можна просто відкрити файл і змінити їх, як звичайно. Файли, управління якими реалізовано з метою збереження конфіденційності, будуть захищені навіть у тому випадку, якщо зловмисник одержить фізичний доступ до комп'ютера. Крім того, навіть користувачі, що мають право на доступ до комп'ютера (наприклад, адміністратори), не мають доступу до файлів, якими потрібно управляти з метою збереження конфіденційності, за допомогою файлової системи EFS іншими користувачами. Проте файлова система EFS підтримує призначені агенти відновлення. При їхньому правильному настроюванні можна гарантувати відновлення даних при необхідності. Файлова система EFS в Windows 7/8 і Windows Server 2012 була вдосконала за рахунок наступних основних можливостей: підтримка зберігання ключів шифрування на смарт-картах; централізоване адміністрування політик захисту файлової системи EFS; шифрування клієнтського кеша (автономних файлів) для кожного користувача; шифрування системного файлу підкачування; спрощення відновлення ключів шифрування за допомогою майстра повторного створення ключів.

Таким чином, виходячи з вищеперахованого, розробка програмного забезпечення системи управління файлами в ОС Windows на основі технології EFS є актуальною задачею.

Список літератури

1. Галатенко В.А. Основы информационной безопасности . М.: ИНТУИТ.РУ "Интернет-университет информационных технологий", 2003.
2. Горбатов В.С., Полянская О.Ю. Доверенные центры как звено системы обеспечения безопасности корпоративных информационных ресурсов .Информационный бюллетень Jet Info, № 11 (78), 1999.
3. Столлингс В. Криптография и защита сетей: принципы и практика (2-е издание). / Пер. с англ. — М.: Издательский дом «Вильямс», 2001.

УДК 004.056(043.2)

Д.В. Таратайко

Науковий керівник – Пєпа Ю.В., канд. техн. наук, доцент
Національний авіаційний університет

Технологія застосування електронного цифрового підпису на державному підприємстві “Укрзалізниця”

Вступ. Захист власної інформації, а також її основних властивостей – цілісності, доступності та конфіденційності, для державних та комерційних підприємств, являє собою першочергову задачу, щодо зниження ризиків від можливих інцидентів інформаційної безпеки [1]. Важливе місце в системі заходів захисту інформації займає використання систем електронного цифрового підпису (ЕЦП) [1]. Послуги ЕЦП надаються центрами сертифікації ключів, які здійснюють свою діяльність в сфері електронного документообігу. Електронний підпис застосовується органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями всіх форм власності, іншими суб'єктами господарської діяльності та фізичними особами.

Основна частина. Укрзалізниця одна з перших державних структур в Україні, яка почала впроваджувати технологію ЕЦП, як для здійснення внутрішнього електронного документообігу [2], так і для взаємовідносин із клієнтами. Завдяки цьому Україна є першою серед країн СНД, де впроваджені електронний підпис при організації перевезення вантажів залізничним транспортом. Використання даної технології значно прискорити розвиток безпаперових технологій на залізничному транспорті, оскільки замінює традиційну печатку та підпис. Вона дозволяє документам, що пересилаються в електронному вигляді між Укрзалізницею та іншими установами, організаціями і клієнтами, набути юридичного статусу. Така процедура суттєво прискорює обробку документації і надає гарантію достовірності та цілісності електронного документообігу з урахуванням механізмів підписування документів [3]. Нововведення сприяють підвищенню ефективності роботи залізничного транспорту, а також покращенню якості обслуговування клієнтів.

На сьогоднішній день впроваджено технологію ЕЦП в процес оформлення та доставки перевізних документів в вантажному сполученні. Це сприятиме прискоренню процесів інформаційного обміну, підвищенню безпеки, надійності, оперативності та ефективності роботи залізничного транспорту, а також підприємств, що користуються його послугами. Так як Укрзалізниця є державним підприємством, то в процесі своєї діяльності необхідно використовувати посилені сертифікати ключів, згідно чинного законодавства [4-5].

Згідно з експертним висновком на об’єкті використовується програмно-технічний комплекс «ІТ ЦСК-1» у складі: апаратний модуль підпису «ІТ АМП «Грядя-41П», апаратний генератор випадкових чисел «Грядя-3», мережевий криптографічний модуль «ІТ МКМ «Грядя-301». Система реалізує такі криптографічні алгоритми: ГОСТ 28147-89, ГОСТ 34.311-95, ДСТУ 4145-2002.

Стандартом [6] рекомендується наступний алгоритм генерації криптографічно надійних параметрів еліптичних кривих.

1. Вибираємо випадкову криву $E(GF(q))$ алгоритмом, вказаним у стандарті.
2. Обчислюємо її порядок $N = |E(GF(q))|$.
3. Перевіряємо чи ділиться N на раніше вибране просте число n ($n > 2^{160}; n > \sqrt[q]{q}$). Якщо ні, то переходимо до кроку 1.
4. Перевіряємо, що n не ділить ні одне з чисел $q^k - 1; k = 1, \dots, 20$. Якщо ні, то переходимо до кроку 1.
5. Перевіряємо, що $n \neq q$. Якщо ні, то переходимо до кроку 1.
6. Вибираємо довільну точку $G' \in E(GF(q))$ та вважаємо, що $G = (N/n)G'$.

Повторюємо, доки не отримаємо $G \neq O$.

Розглянемо переваги впровадження ЕЦП на Укрзалізниці:

- значно скорочується час руху документів у процесі оформлення;
- встановлюється контроль за термінами обробки документів у кожній інстанції;
- удосконалюється та спрощується процедура підготовки, узгодження, доставки, обліку і зберігання документів;
- унеможливується зміна змісту та несанкціонованого використання документів;
- гарантується достовірність документів;
- мінімізується ризик фінансових втрат за рахунок підвищення конфіденційності інформаційного обміну;
- підвищується оперативність доставки та захищеність конфіденційних документів (з грифом «Комерційна таємниця») за рахунок можливостей шифрування;
- забезпечується моніторинг та контроль за електронним документообігом.

Висновки. Використання ЕЦП у документообігу дозволяє:

1. Забезпечити оперативний та надійний обмін з партнерами юридично значимими електронними документами, зменшити, а в деяких випадках зовсім ліквідувати паперовий документообіг;

2. Зменшити навантаження на співробітників залізничного транспорту по підготовці первинних технологічних документів, переклавши частину цієї роботи на клієнтів;

3. Прискорити обмін документами з органами державної влади.

Таким чином, використання ЕЦП суттєво підвищує рівень захищеності електронного документа і, як правило, суттєво ускладнює процедуру підбору ЕЦП до електронного документа.

Список літератури

1. Хорошко В.О. Основи криптографічного захисту інформації: [підруч.] / В.О. Хорошко, Г.М. Гулак. – Вінниця: ВНТУ, 2011. – 199 с.
2. Укрзалізниця: Акредитований центр сертифікації ключів – [Http://www.csk.uz.gov.ua/index.php?page=docshow&docview=6](http://www.csk.uz.gov.ua/index.php?page=docshow&docview=6).
3. Таратайко Д.В. Механізм накладання електронного цифрового підпису на документ / Д.В. Таратайко, Ю.В. Пєпа // Інформатика і комп’ютерні технології: Збірка праць VII Міжнар. наук.-техн. конф. студ., асп. та молод. учених, Донецьк, 22-23 листопада 2011 р. – Донецьк: ДонНТУ, 2011. – Т.1. – С.286-290.
4. Закон України «Про електронні документи та електронний документообіг» // Відомості Верховної Ради. – №36. – 2003. – ст. 275. – №851-IV від 22.05.2003 р.
5. Закон України «Про електронний цифровий підпис» // Відомості Верховної Ради. – №36. – 2003. – ст. 276. – №852-IV від 22.05.2003 р.
6. The Elliptic Curve Digital Signature Algorithm Validation System (ECDSAVS) / L.E. Bassham // National Institute of Standards and Technology (USA), 2004. – 64 p.

УДК 004.738.5

С.С. Тімохін

Науковий керівник – Горбенко І.Б., д-р техн. наук, професор
Харківський національний університет імені В.Н. Каразіна

Кодування інформації точками на еліптичній кривій

Криптосистеми з використанням еліптичних кривих (ЕК) належать до систем з відкритим ключем і були запропоновані у 1985 році. Але до сих пір не було знайдено алгоритму, що дозволив би обчислити особистий ключ швидше ніж з експоненційною складністю. ЕК широко використовуються у цифровому підписі, але не у потоковому шифруванні. Причиною тому є складність подання інформації точками ЕК.

Метою цієї статті є огляд існуючих алгоритмів представлення інформації у вигляді точок на еліптичній кривій, їх порівняння та оцінка за критеріями складності виконання та швидкодії.

У 1985 році Н. Кобліц [1] запропонував імовірнісний алгоритм кодування. Він дозволяє представити інформацію з довільним алфавітом потужності M , $0 \leq m < M$. Обирається достатньо велике число k , $p > kM$, що характеризує вірогідність помилки.

$$P_{\text{пом}} = 1 / 2^k \quad (1)$$

Очевидно, що при збільшенні k збільшується надійність, а розмір алфавіту зменшується і навпаки. Цілі числа представляються у вигляді $0 \leq mk + j < M$, де $1 \leq j \leq k$. Якщо хоча б для одного з $mk + j$ знайдено корінь квадратний за модулем, то вважається, що інформація успішно закодована. Для декодування необхідно обчислити:

$$\begin{cases} m = (x - k) / k, x \equiv 0 \pmod{k} \\ m = (x - x \pmod{k}) / k, x \not\equiv 0 \pmod{k} \end{cases} \quad (2)$$

Перевагою методу є його простота, та у пам'яті необхідно тримати тільки точку з координатами та число k . Алгоритм не вимагає жодних перед обчислень та дотикових витрат. Достатньо простою є процедура вилучення інформації. Недоліками методу є те що він імовірнісний, але при достатньо великому виборі параметра, вірогідність помилки прямує до нуля. Але це зменшує максимальний розмір алфавіту.

Інший алгоритм використовує поняття дуальних ЕК [2]. Дві еліптичні криві:

$$E_{a,b}: y^2 = x^3 + ax + b, E_{a',b'}: y'^2 = x'^3 + a'x' + b' \quad (3)$$

називаються дуальними, якщо виконується умова:

$$\begin{cases} a' = v^2 a \pmod{p} \\ b' = v^3 b \pmod{p} \end{cases} \quad (4)$$

де $v \in Fp$ не є квадратом у полі. Обирається довільний $v \in Fp$ і обчислюються параметри дуальної ЕК. Необхідно знайти, для яких значень $i \in [0, 2M - 2]$ значення виразу $i^3 + ai + b$ не є квадратом, а для яких iv виразу $(iv)^3 + a'iv + b'$. Далі обирається ЕК, що має більше квадратів на цьому відрізку. Інформація кодується послідовно, кожний символ алфавіту у наступний квадрат поля, для якого обчислюється у координата над еліптичною кривою. Перевагами даного методу є те, що він детермінований. Причому для кодування можуть використовуватися усі точки ЕК і потужність алфавіту може дорівнювати порядку ЕК, але це займе багато часу. Недоліками цього методу є велика кількість перед обчислень необхідних для побудови таблиці кодування. І найважливішим недоліком є послаблення стійкості криптосистеми, якщо для кодування використовується дуальна ЕК [3].

