ЗАХИСТ ІНФОРМАЦІЇ

УДК 004.56.5(043.2)

Борозніченко В.О.
Національний авіаційний університет, Київ

АНАЛІЗ ПРОГРАМНИХ ЗАСОБІВ УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ РИЗИКАМИ

На сьогоднішній день інформаційна сфера є ведучою в діяльності держави і чинить вплив на всі елементи соціальних комунікацій. Динамічний розвиток інформаційної сфери спричиняє виникнення інформаційних ризиків і вразливостей захисту інформації. Всі суб′єкти інформаційних взаємин - держава, суспільство, юридичні та фізичні особи – є власниками інформаційних ресурсів, які потребують певного рівня захисту.

Одним і з першочергових етапів побудови комплексних систем захисту інформації є оцінка інформаційних ризиків. З цією метою в інформаційних системах використовуються спеціальні програмні засоби оцінки інформаційних ризиків.

З огляду на це мета наукового дослідження полягає в наступному: проведення аналізу програмних засобів управління інформаційними ризиками; розробка класифікації програмного забезпечення управління інформаційними ризиками, з умов вимог та можливостей суб'єкта інформаційних відносин.

Наукова новизна дослідження полягає в наступному: розроблено класифікацію програмного забезпечення управління інформаційними ризиками, з урахуванням базових можливостей актуальних програмних продуктів згідно сучасних стандартів інформаційної безпеки.

Проведено оцінку можливостей, якості та ефективності використання програмних засобів оцінки інформаційних ризиків. COBRA- засіб для на аналізу та управління інформаційними ризиками, згідно вимог ISO 17799 у вигляді тематичних запитів. RA Software Tool- засіб, який виконує оцінку інформаційних ризиків згідно вимог стандартів ISO 17799 та ISO 13335. CRAMM- програмний засіб, який доцільно використовувати для аналізу інформаційних систем з підвищенними вимогами до інформаційної безпеки, велика точність пошуку ризиків, можливість заощадження матеріальних ресурсів. RiskWatch- потужний засіб для проведення аудиту інформаційної безпеки, в якості критеріїв для оцінки та управління ризиками використовують представлення річних затрат. OCTAVE використовується для оцінки ризиків за допомогою послідовності організованих внутрішніх семінарів, розташованих відповідним чином. Digilal Security Office-засіб для розробки та управління політики безпеки інформаційної системи на основі стандартів ISO 17799, ISO 27001, ISO 27005. RA2 art of risk- для проектування та побудови системи управління інформаційної безпеки використовується процесний підхід, на базі ISO 17799.

Науковий керівник – Юдін О.К., д-р техн. наук, професор

УДК 004.056.5 (043.2)

Волохович Л.С.
Національний авіаційний університет, Київ

МЕТОДИ ОЦІНКИ РИЗИКІВ

На сьогоднішній день актуальним є питанням розробки системи оцінки ризиків, яка за короткий час ґрунтовно буде описувати інформаційну систему, її ресурси, загрози та вразливі місця. Результати оцінки ризику допоможуть спрямовувати та визначити відповідні управлінські дії та пріоритети управління ризиками інформаційної безпеки.

В даній роботі проаналізовано системи оцінки ризиків, які можна б було використовувати для адекватної оцінки ризиків та для впровадження до інформаційних систем за короткий час. Так, постає необхідність в досліджені існуючих систем оцінки ризиків та розробки алгоритму проведення аналізу захищеності інформаційних ресурсів.

При впровадженні різних засобів захисту необхідно визначити баланс між можливим збитком від несанкціонованого витоку інформації та розміром вкладень, які витрачені для забезпечення захищеності інформаційних ресурсів.

Ціль оцінки ризику полягає в тому, щоб визначити ризик витоку інформації з корпоративної мережі підприємства. Такі програмні продукти, як: Risk Watch, CRAMM, COBRA, Авангард, ГРИФ,Конкор+ базуються на різних підходах до аналізу ризиків і рішенню різних завдань.

Програмне забезпечення RiskWatch є засобом для аналізу та управління ризиками, більше орієнтоване на точну кількісну оцінку співвідношення втрат від загроз безпеки та витрат на створення системи захисту.

Обстежити інформаційну систему, провести аудит відповідно до вимог стандарту BS 7799, розробити політику безпеки, можна за допомогою метода CRAMM. Даний комплекс робить оцінку ризиків за різними інформаційнми ресурсами, підраховує сумарний ризик ресурсів, а також веде підрахунок співвідношення збитку й ризику й видає недоліки існуючої політики безпеки.

Розглянуті методики дозволяють оцінити рівень поточного стану інформаційної безпеки автоматизованої системи, знизити потенційні втрати шляхом підвищення стійкості функціонування корпоративної мережі, розробити концепцію й політику безпеки автоматизованої системи, а також запропонувати плани захисту від виявлених загроз та вразливих місць. На сьогоднішній день існують різноманітні й складні по своїй структурі автоматизовані системи, для яких неможливо підібрати конкретну методику оцінки ризиків, тому для одержання адекватних результатів оцінки необхідно використати комплексний підхід до оцінок ризиків на основі вже існуючих методик.

Науковий керівник – Петренко А.Б., канд. техн. наук, доцент

УДК 004.056.52.57.087 (043.2)

Галата Л.П.
Національний авіаційний університет, Київ

БЕЗПЕКА WINDOWS SERVER 2012. ДИНАМІЧНИЙ КОНТРОЛЬ ДОСТУПУ

Сучасні організації все більшою мірою потребують таких компонентів, як гнучкість і здатність швидко реагувати на нові можливості і технології, і одночасно персонал потребує доступу до даних і інформації незалежно від інфраструктури, мережі, пристроїв, або додатків для їх отримання. Виконання вимог нормативних документів по інформаційній безпеці і потреба в захисті конфіденційної інформації – одні з найважливіших проблем для бізнесу і IT.

Наявні в Windows Server 2012 рішення, які використовуються для ідентифікації і забезпечення безпеки, дають IT-фахівцям можливість гнучкої підтримки нового сучасного стилю роботи і технологій хмарних обчислень.

Завдяки появі функції динамічного контролю доступу (Dynamic Access Control, DAC), ОС Windows Server 2012 кардинально змінила підхід до управління ідентифікацією і доступом до даних.

Dynamic Access Control — перший приклад використання заявок (claim) в базовій моделі авторизації Windows. Такого роду доступ забезпечує недоступний у минулому рівень деталізації і гнучкості.

Windows Server 2012 забезпечує нові, розширені способи управління доступом до Ваших файлів, надаючи зареєстрованим користувачам ресурси, яких вони потребують, за допомогою наступних можливостей:

- класифікація: ідентифікація даних за допомогою автоматизованої і ручної класифікації файлів (File Classification Infrastructure, FCI). Наприклад, можна забезпечити тегами дані на файлових серверах по всій організації;
- контроль: управління доступом до класифікованих файлів по всіх серверах, застосовуючи гарантію (safety net) з використанням централізованих політик доступу (Central Access Policies, CAPs);
- аудит: проводити аудит доступу до файлів на файлових серверах, використовуючи централізовані політики аудиту;
- захист даних: шифрування даних для конфіденційних документів Microsoft Office за допомогою автоматичного застосування шифрування з використанням служб управління правами Windows (Rights Management Services, RMS).

За допомогою комбінації технологій DAC, AD RMS і FCI можна створювати потужні схеми управління доступом до документів і захисту конфіденційної інформації, реалізовуючи повноцінну систему DLP (Data Loss Prevention) на базі інфраструктури Windows Server 2012.

Науковий керівник – Корнієнко Б.Я., канд. техн. наук, доцент

УДК 00:45:004.056.5 (043.2)

Ничипорук Р.Я.
Національний авіаційний університет, Київ

ВИКОРИСТАННЯ ПРОГРАМНИХ ЗАСОБІВ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ (НСД)

У наший час розвиток інформаційних технологій сприяє прискоренню для створення та використання нових засобів та способів у сфері інформаційної безпеки. Активно розробляються платформи та програмні коди для апаратного, програмно – апаратного та програмного комплексу. Проаналізувавши статистику використання методів захисту, виявилось , що програмний комплекс являється більш розповсюдженим, адже інформація, яка зберігається в системі та передається каналами зв'язку, подається в деякому коді, що виключає можливість її безпосереднього використання.

За допомогою спеціалізованого програмного забезпечення (ПЗ) можна забезпечити цілісніть, конфіденційність та доступність інформації від його редагування, копіювання та інших не правочинних дій, якій можуть нанести збитки та витік конфіденційних інформаційних ресурсів.

Метою захисту інформації є: обмеження фізичного доступу користувачів до автоматизованих систем (АС), ідентифікація та автентифікація користувачів, криптографічний захист, контроль цілісності, мережевий захист та інших засобів.

Одним з ключових методів захисту інформації від несанкціонованого доступу до каталогів чи файлів, являється розмежування повноважень та прав доступу користувачів до ресурсів АС.

Робота з системними життєво важливими файлами системи, а саме їх перейменування, видалення та створення копій файлів чи каталогів можуть призвести до значних змін в роботі програмного комплексу.

В ході роботи був розроблений програний продукт, який дозволяє захистити теку від НСД. ПЗ блокує правила на зміни атрибутів файлу для певних користувачів. Вибравши теку, необхідно добавити користувачів згідно так званих «чорних» списків. Для користувачів списку вибираються правила на редагування теки. Після чого користувачі списку немають права на зміни атрибутів файлу. Задля узгодженої роботи системи, адміністратор безпеки має правила на зміни всіх фалів та каталогів.

Розроблене ПЗ може використовуватися в АС-1 та АС-2. Робоча станція повинна підтримувати операційну систему (ОС) Windows 7 або Windows 8 з набором бібліотек не нижче NET.Framework 4.5. Розроблене ПЗ являє собою окремий додаток. Клієнтський запускається на кожному комп'ютері мережі, де планується проводити блокування каталогів та блокування несанкціонованих процесів.

Розроблена програма забороняє зміну атрибутів каталогів згідно заданого спику для заданих облікових записів в АС-1 та АС-2, що дозволяє забепечити високий рівень захщеності.

Науковий керівник – Єлізаров А.Б., канд. техн. наук, доцент

УДК 004.056.5(043.2)

Карнацький О.С.
Національний авіаційний університет, Київ

ОСОБЛИВОСТІ ВИКОРИСТАННЯ СТЕГАНОГРАФІЧНИХ МЕТОДІВ

Із розвитком сучасних інформаційних систем зростає роль захисту інформації. Крім традиційних засобів криптографічного захисту для забезпечення таємності важливих даних використовується стеганографія. В залежності від переслідуваних цілей необхідно використовувати відповідні стеганографічні методи. Але іноді обрання контейнеру для приховування повідомлення з певних причин стає неможливим. В таких випадках для наявного контейнеру треба знайти оптимальний стеганографічний метод.

Мета дослідження – з'ясувати основні критерії вибору оптимального стеганографічного методу в залежності від заявленої цілі та при нав'язаному стеганоконтейнері, змінити який неможливо.

Як відомо, основними напрямками використання стеганографії є:

- прихований зв'язок, а саме - передача повідомлення таким чином, щоб інша сторона навіть не підозрювала про його існування;
- захист авторських прав, тобто вбудовування цифрових водяних знаків (ЦВЗ) для підтвердження авторства;
- прихована анотація документів шляхом внесення коментарів, що має бачити лише обмежене коло осіб, яким відомий ключ;
- завадостійка автентифікація, при якої стеганографічні методи використовуються разом із криптографічними, для запобігання реалізації атак на дані користувача.

В першому випадку метод обирається в залежності від декількох факторів, а саме: тип інформації, яка циркулює у системі передачі даних (у потенційного зловмисника не має виникнути підозр щодо повідомлення), об'єму повідомлення та важливості даного повідомлення (оскільки залежність ***[надійність стеганосистеми]/[об'єм повідомлення]*** має зворотно пропорційний характер).

В другому випадку вибір методу залежить лише від типу файлу, у який буде вбудовуватися ЦВЗ (найважливішим фактором у даному випадку є надійність ЦВЗ, тобто стійкість до викривлень).

В третьому ж випадку зазвичай мають справу із текстовими документами, і метод приховування обирається в залежності від розміру повідомлення.

В останньому випадку основним завданням є прихована передача даних користувача до приймальної сторони, тому метод обирається в залежності від рівня надійності, який він забезпечує.

Для кожного повідомлення, яке необхідно приховати, стеганографічний метод обирається індивідуально. Основними критеріями при виборі стеганографічного методу є: тип контейнера, об'єм повідомлення та надійність заповненого контейнера (стійкість до викривлень). Головний критерій обирається в залежності від поставленої цілі.

Науковий керівник – Павлов В.Г., канд. техн. наук, доцент

УДК 004.056.5(043.2)

Касапов А.Е.
Національний авіаційний університет, Київ

МАНДАТНИЙ КОНТРОЛЬ ДОСТУПУ В БАГАТОМАШИННИХ КОМПЛЕКСАХ

Значного прогресу зазнало впровадження примусового (мандатного) контролю доступу в операційних системах. Зокрема, програмний комплекс SELinux став поставлятися в офіційне ядро Linux вже декілька років. Однак розгортання даної технології є доцільним лише для одномашинного комплексу. Можливість міжсистемного та віддаленого керування ресурсами тільки починає з'являтися в SELinux, тому розширення інструменту керування політикою безпеки для багатомашинної системи є відкритим питанням.

У якості можливого вирішення цієї проблеми пропонується застосування централізованого управління безпекою багатомашинної автоматизованої системи із застосуванням мандатного контролю доступу SElinux та використання загальної політики безпеки. Даний спосіб реалізується за допомогою використання серверу керування політиками, виділеного сховища політик безпеки та серверу безпеки.

Сервер керування політиками містить блок генерації політик на основі шаблонів політик безпеки. Замість відтворення цілої політики у ручному режимі, генератор політик надає інструмент для їх автоматизованого створення за попередньо сформованими шаблонами (наборами суб'єктів, об'єктів та правами доступу у відповідності до певного програмного додатку). Для розподілу загальної політики між окремими елементами мережі сервер забезпечує механізм розбиття та доставки необхідних частин політики безпеки.

Розбиття політики відбувається відповідно до функціональних особливостей кожного з компонентів автоматизованої системи. Локальні менеджери безпеки, що встановлені на кожному елементі домену, звертаються за рішенням контролю доступу до серверу безпеки, який посилає запити до бази політик у режимі черги. Для зменшення кількості запитів сервер безпеки містить таблицю кешованих правил, за якими часто виконують запити.

Зазначена вище схема дає можливість позбавитися надлишкового використання ресурсів кожного вузла мережі завдяки усуненню непризначених для цільової системи правил політики безпеки. Разом з цим, більшість систем матимуть спільні класи об'єктів, такі як, socket, file, ipc та ін.

Для забезпечення цілісності загальної політики безпеки модель припускає механізм синхронізації усіх залежних частин загальної політики, розподілених між елементами автоматизованої системи.

Науковий керівник – Корнієнко Б.Я., канд. техн. наук, доцент

УДК 004.627(043.2)

Курінь К.О.
Національний авіаційний університет, Київ

АЛГОРИТМ СТИСНЕННЯ-ВІДНОВЛЕННЯ ЗОБРАЖЕНЬ НА БАЗІ НЕСТАТИСТИЧНИХ МЕТОДІВ КОДУВАННЯ

Інформаційно-комунікаційні системи та мережі в сучасних умовах розвитку суспільства все ширше застосовують графіку різних класів, яка вимагає великих об'ємів пам'яті. Так, кожен піксел зображення кодується 24-ма бітами, стандартні зображення розміром 512×512 пікселів займатимуть 786432 байти, а зображення розміром 1024×1024 пікселів – 3145728 байт. Анімація, що також широко застосовується в комп'ютерних додатках, вимагає ще більшого об'єму пам'яті. Все це пояснює важливість використання сучасних технологій та методів стиснення.

З огляду на це мета наукового дослідження полягає в наступному: розробка алгоритму стиснення-відновлення зображень на базі методів кодування, відмінних від статистичних, з умов підвищення ефективності стиснення даних з одночасною мінімізацією спотворень у відновленому зображенні.

Наукова новизна дослідження полягає в наступному:

1. Розроблено алгоритм стиснення зображень на базі стандарту JPEG, який, на відміну від вказаного підходу: не використовує процедуру «укрупнення пікселів», яка є першопричиною появи артефактів у відновлюваному зображенні; враховує можливість використання алгоритму структурного кодування вмісту трансформант зображення замість алгоритмів статистичного кодування, що дозволяє досягти більшого ступеня стиснення при заданому рівні якості відновленого зображення.

2. Розроблено алгоритм структурного кодування трансформант зображення, що, на відміну від існуючих підходів: враховує доцільність розбиття вмісту квантованих трансформант на бітові шари замість представлення безпосередніми десятковими значеннями компонент; враховує можливість представлення бітових шарів трансформанти порядковими номерами розрахованими згідно методу кодування за кількістю бітових переходів; враховує можливість додаткового стиснення сформованих порядкових номерів з використанням методу RLE.

Практична цінність дослідження полягає в наступному:

1. Проведено оцінку якості відновлених зображень згідно значення пікового співвідношення сигнал/шум. Отримані результати дозволяють дійти висновку, що запропонований алгоритм вносить у відновлене зображення викривлення у допустимих межах чутливості людських органів.

2. Розраховано усереднений коефіцієнт стиснення для тестових зображень Запропонований алгоритм стиснення забезпечує виграш у ступені стиснення в порівнянні з існуючими методами: в 1,63 рази в порівнянні з алгоритмом JPEG для зображень з середнім ступенем кореляції; в 1,87 разів в порівнянні з алгоритмом JPEG для зображень з високим ступенем кореляції; в 1,39 рази в порівнянні з алгоритмом JPEG для зображень з дуже високим ступенем кореляції.

Науковий керівник – Юдін О.К., д-р техн. наук, професор

УДК 004.056.52:57.087.1(043.2)

Лозицька Л.Г.
Національний авіаційний університет, Київ

ЗНАЧЕННЯ OPENSSH ДЛЯ БЕЗПЕКИМ МЕРЕЖІ

Безпека мережі важлива для захисту від атак, джерело яких знаходиться за її межами. Часто буває необхідно отримати доступ до комп'ютера віддалено. Якщо користувач відправляє логін і пароль у вигляді звичайного тексту, вони можуть бути перехоплені і використані зловмисником для отримання доступу до віддаленої системи від імені цього користувача. Комплект програм SSH забезпечує необхідний захист, шифруючи трафік, що передається, включаючи логін і пароль. SSH забезпечує безпечне з'єднання в небезпечній мережі, такій як Інтернет. OpenSSH це вільно поширювана заміна SSH, в якій були видалені всі патентозалежні алгоритми, всі відомі помилки з безпеки і додані нові можливості. У OpenSSH входить мережева служба sshd і три клієнтські додатки командного рядка (ssh - захищений клієнт віддаленого доступу до консолі; scp - захищена команда віддаленого копіювання; sftp - захищений псевдо-ftp клієнт, що дозволяє передавати файли інтерактивно).

Внаслідок проведеного аналізу OpenSSH можна сформувати список можливостей, завдяки яким варто використовувати саме OpenSSH:

- безпечна система аутентифікації; посилена система конфіденційності (всі канали зв'язку автоматично та прозоро зашифровані);
- безпечні X11-сеанси; довільний TCP/IP-порт може бути перенаправлений через захищений канал в обох напрямках;
- при RSA-аутентифікації клієнт перевіряє справжність сервера перед кожним новим з'єднанням;
- "Host authentication key" може використовуватися адміністрацією централізовано, а також створюватися автоматично при першому підключенні до машини;
- будь-який користувач може створити будь-яку кількість RSA-ключів для аутентифікації;
- на стороні сервера є свій власний RSA-ключ, який автоматично регенерується кожну годину;
- агент аутентифікації, що працює на ноутбуці чи Workstation користувача, може бути використаний для зберігання RSA-ключів;
- програмне забезпечення може бути встановлено та використано без root-привілегій;
- клієнт налаштовується за допомогою загальносистемних та користувацьких файлів конфігурації;
- додаткове стиснення всіх даних , що передаються у мережі за допомогою gzip, що може призвести до значного прискорення на повільних з'єднаннях;
- повна заміна функціональності rlogin, rsh та rcp.

