МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ
Учреждение образования
«Белорусский государственный технологический университет»

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

Тезисы докладов 81-й научно-технической конференции профессорско-преподавательского состава, научных сотрудников и аспирантов (с международным участием)

1-12 февраля 2017 года

Минск 2017

УДК 004:005.745(06)
ББК 32.97я73
И 74

Информационные технологии : тезисы 81-й науч.-техн. конференции профессорско-преподавательского состава, научных сотрудников и аспирантов (с международным участием), Минск, 1-12 февраля 2017 г. [Электронный ресурс] / отв. за издание И.В. Войтов; УО БГТУ. – Минск : БГТУ, 2016. – 32 с.

Сборник составлен по материалам докладов научно-технической конференции сотрудников Белорусского государственного технологического университета, в которых отражены новые успехи и достижения в информационных технологиях: алгоритмизации и программировании, передачи и обработки данных.

Сборник предназначен для работников различных отраслей народного хозяйства, научных сотрудников, специализирующихся в соответствующих областях знаний, аспирантов и студентов ВУЗов.

Рецензенты: д-р техн. наук, проф. кафедры информационных систем и технологий В.Л. Колесников;
канд. техн. наук, зав. кафедрой информатики и компьютерной графики Д.М. Романенко;
канд. техн. наук, декан факультета информационных технологий Д.В. Шиман

Главный редактор ректор, профессор И.В.ВОЙТОВ

© УО «Белорусский государственный технологический университет», 2017

СОДЕРЖАНИЕ

1. *Гурин Н.И., Жук Я.А.* Генерация типов связей семантической сети информационной системы 5
2. *Варепо Л.Г., Трапезникова О.В., Бражников А.Ю.* Алгоритм оценки равномерности красочного покрытия на запечатываемой подложке 6
3. *Трапезникова О.В.* Алгоритм оценки цветовоспроизведения печатной системы.....7
4. *Навойчик А.В., Гурин Н.И.* Использование сверточных нейронныхсетей в системах тестирования знаний 9
5. *Бирюк И.А.* Моделирование и анализ процесса синхронизации искусственных нейронных сетей 10
6. *Кобайло А.С.* Особенности архитектурной организации вычислительных систем реального времени 12
7. *Жиляк Н.А., Новицкая А.Д.*Методы распознавания образов в графический изображениях 14
8. *Patsei N., Jabber G.* Naming, routing and security of content-centric networking 15
9. *Шитько А.М.* Проектирование микросервисной архитектуры программного обеспечения.....16
10. *Блинова Е.А., Сухорукова И.Г.* Сравнительная оценка применимости стеганографических методов в графических файлах svg 17
11. *Hassan Ali, Brakovich A.I.* Classification and a brief analysis of existing developments for the search optimization in databases 18
12. *Mohamed Ahmad El Seblani, Ghilyak N.* Class technology analysis of big data 20
13. *Колесников В. Л., Бракович А. И.* Графическая оптимизация условий работы производственного комплекса на основе нейронных сетей.21
14. *Шутько Н.П.* Защита и передача текстовой информации на основе изменения кернинга 22
15. *Цыганенко Н.П.* Математические характеристики систем кэширования.....23
16. *Миронов И.А.* Методы и алгоритмы организации отказоустойчивого кластера для информационной среды университета.....26
17. *Кишкурно Т.В., Брусенцова Т.П.* Оптимизация процесса восприятия экранного пространства компьютера на основе принципов юзабилити 27
18. *Малашко Д. В., Романенко Д.М.* Алгоритмы криптографической защиты передаваемых данных с использованием протоколов ssl и tls 28

19. *Дятко А. А.* Математическая модель радиолокационного сигнала, отраженного от земной поверхности 29
20. *Новосельская О.А., Савчук Н.А.* Разработка гильоширных элементов средствами векторной графики 30
21. *Корзина М. И., Антонов М. И., Корзин Ю.Н.* Автоматизация диагностики контрольно-кассовой техники……31

УДК 004.853

Н. И. Гурин, доц., канд. физ.-мат. наук; Я. А. Жук, асп.
(БГТУ, г. Минск)

ГЕНЕРАЦИЯ ТИПОВ СВЯЗЕЙ СЕМАНТИЧЕСКОЙ СЕТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Извлечение семантического содержания текста требует предварительного синтаксического анализа предложений. В настоящее время используется метод неполного синтаксического анализа путем сравнения простых предложений с записями в базе данных шаблонов предложений при помощи регулярных выражений. Каждый набор из утвердительного и вопросительного предложений соответствует определенному типу семантической связи. Эффективность данного метода напрямую зависит от числа шаблонов в базе данных, поэтому для анализа больших текстов требуется наполнять базу данных типов семантических связей автоматически.

В соответствии с лингвистическим методом актуального членения предложений тип смысловой связи между подлежащим и дополнительными членами предложений определяется сказуемым. Путем исследования текста электронного учебника по электрохимии было выявлено, что наиболее распространенными сказуемыми являются глаголы в форме третьего лица и краткие прилагательные. Таким образом, в основе большинства шаблонов предложений, выражающих семантические связи, стоит глагол в форме третьего лица или краткое прилагательное. Также в шаблоне при помощи специальных тегов отмечены места для подстановки подлежащего, дополнительных членов предложения, окончания и вопросительного слова.

Составление таких шаблонов становится возможным при качественно проведенном морфологическом анализе, который распознает в тексте глаголы в форме третьего лица и краткие прилагательные. Для этого во всех найденных сказуемых выполняется замена их окончаний на соответствующие теги. Затем выполняется формирование шаблонов вопросительного и утвердительного предложений. Для вопросительного предложения перед сказуемым добавляется тег вопросительного слова, а после – тег подлежащего. Шаблон утвердительного предложения дополняется тегом подлежащего перед сказуемым и тегом дополнительных членов предложения – после сказуемого. Так, для предложения «*Электродный потенциал не зависит от количества вещества, прореагировавшего на электродах*» был получен следующий SQL-запрос на вставку типа семантической связи в базу данных: *INSERT INTO шаблоны VALUES ("[В] завис[Г2] [А]", "[А] завис[Г2] [Б]").*

УДК 004.021; 655.3.022.3; 658.562

Л. Г. Варепо, проф., д-р техн. наук; О.В. Трапезникова, асп.
(Омский государственный технический университет, Россия);
А. Ю. Бражников, нач. печатного центра
(ООО «Омскбланкиздат», г, Омск, Россия)

АЛГОРИТМ ОЦЕНКИ РАВНОМЕРНОСТИ КРАСОЧНОГО ПОКРЫТИЯ НА ЗАПЕЧАТЫВАЕМОЙ ПОДЛОЖКЕ

При получении печатного изображения на подложках, имеющих неоднородную поверхность, не всегда удается обеспечить равномерность и целостность красочного слоя на оттиске. Разработка алгоритма оценки распределения красочного покрытия на запечатываемой подложке с элементами тиснения, с целью автоматизации оценки данного показателя, является актуальной задачей.

При решении поставленной задачи использовались положения теории вероятностей и математической статистики, современные программные средства обработки информации. Разработан алгоритм и программное обеспечение для оценки показателя равномерности распределения красочного покрытия. На практике, подразумевая равномерность распределения красочного слоя, чаще упоминают термин укрывистость. Программа реализована с применением среды разработки Microsoft Visual Studio 2010, языка программирования C# на платформе Windows с использованием Framework 4.0. Основа данного алгоритма состоит в поиске закрашенных частей образца и вычисления процентного отношения количества закрашенных пикселей к общему количеству пикселей изображения. Программа работает с отсканированными изображениями голубого, пурпурного, желтого и черного цветов шкалы контроля качества печатного оттиска. При нажатии на кнопку «Открыть файл» открывается диалоговое окно для выбора файла одного из форматов: например, TIFF, JPEG. Считывание запечатанного многокрасочного изображения в массив значений составляющих RGB выполняется с использованием встроенного Graphics. После того, как изображение считано, производится переход из цветовой модели RGB в Lab. Далее вычисляется с учетом неопределенности измерений искомый показатель как отношение количества пикселей, соответствующих цвету образца на цифровой копии оттиска с отсутствием печатной краски на местах изображения, умноженному на 100, к общему количеству пикселей изображения на цифровой копии оттиска, имеющего полное равномерное покрытие изображения печатной краской.