Був запропонований інший детермінований алгоритм кодування інформації на ЕК. Для цього обирається особлива еліптична крива, побудована у кільці Zq :

$$q = \prod_{j=1}^n p_j \quad (5)$$

де p_j - попарно прості числа. Алгоритм використовує представлення числа у системі лишкових класів, використовуючи китайську теорему про лишки. Необхідно побудувати n масивів обчислюючи точки на даній еліптичній кривій для кожного з множників q . Тобто $\forall i, 0 < i < n, \forall x, 0 < x < p_i$ обчислюється символ Лежандра:

$$\left(\frac{a}{p}\right) = \left(\frac{x^3 + ax + b}{p_i}\right) \quad (6)$$

Якщо вираз (11) дорівнює одиниці, тоді у i -тий масив записуються дві точки:

$$P(x, \text{sqrtmod}(x^3 + ax + b)), P(x, p_i - \text{sqrtmod}(x^3 + ax + b)) \quad (7)$$

Функція $\text{sqrtmod}(a)$ обчислює корінь квадратний за модулем. Якщо ж вираз (7) дорівнює нулю, тоді у цей масив записується одна точка з координатами $P(x, 0)$.

Для кожного символу m алфавіту M обирається n точок з кожного з сформованих масивів з індексом $m \pmod{p_i}$. Для того, щоб декодувати отриману інформацію необхідно сформувати тривимірний масив $k[n][p_i][p_i]$. Масив

заповнюється наступним чином: $\forall i, 0 < i < n, \forall x, 0 < x < p_i$, якщо символ Лежандра (7) дорівнює одиниці, тоді

$$k_{i,x,\text{sqrtmod}(x+ax+b)} = t, k_{i,x,p-\text{sqrtmod}(x+ax+b)} = t+1, t = t+2 \quad (8)$$

Якщо він дорівнює нулю, тоді маємо:

$$k_{i,x,0} = t, t = t+1 \quad (9)$$

Отримавши n точок, необхідно обрати з масиву n чисел підставивши по порядку $0 < i < n$ у першу координату масиву та x -, y -координати у відповідно другу та третю координату масиву. Отримані числа є представленням закодованого числа у системі лишкових класів.

Для того, щоб відновити число з системи лишкових класів, необхідно скористатися формулою:

$$X = \left(\sum_{i=0}^{n-1} \frac{q}{p_i} (x_i \left(\frac{q}{p_i}\right)^{-1} \pmod{p_i}) \pmod{q}\right) \quad (10)$$

Перевагами методу є те, що можна закодувати алфавіт великої потужності. Недоліками є те, що рекомендовані ЕК будуються у полі, а не кільці, а також можуть виникнути помилки при $l_i < p_i$.

Список літератури

1. Коблиц Н. Курс теории чисел и криптографии. / Н. Коблиц. К.: ТВП, 2001. – 254 с.
2. Лёвин В.Ю. Кодирование алфавитов точками эллиптических кривых. / В.Ю. Лёвин // Интеллектуальные системы. – 2007. – №4. С. 171—183.
3. Бабенко М.Г. Разработка программного комплекса шифрования данных на основе использования точек эллиптической кривой: научно-исследовательская работа / Бабенко М.Г. и др. - М-во образования РФ, С.: СГУ им. НГ Чернышевского, 2011. - 91 с.

УДК 004.627

А.І. Ускова

Науковий керівник – Рассомахін С.Г., д-р техн. наук, професор
Харківський національний університет імені В.Н. Каразіна

Використання методів кліпуючих перетворень мовних сигналів у комп'ютерних мережах

У зв'язку зі швидкими темпами розвитку комп'ютерних та Інтернет технологій, а також із проблемами обмеженості можливостей пристроїв для збереження та передачі інформації, останнім часом все більшого розвитку набувають технології та методи стиснення інформації. На сьогодні існує багато методів зменшення надмірності мови і одним із є кліпування мовного сигналу.

Кліпування відноситься до методів амплітудної компресії, сутність якої полягає у стисненні динамічного діапазону мовного повідомлення на передаючій стороні, а на приймаючій стороні виконується відновлення динамічного діапазону мовного повідомлення. Таким чином, кліпування мовних даних дозволяє суттєво зменшити об'єм даних, що передаються.

Сутність методу кліпування полягає у обчисленні знакової функції мовного сигналу, тобто заміни мовного сигналу на сигнал із постійною амплітудою, значення якої змінюється у моменти переходу через нуль. Такий сигнал зберігає достатню мовну розбірливість для тих випадків, коли тембр голосу не важливий. Саме через втрату

пізнаваності голосу, яка викликана сильним зашумленням мови при її максимальному амплітудному обмеженні і сильному шумі у паузах розмови, цей метод не знаходить широкого практичного застосування. Таким чином, щоб на приймаючій стороні відновити сигнал необхідно позбутися його артефактів. На сьогодні існує багато програм, таких як CuteStudio Declip, Sony Sound Forge, Adobe Audition, Nero Wave Editor, кожна з яких пропонує свій метод боротьби з проблемою кліпування. Більшість з них використовують різні алгоритми інтерполяції, що дозволяє майже повністю відновлювати сигнал після обробки. До інших методів відновлення сигналу, можна віднести, наприклад:

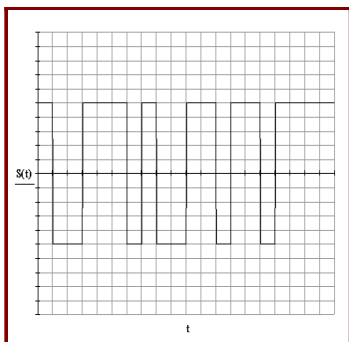


Рисунок 1 – Приклад кліпованого сигналу

1) разом із передачею кліпованого файлу передавати по окремому каналу обвідну мови і на приймаючій стороні відновлювати природну різницю гучності звуків.

2) метод відновлення амплітуди сигналу шляхом оцінювання швидкості зміни значень сусідніх відліків від аналізованого кліпованого відрізка і на основі алгоритму інтерполяції розраховується значення амплітуди даного відрізка.

В даній роботі кліпування розглядається як метод компактного стиснення звукових сигналів і досягається шляхом обрізання амплітуди сигналу. Як метод позбуття артефактів кліпування в даній роботі представлений алгоритм, який відновлює сигнал шляхом визначення прямопропорційної залежності амплітуди сигналу від розмірів відрізків відліків сигналу. Це дозволяє майже повністю відновити сигнал і повернути впізнаваність голосу, а також позбутися сильного зашумлення мови.

Список літератури

1. Попов О.Б. Цифровая обработка сигналов в трактах звукового вещания./ Попов О.Б., Рихтер С.Г. – М.: Горячая линия - Телеком, 2007. – 341 с.
2. Методы непосредственной компрессии речевого сигнала [Электронный ресурс] // Режим доступа: <http://www.avantes.com.ua/node/202>.

УДК 004.492.2

Е.Д. Хамидуллина

Научный руководитель – Губенко Н.Е., канд. техн. наук, доцент
Донецкий национальный технический университет

Прогнозирование и оценка потерь, связанных с угрозами информационных систем

В современном мире вопрос защиты информации на предприятии – это важный аспект ведения бизнеса.

Информационная безопасность — это общее понятие для защиты информационной среды, защита информации представляет собой деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.[1]

Для того чтобы понять как защитить систему, необходимо различать какие угрозы существуют. Угрозы различают по типу и происхождению.

Типы угроз:

- 1) Физические (пожар, наводнение)
- 2) Природные (сейсмическая, вулканическая активности)
- 3) Потеря сервисов (перебои в электричестве, кондиционировании, телекоммуникациях)
- 4) Компрометирование информации (кража медиа, извлечение и использование скрытой информации)

5) Выход из строя техники

6) Неправильное использование прав и т.д.

Происхождение угроз:

- 1) Намеренные (шпионаж, нелегальная обработка данных)
- 2) Случайные (выход из строя оборудования, сбои в программах)
- 3) Среда (природные происшествия)[2]

Основной задачей отдела информационной безопасности предприятия является сведение к минимуму потерь, которые так или иначе связаны с недостатками системы защиты главных свойств информации (доступность, целостность, конфиденциальность).

Расчет потерь от угроз доступности производится по формуле:

$$L = L_{ul} + L_r + L_d + L_{li},$$

где L_{ul} – потери от несвоевременного оказания услуг по доступу к информации; L_r – потери, связанные с восстановлением работоспособности; L_d – потери, связанные с простоем узла системы; L_{li} – потери, связанные с потерей дохода.

Потери, связанные с восстановлением работоспособности рассчитываются:

$$L_r = \frac{\sum_{i=1}^n S_i}{T} * t_r,$$

где S_i — зарплата в месяц сотрудника, восстанавливающего работоспособность атакованного узла системы (АУС); N — количество сотрудников, восстанавливающих работоспособность АУС; t_r — время восстановления работоспособности; T — количество рабочих часов узла системы в месяц.

Потери, связанные с простоем АУС рассчитываются по формуле:

$$L_d = \frac{\sum_{i=1}^n S_i}{T} * t_d,$$

где t_d — время простоя АУС.

Потери, связанные с потерей дохода определяются по формуле:

$$L_{li} = Inc * \frac{t_r + t_d}{T},$$

где Inc – годовой доход от использования АУС.

Аналогично рассчитываются и другие потери от реализации угроз целостности и конфиденциальности. [3]

Широко известно, что прогнозирование является одной из задач современного бизнеса. Прогнозирование потерь является такой же важной задачей, как и прогнозирование прибыли. Предсказание будущих угроз может стать серьезной и сложной задачей для отдела информационной безопасности.

Прогнозирование методом аналогий предполагает наличие опыта и референтных ситуаций, то есть существование модели, которая показывает такое же поведение в аналогичной ситуации. Таким образом, менеджер отдела информационной безопасности может изучить поведение системы в похожей ситуации, которая происходила раньше или с другой компанией, предсказать возникновение угрозы и предполагаемые потери от нее, что может в значительной степени сократить влияние этой угрозы на предприятие.

Для того чтобы проследить частоту появления угроз и методы, которые использовались для борьбы с проблемой, менеджеру необходимо создать базу данных, в которой будут отображаться эти показатели.

Пример такой базы данных:

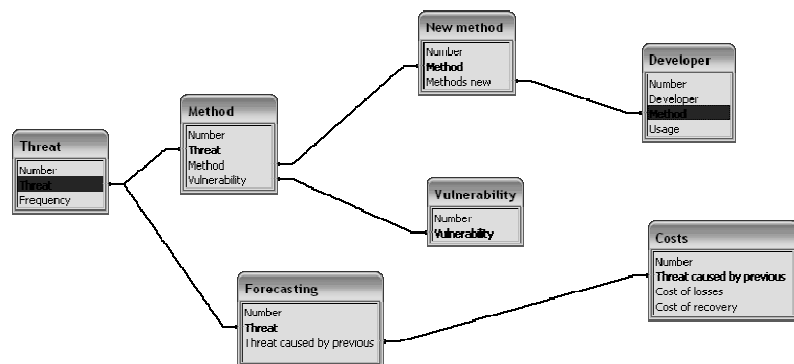


Рисунок 1 – База данных для реализации прогнозирования угроз методом аналогий

Прогнозирование и анализ потерь от информационных угроз является очень важным аспектом в жизни любой компании. То, каким методом производить прогнозирование потерь зависит только от менеджера отдела информационной безопасности. Этот выбор может зависеть от многих факторов. Все методы имеют свои преимущества и недостатки. Например, недостатком метода аналогий является его сложная программная реализация. Кроме того, не всегда можно найти аналогичную ситуацию в прошлом, что также может затруднять дальнейшее прогнозирование.

Список литературы

1. Свободная энциклопедия «Википедия» [Электронный ресурс] / Статья «Информационная безопасность» // Режим доступа к статье: http://ru.wikipedia.org/wiki/Информационная_безопасность.
2. The Free Encyclopedia “Wikipedia” [Электронный ресурс] / Перевод статьи «Threat(computer)» // Режим доступа: [http://en.wikipedia.org/wiki/Threat_\(computer\)](http://en.wikipedia.org/wiki/Threat_(computer)).
3. Анализ модели для оценки потерь, связанных с реализацией угроз и страхованием информационных рисков: сб. текстов выступления на четвертой международной научно-технической конференции «Моделирование и компьютерная графика/ ДонНТУ 5-8 октября – Д.: 2011. – 33с.