Науковий керівник – Мелешко О.О., доцент

УДК 004.056.5 (043,2)

Новицький Є.В.
Національний авіаційний університет, Київ

АНАЛІЗ ПРОТОКОЛІВ КВАНТОВОЇ КРИПТОГРАФІЇ

Основна ідея квантової криптографії полягає в тому, що неможливо скопіювати (розмножити) квантову інформацію; квантове повідомлення або прийде за призначенням, або потрапить до зловмисника, але тоді цей факт можна виявити. Стан квантового об'єкта (тобто, грубо кажучи, об'єкта дуже малої маси і розмірів, наприклад, електрона або фотона) може бути визначено вимірюванням. Проте відразу після виконання цього виміру квантовий об'єкт неминуче переходить в інший стан, причому передбачити цей стан неможливо. Отже, якщо в якості носіїв інформації використовувати квантові частинки, то спроба перехопити повідомлення призведе до зміни стану частинок, що дозволить виявити порушення секретності передачі. Крім того, неможливо отримати повну інформацію про квантовий об'єкт, і отже, неможливо його скопіювати. Ці властивості квантових об'єктів роблять їх «невловимими». Головною перевагою квантових криптографічних протоколів перед класичними є суворе теоретичне обґрунтування їх стійкості: якщо в класичній криптографії стійкість зводиться, як правило, до припущень про обчислювальні можливості зловмисника, то в квантової криптографії перехоплювач може вживати всі допустимі законами природи дії, і все одно у нього не буде можливості дізнатися секретний ключ, що залишився при цьому не поміченим.

Існує безліч протоколів квантової криптографії заснованих на передачі інформації за допомогою кодування в станах одиночних фотонів та їх можифікацій. Були розглянуті наступні:

- BB84 – однофотонний протокол квантової криптографії, згідно з яким фотони можуть приймати чотири стани поляризації. З розрахунку прийнятих фотонів є одним з найефективніших, проте малоефективний в плані безпеки.
- B92 – протокол, який за методами відправлення/розпізнавання фотонів схожий з BB84, але в ньому береться до уваги кут між напрямками поляризації фотонів, що дозволяє впливати на безпеку і швидкість передачі повідомлень.
- BB84 (4 +2) – був першою спробою протистояння PNS-атаці (Photon number splitting attack - атака з поділом за кількістю фотонів). Представляє собою комбінацію протоколів BB84 і B92.
- З шістьма станами – представляє собою протокол BB84, але з ще з одним базисом, що вводить ще два можливих напрямки поляризації для переданого фотона (окрім чотирьох основних: два діагональні, вертикальний і горизонтальний): правоциркулярний і лівоциркулярний.
- Гольденберга-Вайдмана – протокол, в якому використовуються для повідомлення два ортогональних стани, які є суперпозицією двох локалізованих нормалізованих хвильових пакетів. Їх користувач А посилає користувачу Б по двох каналах різної довжини, в результаті чого вони виявляються користувачем Б в різні моменти часу.
- Коаші-Імото – є модифікацією протоколу Гольденберга-Вайдмана.
- E91– протокол, заснований на парадоксі Ейнштейна-Подольські-Розенберга. Запропоновано використати пари фотонів, які народжуються в антисиметричних поляризаційних станах.
- SARG04 – протокол, який був запропонований як альтернатива протоколу «4+2», з огляду на уразливості останнього до PNS-атак. Даний протокол здатний ефективно протистояти PNS-атакам.

Провівши порівняльний аналіз наведених вище протоколів, слід зробити висновок, що розглянуті протоколи квантової криптографії слід використовувати спільно зі спеціальними протоколами для корекції помилок при передачі, а також з протоколами посилення безпеки щодо атак зловмисників.

УДК 004.056.52:57.087.1(043.2)

Підопригора Г.О.
Національний авіаційний університет, Київ

КРИПТОГРАФІЧНА СИСТЕМА ЗАХИСТУ LINUX

На сьогоднішній день жодна криптографічна система захисту інформації не може бути абсолютно надійною. Тому, для того щоб зробити неможливим перехоплення з незахищеної області пам'яті секретні паролі, криптографічні функції мають бути частиною операційної системи. В сімействі Windows, починаючи з Windows 95, забезпечується реалізація шифрування, генерації ключів, створення і перевірка цифрових підписів і других криптографічних задач. Ці всі функції необхідні для роботи операційної системи, однак ними може користуватися і будь-яка прикладна програма – для цього програмісту достатньо лиш звернутися до необхідної підпрограми так, як прописує криптографічний інтерфейс прикладних програм (CryptoAPI).

Розглядаючи Linux/Unix потрібно відмітити, що на даний момент в операційних системах типу Unix, на відміну від Windows, не існує єдиної системи криптографічного захисту. В них в залежності від ядра, використовують різні варіанти, але одними з найпоширенішими є :

1. cryptoloop + cryptoAPI (цей варіант є застарілим і більше не підтримується, але в ядрах гілки 2.4 його будуть ще довго використовувати). Його криптографічні уразливості поки що є некритичними, але від нього вже слід відмовлятися.
2. dm-crypt + cryptoAPI + cryptsetup. У нових ядрах 2.6 і нових дистрибутивах він дає готове шифрування.

a. LUKS - Linuxunifiedkeysetup - продовження і розширення проекту dm-crypt. Нові підходи в шифруванні, використання слотів з системою менеджменту ключів.

3. loop-aes. Альтернативна реалізація cryptoAPI для ядер 2.4 і 2.6. Інтеграція з GPG.

На сьогодні вбудована криптографічна система захисту Linux демонструє високий ступінь захисту, мінімум вірусів і як висновок - високу стабільність в роботі. Так як ця ОС поширюється по ліцензії GNU GPL, вона є безкоштовна і вільна, що дозволяє розробникам користуватися всіма її перевагами перероблюючи їх під свої цілі.

Отже, можна відмітити, що як Windows так і Linux в побудові криптографічної системи захисту використовують CryptoAPI.

Науковий керівник – Мелешко О.О., доцент

УДК 004.735(043.2)

Поповкін В.В.
Національний авіаційний університет, Київ

ОСОБЛИВОСТІ РЕАЛІЗАЦІЇ ГЛОБАЛЬНИХ МЕРЕЖ

Сучасні неприривно змінні вимоги до телекомунікаційних систем зумовили необхідність появи нових технологій. В таких умовах постає невідкладне завдання побудування мережі, яка б відповідала принципово новим напрямкам інформаційного суспільства. Мережа наступного покоління – NGN (Next Generation Network) має на меті в найближчому майбутньому забезпечити суспільство додатковими інноваційними можливостями. За даними Міжнародного союзу електрозв'язку (МСЕ) впродовж 2015-2020 року відбудеться поступовий перехід до мережі майбутнього – FN (Future Network), необхідність якої пояснюється появою нових прикладних галузей, що дозволяють дистанційно керувати технікою.

Мережа майбутнього – це глобальна інформаційна інфраструктура (ГІІ), яка об'єднує у собі вже існуючі інформаційно-комунікаційні мережі з урахуванням компонентів, котрі тільки плануються до впровадження, з єдиним центром управління ГІІ, що здатна надавати повний спектр телекомунікаційних послуг на базі нових та інноваційних технологій. Для побудови мереж майбутнього планується використовувати кремнієві та оптичні технології, а швидкість передачі даних буде досягати 1 Тбіт/с. Також для мережі майбутнього повинна бути розроблена дуже гнучка архітектура та передбачене володіння властивостями безперервної адаптації до навколишніх вимог.

Мережа наступного покоління це результат неймовірних змін основних телекомунікаційних мереж, унаслідок яких різні функції, що стосуються послуг було відокремлено від технологій, пов'язаних з їх транспортуванням. Від мережі Інтернет мережа майбутнього відрізняється тим, що:

- являє собою відкриту мережу, яка утворилось шляхом приєднання мереж;
- має високу надійність та ступінь інтеграції;
- потребує значних додаткових інвестицій.

Перехід до NGN та FN має низку невирішених питань стосовно ціноутворення, захисту, надійності, але відкриває безліч можливостей для новаторських рішень, та в майбутньому може сприяти збільшенню доходів та прибутків. Мережа майбутнього буде здатна встановлювати бездротові, дротові та супутникові широкосмугові з'єднання, розширювати доступ по мережі Інтернет, скорочувати цифровий розрив та підвищувати ступінь проникнення зв'язку.

Отже, як безперечний висновок можна сказати, що розгортання мережі майбутнього це лише питання часу, адже реалізація FN дасть змогу надавати вільний доступ до інтелектуальних ресурсів у будь-який час і у будь-якому місці, гарантуючи високу якість і прийнятну вартість відповідних послуг.

Науковий керівник – Корнієнко Б.Я., канд. техн. наук, доцент

УДК 004.91 (477)(043.2)

Прокопенко А.А.
Національний авіаційний університет, Київ

СУЧАСНИЙ СТАН ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ В УКРАЇНІ

Кожне підприємство, як суб'єкт економічної діяльності, повинно періодично надавати звіти до відповідних державних органів. Традиційна "паперова" форма звітності по-перше дуже незручна, а по-друге потребує суттєвих затрат часу, які зростають із збільшенням кількості звітуючих. Для створення сучасної системи листування та звітування 7 лютого 2002 року був прийнятий закон «Про електронні документи та електронний документообіг», у якому були закладені основні організаційно-правові засади електронного документообігу та використання електронних документів.

Мета дослідження – проаналізувати сучасний стан електронного документообігу в Україні, його основні складові, роль державних органів, які його забезпечують, та створити прогнози його подальшого розвитку.

Як важлива складова електронного документообігу розглядається електронний цифровий підпис, який виступає засобом підтвердження авторства електронних документів. Центри сертифікації ключів, виступають органами, що засвідчують електронні цифрові підписи.

Контроль Центрів сертифікації здійснюється двома уповноваженими державними органами: Міністерством юстиції України та Державною службою спеціального зв'язку та захисту інформації в Україні. Крім контролю системи електронного документообігу в Україні вони формують нормативну та правову базу, вимоги до основних елементів електронного документообігу та електронного цифрового підпису.

Для надійного захисту цілісності електронних документів повинні використовуватися спеціальні програмно-апаратні засоби формування цифрового підпису, котрі пройшли контроль та отримали сертифікат про відповідність усім вимогам, що викладені у нормативної документації.

У доповіді також буде розглянуто:

- правила оформлення сертифікатів;
- послідовність формування рівнів сертифікатів;
- склад пакету документів, що повинен надати замовник сертифікату;
- терміни дії сертифікатів різного рівня;
- процедура отримання сертифікатів фізичними особами та підприємствами;
- відповідальність за компрометацію сертифікатів;
- процедури анулювання та відкликання сертифікатів.

В Україні набуває поширення електронний документообіг, який зараз існує паралельно з традиційним "паперовим".

Науковий керівник – Павлов В.Г., канд. техн. наук, доцент

УДК 004.056.5(043.2)

Ревтюх В.С.
Національний авіаційний університет, Київ

ЗАСТОСУВАННЯ ДЕМІЛІТАРИЗОВАНОЇ ЗОНИ В КОМП`ЮТЕРНИХ СИСТЕМАХ

Демілітаризована зона (ДМЗ) являє собою конфігурацію брандмауера для забезпечення захисту локальних мереж. Сучасні методи розміщення даних на резидентному комп'ютері в ДМЗ використовують відкриття порту в брандмауері між комп'ютером в ДМЗ та внутрішньою мережею. Це створює загрозу безпеці та призводить до значної кількості помилок в налаштуванні брандмауера.

Сценарій, при якому інформація повинна бути передана на резидентний комп'ютер в ДМЗ - це розкриття даних для доступу з Інтернету. При реалізації ДМЗ в якості резидентних комп'ютерів можна використовувати віртуальні машини, які можуть існувати без зв'язку з внутрішньою мережею. Такий спосіб ефективний з точки зору безпеки, але не допускає передачу даних між внутрішньою мережею і резидентними комп'ютерами в ДМЗ.

Існують системи і методи, що забезпечують ІБ комп'ютера в ДМЗ, який не може підключитися до внутрішньої мережі, але при цьому здатний передавати дані з ДМЗ та на нього. Механізм включає в себе передачу файлів з віртуальних жорсткий дисків між внутрішньою мережею та головним комп'ютером.

Головний комп'ютер в ДМЗ може бути налаштований з двома мережевими картами. Один мережевий інтерфейс може бути підключений до мережі ДМЗ. Другий може бути підключений до внутрішньої мережі. Віртуальні машини можуть бути підключені тільки до адаптера ДМЗ. Фізичний хост може обмінюватися даними тільки з внутрішньою мережею.

Щоб передати дані в комп'ютер, розташований в ДМЗ, файл з віртуального жорсткого диска може бути скопійований на хост ДМЗ через внутрішню мережу. Резидентний віртуальний комп'ютер в ДМЗ може визначити наявність нового диска і встановити його. Через відсутність мережевого з'єднання між резидентними комп'ютерами в ДМЗ і внутрішньою мережею, передача файлів може відбуватись без будь-яких маніпуляцій в брандмауері.

Комп'ютерні інструкції, такі як програмні модулі, також можуть бути використані. Взагалі, програмні модулі включають процедури, програми, об'єкти, компоненти, структури даних і т.д., які виконують конкретні завдання або реалізації зокрема абстрактних типів даних. Розподілені комп'ютерні середовища можуть використовуватися там, де завдання виконуються за допомогою дистанційного пристрою обробки, які пов'язані через комунікаційні мережі або інші середовища передачі даних. У розподілених обчислювальних середовищах, програмні модулі та інші дані можуть бути розташовані як в локальному так і віддаленому комп'ютерному носії, включаючи пристрої зберігання пам'яті.

Науковий керівник – Корнієнко Б.Я., канд. техн. наук,доцент

УДК 004.056.5(043.2)

Сніжко В.В., Корнієнко Б.Я.
Національний авіаційний університет, Київ

СПІЛЬНЕ ВИКОРИСТАННЯ МОДЕЛЕЙ БЕЗПЕКИ КОМП'ЮТЕРНИХ СИСТЕМ

Моделі безпеки відіграють важливу роль у процесах розробки і дослідження захищених комп'ютерних систем, тому що забезпечують системотехнічний підхід, що включає вирішення наступних найважливіших завдань:

- Вибір і обґрунтування базових принципів архітектури захищених комп'ютерних систем, що визначають механізми реалізації засобів і методів захисту інформації;
- Підтвердження властивостей (захищеності) систем шляхом формального дотримання політики безпеки (вимог, умов, критеріїв);
- Складання формальної специфікації політики безпеки, як найважливішої складової частини організаційного та документаційного забезпечення розроблюваних захищених комп'ютерних систем.

У реальних автоматизованих системах рідко зустрічаються системи захисту, орієнтовані виключно на забезпечення конфіденційності або виключно на забезпечення цілісності інформації. Як правило, система захисту повинна поєднувати обидва механізми - а значить, при побудові та аналізі цієї системи буде необхідним спільне використання декількох формальних моделей безпеки.

Розглянемо як приклад можливі варіанти спільного використання моделей Белла-ЛаПадули і Біба:

1. Дві моделі можуть бути реалізовані в системі незалежно одна від одної. В цьому випадку суб'єктам та об'єктам незалежно присвоюються рівні секретності та рівні цілісності.
2. Можливо логічне об'єднання моделей за рахунок виділення загальних компонентів. У випадку моделей Біба і Белла-ЛаПадули таким загальним компонентом є порядок розмежування доступу в межах одного рівня секретності.
3. Можливе використання однієї і тієї ж решітки рівнів, як для секретності, так і для цілісності. При цьому суб'єкти та об'єкти з високим рівнем цілісності будуть розташовуватися на низьких рівнях секретності, а суб'єкти та об'єкти з низьким рівнем цілісності - на високих рівнях секретності.

Формалізація механізмів захисту може переслідувати різні цілі, але головна з них - це оцінка стійкості архітектури реальних систем, що проводиться, наприклад, в рамках комплексного аналізу їх захищеності.

УДК 004.056.53(043.2)

Соловей Р.С.
Національний авіаційний університет, Київ

БЕЗПЕКА ІНІЦІАЛІЗАЦІЇ ОПЕРАЦІЙНОЇ СИСТЕМИ ШЛЯХОМ СТВОРЕННЯ ДОВІРЧОГО МІКРОПРОГРАМНОГО СЕРЕДОВИЩА

Безпеку сучасних комп'ютерних систем неможливо забезпечити тільки шляхом установки захищеного операційного середовища та / або зовнішніх засобів захисту інформації. Це пов'язано з тим, що існують методи злому і шкідливі програми, що дозволяють впровадити зловмисний код до завантаження операційної системи, та тим самим відключити або знешкодити механізми безпеки. Через це захист на рівні операційної системи стає неефективним, оскільки він може бути зруйнованим ще на стадії завантаження BIOS. Для вирішення цієї проблеми найчастіше використовуються апаратні модулі довіреного завантаження операційної системи, але якщо шкідливому коду вже вдалось впровадитися у саму програму BIOS, то виникає можливість обминання команд передачі управління цього модулю програмними засобами. Також існує інший суттєвий недолік апаратні модулі довіреного завантаження - такі системи в принципі не підтримують віртуальне операційне середовище, в якому доволі часто працюють користувачі.

Тому заслуговує уваги розгляд інших шляхів створення довірчого мікропрограмного середовища та забезпечення цілісності та безпеки ініціалізації операційної системи, в тому числі віртуальної. Суть пропозиції полягає у доповненні програми BIOS, яка, як звісно, здійснює первинне завантаження комп'ютерних систем, власними модулями, за допомогою яких буде виконане блокування будь-яких змін програми BIOS в майбутньому без відому користувача.

Якщо розглядати процес завантаження операційного середовища як послідовність певних фаз, то важливо з'ясувати, коли відбувається виконання вбудованих модулів та від чого це залежить.

Проведені дослідження показали, що якщо модуль ініціалізації стандартний, то він більше залежить не від розробника материнської плати, а від версії ядра BIOS. Так у досить поширених версіях ядер BIOS AWARD v 4.51, v 6 та AMI v 8, модифікацію можна виконати під час фази 0 за рахунок використання механізму відновлення.

Таким чином, реалізація програмного засобу довіреного завантаження, побудованого на описаних вище принципах, має низку переваг, а саме:

- забезпечує необхідний рівень безпеки комп'ютерних систем, шляхом виключення вразливостей передачі управління, властивих апаратним засобам;
- забезпечує довірене завантаження віртуальних машин, що істотно знижує можливість створення середовища зловмисника в складних інформаційно-обчислювальних комплексах;
- використання програмного засобу має економічну перевагу оскільки не вимагає придбання спеціального електронного модулю.

Науковий керівник – Павлов В.Г., канд. техн. наук, доцент

УДК 004.056:004.415.5(043.2)

Стародуб Ю.І.
Національний авіаційний університет, Київ

ФАЗЗЕРИ ФОРМАТУ ФАЙЛУ

Існує чимало засобів фаззінгу, серед яких фаззери мережевого протоколу, формату файлу та інші. Зважаючи на це виникає актуальна задача в аналізі наявних фаззерів, зокрема фаззерів формату файлу, які мають свої переваги й недоліки**.**.

Для класифікації фаззерів формату файлу було взято сукупність параметрів: вхідні параметри, вихідні параметри, метод фаззінгу, реалізація фаз фаззінгу, тип вхідних даних, мова реалізації та платформа, доступність використання, можливість відтворення виняткової ситуації.

Вхідні параметри – вхідні дані, які подаються фаззеру на початку експерименту.

Вихідні параметри – дані, які видає фаззер наприкінці експерименту.

Метод фаззінгу – метод створення вхідних експериментальних даних (мутаційний або породжуючий).

Реалізація фаз фаззінгу – можливість реалізації наступних фаз фаззінгу: визначення цілі, визначення вхідних значень, генерація(породження) некоректних даних, виконання некоректних даних, моніторинг виключень, визначення працездатності.

Тип вхідних даних – введення з інтерфейсних пристроїв; параметри програмного середовища; параметри командного рядка; комунікаційні протоколи; файли; дані в оперативній пам'яті.

Мова реалізації та платформа – мова програмування, на якій було написано даний засіб фаззінгу та операційна система, яка підтримує використання даного засобу.

Доступність використання – якісна оцінка зручності використання фаззера.

Можливість відтворення виняткової ситуації – незмінність експериментальних даних при повторному експерименті.

В ході даної роботи було проаналізовано більше десятка засобів фаззінгу формату файлу за відібраними параметрами. А саме: MiniFuzz, FileFuzz, SPIKEfile, notSPIKEfile, ZZUF, Intent Fuzzer, fsfuzzer, Ffuzzer, FileH, FileP.

В ході даної роботи було розглянуто фаззери формату файлу та проведено їх порівняльний аналіз. Результати проведеної роботи будуть корисні фахівцям при виборі засобу фаззінгу.

Науковий керівник – Корченко О.Г., д-р техн. наук, професор

УДК 004.056.52:57.087(043.2)

Федоров Р.В.
Національний авіаційний університет, Київ

АНАЛІЗ ЕФЕКТИВНОСТІ БІОМЕТРИЧНИХ СИСТЕМ РОЗПІЗНАВАННЯ ОСОБИСТОСТІ ЗА ГОЛОСОМ

Широке застосування інформаційних технологій призвело до загострення проблеми захисту інформації, що головним завданням має забезпечення цілісності, доступності та конфіденційності даних.

На сьогоднішній день одним з найкращих рішень є використання біометричних технологій (систем) контролю доступу, які мають достатньо високий ступінь надійності та займають гідне місце на ринку.