Разработанный алгоритм программного обеспечения с учетом неопределенности измерений позволяет оперативно количественно оценить равномерность распределения красочного покрытия на оттиске, что отражает новизну и практическую значимость работы.

УДК 004.021; 535.6

О.В. Трапезникова, асп.
(Омский государственный технический университет, Россия)

АЛГОРИТМ ОЦЕНКИ ЦВЕТОВОСПРОИЗВЕДЕНИЯ ПЕЧАТНОЙ СИСТЕМЫ

При оценке качества печатной продукции соответствие цветового оформления оригинала цвету на оттиске является первостепенным. В работе представлена практическая реализация разработанного алгоритма для оценки цветовоспроизведения печатной системы, применение которого позволяет оперативно обеспечить оптимальный состав печатной системы, дающий возможность воспроизводить оригинальное изображение без искажения.

Для оценки цветовых характеристик оригинала осуществляется пересчет, первоначально определенных координат цвета элементов изображения (пикселей) в колориметрическом пространстве *RGB*, в координаты цветового пространства *CIE L*a*b** с учетом неопределенности измерений. С целью оперативного получения результатов данная процедура выполняется с помощью разработанного специального программного модуля в среде Maple 13.

Фрагмент листинга программы для оценки цветовоспроизведения печатной системы представлен ниже.

```
for j from 1 to m do for i from 1 to n do X[k] := img[i,j,1]·0.5767309
    + img[i,j,2]·0.185554 + img[i,j,3]·0.1881852 : Y[k] := img[i,
  j,1]·0.2973769 + img[i,j,2]·0.6273491 + img[i,j,3]
  ·0.0752741 : Z[k] := img[i,j,1]·0.0270343 + img[i,j,2]
  ·0.0706872 + img[i,j,3]·0.9911085 : k := k + 1 : od: od:

                        k2 := 903.3 :
                        e := 0.008856 :

for i from 1 to n·m do xr[i] := X[i]/0.95047 : yr[i] := Y[i]/1 : zr[i]
    := Z[i]/1.08883 : od:

for i from 1 to n·m do if xr[i] > e then fx := xr[i]^(1/3) elif xr[i] ≤ e
    then fx := (k·xr[i] + 16)/116 end if: if yr[i] > e then fy := yr[i]^(1/3)
    elif yr[i] ≤ e then fy := (k·yr[i] + 16)/116 end if: if zr[i] > e then fz
    := zr[i]^(1/3) elif zr[i] ≤ e then fz := (k·zr[i] + 16)/116 end if: L[i]
    := 116·fy − 16 : a[i] := 500·(fx − fy) : b[i] := 200·(fy − fz) :
    od:

                        R := [ L  a  b ]
```

При вхождении всех элементов изображения в тело цветового охвата печатной системы, изображение будет воспроизведено печатной системой без искажений и сжатия общего цветового контраста. При выявлении группы элементов изображения, находящихся вне тела цветового охвата печатной системы, можно сделать вывод о количестве элементов изображения и соответственно о площади изображения, передача цвета на которой, будет выполнена с искажением. Графические интерпретации цветовых охватов представлены на рис.1–2.

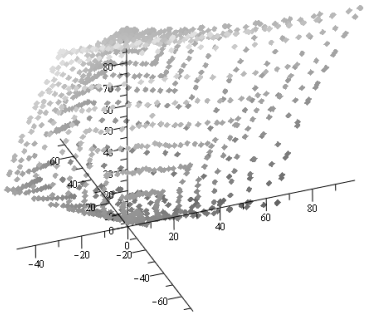

Рисунок 1 – Воспроизведение тела цветового охвата на подложке

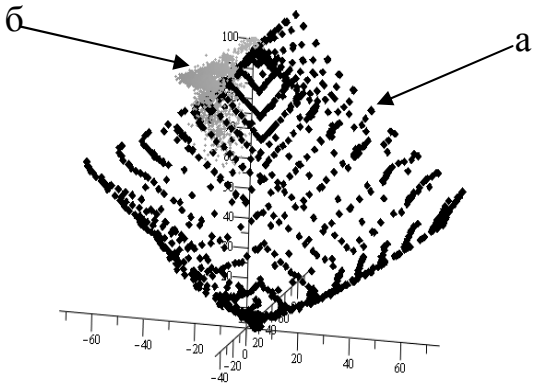

Рисунок 2 – Воспроизведение цветовых характеристик печатной системы (а) и электронной копии оригинала (б) в равноконтрастном цветовом пространстве CIE L*a*b*

Практическая реализация разработанного алгоритма при тестировании различных подложек для печати показывает, что, чем шире окажется цветовой охват печатной системы, тем точнее будет диапазон цветов и их оттенков, которые данная система может воспроизвести.

УДК 004.853

А. В. Навойчик, магистрант; Н. И.Гурин, доц., канд. физ.-мат. наук
(БГТУ, г. Минск)

ИСПОЛЬЗОВАНИЕ СВЕРТОЧНЫХ НЕЙРОННЫХ СЕТЕЙ В СИСТЕМАХ ТЕСТИРОВАНИЯ ЗНАНИЙ

Разработано программное обеспечение для проверки бланков ответов по тестам на основе технологии оптического распознавания рукописных символов. В качестве механизма функционирования приложения использовалась обученная и протестированная сверточная нейронная сеть.

Сверточная нейронная сеть – специальная архитектура искусственных нейронных сетей, нацеленная на эффективное распознавание изображений. Идея сверточных нейронных сетей заключается в чередовании сверточных слоев и субдискретизирующих слоев. Для обучения сети использовался метод обратного распространения ошибки.

Сверточная нейронная сеть была обучена и протестирована на нескольких наборах данных:

1) английские печатные буквы и цифры – 3600 и 360 изображений для обучения и тестирования соответственно, получен результат 94% соответствия;

2) русские рукописные буквы – 330 и 66 изображений для обучения и тестирования соответственно, получен результат 73% соответствия;

3) русские рукописные цифры – 100 и 20 изображений для обучения и тестирования соответственно, получен результат 85% соответствия.

Для улучшения результатов, естественно, потребуется выборка для обучения гораздо большего объема в наборах данных.

При проектировании программного обеспечения для проверки бланков ответов по тестам были заложены следующие требования.

1. Создание разметки бланка ответов с указанием областей данных участника, ответов на задания с вариантами ответа, ответов на задания без вариантов ответа.

2. Оптическое распознавание меток.

3. Оптическое распознавание рукописных символов.

4. Проверка бланка ответов по созданной разметке.

5. Подсчет результата.

Практической полезностью разработанного программного обеспечения является автоматизация процесса проверки бланков ответов по тестам.

Реализация предложенного метода использования сверточной нейронной сети позволяет получить полноценную и рабочую систему оптического распознавания рукописного текста и автоматизировать проверку бланков ответов по тестам. Разработанное программное обеспечение можно использовать в учреждениях образования, исследовательских центрах для проверки различных тестов.