УДК 004.4

О.В. Хейдер

Науковий керівник – Мелешко Є.В., канд. техн. наук, доцент
Кіровоградський національний технічний університет

Розробка програмного забезпечення ЕЦП для автентифікації користувачів у системах дистанційного навчання та тестування

У сучасних умовах збільшення кількості інформації, оброблюваної, переданої й збереженої в системах дистанційного навчання й тестування, привело до підвищення актуальності завдань:

- забезпечення конфіденційності, цілісності, незаперечення авторства електронного документа системи дистанційного навчання й тестування;
- створення захищеного системи дистанційного навчання й тестування;
- забезпечення високої швидкості обробки й підписання електронного документа системи дистанційного навчання й тестування.

У цей час основу забезпечення безпеки системи дистанційного навчання й тестування становлять системи електронного цифрового підпису (ЕЦП). Найбільше широко застосовуваним видом ЕЦП є індивідуальний підпис. Сучасні системи дистанційного навчання й тестування дозволяють обробляти й підписувати документ одночасно тільки одним користувачем, що збільшує час обробки й підписання документа, якщо його повинні підписати трохи користувачів. Отже, розмір ЕЦП збільшується пропорційно числу користувачів, що підписують електронний документ у кілька разів. При цьому процедура перевірки дійсності підпису має на увазі перевірку підписів всіх що підписали.

Крім того, варіант “один документ – один підпис” є не єдиним, необхідним на практиці. Зокрема, питання передачі документів від імені деякого колегіального органа або від імені сукупності суб’єктів роблять актуальним питання розробки систем ЕЦП на основі поняття колективного відкритого ключа. Ідея ЕЦП на основі відкритого колективного ключа полягає в тому, щоб побудувати протокол формування й перевірки підпису таким чином, що ЕЦП звичайного розміру буде підтверджувати дійсність деякого заданого електронного документа системи дистанційного навчання й тестування, підписаного кожним користувачем з деякого заданої безлічі користувачів.

В області теорії й практики розробки ЕЦП, як у нашій країні, так і за рубежом, видана велика кількість праць. З їхнього числа слід зазначити роботи ЭльГамала Т., Шнорра К., Рабина М., Кобліца Н., Горбенко І.Д., Долгова В.І., Ростовцева А.Г., Черемушкина А. В., Молдовяна Н. А., Еремеева М. А., Маховенко Е. Б., і ін.

Створення методу формування й перевірки ЕЦП на основі колективного відкритого ключа дає можливість обробки й підписання документа одночасно декількома користувачами. При цьому розмір ЕЦП не збільшується, що дозволяє скоротити обсяг надлишкової інформації, необхідної для автентифікації електронних

документів і спростити протокол підтримки такого ЕЦП. Час на підписання документа залишається колишнім, як і при стандартній процедурі підпису, а час перевірки дійсності ЕЦП зменшується.

Таким чином, виявлена проблемна ситуація, обумовлена як протиріччя між необхідністю забезпечення дійсності й збереження цілісності інформації в системі дистанційного навчання й тестування при колективній обробці електронних документів і невідповідністю існуючих методів, алгоритмів і засобів організації захищеного документообігу сучасним вимогам захищеності, функціональності, а також оперативності.

Розрішення даної проблемної ситуації вимагає створення методу формування й перевірки електронного цифрового підпису на основі колективного відкритого ключа.

Метою магістерської роботи є розробка програмного забезпечення ЕЦП для автентифікації користувачів у системах дистанційного навчання та тестування.

Для досягнення поставленої мети вирішувалося наукове завдання побудови схем електронного цифрового підпису на основі колективного відкритого ключа.

Досягнення поставленої мети й рішення наукового завдання зажадало рішення наступних часткових завдань досліджень:

1. Проведення аналізу сучасних методів і засобів захисту систем дистанційного навчання й тестування.

2. Здійснення вибору системи електронного цифрового підпису як основного механізму забезпечення оперативного захищеного системи дистанційного навчання й тестування.

3. Розробки методу формування й перевірки електронного цифрового підпису на основі відкритого колективного ключа.

4. Розробки алгоритму вибору параметрів електронного цифрового підпису на основі відкритого колективного ключа.

5. Розробки методики організації захищеної системи дистанційного навчання й тестування.

6. Розробки програмного комплексу по реалізації електронного цифрового підпису на основі відкритого колективного ключа й рекомендації з її впровадження в систему захищеного дистанційного навчання й тестування (системи захищеного дистанційного навчання й тестування).

Об’єктом дослідження є процес реалізації системи дистанційного навчання й тестування

Предмет – методи створення й перевірки електронного цифрового підпису при організації системи дистанційного навчання й тестування.

Список літератури

1. "Дистанционные методы обучения. Состояние, проблемы, перспективы." // Дайджест педагогических идей та технологій "Школа – парк". – 2001. – № 3-4. – С. 81 – 103
2. Трохименко В. Дистанційне навчання педагогічних працівників: досвід і проблеми// Післядипломна освіта в Україні. – 2004. – С. 29 – 32.
3. Ахьян А.А. Виртуальный педагогический вуз. Теория становления. – СПб.: Изд-во "Корифей", 2001. – 170 с.
4. Зайченко Т.П. Основы дистанционного обучения: Теоретико-практический базис: Учебное пособие. – СПб.: Изд-во РГПУ им. А.И. Герцена, 2004. – 167 с.

ПРОГРАМНЕ ТА ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ АВТОМАТИЗОВАНИХ СИСТЕМ КЕРУВАННЯ

УДК 681.518.2

Е.Р. Власюк, Б.А. Март, А.А. Покотило, Б.В. Ступак
Научный руководитель — Ролик А.И., канд. техн. наук, доцент
Национальный технический университет Украины
«Киевский политехнический институт»

Методы оценки состояния элементов корпоративной ИТ-инфраструктуры

Эффективность функционирования автоматизированных систем управления в большой мере зависит от качества и надежности работы информационно-телекоммуникационных систем (ИТС), которые предоставляют информационные и вычислительные ресурсы для решения задач пользователей. Необходимым условием принятия эффективных решений по управлению ИТС является наличие достаточного количества точной и актуальной информации о состоянии системы и ее подсистем. С этой целью выполняется непрерывный мониторинг элементов ИТС. Мониторинг состояния и управление такими системами усложняется их распределенным характером, иерархической структурой, использованием большого количества аппаратно-программных средств. Для мониторинга и управления ИТС используются как специализированные, так и универсальные средства и системы управления. Интеграцию таких средств и систем управления осуществляют системы управления ИТ-инфраструктурой (СУИ) [1, 2], задача которых состоит в обобщении данных мониторинга, предоставлении математически точной и лингвистически понятной оценки состояния каждого элемента ИТ-инфраструктуры, определении соответствия показателей качества функционирования элементов ИТС и системы в целом заданным значениям. В целях обеспечения максимального удобства восприятия текущего состояния системы администраторами целесообразно использовать лингвистические конструкции для отображения состояния элементов ИТС, которые сопоставляются числовым значениям по определенным правилам.

Целью работы является создание подсистемы пересчета метрик и оценки состояния и качества функционирования элементов ИТ-инфраструктуры.

Основой модели ИТ-инфраструктуры, с которой оперирует СУИ, является объект мониторинга и управления (ОМУ) — элемент логической модели системы, основная функциональная единица представления элементов системы. ОМУ отражает состояние реальных объектов ИТС, в качестве которых могут выступать рабочие станции, серверы, сетевое оборудование, сервисы, бизнес-процессы и пр. В ОМУ в виде набора параметров заключены те свойства элементов системы, которые имеют отношение к процессам управления ИТ-инфраструктурой. Параметрами ОМУ являются разнообразные характеристики объекта, а в виде специальных параметров состояния отображаются различные аспекты состояния ОМУ, такие как эффективность, надежность и работоспособность. Для описания взаимных связей между элементами ИТС и их взаимного влияния вводятся соответствующие связи в модели ОМУ [2].

Для оценки состояния ОМУ разных типов используются разнообразные модели, методы и алгоритмы. Подсистема оценки состояний СУИ реализована в виде комплекса унифицированных настраиваемых методов для оценки состояний ОМУ и его параметров, а также сведения метрик. Для каждого типа ОМУ настраивается один или несколько методов оценки, которые, используя числовые значения параметров ОМУ, дают качественную оценку их текущему состоянию.

Методы оценки делятся на те, которые работают на уровне одного параметра, определяя его состояние по численному значению, и те, которые работают с несколькими параметрами. При расчете значения либо состояния некоторого параметра участвующие в расчете параметры могут принадлежать тому же ОМУ, что и данный параметр, либо нескольким ОМУ, находящимся ниже по иерархии. К первой группе методов относятся метод границ состояний и метод нечеткой оценки состояний, ко второй — метод статистического расчета и метод копирования состояния объекта, от которого зависит данный ОМУ. Для возможности оценки состояний с использованием специфических правил, которые нельзя реализовать с помощью предложенных методов, администратор может определить пользовательский метод оценки состояния.

Метод границ состояний заключается в том, что область значений, которые может принимать параметр ОМУ, делится на интервалы, каждому из которых сопоставляется определенное состояние. Метод нечеткой оценки (по Мамдани) [3] обеспечивает наиболее гибкую и точную оценку состояния, но является ресурсоемким и сложным в настройке. В этом случае для каждого лингвистического значения состояния задаются функции принадлежности в виде кривых и состояние объекта определяется путем выбора лингвистической величины, функция принадлежности которой принимает максимальное значение для текущего значения параметра. Метод статистического расчета позволяет при расчете состояния текущего параметра учитывать показатели зависимых параметров, используя следующие алгоритмы статистического расчета: среднего арифметического, среднего геометрического, взвешенной суммы, взвешенной нормированной суммы, взвешенного среднего арифметического, взвешенного среднего гармонического. Использование весов во взвешенных алгоритмах позволяет придать одним параметрам большую важность, чем другим, и таким образом задать приоритеты. Метод копирования состояния объекта, от которого зависит данный, не является методом оценки состояния, однако позволяет отображать состояние ОМУ в случае, если оно зависит только от одного параметра. Для определения пользовательского метода оценки состояния необходимо реализовать определенный программный интерфейс в виде модуля, содержащего один или более алгоритмов оценки состояния, после чего подключить его к системе. Так можно реализовать метод, приспособленный для решения конкретных задач.

Представленные методы реализованы в виде подсистемы оценки состояний и пересчета метрик в СУИ, разрабатываемой на кафедре АУТС НТУУ «КПИ», и показали хорошие результаты для автоматического определения состояний объектов ИТС. Программная реализация подсистемы обеспечивает наглядное представление состояний каждого элемента ИТС и позволяет автоматизировать принятие решения по управлению ИТ-инфраструктурой, ускорить локализацию неисправности, и как следствие, повысить эффективность управления ИТ-инфраструктурой.

Список литературы

1. Теленик С.Ф. Система управління інформаційно-телекомунікаційною системою корпоративної АСУ / С.Ф. Теленик, О.І. Ролік, М.М. Букасов, Р.Л. Соколовський // Вісник НТУУ «КПІ». Інформатика, управління та обчислювальна техніка. — К.: «ВЕК+», — 2006. — № 45. — С. 112—126.
2. Ролік А.І. Система управління корпоративної інформаційно-телекомунікаційної інфраструктурою на основі агентського походу / А.І. Ролік, А.В. Волошин, Д.О. Галушко, П.Ф. Можаровський, О.О. Покотило // Вісник НТУУ «КПІ». Інформатика, управління та обчислювальна техніка: Зб. наук. пр. — К.: «Век+», — 2010. — № 52. — С. 39—52
3. Mamdani E.H. Applications of fuzzy logic to approximate reasoning using linguistic synthesis // IEEE Transactions on Computers. — 1977. — v. 26, No. 12. — P. 1182—1191.