Біометричні системи (БС) використовують статистичні та динамічні характеристики користувачів (власників) інформаційних ресурсів, доступ до яких обмежується.

Мета роботи – проаналізувати біометричні системи розпізнавання голосу, виявити переваги та недоліки даних систем, розробити рекомендації щодо їх оптимального використання.

Розпізнавання за голосом (спектральний аналіз голосу) відрізняється від інших БС тим, що використовує акустичну інформацію, а не зображення. Головними факторами, які впливають на формування людської мови, є фізіологічні особливості, такі як голосові зв`язки, носова порожнина, форма та розмір губ тощо. Головною перевагою системи розпізнавання голосу над іншими БС є можливість передавати голосові дані дистанційно, наприклад, використовуючи телефоні лінії. Процес перевірки відбувається зі швидкістю вимови слів.

Метод розпізнавання голосу використовує три типа верифікації об'єкта мовлення: текст залежний, текст запиту та текст незалежний.

Слід зазначити, що даний метод є найбільш звичним для людини, має невисоку вартість, явною перевагою є його безконтактність.

До недоліків даного методу можна віднести високу чутливість до завад, що викликає необхідність наявності спеціалізованого завадоїзольованого приміщення; можливість перехоплення фрази; високий рівень помилок 1-го і 2-го роду. Якість розпізнавання залежить від багатьох факторів, таких як інтонація, швидкість мовлення, фізичний та психологічний стан джерела тощо.

У результаті аналізу ефективності розпізнавання особистості за голосом з'ясована неможливість забезпечення надійного рівня захисту інформації на базі тільки єдиного методу. Поєднання різних БС є найкращим рішення для контролю доступу, оскільки кожний метод окремо має як свої недоліки, так і переваги, а при використанні мультимодальних методів загроза мінімізується. Щодо системи розпізнавання голосу, то ідентифікацію джерела слід проводити з мінімальним рівнем шуму, для чого створювати відповідні умови, оновлювати базу шаблонів та удосконалювати систему.

Науковий керівник – Дубчак О.В., ст.викладач

ІНЖЕНЕРІЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

УДК 629.735.33(043.2)

Hryshchenko A.B.
National Aviation University, Kyiv

MATURITY MODEL CREATION METHODOLOGY

Since the appearance of first maturity model more than twenty years ago almost two hundreds more came up and still we do not have a clue how good and consistent maturity model should look like. Their application went out of IT boundaries and now they are widely used in different business process now. We can justify this with the central paradigm of these models – processes and their improvement. However, numerous shortcomings have been disclosed referring to both maturity models as design products and the process of maturity model design. Whereas research has already substantiated the design process, there is no holistic understanding of the principles of form and function – that is, the design principles – maturity models should meet.

Maturity models usually include a sequence of levels (or stages) that together form an anticipated, desired, or logical path from an initial state to maturity.

Usually maturity models are created to be independent from application domain peculiarities, so they may refer to processes as well as other entities (e.g. people, specific application domain objects). Aside of that, we can consider them from resources-view side distinguishing assets (i.e., process in- and outputs) and capabilities (i.e., repeatable patterns of action in the use of assets).

We can define three 3 main purposes maturity model can surve: descriptive, prescriptive and comparative.

Descriptive purpose mainly lays in giving a solid explanation on what is maturity in the given case, how we can evaluate current object. Main point here is that maturity model is diagnosis tool.

Prescriptive purpose outlines what we should do, providing specific and detailed courses of action on how to identify desirable maturity levels and provides guidelines on improvement measures.

Comparative purpose is used for internal or external benchmarking. Given sufficient historical data from a large number of assessment participants, the maturity levels of similar business units and organizations can be compared.

While creating a maturity model of our own we can use many different technologies modifying them up to our needs. Technologies used in IT development will perfectly fit, however we should remember to keep the process iterative, because evaluating and defining new stage is very important for thorough and fully described maturity model. In addition to this we should keep in mind that we should create detailed documentation. It is required for a better understanding and for comparative purpose directly. New maturity model should provide an innovative view on the problem and its solution.

Scientific Supervisor M.O Sidorov, Doctor of Technical Studies, professor

УДК 629.735.33(043.2)

Chepyuk N.V
National Aviation University, Kyiv

USAGE OF ONTOLOGIES IN THE SOFTWARE ENGINEERING

Since the appearance of software engineering as the discipline and to these days the problems of modularization, reuse, integration and distribution of software components are among the central issues of the discipline. The more these tasks are automating and extending, the more important the definition and usage of ontologies as conceptual basis of these components becomes.

As ontologies are helping to formally represent knowledge in the form of sets of concepts within the application domain and the relationships between pair of concepts, they can be used to describe the application domain of the software engineering as the discipline itself as well as to describe the application domain of a particular problem software engineering strives to solve.

The usage of modeling principles is the basis of the software design process. Model Driven Development (MDD) is the relatively new software discipline which helps to design and develop software on the basis of modeling. The main concept of MDD is to increase the productivity of software developer's work by increasing the level of abstraction when developing software. To obtain such results MDD uses models, which are defined with the help of modeling languages (UML for instance). The models of the modeling languages are called metamodels.

There exists the synergy between software modeling languages and ontologies. In particular, it's based on the similarities between the standard concepts of UML and those of ontologies (for example, class, relations, inheritance). It was proposed to use UML for modeling ontologies due to the wide acceptance of UML by software engineers. Moreover, the benefit can also be obtained from usage of ontology reasoning services (for example, check for consistency) to reason over UML models, since they nowadays lack the support for formal validation and may contain hidden inconsistencies and redundancies. The practical reasoning contribution is the reasoned which allows to reason over UML class diagram. Ontologies of the application domain can be useful in software design: MDD principles allow using ontologies for extending UML activity diagrams. There is also the work in the area of extending the OWL for the means of using UML composite structures.

Object Management Group (OMG) initiated a standardization process to issue the request for proposal for Ontology Definition Metamodel (ODM). The main goal of this process was to define the metamodel for the two main ontology languages - RDF and OWL, the corresponding ontology of UML profile (to use standard UML tools for modeling ontologies) and the transformations between the ODM and other ontologies and modeling languages. This work resulted in the OMG ODM specification, published in 2009.

Scientific Supervisor M.O Sidorov, Doctor of Technical Studies, professor

УДК 004.4 (043.2)

Книшик М.А.
Національний авіаційний університет, Київ

ЗАСІБ ВИМІРЮВАННЯ МЕТРИК ПОКРИТТЯ КОДУ

Метрики покриття коду – корисний інструмент для контролю якості програмного продукту. І хоча високі значення метрик не є гарантією якості, вони дають змогу знайти місця в коді, що, можливо, потребують додаткової уваги. А відстеження зміни значень протягом проекту допомагає підтримувати якість тестування та проекту вцілому на належному рівні. Проте існують деякі проблеми з їх вимірюванням. Є небагато вимірювачів, призначених спеціально для метрик покриття. Їх вимірювання не є точними та різняться в різних засобах. Дуже мало засобів мають зручний графічний інтерфейс, яким зручно користуватись. І зовсім немає засобів, які підтримували б ручне тестування.

Зважаючи на ці проблеми, було розроблено засіб для вимірювання покриття коду. Програма має простий та зрозумілий графічний інтерфейс, тому не потребує додаткового навчання. Вона здатна виміряти покриття рядків, гілок та шляхів. Результати можна представити графічно, що полегшує їх сприйняття та інтерпретацію. Також для оцінки покриття коду була введена власна метрика. Вона визначається зі значень попередніх трьох, взятих з певними ваговими коефіцієнтами. Метрика розраховується за формулою:

$$M = 0{,}2L + 0{,}3B - 0{,}5P ,$$

де *L*-покриття рядків,*B*-покриття гілок,*P*-покриття шляхів. Вона дає більш комплексне поняття покриття коду, включаючи в себе значення всіх основних метрик.

Ще одна перевага розробленого засобу в тому, що він дозволяє запускати не тільки модульні тести, але й інтерфейс програми, що тестується. Це дає можливість тестувати програми вручну, а вимірювач розрахує покриття для цих тестів.

Для вимірювання засіб використовує інструментування коду. Вихідний код програми, що вимірюється, копіюється в інший каталог. Далі вимірювач аналізує його, та додає свої оператори перед кожним рядком та в оператори умов, одночасно рахується їхня кількість. Створюється два статичних масиви з розмірністю, що відповідає кількості рядків та гілок. Після цього інструментований код запускається, а додані оператори, якщо вони виконуються, змінюють відповідні значення масивів. Незмінені значеня відповідають непокритим елементам. Виходячи з данних у масивах можна обчислити значення всіх чотирьох метрик програми.

Результати вимірювань розробленого засобу були порівняні з результатами інших засобів. Відхилень значень від вимірювачів, що працюють за тим самим принципом немає або вони незначні.

Науковий керівник – Дишлевий О.П., ст. викладач

УДК 51.681.3 (043.2)

Максимець О.М.
Київський Національний Університет ім. Тараса Шевченка

ВЕРИФІКАЦІЯ ПРОГРАМ ЗА ДОПОМОГОЮ МАШИННОГО НАВЧАННЯ

Верифікація програм є одним з найважчих (якщо не найважчим) етапом розробки програмного забезпечення. Труднощі цього етапу полягають у тому, що від розробника, крім знань чисто програмістського характеру, потрібні знання і володіння методами сучасної алгебри, логіки, комбінаторики, теорії чисел та інших суміжних областей. Крім цих суб'єктивних чинників є й об'єктивні чинники, пов'язані з тим, що в даний час наявні методи верифікації не знаходяться на достатньому рівні розвитку, який дозволяв би верифікувати системи індустріальних розмірів. Загалом картина, яка спостерігається на даний момент така, що складність програмного забезпечення постійно зростає, а методи його аналізу істотно відстають.

Теорія машинного навчання є віткою штучного інтелекту, предметом вивченням якої є системи, які можуть навчатися на даних. З розвитком теорії машинного навчання застосування їй знаходиться в інформаційних системах, які містять накопичену історію даних. Одне з відомих застосувань машиного навчання є перевірка орфографії при написанні тексту. Даними для навчання такої системи служать книжки і орфографічно правильні тексти. Підхід до навчання базується на мовних правилах і абстрактному представленні речень.

Завдяки платформам по розміщенню відкритого програмного забезпечення і багатій історії проектів з відкритим кодом існує достатньо данних, на яких міг би навчатися, так званий, верифікатор програмного коду. Таким чином, аналізуючи базу потенційно вірного програмного коду, алгоритм міг би навчитися перевіряти правильність програм і вказувати на «сумнівні» частини програми.

Алгоритм машиного навчання для верифікатора, як і у випадку з лінгвістичною мовою, має мати своє абстрактне представлення програми або її частини, яке було б незалежним від іменування зміних і мови програмування. Але, як і у випадку з орфорграфом, верифікатору не обов'язково знати «значення» програми, тобто враховувати формальну постановку задачі.

Робота алгоритму роботи верифіктора буде зводитись до представлення коду в потрібній абстрактній структурі. Другий етап ─ це пошук відповідних частин програми в базі потенційно «правильних» програм і прийняття рішення, щодо сумнівності чи правильності розглядуваної програми.

Сигналом для розробки такого верифіктора служить і те, що для платформ розміщення відкритого ПЗ певним чином розв'язана проблема оцінки якості коду. Для кожного проекту зберігаються дані про кількість виправлень, скачувань і релізів проекту. Що є своєрідною мірою правильності наявного коду.

Науковий керівник – Кривий С.Л., д-р фіз.-мат. наук, професор

УДК 004.413 (043.2)

Нетреба О.М., Гриненко О.О.
Національний авіаційний університет, Київ

МОДЕЛЮВАННЯ ЕКОСИСТЕМ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Екосистеми програмного забезпечення стають все більш популярним засобом організації промисловості, який використовується провідними розробниками програмного забезпечення. Отже, екосистема програмного забезпечення - це сукупність суб'єктів та відносин, які функціонують як єдине ціле і взаємодіють із ринком програмного забезпечення та послуг. Відносини спираються на єдину технологічну платформу і працюють шляхом обміну інформацією, ресурсами і артефактами. В даний час не існує офіційного стандарту моделювання екосистем програмного забезпечення. Основні наслідки відсутності стандарту - виробники програмного забезпечення мають проблеми виділення конкретних екосистем програмного забезпечення та їх використання.

У інженерних дисциплінах, об'єкти пізнання досліджуються за допомогою моделей. Існує чотири типи засобів моделювання екосистем програмного забезпечення: i* моделі (SD & SR), нормативні i* моделі, PDC (Product deployment Context), SSN (Software Supply Network).

Модель i* відображає соціальні аспекти екосистеми та видає пріорітет соціальним суб'єктам, у яких є цілі, переконання, здібності і зобов'язання. Аналіз фокусовано на тому, як добре цілі різних акторів досягаються в контексті відносин між людиною і системними учасниками, а також як при зміні конфігурації цих відносин можна допомогти учасникам досягти своїх стратегічних цілей. i* стимулювало значний інтерес до соціально-мотивованого підходу до моделювання і проектування, і призвело до низки цих розширень та адаптацій.

PDC забезпечує швидкий огляд архітектури та залежностей програмного продукту в своєму працюючому навколишньому середовищі. Деталі, представлені PDC, показують ієрархію між різними продуктами і компонентами та забезпечують їх почерговий перегляд з різних мережевих локацій.

SSN являє ряд пов'язаних між собою областей, таких як програмне забезпечення, апаратне забезпечення та обслуговування організацій, що співпрацюють для задоволення вимог ринку.

У доповіді було виконано моделювання екосистеми розробників програмних продуктів України.

Науковий керівник – Сидоров М.О., д-р техн. наук, професор

УДК 004.413 (043.2)

Пашук А.В., Сидорова Н.М.
Національний авіаційний університет, Київ

ОНТОЛОГІЇ ГРУПОВОЇ ДИНАМІКИ

Процес розробки програмного забезпечення – це складна, багатоетапна діяльність, яку здійснюють розробники програмного забезпечення в складі команд. Тому процес розробки– це групова діяльність, а важливою її складовою є комунікації. Процес розробки передбачає залучення різних спеціалістів та їх тісну взаємодію, як між собою так і з замовником програмного забезпечення. Ефективність процесу розробки, його своєчасність та правильність залежить від коректно встановлених комунікацій.

Обмеженість комунікацій може привести до збільшення затрат часу на виконання операцій; відсутність чіткого розуміння цілей; погане надходження актуальної інформації; зростання витрат на реалізацію.

Завданнь які потрібно розв'язувати:

- Моделювання комунікацій в колективі, при якому забезпечується створення груп відповідно до поставлених задач та встановлення з'язків між ними;
- Оптимізація комунікацій між групами, забезпечення кращої продуктивності роботи;
- Вирішення проблемних ситуацій комунікацій у випадку реструктуризації груп чи зміни поставлених задач;
- Адаптація процесу розробки під нові вимоги.

Ці завдання можна розв'язати щляхом створення системи з представленням предметної області в формі онтологій.

Онтологія - це концептуальне представлення знань певної предметної області.

Цілі застосування онтологій в груповій динаміці є наступними: структурування інформаційної бази; формалізація опису процесів групової динаміки; автоматизація процесу аналізу; вирішення комунікаційних задач; проектування моделі комунікації; оптимізація комунікаційних процесів.

В доповіді наведено приклад побудови онтології групової динаміки при свторенні програмних продуктів.

Науковий керівник – Романов Є. М., канд. техн. наук, доцент

УДК 629.735.33 (043.2)

Рибачук Я.А.
Національний авіаційний університет, Київ

МОДЕЛЬ ДОВГОІСНУЮЧОЇ ТРАНЗАКЦІЇ ПРИ ПРОЕКТУВАННІ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Розглянута модель довгоіснуючої транзакції (ДТ), яка базується на моделі Sagas – сукупності ДТ, що паралельно виконуються. Щоб полегшити проблеми керування ДТ було запропоновано в [1] поняття саги (англ. saga). ДТ це сага, якщо вона може бути записана у вигляді послідовності транзакцій, які можуть чергуватися з іншими ДТ.

Мета роботи – застосувати модель ДТ для підтримки процесів автоматизації глобальної розробки програмного забезпечення (ПЗ).

Процес створення ПЗ розглядається як виконання ДТ над інформаційною базою проектів (ІБП) від начала до завершення. При цьому ІБП розглядується як розподілена гіпертекстова база ресурсів проектів (програмна документація, тексти програм, графіки, то що). Система керування ДТ базується на сервіс орієнтованої архітектурі.

Головний сенс довгоіснуючої транзакції – виконувати все або нічого. Під час створення ПЗ, виконується безліч дій, які входять до ДТ, тобто або всі повинні бути виконані, зафіксовані, або повністю відмінена вся операція та відбутися повернення до попереднього стану ІБП.

Обробка даних, що поступають, приводить до великої кількості змін програмного забезпечення. Ці зміни потенційно можуть потерпіти невдачу, і чинники, які можуть впливати – досить велика кількість, тому система повинна в разі невдачі коректно повернути ІБП в стан на момент створення чергового контрольного збереження даних. Для цього створюється журнал транзакції.

Журнал транзакцій у поєднанні з сегментом відкату (область, в якій зберігається копія всіх змінних даних), що гарантує цілісність даних. В разі збою запускається процедура відновлення. При цьому аналізується наступне:

1. Якщо пошкоджений запис, то збій стався під час проставляння відмітки в журналі. Значить, нічого важливого не загубилося, ігноруємо цю помилку.
2. Якщо всі записи помічені як успішно виконані, то збій стався між транзакціями, тут також немає втрат.
3. Якщо в журналі є незавершена транзакція, то збій стався під час запису на диск. В цьому випадку ми відновлюємо стару версію даних з сегменту відкоту.

Науковий керівник – Оленін М.В., канд. фіз.-мат. наук, доцент

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ПРОЕКТУВАННЯ

УДК 004.652.3(043.2)

Артамонов А.І.
Киевский национальний университет строительства и архитектуры, Киев

СОТОВАЯ СВЯЗЬ И ТЕЛЕФОНЫ

Сотовая связь - это наиболее современная и быстро развивающаяся область телекоммуникаций. Сотовой она называется потому, что территория, на которой обеспечивается связь, разбивается на отдельные ячейки или соты. Как правило, в каждой соте абонент получает одинаковый набор услуг и в определенных территориальных границах получает эти услуги по равной цене. Таким образом, перемещаясь от одной соты к другой абонент не чувствует территориальной привязанности и может свободно пользоваться услугами связи. Основными элементами подсистемы базовых станций (как не трудно догадаться) являются сами базовые станции (BTS). Они то как раз и создают те соты, о которых говорилось в начале. Каждая базовая станция, как правило, обслуживает три соты. Радиосигнал от базовой станции излучается через 3 секторные антенны, каждая из которых направлена на свою соту. Иногда можно встретить ситуацию, когда на одну соту направлены сразу несколько антенн одной базовой станции. Это связано с тем, что сеть сотовой связи работает в нескольких диапазонах (900 и 1800). Кроме того, на данной базовой станции может присутствовать оборудование сразу нескольких поколений связи (2G и 3G). Наиболее привычным местом размещения базовой станции является башня или мачта, построенная специально для нее.

Сотовый телефон— мобильный телефон, предназначенный для работы в сетях сотовой связи. Принцип работы мобильного телефона основан на приёме-передаче аналогового радиосигнала на различных высоких частотах. Сегодня мобильные телефоны работают в системе GSM, которая действует по следующему принципу на частотах в 850МГц, 900МГц, 1800МГц, 1900МГц.

Сотовые телефоны имеют идентификаторы состоящие из 15 цифр, где в первых восьми цифрах зашифрована модель телефона и место где его выпустили. Оставшиеся семь цифр - это серийный номер мобильника. Для того, чтобы узнать регистрационный номер мобильного телефона, есть номер: *#06# и местонахождение легко вычислить при первой же активности.

Сейчас популярность набирают смартфоны и коммуникаторы, на базе полноценных операционных систем (Android, Windows Mobile, Symbian OS, Apple iOS и др.). Эти системы имеют открытый код, что позволяет разрабатывать множество приложений. В мобильных телефонах операционная система тоже есть, но она закрытая. Также смартфоны и коммуникаторы выделяются наличием многозадачности, лучшей «начинкой», умением работать с различным типом документов, наличием хорошей камеры и в большинстве случаев сенсорного экрана. Наиболее крупными компаниями в этой отрасли являются Apple, HTC, Samsung и др.

