

VINNYTSIA NATIONAL TECHNICAL UNIVERSITY
BAKU STATE UNIVERSITY
TECHNICAL UNIVERSITY VARNA
SOKHUMI STATE UNIVERSITY
GEORGIAN TECHNICAL UNIVERSITY
EUROPEAN UNIVERSITY
CDM A/S
LUBLIN UNIVERSITY OF TECHNOLOGY
OPOLE UNIVERSITY OF TECHNOLOGY
LISBON NEW UNIVERSITY
ACADEMY OF LABOR, SOCIAL RELATIONS AND TOURISM
PETRO MOHYLA BLACK SEA STATE UNIVERSITY
KREMENCHUK MYKHAILO OSTOHRADSKYI NATIONAL UNIVERSITY



PROCEEDINGS

Of The Eleventh International Scientific-Practical Conference
INTERNET-EDUCATION-SCIENCE - 2018



Ukraine Vinnytsia VNTU

22 - 25 May, 2018

Друкується за рішенням Ученої ради Вінницького національного технічного університету
Міністерства освіти і науки України

Відповідальний за випуск В. В. Грабко

Підготовлено до друку: Т. О. Савчук, С. І. Петришин

Доповіді у збірнику згруповані по секціях, відповідно до основних напрямків конференції:

- А. Інтелектуальні інформаційні технології
- В. Комп'ютерні мережеві технології
- С. Комп'ютерна інженерія
- Д. Математичне моделювання
- Е. Комп'ютерні технології та Інтернет в інформаційному суспільстві
- Ф. Інформаційні технології та Інтернет у навчальному процесі та наукових дослідженнях
- Г. Геоінформаційні системи

Матеріали доповідей також представлені на Web-сайті конференції (<http://ies.vntu.edu.ua>), що містить електронну версію даного збірника і базу даних з відомостями про учасників конференції.

Тексти доповідей друкуються в авторській редакції.

«ІНТЕРНЕТ-ОСВІТА-НАУКА-2018», Одинадцята міжнародна
I-73 науково-практична конференція ІОН-2018, 22-25 травня, 2018 :
Збірник праць. – Вінниця : ВНТУ, 2018 –343 с.

ISBN 978-966-641-728-5

Одинадцята міжнародна науково-практична конференція «ІНТЕР-
НЕТ-ОСВІТА-НАУКА-2018» (ІОН-2018) присвячена обговоренню питань
застосування в освіті та наукових дослідженнях нових інформаційних
технологій, що опираються на можливості Інтернет.

УДК 378 + 004

The Eleventh International Scientific-Practical Conference “INTERNET-EDUCATION-SCIENCE-2018” (IES-2018) is dedicated to the discussion of questions of application of new information technologies based on the Internet opportunity in education and scientific researches.

The reports in the Conference Proceeding are grouped on the following sections according to the directions of the Conference:

- A. Intellectual information technologies
- B. Computer network technologies
- C. Computer engineering
- D. Mathematical modeling
- E. Computer technologies and the Internet in informational society
- F. Informational technologies and Internet in education process and scientific research activities
- G. Geoinformation systems

All reports are also submitted on the Conference Web-site (<http://ies.vntu.edu.ua>), which is containing the electronic version of this Conference Proceeding and database with the information about the Conference participants.

The text of the reports are printed in the author's version.

Одиннадцатая международная научно-практическая конференция «ИНТЕРНЕТ-ОБРАЗОВАНИЕ-НАУКА-2018» (ИОН-2018), посвящена обсуждению вопросов применения в образовании и научных исследованиях новых информационных технологий, с использованием возможностей Интернет.

Доклады в сборнике сгруппированы по секциям, соответствующим основным направлениям конференции:

- A. Интеллектуальные информационные технологии
- B. Компьютерные сетевые технологии
- C. Компьютерная инженерия
- D. Математическое моделирование
- E. Компьютерные технологии и Интернет в информационном обществе
- F. Информационные технологии и Интернет в образовательном процессе и научных исследованиях
- G. Геоинформационные системы

Материалы докладов представлены также на Web-сайте конференции (<http://ies.vntu.edu.ua>), содержащем электронную версию данного сборника и базу данных со сведениями об участниках конференции.

Тексты докладов печатаются в авторской редакции.

ГОЛОВА КОНФЕРЕНЦІЇ

Володимир ГРАБКО, Україна

СПІВГОЛОВИ КОНФЕРЕНЦІЇ

Олександр РОМАНЮК, Україна

Абель МАГЕРРАМОВ, Азербайджан

Росен ВАСИЛЕВ, Болгарія

Зураб ХОНЕЛІДЗЕ, Грузія

Арчіл ПРАНГІШВІЛІ, Грузія

Ерік РОСЕНКРАНТЗ, Данія

Петр КОЦЕЙКО, Польща

Марек ТУКЕНДОРФ, Польща

Антонио РЕНДАС, Португалія

Леонід КЛИМЕНКО, Україна

Вікторія БУЯШЕНКО, Україна

Михайло ЗАГІРНЯК, Україна

МІЖНАРОДНИЙ ПРОГРАМНИЙ КОМІТЕТ

Азербайджан

Алекпер Алієв

Грузія

Ромео ГАЛДАВА

Теодор ЗАРКУА

Гамлет МЕЛАДЗЕ

Отар НАТРОШВІЛІ

Польща

Вальдемар ВУЙЦИК

Павел КОМАДА

Крістіна МАЦЕК-КАМІНСЬКА

Португалія

Валентина Василенко

Болгарія

Христо СКУЛЕВ

Адріана АЛЄКСАНДРОВА

Україна

Сергій ПАВЛОВ

Віктор МІЗЕРНИЙ

Тамара САВЧУК

Олексій АЗАРОВ

Андрій ЯРОВИЙ

Максим МУСІЄНКО

Тетяна СЕМИГІНА

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ

Голова оргкомітету

Тамара Савчук

члени оргкомітету

Сергій Петришин, Наталія Приймак,

Володимир Озеранський, Ольга Ольшанська,

Любов Ваховська, Тамара Болотова, Василь Ковальчук,

Ліана Нечепуренко, Михайло Розводюк,

Анатолій Власюк, Володимир Барсагаєв, Вікторія Решетник

ПРЕДСЕДАТЕЛЬ КОНФЕРЕНЦИИ

Владимир Грабко, Украина

СОПРЕДСЕДАТЕЛИ КОНФЕРЕНЦИИ

Александр РОМАНЮК, Украина

Абель МАГЕРРАМОВ, Азербайджан

Росен ВАСИЛЕВ, Болгария

Зураб ХОНЕЛИДЗЕ, Грузия

Арчил ПРАНГИШВИЛИ, Грузия

Эрик РОСЕНКРАНТЗ, Дания

Петр КОЦЕЙКО, Польша

Марек ТУКЕНДОРФ, Польша

Антонио РЕНДАС, Португалия

Леонид КЛИМЕНКО, Украина

Виктория БУЯШЕНКО, Украина

Михаил ЗАГИРНЯК, Украина

МЕЖДУНАРОДНЫЙ ПРОГРАММНЫЙ КОМИТЕТ

Азербайджан

Алекпер Алиев

Грузия

Ромео ГАЛДАВА

Теодор ЗАРКУА

Гамлет МЕЛАДЗЕ

Отар НАТРОШВИЛИ

Польша

Вальдемар ВУЙЦИК

Павел КОМАДА

Кристина МАЦЕК-КАМИНСКАЯ

Португалия

Валентина Василенко

Болгария

Христо СКУЛЕВ

Адриана АЛЕКСАНДРОВА

Украина

Сергей ПАВЛОВ

Виктор МИЗЕРНЫЙ

Тамара САВЧУК

Алексей АЗАРОВ

Андрей ЯРОВОЙ

Максим МУСИЕНКО

Татьяна СЕМИГИНА

ОРГАНИЗАЦИОННЫЙ КОМИТЕТ

Председатель оргкомитета Тамара Савчук

члены оргкомитета

Сергей Петришин, Наталия Приймак,

Владимир Озеранский, Ольга Ольшанская,

Любовь Ваховская, Тамара Болотова, Василий Ковальчук,

Лиана Нечепуренко, Михаил Розводюк,

Анатолий Власюк, Владимир Барсагаев, Виктория Решетник

CHAIRMAN OF THE CONFERENCE

Volodymyr Grabko, Ukraine

COCHAIRMAINS OF THE CONFERENCE

Olexander ROMANYUK, Ukraine
Abel MAHARRAMOV, Azerbaijan
Rosen VASILEV, Bulgaria
Zurab KHONELIDZE, Georgia
Archil PRANGISHVILI, Georgia
Erik ROSENKRANTZ, Denmark
Piotr KACEJKO, Poland
Marek TUKENDORF, Poland
António RENDAS, Portugal
Leonid KLEMENKO, Ukraine
Viktoriiia BUIASHENKO, Ukraine
Mykhaylo ZAGIRNYAK, Ukraine

INTERNATIONAL PROGRAMME COMMITTEE

Azerbaijan	Alekper ALIEV
Georgia	Romeo GALDAVA Teodore ZARKUA Hamlet MELADZE Otar NATROSHVILI
Poland	Waldemar WÓJCIK Paweł KOMADA Krystyna MACEK-KAMIŃSKA
Portugal	Valentina VASSILENKO
Bulgaria	Hristo SKULEV Adriana ALEKSANDROVA
Ukraine	Sergey PAVLOV Viktor MIZERNYY Tamara SAVCHUK Oleksiy AZAROV Andriy YAROVYY Maksym MUSIYENKO Tetyana SEMIGINA

ORGANIZING COMMITTEE

Chairman of the committee	Tamara Savchuk
members of the committee	Serhii Petryshyn, Nataliia Pryimak, Vladimir Ozeranskyy, Olga Olshanska, Lubov Vahovska, Tamara Bolotova, Vasyl Kovalchuk, Liana Nechepurenko, Mykhaylo Rozvodyuk, Anatoly Vlasyuk, Volodymyr Barsagaev, Victoria Reshetnyk

ОСНОВНІ НАПРЯМКИ РОБОТИ КОНФЕРЕНЦІЇ

СЕКЦІЯ А. Інтелектуальні інформаційні технології.

СЕКЦІЯ В. Комп'ютерні мережеві технології.

СЕКЦІЯ С. Комп'ютерна інженерія.

СЕКЦІЯ D. Математичне моделювання.

СЕКЦІЯ Е. Комп'ютерні технології та Інтернет в інформаційному суспільстві.

СЕКЦІЯ F. Інформаційні технології та Інтернет у навчальному процесі та наукових дослідженнях.

СЕКЦІЯ G. Геоінформаційні системи

ОСНОВНЫЕ НАПРАВЛЕНИЯ РАБОТЫ КОНФЕРЕНЦИИ

СЕКЦИЯ А. Интеллектуальные информационные технологии.

СЕКЦИЯ В. Компьютерные сетевые технологии.

СЕКЦИЯ С. Компьютерная инженерия.

СЕКЦИЯ D. Математическое моделирование.

СЕКЦИЯ Е. Компьютерные технологии и Интернет в информационном обществе.

СЕКЦИЯ F. Информационные технологии и Интернет в образовательном процессе и научных исследованиях.

СЕКЦИЯ G. Геоинформационные системы

BASIC STRAIGHTWAY WORK CONFERENCE

SECTION A. Intellectual information technologies.

SECTION B. Computer network technologies.

SECTION C. Computer engineering.

SECTION D. Mathematical modeling.

SECTION E. Computer technologies and the Internet in informational society.

SECTION F. Informational technologies and Internet in education process and scientific research activities.

SECTION G. Geoinformation systems



ВІННИЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

Хмельницьке шосе, 95, Вінниця, 21021, Україна

Тел.: (0432) 56-08-48, Email: vntu@vntu.edu.ua

<http://www.vntu.edu.ua>

Вінницький національний технічний університет - добре відомий як в Україні, так і далеко за її межами, навчальний заклад IV рівня акредитації. За денною формою в університеті навчається більше 4000 студентів, за заочною - більше 1500, в аспірантурі та докторантурі - 140, на підготовчому відділенні - 53. Навчально-наукову діяльність в університеті здійснює 42 кафедри, які створили 33 філії на підприємствах м. Вінниці та області.

Навчання в ВНТУ здійснюється з 28 спеціальностей за освітньо-професійними програмами «Бакалавр» та з 22 спеціальностей за освітньо-професійними програмами «Магістр» за навчальними планами, в яких інтегровано кращі риси вітчизняної систем вищої освіти. Крім опанування основної спеціальності студенти мають можливість за заочною формою набути другу спеціальність. Студенти мають можливість вивчати англійську мову на рівні технічного перекладача і вже за рік до завершення навчання здатні працювати в іноземних представництвах та за кордоном. Крім того, в університеті впроваджено програми академічної мобільності «Подвійний диплом» із університетами-партнерами Польщі, Португалії, Болгарії, Грузії, Чехії.

Університетські корпуси займають 25 гектарів землі в місті, ще на 10 гектарах в 100 кілометрах від Вінниці розкинувся спортивно-оздоровчий табір університету.

Університет має ефективну систему підготовки наукових кадрів вищої кваліфікації, яка не має аналогів. Підготовку науково-педагогічних кадрів здійснюють в аспірантурі з 21 спеціальності і докторантурі - з 10 спеціальностей, функціонують 6 спеціалізованих рад по захисту докторських та кандидатських дисертацій з 10 спеціальностей. За останні 10 років науковцями університету захищено 31 докторських і 249 кандидатських дисертацій.

Університет випускає громадсько-політичний часопис "Імпульс", який користується попитом в усьому регіоні, та наукові журнали, визнані Вищою атестаційною комісією України фаховими в галузях технічних, економічних та педагогічних наук: "Вісник Вінницького політехнічного інституту", "Оптико-електронні інформаційно-енергетичні технології", "Інформаційні технології та комп'ютерна інженерія", "Сучасні технології, матеріали і конструкції в будівництві". Журнал "Sententiae" спеціалізується в галузі філософських наук.

ВНТУ - колективний член Українського відділення Всесвітнього товариства інженерів - енергоменеджерів, Всесвітнього оптичного товариства (SPIE), Європейського товариства "Ергономіка та людський фактор", Міжнародної академії наук вищої школи, Міжнародної кадрової академії, Міжнародної асоціації комп'ютерної техніки (АСМ) (м. Нью-Йорк). З 1994 р. ВНТУ є єдиним від України асоційованим членом Міжнародної асоціації винахідницьких організацій (IFIA) з штаб-квартирою в м. Женеві. З 2004 року - колективний член Міжнародної асоціації університетів.

ВНТУ готує фахівців з вищою освітою рівня магістра та доктора філософії з технічних наук для 25 країн Африки, Азії, Південної та Центральної Америки.



БАКИНСКИЙ ДЕРЖАВНИЙ УНИВЕРСИТЕТ

Баку, Азербайджан

Тел.: (012) 439 05 17, Email: info@bsu.az

<http://bsu.edu.az/>

Университет, который имеет богатую историю, как флагман учебных заведений в Азербайджане, в настоящее время является известным научным центром. Университет - это центр прогрессивных идей и национальной мысли в Азербайджане. Здесь получил образование всемирно известный политик Гейдар Алиев, наш знаменитый земляк Л.Д. Ландау, лауреат Нобелевской премии в 1922-1924 годах, а также сотни ученых, представителей интеллигенции и выдающиеся дипломаты.

Согласно Указу общенационального лидера Азербайджанской Республики Гейдара Алиева от 15 июня 2000 Университета был присвоен статус самоуправления (автономии), с тех пор Университет осуществляет деятельность в соответствии с данным указом. В настоящее время в Бакинском Государственном Университете на 16 факультетах идет подготовка по 55 специальностям и различным научным направлениям, в том числе - 153 специалиста в магистратуре. Ежегодно абитуриенты, поступающие в Бакинский Государственный Университет, проходят большой конкурс: по подсчетам, в среднем на одно место подают документы 3 абитуриента, а по нескольким специальностям даже 10 абитуриентов. Основанную Президентом Азербайджанской республики «Президентскую стипендию» получают 100 студентов-первокурсников, которые имеют высокие баллы в учебе. Из них примерно 40 человек получают образование в Бакинском Государственном Университете. В последние годы началась подготовка кадров по новым специальностям, таким как землеустройства и инспекция земли, кадастр земли, немецкий язык и литература. Студенты, получающие образование в Университете, окружены всесторонней заботой, в их распоряжение переданы аудитории и лаборатории, оснащенные необходимой материально-технической базой. Учебный процесс Университета, основанный на демократических принципах, направлен на подготовку творческих и свободомыслящих лиц.

Наряду со спецпредметами особое внимание в образовании уделяется изучению иностранных языков. С этой целью, в распоряжение студентов передано свыше 10 лингафонных кабинетов, оснащенных новейшим оборудованием. Научная библиотека Университета, фонд которой насчитывает более 2,5 миллионов экземпляров литературы, имеет 12 читальных залов, 5 отделений абонемента, которыми ежедневно пользуются 15 000 преподавателей и студентов.

В Университете создан великолепный спортивно-оздоровительный комплекс. Наряду с успехами в области науки и образования, он помогает стране в воспитании здорового молодого поколения. Университет, который готовит высокоспециализированные кадры, является международным центром. В Университете 121 кафедра, включая кафедры естественных и гуманитарных наук, 37 научно-исследовательских и научных лабораторий, где работают 200 научных сотрудников, Научно-Исследовательский Институт Прикладной Математики и Научно-Исследовательский Институт по проблемам физики.

Международное отношение Университета с каждым днем распространяется. В настоящее время Университет сотрудничает со многими университетами мира и является членом Ассоциации Евразийских университетов, Ассоциации Университетов Прикаспийских стран, Ассоциации Университетов Черного моря, Ассоциации Европейских Университетов, а также осуществляет сотрудничество на основе двусторонних соглашений всеобщего научно-технического педагогического обмена.



ТЕХНІЧНИЙ УНІВЕРСИТЕТ – ВАРНА

<http://www.tu-varna.bg/>

Технічний університет Варни (TUV) був заснований в 1962 році Указом Ради Міністрів Народної Республіки Болгарії і Актом Національних зборів. Мета його створення полягала в забезпеченні умов для підготовки інженерних кадрів для суднобудування, транспорту, машинобудування, електроенергетики і зв'язку. Спочатку університет був названий Вищим інститутом механіки і електротехніки в Варні і включав три факультети: машинобудування, електротехніка і суднобудування. Перший прийом студентів Технічного університету Варни відбувся у 1963 році за такими спеціальностями: Двигуни внутрішнього згоряння; морська техніка і механізми суднобудування; механічні, електричні машини і пристрої радіозв'язку, телекомунікаційне обладнання; автоматика та телеметрія і автоматика.

За 40 років діяльності Технічний університет Варна підготував 28976 фахівців в області «Інженерія», «Природничі науки, Математика та інформатика», "Соціально-економічні та правові дослідження", "Педагогічні науки».

В даний час ТУ Варна має будівлі загальною площею 67542 квадратних метрів. Всі будівлі університету побудовані після 1968 р. Університет має три студентських гуртожитки з загальною кількістю 1450 місць і дві столових. Студентські гуртожитки знаходяться на відстані близько 750 метрів від будівель університету. Компактність доступу на кампусі університету і кафедр створює сприятливі умови для життя і роботи студентів.

В рамках університету освіта і наукові дослідження нерозривно пов'язані між собою. Синергія між ними призводить до зростання і розвитку. Освіта є вбудованою культурою, яка є основою академічних областей університету, в той час як дослідження вимагають дій, що виходять за межі академічного середовища. Інноваційні рішення від Технічного університету - Варна перетворилися в модернізовану лабораторію і сучасне обладнання для проведення експериментів. Велика кількість висококваліфікованих викладачів, вчених, інженерів і техніків і керівників охоплюють широкий діапазон знань і досвіду. Модернізація навчальних програм проводиться на основі вимог ринку ІТ-фахівців з останніми рекомендаціями IEEE (Всесвітньої організації інженерної електротехніки та електроніки) і ACM (Всесвітньої асоціації обчислювальної техніки) і поточних наукових програм провідних світових університетів.

Технічний університет Варни є автономним установою, що включає 4 факультети, 2 коледжі, деканат іноземних студентів і факультет іноземних мов. Факультети мають у складі 31 кафедру.

Факультет машинобудування та технологій Факультет кораблебудування Факультет електротехніки Факультет комп'ютерних наук і автоматизації Технічний університет у Варні є державним освітнім закладом, який орієнтований на задоволення суспільних потреб в підготовці кваліфікованих інженерів і підтримку технічного розвитку в світі, який піддається глобальним, технологічним і культурним змінам. На основі тісного співробітництва з промисловістю, активним дослідницьким сектором, європейськими університетами та власних досягненнях і традиціях, університет готує висококваліфікованих фахівців, орієнтованих на ринок, зокрема, в областях суднобудування і навігації; зв'язку та обчислювальної техніки і технологій; машинобудування та технологій; електротехніки, електроніки та автоматизації; електроенергетики; промислового управління; екології і технології захисту навколишнього середовища.



СУХУМСКИЙ ДЕРЖАВНИЙ УНИВЕРСИТЕТ

<http://www.sou.edu.ge/>

История Сухумского государственного университета начинается 5 февраля 1932 года, когда был основан Сухумский педагогический институт. Сначала в университете было всего два факультета. Но к началу 1960-х годов Педагогический институт стал ведущим учебным и научным центром, где преподавательский процесс был представлен на грузинском, абхазском и русском языках. В 1979 году Сухумский педагогический институт был преобразован сначала в Сухумский государственный университет, а затем (в том же году) в Абхазский государственный университет.

После политических событий 1989 года грузинский сектор университета с большинством профессоров и студентов отделился, а 14 мая 1989 года на его базе был основан Сухумский филиал Тбилисского государственного университета, который с декабря 1993 года продолжил функционировать в Тбилиси. В июле 2007 года Сухумский филиал Тбилисского государственного университета преобразован в Сухумский университет, а в декабре 2008 года Сухумский университет был преобразован в Сухумский государственный университет.

В настоящее время в Сухумском государственном университете действует семь факультетов: юридический, факультет экономики и бизнеса, факультет образования, факультет гуманитарных наук, факультет социальных и политических наук, факультет математики и компьютерных наук, факультет естественных наук и здравоохранения, на которых обучается около 3000 студентов. В университете представлены все 3 степени обучения.

В университете неоднократно проводились финалы школьных олимпиад Грузии по информатике и четвертьфиналы Чемпионата Мира по программированию среди университетов для региона Грузии. В этом году Сухумский ГУ будет принимать участников международной олимпиады по программированию на Кубок Векуа.

Ректором Сухумского ГУ является профессор Зураб Хонелидзе.



ГРУЗИНСЬКИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

Тбілісі, Грузія

Тел.: (+995 32) 2 36 50 93, (+995 32) 2 36 51 53

Факс: (+995 32) 2 36 51 55

Email: info@gtu.ge, rectoroffice@gtu.ge, pr@gtu.ge

<http://www.gtu.ge>

Грузинский технический университет - высшее учебное заведение Грузии, ведущий и крупнейший технический университет страны. Расположен в г. Тбилиси.

История Грузинского технического университета начинается в 1922 году, когда в Тбилисском государственном университете появился политехнический факультет, который через некоторое время стал функционировать как отдельный, независимый институт. В 1930 году Грузинский политехнический институт был разделен на несколько высших учебных заведений, которые специализировались в разных научных областях, а в 1933 году они снова объединились и образовали Транскавказский индустриальный институт. Свое нынешнее название университет получил в 1992 году.

В настоящее время в университете функционируют следующие факультеты: строительный; энергетики и телекоммуникаций; горно-геологический; химических технологий и металлургии; транспорта и машиностроения; архитектуры, урбанистики и дизайна; бизнес-инжиниринга; информатики и систем управления; международная школа дизайна; аграрных наук и инжиниринга биосистем.

На базе университета проходит обучение бакалавров, магистров, а также предлагаются докторские программы.

Университет является участником большого количества международных грантовых научных проектов.

В распоряжении университета современная материально-техническая база, соответствующая международным стандартам и нормам. Библиотека Грузинского технического университета, основанная в 1922 году, является крупнейшей в Грузии. Книжный фонд библиотеки составляет около 2 млн. экземпляров научной и художественной литературы. Ректором университета является академик АН Грузии, Арчил Прангишвили.

В университете систематически проводятся международные научные конференции и симпозиумы.

ГТУ является хост-университетом при проведении полуфинала чемпионата мира по программированию среди ВУЗов для Южно-Кавказского региона. На базе университета систематически проводятся различные высокорейтинговые международные научные конференции, а также студенческие олимпиады. ГТУ дважды принимал участников международной олимпиады по программированию на Кубок Векуа.



ЕВРОПЕЙСКИЙ УНИВЕРСИТЕТ

<http://www.esu.edu.ge/>

Европейский Университет был основан в 1993 году. На данный момент он представлен 3-мя факультетами, 18-ю учебными программами и 2-мя учебными курсами, на которых обучается более 1500 студентов. Университет укомплектован высококвалифицированными профессорами и преподавателями, многие из которых получили образование в ведущих европейских университетах и имеют многолетний научно-педагогический стаж работы в университетах и научно-исследовательских институтах Грузии, Европы и США.

Университет оснащён современной технической базой, богатой библиотекой и всем необходимым инвентарём. У студентов имеется возможность полноценно участвовать в учебном процессе, научных исследованиях и других видах университетской активности, а также получать университетские гранты и обучаться за рубежом.

Европейский университет ориентирован на содействие межкультурному диалогу, поэтому формирует такую образовательную среду, в которой каждый студент может чувствовать себя полноправным членом социума, несмотря на свою этническую, расовую, религиозную или другую принадлежность. С этой же целью иностранные и грузинские студенты университета задействованы в совместных двуязычных проектах различного профиля.

Миссия Европейского университета – с помощью постоянного развития инновационных идей, профессионализма, развития и обмена знаниями подготовить конкурентоспособные кадры для местного и международного трудового рынка. Задача университета – с помощью научно-исследовательского, свободного и комплексного мышления поддерживать развитие передовых научных отраслей. Университет ориентирован на европейские ценности и ставит целью воспитать достойных членов демократического общества.

Должное внимание уделяется развитию IT-технологий. Имеются учебные программы соответствующего профиля. Университет уже имеет опыт организации таких высокорейтинговых международных олимпиад по информатике, как полуфинал Чемпионата Мира по программированию среди Вузов (ACM ICPC), Открытый Чемпионат Южного Кавказа и Международная олимпиада на Кубок И.Н.Векуа.

Ректором университета является господин Лаша Канделакишвили.



CDM

Коккедаль, Данія

тел: +45 70 27 19 27 , Email: info@cdm.dk

<http://www.cdm.dk>

Данська компанія CDM була заснована Хеленою Крох в 1986 році. Починалася CDM як телемаркетингова компанія під назвою Canvas Marketing. Через рік, в 1987 році, керівництво компанії усвідомило необхідність систематизації роботи співробітників, і міс Крох найняла розробника для створення комп'ютеризованої телемаркетингової системи для обробки інформації. Концепція системи була придумана містером Еріком Розенкранцем, партнером міс Крох.

У 1988 році була створена компанія CDM Sales Systems на чолі з містером Розенкранцем, і Canvass Marketing змінила назву на CDM TeleMarketing. І, звичайно ж, у CDM Sales Systems була власна система продажів.

І бізнес і системи розвивалися у відповідності з новими потребами і ринковими тенденціями. До кінця 90х обидві компанії були об'єднані в CDM на чолі з міс Крох і містером Розенкранцем. Компанія, як і завжди, залишається сфокусованою на оптимізації продажів клієнтів та маркетингу.

Основне заняття CDM сьогодні – виробництво і продаж CRM-систем для підтримки і оптимізації продажів і маркетингових процесів. Клієнти CDM – великі Скандинавські компанії в сфері телекомунікацій, фінансів і у фармацевтичному секторі. Представництва CDM в Данії і Швеції підтримують близько 15000 користувачів.

Сім років тому CDM підписала договір про співпрацю з Microsoft. Метою співробітництва є створення ще більш інтегрованих вертикальних рішень для клієнтів.

Перший продукт співпраці між CDM і Microsoft – CRM система для компаній, що працюють в області фармацевтики, під назвою CDM Pharma, вже вийшов у продаж.

В останні роки CDM успішно здійснює поступовий перехід від своєї першої платформи Smalltalk платформи на платформу . Net.

У 2007 році CDM розпочала співпрацю з Вінницьким національним технічним університетом. Метою співробітництва є підготовка фахівців в сфері розробки програмного забезпечення та CRM технологій. У зв'язку з цим CDM проводить курси на базі ВНТУ. Термін навчання – 1 рік, на курсах студенти знайомляться з бізнес поняттями CRM і вивчають технології Microsoft.

В кінці 2008 року CDM відкрило своє перше представництво на Україні, в місті Вінниця, основною спеціалізацією якого є розробка мобільних застосунків, веб-ресурсів про нерухомість та CRM-систем на технологіях Microsoft.



ДЕРЖАВНИЙ УНІВЕРСИТЕТ ЛЮБЛІНЬСЬКА ПОЛІТЕХНІКА

ul. Nadbystrzycka 38D, 20-618, Люблін, Республіка Польща
Tel./fax. +48(081) 5384 657
<http://www.pollub.pl/>

Люблінська Політехніка була заснована 13 травня 1953 року як Вечірня Інженерна Школа з ініціативи люблінських техніків та інженерів. Одночасно з виникненням школи почав функціонувати її перший Відділ – Механічний. У 1965 році навчальний заклад змінив назву на Вищу Інженерну Школу. В цьому ж році створено Відділ Будівництва, а попереднього року - Електричний Відділ. Глибокі зміни у вищій школі відбулися в 70-ті роки. В 1977 році назву Вищої Інженерної Школи змінено на Політехніку. У 1988 році створено Відділ Управління і Основ Техніки, які 28 грудня 2007 року перетворено на Відділ Управління. У 2003 році Електричний Відділ перетворено на Відділ Електротехніки і Інформатики. Від грудня 2007 року у вищому навчальному закладі функціонує шостий відділ – Відділ Основ Техніки. Сенат Люблінської Політехніки Ухвалою від 3 липня 2003 року встановив день 13 травня Святом Люблінської Політехніки.

На даний момент Політехніка складається з 6 факультетів, 16 напрямків та понад 50 спеціальностей. У Політехніці діють підлеглі ректору підрозділи, які реалізують окремі наукові, дидактичні завдання та надають послуги. Підрозділи університету:

- бібліотека;
- бюро розвитку і кооперації;
- інформатичний центр;
- центр інновацій і передових технологій;
- Люблінський інкубатор підприємництва;
- Люблінський центр трансферу технологій.