УДК 004.75

Д.И. БойкоНаучный руководитель – Воронин Д.Ю., канд. техн. наук, ст. преподаватель
Севастопольский национальный технический университет

Автоматизация управления распределенными вычислительными процессами при использовании библиотеки имитационных моделей

В настоящее время распределенные вычислительные процессы (РВП) в большинстве случаев реализуются с применением грид-систем, которые представляют собой сложные вычислительные комплексы гетерогенной структуры, обрабатывающие неоднородный поток вычислительных задач. Дефицит априорной информации, быстрая смена оперативной ситуации, динамичность структуры, а также жесткие директивные требования к реактивности таких систем существенным образом усложняют процессы управления – возникает необходимость создания развитых инструментальных средств автоматизации управления РВП [1]. Одной из базовых задач обеспечения их функциональной безопасности является выбор оптимальной стратегии диспетчеризации.

В связи со значительными временными и финансовыми затратами на реконфигурацию РВП необходимо предварительно промоделировать последствия различных сценариев развития событий при помощи имитационных экспериментов. Принимая во внимание ряд неоспоримых достоинств современного инструментального средства AnyLogic [2], было принято решение повысить адекватность реализуемых моделей путем синтеза специализированной библиотеки Grid Library, компоненты которой учитывают особенности рассматриваемой предметной области.

В состав Grid Library входят следующие компоненты: источник заданий, сеть передачи данных, глобальный диспетчер заданий, вычислительный узел, кластер, локальный менеджер заданий, сборщик пакета заданий. Необходимая статистика экспортируется в формате, пригодном для последующей статистической обработки специализированными инструментальными средствами. Таким образом, у исследователя появляется возможность получить целостную картину изменения эффективности управления РВП в зависимости от выбираемой дисциплины планирования и стратегии диспетчеризации. Каждый компонент библиотеки имеет множество настраиваемых параметров и методов, позволяющих достаточно гибко и на необходимом уровне абстракции управлять ходом имитационных экспериментов. Например, для источника заданий возможна установка следующих параметров: количество заданий в пакете, минимальные и максимальные границы вычислительной трудоемкости каждого из требований задания (в режиме пакетной работы), интенсивность поступления заданий в систему, число одновременно поступающих заданий, закона распределения, согласно которому поступают задания для потоковой обработки и т.д. По умолчанию параметры, определяющие вычислительную трудоемкость и структуру заданий, генерируются случайным образом, однако, в целях тестирования и калибровки модели, имеется возможность загрузки параметров пакета из файла. Для глобального диспетчера заданий возможна установка и динамическое изменение дисциплины планирования, установка пакетного или потокового режима функционирования, настройка чувствительности при формировании адаптационной

стратегії диспетчеризації, получение данных о количестве заданий (распределенных по узлам, ожидающих планирования или находящихся в очереди на планирование), скорости рассасывания очереди заданий глобального диспетчера и т.д.

Проведенный вычислительный эксперимент процесса автоматизации управления РВП продемонстрировал эффективность предлагаемого подхода. Моделирование обработки пакета, содержащего 100 разнотипных заданий, проводилось для гомогенной РВС, состоящей из 10 узлов, имеющих следующую конфигурацию, представленную в таблице 1. Фрагмент пакета заданий приведен на рисунке 1.

Таблица 1 – Конфигурация вычислительных узлов моделируемой системы

Имя узла	HDD	RAM	Кол-во CPU	Произв. MIPS	Активен?
Узел 1	80	50	2	3500	Да
Узел 2	50	70	1	3000	Да
Узел 3	120	350	2	4000	Да
Узел 4	170	200	2	3000	Да
Узел 5	90	170	2	2000	Да
Узел 6	200	350	2	4500	Да
Узел 7	110	60	2	2000	Да
Узел 8	95	180	1	3200	Да
Узел 9	130	65	2	3300	Да
Узел 10	150	350	2	4000	Да

```

JobID = 10 HDD = 27 RAM = 75 TaskSizeMIPS = 25266 CPU_Req = 1 DataSize = 36
JobID = 11 HDD = 24 RAM = 101 TaskSizeMIPS = 29567 CPU_Req = 1 DataSize = 15
JobID = 13 HDD = 29 RAM = 31 TaskSizeMIPS = 27588 CPU_Req = 1 DataSize = 20
JobID = 14 HDD = 18 RAM = 71 TaskSizeMIPS = 23970 CPU_Req = 1 DataSize = 21
JobID = 15 HDD = 35 RAM = 77 TaskSizeMIPS = 19745 CPU_Req = 1 DataSize = 47
JobID = 16 HDD = 28 RAM = 48 TaskSizeMIPS = 19317 CPU_Req = 1 DataSize = 31
JobID = 17 HDD = 39 RAM = 53 TaskSizeMIPS = 22826 CPU_Req = 1 DataSize = 17
JobID = 18 HDD = 28 RAM = 94 TaskSizeMIPS = 26277 CPU_Req = 1 DataSize = 32
JobID = 19 HDD = 11 RAM = 46 TaskSizeMIPS = 21003 CPU_Req = 1 DataSize = 17
JobID = 20 HDD = 27 RAM = 108 TaskSizeMIPS = 21219 CPU_Req = 1 DataSize = 12
JobID = 21 HDD = 10 RAM = 89 TaskSizeMIPS = 23127 CPU_Req = 1 DataSize = 40
JobID = 22 HDD = 10 RAM = 54 TaskSizeMIPS = 25452 CPU_Req = 1 DataSize = 17
JobID = 23 HDD = 37 RAM = 85 TaskSizeMIPS = 19407 CPU_Req = 1 DataSize = 34
    
```

Рисунок 1 – Фрагмент пакета заданий моделируемой системы

Результат эксперимента: время обработки всего пакета заданий методом First-Fit – 361 с., Backfill – 322 с., предлагаемый в [3] подход – 256 с. Таким образом, имеем прирост производительности: 29% в сравнении с First-Fit и 23% для Backfill.

Список литературы

1. Богданов Н.К. Автоматизация технологических процессов в распределенных системах диспетчерского управления на предприятиях : автореферат дис. ... канд. техн. наук : спец. 05.13.06/ Н.К. Богданов. — Москва, 2004. — 19 с.
2. Карпов Ю.Г. Имитационное моделирование систем. Введение в моделирование с AnyLogic 5 / Ю.Г. Карпов. — СПб.: БХВ-Петербург, 2005. — 400 с.
3. Информационные технологии для критических инфраструктур: монография / А.В. Скотков [и др.] — Севастополь: Изд-во «СевНТУ», 2012. — 306 с.

УДК 004.4

К.О. Буравченко

Науковий керівник – Сидоренко В.В., д-р техн. наук, професор
Кіровоградський національний технічний університет

Автоматизована інформаційна система керування водопостачанням об’єкта

Якісне водопостачання одне з основних завдань у сучасному господарстві, промисловості. Проблема питної води постає у 21 ст. досить різко. По даним Всесвітньої організації Юнеско приблизно 60 відсотків населення світу недоотримують якісну питну воду. Вода використовуються не тільки у легкій промисловості, також у важкій промисловості, хімічній галузі. Кругообіг води існує не тільки природний, але і технічний.

Для очищення та передачі води проектується складні системи з використанням сучасних технологій. Якість, структура, температура та багато інших параметрів води контролюються численною кількістю датчиків. На очисних підприємствах проводяться хімічні та біологічні аналізи. Проводиться фільтрація, деаерація, дезінфекція та інші.

Для передачі води від джерела до споживача будуються системи водопостачання. В досить складних системах використовують автоматизовані інформаційні системи керування. Ці системи дозволяють контролювати параметри системи водопостачання у реальному часі, проводити аналіз витрат електричної енергії, визначати об’єм переданої води у трубопроводі, тиск у трубах та інше. Завдяки таким системам стає можливим керувати великими об’єктами водопостачання такими як села, містечка, міста та навіть області, країни.

Система водопостачання складається з блоків: насосні станції, система трубопроводів, датчики, резервуари чистої води.

Насосна станція може містити в собі станцію автоматичного керування (САУ), яка регулює та контролює її параметри. САУ виконує містить в собі регулятор. Існує декілька найпоширеніших методів регулювання параметрів насосної станції. Це регулювання тиску у трубопроводі, або регулювання по рівням у резервуарі. Сьогодні поширена система керування насосом на основі використання методу частотного регулювання. Тим чи іншим способом параметри насосної станції змінюють за рахунок зміни частоти обертів двигуна насосу. Це можуть буди як тиристорні перетворювачі частоти, або перетворювачі частоти з використанням інверторів на основі транзисторів. Багато теоретичних досліджень проводиться для того щоб знайти оптимальний алгоритм регулювання двигуном насоса зберігаючи його ефективність.

Автоматизована інформаційна система керування водопостачання складається з вузлів, з яких знімається інформація, блоку обробки та перетворення даних, та клієнтів, які отримують оброблені дані. Передача інформації виконується в обох напрямках, тобто клієнти можуть отримувати дані про стан системи, а також змінювати його.

Центральний операторський пункт є клієнтом системи. Клієнт отримує інформацію від сервера. Передача інформації можлива як в локальній мережі, так і в глобальній (інтернет). Для збереження тасмниці при передачі інформація шифрується сервером та дешифрується клієнтом. Клієнт, який має достатній рівень доступу, має можливість змінювати стан системи. Приклад: зміна стану насосної станції.

Для доступу до інформації у будь-який час в автоматизовану інформаційну систему водопостачання включають сховище інформації. Це сховище може бути

розміщено на локальному або на глобальному сервері або на обох. Інформації зберігається у зашифрованому вигляді. Формат даних у сховищі – довільний. Це може бути як простий html, так і файл бази даних.

Збір інформації у системі на програмному рівні виконується за рахунок OPC серверів. Технологія OPC підтримується переважною більшістю виробників вузлів промислової автоматизації. OPC сервери мають велику кількість функцій для отримання якісної інформації про стан системи. Існують як універсальні OPC сервери, так і спеціалізовані. Інформаційна система підключається к OPC серверам для отримання інформації і передає їх до сховища даних. За допомогою OPC від розробника такої системи не вимагається розробка протоколів та алгоритмів передачі даних.

В доповіді розглянуто структуру автоматизованої інформаційної системи водопостачання об'єкта. А також програмну модель такої систем і особливості її використання.

Список літератури

1. Втюрин В.А. Автоматизированные системы управления технологическими процессами. Основы АСУТП / Втюрин В.А., - Санкт-Петербург : СГЛА им. С.М. Кирова, 2006. – 639 с.
2. Ливанов Ю.В. Диспетчеризация производственных процессов в газовой и нефтяной промышленности / Ливанов Ю. В., Карась Л. Ю., - Москва : Недра, 1980. – 139 с.
3. Федоренко Д.Ю. Программирование клиентов OPC на С++ и С#. Часть 1. OPC DA / Федоренко Д.Ю., - Москва : OPC, 2003. – 20 с.

УДК 004.45

Є.А. Гостіщев

Науковий керівник – Мелешко С.В., канд. техн. наук, доцент
Кіровоградський національний технічний університет

Розробка програмного забезпечення макромови для керування робототехнічним комплексом і спряження з контролером керування

Ринок комп'ютерного “заліза” стрімко розвивається і ті потужності, які раніше можливо було розмістити лише стаціонарно, зараз вміщуються на плату розмірами 10x7 см, яка важить кілька десятків грамів і споживає при цьому настільки мало електроенергії, що її можна живити від батарей. Це дає змогу створювати рухомі комплекси на базі всім звичних платформ: Linux або Windows CE.

Прикладом такого міні-комп'ютера є mmnet від Польської фірми Prorox на базі ARM9 з тактовою частотою 400MHz, 64 Мб ОЗП та двома портами USB, до яких можна підключити модуль Wi-Fi та веб-камеру. Так як тут використовуються “великі” операційні системи, то можна без проблем налаштувати будь-яке обладнання, але тут є один нюанс – необхідно використовувати заздалегідь скомпільовані програмні пакети або програмні коди для їх подальшої компіляції вже безпосередньо під процесор на архітектурі ARM9.