Науковий керівник - Труш О.І., канд. техн. наук, доцент

УДК 004.415(043.2)

Іванілов Д.В.
Національний авіаційний університет, Київ

ЗАДАЧА ПОШУКУ ШЛЯХУ В СЕРЕДОВИЩІ UNITY 3D

Задача пошуку шляху на заданому середовищі є однією з класичних обчислювальних задач. Пошук шляху на початку активного застосування потужних програмних оболонок (до 90-х років) засновувався на поділі простору на «клітинки» й хвильовому алгоритмі пошуку. Наступний етап (1990-2004) характеризувався створенням графів на т.н. «точках шляху» й пошуку шляху алгоритмом Дейкстри. Третій етап (2004-2008) – простір, як і у першому етапі, поділявся на «клітинки» або «шестикутники», але пошук йшов за допомогою алгоритму A* (A-star). Орієнтовно з 2008 р. по сьогодення в розробках активно використовується так званий «багатокутник шляху» (англ. Pathfinding mesh). Кожен з цих підходів має певні переваги, недоліки та умови ефективного використання. У даній роботі розглядається підхід до вирішення задачі пошуку шляху у середовищі Unity 3D на основі існуючих методів з застосуванням переваг й взяттям до уваги недоліків останніх.

Задача пошуку в запропонованому методі виконується у наступні етапи:

1. Створюється граф на основі поділу простору на «клітинки» зі змінною відстанню, що надає йому гнучкості й точності в поєднанні з простотою реалізацій
2. До оцифрованого простору застосовується алгоритм A* з модифікацією на пошук «фаворитних точок».
3. Отриманний шлях скорочується до оптимального

Такий підхід поєднує простоту та високу швидкодію, що забезпечуєтсья алгоритмом A*, з гнучкою системою розміщення «точок шляху», що дозволяє підвищити точність розрахунку. Окремою частиною підходу є включення до методу "пам'яті" на простір й пройдені шляхи. Це дозволяє швидше розраховувати нові шляхи та знаходження останніх в середовищі з неоднаковою швидкістю переміщення та із статичними/динамічними перешкодами.

Специфічною рисою Unity 3D є поєднання з середою програмування Mono й компілює створений у ньому код одразу після збереження, а також дає останньому доступ до фізичної бібліотеки PhysX 11, що дозволяє моделювати фізичне середовище з високим рівнем реалістичності. До її переваг можна також віднести зручну систему відладки та обширну документацію.

Алгоритми на основі розробленого методу можуть бути у широкому спектрі галузей інформаційних технологій - будь то програми-симулятори біологічних видів, програми створення транспортних шляхів, програми-будівельники та ін. і давати результат необхідної точності за короткий час.

Науковий керівник - Болдаков О.І., канд. техн. наук, доцент

УДК 004.652.3(043.2)

Коваленко Б.О.
Київський національний університет будівництва і архітектури, Київ

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Інформаці́йні техноло́гії, ІТ, інформаційно-комунікаційні технології — сукупність методів, виробничих процесів і програмно-технічних засобів, інтегрованих з метою збирання, опрацювання, зберігання, розповсюдження, показу і використання інформації в інтересах її користувачів.

Це технології, що забезпечують та підтримують інформаційні процеси, тобто процеси пошуку, збору, передачі, збереження, накопичення, тиражування інформації та процедури доступу до неї.

Початок розвитку — з 1960-их років XX століття, разом з появою і розвитком перших інформаційних систем.

Інвестиції в інфраструктуру та сервіси Інтернету викликали бурхливе зростання галузі ІТ в кінці 1990-х років XX століття.

Основоположником ІТ в Україні й у колишньому Радянському Союзі став В. М. Глушков засновник всесвітньовідомого Інституту кібернетики НАН України.

В теперішній час інформаційні технології впроваджуються на багатьох підприємствах, організаціях та різних органах влади. Розроблені концепції впровадження ІТ в наукові заклади, фабрики тощо. Наприклад Концепція впровадження інформаційних технологій у законодавчих органах влади передбачає як автоматизацію самого процесу, так і аналізу роботи, налагодження спілкуванням між різними органами влади та населенням.

Україна за рівнем розвитку інформаційних технологій у світі посідає місце в першій сотні країн. Такі дані оприлюднила міжнародна громадська організація Всесвітній економічний форум у своїй шостій щорічній доповіді. Єдина конкурентна перевага, яку має наша країна в цьому аспекті, це традиційно сильні ІТ-кадри, тобто в Україні дуже високий рівень підготовки програмістів. Україна є одним зі світових центрів офшорного програмування.

В лютому 2012 року відбулась робоча зустріч Прем'єр-міністра України Миколи Азарова з керівниками навчальних закладів України, представниками галузевих асоціацій і провідних ІТ-компаній України. Нарада була присвячена питанням розвитку інформаційних технологій в Україну та освіти в сфері ІТ.

У рамках зустрічі обговорювалися такі актуальні питання, як рівень та якість підготовки фахівців в сфері інформаційних технологій вищими навчальними закладами України, відповідність цього рівня потребам часу.

Прем'єр міністр звернув увагу на те, що студенти повинні бути підготовлені до реалій сучасного життя. "Це вимагає дуже серйозного поліпшення рівня підготовки фахівців. Нам не потрібні просто фахівці з папірцем в кишені – вони тільки створюють проблему для країни". що визначає питання якості підготовки кадрів є дуже актуальними для нашої країни.

Науковий керівник - Труш О.І., канд. техн. наук, доцент

УДК 004.652.3(043.2)

Мельник І.М.
Київський національний університет будівництва і архітектури

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В НАВЧАННІ

Кожен день користувачі використовують інформаційні технології для різних цілей. Комп'ютери стають все більш доступними, крім того, вони продовжують ставати більш потужними в процесі обробки та захисту інформації і більш простими у використанні. Велику роль інформаційні технології відіграють у навчанні.

Взагалі технологія це наука про способи розв'язання задач людства за допомогою технічних засобів. Це використання наукових знань для створення матеріальних об'єктів, полегшення праці та поліпшення умов життя людини.

Інформаційні технології — сукупність методів, виробничих і програмно-технологічних засобів, об'єднаних у технологічний ланцюжок, що забезпечує збирання, зберігання, обробку, висновок і поширення інформації, тпризначені для зниження трудомісткості процесів використання інформаційних ресурсів.

В отриманні знань книга завжди залишається основою всіх видів навчання. Але інформаційна революція внесла істотні корективи. Широке розповсюдження персональних комп'ютерів і створення глобальної мережі Інтернет створило абсолютно нові можливості в системі освіти - від шкільного до вищого спеціального. Інформаційні технології грають одну із найважливіших ролей в процесі навчання. Вони здатні об'єднати праці і здібності кращих викладачів і лекторів. Користувачі мають можливість вивчати їх в інтерактивному режимі.

Інформаційні ресурси мережі Інтернет містять текстовий, аудіо- і відеоматеріал за різноманітною тематикою на різних мовах. Однак для того,щоб користувачі не захлинулись в безлічі інформації різного змісту та різної якості, а найбільш продуктивно використовували її для своїх освітніх та професійних потреб, з явилась необхідність в розробці спеціальних учбових Інтернет-ресурсів, що націлені на навчання працювати з ресурсами всесвітньої мережі. До таких ресурсів відносять хот лист, мультимедіа скрепбук, трежа хант, сабджект семпла, вебквест. Ці інтернет-ресурси створюються винятково для навчальних цілей. Вони можуть бути розроблені по різним предметам.

Завдяки інформаційним технологіям існує доступ до інтерактивних навчальних програм, завдяки яким користувач може пізнати глибше і ширше інформацію. Існує багато онлайн довідників, перекладачів та калькуляторів, задяки яким можна виконувати різні навчальні завдання та робити перевірку.

Сучасні інформаційні технології відкривають користувачам доступ до нетрадиційних джерел інформації, підвищують ефективність самостійної роботи, дозволяють реалізувати принципово нові форми і методи навчання. Інформаційні технології стали невід'ємною частиною навчального процесу.

Науковий керівник - Труш О.І., канд. техн. наук, доцент

УДК 004.652.3(043.2)

Сыч В.В.
Национальный авиационный университет, Киев

РЕШЕНИЕ ЗАДАЧ ЛИНЕЙНОЙ АЛГЕБРЫ И ПРЕОБРАЗОВАНИЙ ФУРЬЕ НА GPU

Технология CUDA — это программно-аппаратная вычислительная архитектура NVIDIA, основанная на расширении языка Си, которая даёт возможность организации доступа к набору инструкций графического ускорителя и управления его памятью при организации параллельных вычислений. CUDA помогает реализовывать алгоритмы, выполнимые на графических процессорах видеоускорителей GeForce восьмого поколения и старше (серии GeForce 8, GeForce 9, GeForce 200), а также Quadro и Tesla.

Для решения задач линейной алгебры была создана библиотека CUBLAS. Это переведённые на язык CUDA стандартные алгоритмы линейной алгебры, на данный момент поддерживается только определённый набор основных функций CUBLAS. Библиотеку очень легко использовать: нужно создать матрицу и векторные объекты в памяти видеокарты, заполнить их данными, вызвать требуемые функции CUBLAS, и загрузить результаты из видеопамяти обратно в системную. CUBLAS содержит специальные функции для создания и уничтожения объектов в памяти GPU, а также для чтения и записи данных в эту память. Поддерживаемые функции BLAS: уровни 1, 2 и 3 для действительных чисел, уровень 1 для комплексных. Уровень 1 — это векторно-векторные операции, уровень 2 — векторно-матричные операции, уровень 3 — матрично-матричные операции.

Библиотека быстрого преобразования Фурье CUFFT — широко используемой и очень важной при анализе сигналов, фильтрации и т.п. CUFFT предоставляет простой интерфейс для эффективного вычисления FFT на видеочипах производства NVIDIA без необходимости в разработке собственного варианта FFT для GPU. CUDA вариант FFT поддерживает 1D, 2D, и 3D преобразования комплексных и действительных данных, пакетное исполнение для нескольких 1D трансформаций в параллели, размеры 2D и 3D трансформаций могут быть в от 2 до 16384 элементов, для 1D поддерживается размер до 8 миллионов элементов.

На сегодняшний день продажи CUDA процессоров достигли до 130 миллионов. Тысячи разработчиков программного обеспечения, ученых и исследователей широко используют CUDA в различных областях, включая обработку видео, вычислительную биологию и химию, моделирование динамики жидкостей, электромагнитных взаимодействий, восстановление изображений, полученных путем компьютерной томографии,информационных технологиях проектирования в сейсмический анализ, трассировку луча и многое другое.

Научный руководитель - Труш А.И., канд. техн. наук, доцент

УДК 004.45:004.51(043.2)

Шеневідько О.Л.
Национальный авиационный университет, Киев

WINDOWS 8 , MODERN ИНТЕРФЕЙС

Windows 8 — операционная система, принадлежащая к семейству ОС Microsoft Windows, в линейке следующая за Windows 7 и разработанная транснациональной корпорацией Microsoft. и ее отличие в использувании Modern интерфейс, который заменяют меню пуск. Так как статистика показала, что большинство пользователей используют пуск только ради поиска (searchbox) и они решили сделать superbar + searchbox.

Новый Modern интерфейс состоит из Тайлов. Тайлы — инновационная идея, которую не побоялись продемонстрировать в новой операционной системе.

Тайлы — это виджеты-ярлыки, разрешающие приложению показывать на его усмотрение самую важную для вас информацию. Это естественная эволюция ярлыков — статичных картинок с ссылкой.

Modern интерфейс занимает отдельно весь экран и работает отдельно от рабочего стола. Тайлы можно группировать и имеют горизонтальный скролинг.
Тайлы имеют два вида отображение по размеру и движению. По размеру они могут занимать 1 колонку или 2, и могут быть динамичными и статическими .

Modern UI имеет свой магазин приложений и отельные приложение, которые работают только в нем. Это связано с работой Windows 8 и на планшетах.
Новый поиск стал более эффективным, так как группированные результаты по приложениям, настройкам, документам и что не мало важно — в любом установленном метро-приложении. Так же можно закреплять на начальном экране любой файл, что позволяет эффективно использовать как barmenu

Новое вплывающее меню при наведении мышкой в правый нижний угол, показывает время, дату состояние сети, а так же кнопку пуска, поиск, общий доступ и подключение устройства.

Панель задач — это статусная строка, которая показывает время, основные параметры, запущенные, либо закреплённые приложения, в отличии от Windows 7, в качестве альтернативы, пользователям в Modern и обычном режиме предложена усечённая копия панели задач, всплывающая по наведению курсора.

Особенность Winodws 8, что она оптимизирована под планшеты, на малочастотных процессорах и применяется на устаревших комплектующих

Проблема Windows 8 в том, что получается два рабочих стола, две панели задач, две панели задач, что и делает систему более громоздкой. Простые действия которые занимали два клика мышкой в Windows 7, в Windows 8 требует больше действий. При введении Modern интерфейса, появилось и новый вид разработки программ, так званный «Магазин Windows», теперь на 1 приложение может быть две программы основная, и магазинная.

Научный руководитель - Труш А.И., канд. техн. наук, доцент

УДК 004.652.3 (043.2)

Яворський М.В.
Київський національний університет будівництва та архітектури, Київ

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ОБРОБКИ ДАНИХ

В нашому сучасному світі найбільш цінним ресурсом є інформація. Людський мозок протягом життя засвоює приблизно 150 трилiонів біт інформації. І цей ресурс є настільки невичерпним, багатомірним, багатогранним, всеоб'ємним, що для його контролю та використання людина, в усі часи створення спеціальних структур з метою моніторингу інформації (АНБ). З плином часу користувачі потребувала збільшення кількості обробляємої інформації і ці засоби розвивалися, вдосконалювалися, систематизувалися і нарешті були об'єднані в одну систему, яку пізніше назвали інформаційні технології.

Інформаційні технології охоплюють всі області створення, передачі, зберігання та сприйняття інформації. Вони покликані вирішувати задачі з ефективної організації інформаційного процесу для зниження витрат часу, праці, енергії та матеріальних ресурсів у всіх сферах людського життя та сучасного суспільства. Інформаційні технології взаємодіють і є основною частиною сфери послуг, керування, виробництва, соціальних процесів.

При цьому інформаційні технології часто асоціюють саме з комп'ютерними технологіями, і це не випадково, адже саме поява комп'ютерів вивела інформаційні технології на якісно новий рівень. Як приклад інформаційних технологій можна навести автоматизоване проектування, автоматизоване управління і т.ін. Зазвичай інформаційні технології реалізуються з використанням засобів обчислювальної техніки, що забезпечують високу швидкість обробки даних, швидкий пошук інформації, розосередження даних, доступ до джерел інформації незалежно від місця їх розташування.

Головною сучасною задачею, яка стоїть перед ІТ, є не тільки обробка документів, але і створення, обробка та передача нових форм представлення знань, орієнтованих на вирішення різноманітних проблем.

ІТ дозволяють об'єднувати і споживачів, і інформаційний ресурс таким чином, щоб ті суб'єкти інформаційного процесу, які потребують допомоги, легко знаходили тих, хто зможе її надати. Частково ця задача реалізована в архітектурі супермагістралі Internet та глобальних мережах (BitNet, CompuServe та інших).

Внаслідок глобальної інформатизації суспільства відбуваються нові геополітичні процеси, які активізують розвиток таких інформаційних технологій, як робота із сховищами даних, WAP-технології, IP-телефонія, нові принципи побудови дисплеїв, , виникнення дата-центрів, дистанційна освіта.

Науковий керівник - Труш О.І., канд. техн. наук, доцент

ІНФОРМАЦІЙНІ УПРАВЛЯЮЧІ СИСТЕМИ ТА ТЕХНОЛОГІЇ

УДК 351.814.331:519.711.3 (043.2)

Водопьянов С.В.
Национальный авиационный университет, Киев

СТАБИЛИЗАЦИЯ ПРОЦЕССА ВЫБОРА ОПТИМАЛЬНОЙ ТОПОЛОГИИ СЕТИ МЕТОДОМ АНАЛИЗА ИЕРАРХИЙ

В перспективных корпоративных сетях систем УВД должна обеспечиваться поддержка всего спектра услуг, как на уровне транспортных сетей, так и на уровне сетей доступа для терминалов, находящихся в распоряжении оператора. По заявкам клиентов необходимо быстро и без остановки работы системы организовывать и/или модифицировать индивидуальные наборы услуг, в том числе и дополнительные виды обслуживания.

Вследствие многофункциональности систем ОВД возникает проблема многокритериальности оценки её эффективности. Для систематизации критериев, выбора иерархии приоритетов целесообразно применять методы скаляризации вектора показателей, в частности, метод анализ иерархий Саати [1], как наиболее простой и универсальный. Устойчивость решения оптимизационной задачи обеспечивается наличием случайных составляющих различной природы в матрице приоритетов. Они играют роль стабилизаторов решения задачи выбора иерархий, которая относится к задачам на собственные значения матрицы. В табл. 1 приведены элементы матрицы парных сравнений для критериев, по которым определяется наиболее важный критерий.

Таблица 1

Номер параметра a_i	I	II	III	IV	W_i	X_i
I	1	3	5	1/3	1,495	0,306
II	1/3	1	1/3	1/3	0,439	0,090
III	1/5	3	1	1/3	0,669	0,137
IV	3	3	3	1	2,280	0,467
Сумма (Y_j)	4,533	10,000	9,333	2,000	4,882	1
$(L_{max})_j$	1,388	0,899	1,278	0,934		

Здесь $W_i=a_i/(a_1+ a_2+...+ a_n)$ – веса, которыми определяется относительная важность параметра, а $X_i=(i*a_{i2}*...*a_{in})*(1/n)$ – оценки компонентов вектора собственных значений.

Для обеспечения устойчивости решений предлагается вводить в значения величин парных сравнений малые возмущения случайного характера. При этом матрица парных сравнений перестает быть строго обратно-симметричной и, соответственно, ее определитель становится не равным нулю.

Научный руководитель – Виноградов Н.А., д-р техн. наук, профессор

УДК 004.73(043.2)

Іванілов Д.О.
Національний авіаційний університет, Київ

ПОРІВНЯЛЬНИЙ АНАЛІЗ ЗАГРОЗ ПРИ АТАКАХ DDOS ТА BOTNET

Мережна безпека існує з того самого часу, коли технологія Інтернет отримала комерційний статус. Розглянемо два найбільш вживаних метода мережних атак – *DDoS* та *BotNet*.

DoS-атака (англ. *Denial of Service*) – це атака на ресурс з метою припинення його дії. Зазвичай, при відправленні запиту на сайт після *DoS*-атаки, користувач бачить на екрані помилки 404 (не знайдено сторінку) та 503 (сервіс тимчасово недоступний). Атаки поділяються на «зламування» сайту (відправка запиту неправильного виду, що призводить до критичної помилки і видає зловмиснику повні дані ресурсу), недостатню перевірку даних користувача, атаку другого роду (фальшива атака для спрацювання системи безпеки) і, найчастіше, затоплення (перенавантаження ресурсу безглуздими запитами). Якщо атака ведеться з декількох машин, то її називають *DDoS* (англ. *Distributed Denial of Service*). Найпростіший метод навантажити цільову систему – пінг-запити (запит, що одразу ж відправляється сервером відправнику, показує користувачеві час затримки між відправленням й прийняттям відповіді).

Логічним продовженням розвитку *DDoS* став *BotNet* (англ. *roBot Network*) – та сама технологія, тільки замість користувачів, що свідомо причиняють шкоду ресурсу, використовуються комп'ютери людей, що можуть і не здогадуватись про свою роль у атаці. Останнім на комп'ютер за допомогою віруса-троянa заноситься програма-бот, що активується за «окликом» зловмисника і непомітно від користувача посилає запити на цільову сторінку. Середня мережа інфікованих комп'ютерів складає десятки тисяч машин, найбільша зареєстрована – понад 12 мільйонів. Понад 80% світового трафіка спам-листів складає листування машин у *BotNet*'і заданою рекламою на випадкові адреси.

Ефективних методів протидії мільйонам користувачів, що одночасно відсилають запити на один й той самий ресурс, за визначенням не може існувати. Проте це не означає, що кожен атакований *DDoS*'ом чи *BotNet*'ом сайт неодмінно «рухне». Найбільш ефективними методами протидії атакам на сьогодні є: 1)поширення пропускної здатності каналу; 2) приєднання додаткових ресурсів (підключення додаткових серверів для обробки запитів); 3) перенаправлення трафіка на інші сервери за домовленістю; 4) встановлення програмного фільтру на певні види запитів та контратаки по цільових ресурсах атакуючих.

Деякі ресурси мають імунітет до такого роду злочину, бо вони заздалегідь розраховані на велику кількість відвідувачів, або не мають прямого виходу до мережі й працюють через так звані проксі-сервери. Підприємствами з виробництва мережного обладнання йде розробка апаратних засобів протидії атакам, але поки що жоден з винаходів не отримав необхідної підтримки з боку потенційних користувачів.

Науковий керівник – Віноградов М.А., д-р техн. наук, професор

УДК 004.73(043.2)

Модэнов С.Ю.
Национальный авиационный университет, Киев

МЕТОДЫ ДИСТАНЦИОННОГО УПРАВЛЕНИЯ МОБИЛЬНЫМИ ТЕРМИНАЛАМИ

В настоящее время все шире применяются методы дистанционного управления компьютером с помощью мобильных терминалов. Функции управления реализуются через беспроводные сети *Wi-fi* или *Bluetooth* в ручном и автоматическом режиме. Также существуют программы для создания пультов управления, предназначенных для «телефонного контроля». Они основаны на использовании «горячих клавиш», позволяют программировать собственные пульты управления и имеют систему поддержки пользователей.