УДК 519.715

И. А. Бирюк, магистрант
(БГТУ, г. Минск)

МОДЕЛИРОВАНИЕ И АНАЛИЗ ПРОЦЕССА СИНХРОНИЗАЦИИ ИСКУССТВЕННЫХ НЕЙРОННЫХ СЕТЕЙ

В связи с бурными темпами развития сети интернет и как следствие увеличение количества информации, которая передаётся при помощи этой сети, все чаще и чаще поднимается вопрос об информационной безопасности. Для безопасной передачи информации применяются различные технологии, наиболее часто применяемая – криптографическое преобразование информации.

Для распределения ключей между пользователями компьютерной сети используются следующие основные способы:

– использование одного или нескольких центров распределения ключей;

– прямой обмен ключами между пользователями сети.

Проблемой первого подхода является то, что центру распределения ключей известно, кому и какие ключи распределены, и это позволяет читать все сообщения, передаваемые по сети. Возможные злоупотребления могут существенно нарушить безопасность сети. При втором подходе проблема состоит в том, чтобы надежно удостовериться в подлинности субъектов сети.

Одна из новых идей касающаяся распространения ключей, применяемых для шифрования, является использование нейронных сетей. Эта идея была выдвинута И. Кантером и В. Кинцелем и основано на использовании архитектуры TPM (англ. Tree Parity Machine, древовидная машина четности). Развитием этой идеи является расширение множества используемых алгебр за счёт использования комплексных и гиперкомплексных чисел [1-3].

Было разработано программное средство для проведения исследований и анализа устойчивости двух искусственных нейронных сетей. Для анализа полученных результатов были рассчитаны индекс Брея-Кёртиса и расстояние по Хеллингеру для того чтобы провести сравнение подобие полученного во время проведения экспериментов

распределения к нормальному. Полученные результаты для опытов проведенных на основании кватернионов представлены в таблице 1.

Таблица 1 = Результаты анализа

Количество входных нейронов	Количество персептронов	Ограничение накладываемые на весовые коэффициенты	Стандартное отклонение числа итераций синхронизации	Индекс Брея-Кёртиса	Расстояние по Хэллингеру
5	5	-5;+5	212,3127	0,236778	39915,92
5	5	-6;+6	360,5353	0,254661	121378,9
5	6	-5;+5	214,9023	0,230132	29147,51
6	5	-6;+6	164,8493	0,205305	18992,93
6	6	-5;+5	147,7051	0,232275	40974,62
6	6	-6;+6	147,7025	0,184315	17536,88
6	6	-7;+7	272,0603	0,226647	38036,79
6	7	-6;+6	144,2508	0,173883	14911,65
6	7	-7;+7	273,0947	0,193843	30154,5
7	6	-6;+6	209,8088	0,215792	26438,17
7	6	-7;+7	385,8097	0,23227	51979,91
7	7	-6;+6	209,6789	0,206227	25823,96
7	7	-7;+7	284,9163	0,197808	33964,22
8	8	-8;+8	273,6395	0,184612	29033,77
9	9	-9;+9	605,6361	0,201454	74716,29

ЛИТЕРАТУРА

1 Плонковски, М. Д. Модели передачи и криптографического преобразования информации на основе нейросетевых технологий и расширения поля используемых чисел: Диссертации на соискание ученой степени кандидата наук: 05.13.19/ М. Д. Плонковски – Минск, БГТУ, 2009 – 103 с.

2 Плонковски, М. Д. Криптографическое преобразование информации на основе нейросетевых технологии / М. Д. Плонковски, П. П. Урбанович // Труды БГТУ. Сер. VI. Физико-математические науки и информатика. – Минск: БГТУ, 2005. – С. 161–164.

3 Плонковски, М. Д. Синхронизация криптографических ключей на основе нейросетевых технологий / М. Д. Плонковски, П. П. Урбанович // материалы междунар. науч.-практ. конф., апрель 2006 г. / Брест. гос. ун-т им. А. С. Пушкина. – Брест: Изд-во БрГУ. – С. 29.

УДК 004.031.43 – 044.962

А. С. Кобайло, доц., канд. техн. наук
(БГТУ, г. Минск)

ОСОБЕННОСТИ АРХИТЕКТУРНОЙ ОРГАНИЗАЦИИ ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМ РЕАЛЬНОГО ВРЕМЕНИ

Одной из основных проблем, возникающих при проектировании вычислительных систем реального времени (ВСРВ), является достижимость требуемого быстродействия (производительности). Для последовательного выполнения алгоритма из j операций необходим ресурс времени, который определяется:

$$T = \sum_{i=1}^{I} \tau'_i \cdot \tau_c ,$$

где τ'_i – код продолжительности выполнения i-й операции; τ_c– такт или время цикла, которому пропорциональны интервалы времени между моментами начала или завершения любых действий в системе (величина обратная тактовой частоте). Повышение быстродействия элементной базы или, что то же самое, уменьшение значения τ_c имеет свой предел, ограниченный скоростью света. Поэтому для решения задачи повышения производительности более перспективными являются пути поиска архитектурной организации ВС, связанные, в первую очередь, с совмещением операций. Два основных подхода к решению проблемы – конвейеризация и параллелизм.

Конвейеризация может быть использована в случаях, когда требуемая скорость обработки потока данных удовлетворяет условию:

$$\Delta t = \tau_{max},$$

где Δt – требуемый период получения данных на выходе структуры; τ_{max} – время выполнения наиболее длинной операции техническими средствами, на которые ориентируется разработчик.

Параллелизм целесообразно применять при возможности накопления или одновременного поступления массива входных данных.

Однако, как показывают исследования, два классических подхода к решению задачи увеличения быстродействия в применении к вычислительным системам реального времени имеют существенные ограничения, так как первый из них может не обеспечить выполнения требований РВ, второй может оказаться принципиально непригодным при обработке последовательных потоков данных.

В тех случаях, когда для реализации некоторых операций алгоритма отсутствуют ФУ с временем выполнения соответствующих операций, не большим, чем требуемый цикл обработки данных, по-

строение архитектур реального времени становится невозможным. Для решения проблемы может быть использован метод на основе параллельно-конвейерных вычислителей (ПКВ).

ОПРЕДЕЛЕНИЕ 1. Параллельно-конвейерным вычислителем называется вычислитель, содержащий ρ параллельных ступеней, выполняющих последовательность однотипных операций с одинаковым временным сдвигом, равным периоду формирования очередных результатов на выходе ПКВ.

В том случае, когда необходима обработка массива данных размерностью n по единому алгоритму (например, вычисление вектора), и нет возможности создать или использовать параллельный n-канальный вычислитель, может быть использован конвейерно-параллельный вычислитель (КПВ).

ОПРЕДЕЛЕНИЕ 2. Конвейерно-параллельным вычислителем будем называть вычислитель, содержащий m идентичных каналов, вычислительный процесс каждого из которых реализован по конвейерному принципу.

Предложенный принцип организации параллельно-конвейерных вычислителей

а) позволяет:

– достигнуть быстродействия обработки потока данных, определяемого только частотой переключения элементной базы;

– увеличить быстродействие по сравнению с конвейеризацией для векторных операций в число раз, определяемое соотношением скоростей выполнения операций умножения и сложения;

б) предоставляет возможность при выполнении векторных операций получить выигрыш по совокупности технических параметров по сравнению с параллелизмом практически при том же быстродействии). Вопрос о целесообразности замены быстродействующего элемента на ПКВ должен решаться в каждом случае индивидуально.

Применение принципа организации вычислительных архитектур на базе конвейерно-параллельных вычислителей позволяет увеличить быстродействие по сравнению с параллельными вычислителями в ρ раз при тех же аппаратных затратах, по сравнению с конвейером – в m раз, где ρ – количество ступеней конвейерной цепи КПВ, m – количество каналов КПВ.

ЛИТЕРАТУРА

1. Кобайло, А. С. Теория синтеза вычислительных систем реального времени / А. С. Кобайло. Минск: БГТУ. 2010 г. – 2016 с.