На території Студентського містечка Люблінської Політехніки знаходиться 14 дидактичних корпусів (частина з них – це палаци – пам'ятки архітектури) між вулицею Надбистжицка і долиною річки Бистриця (на південь від центру Любліна). Біля університетських корпусів знаходиться їдальня, добре налагоджене транспортне сполучення з містом, 4 гуртожитки для студентів, кілька клубів, спортивний зал, танцювальний зал. Адміністративна база навчального закладу знаходиться в пам'ятних будинках давнього палацу Собеських по вул. Бернардинській в центрі Любліна.

При Люблінській Політехніці функціонують студентські організації, як-от - Самоврядування Студентів Люблінської Політехніки - Бюро Студентських Кар'єр Політехніки - журнал Студентів Люблінської Політехніки «Плагіат» - Студентська Фотографічна Агенція (СФА) - Студентська Ініціатива Культури StuArt

При університеті працюють також такі заклади:

- Хор Люблінської Політехніки - Колектив Пісні і Танцю Люблінської Політехніки - Колектив Танцю Люблінської Політехніки «ІАМЗА» - Група Сучасного Танцю Люблінської Політехніки - музичні гурти («Whisky») Активно діють такі спортивні клуби: - Клуб Водолазів «ПАСКУДА» - Секція Спортивної Стрільби Навчального Клубу АЗС ПЛ - Клуб Кік-боксингу - Яхт-клуб Люблінської Політехніки - Клуб Рибалок "ESOX".



ОПОЛЬСЬКИЙ ПОЛІТЕХНІЧНИЙ УНІВЕРСИТЕТ

<http://www.po.opole.pl/>

Опольська Політехніка - це технічний університет, який має майже півстолітні традиції академічної освіти на європейському рівні. Університет займається підготовкою спеціалістів за технологічним, економічним, гуманітарним та медичним напрямками. Університет дуже швидко розвивається та надає підготовку за технічним, економічним, гуманітарним та медичним напрямками. На шести факультетах навчаються більше 11 000 студентів, щорічно близько 200 студентів – іноземців отримують освіту в Опольській політехніці.

Університет має оснащену матеріальну базу, в сучасних наукових лабораторіях вчені та студенти можуть створювати імітацію землетрусу або досліджувати високу напругу та інфразвук. Випускники університету отримують диплом, який забезпечує конкурентоспроможність на європейському ринку праці.

Для студентів працює багато тематичних гуртків, можна приєднатися до академічного хору або студентського оркестру. Найяскравішим акцентом студентського життя вважаються Piastonia - фантастична вечірка, на час якої студенти Опольських вузів беруть владу в місті в «свої руки». Місто Ополе і Опольський регіон - це місцевість для туризму, вивчення культури та звичаїв.

Університет співпрацює з більше 100 європейськими навчальними закладами.



ЛИСАБОНСЬКИЙ УНІВЕРСИТЕТ NOVA

Лисабон, Португалія
<http://www.unl.pt/>

Был основан 11 августа 1973. Название Universidade Nova De Lisboa (NOVA) означает творчество и инновации. Гордясь своей молодостью, как самый молодой государственный университет на метрополийной территории Лиссабона, NOVA проходит через три муниципалитеты: Лиссабон, Алмада и Оэйраш. Несмотря на свою молодость, тридцать семь лет существования в столичном регионе обеспечивают солидный опыт и широкий спектр курсов во всех областях знаний. В настоящее время университет имеет более 19.500 студентов, около 1591 преподавателей и 679 сотрудников. Университет, как государственное учреждение, финансируется главным образом португальским Министерством образования.

В состав университета NOVA входят 9 единиц, имеющие научную, академическую и административную автономию:

- Faculdade de Ciências e Tecnologia (Факультет Науки и Технологий);
- NOVA School of Business and Economics (Экономический Факультет);
- NOVA Information Management School (Информационный менеджмент);
- Faculdade de Direito (Юридический Факультет);
- Социальных и гуманитарных наук: FCSH (Faculty of Social and Human Sciences);
- NOVA Medical School (Медицинский Факультет);
- Instituto de Tecnologia Química e Biológica (Институт Химических и Биологических технологий);
- Instituto de Higiene e Medicina Tropical (Институт Гигиены и тропической медицины);
- Escola Nacional de Saúde Pública (Институт Общественного здоровья).

Университет NOVA имеет 42 научно-исследовательских подразделений, финансируемых Фондом Науки и Технологий Португалии, а также сотрудничает со многими другими университетами по всему миру. В дополнение к интенсивному обмену в Европе, университет развивает широкое сотрудничество с Бразилией и португалоязычными странами, а также активно сотрудничает в инициативах, продвигаемых правительством Португалии, в частности в отношении сотрудничества с американскими университетами, как Университет штата Техас в Остине (UTA), Массачусетский технологический институт (MIT) и университета университета Карнеги-Меллона (CMU), в рамках программ магистратуры и аспирантов и научно-исследовательских проектов.

NOVA является единственным португальским университетом, который входит в 50 лучших университетов мира в возрасте до 50 лет, согласно данным рейтинга QS World University Rankings.

Лиссабонский Университет NOVA имеет роскошную современную библиотеку, оснащенную новейшими техническими средствами и литературой.

Гордостью университета является Madan Parque - один из лучших инкубаторов университетских научно-технологических предприятий, который в 2011 году занял третье место в международном конкурсе 30 стран «Лучший научно-предпринимательский инкубатор» («Best Science Based Incubator").



АКАДЕМІЯ ПРАЦІ, СОЦІАЛЬНИХ ВІДНОСИН І ТУРИЗМУ

Київ, Україна

Тел.: (044) 522-49-40, E-mail: info@socosvita.kiev.ua,

<http://www.socosvita.kiev.ua/>

Академію праці, соціальних відносин і туризму було засновано в травні 1993 року відповідно до Закону України "Про освіту" та постанови Президії Федерації профспілок України. Мета Академії полягає в якісній підготовці фахівців у сферах трудових ринкових відносин, управління організацією, права, соціального партнерства, охорони навколишнього середовища. Саме таких фахівців потребують сьогодні профспілкові організації, державні і недержавні підприємства. Сьогодні Академія — це провідний вищий навчальний заклад України, національний осередок сучасних знань про суспільство та соціальні технології.

Академія має 4-й рівень акредитації, здійснює підготовку бакалаврів, магістрів та докторів філософії, а також надає післядипломні кваліфікації працюючим професіоналам. У структурі Академії діють Юридичний факультет, Факультет економіки, соціальних технологій та туризму і Центр профспілкової освіти. Підготовку фахівців з восьми спеціальностей здійснюють викладачі чотирьох загально-академічних і дев'яти фахових кафедр, близько 80% з них мають науковий ступінь та/або вчене звання. Студенти АПСВТ проходять практику у провідних українських і міжнародних установах, які працюють у сферах юриспруденції, економіки, маркетингових і соціологічних досліджень, соціальної роботи, туристичного і готельного бізнесу. Академія має сучасну матеріально-технічну базу для повного забезпечення навчального та наукового процесу, творчого розвитку та відпочинку студентів і працівників. Відомі вчені, фахівці, політики, діячі культури і мистецтва, банкіри і підприємці запрошуються до роботи в Академії. Все це дає можливість отримати освіту як національних, так і європейських стандартів.

Викладачі та студенти беруть участь у науково-дослідній роботі, мають змогу публікувати її результати в періодичному науковому виданні «Вісник Академії праці, соціальних відносин і туризму».

Академія бере активну участь в міжнародній діяльності. Основними партнерами є вищі навчальні заклади з різних країн, що входять до Міжнародної Асоціації навчальних і наукових закладів з підготовки кадрів для соціально-трудової сфери. Партнерами Академії є також Університет Штайнбайса з Німеччини, Інститут поведінкової наук Університету Колорадо в Боулдері (США), Варшавський педагогічний університет ім. Януша Корчака, Міжнародна організація ЕСПАТ та ін.



ЧОРНОМОРСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ПЕТРА МОГИЛИ

Миколаїв, Україна

Тел.: (0512) 500-333, Факс: (0512) 500-069

E-mail: rector@chdu.edu.ua, <http://www.chdu.edu.ua>

Університет засновано на базі Миколаївського державного гуманітарного університету імені Петра Могили, який був створений Розпорядженням Кабінету Міністрів України від 19.03.2002 р. на базі Миколаївської філії Національного університету Києво-Могилянська академія, створеної постановою Кабінету Міністрів України № 712 від 03.07.1996 року, і розташовано на місці портової ремісничої школи, відкритої в 1862 році.

В університеті сформовано потужний науково-педагогічний колектив, який нараховує 52 доктори наук, 160 кандидатів наук, 12 академіків і членів-кореспондентів галузевих і зарубіжних академій наук, 12 заслужених діячів України та провідних професорів із США, Німеччини, Франції, Швейцарії, Польщі, Румунії, Південної Кореї, Італії, Японії, Китаю, Литви та інших країн. За час існування в університеті ім. Петра Могили викладали більш ніж 100 іноземних викладачів та 15 професорів з університетів США, які є лауреатами найпрестижнішої нагороди за викладання – програми імені Фулбрайта.

У 2009 університет приєднався до Magna Charta Universitatum – Великої хартії університетів та Асоціації університетів Європи.

Структуру університету складають чотири інститути, шість факультетів, науково-дослідна частина, відділення довузівської підготовки, дві науково-технічні бібліотеки, 3 спортивні зали, водна станція, їдальня та 3 кафе, видавництво; видається 13 фахових журналів. У 2008 році створено Тбіліський інститут Чорноморського національного університету імені Петра Могили.

В університеті функціонує аспірантура за 18 спеціальностями та докторантура – за 8. Захист дисертацій здійснюється у п'яти спеціалізованих вчених радах за 9 спеціальностями.

Нині ЧНУ ім. Петра Могили – сучасний багатопрофільний університет, у якому за 24 напрямками підготовки навчається близько 4000 студентів. У розпорядженні студентів – 12 навчальних корпусів, об'єднаних в один комплекс – кампус та 3 гуртожитки.

ЧНУ ім. Петра Могили сприяє всебічному розвитку особистості студента, в ньому створено та активно діють Студентська рада університету, профспілка студентів, юридична клініка «Veritas», екологічний клуб «Студентська екологічна ініціатива», кіноклуб, мовні клуби, танцювальна студія, ренесансний театр, студентські ЗМІ, зокрема газета «Вагант», 13 спортивних секцій тощо

Яскравим прикладом високого визнання є 43-є місце серед 200 найкращих вищих навчальних закладів України в щорічному рейтингу ВУЗів ЮНЕСКО «Топ-200 Україна» та 5-те серед кращих ВУЗів Південного регіону. Університет – єдиний вищий навчальний заклад, який представляв Україну та її систему вищої освіти на Конференції лідерів Таллуарської мережі, результати якої знайшли відображення в книзі D. Watsona, R. M. Hollistera, S. E. Stroud та E. Babcock «The Engaged University International Perspectives on Civic Engagement».



КРЕМЕНЧУЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ МИХАЙЛА ОСТРОГРАДСЬКОГО

<http://www.kdu.edu.ua>

Кременчуцький національний університет імені Михайла Остроградського бере початок з 1920 року, коли було засновано в місті Кременчуці перший вищий навчальний заклад - вищі педагогічні курси з українською мовою викладання. 21 серпня 1997 Кабінет Міністрів України прийняв Постанову "Про створення Кременчуцького державного політехнічного інституту" на базі Кременчуцької філії Харківського державного політехнічного університету, Крюківського машинобудівного і Кременчуцького автомеханічного технікумів. Структуру інституту склали сім факультетів і 17 кафедр. Через три роки він був реорганізований в Кременчуцький державний політехнічний університет. За цей час ВНЗ забезпечив промислові підприємства міста і Придніпров'я висококваліфікованими фахівцями, сформувавши технічну еліту регіону. Розпорядженням Кабінету Міністрів України № 92-р від 7 березня 2007р. Кременчуцькому державному політехнічному університету присвоєно ім'я великого математика Михайла Остроградського.

У серпні 2009 року КДПУ став першим на Полтавщині класичним університетом, 5 серпня 2009 року він отримує статус класичного університету (Кременчуцький державний університет імені Михайла Остроградського, а 21 серпня 2010р. указом Президента України № 863/2010 Кременчуцькому державному університету ім. М. Остроградського було надано статус національного. Станом на сьогодні навчальний процес в КрНУ забезпечують: два навчально-наукові інститути (Інститут електромеханіки, енергозбереження і систем управління, Інститут механіки і транспорту), чотири факультети (факультет електроніки та комп'ютерної інженерії; факультет економіки і управління; факультет права, гуманітарних і соціальних наук; факультет природничих наук), два коледжі (коледж Кременчуцького національного університету імені Михайла Остроградського; Комсомольський політехнічний коледж Кременчуцького національного університету ім. М. Остроградського) та 28 кафедр. В аспірантурі університету здійснюється підготовка кандидатів наук за 19 спеціальностями.

Сьогодні в КрНУ навчається понад 5000 студентів денної та заочної форм навчання; коледжі надають освітні послуги близько 2500 студентам щорічно. Університет співпрацює з 72 зарубіжними ВНЗ та дослідницькими інститутами в 25 країнах, бере участь в міжнародних програмах: ERASMUS+, TEMPUS, HORIZON 2020, OPEN WORLD, DAAD, FULBRIGHT.

СПИСОК АВТОРІВ

АВТОР	СТОРІНКИ	АВТОР	СТОРІНКИ
Alexey Stakhov	147	Груздо Ирина	254
Baeva Desislava	244, 310	Давиденко Євген	22
Basyuk Taras	160	Давидов Сергій	53
Beselia Lali	179	Давыденко Евгений	122
Gakh Dmitri	241	Дітковська Леся	289
Glushko Iryna	169	Дорогий Ярослав	100
Ivanov Ivan	244	Думанський Нестор	273
Kochladze Zurab	179	Закордонець Аліна	136
Leila Sulava	113	Замковий Олександр	67
Odisharia, Kakhaber	103	Заркуа Теодор	291
Rashkova Victoria	244, 310	Захарченко Сергій	87
Richard P. Megrelishvili	175	Іванова Світлана	293, 299
Stolyarevska Alla	2	Кабаченко Ірина	162
Temur Chilachava	113	Кандиба Ігор	287
Teteruk Svitlana	204	Карагодіна Марина	275
Tikhonov Victor	117	Качурівська Ганна	238
Tinatin Mshvidobadze	278	Качурівський Володимир	238
Абабий Виктор	83	Кільдишев Віталій	73
Абабий Константин	83	Кміть Владислав	59
Абрамова Ирина	167	Коваленко Олена	281
Аніскевич Світлана	17, 19	Козачук Андрій	165
Арсенюк Ігор	50	Кокая Гига	216
Архипова Евгения	171	Колесник Ірина	136
Афанасьєва Ирина	167	Колесницький Олег	212
Бенидзе Нана	155	Колодний Володимир	4
Білик Руслан	190	Кольцов Владислав	142
Блинов Сергій	127	Корецька Олександра	93
Бондар Світлана	209	Корчинська Олена	200
Боровська Таїса	124, 133, 136, 142	Корчиста Ольга	26
Буяшенко Вікторія	261	Котик Ольга	152
Ваховська Любов	10, 35	Кошопал Микола	307
Вернигора Інна	133	Крайник Ярослав	90
Верхось Дмитро	56	Крутенко Ігор	10
Волошин Костянтин	133	Кудрявцев Дмитро	4, 30
Габисония Инга	155	Кузнецов Юрій	106
Гайдаш Богдан	235	Кулик Олександр	30
Головко Ярослав	275	Кунанець Наталія	152, 181
Голубь Надежда	258	Куперштейн Леонід	173
Гончар Лариса	208	Куцман Владислав	212
Горбань Гліб	14	Кушнір Андрій	142
Горностаљ Олександр	100	Ліщук Олександр	7
Горобець Юрій	75	Ломаченко Ігор	139
Гранік Михайло	202	Лосіцький Володимир	271
Гришин Дмитро	124	Лукічов Віталій	173

Лученко Микола	145	Сергеев Станіслав	130
Майданюк Володимир	7	Сергієнко Сергій	162
Мамедов Октай	96	Сілагін Олексій	145, 184, 188, 190, 206, 223, 226
Маначинський Олексій	61	Соколюк Олександра	266
Маркіна Ірина	198	Сотнікова Альона	184
Марков Дмитро	226	Спрут Іван	124
Марченко Ігор	157	Станіславський Іван	133
Месюра Володимир	24, 26, 186, 202, 214, 218	Стеценко Володимир	247
Мехтиєв Хиджран	96	Стеценко Надія	247
Михайлюк Лілія	188	Столяревская Алла	106
Мунтян Ольга	28	Судачевски Виорика	83
Мунтяну Сильвія	83	Суприган Олена	10, 35, 198
Мусієнко Максим	93	Супрун Роман	61
Недоснований Олександр	136	Сухомлин Светлана	263
Несен Микола	162	Тасьмук Дмитро	24
Никуляк Артем	214	Татарчук Артем	173
Ніколайчук Максим	221	Титюк Валерій	162
Озеранський Володимир	221	Тихонова Олена	70
Оксьоненко Максим	120	Тіхонов Андрій	73
Охромій Галина	19, 284	Ткачук Галина	247
Очеретний Анатолій	10	Троцишин Іван	304
Павлович Роман	50	Тягній Маргарита	206
Паламарчук Євген	281	Удовенко Сергій	37
Папінов Володимир	250, 252	Федосенко Никита	254
Пасіхов Юрій	296	Фесенко Андрій	193
Педоренко Владислав	218	Філіпов Владислав	299
Переродов Артемій	12	Фісун Микола	287
Перов Владислав	90	Харчук Денис	10
Петришин Сергій	12, 64, 67	Ховпун Олексій	33
Петров Сергій	157	Цирульник Сергій	80
Пікуляк Микола	230	Чала Лариса	37
Пінчук Ольга	266	Чернобай Олексій	47
Поліщук Богдан	145	Чорний Олексій	162
Попова Інна	61	Шамутія Рамаз	109
Приймак Наталія	43, 45	Швед Алена	122
Приходнюк Віталій	256	Швед Альона	22
Путкарадзе Хатуна	268	Шевчук Катерина	87
Решетник Вікторія	64	Шевяков Алексей	263
Роптанов Володимир	80	Шемет Євген	40
Руднєв Андрій	19	Шенгелия София	196
Савчук Тамара	43, 45, 47, 53, 56, 59, 75, 299	Щербіна Євгеній	186
Самоил Іон	83	Ядуха Дарія	193
Северілов Віктор	142	Яковлев Сергій	127, 120, 130
Северілов Павел	124	Яремко Олег	181
Семеренко Василь	307	Ярова Анастасія	223
Семигіна Тетяна	232, 261	Яровий Андрій	30, 40, 61

ЗМІСТ

СЕКЦІЯ А – СЕКЦИЯ А – SECTION A ІНТЕЛЕКТУАЛЬНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ – ИНТЕЛЛЕКТУАЛЬНЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ – INTELLECTUAL INFORMATION TECHNOLOGIES

TECHNOLOGY OF AUTOMATION IN EDUCATION	2
<i>Stolyarevska Alla</i>	
ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ ВІЗУАЛЬНОГО МОДЕЛЮВАННЯ ТА ОБРОБКИ ТЕРНАРНИХ ГЕШТАЛЬТ-РАНЖУВАНЬ	4
<i>Колодний Володимир, Кудрявцев Дмитро</i>	
ПІДВИЩЕННЯ ШВИДКОСТІ ФРАКТАЛЬНОГО МЕТОДУ УЩІЛЬНЕННЯ ЗОБРАЖЕНЬ ЗА РАХУНОК АПРОКСИМАЦІЇ	7
<i>Майданюк Володимир, Ліщук Олександр</i>	
ВИКОРИСТАННЯ ГЕНЕТИЧНИХ АЛГОРИТМІВ ДЛЯ КОРЕГУВАННЯ ВАГ НЕЙРОННИХ МЕРЕЖ	10
<i>Суприган Олена, Ваховська Любов, Очеретний Анатолій, Крутенко Ігор, Харчук Денис</i>	
АНАЛІЗ МЕТОДІВ ПЕРЕТВОРЕННЯ СЛОВА В ВЕКТОР ФІКСОВАНОЇ ДОВЖИНИ ДЛЯ ЗАДАЧІ КЛАСИФІКАЦІЇ ТЕКСТІВ	12
<i>Петришин Сергій, Переродов Артемій</i>	
ПЕРСПЕКТИВИ СТВОРЕННЯ ОБ'ЄКТНОЇ БАЗИ ДАНИХ ЗАСОБАМИ ОБОЛОНКИ КОМАНДНОГО РЯДКА WINDOWS POWERSHELL	14
<i>Горбань Гліб</i>	
ІННОВАЦІЙНІ ПІДХОДИ ФІЗИЧНОГО ВИХОВАННЯ СТУДЕНТІВ СПЕЦІАЛЬНИХ МЕДИЧНИХ ГРУП У ВИЩИХ НАВЧАЛЬНИХ ЗАКЛАДАХ	17
<i>Аніскевич Світлана</i>	
ІННОВАЦІЙНІ ПІДХОДИ ДО ВИКОНАННЯ НАЦІОНАЛЬНОЇ ПРОГРАМИ “ФІЗИЧНА АКТИВНІСТЬ, ЗДОРОВИЙ СПОСІБ ЖИТТЯ - ЗДОРОВ'Я НАЦІЇ”	19
<i>Охромій Галина, Аніскевич Світлана, Руднєв Андрій</i>	
СИСТЕМА ЕФЕКТИВНОГО РОЗПОДІЛУ КОШТІВ НА ОСНОВІ НЕЧІТКОЇ ЛОГІКИ ТА SMART-КОНТРАКТІВ	22
<i>Давиденко Євген, Швед Альона</i>	
ОПТИМІЗАЦІЯ МІСЬКОГО ТРАФІКУ ЗА ДОПОМОГОЮ ГЕНЕТИЧНОГО АЛГОРИТМУ	24
<i>Тасьмук Дмитро, Месюра Володимир</i>	
ГІБРИДНИЙ МОДУЛЬ ПЛАНУВАННЯ ШЛЯХУ МОБІЛЬНОГО РОБОТА У ДИНАМІЧНОМУ СЕРЕДОВИЩІ	26
<i>Корчиста Ольга, Месюра Володимир</i>	
ІНТЕЛЕКТУАЛЬНИЙ АНАЛІЗ МЕДИЧНИХ ДАНИХ	28
<i>Мунтян Ольга</i>	
ЗАСТОСУВАННЯ ГЛИБОКОЇ РЕКУРЕНТНОЇ НЕЙРОННОЇ МЕРЕЖІ ІЗ ВИКОРИСТАННЯМ АЛГОРИТМУ LSTM У СИСТЕМАХ ІНТЕЛЕКТУАЛЬНОЇ ВЗАЄМОДІЇ	30
<i>Яровий Андрій, Кудрявцев Дмитро, Кулик Олександр</i>	
БЛОКЧЕЙН У ПРАВІ	33
<i>Ховпун Олексій</i>	
АНАЛІЗ МОЖЛИВОСТЕЙ ВИКОРИСТАННЯ ГЕНЕТИЧНИХ АЛГОРИТМІВ В ЕЛЕМЕНТАХ НЕЙРОННОЇ МЕРЕЖІ	35
<i>Суприган Олена, Ваховська Любов</i>	
ІНФОРМАЦІЙНА СИСТЕМА ПОШУКУ ЗОБРАЖЕНЬ В ЕЛЕКТРОННИХ ТЕКСТАХ З ВИКОРИСТАННЯМ ГІБРИДНОГО ПІДХОДУ	37
<i>Удовенко Сергій, Чала Лариса</i>	

ПРОГРАМНІ СЕРЕДОВИЩА ДЛЯ ВИКОНАННЯ КВАНТОВИХ ОБЧИСЛЕНЬ	40
<i>Шебет Євген, Яровий Андрій</i>	
ІНФОРМАЦІЙНА МОДЕЛЬ ПРОЦЕСУ ПОШУКУ І ВИКОРИСТАННЯ АСОЦІАТИВНИХ ПРАВИЛ ПРИ РОЗРОБЦІ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ	43
<i>Савчук Тамара, Приймак Наталія</i>	
ОБГРУНТУВАННЯ ВИБОРУ МЕТОДУ ГЕНЕРАЦІЇ ЧАСТИХ ПРЕДМЕТНИХ НАБОРІВ ДЛЯ ПОШУКУ АСОЦІАТИВНИХ ПРАВИЛ ПРИ РОЗРОБЦІ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ	45
<i>Савчук Тамара, Приймак Наталія</i>	
УДОСКОНАЛЕННЯ АЛГОРИТМУ Z-БУФЕРИЗАЦІЇ	47
<i>Савчук Тамара, Чернобай Олексій</i>	
КОЛОРИЗАЦІЯ ЧОРНО-БІЛОГО ЗОБРАЖЕННЯ З ВИКОРИСТАННЯМ ЗГОРТКОВОЇ НЕЙРОННОЇ МЕРЕЖІ	50
<i>Павлович Роман, Арсенюк Ігор</i>	
АНАЛІЗ ПІДХОДІВ ДО ВИРІШЕННЯ ПРОБЛЕМ ВІДОБРАЖЕННЯ ОБ'ЄКТНО-ОРІЄНТОВАНОЇ МОДЕЛІ В РЕЛЯЦІЙНУ СТРУКТУРУ	53
<i>Савчук Тамара, Давидов Сергій</i>	
ПІДХІД ДО АНАЛІЗУ МАРКЕТИНГОВОЇ ДІЯЛЬНОСТІ В АГРОПРОМИСЛОВОМУ КОМПЛЕКСІ	56
<i>Савчук Тамара, Верховсь Дмитро</i>	
ІНТЕЛЕКТУАЛЬНИЙ МОДУЛЬ МОНІТОРИНГУ ВИКОНАННЯ ЗАВДАНЬ	59
<i>Савчук Тамара, Кміть Владислав</i>	
ВЕБ-ОРІЄНТОВАНА ПРОГРАМНА ПЛАТФОРМА ДЛЯ СТВОРЕННЯ ЕКСПЕРТНИХ СИСТЕМ «GIMET»	61
<i>Яровий Андрій, Маначинський Олексій, Супрун Роман, Попова Інна</i>	
ДОСЛІДЖЕННЯ ТА ПОРІВНЯЛЬНИЙ АНАЛІЗ АЛГОРИТМІВ ЗНАХОДЖЕННЯ ОПТИМАЛЬНОГО ШЛЯХУ	64
<i>Петришин Сергій, Решетник Вікторія</i>	
ОЦІНКА ОСНОВНИХ МЕТОДІВ ІНТЕЛЕКТУАЛЬНОГО АНАЛІЗУ ДАНИХ ДЛЯ ЗАДАЧІ ПІДБОРУ ПОКУПОК	67
<i>Петришин Сергій, Замковий Олександр</i>	

СЕКЦІЯ В – СЕКЦИЯ В – SECTION В **КОМП'ЮТЕРНІ МЕРЕЖЕВІ ТЕХНОЛОГІЇ - КОМПЬЮТЕРНЫЕ СЕТЕВЫЕ ТЕХНОЛОГИИ - COMPUTER NETWORK TECHNOLOGIES**

ОПТИМІЗАЦІЯ ПОТОКІВ У БАГАТОПОЛЮСНІЙ МЕРЕЖІ	70
<i>Тихонова Олена</i>	
АНАЛІЗ МЕТОДІВ ЗАХИСТУ ПЕРЕДАВАНОЇ ІНФОРМАЦІЇ В КАНАЛІ ЗВ'ЯЗКУ	73
<i>Кільдишев Віталій, Тіхонов Андрій</i>	
АРХІТЕКТУРА ВЕБ-СЕРВЕРА З БАГАТОПРОЦЕСОВИМ АСИМЕТРИЧНИМ КЕРУВАННЯМ ПОДІЯМИ	75
<i>Савчук Тамара, Горобець Юрій</i>	

СЕКЦІЯ С – СЕКЦИЯ С – SECTION С **КОМП'ЮТЕРНА ІНЖЕНЕРІЯ – КОМПЬЮТЕРНАЯ ИНЖЕНЕРИЯ – COMPUTER ENGINEERING**

ЯК ДОЛУЧИТИСЬ ДО INTERNET OF THINGS	80
<i>Цирульник Сергій, Роптанов Володимир</i>	
ПРИМЕР ПАРАЛЛЕЛЬНОГО УПРАВЛЕНИЯ В ЗАДАЧЕ КОЛЛЕКТИВНОГО ВЗАИМОДЕЙСТВИЯ ГРУППЫ РОБОТОВ	83
<i>Абабий Виктор, Судачевски Виорика, Мунтяну Сильвия, Абабий Константин, Самоил Ион</i>	

МЕТОД ВДОСКОНАЛЕННЯ ОДНОШЛЯХОВИХ ПРОТОКОЛІВ ДИНАМІЧНОЇ МАРШРУТИЗАЦІЇ	87
<i>Шевчук Катерина, Захарченко Сергій</i>	
ОСОБЛИВОСТІ ПОБУДОВИ БЛОКІВ ДЕКОДУВАННЯ ДЛЯ TRC-ДЕКОДЕРУ	90
<i>Крайник Ярослав, Перов Владислав</i>	
НАКОПИЧУВАЧІ ЕНЕРГІЇ ВІБРАЦІЇ ІОТ-ПРИСТРОЇВ НА ОСНОВІ КОНСОЛЬНИХ П'ЄЗОЕЛЕМЕНТІВ	93
<i>Мусієнко Максим, Корецька Олександра</i>	

СЕКЦІЯ D – СЕКЦИЯ D – SECTION D

МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ – МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ – MATHEMATICAL MODELING