Наибольший интерес представляют следующие сервисные функции.

Basic Input – выполняет функцию удалённого тачпада

File Manager – позволяет открывать компьютер и просматривать его содержимое.

Keyboard – виртуальная клавиатура

Power – операции с питанием компьютера (выключение, перезагрузка и др.)

Slide Show – для управления мультимедийными презентациями.

Start – позволяет получить доступ к программам, расположенным в меню «Пуск»-> «Все программы»

Task Manager – выводит на экран список выполняемых программ из диспетчера задач.

Windows Media Center – пульт управления *Windows Media Center*.

Windows Media Player – пульт управления *Windows Media Player*.

В настройках можно выставить несколько пультов для быстрого переключения между ними: *Preferences* → «*Quick Switch*».

Соединение по *Bluetooth* к компьютеру более удобно в настройке, но дальность действия и стабильность сигнала не так велики, как по *Wi-fi*. По *Wi-fi* можно добиться уверенной передачи сигнала, если завязать подключение на точку доступа или уже имеющуюся локальную *Wi-fi* сеть. В случае наличия и *Wi-fi* и *Bluetooth*, при выходе из зоны действия блютуза вы сможете сменить соединение на *Wi-fi*.

Важной проблемой является обеспечение надежной, а главное – безопасной связи с компьютером. Для решения этой проблемы в первую очередь необходимо реализовать такие функции управления, как авторизация и аутентификация. Второй, не менее важной проблемой является аппаратная реализация метода. Для этого необходимо согласовывать требования к оборудованию объекта управления (удаленного терминала) и управляющего устройства (мобильного терминала). Эта задача, по существу, представляет собой задачу управления, оптимального по быстродействию, и может решаться методами общей теории управления с учетом специфики рассматриваемой задачи.

Научный руководитель – Виноградов Н.А., д-р техн. наук, профессор

УДК 004.7(043.2)

Савченко А.С.
Національний авіаційний університет, Київ

ЯКІСТЬ ОБСЛУГОВУВАННЯ В ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ

Невід'ємною частиною підприємства (установи, організації) будь-якої галузі є сучасні інфокомунікаційні технології, які надають транспорт для передачі інформації. Якість функціонування транспортної системи залежить від розвиненості механізмів управління мережею. Сучасні системи управління (СУ) телекомунікаційною мережею (*HP OpenVieW*, *IBM Tivoli*, *Naumen*) дозволяють адміністратору мережі виконувати такі важливі функції як: моніторинг стану мережі, конфігурування окремих мережних вузлів з метою підвищення надійності роботи мережі та оптимізації мережевого трафіку, сегментування завантажених ділянок, складання статистичних звітів.

Аналіз станів мережного середовища ґрунтується на таких інтегральних показниках якості функціонування телекомунікаційної мережі як:

• кількість втрачених пакетів – для *TCP* мережі 1–5% втрачених пакетів, згідно з експертними оцінками, знаходиться в межах норми; 40% втрачених пакетів – граничне значення, при якому мережа практично не працює;

• кількість пакетів, переданих з помилками;

• час затримки доставки пакетів;

• варіація затримки доставки пакетів (джиттер) – особливо важлива для мультимедійних додатків.

Незважаючи на наявні в розпорядженні адміністратора потужні сучасні засоби управління, процес адміністрування залишається трудомістким та складним і багато в чому залежить від інтуїції та досвіду адміністратора. Для підвищення якості управління, пропонується до складу СУ телекомунікаційною мережею інтегрувати елементи штучного інтелекту, наприклад використовувати концепцію «оптимального адміністратора».

СУ мережею повинна швидко реагувати на збої в роботі мережного обладнання та приймати рішення з управління. Досягнення цієї мети можливе за рахунок розподіленої ієрархічної структури. Перший рівень складається з статичних інтелектуальних агентів, розподілених по вузлах мережі. Завдання цього рівня полягає в аналізі станів вузлів та видачі результату цього аналізу другому рівню ієрархії, що дозволяє скоротити службовий трафік. Завдання другого рівня – збір інформації про стан мережі в цілому і прийняття оптимального рішення щодо управління.

Запропонована архітектура СУ дозволяє підвищити надійність та ефективність роботи, як окремих об'єктів комп'ютерної мережі, так і всієї структури в цілому. Крім того, за рахунок прогнозування стану мережі та аналізу ефективності роботи адміністратора можна запобігти появі критичних станів мережі в майбутньому.

Науковий консультант – Віноградов М.А., д-р техн. наук, професор

УДК 004.73(043.2)

Скрипниченко А.А.
Национальный авиационный университет, Киев

МЕТОДЫ СТАТИСТИЧЕСКОГО СИНТЕЗА ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ СИСТЕМ В УСЛОВИЯХ АПРИОРНОЙ НЕОПРЕДЕЛЕННОСТИ

В процессе создания информационно-коммуникационных систем и сетей необходимо учитывать множество различных условий оптимизации. Часто в качестве критерия оптимизации компьютерной сети выбирают стоимость, а такие критерии, как среднее время задержки передачи сообщений, надежность и т.д., используют в качестве ограничений. Но для сетей масштаба мегаполиса или крупной корпорации данный подход не может дать оптимального решения, т.к. при эксплуатации и модернизации возникают отказы элементов и сбои в работе. Поэтому для таких сетей необходимо учитывать и ряд других критериев: производительность, надежность и безопасность, расширяемость и масштабируемость, прозрачность и безопасность, гибкость и поддержка разных видов трафика, управляемость и совместимость. Среди условий оптимизации и принятия концептуальных проектных решений в формальном отношении иногда предлагают выделить следующие разновидности: условия полной определенности, вероятностно-определенные и условия неопределенности [1]. Эффективнее деление на параметрическую и непараметрическую неопределенность [2]. В первом случае можно сделать предположения об априорных параметрах и параметрах наблюдения (например, статистика сетевого трафика, в частности, степень его самоподобия). Круг априорных распределений сводится к не экспоненциальному семейству (распределениям с «тяжелыми» хвостами). При этом широко применяется байесовский подход. При непараметрической неопределенности приходится задаваться наименее благоприятными распределениями типа распределений с максимальной энтропией и получать некие асимптотические оценки ожидаемой эффективности. Для синтеза системы с оптимальной структурой можно применять минимаксный или адаптивный байесовский подход. Выбор того или иного конкретного метода зависит не только от масштаба информационной системы, но и от круга решаемых с ее помощью задач.

Список литературы:

1. *Сафонова И.Е.* Методы формирования и принятия проектных решений в системах автоматизированного проектирования корпоративных компьютерных сетей / И.Е.Сафонова // Известия высших учебных заведений. Поволжский регион. Технические науки. Информатика, вычислительная техника.– 2008.–№ 4.–С.41-49.
2. *Репин В.Г.* Статистический синтез при априорной неопределенности и адаптация информационных систем / В.Г.Репин, Г.П.Тартаковский. – М.: Сов. радио, 1977. – 432 с.

Научный руководитель – Виноградов Н.А., д-р техн. наук, профессор

УДК 351.814.331:519.711.3 (043.2)

Станко П.А.
Национальный авиационный университет, Киев

МАТРИЦА КЛЮЧЕВЫХ ПОКАЗАТЕЛЕЙ ФУНКЦИОНИРОВАНИЯ ОПЕРАЦИОННЫХ СИСТЕМ РЕАЛЬНОГО ВРЕМЕНИ

При оптимизации операционных систем реального времени (ОС РВ) в состав целевой функции входит большое количество основных и дополнительных параметров, от которых зависят ключевые показатели качества сервиса *KQIs*. Оптимизируемыми параметрами задачи являются следующие: оценки топологической и информационной сложности программ c_{ti}; оценки надежности программных систем c_r; оценки производительности ПО c_{sr}; оценки уровня языковых средств c_{ll}; оценки трудности восприятия и понимания программных текстов c_{per}; оценки производительности труда программистов c_{lp}; метрика размера программы по Холстеду c_{sz}; цикломатическое число Маккейба c_M; сетевые программные ошибки c_{ne}. В табл. 1 приведены коэффициенты корреляции параметров оптимизации для гипотетической ОС РВ. Данные для расчета взяты из работы [1]. Для расчетов использовалась стандартная программа множественного корреляционного анализа, приведенная в [2].

Таблица 1

Параметр	Коэффициенты корреляции									
c_{ti}		1,0								
c_r		0,76	1,0							
c_{ll}		0,52	0,47	1,0						
c_{sr}		0,77	0,54	0,39	1,0					
c_{per}		0,34	0,28	0,55	0,77	1,0				
c_{lp}		0,72	0,91	0,22	0,78	0,46	1,0			
c_{sz}		0,38	0,88	0,75	0,72	0,63	0,56	1,0		
c_M		0,21	0,19	0,27	0,57	0,41	0,40	0,21	1,0	
c_{ne}		0,88	0,91	0,92	0,77	0,66	0,75	0,82	0,46	1,0
		c_{ti}	c_{ti}	c_{ti}	c_{ti}	c_{ti}	c_{ti}	c_{ti}	c_{ti}	c_{ti}

Анализ корреляции между основными ключевыми параметрами необходимо проводить с учетом как статистических данных, так и физической природы возникающих ошибок. Результаты корреляционного анализа служат также ключевым индикатором мониторинга и регулирования потоковых данных в ОС РВ. Это необходимо для обеспечения своевременного обмена данными, прогнозирования и предотвращения перегрузок контролируемого сегмента ОС фрагмента. Таким образом, текущий мониторинг и управление уровнем эффективности работы ОС РВ является неотъемлемой частью задачи общего управления качеством сервиса *KQIs*.

Список литературы:

1. *Kreher R.* UMTS Performance Measurement: A Practical Guide to KPIs for the UTRAN Environment. - John Wiley & Sons, Ltd, 2006. – 227 pp.

2. Библиотека численного анализа НИВЦ МГУ. Режим доступа: http://www.srcc.msu.su/num_anal/lib_na/libnal.htm

Научный руководитель – Виноградов Н.А., д-р техн. наук, профессор

УДК 004.73(043.2)

Шевчук Е.И., Каспаревич А.А.
Национальный авиационный университет, Киев

АЛГОРИТМЫ ОПРЕДЕЛЕНИЯ ОРИЕНТАЦИИ КОСМИЧЕСКОГО АППАРАТА С ПОМОЩЬЮ ЗВЕЗДНОГО ДАТЧИКА

В наше время актуальна тема космоса и ориентации в космическом пространстве. Для этого применяются звездные датчики, которые используют программное обеспечение, идентифицирующее сегменты звездного пространства.

Для ориентации КА используется снимок звездного неба. На нем распознаются звездные объекты и их параметры. Данные сравниваются со звездным каталогом и, таким образом, находится месторасположение КА.

Для обработки изображений был разработан алгоритм сканирования двумя окнами с целью упрощения распознавания звездоподобных объектов.

Рассматриваются области для распознавания от маленьких к большим, постепенно получая данные про объект. Организуется проверка на цвет. В результате получаем набор удовлетворяющих нас пикселей, цвет которых влияет на определение звездной величины. Звездная величина – числовая характеристика объекта на небе, чаще всего звезды, которая показывает, сколько света приходит от нее в точку, где находится наблюдатель. Определяется по формуле:

$$A = -2{,}5\log I + C \ ,$$

где I – световой поток от объекта, C – константа.

Далее реализуется следующий этап алгоритма, который заключается в определении размера и координат области, соответствующей звездному объекту.

Для выполнения операций с данными используется интегральное представление изображений. Оно имеет вид матрицы, размерность которой совпадает с размерностью изображения. Элементы матрицы рассчитываются по следующей формуле:

$$L(x,y) = \sum_{i=0,\,j=0}^{i\le x,\,j\le x} I(i,j) \ ,$$

где $I(i,j)$ – яркость пикселя изображения.

По суммарной яркости окна определяется, есть там объект (его часть), или нет. Площадь объекта находится путем подсчета удовлетворяющих цветовому условию пикселей, которые расположены в пределах границ ранее полученных координат.

Обработанные данные можно использовать для получения информации о звездных объектах, которые необходимы для изучения космического пространства, как на локальном расстоянии, так и при полетах космического аппарата на дальние дистанции с целью определения его местоположения.

Научный руководитель – Опанасенко В.Н., д-р техн. наук, професор

КОМП'ЮТЕРИЗОВАНІ СИСТЕМИ УПРАВЛІННЯ

УДК 81.322.2 (043.2)

Бєляков О.О.
Національний авіаційний університет, Київ

АЛГОРИТМИ ВИЛУЧЕННЯ ЗМІСТУ З НАВЧАЛЬНИХ МАТЕРІАЛІВ, ЩО ПРЕДСТАВЛЕНІ ПРИРОДНЬОЮ МОВОЮ

Одним з найважливіших завдань сучасної науки є створення систем автоматизованої обробки інформації. Такі системи знаходять широке застосування в різних сферах діяльності людини. Вони вирішують велику кількість завдань, що включають в себе вилучення інформації, її систематизацію, сортування, обробку, перетворення та представлення у зручній для користувача формі. Через постійне збільшення потоку інформації зростає час та ресурси, які потрібні для виконання вищевказаних завдань. Це відбувається, перш за все, через те, що системи автоматизованої обробки інформації весь час стикаються з проблемою вилучення корисної інформації з суцільного потоку.

Вищевказані проблеми знаходять своє відображення і в сфері навчання. Підчас вивчення навчальних матеріалів людині доводиться самостійно вилучати з них ту інформацію, яка його цікавить на даний момент. Частіше за все доводиться вивчити весь наявний матеріал, а вже потім виділити з нього те, що потрібно. Такий підхід не є оптимальним через те, що доводиться засвоювати інформацію, яка не стосується проблеми, яка вивчається. Для підвищення оптимальності необхідно вивчати матеріал, що був відфільтрований від другорядних тем. Також потрібно розуміти, що один і той самий матеріал можливо використовувати в різному контексті. Наприклад, для його вивчення, перевірки знань матеріалу, тощо.

Все вищезгадане зумовлює потребу використання алгоритмів вилучення змісту з матеріалів, представлених природньою мовою. Вони дозволяють побудувати моделі матеріалів, які потім буде можливо обробляти за допомогою обчислювальних систем. Ці алгоритми дозволяють автоматизувати процес обробки навчальних матеріалів. Зокрема, вони дозволяють виконати авто реферування матеріалів, вилучення частин матеріалу, що мають спільний зміст та стосуються однієї теми. Також ці алгоритми дозволяють проводити аналіз змісту матеріалів, які представлені природньою мовою та робити висновки на основі результатів цього аналізу.

Вищеописані алгоритми можливо використовувати для автоматизації складання запитань до навчальних матеріалів. Це, з одного боку, полегшить процедуру перевірки знань, а з іншого – дозволить людині, що вивчає матеріал, одразу контролювати ступінь засвоєння інформації та виявляти ті теми, які вона ще недостатньо засвоїла. Така обробка не передбачає попередньої підготовки матеріалів та не потребує безпосередньої участі викладача.

Науковий керівник – Литвиненко О.Є., д-р техн. наук, професор

УДК 004.7(043.2)

Мацуєва К.А.
Національний авіаційний університет, Київ

ПРОГРАМНИЙ ЕМУЛЯТОР ДЛЯ ТЕСТУВАННЯ ПРОГРАМ В ХМАРНОМУ СЕРЕДОВИЩІ

На даний момент не існує потужної і унікальної концепції хмарних обчислень. В межах програмного емулятора для тестування програм в хмарному середовищі представлено загальний метод контролю доступу, який базується на декількох атрибутах з суб'єктами і об'єктами динамічної моделі.

Модель контролю доступу для *SaaS* повинна враховувати кілька сервіс-провайдерів, користувачів та сервіс-ресурсів. Представлена динамічна модель контролю доступу з суб'єктами і об'єктами на основі множини атрибутів (*MADAC*) для підтримки складних умов.

Політики контролю доступу у *MADAC* є ключовою технологією для здійснення динамічного контролю. Існують два основні принципи в *MADAC*: 1) Коли тільки суб'єкт і об'єкт знаходяться в одному і тому ж домені, відповідна роль суб'єкта може отримати доступ до відповідної ролі об'єкта. 2) Якщо одна роль суб'єкта SR_1 має приорітет до отримання доступу до іншої ролі об'єкту OR_1 та існують два частково впорядкованих відношення $<OR_2, OR_1>$ і $<SR_1, SR_2>$, то SR_1 має приорітет доступу до OR_2 і SR_2 має приорітет доступу до OR_1.

Ідентифікація і контроль доступу в програмному емуляторі на базі *SaaS* повинні підтримувати два інтерфейси для користувачів і постачальників SaaS для обробки кожної дії. Три шари архітектури: користувацький *SaaS* шар, шар контролю доступу і шар послуг. 1) користувацький *SaaS* шар: слід відокремити різні ролі, які виникають під час використання можливості контролю доступу. *UID* - унікальний ідентифікатор. Він складається з чотирьох елементів групи. *UID* = {*UserID*, *UserGroupID*, *UserEPID*, *PIN*}. Для того, щоб зберегти послідовність ідентифікаційної інформації, UID є єдиною ідентифікацією, яка використовується для входу з двома виразами "*Userid* + *Ename* + *password*" і "*Uid* + *password*". Інформація ролі попередньо обробляється в унікальному форматі для всіх ідентифікаційних даних. Далі дана відформатована інформація передається на другий шар. 2) шар контролю доступу: він відповідає за обробку авторизації користувачів і політику контролю; 3) *SaaS* шар постачальника послуг: коли кілька типів *SaaS* завантажені і опубліковані, даний шар показує загальний інтерфейс для шару контролю доступу. Постачальник *SaaS* відповідає тільки за послуги публікації і надання управління.

Контроль доступу приведений в якості функції ядра служби безпеки для хмарних обчислень. *MADAC* ілюструє представлення і відносини суб'єктів і об'єктів, ролей, атрибутів, навколишніх умов, домену та *SaaS*. Вирішена крок за кроком процес контролю доступу. Використовуючи модель *MADAC*, побудована загальна система контролю для тестування програм в хмарному середовищі.

Науковий керівник – Литвинов В.В., д-р техн. наук, професор

УДК 004.7(043.2)

Васильєв О.С.
Національний авіаційний університет, Київ

МЕТОДИ РОЗПІЗНАВАННЯ ПЕРЕШКОД ПРИ НАЗЕМНОМУ ПЕРЕСУВАННІ

Методи розпізнавання перешкод при наземному пересуванні передбачають використання аналітичних технологій. Це методики, які на основі деяких моделей, алгоритмів, математичних теорем дозволяють за відомими даними оцінити значення невідомих характеристик та параметрів.

Питання розпізнавання образів є актуальним останні 40 років і актуальність не зменшується до сих пір. Так при розробці програмного забезпечення для керування роботизованою технікою задача розпізнавання образів постала при розробці системи автоматичного керування.

На відміну від роботизованої техніки з використання УЗ та ІК датчиків було вирішено використовувати стандартну відеокамеру з ГЫИ-інтерфейсом під'єднання.

Так як формат кольору складається з 24 бітів, то відповідно маємо 2^{24} кольорів. Це 16 млн. кольорів. Людське око не відрізняє зовсім сусідні кольори. І навіть кольори з різницею в 10 також важко відрізнити. Тому з'являється перший параметр – чутливість.

Тут з'являється перший «підводний камінь». Наприклад, кольори #969600 і #96960A мають різницю в 10. Але це різниця фактично є синім кольором. В десятковому виді це числа 9868800 і 9868810 відповідно.

Еталон має параметри 27x54 точок. Це 1458 точок для порівняння. Оригінал має 375x300 точок. Для пошуку прямим перебиранням знадобиться приблизно 140 млн. циклів. Навіть з сучасними засобами обчислювальної техніки це досить об'ємний та громіздкий процес.

На основі проведених досліджень було зроблено наступні висновки:

1. Використання повнокольорових зображень вимагає значних об'ємів пам'яті і швидкодії.

2. Аналізуючи результат потрібно враховувати формат представлення даних #RRGGBB і виділяти переважаючий колір на даному типу зображень.

3. Визначення чутливості визначається зовнішніми умовами і експериментальним методом.

4. Крок руху частини зображення має бути більшим від одиниці – це збільшить швидкодію. Але максимальне значення необхідно налаштовувати у відповідності до зображення. В даному експерименті використовували 1/10 від зразка.

5. Пониження проценту співпадання з еталоном дає хибні результати, але дозволяє визначати зображення з деякими вадами або відмінностями.