УДК 004.41.42

Н. А. Жиляк, канд. техн. наук, доц.;
А. Д. Новицкая, магистрант
(БГТУ, г. Минск)

МЕТОДЫ РАСПОЗНАВАНИЯ ОБРАЗОВ В ГРАФИЧЕСКИЙ ИЗОБРАЖЕНИЯХ

Программные решения на основе обработки изображений и распознавания образов на них широко используются в множестве сфер производства, развлечения, медицины. Теория распознавания образа – раздел информатики, развивающий основы и методы идентификации предметов, которые характеризуются конечным набором некоторых свойств и признаков.

На данный момент самыми быстроразвивающимися областями применения методов и алгоритмов распознавания образов является медицина (рентгенография и ультразвуковые, электромагнитные исследования, микрохирургия), приборостроение (создание микросхем, высокоточные манипуляции для сборки отдельных узлов механизмов), контроль качества на производствах добывающей и обрабатывающей промышленности, системы безопасности и разграничения доступа, системы контроля скорости и мониторинга нарушений дорожного движения, производство фото-видео техники и разработка программного обеспечения для нее, автоматическая обработка больших объемов текстовых данных (например обработка результатов централизованного тестирования) и так далее. Таким образом можно сформулировать основную цель специалистов, занятых в этой области: создание машинного и программного обеспечения для автономной коммуникации с окружающей средой присущими человеку способами, а именно, с помощью зрения. Это выражается в распознавании и классифицировании образов по определенному признаку.

В качестве простейших способов можно назвать методы ковариации и сравнения шаблонов. Алгоритм ковариации двух изображений – возможный способ реализации методов сравнения шаблонов. Контурный анализ является методом решения задачи распознавания конкретного объекта не прибегая к попиксельному сравнению, а также увеличения производительности программного средства.

Реализация вышеназванных методов поможет получить полноценную и рабочую систему анализа передвижения и изменения заданных искомых объектов на кадрах видеопотока (записи камеры видеонаблюдения).

UDK 316.776

N. Patsei, associate professor;
G. Jabber, PhD student
(BSTU, Minsk)

NAMING, ROUTING AND SECURITY OF CONTENT-CENTRIC NETWORKING

Content-centric networking (CCN) is type of the information-centric networks (ICN) architectures. Basic idea of concept is that the object with which communication is carried out is less important as what data is required for this.

Communication is controlled by the recipients, i.e. the data consumers exchange of two packets types: Interest and Data. Both types of packages have a name that identifies a chunk of data in a Data packet. The user makes the desired name in the data part Interest packet and sends it to the network. Routers use the name to send Interest packet to the data provider. When the packet reaches the node that contains the requested data, the Data returns a package that contains both the name and the content provider, together with the signature key.

ICN routes and forwards the packet based on the name, which solves three challenges associated with addresses in the IP-architecture: the exhaustion of the address space, the NAT Tracking and address management. These names are hierarchical in nature, and includes the global name of the content producer -> application where the data will be processed -> instance of the application. In addition, and other necessary data may be in the name of the data - version assignment segments and etc. So the name is generated by content application, in accordance with certain rules and protocols.

This architecture has no separate transport layer. It passes the current transport protocols (demultiplexing, reliable delivery and congestion management) applications to the support libraries and module strategy in promoting the plane. The information of the transport layer, such as a port and a serial number is not necessary. All information required for transport are in the data names.

An important advantage of CCN/ICN is reducing the burden on the resources that provide access to data, logically organizing around the ring, which caches data, that is often accessed by users and so can respond to requests, thus protecting the resource overload.

CCN is only an experimental study. While there is no real-world implementations, and mathematics process is in deep study.

УДК 004.27
А.М. Шитько, асп. (БГТУ, г. Минск)

ПРОЕКТИРОВАНИЕ МИКРОСЕРВИСНОЙ АРХИТЕКТУРЫ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Микросервисная архитектура – это архитектура, в которой сервисы: небольшие, узко сфокусированные, слабосвязанные и высокосогласованные [1]. Небольшие сервисы – сервисы, которые не могут разрабатываться больше чем одной командой. Обычно одна команда разрабатывает не более 6 сервисов. При это каждый сервис решает одну бизнес-задачу, и его способен понять один человек. Узко сфокусированные сервисы – сервисы, которые решают только одну бизнес-задачу и делают это хорошо. Такие сервис можно отделить от системы, дописав некоторую логику, и использовать как отдельный продукт. Слабосвязанные сервисы – сервисы, изменение которых не требует изменений в других. Высокосогласованные сервисы – сервисы, в которых класс или компонент содержит все нужные методы для решения поставленной задачи только в этом классе или компоненте и больше нигде.

Свойства микросервисной архитектуры.

1. Разбиение через сервисы. Построение системы путем соединения вместе различных компонент. Здесь существуют 2 понятия: библиотека и сервис. В микросервисной архитектуре библиотеки – это компоненты, которые подключаются к программе и вызываются ею в том же процессе, в то время как сервисы – компоненты, выполняемые в отдельном процессе и связывающие друг с другом с помощью REST или RPC.

2. Группировка по бизнес-задачам. Любая микросервисная архитектура должна придерживаться закона Конвея [2], который гласит, что структура вашего приложения повторяет структуру вашей команды, т.е. необходимо выделять команды по бизнес-задачам.

3. Умные сервисы и простые коммуникации. Вся логика находится в сервисах, канал передачи только передает данные, он ничего не знает о бизнес-задаче.

4. Децентрализованное управление данными. Каждый сервис имеет свою и только свою БД.

5. Автоматизация развертывания и мониторинга.

6. Проектирование через отказы. Сервисы должны работать при отказе отдельных сервисов.

Изучив свойства микросервисов и их способы построения можно выделить следующие преимущества: модульность, высокая доступность, разнообразие технологий, независимое развертывание. Но в свою очередь есть ряд недостатков: поддержка конечной согласованности (поддержка работы с отложенными данными, что требует по-

стоянной доступности приложения), сложность операционной поддержки (поддержка непрерывного развертывания, непрерывной интеграции и автоматического мониторинга).

ЛИТЕРАТУРА

1. Microservice Architecture [Электронный ресурс]. – Режим доступа: http://microservices.io/. – Дата доступа: 30.01.2017.

2. Ньюмен, С. Создание микросервисов. – СПб.: Питер, 2016. – 304 с.

УДК 003.26

Е. А. Блинова, ст. преп.; И.Г. Сухорукова, ст. преп.
(БГТУ, г. Минск)

СРАВНИТЕЛЬНАЯ ОЦЕНКА ПРИМЕНИМОСТИ СТЕГАНОГРАФИЧЕСКИХ МЕТОДОВ В ГРАФИЧЕСКИХ ФАЙЛАХ SVG

В докладе рассматриваются возможности применения стеганографических методов для файлов SVG (Scalable Vector Graphics) – векторных графических файлов, предназначенных для описания двумерной векторной и смешанной векторной и растровой графики в формате XML. Преимущества данного формата, такие как небольшой размер файлов, масштабируемость, интеграция с HTML документами, возможность встраивания растровой графики, возможность редактирования в текстовых редакторах и поддержка в большинстве современных браузеров делают SVG файлы удобным контейнером для осаждения скрытого сообщения в процессе прямого стеганографического преобразования.

Поскольку SVG файлы являются подмножеством файлов формата XML, то к ним могут быть применены классические методы текстовой стеганографии, такие как метод конечных пробелов и табуляций, а также методы, характерные для файлов разметки, такие как метод замены регистра тегов и метод перестановки атрибутов. Однако особенности формата позволяют использовать и другие методы внедрения скрытой информации. Формат тегов описания путей позволяет размещать скрытую информацию в добавлении дополнительных элементов в геометрических фигурах. При описании фигур используется цветовая модель RGB, что позволяет внедрять скрытую информацию в незначительном изменении параметров цвета. Игнорирование браузерами неверных атрибутов позволяет производить подмену атрибутов по заранее определенному алгоритму.