О ПАРАМЕТРИЗАЦИИ ИНТЕРПРЕТАЦИЙ МНОГООБРАЗИЙ	96
<i>Мамедов Октай, Мехтиев Хиджран</i>	
МУРАШИНИЙ АЛГОРИТМ КЛАСТЕРИЗАЦІЇ	100
<i>Горносталь Олександр, Дорогий Ярослав</i>	
STUDY OF COEFFICIENTS OF RHEUMATOID ARTHRITIS MODEL	103
<i>Odisharia, Kakhaber</i>	
ПРИМЕНЕНИЕ ПАКЕТА GEOGEBRA ПРИ ПОСТРОЕНИИ ТРАЕКТОРИЙ МЕЖПЛАНЕТНЫХ ПОЛЕТОВ КОСМИЧЕСКИХ АППАРАТОВ	106
<i>Кузнецов Юрий, Столяревская Алла</i>	
РАЗРАБОТКА МАТЕМАТИЧЕСКОЙ МОДЕЛИ МНОГОКАНАЛЬНОЙ СИСТЕМЫ МАССОВОГО ОБСЛУЖИВАНИЯ СО МНОГИМИ СОСТОЯНИЯМИ ФУНКЦИОНИРОВАНИЯ	109
<i>Рамаз Шамугия</i>	
MATHEMATICAL AND COMPUTER MODELING OF POLITICAL ELECTIONS	113
<i>Temur Chilachava, Leila Sulava</i>	
TENSOR MODELING OF A QUANTUM SYSTEM	117
<i>Tikhonov Victor</i>	
РОЗПІЗНАВАННЯ ПРИХОВАНИХ MISTY-ПОДІБНИХ ПЕРЕТВОРЕНЬ	120
<i>Оксьоненко Максим, Яковлев Сергій</i>	
ОЦЕНКА ЭКСПЛУАТАЦИОННОГО СОСТОЯНИЯ ОБЪЕКТОВ ВОЕННО-ГРАЖДАНСКОГО НАЗНАЧЕНИЯ В УСЛОВИЯХ НЕОПРЕДЕЛЕННОСТИ	122
<i>Швед Алена, Давыденко Евгений</i>	
УЗАГАЛЬНЕНА МОДЕЛЬ ОПТИМАЛЬНОГО РОЗВИТКУ ЕКОЛОГІЗОВАНИХ ВИРОБНИЦТВ	124
<i>Боровська Таїса, Гришин Дмитро, Северілов Павел, Спрут Иван</i>	
АТАКА ЗБОЇВ НА ARX-КРИПТОСИСТЕМУ NIGHT ТА ЇЇ ЕФЕКТИВНІСТЬ	127
<i>Блинов Сергій, Яковлев Сергій</i>	
СТІЙКІСТЬ ШИФРУ AES ДО ДИФЕРЕНЦІАЛЬНОГО КРИПТОАНАЛІЗУ ВІДНОСНО АЛЬТЕРНАТИВНИХ АЛГЕБРАЇЧНИХ ОПЕРАЦІЙ	130
<i>Сергеев Станіслав, Яковлев Сергій</i>	
МЕТОДИ УПРАВЛІННЯ ПІДПРИЄМСТВОМ НА БАЗІ ІМІТАЦІЙНИХ МОДЕЛЕЙ КЛАСУ «ОДИН НА ФОНІ ВСІХ»	133
<i>Боровська Таїса, Волошин Костянтин, Станіславський Иван, Вернигора Інна</i>	
УЗАГАЛЬНЕНІ МОДЕЛІ ОПТИМАЛЬНОГО УПРАВЛІННЯ СИСТЕМАМИ МАСОВОГО ОБСЛУГОВУВАННЯ	136
<i>Боровська Таїса, Колесник Ірина, Закордонець Аліна, Недоснований Олександр</i>	
ЗАСТОСУВАННЯ БІКЛІК-АНАЛІЗУ ДО ШИФРУ КАЛИНА ТА ЙОГО МОДИФІКАЦІЙ	139
<i>Ломаченко Ігор</i>	
РОЗРОБКА ОПТИМАЛЬНОЇ СИСТЕМИ МАСОВОГО ОБСЛУГОВУВАННЯ З ІДЕНТИФІКАТОРОМ СТАНУ ТА ЗОВНІШНЬОГО ОТОЧЕННЯ	142
<i>Боровська Таїса, Кольцов Владислав, Кушнір Андрій, Северілов Віктор</i>	

НАВЧАЛЬНИЙ ДОДАТОК ДЛЯ ДОСЛІДЖЕННЯ ГОРБКОВОГО АЛГОРИТМУ	145
<i>Сілагін Олексій, Лученко Микола, Поліщук Богдан</i>	
THE MATHEMATICS OF HARMONY. FROM EUCLID TO CONTEMPORARY MATHEMATICS, COMPUTER SCIENCE AND MODERN MATHEMATICAL EDUCATION	147
<i>Alexey Stakhov</i>	

СЕКЦИЯ Е – СЕКЦИЯ Е – SECTION E
КОМП'ЮТЕРНІ ТЕХНОЛОГІЇ ТА ІНТЕРНЕТ В ІНФОРМАЦІЙНОМУ
СУСПІЛЬСТВІ – КОМПЬЮТЕРНЫЕ СЕТЕВЫЕ ТЕХНОЛОГИИ И ИНТЕРНЕТ В
ИНФОРМАЦИОННОМ ОБЩЕСТВЕ – COMPUTER TECHNOLOGIES AND THE
INTERNET IN INFORMATIONAL SOCIETY

ДОСЛІДЖЕННЯ МАШИННОГО ПЕРЕКЛАДУ ЗА ДОПОМОГОЮ ПРОГРАМИ PRAGMA	152
<i>Котик Ольга, Кунанець Наталія</i>	
О НЕКОТОРЫХ АЛГОРИТМАХ РАЗМЫТИЯ ИЗОБРАЖЕНИЙ И СРАВНИТЕЛЬНЫЙ АНАЛИЗ ИХ ПРОГРАММНЫХ РЕАЛИЗАЦИЙ	155
<i>Бенидзе Нана, Габисония Инга</i>	
РОЗРОБКА ІНФОРМАЦІЙНОЇ СИСТЕМИ КОНТРОЛЮ ОБІГУ МЕДИЧНИХ ПРЕПАРАТІВ НА БАЗІ ТЕХНОЛОГІЇ БЛОКЧЕЙН	157
<i>Марченко Ігор, Петров Сергій</i>	
APPROACH TO ARCHITECTURE DESIGN OF THE CONTENT READABILITY DETERMINATION SYSTEM	160
<i>Vasyuk Taras</i>	
КОМП'ЮТЕРИЗОВАНА СИСТЕМА КОНТРОЛЮ ЗНАНЬ ЧЕРЕЗ МЕРЕЖУ INTERNET	162
<i>Чорний Олексій, Сергієнко Сергій, Несен Микола, Кабаченко Ірина, Титюк Валерій</i>	
АНАЛІЗ ЯКОСТІ ПРОГНОЗУ ПОГОДИ ПОПУЛЯРНИХ УКРАЇНСЬКИХ САЙТІВ	165
<i>Козачук Андрій</i>	
УЯЗВИМОСТЬ NOSQL НА ПРИМЕРЕ MONGODB	167
<i>Абрамова Ірина, Афанасьєва Ірина</i>	
THE CLOSURE OF TABLE ALGEBRA OF INFINITE TABLES WITH RESPECT TO OPERATIONS OF MULTISSET TABLE ALGEBRA	169
<i>Glushko, Iryna</i>	
К ВОПРОСУ О ВОСПРИЯТИИ ИНФОРМАЦИИ В ИНТЕРНЕТ-ПРОСТРАНСТВЕ	171
<i>Архипова Евгения</i>	
КЛАСИФІКАЦІЯ ЗАГРОЗ ДЛЯ WI-FI МЕРЕЖ	173
<i>Татарчук Артем, Куперштейн Леонід, Лукічов Віталій</i>	
NEW ASYMMETRIC ALGORITHM FOR FAST MESSAGE TRANSMISSION AND TROPICAL CRYPTOGRAPHY	175
<i>Richard P. Megrelishvili</i>	
NEW BLOCK ENCRYPTION ALGORITHM	179
<i>Kochladze Zurab, Beselia Lali</i>	
РОЗРОБЛЕННЯ ІННОВАЦІЙНОГО ІТ-СТАРТАПУ ПРОГРАМНОГО ПРОДУКТУ «ПОМІЧНИК СІМЕЙНОГО БЮДЖЕТУ» (“FAMILY BUDGET HELPER”)	181
<i>Яремко Олег, Кунанець Наталія</i>	
ВИКОРИСТАННЯ QR-КОДІВ В ПЛАТІЖНИХ СИСТЕМАХ	184
<i>Сотнікова Альона, Сілагін Олексій</i>	

АНАЛІЗ МОВ НАПИСАННЯ СМАРТ КОНТРАКТІВ ІСНУЮЧИХ КРИПТОВАЛЮТ	186
<i>Щербіна Євгеній, Месюра Володимир</i>	
ІНТЕЛЕКТУАЛЬНИЙ МОДУЛЬ СИНХРОНІЗАЦІЇ ДАНИХ В РЕЖИМІ РЕАЛЬНОГО ЧАСУ	188
<i>Михайлюк Лілія, Сілагін Олексій</i>	
ПЕРСПЕКТИВИ ВИКОРИСТАННЯ ТЕХНОЛОГІЇ БЛОКЧЕЙН	190
<i>Білик Руслан, Сілагін Олексій</i>	
ПОБУДОВА АТАК НА КРИПТОСИСТЕМУ AJPS З ВИКОРИСТАННЯМ МОДЕЛІ АКТИВНОГО ЗЛОВМИСНИКА	193
<i>Ядуха Дарія, Фесенко Андрій</i>	
МОЩНЫЕ ФРАКТАЛЬНЫЕ МАТРИЧНЫЕ МНОЖЕСТВА ДЛЯ РЕАЛИЗАЦИИ И СТОЙКОСТИ АЛГОРИТМА	196
<i>Шенгелия София</i>	
ПРИНЦИП ВИБОРУ ОКУЛЯРІВ ВІРТУАЛЬНОЇ РЕАЛЬНОСТІ ПРИ РОЗРОБЦІ ПРОГРАМНИХ ЗАСОБІВ	198
<i>Суприган Олена, Маркіна Ірина</i>	
ВПЛИВ КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ НА ТЕОРІЮ І ПРАКТИКУ МАРКЕТИНГУ В ІНФОРМАЦІЙНОМУ СУСПІЛЬСТВІ	200
<i>Корчинська Олена</i>	
ОБГРУНТУВАННЯ ДОЦІЛЬНОСТІ ВИКОРИСТАННЯ ГЛИБИННОГО НАВЧАННЯ ДЛЯ РОЗВ'ЯЗАННЯ ЗАДАЧІ РОЗПІЗНАВАННЯ НЕПРАВДИВИХ НОВИН	202
<i>Гранік Михайло, Месюра Володимир</i>	
DEVELOPING SPEAKING SKILLS USING THE INTERNET RESOURCES (ON THE EXAMPLE OF TED)	204
<i>Teteruk Svitlana</i>	
ІНТЕЛЕКТУАЛЬНІ ТЕХНОЛОГІЇ ІДЕНТИФІКАЦІЇ В МЕДИЦИНІ	206
<i>Сілагін Олексій, Тягній Маргарита</i>	
ІНКЛЮЗИВНА ОСВІТА В ІНФОРМАЦІЙНОМУ ПРОСТОРІ	208
<i>Гончар Лариса</i>	
МЕРЕЖЕВИЙ ІНДИВІДУАЛІЗМ В СИСТЕМІ КОМУНІКАЦІЙ	210
<i>Бондар Світлана</i>	
РОЗПІЗНАВАННЯ БАГАТОКАНАЛЬНИХ СИГНАЛІВ ЗА ДОПОМОГОЮ СПАЙКІНГОВИХ НЕЙРОННИХ МЕРЕЖ	212
<i>Колесницький Олег, Куцман Владислав</i>	
ВЕБ-ДОДАТОК УПРАВЛІННЯ ТОВАРНИМИ ЗАПАСАМИ НА ОСНОВІ ТРИРІВНЕВОЇ АРХІТЕКТУРИ	214
<i>Никуляк Артем, Месюра Володимир</i>	
К РАЗРАБОТКЕ СИСТЕМ АВТОМАТИЗАЦИИ ПРОИЗВОДСТВА ДЛЯ ПРЕДПРИЯТИЙ ГИДРОПОНИКИ	216
<i>Кокая Гига</i>	
ВИКОРИСТАННЯ RESTFUL API ПРИ РОЗРОБЦІ МОДУЛЯ КЕРУВАННЯ ТОВАРНИМИ ЗАПАСАМИ.	218
<i>Педоренко Владислав, Месюра Володимир</i>	
ВИКОРИСТАННЯ ГЕОЛОКАЦІЇ В СОЦІАЛЬНИХ МЕРЕЖАХ	221
<i>Ніколайчук Максим, Озеранський Володимир</i>	
РОЗРОБКА САЙТУ ПСИХОЛОГІЧНОГО ТЕСТУВАННЯ «ВІКНО ДЖОХАРІ»	223
<i>Ярова Анастасія, Сілагін Олексій</i>	
ОСОБЛИВОСТІ РЕАЛІЗАЦІЇ ПРОГРАМНИХ ПРОДУКТІВ (ДОДАТКІВ) НА БАЗІ БЛОКЧЕЙН ТЕХНОЛОГІЇ	226
<i>Марков Дмитро, Сілагін Олексій</i>	

СЕКЦІЯ F – СЕКЦИЯ F – SECTION F
ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА ІНТЕРНЕТ У НАВЧАЛЬНОМУ ПРОЦЕСІ ТА
НАУКОВИХ ДОСЛІДЖЕННЯХ – ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И
ИНТЕРНЕТ В ОБРАЗОВАТЕЛЬНОМ ПРОЦЕССЕ И НАУЧНЫХ ИССЛЕДОВАНИЯХ
– INFORMATIONAL TECHNOLOGIES AND INTERNET IN EDUCATION PROCESS
AND SCIENTIFIC RESEARCH ACTIVITIES

ЗАСТОСУВАННЯ МЕТОДУ ДИХОТОМІЇ ДЛЯ ПОБУДОВИ МАТЕМАТИЧНОЇ МОДЕЛІ АДАПТИВНОГО ТЕСТУВАННЯ	230
<i>Пікуляк Микола</i>	
НАУКА В ІНФОРМАЦІЙНОМУ СУСПІЛЬСТВІ: ПРОФІЛІ НАУКОВЦІВ ТА АКАДЕМІЧНІ МЕРЕЖІ	232
<i>Семигіна Тетяна</i>	
АНАЛІЗ ВІТЧИЗНЯНОГО ДОСВІДУ ВИКОРИСТАННЯ ХМАРО ОРІЄНТОВАНИХ ТЕХНОЛОГІЙ У НАВЧАЛЬНОМУ СЕРЕДОВИЩІ ВИЩИХ НАВЧАЛЬНИХ ЗАКЛАДІВ	235
<i>Гайдаш Богдан</i>	
СПОСОБИ ВІДБОРУ ДАНИХ ДО JAVASCRIPT СЦЕНАРІЮ ПОБУДОВИ ДІАГРАМИ	238
<i>Качурівська Ганна, Качурівський Володимир</i>	
OPEN SOURCE SOFTWARE TO SUPPORT THE EDUCATION PROCESSES IN SOFTWARE DEVELOPMENT IN POST-SOVIET COUNTRIES	241
<i>Gakh Dmitri</i>	
METHODOLOGICAL APPROACH TO THE CONSTRUCTION OF CULTURAL HERITAGE ONTOLOGY	244
<i>Baeva Desislava, Rashkova Victoria, Ivanov Ivan</i>	
ОСОБЛИВОСТІ ПРОЕКТУВАННЯ ПЕРСОНАЛЬНОГО ОСВІТНЬОГО СЕРЕДОВИЩА В УМОВАХ КОННЕКТИВІСЬКОГО ПІДХОДУ	247
<i>Ткачук Галина, Стеценко Надія, Стеценко Володимир</i>	
ВІДТВОРЕННЯ ПРОМИСЛОВОЇ ЕАМ-СИСТЕМИ У НАВЧАЛЬНІЙ КОМП'ЮТЕРИЗОВАНІЙ ЛАБОРАТОРІЇ	250
<i>Папінов Володимир</i>	
ВІДТВОРЕННЯ ПРОМИСЛОВОЇ ММ-СИСТЕМИ У НАВЧАЛЬНІЙ КОМП'ЮТЕРИЗОВАНІЙ ЛАБОРАТОРІЇ	252
<i>Папінов Володимир</i>	
PREREQUISITES FOR CREATION AND MAIN IDEAS OF THE SEMANTIC WEB	254
<i>Федосенко Никита, Груздо Ирина</i>	
ОНТОЛОГІЧНА СИСТЕМА КЕРУВАННЯ ОСОБИСТИМИ КАБІНЕТАМИ КОРИСТУВАЧІВ ОСВІТНЬОГО ПОРТАЛУ	256
<i>Приходнюк Віталій</i>	
ОСОБЕННОСТИ РАБОТЫ В ЯЗЫКАХ C# / C++ С УКАЗАТЕЛЯМИ И ССЫЛКАМИ В ОБЪЕКТНО-ОРИЕНТИРОВАННОМ ПРОГРАММИРОВАНИИ	258
<i>Голубь Надежда</i>	
УНІВЕРСИТЕТИ У ЦИФРОВУ ЕПОХУ	261
<i>Буященко Вікторія, Семигіна Тетяна</i>	
ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ОБРАЗОВАТЕЛЬНОМ ПРОЦЕССЕ ФОРМИРОВАНИЯ САМОСОЗНАНИЯ ГИПЕРАКТИВНЫХ ДЕТЕЙ	263
<i>Сухомлин Светлана, Шевяков Алексей</i>	
НАВЧАЛЬНО-ПІЗНАВАЛЬНА ДІЯЛЬНІСТЬ УЧНІВ В УМОВАХ ВИКОРИСТАННЯ ІНТЕРНЕТ ОРІЄНТОВАНИХ ОСВІТНІХ ТЕХНОЛОГІЙ	266
<i>Пінчук Ольга, Соколюк Олександра</i>	
РЕАГИРОВАНИЕ СИСТЕМЫ ОБРАЗОВАНИЯ НА ПОТРЕБНОСТИ РЫНКА ТРУДА (РЕАЛЬНОСТЬ И ПЕРСПЕКТИВЫ)	268
<i>Хатуна Путкарадзе</i>	

ІННОВАЦІЙНА МОДЕЛЬ «ШКОЛА НОВІТНІХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ»	271
<i>Лосіцький Володимир</i>	
ОСОБЛИВОСТІ ВІРТУАЛЬНОГО НАВЧАЛЬНОГО СЕРЕДОВИЩА НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ “ЛЬВІВСЬКА ПОЛІТЕХНІКА”	273
<i>Думанський Нестор</i>	
ПІДВИЩЕННЯ РЕЙТИНГУ ВИЩОГО НАВЧАЛЬНОГО ЗАКЛАДУ У МІЖНАРОДНІЙ СИСТЕМІ ОЦІНКИ ДІЯЛЬНОСТІ УНІВЕРСИТЕТІВ WEBOMETRICS	275
<i>Карагодіна Марина, Головка Ярослав</i>	
CHALLENGES OF CRITICAL INFORMATION MANAGEMENT TECHNOLOGY	278
<i>Tinatin Mshvidobadze</i>	
КОНЦЕПЦІЯ СТВОРЕННЯ ЕЛЕКТРОННОГО УНІВЕРСИТЕТУ ДЛЯ ЗАКЛАДУ ВИЩОЇ ОСВІТИ	281
<i>Коваленко Олена, Паламарчук Євген</i>	
СУЧАСНІ СПОСОБИ ОЦІНКИ ПСИХОФІЗІОЛОГІЧНОЇ ЕФЕКТИВНОСТІ РЕАБІЛІТАЦІЇ ВЛАСТИВОСТЕЙ ЦЕНТРАЛЬНОЇ НЕРВОВОЇ СИСТЕМИ	284
<i>Охромій Галина</i>	
ВИКОРИСТАННЯ ПРОГРАМНОЇ СИСТЕМИ ANTLR ДЛЯ СТВОРЕННЯ МОВИ РЕЛЯЦІЙНОЇ АЛГЕБРИ	287
<i>Фісун Микола, Кандиба Ігор</i>	
ВИКОРИСТАННЯ ОНЛАЙН-КУРСІВ У НАВЧАННІ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ	289
<i>Дітковська Леся</i>	
К РАЗРАБОТКЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ АВТОМАТИЗАЦИИ ОБУЧЕНИЯ ДИФФЕРЕНЦИРОВАНИЮ ФУНКЦИЙ	291
<i>Заркуа Теодор</i>	
ЗАСТОСУВАННЯ СУЧАСНИХ ТЕХНОЛОГІЙ ТА ІННОВАЦІЙНИХ МЕТОДІВ НАВЧАННЯ У ВИЩИХ НАВЧАЛЬНИХ ЗАКЛАДАХ	293
<i>Іванова Світлана</i>	
ЄДИНЕ МЕРЕЖЕЦЕНТРИЧНЕ ІНФОРМАЦІЙНО-ОСВІТНЄ СЕРЕДОВИЩЕ ЗАГАЛЬНООСВІТНІХ НАВЧАЛЬНИХ ЗАКЛАДІВ	296
<i>Пасіхов Юрій</i>	
ТЕХНОЛОГІЯ ТЕСТУВАННЯ ЗНАНЬ	299
<i>Савчук Тамара, Філіпов Владислав, Іванова Світлана</i>	

СЕКЦІЯ G – СЕКЦИЯ G – SECTION G ГЕОІНФОРМАЦІЙНІ СИСТЕМИ – ГЕОИНФОРМАЦИОННЫЕ СИСТЕМЫ – GEOINFORMATION SYSTEMS

ПРИНЦИПИ ТА МЕТОДОЛОГІЯ АКТИВНОЇ ПРОТИДІЇ БПЛА ЗА АЛГОРИТМОМ АКАД	304
<i>Троцишин Іван</i>	
ЗАХИСТ ДАНИХ В ЗАДАЧАХ НАВІГАЦІЇ В PHYSICAL WEB	307
<i>Семеренко Василь, Кошолан Микола</i>	
ONTOLOGY-BASED SOFTWARE SYSTEM ABOUT THE SYMBOLIC IN NATIONAL REASONS IN THE DIFFERENT GEOGRAPHICAL REGIONS OF EUROPE AND ASIA	310
<i>Baeva Desislava, Rashkova Victoria</i>	



ОДИНАДЦЯТА МІЖНАРОДНА КОНФЕРЕНЦІЯ
ІОН - 2018
ІНТЕРНЕТ-ОСВІТА-НАУКА-2018



**СЕКЦІЯ А. ІНТЕЛЕКТУАЛЬНІ ІНФОРМАЦІЙНІ
ТЕХНОЛОГІЇ**



THE ELEVENTH INTERNATIONAL
CONFERENCE
IES-2018
INTERNET-EDUCATION-SCIENCE - 2018



**SECTION A. INTELLECTUAL INFORMATION
TECHNOLOGIES**



ОДИННАДЦАТАЯ МЕЖДУНАРОДНАЯ
КОНФЕРЕНЦИЯ
ИОН-2018
ИНТЕРНЕТ– ОБРАЗОВАНИЕ – НАУКА 2018



**СЕКЦІЯ А. ІНТЕЛЛЕКТУАЛЬНІЕ
ІНФОРМАЦІОННІЕ ТЕХНОЛОГІИ**



TECHNOLOGY OF AUTOMATION IN EDUCATION

Stolyarevska Alla

Kharkiv, Ukraine

Abstract

The paper considers the trends in education, which can be traced upon publications of researchers during the last year. The main focus is on the trend of automation in education, the success of which depends in a large extent on the answer to the question: can robots replace teachers in solving the tasks that are easy to perform but hard to describe formally.

Аннотация

В статье рассматриваются тенденции в образовании, которые прослеживаются по публикациям исследователей за последний год. Основное внимание уделяется тенденции автоматизации в образовании, успех которой во многом зависит от ответа на вопрос: могут ли роботы заменить учителей в решении задач, которые легко выполнять, но трудно описать формально.

New race between education and technology

Technology is an ever-changing category. In accordance with the conclusions of the Forbes Technology Council [1], three technologies - automation, cloud computing/cybersecurity and social networks - will be important in the long term. These categories are already experiencing the changes that determine how we build products, protect our intellectual capital and communicate with one another. At once, automation announces a new race between education and technology [2]. However, the ability of citizens to compete with automation is hampered by the poor performance of education systems in most developing countries. Countries continue to give their students basic cognitive skills - the basic skills that the brain uses to think, read, learn, remember and reason. This does not allow many citizens to benefit from a high return on their studies. Education can help, but countries will probably need a lot more of it, and it will need to be of higher quality, and facilitate access to new skills. Economists studying the effects of automation emphasize the importance of "higher-order mental abilities", such as creativity and interpersonal skills.

Education in the era of the fourth industrial revolution

Today is the time of the fourth industrial revolution (Industry 4.0) [3]. The revolution is possible due to development in artificial intelligence (AI), big data, virtual reality, and robotics. They effect on our daily lives, including the way we learn. The aim of Industry 4.0 – to create so-called smart factories in which cyber-systems combined with the internet, cloud computing and machine learning algorithms make decentralized decisions with minimal human input. But the impact and acceleration of Industry 4.0 in education is not as clear as in other industries [4]. AI in education has progressed slowly. The slow pace can perhaps be attributed to a lack of funds available to educational institutions for adopting advanced technologies. There's also some resistance from teachers, that is conditioned by the idea of robots as training machines.

However, AI and robotic process automation (RPA) can benefits to teachers, students, and academic administrators. Many of academic administrators' activities are heavily paper-based, repetitive, and time-consuming, making them an ideal fit for RPA. Automation delivers increased time-liberation and productivity to teachers and academic administrators. Teachers will be able to use automation, specifically RPA, to their benefit. Potential tasks for automation include ones that are burdensome for many teachers: scheduling, keeping track of attendance, and even assignment grading. While automating these tasks will shift the responsibilities of teachers in the long run, it will allow them to spend less time on routine tasks and more time

with their students, who can receive feedback more quickly. Automation allows for more direct and sustained contact between students and teachers. It will be much deeper learning.

AI contribution to education

The main thesis of AI: every aspect of learning or any other feature of intelligence can in principle be so precisely described that a machine can be made to simulate it. The solution is in gathering knowledge from experience. This approach avoids the need for human operators to formally specify all of the knowledge that the computer needs. The hierarchy of concepts allows the computer to learn complicated concepts by building them out of simpler ones. This approach is the basis of AI deep learning [5]. It helps to solve problems like recognizing spoken words or faces in images. In 2010 IBM built the cognitive computer called Watson. Actually, it is a DeepQA system capable of answering questions in a natural language.

In 2016, the first textbook on deep learning was published [6]. Deep learning is a form of machine learning that enables computers to learn from experience and understand the world in terms of a hierarchy of concepts. If we draw a graph showing how these concepts are built on top of each other, the graph is deep, with many layers.

Will educators be with robots?

Automation, AI, and robotics are positioned to make an even bigger splash in education in the future. Robots are now performing tasks that humans simply cannot. Robots take the form of AI software programs or humanoid machines. With change understandably comes anxiety. Could these AI-enhanced entities solve our most pervasive and systemic issues in education?

British education expert A. Seldon claims [7], that robots will replace teachers by 2027. Professor of Learner Centred Design at the London Knowledge Lab R. Luckin states that they (robots) won't be able to for at least the next decade: "I do not believe that any robot can fulfill the wide range of tasks that a human teacher completes on a daily basis, nor do I believe that any robot will develop the vast repertoire of skills and abilities that a human teacher possesses". R. Luckin suggests a compromise: AI and automated systems could have collaborative roles in the education system. "That would enable teachers and students to take advantage of the tech in ways that will benefit them both, and we wouldn't need to worry about lack of oversight for when our AI systems do encounter problems".

For this process to go well, it needs to be slow and iterative. It will likely take decades at best.

References:

1. Dinha F. Three Technology Shifts That Will Create New Economic Opportunities. Forbes Technology Councils. May 31, 2017. [Electronic resource] // The access mode: <https://www.forbes.com/sites/forbestechcouncil/2017/05/31/three-technology-shifts-that-will-create-new-economic-opportunities/#6847209c1702>
2. Patrinos H.A. The implications of automation for education. 11/09/2017. [Electronic resource] // The access mode: <http://blogs.worldbank.org/education/implications-automation-education>
3. Chao R.Jr. Educating for the fourth industrial revolution. University World News. 10 November 2017. Issue No:482 [Electronic resource] // The access mode: <http://www.universityworldnews.com/article.php?story=20171107123728676>
4. VMock Thinks. The Impact of AI, Automation and Machine Learning in Education. Industry Trends, Technology. November 21, 2017. [Electronic resource] // The access mode: <https://blog.vmock.com/impact-ai-automation-machine-learning-education/>
5. Peters M.A. Deep learning, education and the final stage of automation. 25 Jul 2017. [Electronic resource] // The access mode: <https://www.tandfonline.com/doi/full/10.1080/00131857.2017.1348928>
6. Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep learning. MIT Press. 800 pp.
7. Houser K. The Solution to Our Education Crisis Might be AI. December 11, 2017. [Electronic resource] // The access mode: <https://futurism.com/ai-teachers-education-crisis/>

ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ ВІЗУАЛЬНОГО МОДЕЛЮВАННЯ ТА ОБРОБКИ ТЕРНАРНИХ ГЕШТАЛЬТ-РАНЖУВАНЬ

Колодний Володимир, Кудрявцев Дмитро

Вінницький національний технічний університет

Анотація

Розроблено нову інформаційну технологію, засновану на візуалізації тернарних гештальт-ранжувань та їхній подальшій комп'ютерній обробці. Створено комп'ютерну програму, яку можна використовувати як ефективний інструмент для розв'язання багатьох практичних задач прийняття рішень з цільовою та критеріальною невизначеністю.

Abstract

The new information technology based on visualization of ternary gestalt-ranking and their next computer processing has been developed. Computer program was created, which can use as effective instrument for resolving a lot practical tasks of decision-making with target and criterial uncertain.

Теоретичне підґрунтя застосування тернарних трирівневих гештальт-ранжувань для виявлення переваг ОНР

Опишемо теоретичні основи розробленої інформаційної технології, що ґрунтуються на роботах [1-3].

Досить розповсюдженим є клас практичних задач прийняття рішень, що мають такі дві властивості:

- критерії для оцінювання та порівняння альтернатив частково або повністю невідомі (як самі критерії, так і їхні значення на певних шкалах);
- всі наявні альтернативи відомі і їхня загальна кількість є невеликою.

Такі задачі прийняття рішень будемо називати задачами для декількох альтернатив з критеріальною невизначеністю і в подальшому будемо розглядати саме цей клас задач, який, очевидно, є підкласом слабо структурованих задач прийняття рішень.

Інтуїтивно зрозуміло, що єдиним можливим способом структурувати множину альтернатив, тобто визначити переваги ОНР на цій множині, є пред'явлення ОНР для порівняння деяких з множини альтернатив. В найпростішому і тому найрозповсюдженішому випадку альтернативи пред'являються двійками і здійснюється попарне порівняння всіх альтернатив. Якщо ОНР фіксує лише факт переваги однієї альтернативи над іншою, достатньо двох рівнів порівняння.

Якщо ОНР може визначити не лише факт, але і ступінь переваги однієї альтернативи над іншою, застосовується більша кількість рівнів бінарних порівнянь. Наприклад, в шкалі Сааті попарні порівняння відбуваються на дев'яти рівнях [4].

Багаторічне практичне застосування цієї шкали продемонструвало, що 9 рівнів буває забагато для надійного оцінювання ступеня переваги альтернатив ОНР, що не є професійними системними аналітиками.