Науковий керівник – Антонов В.К., канд. техн. наук, доцент

УДК 004.7(043.2)

Длужевський А.О., Панфьоров О.В.
Національний авіаційний університет, Київ

ПРОБЛЕМИ РОЗРОБКИ АПАРАТНО-ПРОГРАМНОГО КОМПЛЕКСУ УПРАВЛІННЯ РОБОТИЗОВАНОЮ ТЕХНІКОЮ

Кожен, хто займався або займається, робототехнікою стикався з безліччю проблем. Всі ці проблеми можна розділити на програмні та апаратні. Кожну категорію можна розділити ще на кілька побічних. Тим не менш, можна скласти список більш-менш типових проблем, які залежать від обраної конфігурації і платформи, як програмної, так і апаратної. Експериментально, на основі розроблених наборів тестів нам вдалося виявити наступні причини несправностей:

1) Середа розробки. Некоректність роботи бібліотек, проблеми при прошивці і розпізнаванні мікроконтролера. Так підключення самої отладочной плати - мікросхема RS232 виступає емулятором COM-порту, при підключенні через USB.

2) Неактуальність схем офіційних плат розширення - серійна схема доопрацьована, а у відкритому доступі знаходиться бета-версія. Саме з цієї причини драйвер двигуна за офіційною схемою відмовився працювати.

3) Посередня якість фабричних компонентів. Як приклади - сервопривід, датчики. Частина датчиків виявилися бракованими ще на етапі калібрування отриманих значень, а механіка сервоприводу взагалі виявилася не відповідною заявленим параметрам.

4) Живлення - проблема будь-яких автономних пристроїв. Перша проблема з живленням полягала в «просіданні» на старті, часом без можливості старту з місця. Виправивши це, з'явилася необхідність розділити живлення електроніки і силових вузлів, з причини перешкод з боку останніх.

5) Вібрація, зіткнення, несприятливі навколишні умови - все це призводило до нескладних, але витратних за часом процедурам обслуговування.

6) Загальний знос деталей - перший редуктор, з пластиковими шестернями, оплавився, не витримавши навантаження, на другому ж лопнули шестерні.

7) Вибір оптимального розташування датчиків. Відмовившись від саморобних інфрачервоних датчиків, з причини невеликої дальності і залежності від рівня освітлення, на користь ультразвукових постало питання визначення найбільш ефективного способу розташування датчиків. Для трьох датчиків найбільш раціональними можна вважати дві схеми - «опуклу» і «увігнуту». Нашим цілям більше відповідала «опукла» схема, тому що, незважаючи на наявність «мертвих» зон, дозволила краще реагувати на невеликі перешкоди.

8) Фільтрація значень, отриманих з датчиків. Були розглянуті наступні фільтри: ковзної середнього значення, логарифмічний середній, «спортивна» система, 10-ти кратного опитування, 5-ти кратного опитування.

Так виявилося, що шлях розробки роботизованої техніки пов'язаний з безліччю практиних рішень теоретичних задач.

Науковий керівник – Артамонов Є.Б., канд. техн. наук

УДК 81.322.2 (043.2)

Скочинський Б.Д.
Національний авіаційний університет, Київ

АВТОМАТИЗАЦІЯ ПОШУКОВИХ ЗАПИТІВ В БАЗІ ДАНИХ БІБЛІОТЕКИ КАФЕДРИ

У наш час всебічної автоматизації до роботи з базами даних залучаються співробітники, які не мають жодного уявлення про структуру, правила роботи та формування запитів навіть для тих баз даних, з якими вони працюють вже не перший рік. Тому основний тягар лягає на плечі розробника баз даних (чи програміста, який відповідає за інтерфейс доступу до бази даних).

Програміст може йти трьома шляхами при розробці інтерфейсу роботи з базами даних:

1) постійно додавати нові запити, щоб в повній мірі реалізувати потреби замовника (такий шлях найпростіший, але вимагає постійної участі в проекті);

2) підняти рівень користувача за рахунок гнучких настроювань системи і можливості формування власних запитів з використанням елементарного конструктора (нажаль, практично неможливий, у зв'язку з тим, що переважна більшість користувачів не бажає розвиватись самостійно для полегшення своєї праці);

3) підняти рівень "інтелектуальності" інтерфейсу за рахунок внесення автоматичних настроювань з мінімальним опитуванням користувача (це доволі складний шлях, але при реалізації дозволяє програмісту залишити працювати програму в автономному режимі без внесення змін доволі довгий час).

Хоча більша частина даних, які обробляються в сучасних інформаційних системах, і носить чіткий, числовий характер. Але при вирішенні проблеми перетворення запитання від кінцевого користувача в запит до баз даних, коли у запитаннях, які намагається формулювати користувач, часто присутні неточності і невизначеності, неможливо обійтися без механізму нечіткої логіки. Даний механізм дозволяє використовувати терміни "молодий", "не дуже дорого", "близько", що мають розмитий, неточний характер. Для вирішення даної задачі використовується способ генерації нових лінгвістичних термів на основі базової терм-множини, який реалізується на основі збережених процедур в межах СКБД.

Але великим недоліком нечітких запитів є відносна суб'єктивність функцій приналежності. Тому що все залежить від коректності функції приналежності. Але, за можливості включення автоматичного аналізу, можна будувати функцію приналежності в автоматичному чи напівавтоматичному режимі, коли користувачу будуть представлені основні параметри трапецеїдальних функцій, які можна розрахувати на основі вихідних даних. Тоді з'являється можливість будувати запити на основі термів, які є найбільш доречними саме для даної вибірки (так зване масштабування).

Науковий керівник – Віноградов М.А., д-р техн. наук, професор

УДК 004.7(043.2)

Говтвяниця А.А.
Національний авіаційний університет, Київ

ПРОГРАМНИЙ КОМПЛЕКС МОНІТОРИНГУ СКЛАДСЬКОЇ ДІЯЛЬНОСТІ З ВИКОРИСТАННЯМ МОБІЛЬНИХ ТЕХНОЛОГІЙ

Комплекс надає можливість моніторингу складської діяльності компанії безпосередньо самими працівниками. За допомогою даної системи, керуючий компанії зможе збирати статистичні дані про діяльність складу, трудомісткості, ефективності роботи кожного співробітника складу. Статистична інформація збирається на сервері і відображається на сайті підприємства після авторизації і перевірки рівня доступу.

Після прибуття товару на склад, працівникові складу слід запустити додаток на мобільному пристрої і натиснути на кнопку «Новий пакет», тим самим створити спеціальну область (пакети) - набір даних для відправки. Після створення такої області, користувачеві необхідно заповнити спеціальні поля для відправки (більшість полів вводяться автоматично або за допомогою розпізнавання образів (штрих-код, наприклад)).

Після заповнення полів з інформацією про що прийшла посилці, користувач зберігає область з даними і відправляє її на сервер, після чого ця інформація стає доступною для керівництва.

Головна форма програми має чотири основні функціональні кнопки (рис.1) у верхній частині вікна, поле-список зі збережених пакетів (займає іншу частину екрана), а також кнопку переходу в режим групового вибору пакетів, яка з'являється при натисканні на апаратну кнопку « Меню».

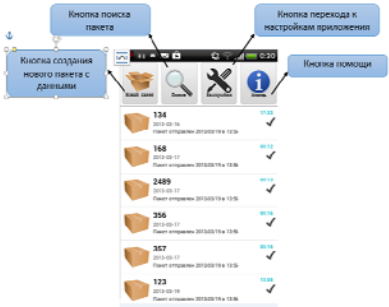


Рис.1. Вигляд главної форми на мобільному пристрої

Даний комплекс спростив обробку даних, що і стало основним економічним ефектом від його впровадження.

Науковий керівник – Артамонов Є.Б., канд. техн. наук

УДК 004.7(043.2)

Бовсунівський А.Ю.
Національний авіаційний університет, Київ

ПРОБЛЕМИ ВИКОРИСТАННЯ ПОТОКІВ В C#

Найпростішим прикладом застосування багатопоточності може слугувати інсталятор, який в одному потоці інсталює файли а в іншому показує процес виконання інсталяції та може отримувати повідомлення з клавіатури та миші. Якщо б інсталятор працював в одному потоці, операційна система позначила б його як не відповідаючий доки той не завершить свою роботу.

Приклад багатопоточності в консольному додатку:

В головному потоці створюється новий потік 't', який виконує метод, що безперервно друкує символ 'y'. Одночасно головний потік безперервно друкує символ 'x'.

Ось результат виконання програми:

xxxxxxxxxxxxxxxxxxxxxxxxxxxxyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyxxxxxxxxxxxxxxx
xxxxxxxyyyyyyyyyyyyyyyyyyyxxxxyyyyyyyyyyyyyyyyyyyyxxxxxxxxxxx...

Кожному потоку дається якийсь час на виконання і вони працюють по черзі. Однією з основних проблем в роботі з потоками являється їхня синхронізація.

Запускаючи програму, що має декілька потоків, які редагують один і той самий файл ми отримаємо ось таку помилку:

The process cannot access the file because it is being used by another process.

Проблема заключається в тому, що поки один потік працює з файлом, ніякий інший не може до нього звернутися. Як результат, тільки один потік вдало завершив роботу.

Допомогти вирішити цю проблему може оператор Lock, який блокує потрібну нам частину коду. Коли два або більше потоків одночасно борються за блокування, всі окрім одного потоку переходять в режим очікування, поки блокування не звільниться.

При запуску відредагованої програми ми отримуємо текстовий файл, в якому видно, що кожен потік виконав свою роботу вдало.

Можливі методи вирішення проблеми багатопоточності:

1) Lock - гарантує, що тільки один потік зможе отримати доступ до ресурсу або секції коду.

2) Mutex - Гарантує, що тільки один потік може отримати доступ до ресурсу або секції коду. Може використовуватись для запобігання запуску декількох екземплярів додатку.

3) Semaphore - гарантує, що не більше заданої кількості потоків може отримати доступ до ресурсу або секції коду.

Науковий керівник – Артамонов Є.Б., канд. техн. наук

КОМП'ЮТЕРНІ СИСТЕМИ ТА МЕРЕЖІ

UDK 004.7.052:004.414.2(043.2)

Lukashenko V., Voynov I.
National Aviation University, Kyiv

ANYCAST ROUTING IN DELAY TOLERANT NETWORKS

Delay Tolerant Networks (DTNs), as a class of useful but challenging networks, are receiving more and more attention. In such networks, no end-to-end contemporaneous path is guaranteed between any two nodes and message delivery can be fulfilled by leveraging nodes' movement.

Anycast is a service that allows a node to send a message to at least one, and preferably only one, of the members in a group. The idea behind anycast is that a client wants to send packets to any one of several possible servers offering a particular service or application but does not really care any specific one. Anycast can be used to implement resource discovery mechanisms which are powerful building blocks for many distributed systems, including file sharing etc.

Anycast in DTNs means that a node wants to send a message to any one of a destination group and intermediate nodes help to deliver the message by leveraging their mobility when no contemporaneous path exists between the sender node and any node of the destination group.

Anycast in the Internet and mobile ad hoc networks has been studied extensively in the past, due to the unpredictability of network connectivity and delay, and limited storage capacity, anycast in DTNs is a quite unique and challenging problem. It requires both re-definition of anycast semantics and new routing algorithms.

Moreover, in unicast in DTNs, the destination of a message is determined when it is generated, while in anycast, the destination can be any one of a group of nodes and during routing, both the path to a group member and the destination can change dynamically according to current mobile device movement situation.

In this paper, I'll also define three semantics models of anycast in DTNs, namely CM (Current Membership), TIM (Temporal Interval Membership) and TPM (Temporal Point Membership Model), which unambiguously define the intended receivers of a message in the anycast routing. Based on the model, I'm also propose a novel routing metric named EMDDA (Expected Multi-Destination Delay for Anycast) which utilizes the uncontrolled random moving characteristic of mobile devices.

References:

1) *S. Jain, K. Fall, and R. Patra*. Routing in a Delay Tolerant Network. In Proc. of the Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication, pages 145–158, Portland, OR, USA, 2004.

2) *D. Katabi and J. Wroclawski.* A Framework for Scalable Global IPAnycast (GIA). In Proc. of the Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication, Stockholm, Sweden, 2000.

UDK 004.4:0047(043.2)

Sandii I.O.
National Aviation University, Kyiv

DIGITAL SIGNAL PROCESSING OF SPECTRUM ANALYSIS

The spectrum analysis is the important field of great scientific and industrial branch named the digital signal processing (DSP). The tasks of digital signal processing are the most diverse ones and they require a certain level of performance of microelectronic components. DSP is concerned with the representation of the signals by a sequence of numbers or symbols and the processing of these signals. Since the goal of DSP is usually to measure or filter continuous real-world analog signals, the first step is usually to convert the signal from an analog to a digital form, by using an analog to digital converter. Often, the required output signal is another analog output signal, which requires a digital to analog converter. Even if this process is more complex than analog processing and has a discrete value range, the stability of digital signal processing thanks to error detection and correction and being less vulnerable to noise makes it advantageous over analog signal processing for many, though not all, applications. The advantages of parallel computing for solving problems of this kind of complexity are quite large, so to implement them in recent times it is often applied FPGA architecture. A currently observed rapid development of electronics technology is characterized by fast increasing usage of digital technologies in existing and future projects. This is due primarily to the known advantages of digital signals application: high potential noise immunity, capability of optimizing the usage of the frequency spectrum, the prospects of application in various telecommunication and information systems of universal hardware and software solutions, etc.

One of the key factors of development in this direction obviously is technological progress. The successful implementation of future development of information technology is largely based on the achievements of digital signal processing (DSP), designed to solve the problems of the reception, generation, processing and transmitting information in real time, which is especially important and often absolutely essential for digital signal analysis. The implementation of complex DSP algorithms in real time requires, in turn, the use of effective fundamental DSP algorithms (filtering, spectral analysis and synthesis of signals), which use efficiently appropriate technical resources. Thus, currently there is an urgent scientific and technical problem of improving the DSP algorithms and devices for the spectrum signal analysis.

The digital spectrum analyzers are employed in such branches as: audio and speech signal processing, sonar and radar signal processing, sensor array processing, spectrum estimation, statistical signal processing, digital image processing, signal processing for communications, biomedical signal processing, seismic data processing, etc.

Scientific supervisor – V.Y. Krakovsky, Ph.D.

УДК 004.057.4:004.715(043.2)

Журавель С.В., Боржимська Є.О.
Національний авіаційний університет, Київ

ПРОТОКОЛИ МАРШРУТИЗАЦІЇ НА ОСНОВІ АНАЛІЗУ СТАНУ КАНАЛУ

При великій кількості роутерів на підприємстві або декількох провайдерів застосування статичних маршрутів стає досить трудомістким. У цьому випадку більш практично використовувати динамічні протоколи маршрутизації. Вони автоматично обмінюються інформацією про відомі їм мережі тим самим вибираючи найкращі маршрути для своїх таблиць маршрутизації та підтримуючи їх актуальними.

В докладі розглянуті протоколи маршрутизації на основі аналізу стану каналу (link-state routing protocols), такі як протокол першого найкоротшого відкритого маршруту Open Shortest Path First (OSPF) і протокол обміну даними між проміжними системами Intermediate System-to-Intermediate System (IS-IS). Обидва протоколу підтримують мережні маски змінної довжини, можуть застосовувати мультикастову розсилку для знаходження прилеглих роутерів, використовуючи hello пакети, і можуть підтримувати аутентифікацію при оновленні маршрутів.

OSPF побудований для маршрутизації IP адрес і сам працює як протокол 3 рівня на IP, IS-IS спочатку є мережним рівнем моделі OSI. Широке впровадження IP адрес сприяло зростанню популярності OSPF. IS-IS не використовує IP адреси в якості маршрутів. Він є нейтральним відносно мережевих адрес, в той час OSPF був спроектований для IPv4. Основна відмінність OSPF і IS-IS полягає в тому як вони ділять автономну систему на зони і як здійснюється маршрутизація між зонами. Недолік IS-IS в тому, що маршрутизатори 2го рівня можуть спілкуватися тільки з такими ж маршрутизаторами, у 1го рівня - така ж ситуація. Для взаємодії між маршрутизаторами 1го та 2го рівня і відповідними зонами використовуються маршрутизатори рівня 1-2. У OSPF зони відмежовуються інтерфейсами на маршрутизаторі, таким чином прикордонний маршрутизатор (area border router, ABR) може перебувати в кількох зонах одночасно, ефективно створюючи кордони всередині себе. Тоді як кордони IS-IS зон знаходяться між маршрутизаторами рівня 2 або рівня 1-2, що робить маршрутизатор IS-IS частиною лише однієї зони. Також IS-IS не підтримує нульову зону (магістральну область, через яку може пройти весь міжобласний трафік). Логічним поясненням цього є те, що OSPF створює мережу з топологією зірка з багатьма зонами пересічними з нульовою, тоді як IS-IS створює логічну топологію з основним рівнем з маршрутизаторів 2го рівня, філій - маршрутизаторів рівня 1-2 і окремих областей з маршрутизаторів рівня 1 .

У протоколі OSPF більше розширень і додаткових функцій. Однак протокол IS-IS відправляє меншу кількість службового трафіка і може масштабуватися для великих мереж. Якщо взяти однакову кількість ресурсів, IS-IS зможе підтримувати більшу кількість маршрутизаторів в зоні аніж OSPF. Це сприяє тому, що IS-IS використовується в інтернет-провайдерів.

Науковий керівник – Мартинова О.П., канд. техн. наук, доцент

УДК 004.7(043.2)

Іваненко О.А.
Національний авіаційний університет,Київ

ТЕХНОЛОГІЯ ЗАБЕЗПЕЧЕННЯ ГАРАНТОЗДАТНОСТІ БЕЗПРОВІДНИХ МЕРЕЖ

Сучасні тенденції розвитку телекомунікацій пов'язані з появою нових послуг та сервісів, що є більш вимогливими до існуючих мереж. З кожним днем ці послуги стають більш актуальними серед користувачів. Побудова, сучасної мультисервісної бездротової мережі є дуже зручним рішенням для існуючих провайдерів, як результат - залучення ще більшої кількості абонентів.

При переході до створення систем широкосмугового радіодоступу з інтеграцією послуг стало зрозуміло, що основні принципи, закладені в бездротові системи на попередніх етапах, потребують значної корекції. На сигнальному рівні першочергове значення дістало оптимальне використання спектрального ресурсу радіоканалу при будь-яких співвідношеннях "швидкість - перешкодозахищеність". На рівні протоколів стало необхідним забезпечувати заданий рівень якості обслуговування (QoS) будь-якому абоненту мережі. З цією метою в 2004 році був розроблений стандарт IEEE 802.16-2004, що являє собою розраховану на введення в міських бездротових мережах (WirelessMAN) технологію безпровідного широкосмугового доступу операторського класу.

Для диференціації сервісу і підтримки якості обслуговування система WiMAX має спеціальний механізм, успадкований від технології ATM, званий підрівнем конвергенції ConvergentSublayer (CS). Підрівень конвергенції WiMAX являє собою програмний інтерфейс канального рівня до мережевого рівня мережі. Робота підрівня конвергенції заснована на фільтрації в загальному мережевому трафіку за спеціальними ідентифікаторами, званих класифікаторами Classifier, так званих сервісних потоків ServiceFlow (SF), с наданням кожному виділеному SF на канальному MAC рівні мережі необхідної якості обслуговування QoS.Крім ServiceFlow в WiMAXопціонально використовується поняття клас обслуговування ServiceClass (CS), що представляє собою опис використовуваного типу QoS і його параметрів (атрибутів).

Таким чином, в мережі WiMAX, по-перше, весь трафік може бути класифікований і розділений на безліч сервісних потоків SF, по-друге, для кожного сервісного потоку, обслуговуючого роботу того чи іншого додатка і / або користувача задається рівень якості QoS обслуговування з необхідними параметри каналу зв'язку.

Науковий керівник – Гузій М.М., канд. техн. наук, доцент

УДК 004.057.4:004.715(043.2)

Мартинова О.П., Битько В.В.
Національний авіаційний університет, Київ

ДОСЛІДЖЕННЯ ПРОТОКОЛІВ МІЖДОМЕННОЇ МАРШРУТИЗАЦІЇ

Інтернет – множина автономних систем (AS), кількість яких постійно збільшується. В зв'язку з цим все більш актуальним стає питання маршрутизації між цими системами та взаємодії різних протоколів маршрутизації. Від вибору протоколу залежить ефективність функціонування всієї мережі, оптимальність та стабільність її роботи. Для визначення маршруту між автономними системами використовуються принципи динамічної маршрутизації, саме вони були розглянуті в доповіді. При такій маршрутизації запити про маршрути розраховуються програмним забезпеченням пристроїв.

Однією з ключових проблем маршрутизації є те, що трафік в інформаційній мережі в значній мірі гетерогенний: по мережі передаються як різного роду дані, так і аудіо та відео в реальному часі. Це може призводити до перевантаження мереж передачі даних та маршрутизуючого обладнання і навіть до їх відмови.

Сучасний стан мереж передачі даних вимагає використання алгоритмів маршрутизації які здатні об'єктивно визначати маршрути, беручи при цьому до уваги поточну завантаженість каналів, тип трафіку, пропускну здатність і надійність каналів зв'язку.