Комбинированное применение нескольких стеганографических

методов позволяет решить две задачи. С одной стороны, использовать несколько стеганографических ключей для передачи конфиденциальной информации нескольким корреспондентам. С другой стороны, контролировать целостность осаждаемой скрытой информации, что может быть использовано, например, при решении задачи защиты права интеллектуальной собственности на изображения либо их частей.

UDC 004.657

Ali Hassan, PhD student;
A.I. Brakovich, PhD, associated prof.
(BSTU, Minsk)

CLASSIFICATION AND A BRIEF ANALYSIS OF EXISTING DEVELOPMENTS FOR THE SEARCH OPTIMIZATION IN DATABASES

Nowadays there is a development and dissemination of "cloud computing" technology. The growing demand for services offering a broad range of cloud computing services for large numbers of users all over the world, therefore increase in the number of applications, the purpose is to process large data sets. The operation of the database in the cloud leads to the need to find new instruments.

Most often this concept is treated as a "complex of information collection and procedures: management, updates, information retrieval and post-processing - which allows to accumulate, store, update and provide information", processing and organizing information, should take into account. User no longer divides his activities on information search object can not be clearly defined in advance [1].

The search tools and technologies used for the implementation of information requirements, depend on the type and condition of the problem to be solved by the user operations. The process user interaction with the system is determined by the level of knowledge of user resource content (completeness, reliability of the source, etc.) and the functionality of the system as a tool. In general, these factors are usually limited to the notion of professionalism - information (trained / untrained user) and objective (professional / amateur). For solving the problem of query optimization in the cloud storage system should also be taken into account. For network topology used two methods:

1) Query Optimization in the Cloud SQL type database architecture are as follows: all files are stored in the local file system; cloud database is designed to store and manage huge amounts of index files and metadata;

enter the query and get the results performed by the web user interface; user request is executed the current search query plan (as a subset).

2) Query optimization in cloud databases NoSQL type since there is one sever: used programming model map-reduce (MR) – platform for cloud computing, which allows analysis of large amounts of data in the cloud. MR facilitates parallel execution for long-term problems of the analysis of large data. In MR each task is represented as a map for reduce tasks. MR Kernel for storage and data uses a distributed file system with MRQL language. It allows user to write own scripts for a large tasks in declarative form, and at the same time itself to optimization. This procedure consists of the following steps: simplification of the request, building a query graph and query graph representation in algebraic form [2].

In this work another method is proposed for similar purposes, based on virtual machines and processing centers. The main interest of this approach lies in the fact that its purpose is to balance the load of virtual machines in the cloud environment which indirectly leads to an increase in the quality of the search (it is obvious that the speed with which the cloud responds to user requests, is one of the search quality criteria). For resource management in large-scale data centers are developed and implemented a centralized solution, but in this case the occurrence of a failure at the control node, resulting in malfunction of the whole system. The average length of the vector unit load is equal to the number of iterations of sending the index. A load information will be stored in a decentralized, in order to avoid trouble in the event of a failure of the node, another positive aspect is that the network traffic is distributed across all active nodes (as opposed to the scheme with centralized management, where all packets should go through common node). The decision on the virtual machine migration can be taken in two cases: when the CPU usage exceeds a certain level (the upper limit), freeze mode or when the CPU usage is below a certain level (the lower limit) transferred to the "sleep" mode.

Each methods have both advantages and disadvantages. Common to all is a lack of synthetic nature of the results, that the introduction of statistics obtained in artificial systems created just for testing approach. Optimization such developments in the near future will be in demand.

REFERENCES

1. Vakkari P., Hakala N. An Appropriate Boolean Query Reformulation Interface for Information Retrieval Based on Adaptive Generalization. In WIRI, 2015. – p. 145-150.

2. Ullman J.D., Hector G.M., Widom J. Database Systems. – USA: Pearson, 2013. – 256 p.

UDC 004.27

Mohamed Ahmad El Seblani, PhD student;
N. Ghilyak, PhD, associated prof.
(BSTU, Minsk)

CLASS TECHNOLOGY ANALYSIS OF BIG DATA

The category of large Big Data includes information which is no longer possible to process by conventional methods, including structured data, media and random objects. Some experts believe that in order to work with them to replace the traditional monolithic systems have new massively parallel solutions. From the name we can assume that the term `great data` simply refers to the large amounts of data management and analysis. According to the report McKinsey Institute `big data: the new frontier for innovation and competition` (Big data: The next frontier for innovation, competition and productivity), the term` great data` refers to data sets whose size is beyond the capabilities of typical databases for named, storage, management and analysis of information. And global repository of data, of course, continue to grow [1].

Big Data suggest something more than just an analysis of huge amounts of information. The problem is not that organizations create huge amounts of data, but the fact that most of them are presented in a format that bad associated traditional structured format database – a web-based magazines, videos, text documents, computer code, or, for example, geospatial data. Everything is stored in a variety of different storage facilities, sometimes even outside the organization. As a result, corporations can have access to a huge amount of their data and do not have the necessary tools to establish the relationship between these data and make on the basis of their significant conclusions. Add to this the fact that the data is now updated more and more, and you get a situation where the traditional data analysis methods can not keep up with the vast amounts of constantly updated data, which ultimately paves the way for big data technologies [2]. The aim of the further work with big data is the development of methods and algorithms for processing large data scoring model.

REFERENCES

1. Konstantin B. Optimizations in computing the Duquenne–Guigues basis of implications / B. Konstantin // Annals of Mathematics and Artificial Intelligence. 2014. Vol. 70. No. 1-2. P. 5-24. doi

2. Obiedkov S. Modeling ceteris paribus preferences in formal concept analysis, in: Formal Concept Analysis / S.Obiedkov //Ed. by P. Cellier, F. Distel, B. Ganter. Vol. 7880. Berlin, Heidelberg : Springer, 2013. P. 188-202.

УДК 004.94

В. Л. Колесников, проф., д-р техн. наук;
А. И. Бракович, доц., канд. техн. наук
(БГТУ, г. Минск)

ГРАФИЧЕСКАЯ ОПТИМИЗАЦИЯ УСЛОВИЙ РАБОТЫ ПРОИЗВОДСТВЕННОГО КОМПЛЕКСА НА ОСНОВЕ НЕЙРОННЫХ СЕТЕЙ

В предыдущих работах авторов разработано интерактивное программное средство, имитирующее все основные условия функционирования реального предприятия [1]. Многообразие условий работы производственного комплекса определяют 16 параметров окружения, 9 параметров для оперативного управления, 6 параметров результатов, оценивающих качество и себестоимость продукции, загрязнение окружающей среды. Работа осуществляется в режиме реального времени и сопровождается фиксацией условий и результатов в базе данных, которая содержит информацию по 26 столбцам. Системным временем является время выработки одной тонны продукции. Таким образом, размерность базы данных для анализа составляет 500 – 1000 строк и 26 столбцов.

В предлагаемом примере снижена размерность решаемой задачи. Количество признаков, характеризующих условия, уменьшено до 9. Задача классификации данных этого примера методом нейронных сетей решается быстро и просто. Интерпретировать результаты очень сложно. Только парных взаимодействий придется рассмотреть 36, а с учетом взаимовлияния различных значений внутри признаков это количество возрастает до 630.

В таких случаях эффективным оказывается применение метода прогрессивной централизации. Для снижения размерности решаемой задачи можно, например, сосредоточиться на проблеме коррекции технологического режима для различных сезонных условий.