З іншого боку, досвідчені фахівці-професіонали, що мають розвинене числове мислення, іноді вважають, що 9 рівнів шкали недостатньо для адекватного вимірювання ступеня переваг. Саме тому постає задача «підлаштовування» під ОНР і надання їй можливості працювати з найбільш прийнятною кількістю рівнів порівнянь альтернатив в кожній конкретній ситуації прийняття рішень.

Практика показує, що в більшості випадків двох рівнів порівняння (відношень $>$ і $\sim$), виявляється явно замало. ОНР досить часто намагається не обмежуватися лише констатацією факту переваги однієї альтернативи над іншою, але й

спробувати хоч якось оцінити ступінь цієї переваги (причому, як правило, вербально, а не кількісно!).

Прикладами таких розповсюджених вербальних оцінок ОНР є такі словесні конструкції:

- (1) «альтернатива А значно переважає альтернативу В»;
- (2) «альтернатива В безумовно краща ніж А, але трохи гірша, ніж С»;
- (3) «альтернатива А набагато краща за В, але приблизно однакова за якістю з С».

В результаті проведених досліджень було зроблено висновок, що в більшості випадків ОНР можуть і бажають визначити ступінь переваги між альтернативами, але впевнено розрізняють лише два ступеня переваг: звичайну строгу перевагу $\succ$ та сильну (безумовну, беззаперечну) перевагу $\succ\succ$ [2, 3]. З урахуванням відношення еквівалентності ($\sim$) отримуємо три рівні порівняння для двох альтернатив.

Також виявилось, що ОНР досить часто розширюють контекст порівнянь, намагаючись додати до попарного порівняння третю альтернативу, як в словесних конструкціях (2), (3). Зрозуміло, що попарних порівнянь в таких випадках для адекватного відображення думки ОНР виявляється недостатньо.

З урахуванням введення символу сильної переваги можна досить легко та наочно записати в символічній формі словесні конструкції (1) – (3):

- $$\begin{aligned} (1) &\Leftrightarrow A \succ\succ B; \\ (2) &\Leftrightarrow C \succ B \succ A; \\ (3) &\Leftrightarrow A \sim C \succ\succ B. \end{aligned}$$

Подальше розширення контексту порівнянь ОНР, як правило, не відбувається, тому що згадування в одному реченні чотирьох і більшої кількості альтернатив з описом ступеня переваг між ними робить відповідну словесну конструкцію дуже громіздкою та мало зрозумілою. Тому було зроблено такий висновок: ОНР досить впевнено та надійно можуть одночасно оперувати трьома альтернативами і порівнювати їх на трьох рівнях, тобто здійснювати тернарні трирівневі гештальт-ранжування.

Поняття гештальт-ранжування введено в роботі [3] і означає одночасне пред'явлення ОНР декількох альтернатив для їхнього наочного порівняння з активізацією швидкої системи інтуїтивного мислення ОНР [5].

З усіх гештальт-ранжувань найбільш природними, надійними та ефективними є саме тернарні трирівневі гештальт-ранжування [3]. Кожне тернарне трирівневе гештальт-ранжування породжує трійку бінарних трирівневих ранжувань.

Очевидно, що тернарні трирівневі гештальт-ранжування, надають ОНР набагато більші можливості різноманітно, надійно та точно виразити свої переваги між різними альтернативами, ніж бінарні порівняння на двох та трьох рівнях. Зрозуміло, що роздільна здатність тернарних трирівневих ранжувань є набагато більшою.

Візуальна модель тернарних трирівневих ранжувань є досить наочною та зрозумілою для системного аналітика, але, на жаль, виявилася незручною для ОНР, які не є фахівцями в галузі теорії прийняття рішень. Тому було поставлено завдання створити нову зручну та інтуїтивно зрозумілу інформаційну технологію для візуалізації та подальшої комп'ютерної обробки інформації у вигляді тернарних гештальт-ранжувань.

Опис розробленої інформаційної технології

Розроблена інформаційна технологія візуального моделювання та обробки тернарних гештальт-ранжувань не передбачає ніяких запитань для ОНР і не потребує ніякої інформації від ОНР в числовій або вербальній формі. Потрібно лише перетягнути зображення трійки кружечків-альтернатив на круг переваг згідно з вподобаннями ОНР. Це збільшує ефективність використання швидкого інтуїтивного мислення [5] із залученням візуальної інформації та зорової пам'яті ОНР. Таким чином, під час проведення кожного тернарного гештальт-ранжування візуалізується трійка альтернатив,

які ОНР має розмістити на крузі переваг за принципом: чим вище для ОНР якість альтернативи, тим ближче до центру круга переваг потрібно її розташовувати.

Розроблена інформаційна технологія складається з таких етапів:

1. Введення бажаних для ОНР кількості і назв альтернатив та кількості градацій (рівнів) порівняння. Кількість градацій ОНР може змінювати за своїм бажанням.

2. Проведення тернарних гештальт-ранжувань з візуальним моделюванням на крузі переваг.

3. Числове вимірювання якості альтернатив з урахуванням їхнього розташування на крузі переваг та автоматична генерація (отримання) трійки бінарних трирівневих ранжувань, що відповідають поточному тернарному гештальт-ранжуванню.

4. Аналіз кожного отриманого поточного бінарного трирівневого ранжування на суперечливість з раніше отриманими бінарними трирівневими ранжуваннями.

5. Призупинення гештальт-ранжувань з можливістю пошуку та виправлення виявлених помилок ОНР.

6. Візуалізація всіх проведених тернарних гештальт-ранжувань, в які входить задана альтернатива.

7. Повернення до попередніх гештальт-ранжувань з метою виправлення виявлених помилок.

8. Обчислення результуючих нормованого та центрованого кардинальних ранжувань всієї множини альтернатив.

9. Візуалізація спектру переваг усіх альтернатив та обчислених результуючих ранжувань у вигляді кольорових діаграм.

Для більш зручного користування ОНР створена інтерактивна система підказок.

Розроблену інформаційну технологію було реалізовано у вигляді комп'ютерної програми «Інформаційна технологія візуального моделювання тернарних гештальт-ранжувань на крузі переваг (ТеГР)» у середовищі програмування Visual Studio 2015 на мові C# 6.0 із використанням технології WPF.

Висновки

Розроблена інформаційна технологія є зручною для ОНР, наочною, надійною та не складною у використанні. Представлення альтернатив і переваг між ними у вигляді простих візуальних образів потребує від ОНР значно менших когнітивних зусиль порівняно з традиційними методами, заснованими на отриманні значень числових або лінгвістичних змінних. Створену на основі цієї інформаційної технології комп'ютерну програму можна використовувати як ефективний інструмент для розв'язання рішень з цільовою та критеріальною невизначеністю.

Список використаних джерел:

1. Трирівневі ранжування та їх застосування для виявлення переважань / В. В. Колодний // Контроль і управління в складних системах. – Вінниця: «УНІВЕРСУМ-Вінниця», 2003. – с. 238.

2. Метод некритееріального структурування множини альтернатив за допомогою аналізу тернарних трирівневих ранжувань / В. В. Колодний, В. В. Зубко // «ІНТЕРНЕТ–ОСВІТА–НАУКА–2014»: Збірник праць конференції.– Вінниця: ВНТУ, 2014. – с. 13-14.

3. Застосування гештальт-ранжувань для виявлення переваг ОНР / В. В. Колодний, В. В. Зубко // «ІНТЕРНЕТ–ОСВІТА–НАУКА–2016»: Збірник праць конференції. – Вінниця : ВНТУ, 2016. – С. 43-44.

4. Саати Т. Л. Принятие решений. Метод анализа иерархий / Т. Л. Саати. – М.: Радио и связь, 1989. – 316 с.

5. Канеман Д. Думай медленно... решай быстро / Д. Канеман. – Москва: АСТ, 2014. – 653 с.

ПІДВИЩЕННЯ ШВИДКОСТІ ФРАКТАЛЬНОГО МЕТОДУ УЩІЛЬНЕННЯ ЗОБРАЖЕНЬ ЗА РАХУНОК АПРОКСИМАЦІЇ

Майданюк Володимир, Ліщук Олександр

Вінницький національний технічний університет

Анотація

Проаналізовано фрактальний метод ущільнення зображень. Виконано аналіз варіантів оптимізації та підвищення швидкодії фрактального ущільнення зображень. На основі досліджень розроблено швидкодіючий алгоритм фрактального ущільнення та його програмна реалізація

Abstract

The fractal image compression method is analyzed. The analysis of variants of optimization and increase of speed of fractal coding of images is carried out. On the basis of researches, a high-performance fractal sealing algorithm and its software implementation are developed.

Вступ

Зображення, які представлені в цифровій формі, необхідно зберігати на носіях та передавати каналами зв'язку. Для економії пам'яті та більш ефективного використання ресурсів системи створюють спеціальні алгоритми кодування [1-4]. Зображення – це особливий вид даних, який має надлишковість в двох вимірах, що дає додаткові можливості для ущільнення [4]. Одним із перспективних методів ущільнення зображень є фрактальний метод [4]. Фрактальне кодування - це математичний процес для кодування растрів, які містять реальне зображення, в сукупність математичних даних, що описують фрактальні властивості зображення. Цей вид кодування заснований на тому, що усі природні і більшість штучних об'єктів містять надмірну інформацію у вигляді однакових блоків зображення, що повторюються. Вони отримали назву фракталів. Фрактал - це структура, яка складається з подібних форм і малюнків, що зустрічаються в різних розмірах.

Актуальність

Алгоритм фрактального ущільнення відомий тим, що в деяких випадках дозволяє отримати дуже високі коефіцієнти ущільнення (найкращі приклади - до 1000 разів при прийнятній візуальній якості) для реальних фотографій природних об'єктів, що неможливо для інших алгоритмів ущільнення зображень з втратами.[1-2]

Основним недоліком фрактального методу є низька швидкість кодування, яка пов'язана з тим, що для отримання високої якості зображення для кожного рангового блоку необхідно виконати перебір всіх доменних блоків, і для кожного доменного блоку необхідно виконати не менше восьми афінних перетворень [3-5]. Одна з можливих ефективних та швидких схем кодування зображень фрактальним методом, запропонована Арно Жакеном (Arnaud Jacquin) [2]. Але якщо порахувати кількість операцій множення для знаходження коефіцієнтів афінних перетворень одного рангового блоку у зображенні в градаціях сірого розміром 512x512 пікселів при розмірі рангового блоку 4x4 ($n=4$), доменного 8x8 і кроці вибору доменних блоків 2, то навіть для алгоритму запропонованого Жакеном загальна кількість операцій множення складе [1]:

$$M = 8(4n^{k+1}(n^{k-1} - 3) + 9n^2) = 8(4 \cdot 4^{5,5} \cdot (4^{3,5} - 3) + 9 \cdot 4^2) = 8193152.$$

Отже, задача підвищення швидкості ущільнення зображень фрактальним методом є досить актуальною. При покращенні показників швидкодії алгоритм фрактального

ущільнення може стати одним з найбільш ефективних алгоритмів ущільнення зображень[1].

Підвищення швидкості фрактального алгоритму ущільнення зображень

Для підвищення швидкодії методу за схемою Арно Жакена запропоновано виконувати попередній відбір доменних блоків на основі коефіцієнтів апроксимації.

При лінійній апроксимації значення пікселя для двовимірного зображення визначається так:

$$f(x, y) = ax + by + c. \quad (1)$$

В загальному випадку значення $f(x, y)$ відрізняються від значення пікселя z_{xy} . Мінімальне значення відстані досягається при мінімальному значенні суми квадратів відстаней, тобто:

$$S = \sum_{x=1}^N \sum_{y=1}^M (ax + by + c - z_{xy})^2 = \text{Min!}, \quad (2)$$

де M, N – розміри зображення,

z_{xy} – значення пікселя в точці зображення з координатами x, y .

Функції S має мінімальний екстремум у точці, де частинні похідні від коефіцієнтів дорівнюють нулю:

$$\frac{\partial S}{\partial a} = 0, \quad \frac{\partial S}{\partial b} = 0, \quad \frac{\partial S}{\partial c} = 0. \quad (3)$$

Таким чином отримаємо систему із трьох рівнянь для трьох невідомих.

Для рангових блоків з розміром $n=4$ система рівнянь така:

$$\begin{cases} 120a + 100b + 40c = \sum_{y=1}^4 \sum_{x=1}^4 z_{xy} x \\ 100a + 120b + 40c = \sum_{y=1}^4 \sum_{x=1}^4 z_{xy} y \\ 40a + 40b + 16c = \sum_{y=1}^4 \sum_{x=1}^4 z_{xy} \end{cases} \quad (4)$$

Розв'язавши систему рівнянь (4) можна для кожного рангового і доменного блоків визначити коефіцієнти апроксимації a, b, c .

Таким чином, процес кодування буде включати такі додаткові кроки:

1. Кожен доменний і ранговий блок подаємо у вигляді коефіцієнтів апроксимації. Для $n=4$ коефіцієнти апроксимації з (4) обчислюються так:

$$b = \frac{-3 \sum_{x=1}^4 \sum_{y=1}^4 z_{xy} + 1,2 \sum_{x=1}^4 \sum_{y=1}^4 z_{xy} y}{24}, \quad (5)$$

$$c = \frac{3 \sum_{x=1}^4 \sum_{y=1}^4 z_{xy} - \sum_{x=1}^4 \sum_{y=1}^4 z_{xy} x - 20b}{8}, \quad (6)$$

$$a = \frac{3 \sum_{x=1}^4 \sum_{y=1}^4 z_{xy} - \sum_{x=1}^4 \sum_{y=1}^4 z_{xy} y - 8c}{20}, \quad (7)$$

2. Для кожного рангового блоку виконується попередній відбір доменних блоків за трьома коефіцієнтами апроксимації, наприклад, за квадратичним відхиленням:

$$\begin{aligned} S_{rd1} &= (a_r - a_d)^2 + (b_r - b_d)^2 + (c_r - c_d)^2, \\ S_{rd2} &= (a_r - b_d)^2 + (b_r - a_d)^2 + (c_r - c_d)^2 \end{aligned} \quad (8)$$

де a_r, b_r, c_r – коефіцієнти апроксимації для рангового блоку;
 a_d, b_d, c_d – коефіцієнти апроксимації для доменного блоку.

З відібраними блоками виконуються перетворення характерні для фрактального ущільнення методом Жакена. Оскільки вибраних блоків значно менше загальної кількості доменних блоків, то слід очікувати значного виграшу в швидкодії.

Висновок

Аналіз фрактального ущільнення зображень показав, що даний метод здатен забезпечити найкраще співвідношення ступеня ущільнення і якості відновленого зображення та має хороші перспективи для подальшого розвитку. Основним недоліком фрактального методу є низька швидкість ущільнення. Вона пов'язана з тим, що для отримання високої якості зображення, для кожного рангового блоку необхідно виконати перебір всіх доменних блоків. Для кожного доменного блоку необхідно виконати не менше восьми афінних перетворень. Ця проблема розв'язана тільки частково. Внаслідок відзначених недоліків цей метод застосовується на практиці порівняно рідко.

Запропоновано метод підвищення швидкості фрактального ущільнення шляхом подання рангових та доменних блоків у вигляді коефіцієнтів апроксимації, що дозволяє виконати швидкий попередній відбір доменних блоків, що в результаті значно підвищить швидкість фрактального ущільнення.

Список використаних джерел:

1. Кожем'яко В.П. Аналіз та перспективи розвитку кодування зображень / В.П. Кожем'яко, В.П. Майданюк, К.М. Жуков - Вісник ВПІ, 1999, № 3. – 42-48с.
2. Майданюк В. П. Методи і засоби комп'ютерних інформаційних технологій. кодування зображень. навчальний посібник // Вінниця: вду, 2001. – 63 с.
3. Кожем'яко В.П., Майданюк В.П., Жуков К.М., Хамді Р.Р., Піка С.О. Фрактальне стиснення зображень природного походження // Міжнародний науково-технічний журнал "Вимірювальна та обчислювальна техніка в технологічних процесах", Хмельницький, 1999, № 2, с. 50-54
4. Kozhemiako V.P., Maidanuk V.P., Pika S., Zhukov K.M. Speeding up of fractal image compression // Proceeding of spie, 2001, vol. 4425, p. 9-16.
5. Майданюк В. П., Ліщук О. О., Король Д. С. Аспекти оптимізації швидкості фрактального ущільнення зображень // Оптико-електронні інформаційно-енергетичні технології. Міжнародний науково-технічний журнал, №1 (33), 2017. - С. 24-32.

ВИКОРИСТАННЯ ГЕНЕТИЧНИХ АЛГОРИТМІВ ДЛЯ КОРЕГУВАННЯ ВАГ НЕЙРОННИХ МЕРЕЖ

*Суприган Олена, Ваховська Любов,
Очеретний Анатолій, Крутенко Ігор, Харчук Денис*

Вінницький національний технічний університет

Анотація

В матеріалах розглядається спосіб використання генетичних алгоритмів для корегування ваг нейронних мереж для прискорення їх навчання та підвищення ефективності роботи.

Abstract

The materials consider the use of genetic algorithms for correcting the weights of neural networks to accelerate their training and increase the efficiency of work.

Основний механізм еволюції - це природний відбір. Його суть полягає в тому, що більш пристосовані особи мають більше можливостей для виживання і розмноження і, отже, приносять більше нащадків, ніж погано пристосовані особи. При цьому завдяки передачі генетичної інформації (генетичному спадкуванню) нащадки успадковують від батьків основні їхні якості. Таким чином, нащадки сильних індивідумів також будуть відносно добре пристосованими, а їхня частка в загальній масі особ буде зростати.

Завдання полягає в оптимізації ваг нейроної мережі(НМ), що має апіорі задану топологію. Ваги кодуються у вигляді двійкових послідовностей (хромосом). Кожна особина популяції характеризується повним набором ваг НМ. Оцінка пристосованості особин визначається функцією пристосованості, що задається у вигляді суми квадратів погрешностей, тобто різниць між очікуваними (еталонними) і фактично отримуваними значеннями на виході НМ для різних вхідних даних. Приведемо два найважливіші аргументи на користь застосування ГА для оптимізації ваг НМ. Перш за все, ГА забезпечують глобальний перегляд простору ваг і дозволяють уникати локальні мінімуми. Крім того, ГА можуть використовуватися в завданнях, для яких інформацію про градієнти отримати дуже складно або вона виявляється дуже дорогою.[1]

НМ навчена за допомогою алгоритму зворотного розповсюдження(ЗР) дуже часто використовується для вирішення широкого спектра проблем реального світу. Зазвичай алгоритм спуску градієнта використовується для адаптації ваг, виходячи з порівняння бажаної та фактичної реакції мережі на заданий вхідний стимул. Всі навчальні пари, кожен з яких складаються з вхідного вектора та бажаного вихідного вектора, формують більш-менш складну багатовимірну поверхню помилки під час тренувального процесу. Було зроблено численні пропозиції, щоб алгоритм спуску градієнта не міг бути захопленим в будь-якому мінімумі при обробці великої помилки. Цей документ описує підхід, щоб повністю замінити його генетичним алгоритмом. За допомогою деяких стандартних застосувань пояснюються характерні властивості як генетичного алгоритму, так і НМ.

Популярний інструмент оптимізації навчання НМ, градієнтний спуск має ряд недоліків. Це залежить від типу помилки, відправної точки (зазвичай значення випадково ініціалізованої ваги) та деяких додаткових параметрів. Зазвичай типи помилок мають багато локальних мінімумів, які зазвичай не відповідають бажаному критерію збіжності[2].

Існують деякі підходи, щоб запобігти закріпленню алгоритму зниження градієнта в будь-якому місцевому мінімумі при переміщенні по поверхні помилки. Деякі з них, що

часто використовуються, - це введення терміна імпульсу (корисно для точок високої кривизни) та використання синхронізованого зменшення швидкості навчання. Як тільки система застрягає в будь-якому місцевому мінімумі, вага може бути пробіжкою; до наступної ітерації продовжується додавання невеликого випадкового зсуву. Однак все це не в змозі дійсно подолати багато існуючих проблем.

Генетичні алгоритми (ГА) пропонують пошук ефективних методів вирішення складних проблем і можуть бути використані як потужний інструмент оптимізації. Що стосується вищезгаданих проблем градієнтного спуску, то повна заміна на ГА може бути вигідною. Окрім оптимізації дизайну НМ з використанням генетичних алгоритмів, це ще один дуже цікавий та біологічно мотивований симбіоз штучних НМ та еволюційного обчислення.

Для того, щоб отримати відповідне хромосомне уявлення про вагу мережі, вони повинні бути кілька разів ініціалізовані довільним чином і, відповідно, закодовані в лінійну структуру. Оскільки архітектура НМ попередньо визначена і залишається фіксованою після ініціалізації, хромосома виключно складається із значень ваги і не містить топологічної або структурної інформації. Тепер функція пристосованості кожного члена поточного населення обчислюється шляхом повторного виклику мережі для кожного набору ваг. Для того, щоб відповідати топології мережі, всі хромосоми потрібно знову декодувати.

Вибравши відповідні параметри для керування ГА, можна досягти високої ефективності та продуктивності. НМ працюють тільки в режимі виклику, які можна легко застосувати та, які гарантують досить просту адаптацію до будь-яких вимог щодо їх поведінки, які виконують поставлену задачу. В подальшому, принаймні, одна особа повинна відповідати критерію зупинки (конвергенції).

Він являє собою набір ваг найуспішнішої мережі. Це може бути застосоване до актуальної проблеми, так само як би це було навчений зворотним поширенням або будь-якою навчальною послідовністю. Відтепер неважливо, як насправді тренувалася мережа.

Симбіоз штучних НМ та генетичних алгоритмів не є новою ідеєю. Тим не менше, використання генетичних алгоритмів у навчанні НМ все ще варто дослідити, особливо, якщо можна уникнути деяких недоліків навчання НМ. Насправді алгоритм ЗР для навчання НМ іноді стикається з деякими серйозними проблемами, і його повна заміна генетичним алгоритмом може бути дуже перспективним рішенням.

Таким чином, було розглянуто обставини, в яких це може бути корисним і як це може бути досягнуто, та виконання відповідної реалізації. Припускаючи, що як зворотне поширення, так і генетичні алгоритми працюють з максимально наближеними оптимальними параметрами при порівнянних умовах, зворотне поширення перевершує генетичні алгоритми у випадку простих стандартних застосувань.

Список використаних джерел:

1. M. Minsky and S. Papert, *Perceptrons: An introduction to computational geometry* (Cambridge MA.: MIT Press, 1969).
2. Кононюк А.Ю. Нейронні мережі і генетичні алгоритми/ А.Ю. Кононюк – К.:«Корнійчук», . 2008. – 446 с. – ISBN 978-966-7599-50.

АНАЛІЗ МЕТОДІВ ПЕРЕТВОРЕННЯ СЛОВА В ВЕКТОР ФІКСОВАНОЇ ДОВЖИНИ ДЛЯ ЗАДАЧІ КЛАСИФІКАЦІЇ ТЕКСТІВ

Петришин Сергій, Переродов Артемій

Вінницький національний технічний університет

Анотація

Розглянуто поняття векторизації слів. Наведено основні задачі, для яких використовується векторизація слів. Розглянуто такі методи перетворення слів у вектор як one-hot encoding, word2vec, glove.

Abstract

The concept of word vectorization is considered. The main tasks, for which the word vectorization is used, are given. The following algorithms for word conversion into vector like one-hot encoding, word2vec, glove are considered.

Вступ

Векторизація слова – це перетворення слова у вектор дійсних чисел фіксованої довжини. Задача перетворення слова у вектор є досить актуальною проблемою при обробці тексту. Наприклад, ця проблема постає при вирішенні таких задач, як:

- класифікація текстів;
- аналіз емоційного забарвлення тексту;
- машинний переклад;
- підсумовування об'ємних текстів.

Аналіз основних методів векторизації слів

Основними методами, які використовуються для перетворення слів у вектор, є:

- one-hot encoding;
- word2vec;
- glove.

Метод one-hot encoding є найбільш простим методом векторизації слів. В даному методі кожне слово кодується за допомогою вектора фіксованої довжини, що дорівнює кількості використовуваних слів в вибірці. Кожен вектор складається з нулів і однієї одиниці. Недоліком цього методу є величезна довжина вектору слова, так як в основному вибірка слів складається з десятків, а то і сотень тисяч слів.

Word2vec – це метод розрахунку векторних представлень слів, який реалізує дві основні архітектури: [1]

- Continuous Bag of Words (CBOW);
- Skip-gram.

На вхід подається корпус тексту, а на виході виходить набір векторів слів. Знаходження зв'язків між контекстами слів згідно з припущенням, що слова, що знаходяться в схожих контекстах, мають тенденцію означати схожі речі, тобто бути семантично близькими. Більш формально завдання стоїть так: максимізація косинусної близькості між векторами слів (скалярний добуток векторів), які з'являються поруч один з одним, і мінімізація косинусної близькості між векторами слів, що не з'являються поруч один з одним. Поруч один з одним в даному випадку означає в близьких контекстах.

Косинусна міра близькості (косинусна схожість) - це міра подібності між двома векторами. Косинусна схожість між векторами A і B обчислюється за формулою [1]:

$$similarity = \cos \theta = \frac{A * B}{\|A\| \|B\|} = \frac{\sum_{i=1}^n A_i \times B_i}{\sqrt{\sum_{i=1}^n (A_i)^2} \times \sqrt{\sum_{i=1}^n (B_i)^2}}$$

CBOW і Skipgram - це неймережеві архітектури, які описують, як саме неймережа «навчається» на даних і «запам'ятовує» представлення слів. Принципи у обох архітектур різні. Принцип роботи CBOW - передбачення слова по заданому контексті, а skip-gram навпаки - передбачення контексту по заданому слові. Skipgram модель працює повільніше, але зазвичай за допомогою неї досягається краща якість класифікації текстів.

Недоліком методу word2vec є те, що для навчання моделі word2vec хорошої якості потрібен дуже великий корпус текстів, але в мережі Інтернет доступні вже «навчені», на великих об'ємах даних, моделі.

Ще одним методом, який використовується для векторизації слів є метод Glove. Нехай об'єм словника даних рівний V . Усі слова, які зустрічаються в даних нумеруються від 1 до V . Складається матриця слово-слово $X \in R^{V \times V}$, де x_{ij} - кількість слів, коли слово i зустрічається в контексті слова j . Позначимо $X_{ij} = \sum_k V_{ik}$ (сума i -ої стрічки). Тоді ймовірність того, що слово j зустрілось в контексті слова i дорівнює $P_{ij} = P(j|i) = \frac{x_{ij}}{x_i}$ [2].

Для того, щоб зрозуміти, яке слово i або j зустріне в контексті слова k слід побудувати функцію: [2]

$$F(w_i, w_j, \hat{w}_k) = \frac{P_{ik}}{P_{jk}}$$

Автори метода Glove пропонують використовувати таку функцію [2]:

$$F((w_i - w_j)^T \hat{w}_k) = \frac{F(w_i^T \hat{w}_k)}{F(w_j^T \hat{w}_k)}, \text{ де}$$

$$F(w_i^T \hat{w}_k) = P_{ik} = \frac{X_{ik}}{X_i}$$

Отже, вектор w_i повинен бути таким, щоб: [2]

$$w_i^T \hat{w}_k = \log(P_{ik}) = \log(X_{ik}) - \log(X_i)$$

Недоліком цього методу, як і методу word2vec, є те, що для навчання моделі хорошої якості потрібен дуже великий корпус текстів. Також недоліком є складність обчислень.

В ході аналізу методів перетворення слова у вектор фіксованої довжини було розглянуто такі методи, як one-hot encoding, word2vec, glove. Для вирішення задачі класифікації текстів для перетворення слова в вектор був обраний метод word2vec, так як він забезпечує схожість векторів семантично близьких слів та має відносно невелику розмірність.

Список використаних джерел:

1. Метод векторизації слів - word2vec – [Електронний ресурс]. – Режим доступу: <http://nlpx.net/archives/179>
2. GloVe: Global Vectors for Word Representation – [Електронний ресурс]. – Режим доступу: <https://nlp.stanford.edu/pubs/glove.pdf>

ПЕРСПЕКТИВИ СТВОРЕННЯ ОБ'ЄКТНОЇ БАЗИ ДАНИХ ЗАСОБАМИ ОБОЛОНКИ КОМАНДНОГО РЯДКА WINDOWS POWERSHELL

Горбань Гліб

Чорноморський національний університет імені Петра Могили

Анотація

У доповіді представлені основні принципи роботи у командній оболонці PowerShell для операційної системи Windows на прикладі виведення вмісту каталогу. Показано, що результат виконання команд є сукупністю об'єктів певних класів .NET. Представлені команди, що можуть здійснювати фільтрацію об'єктів, та проведена їх аналогія із SQL-запитами для реляційних баз даних. Показана можливість створення власних класів у PowerShell та побудові на їх основі об'єктної бази даних.

Abstract

The paper presents the basic principles of working in the PowerShell shell for the Windows operating system as an example of outputting the contents of a directory. It is shown that the result of executing commands is a set of objects of certain .NET-classes. The commands that can filter objects are presented, and their analogy with SQL queries for relational databases is carried out. The ability of own classes creation in PowerShell and building on their basis an object database is shown.

Командна оболонка PowerShell для операційної системи Windows є відносно новою. Перша її версія вийшла у 2006 році, а починаючи з Windows 7, PowerShell є невід'ємною частиною даної операційної системи.

Дана оболонка була покликана замінити більш старі засоби автоматизації завдань у ОС Windows: командної оболонки cmd.exe та сервера сценаріїв Windows Script Host (WSH) [1,2]. Кожен з даних засобів мав свої недоліки. Cmd.exe хоча і був найбільш універсальним та простим у вивченні засобом автоматизації, втім за його допомогою можна було вирішити достатньо обмежене коло задач, оскільки дана командна оболонка не забезпечувала доступ до багатьох об'єктів, що підтримуються операційною системою. У свою чергу WSH представляв собою технологію написання сценаріїв, виконуваних у ОС Windows, на мовах програмування високого рівня, однак не був командною оболонкою. До того ж WSH вимагав великої роботи по вивченню даних мов (VBScript, Jscript) та суміжних технологій управління.

З появою PowerShell було вирішено багато проблем, що виникали при автоматизації рутинних задач у ОС Windows, зокрема проблема інтеграції командного рядка з об'єктами COM, WMI та .NET; робота з довільними джерелами даних в командному рядку за принципом файлової системи.

Головною особливістю нової командної оболонки стало те, що результатом виведення її команд є не текст, як було у командній оболонці Cmd.exe або у командних оболонках UNIX-подібних систем, а об'єкт. При цьому можна як вивести потрібні значення властивостей даних об'єктів, так і виконати їх методи. Оскільки сама оболонка PowerShell побудована на платформі .NET, будь який об'єкт, дані якого виводяться певною командною, є об'єктом .NET. До того ж внутрішня команда у PowerShell називається командлетом і теж представляє собою деякий клас .NET, який є нащадком класу Cmdlet, що є базовим класом для всіх внутрішніх команд. Більша кількість командлетів повертає певну інформацію, що виводиться на консоль та представляє сукупність об'єктів певного класу .NET.