Такі мікропроцесорні системи можуть бути гарною базою для створення рухомих робототехнічних комплексів для застосування у різних цивільних та військових цілях.

У даній роботі пропонується до mmnet1002 додати шасі, підключити веб-камеру

та wi-fi адаптер і на прикладі цієї системи розробити універсальний інтерфейс керування будь-яким робототехнічним комплексом, для кожного нового робототехнічного комплексу потрібно буде тільки написати драйвер або скористатись універсальним. Список задач також може динамічно змінюватись шляхом додавання/вилучення сенсорів безпосередньо із робототехнічної системи та забіндування команд на клавіші інтерфейсу керування роботом.

Метою роботи є розробка програмного забезпечення макромови для керування робототехнічним комплексом і спряження з контролером керування.

Об'єктом дослідження є процес керування робототехнічним комплексом.

Предметом дослідження є методи та алгоритми дистанційного керування і передачі інформації з відеопристрою роторототехнічної системи за допомогою бездротових мереж.

Методи дослідження базуються на теорії алгоритмів, теорії зв'язку й теорії телеграфіку, використанні булевої алгебри та чисельних методів.

Практична значимість роботи визначається тим, що створення і розробка даного програмного забезпечення сприятиме процесу безпечного для життя і здоров'я людини збору необхідної інформації в екстремальних умовах та небезпечних середовищах за допомогою дистанційно керованих робототехнічних комплексів, а також для спрощення та захисту життя навіть у повсякденному побуті.

Список літератури

1. Смірнов О.А., Мелешко С.В., Семенов С.Г. Методи та засоби обробки сигналів і даних в інформаційних системах. Навчальний посібник. – Кіровоград: Вид. КНТУ, 2012.
2. Інструкція користувача mmnet1002: http://www.propox.com/download/docs/MMnet1002_en.pdf.

УДК 004.738.5

В.А. Погонів

Науковий керівник – Смірнов В.В., канд. техн. наук, доцент
Кіровоградський національний технічний університет

Сучасні напрямки використання мікроконтролерів та процесорів архітектури ARM

Зараз сімейство ARM займає приблизно 75% всіх портативних 32-бітних RISC процесорів, що робить її найбільш використовуваною серед всіх 32-бітних архітектур. Основою такої популярності слугувала енергоефективність цих процесорів, особливо в порівнянні з процесорами для ПК. Саме тому вони використовуються в приладах, де це важливо – КПК, планшети, плеєри, телефони, маршрутизатори. Усім відомим прикладом можуть слугувати телефони Nokia, портативні пристрої Apple. Водночас з цим менш продуктивні ARM процесори, наряду з готовими рішеннями Arduino, набувають популярності серед ентузіастів як платформи для розробки власних пристроїв. Вони об'єднують доступність, легкість вивчення і сучасні можливості процесорів. Прикладом такого рішення є плата STM32vIDiscovery, яка має все для початку роботи з ARM. Вона суміщує програматор і мікроконтролер, що достатньо для початку розробки. Низький «поріг входження» дозволяє почати знайомство з платформою практично будь-якому програмісту. Окрім готових інтерфейсів присутня і пряма робота з виводами процесора, що дозволяє реалізувати власні драйвери для

роботи практично з будь-якими пристроями – такими, як дисплеї, різноманітні датчики, клавіатури.

Список літератури

1. П.П. Редькин 32-16 битные микроконтроллеры ARM7 семейства AT91SAM7 фирмы Atmel. – М.: «Додека-XXI», 2008. – 704 с.
2. J.P. Lynch ARM cross development with Eclipse, 2005. – 164 с.
3. Болл Стюарт Р. Аналоговые интерфейсы микроконтроллеров. – М.: «Додека-XXI», 2007. – 360 с.
4. Л.Н. Преснухин Архитектура и проектирование Микро-ЭВМ. Организация вычислительных процессоров. – М.: Высш. шк., 1986. – 495 с.
5. Б.А. Баев Микропроцессоры бытовой техники. – М.: Горячая линия - Телеком, 2005. – 480 с.

УДК 004.45

А.О. Тарасенко

Науковий керівник – Приходькіна А.І., ст. викладач
Кіровоградський національний технічний університет

Програмне забезпечення системи побудови зображення TV-тюнера цифрового телебачення стандарту DVB-T2

В останній час на території України поширився стандарт віщання T2. DVB-T2 (Digital Video Broadcasting - Second Generation Terrestrial) це друге покоління стандарту DVB-T, європейського стандарту ефірного цифрового мовлення.

Стандарт DVB-T2 покликаний як мінімум на 30% покращити ємність мереж у порівнянні з DVB-T, при тій же інфраструктурі мережі і частотних ресурсах. DVB-T2 принципово відрізняється як архітектурою системного рівня (MAC-рівня), так і особливостями фізичного рівня.

У DVB-T2 використовується OFDM модуляція з великою кількістю піднесучих, що забезпечує стійкий сигнал. Подібно DVB-T, DVB-T2 передбачає велику кількість різних режимів, це робить DVB-T2 дуже гнучким стандартом. Для виконання корекції помилок в DVB-T2 застосовується таке ж кодування, яке було вибрано для DVB-S2.

Поєднання кодування з низькою щільністю перевірок на парність (LDPC) і кодування Боуза-Чоудхурі-Хоквінгема (BCH) забезпечує дуже стійкий сигнал і чудову якість в умовах з високим рівнем шумів і перешкод.

Цифрове ТБ в Україні. Проаналізуємо тенденцію розвитку стандарту.

24 червня 2010 року на території України в м. Одесі проведено тестовий сеанс мовлення в стандарті DVB-T2.

З середини вересня поступово по всій країні запускається мовлення пакету з 32 каналами компанії "Зеонбуд".

Лютий 2012 сигнал DVB-T2 кодується по всій території України.

Березень 2012 року початок масової реалізації для населення України ресиверів-приставок STRONG SRT 8500 та Trimax tr-2012HD для забезпечення можливості прийому цифрового ефірного телебачення.

Є новий тип телебачення, нове обладнання але немає якісного програмного забезпечення для його використання, зокрема використання внутрішніх карт під стаціонарні ПК.

Таким чином, виходячи з вищеперахованого, розробка програмного забезпечення системи побудови зображення TV-тюнера цифрового телебачення стандарту DVB-T2 є актуальною задачею.

Основне призначення системи – перегляд програм на ПК у цифровому стандарті телебачення DVB-T2 за допомогою комп'ютерної плати TBS6280 PCI-E DVB-T2/T Dual Tuner Card.

Основне застосування системи – перегляд телепрограм користувачами та захвату відео зображення через комп'ютерні плати типу «TBS6280 PCI-E DVB-T2/T Dual Tuner Card».

УДК 004.4

Д.В. Усенко

Науковий керівник – Смірнов О.А., канд. техн. наук, доцент
Кіровоградський національний технічний університет

Розробка програмного забезпечення системи дистанційного голосового керування робототехнічним комплексом

У цей час у міру росту обсягів інформації комп'ютерна техніка усе більше й більше проникає в людське життя. Відбувається вдосконалювання інтерфейсу людина-комп'ютер. Винаходяться нові способи відображення інформації, модернізуються пристрої уведення, тривають пошуки такого інтерфейсу, що влаштував би всіх. На що роль зараз претендує мовний інтерфейс. Власне кажучи, це саме те, до чого людство завжди прагнуло в спілкуванні з комп'ютером.

Роботи в цьому напрямку велися ще в той час, коли про графічний інтерфейс ніхто навіть і не думав. За порівняно короткий період був вироблений вичерпний теоретичний базис, і практичні досягнення обумовлювали тільки продуктивністю комп'ютерної техніки. В 60-70х роках були створені пристрої, здатні розпізнавати десятком мовних команд.

Істотний внесок у розвиток систем розпізнавання мови (СРМ) внесли радянські й російські вчені В.Н. Трунін-Донської, Т.К. Винцюк, Н.Г. Загоруйко, Л.Л. М'ясников, закордонні вчені Д.Д. Маркел, А.Х. Грій, Б. Гоулд, Г. Фант і ін. Безліч сучасних ідей при створенні систем розпізнавання мови взято з області цифрової обробки сигналів. Великий внесок у теоретичному й практичному планах внесли А.А. Пирогов, А.А. Ланнэ, Л. Рабинер, Р. Боярин, Д. Макхоул і ін.

Сучасні розробки, як правило, ґрунтуються на біонічній моделі сприйняття мови людиною. Такі системи є ієрархічними, детермінованими, з навчанням і складаються з декількох взаємозалежних рівнів. Виділяються акустична (одержання первинних ознак мовних сигналів) і лінгвістична (робота зі словниками) складові.

Системи розпізнавання зливої мови будуються на базі імовірнісних моделей граматики мови. На словниках обсягом до 5000 слів вірогідність розпізнавання цілих фраз становить більше 95%, що вважається достатнім для забезпечення успішного мовного уведення тексту на ПК.

Для завдання голосового керування різними пристроями необхідно розпізнавання окремих мовних команд. Як правило, такий спосіб керування вимагає високої надійності (99% точності розпізнавання). Найчастіше команди вимовляються в умовах підвищеної зашумленості, наприклад на виробництві. Сучасні розробки в лабораторних умовах досягають 95% точності на словниках до 100 команд і вимагають навчальні вибірки більших обсягів (10 і більше варіантів проголошення кожного слова різними дикторами).

Таким чином, проблема побудови ефективних алгоритмів розпізнавання мовних команд є актуальною.

Мета роботи полягає у розробці програмного забезпечення, яке призначено для системи дистанційного голосового керування робототехнічним комплексом.

Для досягнення поставленої мети необхідно в ході виконання теоретичних і експериментальних досліджень вирішити наступні завдання:

1. Провести огляд моделей систем розпізнавання мови, проаналізувати структуру їхніх модулів, виявити основні недоліки.
2. Зробити обґрунтований вибір методу формування первинних ознак мовних сигналів.
3. Вибрати принцип побудови й роботи зі словниками еталонів.
4. Уточнити математичну модель системи розпізнавання мовних команд.
5. Розробити програмний комплекс для проведення досліджень і тестування моделі розпізнавання.
6. Здійснити перевірку запропонованих алгоритмів розпізнавання мовних команд на тестових вибірках, зробити порівняння з існуючими СРМ.

Об’єктом дослідження є процес голосового керування.

Предметом дослідження є системи дистанційного голосового керування робототехнічним комплексом.

Достовірність наукових результатів підтверджена теоретичними викладеннями, даними комп’ютерного моделювання, коректними дослідженнями параметрів на функціонуючій обчислювальній мережі, а також відповідністю отриманих результатів окремим результатам, наведеним у науковій літературі.

Список літератури

1. Потапова, Р.К. Речевое управление роботом / Р.К. Потапова. – М.: КомКнига, 2005. – 328 с.
2. Потапова, Р.К. Речь: коммуникация, информация, кибернетика / Р.К. Потапова //М.:Едиториал УРСС, 2003. – 568 с.
3. Рабинер, Л. СММ и их применение в избранных приложениях при распознавании речи / Л. Рабинер // ТИИЭР. 1989. – Т. 77. – №2. – С. 86-120.
4. Рабинер Л. Цифровая обработка речевых сигналов / Л. Рабинер, Р. Шафер. – М.: Радио и связь, 1987. – 264 с.
5. Распознавание слуховых образов. / Под ред. Н.Г. Загоруйко. – Новосибирск: «Наука», 1970.–340 с.
6. Ронжин А. Метод распознавания слитной речи на основе анализа сигнала в скользящем окне и теории размытых множеств / А. Ронжин и др. // Искусственный интеллект. – Выпуск 4. – 2002. – С. 256-263.