Определение оптимальных значений параметров осуществляется графически в среде JMP SAS путем фиксации координат минимума (максимума) критерия оптимальности секущими плоскостями доминирующих признаков с соответствующим подбором значений всех остальных атрибутов базы данных (рисунок 1).

Нейронные сети оказываются мощным средством не только для классификации данных, но и для графического решения оптимизационных задач в разнообразных формулировках.

По простоте и гибкости настройки этот метод оптимизации превосходит классические и градиентные методы.

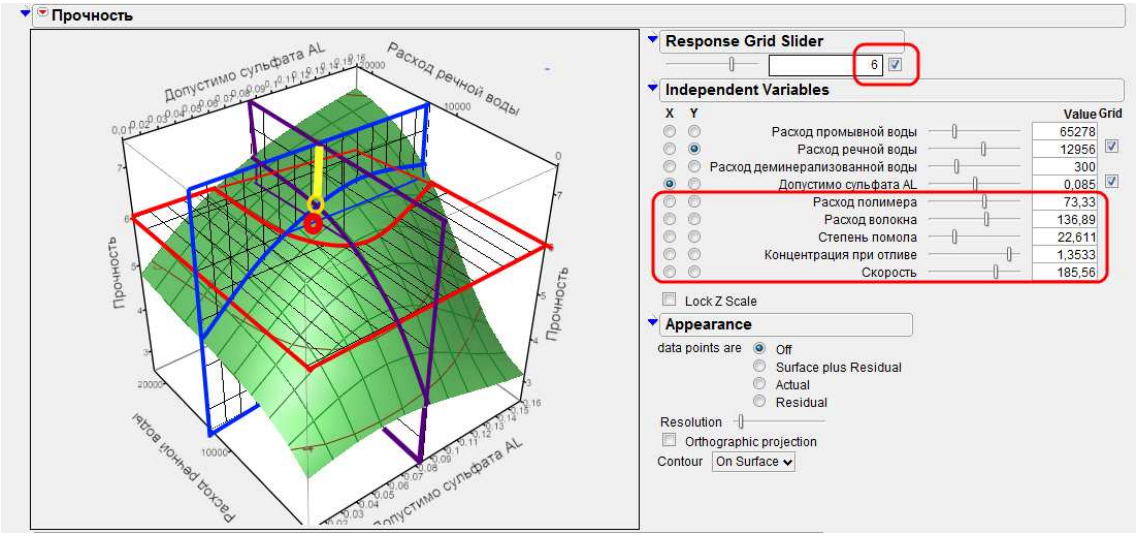

Рисунок 1 – Оптимальные условия получения продукции с заданным значением прочности для зимних условий

Поскольку в данном случае используются не традиционные математические модели, а базы данных результатов наблюдений за длительный период времени, то предлагаемый метод обладает наибольшей оперативностью и экспрессностью в подстройке задач при изменении текущих условий функционирования производственного комплекса.

ЛИТЕРАТУРА

1. Kolesnikov Vitaliy. Modeling and software implementation of fibrous waste disposal processes / Kolesnikov Vitaliy, Urbanovich Pavel, Brakovich Andrei // Electrical Review. – 2016. – №8. P. 33-35.

УДК 003.26+347.78

Н. П. Шутько, ассист., канд. техн. наук
(БГТУ, г. Минск)

ЗАЩИТА И ПЕРЕДАЧА ТЕКСТОВОЙ ИНФОРМАЦИИ НА ОСНОВЕ ИЗМЕНЕНИЯ КЕРНИНГА

Развитие информационных технологий привело к тому, что значительная часть информации теперь находится в электронном виде (в системах хранения данных). Поэтому особенную остроту приобретает проблема доказательства авторских прав на текстовые документы и надежной защиты этих ресурсов, а также иных текстовых документов, программных кодов, баз данных от несанкционированного использования. Проблема защиты авторского права в стране отнесена к числу приоритетных.

Цифровые технологии дали новый импульс исследованиям

в области стеганографии, которая является одним из инструментов для решения указанной задачи.

В докладе были рассмотрены алгоритмические особенности нового метода текстовой стеганографии, который основывается на принудительном применении кернинга (изменении расстояния между особыми парами символов — кернинговым парам), не зависящем от установок параметров текста-контейнера, созданных средствами текстового процессора или иного специализированного текстового редактора. Результатом работы стало создание алгоритмов осаждения и извлечения информации на основе предлагаемого метода. Учитывая специфическую особенность процессора MS Word, состоящую в том, что кернинг применяется к символам, размер (кегль) которых не ниже заданного специальной опцией во вкладе Шрифт, и такая опция может применяться независимо к любым знакам текста, предложены два варианта практической реализации метода.

Модификация указанного пространственно-геометрического параметра шрифта позволяет осаждать тайное сообщение в процессе прямого стеганографического преобразования защищаемого текста-контейнера либо передавать эту информацию по стегоканалу. В первом случае решается задача защиты права интеллектуальной собственности, во втором — обеспечения повышенного уровня конфиденциальности передаваемых сообщений между абонентами.

УДК 51-74

Н.П. Цыганенко, асп.
(БГТУ, г. Минск)

МАТЕМАТИЧЕСКИЕ ХАРАКТЕРИСТИКИ СИСТЕМ КЭШИРОВАНИЯ

Основная цель веб-приложений и других интернет-ресурсов заключается в предоставлении посетителям информации в различных формах (текст, графика, видео и т. д.). Интернет-пространство сегодня – это насыщенная данными среда. Поэтому, в условиях жесткой конкуренции за внимание пользователей, проблема скорости получения пользователем информации более чем актуальна. Ее решением является минимизация времени между запросом, посылаемым на сервер, и моментом полной загрузки ответного сообщения с запрашиваемым контентом [1].

Двумя наиболее важными характеристиками эффективности системы кэширования являются скорости доступа к хранимой информации и вероятность попадания в кэш. Скорость доступа к информации в кэше – это время от запроса информации веб-приложением у

системы кэширования до полного получения необходимых данных. Вероятность попадания в кэш – это процент успешных разрешений запросов на получение определенной информации к их общему числу.

Поскольку обе основные характеристики являются числовыми, то для того, чтобы получить наилучшие результаты при использовании систем кэширования, можно применить методы решения задач оптимизации. Эти методы относятся к математическому программированию и требуют наличия математической модели оптимизируемой системы в виде целевой функции [2].

Множество записей в базе данных R мощностью n состоит из записей r_i:

$$r_i \in R, \qquad (1)$$

где i – порядковый номер записи в базе данных.

Множество записей в кэше C мощностью m состоит из записей c_j:

$$c_j \in C, \qquad (2)$$

где j – порядковый номер записи в кэше.

Множество записей в кэше C является подмножеством множества записей в базе данных R:

$$C \subset R. \qquad (3)$$

Число обращений к множеству записей в базе данных состоит из количества обращений к отдельным записям:

$$U = \sum_{i=1}^{n} u_i, \qquad (4)$$

где u_i – количество обращений к записи r_i.

Воспользовавшись формулой (4), выведем формулу для вычисления вероятности обращения к записи r_i через отношение количества обращений к данной записи к общему числу обращений к базе данных:

$$p_i = \frac{u_i}{U}. \qquad (5)$$

Обозначим через P_i вероятность того, что запись r_i находится в кэше, т. е.:

$$r_i \in C. \qquad (6)$$

Проанализировав несколько частных случаев, можно вывести рекуррентную формулу для определения вероятности попадания записи r_i в кэш:

$$P_i = \begin{cases} 0, m = 0, \\ p_i + \sum\limits_{j=1, j \neq i}^{n} p_j P_i(R \setminus i, CP_{pjn}, m-1, n-1), \end{cases} \quad (7)$$

где *CP* – функция для вычисления условных вероятностей на основании вектор-строки *p* и выбранного элемента p_j.