Розглянемо, наприклад, командлет Get-ChildItem, що виводить вміст певного каталогу (якщо ім'я каталогу не задане, буде виведено вміст поточного робочого

каталогу). Даний командлет можна також викликати за псевдонімами `dir` та `ls` відповідно до назв команд оболонки `cmd.exe` та оболонок UNIX-подібних систем. Виконаємо його для виведення каталогу `C:\Windows`:

```
Get-ChildItem C:\Windows
```

В результаті буде виведена наступна інформація:

Каталог: `C:\Windows`

Mode	LastWriteTime	Length	Name
----	-----	-----	----
d-----	16.07.2016	11:30	addins
.....			
-a----	16.07.2016	11:26	707 _default.pif

По суті кожний виведений рядок представляє властивості окремого об'єкту деякого класу `.NET`. Однак за замовчуванням виводяться не всі властивості. Для того, щоб отримати назву класу, що є типом об'єктів, а також всі члени даного класу (властивості та методи), потрібно використати командлет `Get-Member`:

```
Get-ChildItem | Get-Member
```

Результат виконання командлету:

`TypeName: System.IO.DirectoryInfo`

Name	MemberType	Definition
----	-----	-----
LinkType	CodeProperty	System.String
LinkType{get=GetLinkType;}		
.....		
Root	Property	System.IO.DirectoryInfo
{get;}		
BaseName	ScriptProperty	System.Object
{get=\$this.Name;}		

Подібний механізм виклику в оболонках командного рядка називається конвеєром, який представляє собою ланцюг виконуваних команд, у якому результат виведення попередньої команди подається на вхід наступної. У конвеєрах часто використовуються команди, що здійснюють фільтрацію виведеної інформації.

Наприклад, командлет `Where-Object` здійснює вибірку об'єктів за певною умовою. Для прикладу, виведемо інформацію тільки про виконувані файли (`.exe`):

```
Get-ChildItem C:\Windows | Where-Object {$_.Extension -eq ".exe"}
```

Іншим прикладом роботи конвеєра є командлет `Select-Object`, що дозволяє вивести тільки вказані властивості об'єктів. Виведемо, наприклад, вміст каталогу, залишивши тільки ім'я підкаталогів або файлів та розмір файлів (для підкаталогів властивість розміру залишається порожньою).

```
Get-ChildItem C:\Windows | Select-Object Name,Length
```

До того ж існує командлет `Group-Object`, який виконує групування об'єктів за відповідною властивістю. Так, наприклад, можна дізнатись, скільки файлів, що мають відповідне розширення знаходиться у каталозі.

```
Get-ChildItem C:\Windows | Group-Object Extension
```

Результати роботи розглянутих вище командлетів нагадують результати запитів на мові SQL для реляційних баз даних. Дійсно, у сукупності об'єктів, що повертаються у якості результату виконання певних командлетів можна знайти аналогію з реляційною таблицею.

Однак в даному випадку дані все ж представлені у вигляді об'єктів класів. Все ж існує аналогія між табличними даними та даними, представленими у вигляді об'єктів. Так клас представляється таблицею, об'єкт – одним рядком таблиці, властивість – стовпчиком таблиці.

Об'єктно-орієнтована парадигма у свій час поклала початок розвитку об'єктної моделі даних, яка повністю побудована на класах [3,4]. Однією з основних відмінностей з реляційною моделлю даних є те, що зв'язки між об'єктами здійснюються не за полями (властивостями), а за посиланнями. У свою чергу посилання представляють такі самі властивості, тільки їх типами є не прості типи даних, а класи. Іншою відмінністю є те, що зв'язки між об'єктами є двонаправленими.

PowerShell дозволяє описувати свої власні класи [5]. У якості прикладу опишемо класи «Студент» та «Група» та оголосимо зв'язки між ними.

```
class Student
{
    [int]$id; [string]$surname
    [string]$name; [string]$midname
    [Group]$group;
}
class Group
{
    [int]$number; [string]$specialty
    [Student[]]$students
}
```

Так, об'єкт класу «Студент» містить посилання на об'єкт класу «Група», оскільки студент може належати до однієї групи, у свою чергу до однієї групи входить множина студентів, що відображується у властивості, що представляє собою масив посилань на об'єкти класу «Студент».

Створити нові об'єкти власних класів дозволяє командлет New-Object.

```
$s=New-Object Student; $g=New-Object Group; $s.Group=$g
```

Довгостроково ж зберегти об'єкти дозволяють файли у форматі XML, з якими у PowerShell існують достатньо розвинуті методи роботи [6]. У подальші плани автора входить дослідження побудови повноцінної об'єктної бази даних засобами оболонки PowerShell у ОС Windows.

Список використаних джерел:

1. Попов А. В. Введение в Windows PowerShell. – СПб.: БХВ-Петербург, 2009.- 464 с.
2. Б. Книттель. Windows 7. Скрипты, автоматизация и командная строка. СПб.: Питер, 2012, 764с.
3. The Object Data Standard: ODMG 3.0. Edited by R.G.G. Cattell Douglas K. Barry. Morgan Kaufmann Publishers San Francisco, California, 2000.
4. Харрингтон Д. Проектирование объектно-ориентированных баз данных: Пер. с англ. – М.: ДМК Пресс, 2001. – 272 с.: ил.
5. B. Payette, R. Siddaway. Windows PowerShell in Action, Third Edition. Manning Publications Co, 2018., 897 p.
6. M. Shepard, C. Venkatesan, S. Talaat, B. Blawat. PowerShell: Automating Administrative Tasks. Packt Publishing Ltd., 2017, 718 p.

УДК 159.946.2

ІННОВАЦІЙНІ ПІДХОДИ ФІЗИЧНОГО ВИХОВАННЯ СТУДЕНТІВ СПЕЦІАЛЬНИХ МЕДИЧНИХ ГРУП У ВИЩИХ НАВЧАЛЬНИХ ЗАКЛАДАХ

Аніскевич Світлана

ДВНЗ "Український державний хіміко-технологічний університет"

Анотація

У статті розглянуто значення тестування студентів, віднесених за станом здоров'я до спеціальних медичних груп, проаналізовано захворювання серед студентів, розроблено науково-методичне обґрунтування побудови програми із фізичного виховання в спеціальних медичних групах.

Abstract

The article examines the importance of testing students who are classified into special medical groups according to the status of health, analyzed the disease among the students, developed the scientific and methodological substantiation of building a program of physical education in special medical groups.

Актуальність дослідження

Фізичне здоров'я студентської молоді є актуальною проблемою сучасного суспільства. На державному рівні велика увага приділяється розробці і реалізації програм з оздоровлення нації. І для успішної реалізації програм, спрямованих на підвищення рівня фізичного розвитку і активного способу життя, необхідною умовою є потреба людини в руховій активності.

На жаль, у сучасного студента рухова активність мізерно мала. Однією з причин недостатньої рухової активності студентів є режим дня. Велика частина часу приділяється освіті, а вільний час від навчання сучасна молодь приділяє інтернет-простору [3].

Методи дослідження

При проведенні дослідження нами були використані статистичні показники, для обробки яких були використані методи системного підходу, статистичний метод та метод соціологічного аналізу.

База дослідження

Дослідження проводилось на базі дослідження структури захворюваності, медичних протипоказань до фізичних навантажень, термінів поновлення занять вправами реабілітації [1, 2].

Результати дослідження

На основі медичного обстеження 2017-2018 навчального року були зібрані статистичні дані стосовно захворюваності студентів вищих навчальних закладів.

Викладачами і лікарями відзначаються факти невідповідності вікових показників стану здоров'я та фізичної підготовленості студентів. Нами також було проведено аналіз захворювань студентів. У таблиці 1 показані в процентному співвідношенні захворювання, що є у студентів на момент початку навчального року.

Таблиця 1 – Аналіз захворювань студентів у 2017-2018 н.р.

№	Захворювання	%
1	Опорно-руховий апарат	40,68%
2	Міопія	5%
3	Серцево-судинні захворювання	13,65%
4	Бронхіальна астма	5,36%

Інтелектуальні інформаційні технології

5	Вегето-судинна дистонія	26,90%
6	Жовчнокам'яна хвороба	7,58%
7	Хронічний пієлонефрит	1,20%

Проаналізувавши дані з дослідження структури захворюваності, медичні протипоказання до фізичних навантажень, терміни поновлення занять вправами реабілітації, ми розробили науково-методичне обґрунтування побудови програми фізичного виховання в спеціальних медичних групах, у яких ураховується:

1. розвиток творчої спрямованості та потреби в пошуковій діяльності студентів СМГ, формування в них здатності виявляти, формулювати, аналізувати вправи із фізичного виховання відповідно до типу захворюваності;

2. опанування основ й методів педагогічних досліджень фізичного виховання, ознайомлення з основними поняттями інноваційних технологій навчання для використання вправ реабілітації;

3. освоєння технології інноваційної діяльності. Студенти беруть участь у розробці авторської програми (як колективної, так і індивідуальної), учаться аналізувати та прогнозувати розвиток нововведення, труднощі його впровадження;

4. практична робота з застосування нововведення, корекцію, відстеження результатів експериментальної роботи, самоаналіз діяльності.

Керуючись методами соціально-педагогічного й психологічного впливу, які сприяють формуванню мотиваційно-ціннісного ставлення до фізкультурно-спортивної освіти та забезпечення здорового способу життя студентів спеціальних медичних груп, пропонується тісний зв'язок самостійної роботи студента, звільненого від занять із викладачем фізичного виховання у форматі, наприклад, пошуку інформації, теоретичних завдань, контрольних робіт, також за допомогою Інтернету та електронної пошти. Для переходу до використання спеціальних фізичних вправ для реабілітації стану студента на основі самостійно зібраної інформації враховують нормування фізичних навантажень, компоненти (тривалість виконання вправ, їх інтенсивність, тривалість інтервалів відпочинку між вправами, характер відпочинку, число повторень фізичних вправ), виконуючи систематичний контроль із боку викладача за станом здоров'я студентів

Висновки та рекомендації

Розробка сучасних оздоровчо-профілактичних програм і технологій здорового способу життя, які сприятимуть зміцненню й підтримці здоров'я студентів та ліквідації бар'єрів, що перешкоджають використанню потенційних можливостей організму, є найважливішим завданням сучасної фізкультурно-оздоровчої освіти студентів спеціальних медичних груп.

Визначено, що впровадження тестів фізичного виховання в спеціальних медичних групах (СМГ) потрібне за умов якісного проведення поглибленого медичного огляду студентів; вивчення рівня реакції організму кожного з них на певне фізичне навантаження; використання рухових тестів не для визначення навчальної оцінки студента, а як «інструмента» сумісної діяльності викладача та студентів у підвищенні рівня їхнього оздоровчого спрямування; систематичний контроль із боку викладача за станом здоров'я студентів.

Список використаних джерел:

1. Корягін В. М. Фізичне виховання студентів у спеціальних медичних групах : навч. посіб. / В. М. Корягін, О. З. Блавт. – Львів : Вид-во «Львівська політехніка», 2013. – 488 с.

2. Магльований А. В. Основи фізичної реабілітації : навч. посіб. / А. В. Магльований, В. М. Мухін, Г. М. Магльована. – Львів : ВМС, 2006. – 148 с.

3. Попова О. В. Становлення і розвиток інноваційних педагогічних ідей в Україні у ХХ столітті / О. В. Попова. – Х. : ОВС, 2001. – 256 с.

УДК 159.946.2

ІННОВАЦІЙНІ ПІДХОДИ ДО ВИКОНАННЯ НАЦІОНАЛЬНОЇ ПРОГРАМИ “ФІЗИЧНА АКТИВНІСТЬ, ЗДОРОВИЙ СПОСІБ ЖИТТЯ - ЗДОРОВ'Я НАЦІЇ”

Охромій Галина, Аніскевич Світлана, Руднєв Андрій

ДВНЗ "Український державний хіміко-технологічний університет"

Анотація

У статті розглянуті сучасні тенденції та актуальний рівень загального стану здоров'я населення країни, розглянуто вплив економіко-соціального стану країни на стан показників залученості до спортивної активності населення та рівня стану здоров'я населення в сучасних умовах країни.

Abstract

The article considers the current trends and the actual level of general health status of the state population, considers the impact of the economic and social situation of the state on the indicators of the level of involvement to sports activities and health status of the population in current conditions of the state.

Актуальність дослідження

Відповідно до офіційних статистичних даних загальний стан здоров'я та рівень фізичного розвитку населення, зокрема молоді, як в Україні, так і в інших країнах світу у сучасних умовах із кожним роком стрімко погіршується. [1]

За даними Всесвітньої організації охорони здоров'я: лише 5% населення України займаються оздоровчої тренуванням (в той час як в Японії та США цей показник становить 80% та 70% відповідно). [2]

Дефіцит рухової активності і стреси в умовах розвитку суспільства є найважливішими причинами негативних змін в стані здоров'я населення, які спостерігаються у всіх економічно розвинених країнах. Гіподинамія і нервові перевантаження не тільки послаблюють опірність організму людини, але і служать причиною важких патологічних явищ. [4]

Проте, не зважаючи на великий внесок у дослідження проблеми сучасного рівню здоров'я населення, лише невелика кількість досліджень пов'язана із впливом економічного стану країни на показники рівню залученості до фізичної активності, фізичного розвитку населення та загального здоров'я нації.

Методи дослідження

При проведенні дослідження нами були використані статистичні показники, для обробки яких були використані методи системного підходу, статистичний метод та метод соціологічного аналізу.

База дослідження

Дослідження проводилось на базі статистичних матеріалів Державної служби статистики України, результати національного дослідження спортивної активності населення України, яке було ініційовано управлінням з питань фізичної культури і спорту. Опитування було проведено Центром соціальних експертиз Інституту соціології НАН України та центру Медичної статистики Міністерства Охорони Здоров'я України. [3, 5, 6, 7]

Результати дослідження

На основі отриманих даних було встановлено, що на рівень фізичного здоров'я населення впливає ряд причин, що призводять до пасивного ставлення до фізичних навантажень та спорту, серед яких основними є соціально-економічні, які визначають

рівень і якість життя населення (цими причинами є нестача коштів, відсутність вільного часу та ін.).

Поряд з цим існує цілий ряд факторів, пов'язаних з недостатньо ефективною роботою системи фізичного виховання і спорту: висока вартість послуг у спортивних центрах, недостатня кількість спортивних комплексів та ін.(Табл.1)

Таблиця 1 – Причини пасивного ставлення до спорту.

№	Причини пасивного ставлення до спорту	жінки, %	чоловіки, %	загалом, %
1.	Ціна послуг спортивних комплексів	82	80	81
2.	Нестача коштів	78	78	78
3.	Відсутність вільного часу	74	79	77
4.	Рівень фізичної культури	72	76	74
5.	Стан здоров'я	70	67	68,5
6.	Низький рівень добробуту спортивних комплексів	68	69	68,5
7.	Недостатня кількість спортивних комплексів	64	64	64
8.	Відсутність стимулів	60	62	61

Висновки та рекомендації

Основними причинами пасивного ставлення до спортивних занять є економічні причини. У кризових умовах гострої нестачі грошових коштів люди не схильні витратити їх на відвідування спортивних закладів для підтримання стану свого здоров'я.

Друге місце займають причини, пов'язані із нестачею вільного часу на зайняття спортом, що зумовлені, насамперед, ростом так званого "темпу життя". На наш погляд, ці дані говорять про проблему ціннісних орієнтацій сучасної людини. На тлі зростання значущості освіти, кар'єри, матеріального успіху поступово слабшають цінності здорового способу життя та спорту.

На третьому місці можна відзначити проблеми, пов'язані із низьким рівнем індивідуальної фізичної культури людини, здоров'ям населення і частими захворюваннями. Роль спорту в процесі зміцнення здоров'я людини на сучасному етапі є недооціненою, внаслідок практичної відсутності поняття про значимість спорту і здорового способу життя.

Проблеми низького рівня благоустрою спортивних комплексів в сучасних умовах повсюдного прагнення до комфортності та економії часу зумовлюють ще одну ланку причин пасивного ставлення до спортивної сфери життя людини.

Розпорядженням від 9 грудня 2015 року № 1320-р. Кабінет Міністрів затвердив Концепцію Державної цільової соціальної програми розвитку фізичної культури і спорту на період до 2020 року. [8]

Фінансування планується здійснювати за рахунок коштів держбюджету, інвестицій та інших джерел.

Міністерство молоді та спорту визначено державним замовником цієї програми.

У документі наголошується, що для подальшого розвитку фізкультури і спорту в Україні найоптимальніший варіант - об'єднання зусиль органів виконавчої влади, органів місцевого самоврядування, інститутів громадянського суспільства для проведення реформи.

Для цього пропонується визначити як основу європейську модель реформування і побудови взаємин між органами державної влади та громадськими організаціями фізкультурно-спортивної спрямованості, підвищити рівень публічності та прозорості діяльності Мінспорту, автономності спортивних федерацій. [8]

Для реалізації державної програми вважаємо необхідним проведення:

- заходів, спрямованих на залучення населення до спортивної активності і відведення фізичній культурі провідної ролі;
- агітаційної політики здорового способу життя, популяризація усіх видів фізичної активності серед населення;
- інформаційних заходів щодо впливу шкідливих звичок на здоров'я людини;
- заходів серед населення з метою впливу та допомоги людям у відмові від шкідливих звичок;
- поліпшення стану забезпечення сфери фізичної культури та спорту;
- забезпечення розвитку стану спорту для осіб із обмеженими можливостями;
- створення сприятливих умов для існування та розвитку спортивних клубів, спортивних кружків у всіх типах навчальних закладів та фінансова державна підтримка;
- розбудова спеціалізованих спортивних майданчиків у місцях масового відпочинку та місцях проживання;
- створення та покращення існуючої інфраструктури велоспорту, розмітка нових велодоріжок, підтримка у створенні та наданні населенню послуг прокату велотранспорту, розбудова велопарковок біля громадських місць та місць масового відпочинку;
- відведення та підтримання належного стану доріжок, призначених для занять біговим спортом;
- використання сучасних методів залучення та заохочення молоді до регулярних занять фізичною культурою, таких як, наприклад, створення мобільних додатків-трекерів, розробка доступних для всіх верств населення смарт-годинників із вбудованими засобами фітнес-трекінгу.
- використання сучасних методів та засобів донесення інформації, таких як інтернет-платформи, соціальні мережі та ін. для залучення молоді до участі у спортивних заходах, відвідуванні спортивних закладів, проведення організації спортивно-оздоровчих програм та заохоченні молоді до безпосередньої участі у процесі.

Список використаних джерел:

1. Весельський В.Л. Закономірності змін стану здоров'я населення України / В.Л. Весельський // Україна. Здоров'я нації. – 2007. – № 2. – С. 16–20.
2. Coordinated monitoring of participation in Sport in Europe. – London: UK Sport. – 65 – р.10.
3. Результати опитування українців щодо стану здоров'я. Rating Group Ukraine. – 2017. – Режим доступу: http://ratinggroup.ua/research/ukraine/zdorove_ukraincev.html.
4. Factors determining physical activity of Ukrainian. – 2016. – Режим доступу: <https://www.ncbi.nlm.nih.gov/pubmed/25292139>.
5. Центр медичної статистики МОЗ України. – Режим доступу: <http://moz.gov.ua/statistika>.
6. Державна служба статистики України. – Режим доступу: <http://www.ukrstat.gov.ua/>
7. Центр соціальних експертиз Інституту соціології НАН України. – 2017. – Режим доступу: <http://i-soc.com.ua/ua/edition/>.
8. Розпорядження від 9 грудня 2015 року № 1320-р. – Режим доступу: http://search.ligazakon.ua/l_doc2.nsf/link1/KR151320.html.

СИСТЕМА ЕФЕКТИВНОГО РОЗПОДІЛУ КОШТІВ НА ОСНОВІ НЕЧІТКОЇ ЛОГІКИ ТА SMART-КОНТРАКТІВ

Давиденко Євген, Швед Альона

Чорноморський національний університет імені Петра Могили

Анотація

Розглянуто створення системи передачі коштів головної організації між її інстанціями у вигляді smart-контракту. Цей контракт повністю покриває витрати на третіх сторін, забезпечує підтримку інформаційної стійкості у мережі та підтримує протокол безпеки, який є гарантом недоторканості коштів ніким, крім зазначених адресатів.

Abstract

The creation of a system for transferring funds from the parent organization between its instances in the form of a smart contract is considered. This contract fully covers the expenses of third parties, provides support for information security on the network and supports a security protocol that guarantees the inviolability of funds by no one except the specified addressees.

Технологія blockchain продовжує набирати популярність і впроваджуватися в різні сфери нашого життя. Основа технології blockchain – розподілене зберігання інформації. Це дозволяє розміщати важливу інформацію одночасно на декількох серверах, при цьому зберігати відкрито і безпечно. Інформацію, яка одночасно зберігається у багатьох місцях неможливо підробити тому, що оригінальні записи тут же можуть бути відновлені з сусідніх джерел [1].

Метою даної роботи є автоматизація процесу розподілу та передачі коштів головної організації між її інстанціями без допомоги третіх сторін та мінімізація корупції за допомогою blockchain сценарію.

В роботі головну увагу приділено використанню математичного апарата нечіткої логіки та нечітких множин при управлінні складними нелінійними системами з нестационарними процесами [2]. База правил системи нечіткого виводу призначена для формального подання знань експертів в області використання системи. У системах нечіткого виведення використовуються правила нечітких продукцій, в яких умови і виведення сформульовані в термінах нечітких лінгвістичних висловлювань. Сукупність таких правил називаються базами правил нечітких продукцій.

База правил нечітких продукцій являє собою кінцеву безліч правил нечітких продукцій, узгоджених щодо лінгвістичних змінних. В даному випадку база правил представляється в формі структурованого тексту [3]:

RULE_1: IF Condition_1 THEN Conclusion_1 (F1)

RULE_2: IF Condition_2 THEN Conclusion_2 (F2)

...

RULE_n: IF Condition_n THEN Conclusion_n (Fn)

Тут через $Fi(i\{1, 2, \dots, n\})$ позначені коефіцієнти визначеності або вагові коефіцієнти відповідних правил. Ці коефіцієнти можуть приймати значення з інтервалу $[0, 1]$. У разі якщо ці вагові коефіцієнти відсутні, зручно прийняти, що їх значення рівні 1.

Узгодженість правил щодо лінгвістичних змінних означає, що в якості умов і виведень правил можуть використовуватися тільки нечіткі лінгвістичні висловлювання, при цьому в кожному з нечітких висловлювань повинні бути визначені функції приналежності значень терм-множини для кожної з лінгвістичних змінних.

Перед тим як створювати систему, було проаналізовано існуюче програмне забезпечення. Визначено слабкі сторони:

- неможливість інтеграції з web-середовищем, лише локальне використання;
- дані неможливо пов'язати з окремими користувачами системи;
- неможливий збір статистичних даних.

В ході досліджень сформувались додаткові вимоги до системи, яка повинна вирішувати всі вказані недоліки та надавати можливості використання застосунку у web-середовищі разом зі збором усіх статистичних даних різних експертів.

Встановлення нових лінгвістичних змінних здійснюється на етапі обробки контрактів експертами. Експерт має право створити лінгвістичні змінні, визначити певні характеристичні показники для неї, та має можливість продивлятися графіки даних для наочності змін (рис. 1).

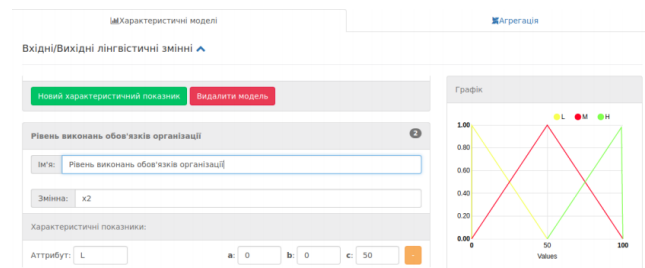


Рисунок 1 – Встановлення нових змінних та корегування графіку розподілу

Вирішення проблеми розподілу делегується на дефазифіковані дані. Дефазифікація проводиться завдяки трьом алгоритмам, які надають можливість вивести найбільш точну відповідь щодо результату розподілу коштів частками. Використані алгоритми: MINMAX, PRODMAX, MEANMAX.

Уся система покрита тригерами перевірки ролей. Клієнтська частина надає більше можливостей, оскільки тут є і перегляд транзакцій, і можливості підтвердження логіну, реєстрації користувачів.

Smart-контракт – це електронний алгоритм або умова, при виконанні якого сторони можуть обмінюватися грошима, нерухомістю, акціями та іншими активами. Для реалізації «розумного» договору необхідно мати децентралізовану мережу, де всі учасники мають рівні права. В якості фінансового інструменту використовується криптовалюта. Smart-контракт представляється у вигляді програмного коду на платформі Ethereum [4].

В результаті створено систему автоматизації процесу розподілу та передачі коштів. Процес обробки даних в якій є безпечним тому, що усі дані заведені до blockchain і через це їх неможливо підробити, також виключається можливість корупції та розтрат.

Список використаних джерел:

1. Бузов Г. А., Калинин С. В., Кодратьев А. В. Защита от утечки информации по техническим каналам. – М. : Горячая линия – Телеком, 2005. – 416 с.
2. Zadeh, L. A. (1968). Fuzzy algorithms. Information and Control 12 (2). с. 94. doi:10.1016/S0019-9958(68)90211-8. (англ.)
3. Сявавко М., Рибицька О. Математичне моделювання за умов невизначеності – Львів: Українські технології, 2000. – 320 с.
4. Що таке Ефіріум [Електронний ресурс] – Режим доступу <https://prostocoin.com/blog/what-is-ethereum> – Загол. з екрану.

ОПТИМІЗАЦІЯ МІСЬКОГО ТРАФІКУ ЗА ДОПОМОГОЮ ГЕНЕТИЧНОГО АЛГОРИТМУ

Тасьмук Дмитро, Месюра Володимир

Вінницький національний технічний університет

Анотація

З метою оптимізації міського трафіку запропоновано використати систему управління рухом в режимі реального часу. Систему створено з використанням генетичного алгоритму для керування сигналами світлофора. Наведено результати роботи розробленої системи, які показали збільшення продуктивності.

Abstract

In order to optimize urban traffic, it is suggested to use a real-time traffic control system. The system was created using a genetic algorithm for controlling traffic signals. The results of the work of the developed system, which showed an increase in productivity, are presented.

Вступ

Урбанізація та зростання заторів на дорогах створює нагальну потребу в максимально ефективному використанні транспортних систем [1]. Одним з найбільш економічно ефективних заходів для вирішення цієї проблеми є управління дорожнім рухом. Управління дорожнім рухом – це система для синхронізації часу будь-якої кількості світлофорів в певній зоні, з метою зменшення зупинок і загальної затримки транспортних засобів, а також збільшення загальної пропускної здатності. Системи керування сигналами світлофорів відрізняються за складністю: від простих систем, які використовують історичні дані для встановлення фіксованих проміжків перемикавання сигналів, до адаптивних систем управління, які оптимізують проміжки перемикавання сигналів відповідно до ситуації на дорозі в режимі реального часу [2].

Зазвичай система керування дорожнім рухом не забезпечує оптимальну пропускну здатність транспортних засобів через перехрестя. Забезпечення ефективного управління рухом в реальному часі для великої системи є надзвичайно складною задачею розподіленого керування. Тому управління рухом вимагає евристичного методу для підвищення його пристосованості до динамічних змін [3].

Застосування генетичного алгоритму

Для вирішення даної задачі використаємо генетичний алгоритм. Генетичний алгоритм – це евристичний метод пошуку, заснований на біологічному процесі еволюції. Застосуємо генетичний алгоритм для пошуку оптимального часу зеленого сигналу світлофора на основі дорожньої ситуації.

Метою є розробка ефективної стратегії адаптивного управління рухом, яка визначає ситуацію на дорозі на невеликих проміжках (інтервал спостереження) в режимі реального часу і обраховує проміжки сигналів світлофора для мінімізації функції пристосованості, що складається з лінійної комбінації показників ефективності для чотирьох смуг (рисунок 1).

Подамо функцію пристосованості як:

$$f = PI_1 + PI_2 + PI_3 + PI_4 \quad (1)$$

PI (performance index) залежить від ваги кожної дороги (тобто, пропускної здатності і пріоритету руху) та кількості автомобілів на дорозі.

$$PI_i = W_i * S_i \div GT_i, \quad i = 1, 2, 3, 4 \quad (2)$$

де W_i – вага дороги i ; S_i – кількість автомобілів на дорозі i ; GT_i – сума мінімального часу зеленого сигналу (G_{min}) та часу продовження зеленого сигналу (g).

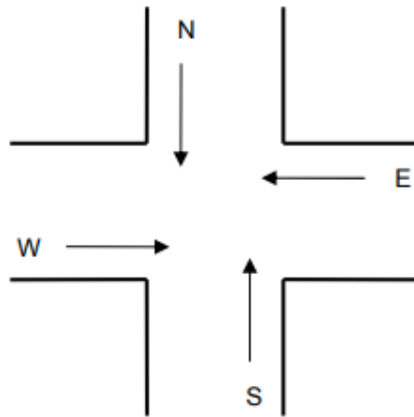


Рисунок 1 – Приклад перехрестя з чотирма смугами

Провівши тестування було отримано такі результати (таблиця 1): за 5 хвилин тестування система управління рухом в реальному часі пропустила 662 автомобілі і система з фіксованим часом змогла – 573 автомобілі. Таким чином у випадку системи управління рухом в реальному часі продуктивність збільшилась на 13,4 %.

Таблиця 1 – Порівняння системи з фіксованим часом і системи управління рухом в реальному часі

Час (в хвиликах)	Вихідний трафік (система з фіксованим часом)	Вихідний трафік (система управління рухом в реальному часі)
1	30	37
2	75	73
3	120	141
4	158	181
5	190	230
	Загалом: 573	Загалом: 662

Висновки

У даній роботі було розроблено «інтелектуальну» систему контролю світлофора на перехресті. Розроблена інтелектуальна система в режимі реального часу приймає рішення чи збільшувати час зеленого сигналу світлофора. Система показала підвищену продуктивність в порівнянні з системою, що заснована на фіксованому часі. Розроблена система базується на генетичному алгоритмі, який оптимізує час сигналу світлофора та надає набір оптимального часу зеленого сигналу для всіх чотирьох смуг на перехресті, в залежності від поточної ситуації на дорозі.