СУЧАСНІ ІТ-ТЕХНОЛОГІЇ ПІДГОТОВКИ ФАХІВЦІВ З ПРОГРАМУВАННЯ

УДК 004.2

І.С. Бондаренко

Науковий керівник – Помазан Л.В., канд. техн. наук, доцент
Кіровоградський національний технічний університет

Програмна модель роботи підсистеми Win API 32 ОС Windows

Дослідження ринку ПЕОМ показало, що на даних час ліву частку ринку займають ПЕОМ побудовані на архітектурі 32-х розрядних мікропроцесорів. Відповідно, на сучасному рівні існує потреба в кваліфікованих спеціалістах по розробці програм під архітектуру 32-х розрядних мікропроцесорів. Але для того, щоб програмувати під цю архітектуру, потрібно добре знати складові ПК, зв’язки та взаємодію між ними тобто підсистему сповіщень Win API 32/64. Останні декілька десятиріч бурхливо розвивається область інформаційних технологій. Але усі ці технології не можливі без використання персональних електронно-обчислювальних машин (ПЕОМ). В процесі навчання спеціалістів виникають потреби в навчальних засобах. Це різноманітні програми, мови програмування, навчальні стенди тощо. Однак, не всі з перерахованих вище потреб, може забезпечити сучасний комп’ютерний ринок. Отже, виникає потреба в створенні принципово нових навчальних засобів.

Створення програмної моделі має велике значення, як для навчального процесу, так і для створення складних систем, оскільки будь-яка потужна система базується саме на операціях низького рівня і розуміння цього процесу значно полегшує роботу зі складними системами, дії яких замасковані від користувача. В процесі роботи над програмною моделлю необхідно виконати аналіз існуючих апаратних та програмних засобів. Також необхідно в повній мірі описати всі компоненти персонального комп’ютера, реалізувати основні зв’язуючі елементи та контролери пристроїв. Окрім цього, програмна модель повинна включати в себе підрозділи глосарію, документації, посилання на виробників материнських плат та приклади організації портів введення-виведення.

Таким чином, виходячи з вищеперерахованого, розробка програмної моделі роботи підсистеми Win API 32 ОС Windows, є актуальною задачею.

Призначення системи – вивчення користувачем основ роботи підсистеми Win API 32.

Область застосування – студенти вищих навчальних закладів чи інші особи яким необхідно вивчити зазначену проблематику.

УДК 004.432.2

Н.М. Мартыненко

Научный руководитель – Малыхина Т.В., старший преподаватель
Харьковский национальный университет имени В.Н. Каразина

Онлайн-экзамен оценки знаний по курсу: «Язык программирования JavaScript»

Интернет на данный момент является одним из наиболее распространенных и доступных источников информации. Он стал неотъемлемой частью жизни современного человека и основных сфер его деятельности. Интернет по сути можно рассматривать с трёх основных сторон: во-первых, как средство коммуникации, общения и построения взаимоотношений отношений между людьми, которые могут находиться даже в другом конце света; во-вторых, как огромная библиотека, содержащая знания, и инновационные, только что полученные учеными в лабораториях, и древние знания, накопленные в течении тысячелетий, и что очень важно, в большинстве своём доступные практически каждому; в-третьих, это перспективная и уже сейчас активно используемая площадка для развития бизнеса. Исходя из этого, трудно переоценить роль специалистов, которые работают в столь значимой отрасли как Интернет. И, следовательно, не стоит недооценивать роль образования в их подготовке.

Целью моей работы является создание онлайн-экзамена по курсу языка JavaScript.

На данный момент в Интернете существует множество сайтов, на которых содержится информация по данному курсу и, соответственно, некие экзамены, с помощью которых пользователь может оценить уровень полученных знаний. Например, такие как intuit.ru или javascript.ru. Кстати, на данный момент в нашем университете используется локальная версия курса, который приведен на сайте intuit.ru.

Основными особенностями и задачами моего проекта являются:

- согласованность с программой, утвержденной Министерством образования и науки, молодежи и спорта Украины, для того чтобы тест можно было бы полноценно использовать при оценивании знаний студентов;

- подбор вопросов с учетом актуальных в данной области тенденций и требований, выдвигаемых при приеме на работу;

- направленность на оценку базовых знаний необходимых в данной области

- мультиязычность (английский, русский, украинский) и «адаптированность» терминологии, принятой в каждом из этих языков;

- частично неформальный подход в формулировке вопросов и пояснений к ним, так как, с моей точки зрения, это вполне соответствует идеологии веб-программирования. Ярким примером такого похода является тест, приведенный на сайте en.pudn.com [1];

- дополнительные требования, выдвигаемые к системе безопасности для снижения вероятности жульничества. В этом плане точки зрения структуры проект

базирується на принципах, приведенных в справочнике Дж. Бранденбау «JavaScript: Сборник готовых рецептов» [2].

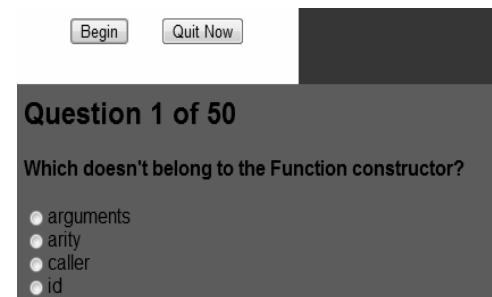


Рисунок 1 – Английская версия теста. Вопросы

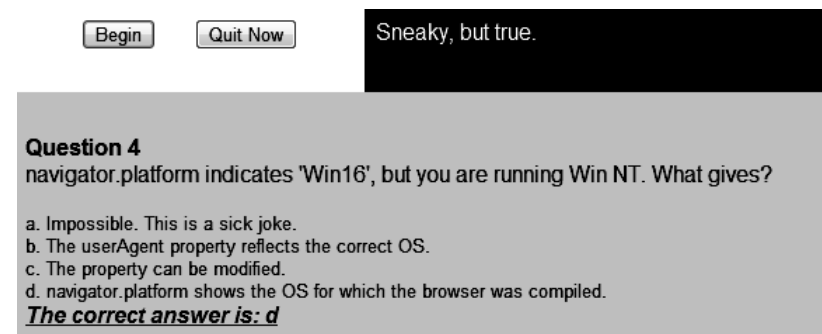


Рисунок 2 – Английская версия теста. Результаты оценивания с пояснениями

В заключение мне хотелось бы добавить, что, с моей точки зрения, качественное тестирование должно не только помогать определить уровень знаний студента, но и стимулировать его к совершенствованию своих знаний и умений, так как анализ ошибок и усердие в повышении своих навыков и есть одни из главных качеств специалиста. По словам Конфуция: «Три пути ведут к знанию: путь размышления - это путь самый благородный, путь подражания - это путь самый легкий и путь опыта - это путь самый горький». И, с моей точки зрения, хотя необходимо использовать все возможные подходы, последний для программиста и является наиболее продуктивным.

Список литературы

1. Programmers united develop net [Электронный ресурс] // Режим доступа: http://read.pudn.com/downloads88/doc/338270/Javascript/Sample/jac/JSAppCookBook/ch02/questions.js_.htm
2. Бранденбау, Дж. JavaScript: Сборник рецептов для профессионалов /Дж. Бранденбау. — СПб.: Питер, 2000. – С. 55-79.

С.М. Гнезділов

Науковий керівник –Добренький О.П., викладач
Кіровоградський національний технічний університет

Дослідження ефективності впровадження у навчальний процес емуляторів пристроїв і систем

Впровадження інформаційних освітніх технологій у навчальних закладах України є одним з головних чинників у підготовці високоякісного фахівця [1]. Найбільш характерною ознакою освіти на сучасному етапі розвитку є її інформатизація, обумовлена насамперед розповсюдженням у навчальних закладах сучасної комп'ютерної техніки та програмного забезпечення, використанням можливостей Інтернет, набуттям і накопиченням фахівцями досвіду використання інформаційних технологій (ІТ) у своїй діяльності [2]. Тому формування знань і навичок застосування різних ІТ-інструментів є важливим аспектом у процесі підготовки майбутнього фахівця. Крім того, застосування новітніх технологій у навчальному процесі викликає неабиякий інтерес у молодого покоління. А від нього належить особлива роль у свідомому та активному засвоєнні знань. У той же час завданням викладача є формування, в тому числі й за допомогою програмно-апаратних засобів, стійкого інтересу до навчальної дисципліни і навчання в цілому.

Дослідження [3-9] показало, що на сьогоднішній день застосування програмних моделей (емуляторів) пристроїв, мікросхем, систем та процесів є перспективним, економічно вигідним та ефективним для організації якісного навчального процесу. Вони також є особливо важливими для створення гнучкої лабораторної бази з врахуванням стрімкого розвитку обчислювальної техніки. У системі вищої освіти вже використовуються апаратні емулятори пристроїв і процесів, навчальні стенди [11], які забезпечують можливість організації якісного навчального процесу.

Метою науково-дослідної роботи є аналіз апаратних та програмних емуляторів пристроїв і процесів комп'ютерної техніки, розробка пропозицій щодо перспектив їх розробки та застосування з погляду економічних, психологічних, педагогічних показників, тобто ефективності впровадження у навчальний процес ВНЗ.

Дослідження [3, 5-7] показали, що на сьогоднішній день у вітчизняній системі освіти використовуються апаратні емулятори (стенди) та програмні імітаційні моделі, призначені для вивчення обчислювальної техніки, її складових й процесів, які в ній протікають.

Досліджені програмні емулятори [3-7] дозволяють візуалізувати процес програмування мікросхем у спрощеному вигляді, а також процеси системи. Так, наприклад, програма-емулятор інтервального таймера i8253 [6] дозволяє візуалізувати процес програмування та функціонування цієї мікросхеми. Реалізація емулятора повністю відповідає внутрішній будові та принципам функціонування реальної схеми та системи [10]. Програмні моделі демонструють функціональні взаємозв'язки і взаємодію вказаного пристрою, відображають результати його програмування, а також дозволяють спостерігати користувачу за всіма функціями та внутрішніми процесами.

Робота програмного забезпечення моделей дозволяє також здійснювати спостереження за процесом у необхідному масштабі часу, реалізовано покроковий режим роботи, що наочно відображає принцип функціонування пристрою та стане невід'ємним засобом для кращого розуміння і вивчення відповідної теми навчальної

дисципліни. Крім того, програми-емулятори дають можливість провести дослідження та проаналізувати відповідні системи або пристрої [3].

Демонстраційний експеримент не вичерпує всіх можливостей активного сприйняття студентами досліджуваних явищ, не завжди забезпечує отримання ними дійових знань, оскільки його тільки спостерігають, а не проводять самі. А тому демонстрації із залученням програм-емуляторів потрібно доповнювати виконанням студентами лабораторних робіт з їх допомогою. Програмний емулятор дозволяє проводити відповідну роботу і самостійно (позааудиторно), без залучення викладача. Це дозволяє розширити область зв'язку теорії з практикою, привчити студентів до самостійної дослідницької роботи. Крім того, можливість проводити досліді віддалено від ВНЗ вказує на перспективу використання емуляторів для дистанційного навчання.

Програмні моделі загалом дають можливість організувати якісний навчальний процес підготовки фахівців з обчислювальної техніки та комп'ютерних систем. На рисунку 1 наведено програмний емулятор [3].