Функция *CP* состоит из удаления из вектор-строки указанного элемента с помощью булевой матрицы *A* и нахождения условной вероятности для оставшихся элементов с помощью матрицы *B*:

$$CP(p, x, n) = p \times A \times B. \quad (8)$$

Значения для ячеек матрицы *A* вычисляются по следующей формуле:

$$a_{ij} = \begin{cases} 1, & (i > x \wedge i = j-1) \vee (i < x \wedge i = j), \\ 0. \end{cases} \quad (9)$$

Для ячеек матрицы *B* применяется следующее выражение:

$$b_{ij} = \begin{cases} \dfrac{1}{1-p_i}, & i = j, \\ 0. \end{cases} \quad (10)$$

Используя вероятность попадания в кэш (7), можно вывести формулу для вычисления среднего времени чтения записи r_i:

$$T_i = t_c + t_i(1 - P_i), \quad (11)$$

где t_c – время чтения из кэша; t_i – время чтения записи r_i из базы данных.

ЛИТЕРАТУРА

1. Siewiorek D. Computer Structures: Principles and Examples. NY: Mc Graw Hill, 1981. P. 960.

2. Janert P. Data Analysis with Open Source Tools. Sebastopol: O'Reilly Media, Inc., 2010. P. 540.

УДК 004.75

И.А. Миронов, ассист. (БГТУ, г. Минск)

МЕТОДЫ И АЛГОРИТМЫ ОРГАНИЗАЦИИ ОТКАЗОУСТОЙЧИВОГО КЛАСТЕРА ДЛЯ ИНФОРМАЦИОННОЙ СРЕДЫ УНИВЕРСИТЕТА

Бурное развитие информационных технологий, рост обрабатываемых и передаваемых данных и в то же время повышение требований к надежности, степени готовности, отказоустойчивости и масштабируемости приводит к возникновению различных проблем в существующий информационных средах.

В существующей информационной среде университета можно выделить ряд проблем: рост требований к числу и качеству предоставляемых информационных сервисов, неоптимальное распределение вычислительных ресурсов и снижение доступности в следствии неустойчивости к отказам.

При анализе существующих проблем была предложена организация отказоустойчивого кластера с применением технологии виртуализации.

Кластер — группа компьютеров, объединённых высокоскоростными каналами связи, представляющая с точки зрения пользователя единый аппаратный ресурс. Сервера, являющиеся составными узлами кластера, соединены между собой и системой хранения данных оптическими каналами формата Fibre Channel со скоростью передачи информации 8 Гбит/с. Данная связь строится по базе SAN-коммутации. Это позволит увеличить производительность, повысить эффективность развертывания виртуальных серверов и сократить расходы на хранение данных.

Гипервизор VMware vSphere предусматривает широкий спектр служб и программ для повышения отказоустойчивости. Реализация High Availability (отказоустойчивого кластера) реализуется следующим образом: несколько физических хостов объединяется в кластер и при выходе из строя одного из хостов, виртуальные машины, которые были на нем, запускаются на других хостах кластера, на которых зарезервированы ресурсы.

В результате получим следующие преимущества: упрощение IT-инфраструктуры, минимизация плановых, и незапланированных простоев серверов, повышение эффективности внедрения информационных сервисов от использования виртуальных машин, репликация виртуальных машин на локальные или удаленные системы хранения данных.

УДК 004.5(075.8)

Т.В. Кишкурно, ст. преп.; Т.П. Брусенцова ассист.
(БГТУ, г. Минск)

ОПТИМИЗАЦИЯ ПРОЦЕССА ВОСПРИЯТИЯ ЭКРАННОГО ПРОСТРАНСТВА КОМПЬЮТЕРА НА ОСНОВЕ ПРИНЦИПОВ ЮЗАБИЛИТИ

При разработке пользовательских интерфейсов словом юзабилити обозначают общую концепцию их удобства при использовании программного обеспечения, логичность и простоту в расположении элементов управления. Рассмотрим наиболее важные особенности восприятия интерфейсов пользователем с точки зрения юзабилити.

Интерфейс должен *снижать когнитивную нагрузку* на пользователя. Для этого он должен быть ясным, простым и интуитивно понятным. Поскольку память пользователя фокусируется на достижении конкретных целей, *ненужные действия* заставляют пользователя приложить больше усилий, что влечет за собой дополнительную *когнитивную нагрузку* на пользователя.

Одним из основных препятствий для получения легко воспринимаемого интерфейса является *визуальный шум*. *Перегруженный* интерфейс отвлекает внимание пользователя от восприятия основной информации, и они пытается игнорировать ее или совсем исключать из поля зрения (принцип *баннерной слепоты)*.

Когнитивную нагрузку вызывает и *большое количество контента***.** Чтобы уменьшить ее необходимо создать ясную визуальную иерархию: более важный элемент должен быть самым заметным на веб-странице, элементы логически связанные между собой, также должны быть связаны визуально, элементы, которые представляются в виде вложений, должны являться частями друг друга. Кроме этого необходимо разделять веб-страницы на четкие области. При написании текстов необходимо придерживаться принципа *перевернутой пирамиды*. Статья должна начинаться с итогового вывода, за которым следуют ключевые моменты, а завершаться наименее важной для читателей информацией.

Неоднозначный интерфейс также приводит к когнитивной перегрузке. Необходимо использовать в интерфейсах принятые условности и общие правила, например метафор или стандарты.

Разрабатывать интерфейс пользователя необходимо по принципам юзабилити, с использованием законов психологии восприятия, теории передачи информации, а также психофизиологии человека. Это даст возможность удовлетворить потребности пользователя, снизить когнитивную нагрузку на пользователя, уменьшить время для поиска нужной информации, нивелировать риск ошибок при работе на компьютере.

УДК 519.6+519.7

Д. В. Малашко, магистрант; Д.М. Романенко, доц.
(БГТУ, г. Минск)

АЛГОРИТМЫ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ПЕРЕДАВАЕМЫХ ДАННЫХ С ИСПОЛЬЗОВАНИЕМ ПРОТОКОЛОВ SSL И TLS

Протокол SSL интегрирован в большинство браузеров и веб серверов и использует ассиметричную криптосистему с открытым ключом, разработанную компанией RSA. Для осуществления SSL соединения необходимо, чтобы сервер имел инсталлированный цифровой сертификат. Цифровой сертификат – это файл, который уникальным образом идентифицирует пользователей и серверы. Это своего рода электронный паспорт, который проводит аутентификацию сервера до того, как устанавливается сеанс SSL соединения. Обычно цифровой сертификат независимо подписывается и заверяется третьей стороной, что гарантирует его достоверность.

Протокол SSL предоставляет «безопасный канал», который имеет три основных свойства:

1. Канал является частным;
2. Канал аутентифицирован. Серверная сторона диалога всегда аутентифицируется, а клиентская делает это опционально;
3. Канал надежен. Транспортировка сообщений включает в себя проверку целостности.

Преимуществом SSL является то, что он независим от прикладного протокола. Протоколы приложений (HTTP, FTP, TELNET и т. д.) могут работать поверх протокола SSL совершенно прозрачно, то есть SSL может согласовывать алгоритм шифрования и ключ сессии, а также аутентифицировать сервер до того, как приложение примет или передаст первый байт сообщения.

Развитием протокола SSL является протокол TLS. Как указано в RFC, «различия между этим протоколом и SSL 3.0 не критичны, но они значительны для появления несовместимости при взаимодействии TLS 1.0 и SSL 3.0». TLS 1.0 действительно включает средства, с помощью которых реализация подключения TLS к SSL 3.0 ослабит безопасность.