Список використаних джерел:

1. Тасьмук Д. І. Задача розфарбування графу для керування рухом на перехресті [Електронний ресурс] / Д. І. Тасьмук, В. І. Месюра // ВНТУ. – 2018. – Режим доступу до ресурсу: <http://conferences.vntu.edu.ua/index.php/all-fitki/all-fitki-2018/paper/view/5277/4321>
2. Leena Singht Time optimization for traffic signal control using genetic algorithm // International Journal of Recent Trends in Engineering. – 2009. – Volume 2, No. 2, P. 4 – 6.
3. Min K. Tan Optimization of Urban Traffic Network Signalization using Genetic Algorithm [Електронний ресурс] / Min Keng Tan, Helen Sin Ee Chuo, Renee Ka Yin Chin // Universiti Malaysia Sabah. – 2016. – Режим доступу до ресурсу: <https://pdfs.semanticscholar.org/6930/3b3bddb7956bc17c6eb958bfe7140fa00af1.pdf>

ГІБРИДНИЙ МОДУЛЬ ПЛАНУВАННЯ ШЛЯХУ МОБІЛЬНОГО РОБОТА У ДИНАМІЧНОМУ СЕРЕДОВИЩІ

Корчиста Ольга, Месюра Володимир

Вінницький національний технічний університет

Анотація

З метою підвищення ефективності планування шляху автономного мобільного робота пропонується створення гібридної системи, заснованої на сполученні нечіткої логіки та метаевристики мурашкової колонії.

Abstract

In order to increase the efficiency of path planning of autonomous mobile robot, it is proposed to create a hybrid system based on the combination of fuzzy logic and ant's colony metaheuristics.

Вступ

Бурхливий розвиток робототехніки робить все більш актуальною задачу динамічного планування шляху автономних мобільних роботів. У загальному випадку планування шляху належить до NP-повних задач, тобто потребує різкого зростання ресурсних витрат на пошук рішення при збільшенні масштабу задачі. Використання еволюційних алгоритмів дозволяє суттєво знизити розмірність задач дозволяє, але воно призводить до отримання наближеного результату [1]. Перспективним шляхом підвищення ефективності вирішення задачі динамічного планування шляху представляється використання гібридних систем обчислювального інтелекту, побудованих на сполученні нечіткої логіки та еволюційних алгоритмів [2].

Нечіткий мурашковий алгоритм

Для рішення складних комплексних задач оптимізації, метою яких є пошук і визначення найбільш прийнятної з дискретної множини можливих рішень, часто успішно застосовують метаевристику мурашкової колонії, засновану на імітації самоорганізації колони мурах. Колонія мурах може розглядатись як багатоагентна система, в якій кожний агент (мураха) автономно функціонує по дуже простих правилах. При цьому, на противагу до майже примітивної поведінки агентів, поведінка системи виявляється достатньо розумною [3].

Динамічний пошук оптимального шляху стикається з необхідністю враховувати певних додаткових параметри, наприклад таких як якість дороги, вартість проїзду, непередбачувані перешкоди штучного або природного характеру і т. ін. Досить часто врахувати дані параметри у тому вигляді, в якому вони подані, буває достатньо складно. Проблема може бути обумовлена неможливістю побудови аналітичної моделі об'єкта або її великою складністю, відсутністю достатньої інформації або досвіду для побудови експертної системи, недостатньою кількістю експериментальних даних для статистичного моделювання. Рішенням цієї проблеми може бути перехід до нечітких моделей.

Введення додаткової змінної, яка якимось чином характеризує той чи інший участок, вимагає визначення термів для новоствореної лінгвістичної змінної та подальшої модифікацій правил-продукцій.

Правила мають наступний вигляд:

$$IF x_1 = A_{1i} AND x_2 = A_{2i} AND ... AND x_n = A_{ni} THEN y = r_i, \quad (1)$$

де A_{ij} – лінгвістичний терм, яким оцінюється змінна x_j ; r_i – дійсне число, яким оцінюється вихід y .

Нечітка система здійснює відображення $f: \mathcal{R}^n \rightarrow \mathcal{R}$:

$$f(x) = \sum_{i=1}^R \mu_{A1i}(x_1) * \mu_{A2i}(x_2) * \dots * \mu_{Ani}(x_n) * r_i / \sum_{i=1}^R \mu_{A1i}(x_1) * \mu_{A2i}(x_2) * \dots * \mu_{Ani}(x_n), \quad (2)$$

де x – вхідний вектор; R – число правил; n – кількість вхідних параметрів; μ_{Aij} – функція належності, що визначається набором своїх параметрів.

Нечітка система може бути представлена як

$$y = f(x, \theta), \quad (3)$$

де $\theta = \|\theta_1, \dots, \theta_N\|$ – вектор параметрів; $N = n$ – число параметрів, що описують функцію належності; y – скалярний вихід системи.

Як і у випадку з класичним алгоритмом, важливими факторами модифікованого алгоритму є правила відкладання і випаровування феромонів, параметри налаштування, правило відбору шляху, кількість мурах та їх початкове розміщення.

Створюваний програмний продукт, функцією якого є вирішення задачі планування шляху на графі на основі нечіткого мурашкового алгоритму складається з таких основних складових: модуль створення графу; модуль реалізації нечіткого мурашкового алгоритму; нечітка продукційна база знань; модуль генерування нечітких правил динамічного планування шляху, який у режимі само навчання поповнює нечітку базу знань.

Отже, гібридний модуль динамічного планування оптимального шляху базується на нечітких правилах включає два компонента: нечітку базу знань, що подає знання про розв'язувану задачу вигляді продукційних правил з механізмом логічного виведення, заснованим на інформації що надходить від нечітких мурашкових агентів.

Розроблюваний програмний продукт орієнтований на мобільну платформу Android, тому модуль роботи мурашкового алгоритму винесено з головного потоку, оскільки проведення у ньому інтенсивних обчислень негативно впливає на досвід використання додатку користувачем. Архітектура системи базується на основі MVP-паттерну, що дозволяє відділити логіку програми, що реалізується на мові програмування Java без використання особливостей Android-системи, для більш ефективного її тестування.

Список використаних джерел:

1. Корчиста О.В. Інтелектуальний модуль планування шляху мобільного робота / О.В Корчиста, В. І. Месюра // – Вінниця: ВНТУ, 2017. – Режим доступу до ресурсу: <https://conferences.vntu.edu.ua/index.php/all-fitki/all-fitki-2017/paper/view/2026/1890>.
2. Корчиста О.В. Навігація мобільного робота у динамічному середовищі / О.В. Корчиста, В. І. Месюра // Вінниця: ВНТУ. – 2018. – Режим доступу до ресурсу: <http://conferences.vntu.edu.ua/index.php/all-fitki/all-fitki-2018/paper/view/5277/4321>
3. Bo Xing. Innovative Computational Intelligence: A Rough Guide to 134 Clever Algorithms [Електронний ресурс] / Bo Xing, Wen-Jing Gao // Intelligent Systems Reference Library. Volume 62. Springer. – 2014. – Режим доступу до ресурсу: www.springer.com/series/8578

ІНТЕЛЕКТУАЛЬНИЙ АНАЛІЗ МЕДИЧНИХ ДАНИХ

Мунтян Ольга

Вінницький національний медичний університет імені М.І. Пирогова

Анотація

Дослідження присвячено проблемі розробки уніфікованої методики інтелектуального аналізу медичних даних в рамках нової методології, яка базується на системному аналізі та сучасній статистичній парадигмі. Розглядаються критерії узгодженості та їх реалізація в сучасних пакетах прикладних програм математико-статистичного аналізу.

Abstract

The research is devoted to the problem of developing a unified methodology for the intellectual analysis of medical data in the framework of a new methodology based on system analysis and a modern statistical paradigm. Criteria of consistency and their realization in modern packages of applied programs of mathematical-statistical analysis are considered.

Інтелектуальний аналіз медичних даних (ІАМД) відіграє надзвичайно важливу роль в доказовій медицині, а його методи є інструментом (засобом) як безпосереднього оброблення результатів клінічних досліджень, так і функціоналом інтелектуальних систем підтримки прийняття лікарських рішень. Одним із методів ІАМД є математико-статистичний аналіз (МСА) результатів клінічних досліджень, який дозволяє виявити закономірності в досліджуваних процесах і явищах, обчислити статистичні параметри вибірок та оцінити параметри генеральної сукупності, встановити і дослідити причинно-наслідкові взаємозв'язки між даними. Результати цього аналізу є підґрунтям для прийняття чи відхилення висунутих в дослідженні гіпотез, вироблення висновків й узагальнень, та за висловом відомого американського математика, одного з основоположників послідовного статистичного аналізу А. Вальда – «прийняття оптимальних рішень в умовах невизначеності».

Незважаючи на велику кількість наукових публікацій та навчально-методичної літератури, присвячених питанням методології МСА та методики застосування його процедур, проблема вибору методів МСА, адекватних задачам дослідження, та коректного їх застосування на сьогодні залишається актуальною.

В роботі [1] визначені завдання, які необхідно виконати для розробки уніфікованої методики МСА результатів наукових досліджень в рамках нової методології, яка базується на системному аналізі та сучасній статистичній парадигмі. Одним із завдань є визначення передумов застосування кожного методу МСА.

В цій роботі розглядаються методи аналізу виду розподілу значень ознак (даних експерименту) та їх реалізація в поширених пакетах прикладних програм (ППП) МСА даних. Такий аналіз має бути першим етапом МСА, оскільки від його результатів залежить вибір способу опису дескриптивних (описових) статистик, зокрема характеристик центральної тенденції і розсіювання, та вибір адекватних методів подальшого аналізу даних. Якщо спосіб (формат) опису дескриптивних статистик є принципово важливим для подання результатів в наукових публікаціях, то правильний вибір методів МСА, наприклад, для порівняння груп, має вирішальне значення.

Традиційно перевіряється відповідність розподілу значень кількісних ознак закону нормального розподілу в припущенні, що розподіл значень ознаки в генеральній сукупності визначається за вибіркою.

Таку перевірку можна виконати різними способами:

1-й спосіб (якісний): побудова гістограми розподілу значень ознаки і візуальна її оцінка – наскільки вона близька до дзвону нормального розподілу (зазвичай виділяється

на гістограмі червоною лінією). Гістограма – це стовпчаста діаграма, яка відображає частотні дані. Всі ППП МСА і табличні процесори офісних пакетів (MS Excel та LibreOffice Calc) включають засоби побудови гістограм.

2-й спосіб (кількісний): Обчислення дескриптивних статистик та їх порівняння.

Вказані статистики обчислюються за допомогою відповідних інструментальних засобів ППП МСА або за допомогою бібліотечних статистичних функцій табличних процесорів офісних пакетів: AVERAGE (середнє арифметичне), MODE (мода – найчастіше повторюване значення), MEDIAN (медіана – значення, розташоване посередині набору), KURT (ексцес), SKEW (асиметрія) тощо.

Відзначимо, що для нормального розподілу: Mean=Mode=Median, Skewness=0, KURT=3.

3-й спосіб (кількісний): оцінка симетричності розподілу ознаки з тільки додатними значеннями. Якщо $SD < Mean/2$, то розподіл можна вважати симетричним. Але при цьому неможливо оцінити ексцес.

4-й спосіб (надійний): перевірка статистичних гіпотез про вид розподілу.

Формулюються дві гіпотези:

– нульова гіпотеза H_0 – про те, що розподіл ознаки в генеральній сукупності відповідає закону нормального розподілу (або близький до нього);

– альтернативна гіпотеза H_1 – про те, що розподіл ознаки в генеральній сукупності не відповідає закону нормального розподілу.

Перевірка статистичних гіпотез про вид розподілу значень ознаки виконується за допомогою статистичних критеріїв узгодженості. Найчастіше застосовуються наступні критерії узгодженості:

– Колмогорова-Смірнова (статистика D) та з поправкою Лілліфорса для випадків, коли середнє значення (Mean) та середнє квадратичне відхилення (СКВ, Standard Deviation – SD) ознаки відомі апіорі невідомі, а обчислюються за вибіркою;

– Шапіро-Вілка (статистика W) – найбільш потужний, строгий та універсальний – для випадків, коли Mean та SD ознаки апіорі невідомі;

– Д'Агостіно (асиметрія, ексцес);

– Андерсона-Дарлінга (статистика A-Sq);

– Крамера-Мізеса (статистика W-Sq);

Якщо розподіл кількісних значень ознаки нормальний або близький до нього, то МСА, зокрема, порівняння груп за цією ознакою, виконується параметричними методами. Якщо ж розподіл кількісних значень ознаки відмінний від нормального або значення ознаки є категоріальними (якісними), то для МСА, зокрема, для порівняння груп за цією ознакою, слід застосовувати непараметричні методи.

В дослідженні детально розглядаються інструментальні засоби перевірки відповідності розподілу значень кількісних ознак закону нормального розподілу найпоширеніших ППП МСА IBM SPSS (Statistical Package for Social Science), Statistics (IBM Corp., США), Statistica (StatSoft Inc., США), TIBCO Statistica (TIBCO Software Inc., США), StatPlus та BioStat (AnalystSoft Inc., США).

Список використаних джерел:

1. Мунтян О.А., Мунтян М.Л., Яровенко А.Г. Пакети прикладних програм статистичного аналізу результатів наукових досліджень / Суч. інф. технології та інноваційні методики навч. у підготовці фахівців: методологія, теорія, досвід, проблеми// 36. наук. пр. – Випуск 49 / редкол. – Київ-Вінниця: ТОВ фірма «Планер», 2017. – 186 с. – С.135-138.

ЗАСТОСУВАННЯ ГЛИБОКОЇ РЕКУРЕНТНОЇ НЕЙРОННОЇ МЕРЕЖІ ІЗ ВИКОРИСТАННЯМ АЛГОРИТМУ LSTM У СИСТЕМАХ ІНТЕЛЕКТУАЛЬНОЇ ВЗАЄМОДІЇ

Яровий Андрій, Кудрявцев Дмитро, Кулик Олександр

Вінницький національний технічний університет

Анотація

В ході проведеного дослідження проаналізовано прикладні аспекти використання різних типів нейронних мереж у галузі інформаційних відносин. Відзначено актуальність використання технології глибокого навчання у сфері обробки текстових масивів змінної довжини. Розроблено прототип системи із використанням нейронної мережі, на прикладі чат-боту.

Abstract

In the given research applies aspects of using different types of neural networks in information relations was analyzed. The actuality of using deep neural network in sphere of processing text arrays with variable length was noted. The prototype of system with using neural network on example of chat-bot was made.

Вступ

Сучасна сфера інформаційних відносин є однією з найбільш розвинених в останній період [1]. Базуючись на даному твердженні, більшість інформації, що оброблюється натеper складається із ланцюгів та послідовностей у вигляді діалогів. Спостерігаючи за популярністю та активністю соціальних мереж та корпоративних мереж [2], можна зробити висновок, що більшість сучасної інформації можливо розбити на кластери і класифікувати за певними ознаками. Наступним етапом, систематизувати у вигляді відповідних тематик та предметних областей, що значно підвищить рівень обробки вхідної інформації. Особливо, це стосується сфери інформаційної підтримки та систем підтримки прийняття рішень. Однією з ключових проблем є вибір засобу для обробки вхідної інформації, у даному випадку типу, архітектури та методу навчання нейронної мережі для задачі класифікації та розпізнання.

Порівняльний аналіз основних типів нейронних мереж

Натеper, значну швидкодiю виявляють нейронні мережі глибокого навчання, які дозволяють обробляти інформацію з великою пропускнуою та результативною здатністю [3]. Для обробки вхідної інформації, на вхід нейронної мережі подається набір сигналів, що характеризуються функціонально повноцінним змістовим значенням для розподілу між усіма нейронами першого шару. При використанні змінної розмірності вхідного набору даних, виникає необхідність застосування нейронної мережі з можливістю повторного використання. Дана вимога формується у разі використання чат-ботів та систем підтримки користувачів у веб-орієнтованих додатках.

У вказаних сферах, інформація являє собою діалоги між користувачем та інтелектуальною інформаційною системою, що представлена для користувача чат-ботом, системою підтримки прийняття рішень чи набором бізнес-правил [4]. При обробленні текстових повідомлень основна увага звертається на швидкодiю та точність розпізнання повідомлення. Для цього застосовується алгоритм LSTM (long short-term memory) [5], що використовує два вектори для кодування та декодування вхідних та вихідних наборів даних відповідно. Сутність даного алгоритму полягає у розбитті вхідної послідовності на менші частини, що значно спрощує задачу класифікації [4]. Основний принцип роботи даного алгоритму базується на використанні рекурентної нейронної мережі.

Передумовами створення даного алгоритму стала недостатня ефективність використання технології машинного навчання для типу послідовність-послідовність [4]. Застосовуючи даний алгоритм було досягнуто значного підвищення якості обробки вхідних наборів даних, а також підвищення точності матриці кореляцій [6]. В літературних джерелах описано спробу застосування згорткової нейронної мережі при тестових вибірках із, результатом якої було досягнуто точності розпізнання – 93%. Проте, при цьому загальне навчання нейронної мережі із використанням 8 GPU-систем зайняло 10 діб [6].

Глибокі нейронні мережі (Deep Neural Networks) – достатньо потужний засіб машинного навчання [4, 5], що надає високу продуктивність при розв’язанні складних задач, таких як розпізнання текстів та графічних зображень, що складають значну частину сучасних інформаційних об’єктів [3]. Однією з головних переваг мереж даного типу є їх спроможність до паралелізму [7], що значно пришвидшує оброблення вхідного набору даних. Загальна структура глибокої нейронної мережі, що застосовується при паралельній обробці зображена на рисунку 1.

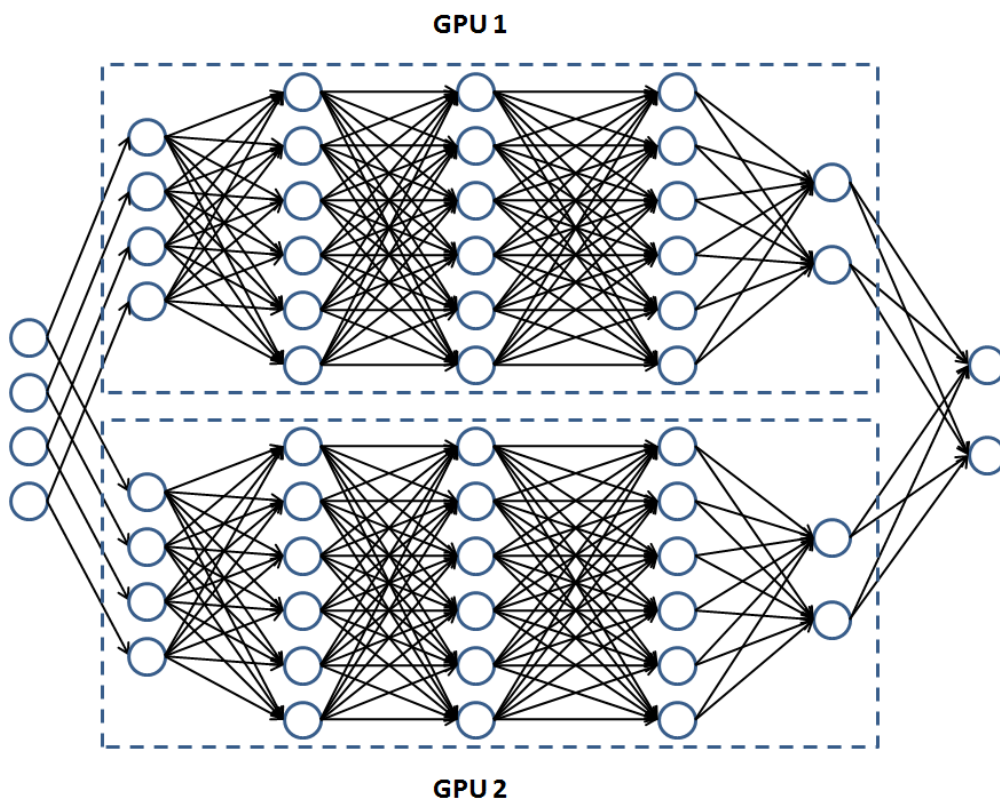


Рисунок 1 – Загальна схема багатошарової глибокої нейронної мережі із використанням двох GPU систем

При застосуванні глибокої рекурентної нейронної мережі виникає складність в задачах розпізнання тексту через змінну довжину вхідної та вихідної послідовностей зі складними немонотонними семантичними зв’язками [8]. Звичайна рекурентна нейронна мережа формує послідовність вхідних сигналів та формує вихідну послідовність за виразами [4]:

$$h_t = \text{sigm}(W^{hx}x_t + W^{hh}h_{t-1}) \quad (1)$$

$$y_t = W^{yh}h_t \quad (2)$$

Даний тип нейронної мережі із використанням алгоритму LSTM є досить перспективним рішенням для задачі розпізнання текстових повідомлень у сфері інформаційних відносин. Різниця у якості розпізнання тексту між двома рекурентними нейронними мережами з використанням алгоритму LSTM та без, склала понад 10% на користь алгоритму LSTM [9, 10].

Приклад використання

Для прикладу було створено чат-бот із використанням глибокої рекурентної нейронної мережі на основі пакетів прикладних бібліотек від Microsoft Cognitive Toolkit [11] та когнітивних сервісів Microsoft Cognitive Services. Також, застосовано фреймворк Microsoft Bot Framework та хмарний сервіс Azure Bot Service. Після тренування нейронної мережі (10^3 речень), на апробаційній вибірці (100 речень) було досягнуто точність розпізнання 94%.

Висновки

В ході проведених досліджень, здійснено порівняльний аналіз різних типів нейронних мереж для задачі розпізнання тексту змінної довжини, зокрема, згортовку, рекурентну та глибоку рекурентну нейронні мережі. Виокремлено проблемні аспекти використання звичайних рекурентних нейронних мереж для вказаної задачі. Відзначено ефективність використання алгоритму LSTM для розпізнання тексту змінної довжини та запропоновано його використання в роботі глибокої рекурентної нейронної мережі. Розроблено чат-бот із використанням когнітивного сервісу Microsoft, експериментальні результати якого підтверджують доцільність та перспективність застосування глибокої рекурентної нейронної мережі із використанням алгоритму LSTM у системах інтелектуальної взаємодії.

Список використаних джерел:

1. Joy Goodman-Deane, Anna Mieczakowski, Daniel Johnson and more. The impact of communication technologies on life and relationship satisfaction / Joy Goodman-Deane, Anna Mieczakowski, Daniel Johnson and more. – Engineering Design Centre, University of Cambridge, vol 57, pp. 219-229, April 2016.
2. C. Canali, M. Colajanni, R. Lancelotti. Data Acquisition in Social Networks: Issues and Proposals / C. Canali, M. Colajanni, R. Lancelotti – Department of Information Engineering, University of Modena and Reggio Emilia, pp 1-12, June 2011.
3. Tsung-Hsien Wen, Milica Gasic, Nikola Mrksic and more. A Network-based End-to-End Trainable Task-oriented Dialogue System / Tsung-Hsien Wen, Milica Gasic, Nikola Mrksic and more – Engineering Department, University of Cambridge, pp 1-12, 2016.
4. Ilya Sutskever, Oriol Vinyals and Quoc V. Le. Sequence to Sequence Learning with Neural Networks / Ilya Sutskever, Oriol Vinyals and Quoc V. Le, Advances in neural information processing systems, pp 3104-3112, 2014.
5. K. Yao and G. Zweig. Sequence-to-Sequence Neural Net Models for Grapheme-to-Phoneme Conversion, INTERSPEECH, pp 1-5, 2015.
6. Ross Girshick. Fast R-CNN, International Conference on Computer Vision, 2015.
7. А. Яровий, С. Кашубін і О. Кулик, Розпізнавання мімічних мікровиразів обличчя людини на основі комбінування Time Delay Neural Network та Deep Belief Network, Оптико-електронні інформаційно-енергетичні технології, vol 29, no 1, pp 76-83, Лип 2015.
8. Ramesh, Nallapati, Zhou, Bowen, Gulcehre, Caglar, Xiang, Bing et al. Abstractive Text Summarization using Sequence-to-sequence RNNs and Beyond. In Proc. of EMNLP, 2016.
9. Dahl, G. E., Yu, D., Deng, L & Acero, A. Context-Dependent Pre-Trained Deep Neural Networks for Large-Vocabulary Speech Recognition. IEEE Trans. Audio Speech Lang. Process, vol 20, pp 33-42, 2012.
10. Graves, Alex. Generating Sequences With Recurrent Neural Networks. Technical report, arXiv preprint arXiv:1308.0850, p 43, 2013.
11. Cho, K. Et al. Learning Phrase Representations using RNN Encoder-Decoder for Statistical Machine Translation. In Proc. Conference on Empirical Methods in Natural Language Processing, pp 1724-1734, 2014.

БЛОКЧЕЙН У ПРАВІ

Ховтун Олексій

Академія праці, соціальних відносин і туризму

Анотація

Охарактеризовано технологію блокчейн і її потенційне використання у суспільних галузях, зокрема у тих галузях, що пов'язані з юридичним регулюванням. Визначено переваги цієї технології та її можливості для системи права.

Abstract

The blockchain technology and its potential use in social sectors, in particular those related to legal regulation, are characterized. The advantages of this technology and its possibilities for the system of law are determined.

Вступ

Питання зміни сучасної системи права перебуває на порозі великих змін. Цифровий світ знаходить своє виявлення у кожній суспільній галузі і також він починає все більше проявляти себе в системі права.

Останні роки з'явилась технологія, котра набирає популярності у всьому світі. Така технологія – це блокчейн (у перекладі з англійської це «ланцюг блоків»). Блокчейн – це база даних, що послідовно фіксує кожну операцію і неможлива для хакерських атак, які в останній час все частіше зустрічаються в інтернет просторі. Технологія блокчейн – одна з тих, що швидше за всіх увійде у правове середовище. А чи готове суспільство до такого виклику?

Ця наукова розвідка розглядає технологію блокчейн і її потенційне використання у суспільних галузях, зокрема у тих галузях, що пов'язані з юридичним регулюванням.

Основні результати

Блокчейн – універсальна система зберігання, передачі, перевірки, захисту інформації і документації. Це розподілена база, тобто інформація зберігається не в єдиному центрі (сервері, реєстратора та ін.), а одночасно у великій кількості користувачів, і при цьому доступна всім учасникам ланцюга. Вони можуть відстежити ланцюжок транзакцій і історію дій того чи іншого користувача. Відповідно, в базі даних не можна змінити інформацію "заднім числом", підробити, втратити. Вона є у всіх контрагентів розподіленої системи і тому надійно захищена, залишаючись відкритою і прозорою. Відпадає необхідність додаткової перевірки, верифікації інформації, документів (факти, рахунки, підписи і ін.). Це автоматично роблять учасники всередині системи. Наявна економія часу, праці та інших витрат [1].

Ця технологія вже входить у велику кількість суспільних благ, які використовують в суспільстві. Так, блокчейн використовують у багатьох європейських банках. Ця технологія показала себе як інструмент з особливо високим рівнем безпеки та простотою використання. Також вона зменшує вартість банківських операцій та робить такі операції дуже швидкими та безпечними.

На сьогоднішній день дана технологія починає набирати популярність і в нашій країні. Сьогодні ця технологія використовується в СЕТАМ (система електронних торгів арештованим майном), що дає змогу систематизувати цю систему та унеможливити внесення змін певними особами. Така система повністю витіснить корупційну складову. Також в Україні пілотний проект застосування блокчейн в системі державного управління відбувається на ринку оренди та продажу державного майна [2].

Таку систему можливо назвати «істиною», оскільки вона фіксує факти та вносити зміни в неї може лише одна особа, спроба хакерським способом внести зміну в таку систему неможливо, оскільки вона записується одразу на мільйонах комп'ютерів, котрі

знаходяться он-лайн в інтернет просторі та підтвердження даної операції йде на всіх комп'ютерах одночасно.

Систему блокчейн необхідно почати впроваджувати у всіх суспільних галузях, а особливо в галузях, пов'язаних з юридичним регулюванням. Якщо взяти на прикладі земельний кадастр, то відомо що постійно проходять шахрайські схеми в даній галузі, помістивши всі дані в систему блокчейн шахрайські схеми відпадуть одразу, оскільки внести зміни стосовно конкретного об'єкта зможе лише власник особи.

Запроваджуючи блокчейн в систему державного регулювання, велика кількість бюрократичних факторів відпаде одночасно, на прикладі отримання певних довідок з державних реєстрів, достатньо буде зробити лише витяг з бази, що підтверджена системою блокчейн і дана довідка буде відповідати всім нормам, оскільки вона зроблена з бази, котра є «істиною».

Вагому частину змін займає питання документів, що ідентифікують особу. Сьогодні ці документи: паспорт та водійське посвідчення (дані документи найчастіше зустрічаються в нормативній базі, для ідентифікації особи). Паспортні дані починають оцифровуватись у всьому світі, водійське посвідчення не є обов'язковим для пред'явлення в деяких країнах, якщо ти здав всі іспити і тебе ввели в базу даних.

Питання відсутності паспорта в друкованому виді – це питання часу. На сьогоднішній момент питання ідентифікації особи за обличчям, статуєю, іншими фізичними ознаками, що можуть бути оцифровані набагато точніше, ніж друкований документ. Візьмемо, наприклад, ідентифікацію особи, що вчинила злочин, перш за все, якщо є запис на камери спостереження, можливо встановити особу за ознаками, які встановить програма та на які людина не звернула би увагу, наприклад, як особа ступає при кроці по сходах. Цифрова ідентифікація може дійти до рівня, котрий дасть можливість укладати угоду лише за наявності особи, що повністю змінить підхід до права власності. Оскільки дані будуть ідентифіковані автоматично і сторонам не потрібно буде мати с собою документи на майно, а й паспорт громадянина.

Система блокчейн змінить систему голосування, оскільки у кожного буде право проголосувати з власного телефону і лише один «голос». Це підвищить рівень відповідальності громадян, дасть можливість більшій кількості громадян проявити своє право голосу, оскільки на голосування піде значно менше часу. Також це спростить спосіб голосування для осіб з певними фізичними вадами, що відповідно до свого стану не мають можливості відвідати виборчі дільниці. Також це унеможливить процес фальсифікації виборів, оскільки система не дасть можливості внести в неї неправдиві дані. Великою перевагою буде зменшення витрат бюджетних коштів, оскільки програма зменшить кількість осіб, залучених до підрахунку голосів.

Система блокчейн, підключена до системи міністерства внутрішніх справ, може зробити революцію по багатьом напрямкам. В процесі вчинення особою адміністративного правопорушення (перевищення швидкості автомобілем, перехід вулиці на заборонений колір світлофора тощо) система буде автоматично притягувати особу до відповідальності, знімаючи з її рахунку кошти за штраф. Особа, яка вчинить правопорушення, що не дають змоги керувати транспортним засобом певний час, не зможе придбати автомобіль або паливо для нього. Не пройшовши медичної комісії не зможе вчиняти певні дії.