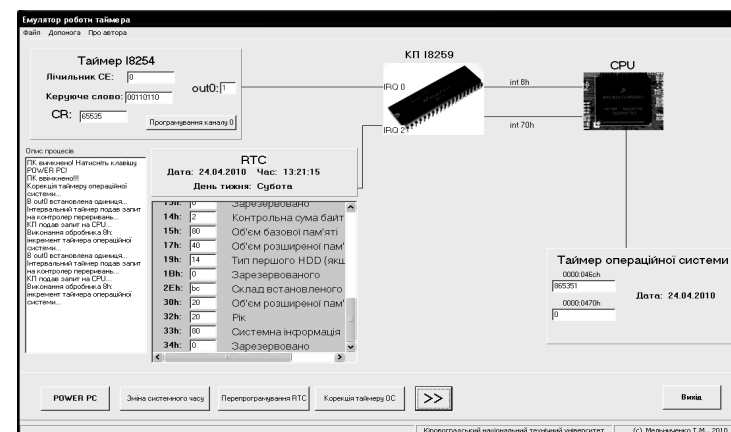


Рисунок 1 – Емулятор організації системного часу ПК IBM PC

У ВНЗ також використовуються апаратні емулятори (стенди), які призначені для вивчення проектування та обслуговування ЕОМ, побудованих на реальних процесорах та мікроконтролерах. Наприклад, навчально-мікропроцесорний комплект (НМК) мікросхеми i8253, наведений на рисунку 2, є розробкою кафедри програмного забезпечення Кіровоградського національного технічного університету. Він представляє собою мікро-ЕОМ, призначений для вивчення мікросхеми KP580ИК83А, дозволяє візуалізувати процес програмування мікропроцесорної ВІС, а також емулювати процес її функціонування.

Стенд дозволяє за допомогою ПК та програмного емулятора програмувати мікросхему. Основні регістри та їх стани ідентифікуються відповідними світлодіодами, що дозволяє виводити користувачеві дані, які в даний момент містяться у регістрах мікросхеми. Крім того, НМК візуалізує внутрішню роботу мікросхеми після її програмування, а також процеси, які в ній протікають.

Проте слід зазначити, що переваги програм-емуляторів у порівнянні з апаратними стендами очевидні та суттєві. Досліді з використанням програм-емуляторів зводять до мінімуму час на їх підготовку, демонстрація проводиться оперативно, без необхідності технічного налаштування та обслуговування. Крім того,

копіювання програмного забезпечення дозволяє забезпечити не тільки аудиторне навчання, але й самостійне чи дистанційне. Цих можливостей не надають апаратно-технічні емулятори. Вони, на відміну від програмних, є економічно невідгідними, призначені тільки для аудиторного застосування в приміщенні ВНЗ, вимагають спеціального обслуговування, амортизуються, можуть вийти з ладу тощо.



Рисунок 2 – Апаратний емулятор (стенд) мікросхеми інтервального таймера

Виходячи з викладених результатів досліджень, беручи до уваги рівень сучасного розвитку інформаційних технологій, можна зробити висновок, що розробка та застосування програм-емуляторів у навчальних закладах є перспективним, ефективним та економічно вигідним. Програми-емулятори є потужним інструментом реалізації якісного

навчального процесу підготовки фахівців, який, разом з тим, вже доводить свою результативність. Переваги програмних емуляторів над апаратними (стендами) суттєві: вони практичні, економічно вигідні, не потребують обладнання спеціального місця та додаткового устаткування, а також дають можливість організації дистанційного навчання шляхом розміщення їх в мережі Internet тощо. Таким чином, можна стверджувати про доцільність розвитку і використання саме програмних емуляторів, а не їх апаратно-технічних аналогів.

Список літератури

- Захарова І. Г. Інформаційні технології в освіті: Навчальний посібник. – К.: “Академія”, 2003.–192 с.
- Дима Я.Ю. Емулятори вимірвальних приладів як інструмент ІКТ для реалізації міжпредметних зв’язків фізики та математики. / Я.Ю. Дима, І.В. Лапенко, О.В. Сасенко. // Збірник наукових праць Бердянського державного педагогічного університету. – 2011. – № 3. – С. 77-83.
- Мельниченко Т.М. Програмний емулятор системного та реального часу на платі IBM PC в навчальному процесі підготовки спеціальних програмістів. // Матеріали III Міжнародної науково-технічної конференції “Комп’ютерні системи та мережні технології” (CSNT-2010).–К.:НАУ,2010.– С. 73.
- Завгородній О.К. Програмне забезпечення візуалізації процесу роботи і системного програмування передачі даних через USB. // Збірник тез доповідей XLIII наукової конференції студентів і магістрантів Кіровоградського нац. техн. ун-ту. – Кіровоград: РВЛ КНТУ, 2009. – С. 65
- Сидоренко В.В. Використання програмних емуляторів пристроїв обчислювальної техніки в навчальному процесі. / В.В. Сидоренко, О.В. Коваленко, О.П. Дорєнський. // Матеріали III МНТК “Комп’ютерні системи та мережні технології” (CSNT-2010). – К.: НАУ, 2010. – С. 89.
- Валова К.М. Програма-емулятор системного таймера. // Збірник тез доповідей ХLI наукової конф. студентів і магістрантів Кіровоградського нац. техн. ун-ту. – Кіровоград: РВЛ КНТУ, 2007. – С. 65.
- Гуртовий Є.О. Програма-емулятор годинника реального часу (RTC) на платі IBM PC. // Збірник тез доповідей ХL наукової конференції студентів і магістрантів Кіровоградського національного технічного університету. – Кіровоград: РВЛ КНТУ, 2006. – С. 66.
- Коржова К.М. Психолого-педагогічні аспекти навчання архітектури еом майбутніх інженерів-педагогів засобами комп’ютерного імітаційного моделювання. / К.М. Коржова, В.Г. Хоменко. [Електронний ресурс] – Бердянський держ. пед. ун-т, <http://vuzlib.com/content/view/415/84/>
- Дима Я.Ю. Методичні аспекти використання програм-емуляторів вимірвальних приладів у демонстраційному експерименті. / Я.Ю. Дима, О.В. Сасенко. // Впровадження електронного навчання в освітній процес: концепції, проблеми, рішення : Матеріали Міжнар. інтернет-конференції (21–22 жовтня 2010 р.) [Електронний ресурс]. – <http://conf.fizmat.tnpu.edu.ua/?p=158>.
- Гуржий А.М. Архітектура, принципи функціонування та керування ресурсами IBM PC: Навчальний посібник. / А.М. Гуржий, С.Ф. Коряк, В.В. Самсонов, О.Я. Склярів.–Х.:“Компанія СМІТ”,2003.–511 с.
- Папінов В.М. Рациональні способи моделювання елементів і систем управління в навчальних комп’ютеризованих лабораторних стендах. / В.М. Папінов, О.М. Бевз. // Сучасні тенденції розвитку інформаційних технологій в науці, освіті та економіці : матеріали V Всеукр. науково-практичної конф. : в 2-х т. (Луганськ, 7–9 квітня 2011 р.). – Луганськ : Phoenix, 2011. – Том 1. – С. 120-123.

Організаційний комітет конференції

Голова

Кропівний В.М., канд. техн. наук, професор, проректор з наукової роботи Кіровоградського національного технічного університету;

Заступник голови

Сидоренко В.В., д-р техн. наук, професор, завідувач кафедри програмного забезпечення Кіровоградського національного технічного університету;

Відповідальний секретар

Дорєнський О.П., науковий керівник Студентського наукового товариства Кіровоградського національного технічного університету, викладач кафедри програмного забезпечення Кіровоградського національного технічного університету.

Члени оргкомітету

Гришак В.З., д-р техн. наук, професор, академік АН Вищої школи України, проректор з наукової роботи Запорізького національного університету;

Остапов С.Е., д-р фіз.-мат. наук, професор, завідувач кафедри програмного забезпечення комп’ютерних систем Чернівецького національного університету імені Юрія Федьковича;

Кузнєцов О.О., д-р техн. наук, професор кафедри безпеки інформаційних технологій Харківського національного університету радіоелектроніки;

Задорожний З.-М.В., д-р екон. наук, професор, проректор з наукової роботи Тернопільського національного економічного університету;

Стервостов М.Г., канд. техн. наук, доцент, заступник декана з наукової роботи факультету комп’ютерних наук Харківського національного університету імені В.Н. Каразіна;

Окіпний І.Б., канд. техн. наук, доцент, голова Студентського наукового товариства Тернопільського національного технічного університету імені Івана Пулюя;

Євсєєв С.П., канд. техн. наук, старший науковий співробітник кафедри інформаційних систем Харківського національного економічного університету;

Ковтун В.Ю., канд. техн. наук, доцент кафедри безпеки інформаційних технологій Національного авіаційного університету;

Семенов С.Г., канд. техн. наук, доцент кафедри обчислювальної техніки та програмування Національного технічного університету “Харківський політехнічний інститут”;

Смірнов О.А., канд. техн. наук, професор кафедри програмного забезпечення Кіровоградського національного технічного університету;

Кавун С.В., канд. техн. наук, доцент кафедри комп’ютерних систем і технологій Харківського національного економічного університету;

Якименко Н.М., канд. фіз.-мат. наук, доцент кафедри програмного забезпечення Кіровоградського національного технічного університету;

Осадчий В.І., регіональний представник корпорації “Microsoft”;

Загорський Р.М., провідний інженер-програміст відділу розробки програмного забезпечення мобільних систем Інтернет-компанії “Онік”;

Коробко Ю.О., старший адміністратор “Інтернет-Сервіс-Провайдер “Шторм”;

Доляченко А.А., провідний інженер-програміст СРКП “Applejuice Studio”;

Даркіна В.О., голова Студентського наукового товариства Кіровоградського національного технічного університету;

Мяснянікіна К.А., голова Наукового товариства студентів та аспірантів Запорізького національного університету;

Фридель В.І., аспірант, заступник голови Наукового студентського товариства Київського національного економічного університету;

Коваль О.В., голова Студентського наукового товариства Тернопільського національного економічного університету;

Зімовін О.І., голова Правління Студентського наукового товариства Харківського національного університету імені В.Н. Каразіна;

Стратейчук Я.Р., голова Студентського наукового товариства Сумського національного аграрного університету;

Попова Я.С., студентський декан факультету комп’ютерних наук Харківського національного університету імені В.Н. Каразіна;

Ішуніна Н.М., керівник методично-організаційного відділу Кіровоградського національного технічного університету;

Кава Т.В., фахівець I категорії методично-організаційного відділу Кіровоградського національного технічного університету.

Учасники конференції

АЛІЦОВА <i>Ольга Анатоліївна</i>	Харківський національний університет будівництва та архітектури
БЕРЧІЯН <i>Давід Артурович</i>	Національний технічний університет “Харківський політехнічний університет”
БІГУН <i>Мар'яна Богданівна</i>	Івано-Франківський національний технічний університет нафти і газу
БЛИЗНЮК <i>Марина В'ячеславівна</i>	Український державний хіміко-технологічний університет
БОБРИШОВА <i>Руслана Олександрівна</i>	Кіровоградський національний технічний університет
БОГАТИРЕНКО <i>Анна Сергіївна</i>	Кіровоградський національний технічний університет
БОЙКО <i>Дмитро Ігоревич</i>	Севастопольський національний технічний університет
БОЛТОВА <i>Юлія Володимирівна</i>	Національний технічний університет “Харківський політехнічний університет”
БОНДАРЕНКО <i>Інна Сергіївна</i>	Кіровоградський національний технічний університет
БОНДАРЕНКО <i>Роман Анатолійовичу</i>	Кіровоградський національний технічний університет
БОНДАРЧУК <i>Андрій Петрович</i>	Державний університет інформаційно-комунікаційних технологій
БРУШНІЦЬКА <i>Анастасія Сергіївна</i>	Тернопільський національний економічний університет
БУБЕНКОВА <i>Варвара Сергіївна</i>	Національний авіаційний університет
БУРАВЧЕНКО <i>Костянтин Олегович</i>	Кіровоградський національний технічний університет
ВЕРХОВСЬКИЙ <i>Олександр Сергійович</i>	Кіровоградський національний технічний університет