У загальному значенні слова маршрутизація означає пересування інформації від джерела до пункту призначення через об'єднану мережу. Вона не може бути ефективною без раціонального використання наявних ресурсів - в першу чергу маршрутизаторів і каналів зв'язку. Функціонуванням протоколів маршрутизації можна вважати ефективним, коли кожен ресурс завантажений, але не перевантажений. Це означає, що коефіцієнт використання ресурсу повинен наближатися до одиниці, але не настільки, щоб черги пакетів до нього - неминуче явище в пакетних мережах - були б постійно великими, приводячи до затримок і втрат через переповнення внутрішніх буферів маршрутизаторів.

В доповіді розглядаються протоколи міждоменної маршрутизації, принципи їх роботи, критерії вибору оптимального шляху передачі даних, їх переваги та недоліки.

Рішення, які існують сьогодні в області маршрутизації дозволяють забезпечити стійке з'єднання та передачу, однак питання підвищення ефективності передачі інформації, (ефективного вибору шляхів передачі даних, перевантаженість, скорочення числа вузьких місць) залишаються, як і раніше, актуальними.

УДК 004.274 (043.2)

Пильник В.М., Тищенко І.В.
Національний авіаційний університет, Київ

СТРУКТУРНА ОРГАНІЗАЦІЯ ПРОБЛЕМНО-ОРІЄНТОВАНИХ СИСТЕМ НА ПЛІС

Проблемно-орієнтовані обчислювальні комплекси та системи призначені для розв'язання визначеного класу задач в проблемній галузі. Це об'єднання апаратних і програмних засобів універсального і спеціалізованого підходів для розв'язання задач.

Реконфігуровні комп'ютери на базі ПЛІС ефективно застосовуються в багатьох областях: реконфігуровні високопродуктивні багатопроцесорні обчислювальні системи; емуляція й проектування нових бездротових систем зв'язку; наукове обчислення в реальному масштабі часу й моделювання; спеціалізовані автономні вбудовані пристрої; кодування-декодування інформації; цифрова обробка сигналів; робототехніка й нейронні мережі; комунікаційні засоби; контролери для керування складними об'єктами.

Базовою компонентою сучасних реконфігурованих комп'ютерів є кристали FPGA. Для розробки системи за основу взято інструментальний модуль xilinx ZC702 Evaluation Board сімейства SoC Zynq-7000. Реалізована за 28-нм технологією Zynq-7000 містить 2-ядерну процесорну систему ARM Cortex-A9 MPCore, що оснащена мультимедіа-підсистемою NEON і модулем обробки операцій з плаваючою комою подвійної точності, а також кеш-пам'яттю 1-го та 2-го рівня, контролером мультистандартної памяті і широким набором периферії. Платформа Zynq-7000 EPP унікальна тим, що головна в ній – процесорна система ARM, а не програмована логіка. Це означає, що створена компанією Xilinx система забезпечує загрузку процесора за включенням живлення (до старта логіки FPGA) і запускає необхідні операційні системи незалежно від комутованої матриці програмованої логіки. Після загрузки розробники можуть запрограмувати процесорну систему, щоб при необхідності зконфігурувати програмовану логіку.

Проект розроблений засобами САПР ISE 14.4 компанії Xilinx.

Науковий керівник - Опанасенко В.М., д-р техн. наук, професор

УДК 629.735.33(043.2)

Семко О.В., Наумець М.В.
Національний авіаційний університет, Київ

СИСТЕМА ПЕРЕДАЧІ ДАНИХ В ТЕЛЕКОМУНІКАЦІЙНІЙ МЕРЕЖІ КОСМІЧНИХ АПАРАТІВ

На протязі останнього десятиріччя у світі дуже гостро постала проблема заміни стандартів передачі даних телекомунікаційного обладнання у сфері авіоніки, оскільки вони не відповідають сучасним вимогам у швидкості передачі даних.Саме ця проблема була вирішена введенням нового стандарту телекомунікацій авіаційного і космічного обладнання , який зараз носить назву SpaceWire , яка має нову, модифіковану систему передачі даних.

SpaceWire - нова телекомунікаційна мережа для космічних апаратів з пропускною здатністю до 400 Мбіт / сек , заснована на частині стандарту з'єднання IEEE 1355, вузлі якої з'єднуються за допомогою послідовніх з'єднань типу точка-точка, яка працює в повнодуплексному режимі.

Мережа SpaceWire складається, в загальному випадку, з деякого числа вузлів абонентів і мережевих вузлів - маршрутизуючих комутаторів. Вузли-абоненти мережі SpaceWire - це пристрої, передавальні і приймаючі потоки даних. Вони пов'язані з маршрутизуючим коммутатором або один з одним дуплексними каналами, званими лінками (link). Вузол оснащений одним або декількома лінк-портами і інтерфейсом з джерелом даних. Від хост-пристрою вузол приймає дані, кодує їх і відправляє в свій передавач, безпосередньо підключений до лінку. На іншому кінці лінка дані приймає приймач, який їх відновлює (декодує) і передає адресатові (іншому хост-пристрою) або на вихідний порт маршрутизуючого комутатора. Приймач і передавач з необхідними елементами управління і інтерфейсами до хост-пристрою утворюють контролер лінка SpaceWire. При надходженні заголовка пакета у вхідний порт маршрутизатора пакет відразу маршрутизується і починається наскрізна передача потоку символів пакета у вихідний порт, без проміжної буферизації і зберігання в маршрутизаторі . Таким чином, в мережевому вузлі відбувається і маршрутизація вхідного пакету, і його комутація.

Роздільне DS - кодування кожного з лінків забезпечує спрощення передачі на високих швидкостях на значні, недосяжні в паралельних шинах відстані. Крім того, це дозволяє і далі нарощувати пропускну здатність каналу SpaceWire.

Таким чином, введення такого стандарту з даною системою передачі даних потрібно впровадити в Україні , що забезпечило б позитивний результат в захисті і розвитоку галузі авіоніки і космонафтики в нашій державі.

Науковий керівник – Лукашенко В.В. канд. техн. наук, доцент

УДК 004.4:0047(043.2)

Яценко М.М., Герасімов О.С.
Національний авіаційний університет, Київ

ПРОГРАМНІ ЗАСОБИ ПРЕДСТАВЛЕННЯ СИГНАЛІВ В КОМП'ЮТЕРНІЙ МЕРЕЖІ РУХОМИХ ЕОМ

Важливою частиною комунікацій більшості сучаних компаній стали безпроводові широкосмугові мережі передачі даних. Мережеве обладнання дає змогу швидко конфігурувати локальні обчислювальні мережі в середені будівель і створювати лінії радіозв'язку з віддаленими на десятки кілометрів офісами. З їх допомогою можливо організувати міські опорні мережі зв'язку, котрі забезпечують широкосмуговий доступ до Інтернету для приватних підприємств та державних установ. На додачу вищезгаданих переваг, для безпроводових мереж розроблено ряд програмних та апаратних засобів контролю за трафіком і управління безпекою.

Розповсюдженість безпроводових технологій в наш час ставить під загрозу ті мережі, де вони вже використовуються і ті в котрих не мають застосовуватися. Традиційні засоби захисту беззахисні перед принципово новими класами безпроводових загроз. При цьому ситуація ускладнюється тим, що необхідно захищати своїх користувачів (котрі можуть бути віддаленими від офісу), непорушуючи при цьому функціонування сусідніх мереж, яким би підозрілим воно не було.

Для аналізу трафіку бепроводової комп'ютерної мережі на фізичному рівні пропонується використати програмний засіб «Тригонометрический ряд Фурье», що дає змогу аналізувати дані представлені в імпульсному вигляді. Інтерфейс програми дозволяє ввести тестову послідовність, що в подальшому використовується для розрахунку координат послідовності точок графіку моделюючої послідовності біт в беспроводовій комп'ютерній мережі. Для кодування біт використовується частотна модуляція.

Після отримання функції на попередньому етапі є можливість розкласти її в ряд Фурьє. Інтерфейс додатку дає змогу задати кількість гармонік, а також зменьшувати завантаженість графіку отриманими даними.

Таким чином з допомого розкладання функції, що описує трафік в безпроводвій комп'ютерній мережі, в класичний ряд Фурьє є можливість отримати додаткову інформацію на основі которої провести класифікацію об'єкта розпізнавання.

Науковий керівник – Печурін М.К., д-р техн. наук, професор

МАТЕМАТИКА ТА КОМП'ЮТЕРНІ ТЕХНОЛОГІЇ

UDC: 681.326(043.2)

Chervoniak E.
National Aviation University, Kyiv

GRAPHICAL COMPUTING - THE MODERN METHOD OF COST EFFECTIVE AND SUPERFAST DATA PROCESSING

Multi-core processors are no longer the future of computing – they are the present day reality. Since 2003 multicore processors, especially the GPUs, have led the race of floating-point performance. While the performance improvement of general-purpose microprocessors has slowed significantly, the GPUs have continued to improve relentlessly. As of 2009, the ratio between multicore GPUs and multicore CPUs for peak floating-point calculation throughput is about 10 to 1. So, we have the possibility to unite the performance of CPU and GPU, which will allow performing of programming operations much faster and effectively. This possibility is very important today, because it reduces the computational cost in few times.

This work is dedicated to the question of applying of parallel computing in practice. During the development of GPU programming technologies a few program environments were created, such as Open CL (Open Computing Language) – free software, which are used for creating the programs connected with the parallel computing with the help of various GPU and CPU. But I used less universal, but more convenient software – CUDA (Compute Unified Device Architecture). But it is not simply a programming environment, but rather the whole software and hardware architecture of the parallel computing. It can be applied only for GPUs of NVIDIA Company. CUDA includes a lot of additional programs, tools and so on, it uses C programming language, that makes the transfer for the programmer to CUDA technology much easier. In my work I used Microsoft Visual Studio (further MVS) as a programming environment, which supports CUDA technology. To use GPU for mathematical calculations I wrote a program. At last, it is the necessity to check the "participation" of graphical unit in calculation process. The simple software - TechPowerUp GPU-Z solves this problem. The result of an experiment is shown in my work. So, the information about the great performance of graphical processing unit and its advantages in comparison with central processing unit is actual for resource-aided computations. The ways of applying this possibility in practice are different, one of them have been described in detail. The MVS supports CUDA technology and gives the programmer a possibility to write the programs through C programming language and to perform calculations by GPU mediation. At last, the programmer can to see the GPU load with the help of special software, for example TechPowerUp GPU-Z.

Scientific adviser – Prof. Shkvar Ye.O.

UDC 532.526(043.2)

Dyagel' A., Slavinska T.
National Aviation University, Kyiv

APPLICATION OF INTEGRAL RELATIONS FOR CALCULATING THE BOUNDARY LAYER THAT DEVELOPS ALONG THE SURFACE OF THE POROUS CONICAL DIFFUSER

Taking as the initial velocity profile expression $u/u_m = \bar{y}(2-\bar{y}), \quad \bar{y} = y/\delta$, Mamchuk V. received the following relation for calculating the parameters of the boundary layer (BL):

$$z_1 = \frac{6k_1 u_m^{k_2}}{R^2}\exp\left(-3k_1\int_{x_0}^{x}\frac{u_H}{u_m^2}u_H' dx\right)\int_{x_0}^{x}\frac{R^2}{u_m^{k_2+1}}\exp\left(3k_1\int_{x_0}^{x}\frac{u_H}{u_m^2}u_H' dx\right)dx, \quad (1)$$

$$z_2 = \frac{u_m^{k_2}}{R^2}\exp\left(-3k_1\int_{x_0}^{x}\frac{u_h}{u_m^2}u_H' dx\right)\int_{x_0}^{x}\frac{2k_1(3+\theta_1)}{u_m^{k_2+1}}R^2\exp\left(3k_1\int_{x_0}^{x}\frac{u_h}{u_m^2}u_H' dx\right)dx, \quad (2)$$

where $\theta = v_0\delta/v$; $z = \delta^2/v$; stroke is a derivative of x; z_1, z_2 are respectively the first and second approximation for the existing transverse velocity component on a streamlined surface.

If we apply the expressions (1-2) in the calculation of the pancreas in porous conical diffuser ($u_m = u_H = u_в r_0^2/x^2$, where $u_в$ is a speed in the input section; r_0 is a distance from the vertex of the cone to the input section, $R = x\sin\alpha$), we can gain the expression:

$$z_1 = 4{,}39\frac{r_0}{u_в}\left(\left(\frac{x}{r_0}\right)^{8{,}86} - \left(\frac{x}{r_0}\right)^3\right)\cdot \quad (3)$$

If we limit ourself with the the first term in equation (3), then the second approximation of equation (2) we obtain:

$$z_2 = 4{,}39\frac{r_0}{u_в}\left(\left(\frac{x}{r_0}\right)^{8{,}86} - \left(\frac{x}{r_0}\right)^3\right) + 12{,}56\frac{r_0 v_0}{u_в u_в}\sqrt{\mathrm{Re}}\left(\left(\frac{x}{r_0}\right)^{8{,}86} - \left(\frac{x}{r_0}\right)^{7{,}43}\right), \quad (4)$$

where $\mathrm{Re} = \frac{u_в r_0}{v}; v_0 = \mathrm{const}$. Tension friction is determined by the formula:

$$\tau_w = \frac{\mu u_в}{\sqrt{v}x_1^2\sqrt{z_2}}\left(1{,}7143 - 0{,}4756\frac{u_в z_2}{r_0 x_1^3} - 0{,}4286\cdot v_0\sqrt{\frac{z_2}{v}}\right)\cdot \quad (5)$$

Scientific supervisor V.I.Mamchuk, associate professor

UDC 629.784(043.2)

Makarov I. A.
National Aviation University, Kyiv

MATHEMATICAL MODELING OF ROCKET LAUNCHING FROM THE BOARD OF AIRCRAFT – CARRIER

Ukraine is the space state because there are such gigants of cosmic industry as CB "Yuzhnoe" and "Yuzhmash" which not only design these launch vehicles and spaceships, but produce them at the current plant. Just due to such enterprises Ukraine takes part in many international projects as: the project of new type of engines "Vega"; "Sea launch"; with using the Ukrainian launch vehicle "Zenit – 3SL" as the main spaceship launch vehicle. To this project we can add the reproducing of intercontinental ballistic rocket "Dnepr" for launching of small spaceships and the project "Cyclone -4" together with the cosmic Brazilian agency for launching spaceships from the Alcantara start site; and many others. The idea of launching rockets from the board of the plane is not new. In the XX century the scientists of the Soviet Union and United States developed the projects on the base of different planes. But because of the numbers of risk factors any project has got its realization.

A spaceport (launching site) or cosmodrome is a site for launching (or receiving) spacecraft, by analogy with seaport for ships or airport for aircraft. The word spaceport, and even more so cosmodrome, has traditionally been used for sites capable of launching spacecraft into orbit around Earth or on interplanetary trajectories. In this work you can find absolutely new type of such construction with new meaning, and fresh ideas. The project can be applied in close time and with minimal costs in comparision with constructing of new spaceport or reconstructing old launch sites.

The goal of this research project is to elaborate the strategy for launching the space vehicle from the board of airplane.

The main purpose was to make the mathematical model, which would be able to describe the flight of the given launch vehicle after its separation from the aircraft and climbing the altitude with the following flight into space.

In the process of work on this project the following operations were done: the wing of launch vehicle was developed. It is the oval-looking wing construction with internal frame, additional external hinged ruling components as elevons, also additional ruling engines (which is mounted on the rocket frame perpendicularly to the direction of flight) and many other small components. All these elements work on the electro-distance conducting system. The whole operations of controlling of the rocket flight are done by the board calculating system (central computer).

Due to the results of the fulfilled work it was proved that the launching of the rockets from the board of the airplane is possible, and even more conveniently in comparison with fixed launch stations.

Ukraine will be able to construct its own launching site and to launch rockets from it.

Scientific supervisor E. A. Shkvar, professor

UDC 515.126(043.2)

Rybalkina T.V.
National Aviation University, Kyiv

TOPOLOGICALLY ISOMORPHIC CHAINS OF LINEAR MAPPINGS

This is a joint work with V. Sergeichuk. We consider systems of linear mappings $A_1,...,A_{t-1}$ of the form

$$\mathrm{A}:\ U_1 \overset{A_1}{-} U_2 \overset{A_2}{-} U_3 \overset{A_3}{-} \dots \overset{A_{t-1}}{-} U_t$$

in which $U_1,...,U_t$ are unitary (or Euclidean) spaces and each line is either the arrow $\rightarrow$ or the arrow $\leftarrow$. Let A be transformed to

$$\mathrm{B}:\ V_1 \overset{B_1}{-} V_2 \overset{B_2}{-} V_3 \overset{B_3}{-} \dots \overset{B_{t-1}}{-} V_t$$

(with the same orientation of arrows) by a system $\{\varphi_i : U_i \to V_i\}_{i=1}^{t}$ of bijections, that is,

$$\begin{aligned} B_i\varphi_i &= \varphi_{i+1}A_i, \quad \text{if } A_i : U_i \to U_{i+1} \\ \varphi_i A_i &= B_i\varphi_{i+1}, \quad \text{if } A_i : U_i \leftarrow U_{i+1} \end{aligned} .$$

We say that A and B are linearly isomorphic if all φ_i are linear. Considering all U_i and V_i as metric spaces, we say that A and B are topologically isomorphic if all φ_i and φ_i^{-1} are continuous.

Theorem. [2]. Two chains of linear mappings on unitary (or on Euclidean) spaces are
topologically isomorphic if and only if they are linearly isomorphic.

1. *Sergeichuk V.V.,* Computation of canonical matrices for chains and cycles of linear mappings, Linear Algebra Appl. 376 (2004) 235-263.
2. *Rybalkina T.V., Sergeichuk V.V.,* Topological classification of chains of linear mappings, Linear Algebra Appl. 437 (2012) 860-869.

UDC 371.132:656.7

Tymoshenko A.V.
Kirovograd Flight Academy of National Aviation University, Kirovograd

RESEARCH OF HYBRID SYSTEMS FOR SIMULATION OF AIR TRAFFIC FLOW

Nowadays, the problem of oversaturated air traffic flow is extremely important, because every day it becomes more difficult to control it. Existing simulation tools of the national airspace have functionality that combines runway modeling and airport capacity, but it is not enough to display the full real picture.

Hybrid (complex dynamic) systems – is the hierarchical, event-driven systems with variable structure. Complex dynamic systems are extremely in demand for practice and for their modeling in the whole world are created visual modeling software systems that include graphic language design and adjustent of models, operation of computational experiments, visualization and interactive intervention in the course of the experiment. Complex dynamic systems are highly abstract, hard for human understanding and require visualization at the stage of model's design. Today, the term of hybrid systems is used to indicate the continual systems which are governed by computers and the class of models in which simultaneously are modeled both: discrete and continual behavior of the object.

Air traffic flow is an open complex continual dynamic system with mixed structure. As a result, it is expedient to use the theory of hybrid systems, which in the world of rapid development of modern technologies will not just allow us to describe the system, but also let us to get its adequate model. The difficulty of model's behavior which is connected with the presence of several modes, which change caused by the onset of external or internal events. Today it is not enough to study each mode separately. It is necessary to build a model of the whole object. For the description and research of complex objects we need new models which were based on modern technologies.

In 2004, professors from the Stanford University brought control theoretical model of the air traffic flow, based on sectors, using the theory of hybrid automation. Then it was used as a subset of this model to generate Lagrangian analytic predictions of the traffic flow (dynamic sector capacity, extend of traffic jams), which were linked to Eulerian models of the National Airspace System.

The results were used to predict the conditions under which the saturation of airspace can not be solved at the level of a single sector, and requires centralized solution. These predictions were checked by comparison with an abstraction of the real system. Finally, the flow conditions were generated under which they can be decorrelated metering from conflict resolution.

In conclusion we can note that with the help of hybrid systems' research we can get an adequate model of the flow, which gave us an opporunity to improve the control of air traffic flow, and what is the most important is that this model will increase the safety and efficiency of air traffic control.

Scientific supervisor – L.M.Juma c.t.s., associate professor

UDC 517:61(043.2)

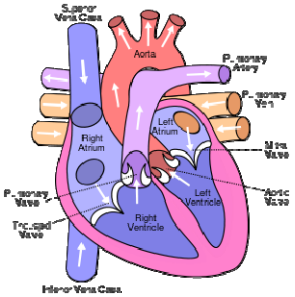
Voinalovych G.O., Vlasov V.Ye., Donchenko L.A.
National Aviation University, Kyiv

APPLICATION OF INTEGRATION IN MEDICINE

Definite integral has many applications. Applying definite integrals we find areas, length of curve, volume of solid, centre of mass, moments of inertia, force due to liquid pressure, average value, work by a variable force and so on. There are some applications of integration in economics (consumer surplus), biology and medicine (blood flow, cardiac output).

We'll consider example of evaluation of cardiac output.

Figure shows the human cardiovascular system.



Cardiac output is the volume of blood pumped by the heart per unit time, that is the rate of flow into the aorta. Cardiac output is a function of heart rate and stroke volume. The heart rate is simply the number of heart beats per minute. The stroke volume is the volume of blood, in milliliters (mL), pumped out of the heart with each beat.