Таких прикладів можна навести чимало, але ця система почне функціонувати лише тоді, коли держава впровадить систему блокчейн у всіх сферах. Питання запровадження цієї системи в праві стоїть дуже гостро. Багато правників критикують дану систему, проте регулювання правових норм, запроваджених системою блокчейн, не дасть можливості подвійному трактуванню норм, що зробить правову систему «ідеальною».

Список використаних джерел:

1. Swan M. Blockchain: Blueprint for a New Economy. O'Reilly Media, 2015. 152 p.
2. Що таке блокчейн і як криптовалюта допоможе перемогти корупцію в Україні // Axon Partners. 2017. URL: <http://axon.partners/uk/blog/what-is-a-blockchain-and-how-cryptocurrency-will-help-to-defeat-corruption-in-ukraine>.

АНАЛІЗ МОЖЛИВОСТЕЙ ВИКОРИСТАННЯ ГЕНЕТИЧНИХ АЛГОРИТМІВ В ЕЛЕМЕНТАХ НЕЙРОННОЇ МЕРЕЖІ

Суприган Олена, Ваховська Любов

Вінницький національний технічний університет

Анотація

В матеріалах розглядається аналіз застосування генетичних алгоритмів для підвищення ефективності роботи нейронних мереж за рахунок інтегрування принципів навчання на базі генетичного алгоритму в елементи нейронної мережі.

Abstract

There is the analyze of genetic algorithms application for improving the efficiency of neural networks by integrating the principles of training based on the genetic algorithm into elements of neural network.

При розв'язанні технічних задач, які є важко розв'язуваними традиційними методами, доцільно використовувати методики, що забезпечують одночасну обробку та аналіз великої кількості різноманітних даних. Найочевиднішим рішенням такої проблеми є паралельна обробка інформації яка буде забезпечуватись за допомогою одночасного використання багатьох аналогічних шляхів обробки. Слід зауважити, що всі шляхи повинні постійно підтримувати взаємозв'язок, що приводить до формування мережі, здатної виконувати глобальну оцінку всіх даних які впливають один на одного, але не змішуються. Такий принцип реалізується за допомогою нейронних мереж (НМ) [1]. Вони не тільки забезпечать високий ступінь автоматизації, але й дозволяють виконувати динамічну обробку великих масивів даних. Їх властивість одночасної обробки інформації зводиться до розпаралелювання алгоритмів роботи з даними та надає можливість розвитку та еволюції даних за рахунок здатності навчання.

А в свою чергу, навчання дає можливість використовувати НМ для вирішення задач, які не мають чітко визначених даних. Таким чином, НМ не тільки дають змогу обробляти інформацію, але й створювати принципово нові характеристики, що описують можливі еволюційні зміни між початком роботи та кінцевим результатом. В результаті виникає можливість застосування нейромережевого принципу в системах адаптивного спрямування, тобто чутливих до зовнішніх змін.

Однак при детальному дослідженні НМ впливають проблеми, які пов'язані зі специфікою використання НМ у спеціалізованих випадках. Так при використанні стандартних методів аналізу НМ не здатні проводити багатоаспектну оцінку математичних задач, що приводить до концентрації на одному варіанті рішення без врахування варіативних можливостей. Якщо ж спробувати змінити варіанти результатів, то виникає необхідність застосування не найближчих наборів даних, а все, що було відомо раніше, тобто операції обробки даних зростають в геометричній прогресії, що тягне за собою значне збільшення ресурсів, але точність та швидкодія при цьому залишається на сталому рівні.

Для виправлення згаданих проблем досить ефективно використовувати принципи, які не будуть жорстко регламентувати використання даних та ресурсів. Для цього доцільно застосовувати методи, побудовані на використанні генетичних алгоритмів [2].

Генетичні алгоритми (ГА) дозволяють здійснювати пошук оптимальних рішень прикладних задач з врахуванням різноманітних можливостей використання та застосування даних, які за об'ємом залишаються сталими. Це досягається за рахунок того, що дані вважаються особинами, а їх обробка будується на механізмах природнього відбору і спадковості, на яких базується еволюційний принцип виживання найбільш пристосованих особин. При розгляді характеристик ГА спостерігаються такі їх переваги перед класичними оптимізаційними методами: вони не вимагають стандартизації та обмеження цільових функцій, а також дозволяють здійснювати пошук екстремуму одночасно по багатьох напрямках варіативного рішення, при цьому ГА не вимагає суттєвих обчислювальних витрат, тобто всі обчислення такого методу зводяться до визначення поліномів.

Для використання ГА в НМ необхідно чітко з'ясувати, яка саме задача буде вирішуватись та який рівень складності вона складає. Ці параметри важливі для формування вимог щодо тривалості навчання мережі та прийняття кінцевого рішення. Причому слід пам'ятати, що ГА використовує принцип випадковості створення нових даних (популяцій). Це важливо для проведення аналізу проміжних результатів та формування бази даних, так як під час процесу виконання ГА не тільки дасть можливість вирішити задачу, але й створити її можливі еволюційні варіанти рішення. Саме ці факти вимагають проводити дослідження проміжних результатів роботи, які формуються на різних етапах процесу навчання.

Під час процесу навчання НМ спостерігається велика кількість поколінь особин та епох ГА, що дозволяє одночасно досягти максимальної точності та провести аналіз можливих варіантів розв'язку задач. Але основною проблемою при цьому є саме велика кількість епох, що забирає значний час та ресурси. Вирішення цього протиріччя досягається за рахунок зменшення циклів формування поколінь, але не зменшити при цьому характеристики результатів (точність, варіантність). Тобто доцільно розглянути можливість створення той самої кількості популяцій за менший час.

Для вирішення такої задачі перш за все доцільно розглянути процес паралелізму ГА, тобто одночасно повинно відбуватись формування декількох популяцій, що дозволить створити покоління та завершити епоху значно швидше, за рахунок паралельного формування варіантів розв'язків.

Якщо використати паралельний ГА в НМ, то слід врахувати, що він застосовується як інструмент навчання цілої мережі, але при цьому не іде мова про можливість підвищення ефективності використання НМ за рахунок використання її особливостей. Мова іде про архітектуру НМ, адже вона від самого початку має паралельну будову, що можна використати для формування принципів розпаралелювання обробки інформації на будь-якому рівні.

Виходячи з цього виникає можливість використання цього паралелізму. Тобто навчання мережі проводити одразу по декількох шляхах, при цьому створювати паралельно декілька популяцій, які будуть враховувати характеристики еволюційного спрямування в межах однієї епохи. В результаті будуть створюватись одночасно декілька поколінь не чекаючи закінчення попередніх, що приведе до значного скорочення часу обробки при формуванні однакової кількості популяцій.

Пропонується для збільшення швидкості завершення епохи використовувати популяції особин не як єдину базу даних, а створювати їх в кожному окремому шарі НМ, що буде можливо у випадку використання елементарної НМ як нейрона, тобто постає питання про інтеграцію елементарних персептронів в глобальну НМ. При цьому кожний персептрон буде підлягати навчанню генетичним алгоритмом. Такий підхід дозволить одночасно формувати стільки популяцій, скільки містить нейронів кожний шар мережі, тобто створюється максимально можливий набір особин, що дозволяє аналізувати покоління за мінімальну кількість циклів навчання мережі, та обмежений лише розміром мережі.

При цьому в динамічному режимі будуть відстежуватись зміни функції пристосовуваності, що дозволить прийти до формування умов для адаптації мережі під наступну популяцію. В залежності від особливостей особин, що схрещуються, змінюються ймовірності мутацій, що дозволяє мережі самоналаштовуватись для подальшої адаптації.

Як наслідок, виникає можливість досліджувати архітектуру НМ, щодо здатності самоналаштовуватись під кожну конкретну ситуацію існування популяцій. Такий підхід дозволяє припустити, що використання стандартної архітектури НМ не буде обмежувати клас вирішуваних задач.

Таким чином, інтеграція генетичного алгоритму до нейромережі на всіх шарах дозволить перш за все зменшити час навчання та розвитку бази даних, а також дозволить використовувати НМ з простою стандартною структурою для вирішення різноманітних задач за рахунок здатності до адаптації.

Список використаних джерел:

1. Хайкин С. Нейронные сети: полный курс / пер. с англ. – 2-е изд. – М. : ИД «Вильямс», 2006. – 1104 с.
2. Гладков Л.А. Генетические алгоритмы / Л.А. Гладков, В.В. Курейчик, В.М. Курейчик. – М. : ФИЗМАТЛИТ, 2006. – 320 с.

ІНФОРМАЦІЙНА СИСТЕМА ПОШУКУ ЗОБРАЖЕНЬ В ЕЛЕКТРОННИХ ТЕКСТАХ З ВИКОРИСТАННЯМ ГІБРИДНОГО ПІДХОДУ

Удовенко Сергій¹, Чала Лариса²

¹Харківський національний економічний університет імені С. Кузнеця

² Харківський національний університет радіоелектроніки

Анотація

В доповіді розглядається гібридний підхід до створення інформаційної системи автоматичного пошуку зображень в електронних документах. Система передбачає можливість комбінованого аналізу текстових та візуальних характеристик кожного зображення для подальшого пошуку зображень, що відповідають запитам користувачів. Здійснено програмну реалізацію запропонованої системи.

Abstract

The report examines the hybrid approach to creating an information system for automatic image search in electronic documents. The system provides for the combined analysis of the text and visual characteristics of each image to further search for images that meet the user's queries. The program implementation of the proposed system was implemented.

Вступ

В даний час отримали розповсюдження цифрові технології, що сприяють стрімкому збільшенню кількості інформації, яка зберігається в базах даних різного тематичного призначення, з метою швидкого доступу до слабо структурованих текстово-графічних електронних документів [1]. Прогрес у методах зберігання даних і технологіях збору зображень дозволив створити великі бази даних з зображеннями, які використовуються в таких сферах, як техніка, торгівля, медицина, розваги, менеджмент, екологічний контроль тощо. Це викликає потребу розробки інформаційних систем для ефективного керування цими базами зображень та оперативного пошуку зображень за запитами користувачів. В доповіді розглядається гібридний підхід до створення такої системи, що передбачала б комбінований аналіз текстових та візуальних змістовних характеристик кожного зображення для подальшого пошуку зображень, що відповідають запитам користувачів пошукової системи.

Основна частина

Відзначимо, що всі системи пошуку зображень об'єднує необхідність аналізу подібності зображень для подальшого анотування або класифікації. Для реалізації цих завдань зазвичай застосовуються дві основні групи методів: перша з них ґрунтується на текстових метаданих кожного зображення для здійснення пошуку за ключовими словами; друга група ґрунтується на аналізі змістовних характеристик кожного зображення для подальшого пошуку зображень, що відповідають запитам користувачів. Пошук за ключовими словами в більшості випадків забезпечує кращі результати, ніж пошук за змістом в термінах часу відгуку та точності. Однак цей підхід вимагає апіорі наявності анотацій в базах даних зображень, внаслідок чого завдання пошуку є дуже трудомістким і часто суб'єктивним. Пошук за змістовними візуальними характеристиками буває необхідним, коли текстові анотації відсутні або неповні. Крім того, пошук за контентом потенційно може бути більш якісним, навіть якщо текстові анотації попередньо існували, завдяки додатковому інформаційному внеску змісту зображень.

В сучасних системах автоматичного пошуку та аналізу електронних документів часто виникає необхідність оброблення великих обсягів зображень, які можуть з часом

змінюватися. У базі зображень накопичується чимало графічних та текстово-графічних об'єктів, які або вже проіндексовані та проанотовані, або лише знаходяться в черзі на індексацію та анотацію (нещодавні надходження). Оскільки така база не анотована рівномірно, то необхідним є здійснення доступу до графічної інформації через текстові запити. На цей час існують різні методи взаємодії, навігації та пошуку графічних та текстово-графічних об'єктів в базах зображень. Насамперед, це модель короткотермінової взаємодії, що використовується для підвищення точності системи, та модель довготривалої взаємодії, що допомагає пов'язати текстові слова та візуальні характеристики для пошуку зображень за текстом, за візуальним наповненням чи за змішаними характеристиками (текст / зображення). Остання модель пошуку зображень дозволяє ітеративно формувати та уточнювати анотації до зображень.

Визначимо основні особливості гібридної системи пошуку зображень в текстово-графічних документах, яка розглядається у цій доповіді. По-перше, це мультимодальна система пошуку зображень, яка об'єднує різні джерела даних, зокрема, вміст зображення та текст. Ця система дозволяє проводити опитування за зображенням, опитування за ключовим словом або використання гібридних запитів. По-друге, це нова методика зворотного зв'язку, що поєднує класичні методи, які використовуються при пошуку інформації: рух точки запиту і розширення запитів. Ця методика дає хороші результати для інтерактивного пошуку зображень. По-третє, це застосування моделі під назвою «KVR» (Keyword Visual Representation – ключове слово «візуальне представлення») для створення зв'язків між семантичними поняттями та візуальними уявленнями. Завдяки послідовній стратегії навчання ця модель забезпечує зв'язок міжсемантичних понять та візуальних характеристик, що допомагає поліпшити точність анотації на зображення та результати пошуку. Четвертим пунктом є допоміжний алгоритм побудови відповідної бази знань, починаючи з нуля. Слід відзначити, що в запропонованій системі не розділяються етапи побудови анотацій та пошуку. Крім того, також користувач може робити запити відразу після запуску системи, яка буде навчатися в процесі експлуатації.

Система доповнюється інтерфейсом, що дозволяє візуалізувати змішані текстово-графічні запити. Навіть якщо на даний момент використовуються лише окремі типи інформації, тобто текстовий або візуальний, загальна пропонована модель дозволяє її розширити з залученням зовнішніх даних, таких як місцезположення (GPS) та час.

Розглянемо деякі аспекти реалізації запропонованої системи. Як вже було зазначено, база даних зображень запропонованої системи корегується в режимі реального часу. Обсяг зображень цієї бази не є фіксованим, адже інформація про зображення постійно розвивається, в залежності від нових зовнішніх подій, які можуть виникнути в будь-який час. Зазначимо припущення, які є важливими для використання та розвитку нашої системи:

- екземпляри зображень бази не завжди містять повну текстово-графічну інформацію;
- загальна кількість зображень не є фіксованою і обробка нових зображень здійснюється в режимі реального часу;
- база знань системи ґрунтується на анотаціях зображень, доповнених текстом, а також на їх візуальних характеристиках (колір, текстура, форма, просторова диспозиція);
- навчання є інтерактивним і може бути виконане шляхом використання методів навчання з підкріпленням. Взаємодія між користувачами та експертами системи має здійснюватися у простий спосіб для фільтрації не релевантних запитам зображень під час пошуку;
- навчання здійснюється на малих вибірках навчальних даних (до 20 екземплярів).
- система має формувати (аналізувати) анотації зображень в режимі реального часу.

З оглядом на ці гіпотези, в кожний поточний момент можуть розглядатися три типи зображень в пропонованій системі: зображення без анотації; зображення з додатковою

інформацією (наприклад, додатковий опис або довідкові дані); зображення з автоматично доданою інформацією (з «розширеними» анотаціями).

Можливість еволюції бази даних зображень і відповідної бази знань визначила такі сценарії формування запитів:

- сценарій 1: зображення без анотації використовується як запит, спрямований на пошук близьких зображень з бази даних;
- сценарій 2: набір слів в текстово-графічних документах використовується як повноцінний запит;
- сценарій 3: зображення та слова в текстово-графічних документах використовуються як повноцінний запит.

Проблема застосування двох останніх сценаріїв виникає, коли частина бази даних зображень не анотована, що робить цю частину недоступною через текстові запити. У цьому випадку необхідно використовувати зв'язок між текстовими словами та візуальними характеристиками для мультимодального пошуку та анотування зображень, які містять текстову частину.

Мультимодальний пошук зображень – це поєднання візуального пошуку зразків зображень та текстового пошуку за ключовими словами. Візуальна подібність між запитом, пов'язаним з зображенням в запиті, та текстово-графічним зображенням в базі даних оцінюється за величиною скалярного добутку відповідних векторів.

В доповіді запропоновано локальний критерій для визначення текстової подібності між запитом, пов'язаним з зображенням в запиті, та текстово-графічним зображенням в базі даних пошукової системи, що пропонується. Інтегроване значення подібності визначається з застосуванням глобального критерію, який передбачає використання вагових коефіцієнтів для зображень з розширеними анотаціями та для зображень без анотацій.

Структура запропонованої системи передбачає можливість постійної корекції елементів бази зображень з текстовими анотаціями та збільшення її розмірності. До основних блоків системи належать блок «KVR» (для створення зв'язків між семантичними поняттями та візуальними уявленнями), блок «ANOT-IMAGE» (для індексації та анотування текстової частини зображень) та блок навчання з підкріпленням «RL-IMAGE».

На основі запропонованого підходу розроблено програмний модуль інформаційної системи, пошуку зображень за запитом користувачів.

Результатом реалізації запропонованої гібридної схеми може бути формування електронної форми «Індикація можливості плагіату текстово-графічних документів», що створюється для кожного аналізованого об'єкту, з визначенням загальних коефіцієнтів подібності документів, які перевіряються, та побудовою порівняльної гістограми. Запропонована гібридна схема порівняння зображень здійснює перевірку оригінальності текстово-графічного об'єкту, що аналізується, як за джерелами мережі Інтернет, так і за власними базами текстів з зображеннями. Схема передбачає можливість аналізу подібностей та виявлення повного або часткового дублювання зображень.

Отримані результати можуть бути, зокрема, використані для розширення функціональних можливостей існуючих систем виявлення плагіату в наукових текстах, що містять текстово-графічні об'єкти [2].

Список використаних джерел:

1. Чалая Лариса Ернестовна. Поиск неполных дубликатов в системах анализа цифровых изображений / Л.Э. Чалая, П.Ю. Попаденко // Вісник КрНУ імені Михайла Остроградського. Вип. 5/2014 (88). – 2014. – С.42 – 47.
2. Лізунов Петро Петрович. Автоматичний аналіз подібностей схем та діаграм в електронних текстових документах / П. П. Лізунов, А. О. Білощицький, Л. Е. Чала, С.В. Білощицька, О. Ю. Кучанський, С. Г. Удовенко // Управління розвитком складних систем. – 2016. – № 28. – С. 147 – 156.

ПРОГРАМНІ СЕРЕДОВИЩА ДЛЯ ВИКОНАННЯ КВАНТОВИХ ОБЧИСЛЕНЬ

Шемет Євген, Яровий Андрій

Вінницький національний технічний університет

Анотація

В ході проведеного дослідження проаналізовані доступні програмні середовища для виконання квантових обчислень. Проведено порівняння програмних середовищ для імітаційного моделювання квантового комп'ютера за функціональними можливостями. Відзначено актуальність дослідження квантових обчислень в задачах криптографічного кодування.

Abstract

In the given research program environments for quantum computations were analyzed. Environments have been compared by functionality. The actuality of such quantum computations in cryptographic problem solving was denoted.

Вступ

Створюється велика кількість теоретичних і практичних розробок в сфері квантових обчислень [1]. Висока актуальність теми пов'язана з можливостями, які потенційно може надавати квантовий комп'ютер. Особливо важливі можливості (і навіть загрози) пов'язані з криптографією (наприклад, технологія блокчейн), призвели до створення нового напрямку пост-квантової криптографії [2]. До-квантова криптографія базувалася на трьох складних математичних задачах: “Факторизація цілих чисел”, “Визначення дискретного логарифму” та “Побудові еліптичних кривих”. Всі ці задачі можуть бути ефективно вирішені за допомогою алгоритму Шора на квантовому комп'ютері [3].

Для роботи з квантовим комп'ютером можна використовувати реальний квантовий комп'ютер або імітувати його роботу.

Способи задання квантового алгоритму

Для виконання квантових обчислень в програмному середовищі необхідно використати один із зазначених способів задання квантового алгоритму:

1. QASM - спеціальна мова подібна до асемблерної [4];
2. Схема - створення схеми в графічному режимі [5];
3. Предметно-орієнтована мова (Domain-specific language) - інструменти для імітаційного моделювання, розповсюджуються у вигляді бібліотеки для певної мови програмування та надають програмний інтерфейс.

Програмні середовища для імітаційного моделювання квантового комп'ютера

Програмні середовища для імітаційного моделювання квантового комп'ютера поділяються на:

1. Локальні - коли моделювання відбувається безпосередньо на комп'ютері користувача;
2. Онлайн - коли квантовий алгоритм, заданий певним чином, передається по мережі Internet і виконується в хмарному середовищі.

Необхідно відзначити, що існує велика кількість програмних розробок для імітаційного моделювання роботи квантового комп'ютера. Проте, більшість із них створено в учбових цілях. Разом з тим, велика кількість із них застаріла та більше не підтримується розробниками [6].

Локальні симулятори

Серед локальних симуляторів варто відзначити нову розробку LIQUi|) Microsoft. LIQUi|) (або Liquid) - високооптимізований інструмент що дозволяє симулювати до 30 кубіт одночасно, у локальному середовищі [7]. На даний момент локальні симулятори надають найбільш широкі можливості для проведення досліджень складних алгоритмів, з схемами що вимагають велику кількість кубіт.

Liquid може працювати в трьох режимах [8]:

1. Фізичне моделювання - моделювання, що намагається відтворити фізичні аспекти роботи квантового комп'ютера. Імітаційне моделювання повільне у зв'язку з тим, що доводиться вирішувати велику кількість диференціальних рівнянь. Може оперувати відносно невеликою кількістю кубітів (до 30);

2. Універсальне моделювання - гнучке імітаційне моделювання, що може оперувати з великою кількістю різних операцій (враховуючи ті, що задав користувач). Може оперувати невеликою кількістю кубітів (до 30);

3. Стабілізаційне моделювання - може опрацьовувати велику кількість кубітів одночасно (~10000). Обмежене невеликою кількістю операцій, що можуть виконуватись (група Кліфорда [9]).

Онлайн симулятори

Серед онлайн симуляторів існує дві групи розробок - симулятори, що використовуються для підготовки до виконання на реальних квантових комп'ютерах та окремі незалежні симулятори.

1.Forest - дозволяє здійснювати імітаційне моделювання роботи 26-кубітового квантового комп'ютера. Доступ через програмний інтерфейс (Python). Працює поряд з реальним квантовим комп'ютером [10].

2.IBM Q Experience - надає доступ до імітаційного моделювання на 5-ти кубітовому комп'ютері через графічний інтерфейс, та до 16-ти і 20-ти кубітовому комп'ютері через програмний інтерфейс QISKIT (Python). Працює поряд з реальним квантовим комп'ютером [11].

3.QuantumPlayground - імітаційне моделювання квантового комп'ютера від Google. Має графічний інтерфейс та дозволяє здійснювати імітаційне моделювання роботи 22-кубітового квантового комп'ютера [12].

Доступ до реального квантового комп'ютера

Наразі є кілька квантових комп'ютерів що надають доступ онлайн. Вони надаються безкоштовно або умовно безкоштовно (з певними обмеженнями).

1.Forest - надає доступ до реального 19-кубітового квантового комп'ютера. Доступ через програмний інтерфейс (Python), безкоштовно [10].

2.IBM Q Experience - дозволяє працювати на 5-ти кубітовому комп'ютеру через графічний інтерфейс, та до 16-ти і 20-ти кубітовому комп'ютеру через програмний інтерфейс QISKIT (Python). 5-ти та 16-ти кубітові процесори - безкоштовно. 20-ти кубітовий процесор - тільки для партнерів [11].

3.Quantum in the Cloud - розроблений The University of Bristol. Надає безкоштовний доступ до квантового комп'ютера на 4 кубіта [13].

Оскільки ресурс реального квантового комп'ютера обмежений, запуск алгоритму ставиться в чергу та очікує деякий час на виконання. IBM Q Experience пропонує, при наявності, отримати готові результати з минулих запусків подібних алгоритмів.

Особливістю реальних квантових комп'ютерів є те що на відміну від симуляторів, вони можуть підтримувати лише обмежену кількість зв'язків між кубітами, що обумовлене топологією.

Висновки

В ході дослідження здійснено порівняння програмних середовищ для квантових обчислень. Виокремлено ряд розробок великих міжнародних компаній, таких як: Google, Microsoft, IBM, що підтверджує високу зацікавленість сучасних ІТ-компаній в цьому напрямку. Поряд із ними існують розробки університетів (The University of Bristol), що підтверджує актуальність даного напрямку досліджень для наукових розробок. Також, виокремлено розробки невеликих компаній (стартапів), які будують свою бізнес-модель навколо квантових обчислень, що відкриває доступність квантових обчислень для невеликого бізнесу.

Не дивлячись на обмежені можливості існуючих квантових комп'ютерів, вони вже наближаються до потужностей, що можуть загрожувати криптографічній безпеці сучасних алгоритмів. Зокрема потужність окремого квантового комп'ютера порівнюють з потужністю усієї мережі розподіленої криптовалюти Bitcoin [14].

Досліджено ряд програмних сервісів, що надають безкоштовний доступ до потужностей справжнього квантового комп'ютера. Незважаючи на це, імітаційне моделювання залишається актуальним інструментом для підготовки алгоритмів до виконання на реальному квантовому комп'ютері та для імітування роботи алгоритмів високої складності, для яких й досі не існує необхідних апаратних потужностей.

Список використаних джерел:

1. Душкин Р. В. Квантовые вычисления и функциональное программирование. / Р.В.Душкин – М: ДМК Пресс, 2014. - 270 с.
2. Leon Groot Bruinderink. Towards Post-Quantum Bitcoin / Leon Groot Bruinderink – Master's thesis, Eindhoven University of Technology, 2016. - [Електронний ресурс] - Режим доступу: <http://repository.tue.nl/844305>
3. Daniel J. Bernstein. Introduction to post-quantum cryptography. / Daniel J. Bernstein - Department of Computer Science, University of Illinois at Chicago. – 2009.
4. Andrew W. Cross, Lev S. Bishop, John A. Smolin, Jay M. Gambetta. Open Quantum Assembly Language. – Cornell University Library, 2017. - [Електронний ресурс] - Режим доступу: <https://arxiv.org/abs/1707.03429>
5. Kosuke Mitarai, Makoto Negoro, Masahiro Kitagawa, Keisuke Fujii. Quantum Circuit Learning. – Cornell University Library, 2017 – [Електронний ресурс] – Режим доступу: <https://arxiv.org/abs/1803.00745>
6. List of QC simulators. - [Електронний ресурс] - Режим доступу: <https://www.quantiki.org/wiki/list-qc-simulators>
7. LIQUi) by Microsoft. - [Електронний ресурс] - Режим доступу: <http://stationq.github.io/Liquid/>
8. LIQUi) User's Manual. - [Електронний ресурс] - Режим доступу: <https://msr-quarc.github.io/Liquid/LIQUiD.pdf>
9. Maris Ozols. Clifford group / Maris Ozols – Essays at University of Waterloo – 2008.
10. Forest. - [Електронний ресурс] - Режим доступу: <https://www.rigetti.com/index.php/forest>
11. IBM Q Experience. - [Електронний ресурс] - Режим доступу: <https://www.research.ibm.com/ibm-q>
12. Quantum Playground by Google. [Електронний ресурс] - Режим доступу: <http://www.quantumplayground.net>
13. Quantum in the Cloud by The University of Bristol. - [Електронний ресурс] - Режим доступу: <http://www.bristol.ac.uk/physics/research/quantum/engagement/qcloud>
14. Divesh Aggarwal, Gavin K. Brennen, Troy Lee, Miklos Santha, Marco Tomamichel. Quantum attacks on Bitcoin, and how to protect against them. – Cornell University Library, 2017 – [Електронний ресурс] – Режим доступу: <https://arxiv.org/abs/1710.10377>

ІНФОРМАЦІЙНА МОДЕЛЬ ПРОЦЕСУ ПОШУКУ І ВИКОРИСТАННЯ АСОЦІАТИВНИХ ПРАВИЛ ПРИ РОЗРОБЦІ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Савчук Тамара, Приймак Наталія

Вінницький національний технічний університет

Анотація

У даній роботі запропоновано інформаційну модель процесу пошуку і використання асоціативних правил при розробці програмного забезпечення, що може бути використана при проектуванні відповідної інформаційної технології. Інформаційну модель представлено математично та графічно, описано її основні елементи та блоки.

Abstract

The information model of the process of searching and usage of associative rules while the development of software that can be used for designing of appropriate information technology is described in this paper. The information model is represented mathematically and graphically, its main elements and blocks are described.

Застосування технології Data Mining можливе майже на всіх етапах розробки програмного забезпечення (ПЗ): аналіз вимог, проектування та кодування, тестування та виправлення помилок. Пошук асоціативних правил є засобом штучного інтелекту, що дозволяє підвищити ефективність процесу розробки ПЗ, за рахунок знаходження залежностей, які можуть бути використані для удосконалення та покращення даного процесу.

В роботі [1] пропонується використання асоціативних правил для визначення вразливих місць в архітектурі ПЗ на ранніх етапах його розробки, що дозволить уникнути додаткових матеріальних витрат на їх виправлення в майбутньому. У [2] автори пропонують застосовувати алгоритм пошуку асоціативних правил Apriori та теорію нечітких множин для оцінки необхідних людських ресурсів в процесі розробки ПЗ. Отже, використання технологій пошуку асоціативних правил під час процесу розробки ПЗ є актуальною задачею, що може допомогти усім його учасникам розробити якісне програмне забезпечення у заданий термін та у межах виділеного бюджету.

Метою даної роботи є розробка інформаційної моделі процесу пошуку і використання асоціативних правил при розробці програмного забезпечення.

Інформаційну модель процесу пошуку і використання асоціативних правил при розробці програмного забезпечення (рисунк 1) можна подати у вигляді кортежа IMARM :

$$IMARM = \langle Task, Dev, minsupp, minconf, method, AR, newTask, PredictTask \rangle,$$

де *Task* – множина завдань, що були виконані під час розробки ПЗ; *Dev* – множина розробників, які можуть виконати поставлене завдання; *minsupp* – мінімальне значення підтримки АП; *minconf* – мінімальне значення достовірності АП, що задається менеджером проекту; *method* – метод, за допомогою якого буде здійснюватися пошук АП; *AR* – множина знайдених асоціативних правил; *newTask* – множина завдань, для яких необхідно визначити тривалість їх реалізації певним розробником. *PredictTask* – множина завдань з часом необхідним на їх виконання певним розробником.

Зазвичай значення *minsupp* визначається експертом в даній області (менеджером проекту), але для даної інформаційної моделі буде використовуватися формула, вперше запропонована в [3]:

$$minsupp = (e^{(-ax - b)}) + c$$

де x – це кількість записів в базі даних; a, b, c – додатні константи, що задаються експертом.