В настоящее время наиболее распространены следующие виды атак: атака по словарю; атака отражением; атака протокола рукопожатия; раскрытие шифров; атака «злоумышленник посередине». Анализ возможности применения указанных вариантов атак показал, что протокол TLS способен противостоять им, и вследствие этого широко используется веб-серверами для обеспечения конфиденциальности информации.

УДК 621.391.26

А. А. Дятко, доц., канд. техн. наук,
(БГТУ, г. Минск)

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ РАДИОЛОКАЦИОННОГО СИГНАЛА, ОТРАЖЕННОГО ОТ ЗЕМНОЙ ПОВЕРХНОСТИ

При разработке, испытаниях и эксплуатационном контроле радиолокационных станций (РЛС) традиционно используются натурные испытания. Однако они имеют ряд недостатков: высокую стоимость, сложность получения повторяющихся условий, а также практическую неосуществимость на ранних стадиях разработки. В связи с этим все большее распространение получают полунатурные испытания. В этом случае совокупность сигналов и помех на входе РЛС моделируется с помощью имитаторов. В связи с этим важное значение приобретает разработка алгоритмов для имитационного моделирования на ЭВМ входных сигналов РЛС, соответствующих различным условиям их работы.

Представленная работа посвящена вопросу разработки математической модели сигнала, отраженного от плоской земной поверхности и реализации ее в виде программного обеспечения для ЭВМ.

В работе рассмотрена математическая модель сигнала, отраженного от плоской земной поверхности по главному лепестку диаграммы направленности антенны радиолокационной станции для случая диффузионной модели рассеяния электромагнитных волн. Модель построена с учетом флуктуаций эффективной площади рассеивания, обусловленных влиянием различных климатических факторов. Получены алгоритмы математического моделирования такого сигнала и определены требования к их параметрам.

Предложенная модель позволяет выполнить тестирование работоспособности радиолокационных комплексов различного назначения на ЭВМ уже на этапе их разработки, не прибегая к натурным испытаниям, которые могут потребовать значительных материальных затрат.

Разработанная математическая модель радиолокационного сигнала, отраженного от земной поверхности, может быть использована при проектировании радиолокационных систем различного назначения на этапе имитационного моделирования их работы на ЭВМ.

УДК 655.533, 535.421

О. А. Новосельская, ст. преп., канд. техн. наук; Н. А. Савчук, студ.
(БГТУ, г. Минск)

РАЗРАБОТКА ГИЛЬОШИРНЫХ ЭЛЕМЕНТОВ СРЕДСТВАМИ ВЕКТОРНОЙ ГРАФИКИ

Основу защиты документов составляют специальные штриховые изображения, которые воспроизводятся на бумаге специальными способами печати. Это является средством защиты полиграфической продукции от фальсификации и злоупотреблений. Под формами защиты от фальсификации понимается уровень сложности и доступности идентификации наличия защит в продукте. Выделяются условно три формы защиты: объявленные защиты, сертифицированные и скрытые [1]. Анализ показывает, что самыми эффективными являются скрытые защиты, которые могут быть идентифицированы только в условиях профессионального окружения (то есть в экспертных лабораториях и оборудованных сертификационных центрах). Применение этой формы защит наиболее целесообразно для документарной группы изделий.

В работе разработаны видимые глазом цветные гильоширные элементы, создающие имитацию радужной печати, на основе векторных штриховых изображений. При этом особенностью элементов является сохранение штриховых элементов при многокрасочной печати даже с использованием стандартного печатного оборудования. Эффект радужности реализуется за счет смешения субтрактивного и аддитивного видов синтеза. Особенностью разработки таких изображений является высокая трудоемкость работ по их созданию. Это потребовало автоматизировать процесс путем внедрения средств программирования в пакеты векторной графики. Одним из наиболее распространенных программных продуктов является Visual Basic for Applications, которые можно интегрировать под формат CDR. Однако это приводит к ограничению внедрения таких элементов в графические изображения, поскольку требует обязательного наличия этого приложения в программном обеспечении и зависимости от приложений. Одним из путей решения данной проблемы является применение универсального формата векторной графики SVG, который достаточно просто задает векторные элементы, позволяет изменять алгоритм их позиционирования и получать самоподобные изображения с заданными параметрами, с последующим внедрением их в макеты изданий.

ЛИТЕРАТУРА

1. Кошин, А. А. Защита полиграфической продукции от фальсификации / А. А. Кошин. – М.: Синус, 1999. – 160 с.

УДК 004.414.2

М. И. Корзина, ст. преп. (САФУ, Архангельск);
М. И. Антонов, ассист. (Технологический колледж, САФУ, Архангельск);
Ю.Н. Корзин, ст. сист. инж. (ГК «Панорама Ритейл», Архангельск)

АВТОМАТИЗАЦИЯ ДИАГНОСТИКИ КОНТРОЛЬНО-КАССОВОЙ ТЕХНИКИ

Обслуживание контрольно-кассовых машин требует подготовки кадров и больших знаний в данной области. С каждым днем количество техники становится все больше и больше, как новых моделей, так и модификаций уже имеющихся. У каждой модели есть свой набор ошибок, инструкции и правил по эксплуатации, а, следовательно, с ростом количества техники растет и количество этих данных. Поэтому автоматизация диагностики контрольно-кассовых машин значительно бы упростила работу с ними.

В результате анализа предметной области выявлено, что такая информационная система должна иметь следующие возможности: использования без установки и наличия каких-либо дополнительных программных продуктов и библиотек; разграничения прав пользователей информационной системы; получения перечня ошибок по заданному номеру модели контрольно-кассовой техники (ККТ); поиска решения устранения ошибки по заданному коду ошибки; нахождения альтернативного решения по устранению ошибки; просмотра рейтинга решения по заданной проблеме в работе ККТ; группировки определенных моделей ККТ; редактирования перечня ошибок определенной ККТ; редактирования решения по устранению ошибки; получения сведений о выбранной ККТ; добавления новой контрольно-кассовой техники и сведений о ней; создания текстового отчета; вывода результата запроса; поиска необходимой информации; синхронизации базы данных между разными версиями информационной системы; воспользоваться подсказкой по использованию информационной системы специалисту.

В процессе проектирования системы были рассмотрены следующие аналоги: ALV Brain 1.31, Typer 1.23 SE, Expert Developer Pro МЭС 2.0 и др. Но данные программные продукты имеют ряд недостатков, например, отсутствие возможности создания текстового отчета, вывода результата запроса, иерархии каталогов данных и др.

Определены требования к информационной системе (ИС). ИС должна быть портативной и запускаться на любом устройстве под ОС Windows. В ИС должна присутствовать авторизация с разграничением прав пользователей, например, для возможности или ее отсутствия

добавления и редактирования данных. Должна быть возможность добавления и редактирования данных внутри информационной системы без перекомпиляции системы. Данные должны быть представлены в виде иерархии каталогов с возможностью их сортировки и поиска по заданным критериям.

В качестве реализации базы данных на этапе физического моделирования было выбрано решение в качестве СУБД “MySQL”, язык программирования “PHP”, “JavaScript” для элементов управления ИС, взаимодействие между “JavaScript” и “PHP” будет осуществляться при помощи “Ajax”, оболочкой для реализации БД был выбран программный продукт “cPanel”, а клиент-серверного приложения – “Notepad++”.

Проведено тестирование на следующих устройствах: ноутбук с ОС “Windows 7 Home Premium x64” в браузере “Opera 37”; планшетное устройство на ОС “Android 4.4.2” в браузере «Chrome»; мобильный телефон на ОС “Windows 8.1”; мобильный телефон на ОС “iOS 7”. На всех устройствах информационная система работает корректно.

Рабочая ИС удобна и проста в использовании с наличием справки при возникновении вопросов по ее работе. ИС работает на любой ЭВМ типа ПК или мобильного устройства независимо от архитектуры ЭВМ и ОС.