According to dilution method the output of heart is equal to the amount of indicator injected divided by its average concentration in the arterial blood after a single circulation through the heart.

That is, cardiac output is

$$F = \frac{A}{\int_0^T c(t)dt},$$

where the amount of dye A is known and the integral can be approximated from the concentration readings.

Scientific supervisor – T.A.Oleshko, c.ph.-m.s., associate professor

UDC 519.2(043.2)

Voinalovych A.O.
National Aviation University, Kyiv

APPLICATIONS OF CORRELATION AND REGRESSION ANALYSIS

The correlalion is one of the most common and most useful statistics. A correlation is a single number that describes the degree of relationship between two variables.

Regression is a way of describing how one variable, the outcome, is numerically related to predictor variables.

Regression analysis involves identifying the relationship between a dependent variable and one or more independent variables. A model of the relationship is hypothesized, and estimates of the parameter values are used to develop an estimated regression equation.

Correlation and regression analysis is widely used in various fields of science, business and industry.

For example, there are three main uses for correlation and regression in biology. One is to test hypotheses about cause-and-effect relationships. In this case, the experimenter determines the values of the X-variable and sees whether variation in X causes variation in Y.

The second main use for correlation and regression is to see whether two variables are associated, without necessarily inferring a cause-and-effect relationship. In this case, neither variable is determined by the experimenter; both are naturally variable. If an association is found, the inference is that variation in X may cause variation in Y, or variation in Y may cause variation in X, or variation in some other factor may affect both X and Y.

The third common use of linear regression is estimating the value of one variable corresponding to a particular value of the other variable.

Correlation and regression analysis can help business to investigate the determinants of key variables such as their sales. Variations in companies sales are likely to be related to variation in product prices, consumers, incomes, tastes and preference's multiple regression analysis can be used to investigate the nature of this relationship and correlation analysis can be used to test the goodness of fit. Regression can also be used to estimate the trend in a time series to make forecast.

The stockbroker wishes to predict stock market behaviour as a function of a number of observable key indices. The sales manager of a chain of retail stores wishes to predict the monthly sales volume of each store from the number of credit customers and the amount spent of advertising. The political scientist may wish to relate success in a political campaign to the characteristics of a candidate, the opposition, and various campaign issues and promotional techniques.

Regression and correlation can be used wherever it is necessary to study the behaviour of one or more variables and how they affect the final result.

Scientific supervisor – T.A.Oleshko, c.ph.-m.s., associate professor

МУЛЬТИМЕДІЙНІ СИСТЕМИ ТА ТЕХНОЛОГІЇ

УДК 778.38:658.62(043.2)

Коваль Ю.В.
Національний авіаційний університет, Київ

ДИНАМІЧНА ГОЛОГРАФІЯ

Сьогодні голографія більш широко використовується не тільки для захисту продукції, але й для виготовлення спеціальної унікальної документації (права водія, біометричні паспорти, тощо).

Замість одного тривимірного зображення на голографічній емульсії планується розміщувати два, які будуть динамічно змінюватися під впливом зовнішнього середовища. Подразником до зміни зображення виступає магнітне поле, яке ініціює рух мініатюрних частинок з нанесеною на них голографічною емульсією по обидва боки пластинок. Мініатюрні частинки являються доменами, що реагують на дію магнітного поля через їх структуру та фізичні властивості. Залежно від напрямку магнітного потоку, що проходить через домени, покриті голографічною емульсією, мікропластинки змінюють своє положення відносно площини поверхні, на яких вони розміщені. При цьому відкривається та грань мікропластинок, на якій нанесено одне цілісне зображення.

Для того, щоб на мікропластинках розмістити цілісне зображення, розбите на безліч окремих частин, потрібно на поверхні, на якій буде розміщено зображення, виставити домени (мікропластинки) в одному порядку, щоб під дією магнітного поля домени поверталися в одному і тому ж самому напрямку. Це планується робити за допомогою того ж магнітного поля, яке розставить домени залежно від їх полярності до того, як на них буде нанесено голографічну фотоемульсію. Після нанесення одного шару емульсії домени повертаються в зворотному порядку і наноситься другий шар. Таким чином утворюється зображення з двох сторін.

Пружний шар речовини, на якому закріплені мікропластинки, буде утримувати їх в такому порядку, що за замовчуванням (без дії магнітного поля) завжди буде видиме одне цілісне тривимірне голографічне зображення, а інше в цей момент буде приховане. Саме на зображення, приховане за замовчуванням, потрібно наносити інформацію, яка потребує захисту. Відкриватися вона буде тільки у випадку дії магнітного поля на площину, що можливо вже при втручанні людини.

Магнітне поле буде створювати сітка з котушок індуктивності, розміщених під пружним шаром. Імпульси подаються не на всю площину сітки одночасно, а на окремі частини, за допомогою транзисторних ключів, що регулюють подачу струму на окремі ділянки сітки з котушок індуктивності. На самі ключі в свою чергу імпульси подаються з пристрою введення, що реагує на дотик (touchpad), для того, щоб відкривати не все зображення, а окремі його ділянки. При чому імпульси подаються після ідентифікації відбитка клієнта, до того приховане зображення не відкривається через механічну дію пружного шару та імпульсів, які подаються на сітку котушок індуктивності.

Науковий керівник – Малярчук В.О., доцент

УДК 004.4'27:378(043.2)

Біляєва М.М.
Національний авіаційний університет, Київ

ВИКОРИСТАННЯ ПРИНЦИПІВ ДИЗАЙНУ ДЛЯ ОПТИМІЗАЦІЇ РОБОТИ З ІНТЕРАКТИВНИМИ МУЛЬТИМЕДІЙНИМИ ЗАСОБАМИ У СИСТЕМІ ОСВІТИ

Сьогодні у більшості освітніх закладів використання мультимедіа є вимогою для подання матеріалу, проте способу його способу подачі приділяється дуже мала увага. При створенні веб-сайту чи навчальної програми обов'язково має враховуватись аудиторія, для якої розроблюються дані додатки. Ця аудиторія заслуговує не тільки на гідний її дизайн, але й на такий метод представлення інформації, який би сприяв максимальному засвоєнню матеріалу. Сьогодні мультимедіа-технології - один із перспективних напрямів у інформатизації навчального процесу. Мультимедіа- та гіпермедіа-технології інтегрують у собі потужні розподілені освітні ресурси, що здатні забезпечити середовище для формування та розвитку ключових компетентностей, до яких відносяться в першу чергу інформаційна й комунікативна.

Мультимедіа- та телекомунікаційні технології відкривають принципово нові методичні підходи до організації педагогічного процесу в системі загальної освіти. Під час роботи над даною темою головним було зрозуміти спосіб мислення суб'єктів навчання, на що вони в першу чергу звертають увагу і як цю увагу привернути. Відповідно було визначено, що зір являється основним каналом сприйняття. Половина ресурсів головного мозку використовується для обробки та інтерпретації зорової інформації. Звісно, те, що сприймають наші очі є лише частиною загального процесу.

Наступним етапом став розгляд процесу мислення людини. Саме розуміння мислення є ключовим моментом для дизайну будь-якого додатку, а особливо навчального. При створенні інтерактивних освітніх мультимедіа враховується також метод фокусування уваги. Що може змусити помітити будь-що, як привернути і втримати чиюсь увагу, як людина обирає на що звернути увагу і на чому зосередитись? Ці питання є одним з основних аспектів, що мають враховуватись при створенні мультимедійних засобів. У процесі освіти основним рушієм засвоєння інформації є мотивація, чи то прагнення дізнатись більше про якийсь об'єкт, чи то взагалі дізнатись що це за об'єкт. Розуміння, що саме мотивує студента чи учня є вагомим критерієм для організації інтерактивного мультимедіа таким чином, щоб можна було не тільки привернути увагу, але і максимально зацікавити останніх. Робота над даною темою дала змогу розглянути і виокремити основні принципи дизайну, які мають бути використанні для оптимізації роботи суб'єктів навчання з інтерактивними мультимедійними засобами у процесі навчання. Це відкриває нове бачення на сучасні і майбутні навчальні програмні засоби, будь то інтерактивна 3D-аудиторія чи міжнародний сайт, призначений для дистанційної освіти людей різнох поглядів і віку.

Науковий керівник – Таран В.М., ст. викладач

УДК 004.92(043.2)

Кубай Ю.В.
Національний авіаційний університет, Київ

РОЗРОБКА FLASH-ВЕРСІЙ WEB-САЙТІВ З ВИКОРИСТАННЯМ HTML

Створення Flash сайт означає відразу привернути увагу до свого проекту. Статичні сайти просто не можуть створити конкуренцію яскравим флешам.

Створення Flash сайту достатньо довгий і трудомісткий процес, котрий потребує особливої уваги.

Основні переваги проектів подібного виду:

- Якісне відображення в будь-якому браузері і миттєва оптимізація до розширення екрану. Відбувається це завдяки тому, що коли ми створюємо Flash сайт, то використовуємо векторну графіку, котра основується на використанні геометричних примітивів,чим і обгрунтовує її гнучкість.
- Збільшення, чи зменшення масштабу не представляє загрози для Flash сайту – в будь-якому випадку він відображається коректно.
- Створення Flash сайту під цим розуміється такі додаткові блага, як можливість доповнення проекту музикальний супровід, а також складною анімацією, що робить сайт більш привабливими для користувача, з естетичної точки зору.
- Завдяки використанню флеша можна створювати відмінні сайти для презентації своїх продуктів та послуг. Можливість облаштувати свою пропозицію динамічними зображеннями, чи навіть привабливою музикою, що дозволить зробити сайт більш привабливішим і інформаційнішим, а також спростить його сприйняття користувачів.

Особливості Flash-сайту:

Перед тим, як показати розробку Flash сайту, потрібно також звернути увагу на ряд особливостей, котрі належать йому, ніж потім бути розчарованим.

- Перший і основний недолік Flash-сайту – це відсутність можливостей пошукового просування такого сайту. Діло в тім, що пошукові системи просто не сприймають вміст, проте всі вони створенні виключно за допомогою Flash технологій.
- Достатньо довга загрузка сайту, створеного на флеші. Звичайні сайти працюють швидше, це означає, що частина користувачів можуть знервуватись, не дочекавшись завершення загрузки сторінки, проте це на справді грозить лише тим, у кого швидкість підключення до Інтернету залишається бажати кращого.

Для того щоб уникнути певних проблем і створити Flash сайт корисним і пізнавальним інструментом можна вдало скомбінувати флеш і звичайний, статичний сайт. Ця хитрість дозволить залишити яскраве враження динаміки сайту, а також зробити можливість успішно пошукову оптимізацію і скоротити до розумних розмірів, швидкість загрузки сторінки сайту.

Науковий керівник – Малінкін І.В., канд. техн. наук, доцент

УДК 027.7:004(043.2)

Несен О.О.
Національний авіаційний університет, Київ

ЕЛЕКТРОННІ БІБЛІОТЕКИ НА РІВНІ ЗАВАНТАЖЕННЯ ДАНИХ ТА ДОСТУПУ ДО НИХ

На даний момент програмне забезпечення електронної бібліотеки чітко поділяється на чотири підрозділи, які тісно зв'язані між собою:

- програмне забезпечення керування цифровим архівом;
- програмне забезпечення керування електронною бібліотекою;
- програмне забезпечення пошукової системи;
- програмне забезпечення автентифікації.

Завантаження та доступ до даних реалізується в програмному забезпеченні керування цифровим архівом (завантаження даних в архів і доступ до них) та в програмному забезпеченні автентифікації (надання прав завантаження, зміни, перегляду, видалення даних та інше)

Контроль за правами користувача в електронній бібліотеці здійснюється на рівні автентифікації. Автентифікація- це перевірка достовірності пред'явленого користувачем ідентифікатора. Система автентифікації включає в себе наступні елементи: суб'єкт, який буде проходити автентифікацію; характеристика суб'єкта – відмінна риса; адміністратор системи; механізм автентифікації, тобто принцип її роботи.

Відповідно до автентифікації суб'єкт електронної бібліотеки по своїм відмінним рисам може набути прав користування електронною бібліотекою як:

- читач. Відповідно до автентифікації читачеві надаються права доступу до окремих видань, одні з них він має право лише переглядати, а інші може копіювати (встановлюється при автентифікації відповідно до відмінної риси суб'єкта). Також користувач може оплачувати окремі видання (при наявності даного сервісу) і надалі користуватися ними на вільних засадах. Профіль читача створюється ним самим автоматично при вході до електронної бібліотеки;
- видавництво (окремий видавець). Автентифікувавшись в електронній бібліотеці, як видавництво, суб'єкт набуває прав відмінних від користувача. Видавець (відповідно від наданих йому прав адміністратором) має право завантажувати свої видання до електронної бібліотеки, корегувати їх, видаляти, встановлювати права доступу до них та інше. Також при наявності платного сервісу він може встановлювати ціни на свої видання, після оплати яких, видання стає доступним. Профіль і права видавця встановлює адміністратор після заявки останнього;
- адміністратор електронної бібліотеки. Автентифікувавшись в електронній бібліотеці як адміністратор, суб'єкт набуває повних прав користування і редагування електронної бібліотеки (в тому числі і зміни механізму автентифікації). Адміністратор регулює дії видавців і читачів. Профіль адміністратора створюється при розробці електронної бібліотеки.

Науковий керівник – Мелешко М.А., канд. техн. наук, професор

УДК 004.5(043.2)

Кацалап Р.Г.
Національний авіаційний університет, Київ

ПЕРЕТВОРЕННЯ CSS3 У ДВО- І ТРИМІРНОМУ СЕРЕДОВИЩІ ПРИ РОЗРОБЦІ ВЕБ-САЙТУ

Перед веб-дизайнером постійно постає проблема художнього оформлення веб-проекту і вибору найбільш кращого рішення у способі подачі інформації. Новий стандарт оформлення веб-сторінок (CSS3) надає ряд нових можливостей: дво- і тримірні перетворення. Використовуючи ці можливості можна вийти на новий рівень розробки веб-сайтів або модернізувати вже створений сайт. 3D-технології набувають все більш широкого поширення при проектуванні сайту.

Дво- і тримірні перетворення CSS3 забеспечують набагато цікавіше і гнучке управління елементами веб-сайту, чим те, яке було доступним раніше для розмітки CSS. Специфікація надає підтримку повороту, перетворення, масштабування і нахилу. В поєднанні з можливістю маніпулювання елементами в тримірному просторі, зміною центру проекції і впливом на джерело перетворень, перетворення CSS3 є досить ефективними.

Перетворення CSS3 визначаються щодо набору осей, що складають систему координат. Двовимірні перетворення визначаються щодо двох осей. Вісь y продовжується вниз, а не вгору, як у випадку більшості декартових систем координат. Тримірні перетворення визначаються щодо трьох осей. Вісь z системи координат перпендикулярна осям x і y.

Застосувати перетворення до елементу веб-сайту дуже легко. Необхідно просто додати в селектор властивість transform і вказати список функцій перетворення.

Можна застосовувати декілька перетворень, з'єднавши їх в ланцюжок, - тобто додавши кілька функцій перетворення в одну властивість перетворення в тому порядку, в якому їх слід застосувати. Порядок, в якому додається перетворення, впливає на кінцевий результат.

Тримірні перетворення застосовуються так само, як двовимірні (додаванням властивості transform до стилю елемента). Щоб скористатися перевагами третього виміру, список доступних функцій перетворень розширений. За замовчуванням тримірні перетворення виконуються з відсутністю перспективи. Внаслідок цього не можна отримати бажаного ефекту. Для того, щоб отримати ефект перспективи необхідно використати властивість perspective, що додає ілюзію глибини в перетворення CSS3. Перспектива (її також називають глибиною перспективи) в CSS3 - це відстань, що рахується по осі z, між уявним спостерігачем і поверхнею батьківського елемента, над яким виконується перетворення.

Отже, перетворення CSS3 дають можливість створення різноманітної і іммерсивної взаємодії в Інтернеті, збільшують можливості веб-дизайнерів при розробці своїх проектів стосовно дизайну і представлення інформації.

Науковий керівник – Кучеров Д.П., д-р техн. наук, професор

УДК 004.358 (043.2)

Пясківський М.І.
Національний авіаційний університет, Київ

3D МОДЕЛЮВАННЯ СТРУКТУРИ АВІАЦІЙНОГО ДВИГУНА

В доповіді розглядаються етапи створення 3D моделі авіаційного двигуна. Тематика створення трьохвимірної моделі є надзвичайно актуальною в наший час, адже 3D технології все більше і більше проникають у повсякденне життя, і її використовують для все більш різноманітних цілей – кіно, архітектура, комп'ютерні ігри, проектування і т.д. Дану модель можна буде застосовувати в різних цілях – наприклад для навчання технічного персоналу обслуговування двигуна, пояснення принципу роботи турбовалового двигуна, представлення можливостей двигуна.

Існує декілька 3D редакторів для створення моделей, такі як Conitec 3D Game studio, MilkShape 3D, Maya, 3Ds Max та інші. Вибір зупиняється на 3Ds Max 10, тому що, окрім створення 3D моделей, цей редактор дозволяє і створювати трьохвимірну анімацію, пробляти фізичні властивості моделей, такі як, вага, пружність, і при цьому він має зручний та простий інтерфейс.

Сам процес створення 3D моделі поділяється на декілька етапів:

Спершу відскановуються всі креслення або схеми двигуна Зображення креслень потім будуть накладатися на площини в редакторі, і з їх допомогою будуть точно розміщатися всі елементи двигуна. Також з допомогою цього можна домогтися створення моделі двигуна в точному масташбуванні.

Далі настає створення самих елементів двигуна. Відповідно по кресленням, створюється, компресор низького тиску, компресор високого тиску, камера згорання, ротор турбіни 1 ступеня, ротор турбіни 2 ступеня, вільна турбіна.

Складання всіх елементів в один об'єкт. Перед складанням деякі об'єкти потрібно згрупувати. Робиться це для того, щоб на наступному етапі анімування моделі, спростити роботу. Наприклад компресор високого тиску і ротор турбіни 1 ступеня, пов'язані між собою одним валом, тому виділяється, компресор, вал та ротор і групуються. Також на цьому етапі важливо визначитися із типами матеріалів, із яких виконаний кожен компонент. Наприклад лопатки роторів 1 ступені хоч і виконані із металу, але через те що вони знаходяться постійно під впливом високої температури, вони не мають характерного для металів відблиску. Всі ці нюанси уточнюються і доповнюють модель. І останнім етапом лишається створення анімації. Вона показує принцип роботи двигуна, і призначення основних елементів двигуна.

Науковий керівник – Мелешко М.А., д-р техн. наук, професор

УДК 004.001.76 (043.2)

Савченко М.С.
Національний авіаційний університет, Київ

ВИКОРИСТАННЯ НОВІТНІХ КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ З МЕТОЮ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ СПРИЙНЯТТЯ ІНФОРМАЦІЇ

На сучасному етапі інформатизації суспільства все більшого поширення в різноманітних сферах життя набувають комп'ютерні технології, вони виступають як один із інструментів пізнання.

Розвиток комп'ютерної техніки не тільки якісно змінює життя суспільства, але й впливає на культуру, залучає людство до накопичення культурного багатства. Новітні інформаційні технології орієнтують людину на саморозвиток та самонавчання. Значно розширюють можливості доведення і сприйняття інформації завдяки використанню комп'ютерних технологій.

Використання в навчальному процесі комп'ютерних технологій спонукає студентів до самостійного ознайомлення з матеріалом, що вивчається, створює сприятливу, комунікативну ситуацію та умови для розвитку творчих здібностей особистості; підвищує мотивацію та пізнавальну активність учнів; розширює та поглиблює міжпредметні зв'язки; систематизує та інтегрує знання окремих навчальних предметів; організовує систематичний та достовірний контроль; уникає суб'єктивізму в оцінці.

Для підвищення ефективності навчального процесу сучасні технічні засоби необхідно використовувати як цілісний самостійний продукт. Завдяки комп'ютерних технологій можна одночасно поєднати разом різного роду інформацію: зорово-ілюстративну, текстову, звукову, що значно підвищує ефективність сприйняття інформації. Застосування новітніх комп'ютерних технологій дає змогу створювати та користуватись електронними підручниками, які мають значно більший об'єм інформації, використовувати інтернет для отримання інформації та її передачі іншим користувачам. Тому комп'ютерні технології на сучасному етапі є дієвим засобом навчання.

Пріоритетним для будь-якого фахівця, в сучасному інформаційному середовищі, є максимальне використання комп'ютерних технологій як методів та інструментів у професійній діяльності.

З вище приведеного слідує, що використання новітніх комп'ютерних технологій значно підвищує ефективність сприйняття значно більшого об'єму інформації, надає можливість проводити обмін цією інформацією та значно підвищує рівень професійної підготовки тих, хто навчається.

Науковий керівник – Малярчук В.О., доцент