ВЕТРОГОН <i>Олексій Михайлович</i>	Одеський національний політехнічний університет
ВЛАСЮК <i>Євгеній Романович</i>	Національний технічний університет України «Київський політехнічний інститут»
ВОВК <i>Оксана Володимирівна</i>	Харківський національний університет імені В.Н. Каразіна
ВОЙТИШЕН <i>Лілія Іванівна</i>	Державний університет інформаційно-комунікаційних технологій
ВОЛОХОВ <i>Євгеній Юрійович</i>	Кіровоградський національний технічний університет
ВРУБЛЕВСЬКИЙ <i>Дмитро Васильович</i>	Кіровоградський національний технічний університет
ГАЖУР <i>Дмитро Миколайович</i>	Харківський національний університет імені В.Н. Каразіна
ГАРАЖА <i>Віталій Олександрович</i>	Кіровоградський національний технічний університет
ГАРБУЗ <i>Ігор Євгенійович</i>	Кіровоградський національний технічний університет
ГЛАДИШЕВ <i>Дмитро Вікторович</i>	Кіровоградський національний технічний університет
ГНЕЗДЛОВ <i>Сергій Михайлович</i>	Кіровоградський національний технічний університет
ГОДЛА <i>Анастасія Сергіївна</i>	Донецький національний технічний університет
ГОЛОВАТЮК <i>Олександр Юрійович</i>	Кіровоградський національний технічний університет
ГОНЧАРОВА <i>Юлія Володимирівна</i>	Харківський національний університет імені В.Н. Каразіна
ГОСТИЩЕВ <i>Євгеній Анатолійович</i>	Кіровоградський національний технічний університет
ГУМЕНЮК <i>Сергій Сергійович</i>	Кіровоградський національний технічний університет
ГУСЄВ <i>Анатолій Сергійович</i>	Східноукраїнський національний університет імені В. Даля

ДАВИДОВ <i>Денис Олегович</i>	Кіровоградський національний технічний університет
ДЕМІШОНКОВА <i>Аліна Олександрівна</i>	Кіровоградський національний технічний університет
ДЕРКАЧ <i>Олексій Ігорович</i>	Державний університет інформаційно-комунікаційних технологій
ДЕРПОЛЮК <i>Станіслав Миколайович</i>	Кіровоградський національний технічний університет
ДЕСЯТНИК <i>Альона Володимирівна</i>	Кіровоградський національний технічний університет
ДЖЕБКО <i>Володимир Валерійович</i>	Кіровоградський національний технічний університет
ДЗЮБЕНКО <i>Євгеній Олександрович</i>	Кіровоградський національний технічний університет
ДОЛЖЕНКО <i>Антон Андрійович</i>	Кіровоградський національний технічний університет
ЄСІНА <i>Марина Віталіївна</i>	Харківський національний університет імені В.Н. Каразіна
ЖАК <i>Олена Сергіївна</i>	Кіровоградський національний технічний університет
АЗИМКО <i>Артем Валерійович</i>	Кіровоградський національний технічний університет
ЗАХАРЧУК <i>Наталія Вікторівна</i>	Національний авіаційний університет
ЗЕМЛЯНКО <i>Владислава Владиславівна</i>	Харківський національний університет імені В.Н. Каразіна
ЗІНОВ'ЄВ <i>Євген Анатолійович</i>	Кіровоградський національний технічний університет
ЗМЕУЛ <i>Олена Миколаївна</i>	Кіровоградський національний технічний університет
ЗУБЕНКО <i>Вікторія Володимирівна</i>	Кіровоградський національний технічний університет
ІВАНЧЕНКО <i>Олександр Олександрович</i>	Кіровоградський національний технічний університет

ІВАСИШИН <i>Тарас Михайлович</i>	Національна академія Служби безпеки України
ІГУМІН <i>Артем Анатолійович</i>	Харківський національний університет імені В.Н. Каразіна
ІЩЕНКО <i>Андрій Олександрович</i>	Кіровоградський національний технічний університет
КАСЯН <i>Олексій Валерійович</i>	Кіровоградський національний технічний університет
КАТРУХІН <i>Олександр Сергійович</i>	Кіровоградський національний технічний університет
КИСЛИЙ <i>Данііл Ігорович</i>	Запорізький національний університет
КІКОТЬ <i>Володимир Миколайович</i>	Кіровоградський національний технічний університет
КОВАЛЕНКО <i>Ігор Іванович</i>	Кіровоградський національний технічний університет
КОВАЛЬЧУК <i>Сергій Абдулжаббарович</i>	Кіровоградський національний технічний університет
КОЗЕКІН <i>Юрій Михайлович</i>	Національний технічний університет “Харківський політехнічний інститут”
КОМАНДИР <i>Антон Ярославович</i>	Харківський національний університет імені В. Н. Каразіна
КОСЕНКО <i>Олександра Олегівна</i>	Кіровоградський національний технічний університет
КОТЕНКО <i>Ольга Юрївна</i>	Харківський національний університет будівництва та архітектури
КРАВЧУК <i>Олександр Васильович</i>	Івано-Франківський національний технічний університет нафти і газу
КУДРІНА <i>Анастасія Геннадіївна</i>	Харківський національний університет імені В.Н. Каразіна
КУДРЯ <i>Марина Юрївна</i>	Кіровоградський національний технічний університет
КУЗЬМЕНКО <i>Михайло Володимирович</i>	Кіровоградський національний технічний університет

КУЛИК <i>Дмитро Іванович</i>	Запорізька державна інженерна академія
КУЧЕРЕНКО <i>Інна Сергіївна</i>	Кіровоградський національний технічний університет
КУЧЕРУК <i>Валентина Тимофіївна</i>	Запорізький національний університет
ЛАКТИОНОВ <i>Олександр Валерійович</i>	Кіровоградський національний технічний університет
ЛІСШИН <i>Василь Валерійович</i>	Олександрійський політехнічний коледж
МАЛАХОВСЬКИЙ <i>Віталій Юрійович</i>	Кіровоградський національний технічний університет
МАРТ <i>Богдан Анатолійович</i>	Національний технічний університет України “Київський політехнічний інститут”
МАРТИНЕНКО <i>Наталія Максимівна</i>	Харківський національний університет імені В.Н. Каразіна
МАРТИНЮК <i>Віктор Михайлович</i>	Національний авіаційний університет
МИНДРА <i>Микола Володимирович</i>	Кіровоградський національний технічний університет
МОГИЛЕВСЬКА <i>Наталія Юрівна</i>	Східноукраїнський національний університет імені В. Даля
МОЛДАВСЬКИЙ <i>Павло Семенович</i>	Кіровоградський національний технічний університет
МОЛЧАНОВ <i>Ігор Сергійович</i>	Кіровоградський національний технічний університет
МЯСНЯНкіНА <i>Ксенія Андріївна</i>	Запорізький національний університет
НАУМОВА <i>Вікторія Олександрівна</i>	Харківський національний університет імені В.Н. Каразіна
НЕДОЛУЖКО <i>Андрій Анатолійович</i>	Кіровоградський національний технічний університет
ОБЖЕНСЬКИЙ <i>Дмитро Анатолійович</i>	Кіровоградський національний технічний університет

ОРЕЛ <i>Андрій Володимирович</i>	Кіровоградський національний технічний університет
ОСАУЛЕНКО <i>Костянтин Іванович</i>	Кіровоградський національний технічний університет
ПАЇЦЬКИЙ <i>Сергій Володимирович</i>	Кіровоградський національний технічний університет
ПАНАСЮК <i>Олександр Миколайович</i>	Кіровоградський національний технічний університет
ПАХОМОВ <i>Олег Володимирович</i>	Кіровоградський національний технічний університет
ПЕЧЕНЮК <i>Сергій Валерійович</i>	Кіровоградський національний технічний університет
ПОГОНІЄВ <i>Валерій Андрійович</i>	Кіровоградський національний технічний університет
ПОКОТИЛО <i>Олексій Олександрович</i>	Національний технічний університет України “Київський політехнічний інститут”
ПОНОМАР <i>Олександр Олександрович</i>	Кіровоградський національний технічний університет
ПОПОВА <i>Яна Сергіївна</i>	Харківський національний університет імені В.Н. Каразіна
ПРАЧОВ <i>Андрій Олександрович</i>	Національний технічний університет України “Київський політехнічний інститут”
ПРОКОПОВ <i>Олександр Олегович</i>	Кіровоградський національний технічний університет
ПУЛЕКО <i>Костянтин Ігорович</i>	Національний авіаційний університет
ПШЕНИЧНИЙ <i>Іван Миколайович</i>	Кіровоградський національний технічний університет
РАЛО <i>Олександр Миколайович</i>	Харківський національний університет імені В.Н. Каразіна
САЛТАН <i>Віталій Сергійович</i>	Кіровоградський національний технічний університет
САЛЬНИКОВ <i>Максим Саргійович</i>	Державний університет інформаційно-комунікаційних технологій

СЕМЕНОВ <i>Федір Олександрович</i>	Кіровоградський національний технічний університет
СЕРБІН <i>Роман Сергійович</i>	Кіровоградський національний технічний університет
СКАКУН <i>Павло Павлович</i>	Кіровоградський технічний національний університет
СОРОКОЛАТ <i>Станіслав Дмитрович</i>	Кіровоградський національний технічний університет
СТАРИЦІН <i>Максим Володимирович</i>	Кіровоградський національний технічний університет
СТУПАК <i>Богдан Володимирович</i>	Національний технічний університет України “Київський політехнічний інститут”
СУВОРОВ <i>Олександр Олександрович</i>	Кіровоградський національний технічний університет
СУРІН <i>Віктор Вікторович</i>	Кіровоградський національний технічний університет
ТАГІЄВ <i>Артем В’ячеславович</i>	Кіровоградський національний технічний університет
ТАРАСЕНКО <i>Андрій Олександрович</i>	Кіровоградський національний технічний університет
ТАРАТАЙКО <i>Дар’я Валеріївна</i>	Національний авіаційний університет
ТИМОХІН <i>Сергій Сергійович</i>	Харківський національний університет імені В.Н. Каразіна
ТРОЦЬКИЙ <i>Сергій Олександрович</i>	Національний технічний університет України “Київський політехнічний інститут”
УСЕНКО <i>Дмитро Володимирович</i>	Кіровоградський національний технічний університет
УСКОВА <i>Альона Ігорівна</i>	Харківський національний університет імені В.Н. Каразіна
ХАМІДУЛЛІНА <i>Катерина Дмитрівна</i>	Донецький національний технічний університет
ХЕЙДЕР <i>Олександр Васильович</i>	Кіровоградський національний технічний університет

ХОТКЕВИЧ <i>Катерина Володимирівна</i>	Харківський національний університет імені В.Н. Каразіна
ЦИМБАЛ <i>Катерина Станіславівна</i>	Кіровоградський національний технічний університет
ЧЕРНЯВСЬКИЙ <i>Руслан Віталійович</i>	Кіровоградський національний технічний університет
ЧУЖИКОВА-ПРОСКУРНІНА <i>Ольга Дмитрівна</i>	Севастопольський національний університет ядерної енергії та промисловості
ШЕВКУН <i>Богдан Олександрович</i>	Кіровоградський національний технічний університет
ШЕВЧЕНКО <i>Денис Геннадійович</i>	Кіровоградський національний технічний університет
ШНУРЕНКО <i>Ігор Миколайович</i>	Харківський національний університет імені В.Н. Каразіна
ШПИНКОВСЬКА <i>Марія Іванівна</i>	Одеський національний політехнічний університет
ШПУРІК <i>Вероніка Володимирівна</i>	Кіровоградський національний технічний університет
ЯРИФА <i>Михайло Сергійович</i>	Харківський національний університет імені В.Н. Каразіна
ЯТЕЛ <i>Олексій Васильович</i>	Кіровоградський національний технічний університет

Напрямки роботи конференції

- Сучасні інформаційні технології та комп’ютерні системи.
- Теорія розробки програмного забезпечення.
- Програмне забезпечення комп’ютерних систем і мереж.
- Захист інформації в інформаційно-телекомунікаційних системах.
- Програмне та інформаційне забезпечення автоматизованих систем керування.
- Сучасні ІТ-технології підготовки фахівців з програмування.