Інформаційна модель пошуку і використання асоціативних правил при розробці програмного забезпечення розділена на два окремих блоки:

1. У блоці пошуку асоціативних правил описано процес пошуку асоціативних правил у БД завдань, що виконувалися розробниками, результатом якого є множина асоціативних правил AR , що використовуються для прогнозування часу необхідного на виконання завдання конкретним розробником у наступному блоці.

2. У блоці використання асоціативних правил описано процес використання асоціативних правил, а саме визначення часу необхідного на виконання завдання конкретним розробником. В результаті чого утворюється множина завдань $Predict Task$ для яких визначено час необхідний на реалізацію певним розробником.

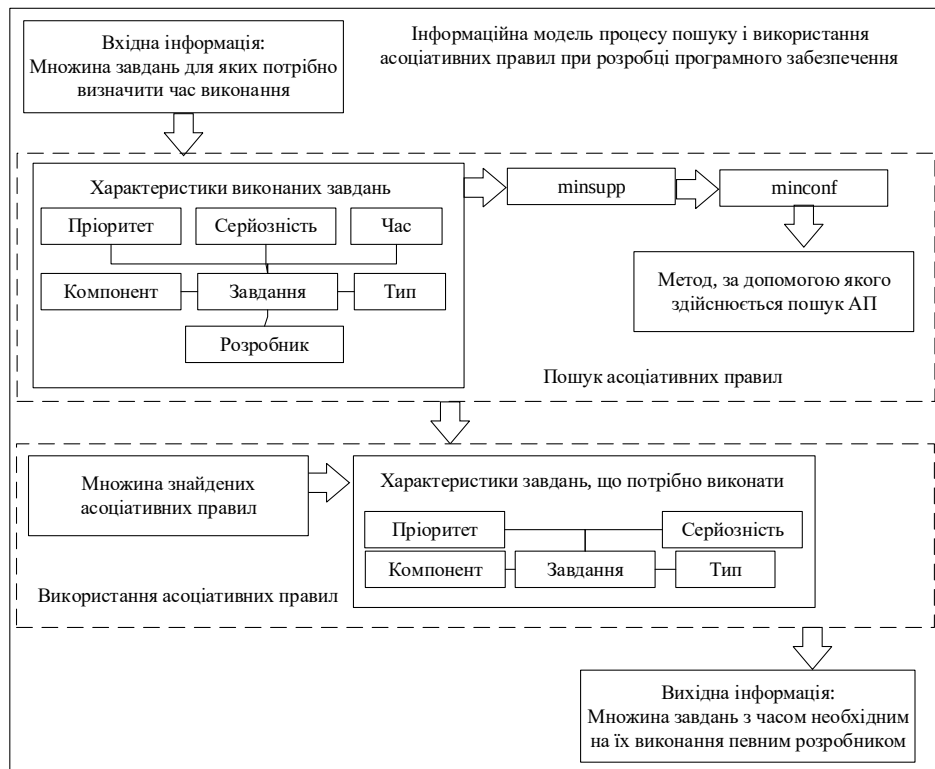


Рисунок 1 – Інформаційна модель процесу пошуку і використання АП при розробці програмного забезпечення

Отже, розроблено інформаційну модель процесу пошуку і використання асоціативних правил при розробці програмного забезпечення, що дозволяє знаходити залежності, які виникають під час даного процесу, та використовувати їх для визначення часу, необхідного для виконання завдання конкретним розробником.

Список використаних джерел:

1. Maffort C. Mining Architectural Patterns Using Association Rules/ C. Maffort, M. Tulio Valente, M. Bigonha// International Conference on Software Engineering and Knowledge Engineering (SEKE'13). – 2013. – pp.45-51.
2. Azzeh M. Software Stage-Effort Estimation Using Association Rule Mining and Fuzzy Set Theory/ M.Azzeh, P. I. Cowling // Computer and Information Technology (CIT). – 2010. – pp.105-113
3. Fournier-Viger, P, Un modèle hybride pour le support à l'apprentissage dans les domaines procéduraux et mal-définis: Ph.D. Thesis/ P. Fournier-Viger – Montreal:University of Quebec in Montreal, 2010. – p.67.

ОБГРУНТУВАННЯ ВИБОРУ МЕТОДУ ГЕНЕРАЦІЇ ЧАСТИХ ПРЕДМЕТНИХ НАБОРІВ ДЛЯ ПОШУКУ АСОЦІАТИВНИХ ПРАВИЛ ПРИ РОЗРОБЦІ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Савчук Тамара, Приймак Наталія

Вінницький національний технічний університет

Анотація

У даній роботі здійснено порівняльний аналіз методів генерації частих предметних наборів, що використовуються для пошуку асоціативних правил. Для кожного методу визначено його переваги та недоліки та обрано метод, який варто застосовувати для пошуку асоціативних правил при розробці програмного забезпечення.

Abstract

In this article a comparative analysis of the methods of generating frequent subject sets used to search for associative rules was done. For each method the advantages and disadvantages were determined and also the method, which should be used to search for associative rules in software development, was chosen.

Використання засобів та методів штучного інтелекту під час розробки програмного забезпечення (ПЗ), а саме методів пошуку асоціативних правил є актуальною задачею, що може бути застосована до основних етапів даного процесу, що допоможе розробити якісне програмне забезпечення у заданий термін та у межах виділеного бюджету, за рахунок використання знайдених залежностей.

Метою даної роботи є обґрунтування вибору методу генерації частих предметних наборів, серед яких здійснюється пошук асоціативних правил при розробці ПЗ.

Асоціативні правила (АП) описують закономірності виду $X \rightarrow Y$ для яких виконується умова $X \cap Y \rightarrow \emptyset$. Задачу пошуку асоціативних правил при розробці ПЗ можна розділити на дві підзадачі: підзадачу генерації наборів даних, що часто зустрічаються – так званих частих предметних наборів, та підзадачу генерації правил $X \rightarrow Y$, що мають рівень достовірності не нижче заданого експертом порогового значення $\text{minconf}(X \rightarrow Y)$ [1]. Підзадача генерації частих предметних наборів даних вирішується з використанням методів, що можуть бути класифіковані за способом цієї генерації (рисунк 1).

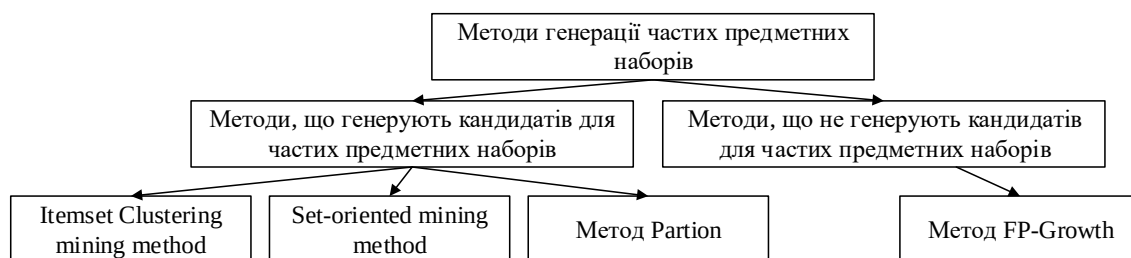


Рисунок 1 – Методи генерації частих предметних наборів

1) Методи, що генерують кандидатів для частих предметних наборів.

Set-oriented mining method – наперший запропонований метод генерації частих предметних наборів, серед яких можна здійснювати пошук АП при розробці ПЗ. Перевагами даного методу є його простота для розуміння та можливість застосування до великих БД. Серед недоліків можна виділити те, що даний метод потребує багато часу,

місця та пам'яті комп'ютера для процесу генерації можливих частих кандидатів, а також необхідне багаторазове сканування БД [2].

Метод Partition дозволяє здійснювати пошук асоціативних правил у великих БД, що містять інформацію про розробку ПЗ. Особливістю даного методу є розподіл БД на декілька частин, кожна з яких обробляється окремо. Серед переваг можна виділити швидкий пошук у великих БД та лише два сканування БД для генерації частих предметних наборів. Недоліки: виконання даного методу потрібно здійснювати на комп'ютері з великою оперативної пам'яттю, недосконалий підхід поділу БД на частини на першому етапі [3].

В методі Itemset Clustering mining method генеруються потенційні максимальні часті предметні набори, для чого використовуються методи кластеризації: на основі класів еквівалентності або maximal Hypergraph Clique. Для генерації кінцевих частих предметних наборів, серед яких можна здійснювати пошук АП при розробці ПЗ, використовуються методи проходження по графу: з низу до верху та гібридний (з низу до верху та зверху до низу). Переваги методу: використовується мало оперативної пам'яті, не потрібно будувати складну хеш-структуру для генерації частих предметних наборів, відбувається лише одне сканування БД. Серед недоліків виділяють необхідність у здійсненні вибору параметрів для алгоритму кластеризації [4].

2) Методи, що не виконують генерація кандидатів перед пошуком частих предметних наборів

Першим етапом реалізації методу FP-Growth є процес перетворення БД в деревовидну структуру, що називається FP-дерево під час чого підраховується значення підтримки для кожного елемента. На другому етапі здійснюється добування частих предметних наборів із FP-дерева, серед яких буде здійснюватися пошук АП при розробці ПЗ. Перевагами даного методу є те, що розмір FP-дерева досить малий, що дозволяє уникнути затратної процедури генерації кандидатів, швидкість пошуку частих предметних наборів вища ніж в попередніх методах. До недоліків відносять не можливість побудувати FP-дерево, що матиме розмір більший ніж основна пам'ять комп'ютера [5].

Отже, в результаті проведеного аналізу методів генерації частих предметних наборів, що можуть бути використані для пошуку асоціативних правил при розробці програмного забезпечення, було з'ясовано, що варто застосовувати метод FP – Growth, оскільки він відповідає таким вимогам: дозволяє обробляти потужні БД; швидкість генерації частих предметних наборів досить висока.

Список використаних джерел:

- 1.Zayko T.A. Association rules in data mining / T.A. Zayko, A.A. Oliinyk // Herald of the National University "KhPI". Subject issue: Information science and Modeling. – Kharkov: NTU "KhPI". – 2013. – № 39 (1012). – p. 82-96.
- 2.Swami A. Mining Associations between Sets of Items in Massive Databases / A. Swami, R. Agrawal, T. Imielinski // Proc. of the Intel Conference on Management of Data. – Washington. – 1993. – p. 134-141.
- 3.Savasere A. An Efficient Algorithm for Mining Association Rules in Large Databases / A. Savasere, E. Omiecinski, Shamkant B. Navathe // VLDB '95 Proceedings of the 21th International Conference on Very Large Data Bases – San Francisco. – 1995. – p. 432-444.
- 4.Zaki M. New Algorithms for Fast Discovery of Association Rules / M. J Zaki // Proceedings of the Third International Conference on Knowledge Discovery and DM. – New York. – 1997. – p. 283-286.
- 5.Han J. Mining frequent patterns without candidate generation/J. Han, J. Pei // Proceedings of the 2000 ACM SIGMOD international conference on Management of data. – New York. – 2000. – №2. – p. 1-12.

УДОСКОНАЛЕННЯ АЛГОРИТМУ Z-БУФЕРИЗАЦІЇ*Савчук Тамара, Чернобай Олексій*

Вінницький національний технічний університет

Анотація

У доповіді запропоновано удосконалення алгоритму z-буферизації з використанням ієрархічного розбиття полігона по середній точці та порівняння значень вершин та середньої точки полігона зі значеннями z-буфера, що забезпечує зменшення кількості порівнянь z-координат, і як наслідок, зменшення часу виконання рендерингу тривимірного зображення. Перевагою даного удосконалення є можливість регулювання швидкості роботи z-буферизації шляхом зменшення або збільшення кількості ітерацій розбиття полігона.

Abstract

The report proposes an improvement of the z-buffering algorithm using the hierarchical breakdown of the polygon along the midpoint and compares the values of the vertices and the mean point of the polygon with z-buffer values, which reduces the quantity of z-coordinates comparisons, and as a consequence, reduces the rendering time of the three-dimensional image. The advantage of this improvement is the ability to control the speed of z-buffering by reducing or increasing the quantity of iterations of the polygon breakdown.

Алгоритм, що використовує z-буфер - це один з найпростіших алгоритмів видалення невидимих поверхонь у просторі зображення [1]. Ідея z-буфера є простим узагальненням ідеї про буфер кадру, що використовується для запам'ятовування координати z чи глибини кожного видимого пікселя в просторі зображення. В процесі роботи алгоритму глибина чи значення z кожного нового пікселя, який потрібно занести в буфер кадру, порівнюється з глибиною того пікселя, який вже занесений в z-буфер. Якщо це порівняння показує, що новий піксель розташований попереду пікселя, що знаходиться в буфері кадру, то новий піксель заноситься в цей буфер і, крім того, проводиться коригування z-буфера новим значенням z. Якщо ж порівняння дає протилежний результат, то ніяких дій не проводиться.

Алгоритм z-буферизації практично не має недоліків, якщо реалізується апаратно. Програмно ж існують інші методи, здатні конкурувати з ним: Z-сортування («алгоритм художника») і двійкове розбиття простору (BSP). Основний недолік z-буферизації полягає в споживанні великого обсягу пам'яті: в роботі використовується так званий буфер глибини або Z-буфер [2].

Існуючі рішення по удосконаленню z-буферизації можна поділити на такі, що покращують швидкість роботи алгоритму, і такі, що зменшують витрати пам'яті.

До рішень, покращуючих швидкість роботи алгоритму, відносять такі:

- використання половини розрядності z-буфера для уникнення щокadroвого очищення даних [2];
 - попереднє сортування полігонів за дальністю [2];
 - рекурсивне розбиття об'єктного простору та простору зображення на тайли (зазвичай 8x8) та порівняння даних z-буфера з середнім значенням глибини тайлу (ієрархічний z-буфер) [3];
 - використання перехідної когерентності (застосовується у анімації тривимірних зображень) [3];
 - обчислення потенційно видимих поверхонь (PVS) за даними розміщення та повороту камери та полігонів [3];
 - використання z-піраміди (декількох буферів з різними рівнями точності) [3].
- Рішення, які зменшують витрати пам'яті:

- використання z-буфера з фіксованою точністю [1];
- зменшення розміру z-буфера та розбиття простору зображення на ділянки розміру z-буфера [1];
- стиснення без втрат та відновлення z-буфера для економії пропускну можливості оперативної пам'яті [2].

Більшість вищезначених рішень сумісні між собою і можуть застосовуватися разом. Узагальненням багатьох рішень є ієрархічний z-буфер. Його використання дозволяє зменшити розмір z-буфера до розміру тайлу (зазвичай 8×8), а також зменшити кількість порівнянь z-значень полігона з даними z-буфера. При цьому витрачається додаткова пам'ять на зберігання даних z-піраміди (багатошарового z-буфера з різними рівнями точності) та ієрархічно поділеного об'єктного простору (причому збереження даних об'єктного простору витрачає на 33,3% більше пам'яті, ніж збереження даних простору зображення), з чого можна зробити висновок, що витрати пам'яті в даному рішенні набагато вищі за допустимі для середньостатистичних відеокарт [3]. Тому необхідно розробити рішення, яке б прискорювало роботу алгоритму z-буферизації, але не витрачало великих об'ємів відеопам'яті.

З метою усунення означених недоліків доцільно в алгоритмі z-буферизації передбачити розбиття полігонів. Такий підхід необхідно реалізувати з врахуванням когерентності у просторі зображення, що базується на припущенні, що однократне обчислення загальної z-глибини певного елемента (в даному випадку, полігона) дозволить визначити видимість об'єкта, який покриває групу пікселів на екрані [3]. Розбиття полігонів може призводити до більших витрат обсягів пам'яті, але використання когерентності у просторі зображення дозволить мінімізувати ці витрати. Об'єм витрат пам'яті також залежить від способу розбиття полігонів. Їх можна розбивати на тайли [3] або через обчислення середньої точки полігона та його розбиття по ній. Необхідно, щоб кількість отримуваних полігонів після розбиття була завжди однаковою. Розглянемо можливі ситуації розбиття полігона, що представлені на рисунку 1:

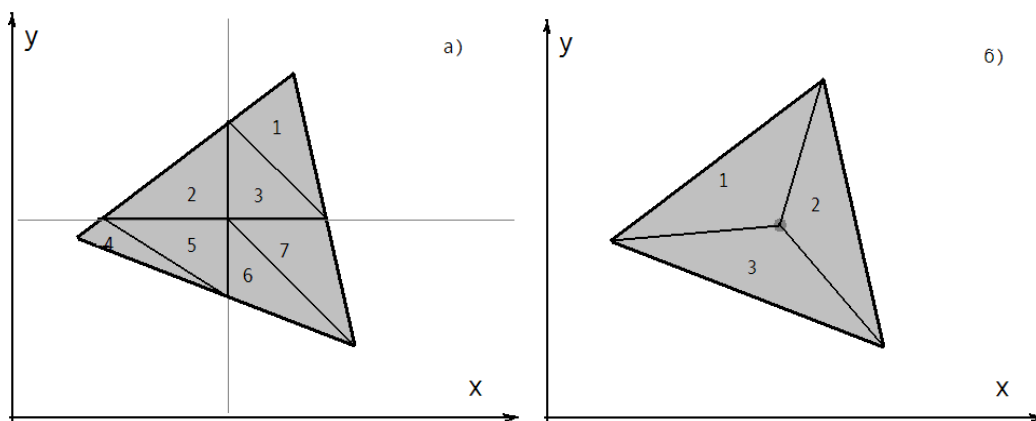


Рисунок 1 – Порівняння методів розбиття полігона тайлами (а) та середньою точкою (б)

Як видно, другий метод є більш прийнятним, оскільки при кожному розбитті отримується завжди 3 полігона. Для реалізації даного метода необхідна структура даних, яка б забезпечувала зберігання дочірніх полігонів протягом визначення видимості обчислюваного полігона. Отже, алгоритм працюватиме наступним чином:

- 1) обчислюється середня точка приведенного до екранних координат полігона за координатами його вершин;
- 2) z-значення вершин та середньої точки порівнюються з відповідними z-значеннями буфера глибини (z-буфера);

- 3) якщо всі z-значення вершин та середньої точки більші за z-значення буфера глибини – полігон вважається невидимим, і алгоритм починає обробку наступного полігона. Якщо всі z-значення менші за відповідні значення буфера глибини – полігон вважається повністю видимим і рендериться на екрані, після чого алгоритм починає обробку наступного полігона. Інакше – перехід до етапу 4;
- 4) у спеціальну структуру даних записуються 3 нових полігона.
Перехід до етапу 1.

Даний алгоритм може спрацювати неточно, якщо край більш близького полігона або зазір між більш дальніми полігонами не буде співпадати з вершинами та середньою точкою обчислюваного полігона. В такому випадку необхідно проводити більше однієї ітерації розбиття полігона перед першим порівнянням його z-значень з відповідними значеннями буфера глибини. Також необхідно обмежувати кількість рекурсій для уникнення зациклювання роботи алгоритму.

Для перевірки роботи алгоритму проведемо рендеринг однієї сцени на екрані розміром 800x600 пікселів з використанням ієрархічної z-буферизації та z-буферизації з використанням розбиття полігона по середній точці (на початку роботи – 2 ітерації розбиття). Результати дослідження представлені в таблиці 1.

Таблиця 1 – Результати дослідження

Алгоритми	Кількість порівнянь z-координат	Час рендерингу, мс
Ієрархічна z-буферизація	20216	57
Z-буферизація з використанням розбиття полігона по середній точці	12635	51

Як видно із таблиці 1, кількість порівнянь z-координат та час рендерингу при виконанні z-буферизації з розбиттям полігонів зменшилась, що свідчить про ефективність даного алгоритму.

Отже, проведені дослідження показали, що z-буферизація з використанням ієрархічного розбиття полігона по середній точці та порівнянням його вершин та середньої точки зі значеннями z-буфера може забезпечити зменшення кількості порівнянь z-координат на 7581, що складає 40%, та зменшення часу виконання рендерингу тривимірного зображення на 6 мс, що складає 10%. Перевагою даного удосконалення є можливість регулювання швидкості роботи z-буферизації шляхом зменшення або збільшення кількості ітерацій розбиття полігона. Запропоноване удосконалення алгоритму z-буферизації може бути використано у мобільних додатках, які використовують тривимірну графіку.

Список використаних джерел:

1. Алгоритм, що використовує z-буфер [Електронний ресурс] – Режим доступу: <http://compgraph.tpu.ru/zbuffer.htm>
2. Z-буферизація [Електронний ресурс] – Режим доступу: <https://ru.wikipedia.org/wiki/Z-буферизация>
3. Ієрархічний z-буфер [Електронний ресурс] – Режим доступу: <https://www.ixbt.com/video/hierar-z.html>

КОЛОРИЗАЦІЯ ЧОРНО-БІЛОГО ЗОБРАЖЕННЯ З ВИКОРИСТАННЯМ ЗГОРТКОВОЇ НЕЙРОННОЇ МЕРЕЖІ

Павлович Роман, Арсенюк Ігор

Вінницький національний технічний університет

Анотація

У статті розглянуто типову архітектуру згорткової нейронної мережі, наведено переваги її використання в задачах пов'язаних з розпізнаванням образів. Запропоновано підхід до розфарбування чорно-білого зображення з використанням згорткової нейронної мережі.

Abstract

The article deals with the typical architecture of the convolutional neural network, the advantages of their use in problems associated with pattern recognition are presented. The approach to color black-and-white image using a convolutional neural network is proposed.

Вступ

Сьогодні фактично весь світ взяв стрімкий курс на освоєння штучного інтелекту та використання його під час розв'язання різноманітних, погано формалізованих, задач. Однією з таких задач є задача обробки зображень [1 – 5] зокрема колоризація чорно-білих фото. Очевидно, що це досить складна задача, проте наукові відкриття в галузі штучного інтелекту дають нам змогу її розв'язати.

Результати дослідження

Для реалізації модулю, що буде колоризувати чорно-білі зображення було обрано модель згорткової нейронної мережі (ЗНМ), оскільки цей вид нейронних мереж найбільше підходить для задач, що потребують розпізнавання зображень, у той час, як, наприклад, традиційні моделі багатосарового перцептрону (БШП) успішно застосовувалися для розпізнавання зображень, через повну з'єднаність між вузлами, але вони потерпають від проблеми великої розмірності, і, отже, не дуже добре масштабуються на зображення вищих розмірностей.

На противагу БШП, ЗНМ мають такі характерні ознаки:

- тривимірні ємності нейронів. Шари ЗНМ мають нейрони, впорядковані у трьох вимірах: ширина, висота та глибина;
- локальна з'єднаність: відповідно до концепції рецептивних полів, ЗНМ використовують просторову локальність шляхом застосування схеми локальної з'єднаності між нейронами сусідніх шарів;
- спільні ваги. У ЗНМ кожен фільтр повторюється на всьому зоровому полі.

Разом ці властивості дозволяють ЗНМ досягати кращого узагальнення на задачах бачення. Спільне використання ваг різко зменшує кількість вільних параметрів, яких вчиться мережа, знижуючи, таким чином, вимоги до пам'яті для роботи мережі та уможливаючи тренування більших, потужніших мереж [6].

У машинному навчанні згорткова нейронна мережа (Convolutional Neural Network, CNN) – це такий тип штучної нейронної мережі прямого поширення, в якому схема з'єднання її нейронів заснована на організації зорової кори тварин, окремі нейрони якої впорядковано таким чином, що вони реагують на області, які покривають зорове поле, частково перекриваючись [6].

Ідея згорткових нейронних мереж полягає в чергуванні згорткових шарів (Convolutional), субдискретизуючих шарів (Pooling) і повнозв'язних шарів (Fully connected) на виході. На рисунку 1 наведено типову архітектуру згорткової нейронної

мережі [7].

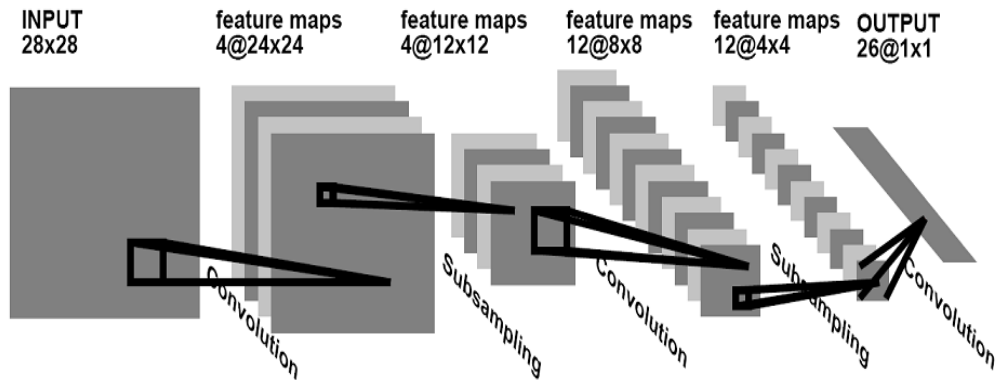


Рисунок 1 – Типова архітектура згорткової нейронної мережі

Чорно-білі зображення можна представити у вигляді сітки пікселів. Кожен піксель характеризується певним значенням яскравості, що лежить у діапазоні від 0 (чорний колір) до 255 (білий). Кольорові зображення складаються з трьох шарів: червоного, зеленого і синього. Як відомо, нейромережа встановлює взаємозв'язок між вхідним і вихідним значеннями. У нашому випадку нейромережа повинна знайти спільні риси між чорно-білими і кольоровими зображеннями. Тобто, слід відшукати властивості, за якими можна співставити значення з чорно-білої сітки зі значеннями з трьох кольорових каналів.

Спочатку пропонується скористатися алгоритмом зміни кольірних каналів з RGB на Lab (тут L означає світлість (lightness), а та b – декартові координати, що визначають положення кольору в діапазоні, відповідно, від зеленого до червоного і від синього до жовтого). Зображення у просторі Lab на рисунку 2 містить один шар градацій сірого, а три кольорових прошарки запаковані у два. Тому ми можемо використовувати в остаточному зображенні вихідний чорно-білий варіант. Залишилося обчислити ще два канали.

$$f \left(\begin{matrix} L \\ \begin{pmatrix} 93 & 92 & 83 & 77 & 77 \\ 92 & 77 & 77 & 77 & 92 \\ 92 & 77 & 83 & 77 & 92 \\ 77 & 77 & 77 & 92 & 92 \\ 77 & 77 & 92 & 92 & 92 \end{pmatrix} \end{matrix} \right) = \begin{matrix} a \\ \begin{pmatrix} 99 & 99 & 99 & 52 & 52 \\ 99 & 52 & 52 & 34 & 20 \\ 99 & 52 & 52 & 20 & 83 \\ 52 & 52 & 20 & 83 & 83 \\ 83 & 83 & 83 & 83 & 83 \end{pmatrix} \end{matrix} \begin{matrix} b \\ \begin{pmatrix} 88 & 88 & 60 & 52 & 71 \\ 88 & 40 & 52 & 52 & 71 \\ 40 & 52 & 52 & 20 & 71 \\ 40 & 52 & 20 & 83 & 83 \\ 52 & 20 & 83 & 83 & 83 \end{pmatrix} \end{matrix}$$

0 to 100 -128 to 128 -128 to 128

Рисунок 2 – Зображення в просторі Lab

Для отримання двох шарів з одного прошарку, скористаємося згортковими фільтрами. Фільтри визначають, що ми побачимо на картинці. Вони можуть підкреслювати або приховувати якусь частину зображення, щоб наше око отримало потрібну інформацію. Нейромережа теж може за допомогою фільтра створити нове зображення або звести кілька фільтрів в одну картинку.

У ЗНМ кожен фільтр автоматично підлаштовується, щоб легше було отримати потрібні вихідні дані [7]. Таким чином, ми накладемо сотні фільтрів, а потім зводимо їх воедино та отримуємо шари а та b.

Нейромережа діє за принципом проб і помилок. Спочатку вона випадковим чином призначить колір кожного пікселя, а потім по кожному пікселю обчислить помилки та скоригує фільтри, щоб у наступній спробі поліпшити результати. Загальна формула

визначення помилки матиме вигляд

$$E_p = \frac{1}{2} \sum_j (t_{pj} - y_{pj})^2,$$

де E_p – величина функції помилки для образу p ; t_{pj} – бажаний вихід нейрона j для образу p ; y_{pj} – активований вихід нейрона j для образу p [8].

Нейромережа підлаштовує свої фільтри, відштовхуючись від результатів з найбільшими значеннями помилок. У нашому випадку нейромережа вирішуватиме, чи потрібно розфарбовувати чи ні, і як розташувати на зображенні різні об'єкти. Спочатку вона фарбуватиме усі об'єкти у коричневий колір, оскільки саме цей колір найбільше схожий на всі інші кольори, і з ним, при його використанні, будуть найменші помилки [7].

Головна ідея нашої нейромережі полягає в тому, що вона шукатиме характеристики, які зв'язують чорно-білі зображення з їх кольоровими версіями. Спочатку варто шукати прості характерні структури (діагональні лінії, тільки чорні пікселі тощо), а потім слід зафарбовувати ці характерні структури.

Список використаних джерел:

1. Майданюк В. П. Поліпшення якості зображень. / В. П. Майданюк, І. Р. Арсенюк. // Оптико-електронні інформаційно-енергетичні технології. – 2015. – N 2 (30). – С. 19 – 32.
2. Арсенюк І. Р. Застосування апарату нечіткої логіки для оцінки якості графічних растрових зображень. / І. Р. Арсенюк, О. В. Сілагін, С. О. Кукунін // Матеріали IX Міжнародної науково-практичної конференції “Інтернет - Освіта - Наука” (ІОН-2014). – Вінниця: УНІВЕРСУМ – Вінниця, 2014. – С. 223 – 225.
3. Арсенюк І. Р. Оцінювання якості графічних зображень [Електронний ресурс] / І. Р. Арсенюк, О. В. Сілагін, О. С. Радченко // Тези доповідей XLV науково – технічної конференції ВНТУ, факультет інформаційних технологій та комп'ютерної інженерії. – Вінниця: ВНТУ. – 2016. – Режим доступу <http://conferences.vntu.edu.ua/index.php/all-fitki/all-fitki-2016/paper/view/1024/637>.
4. Майданюк В. П. Поліпшення якості зображень. / В. П. Майданюк, І. Р. Арсенюк. // Оптико-електронні інформаційно-енергетичні технології. – 2015. – N 2 (30). – С. 19 – 32.
5. Яровий А. А. Інтелектуальна система цифрової корекції та підвищення якості растрових зображень. / [Електронний ресурс] / А. А. Яровий, І. Р. Арсенюк, Р. А. Василічишин // Матеріали сьомої міжнародної науково-технічної конференції "Моделювання і комп'ютерна графіка". – 2017. – Режим доступу <http://ir.lib.vntu.edu.ua/bitstream/handle/123456789/19129/яровдон202017.pdf?sequence=1&isAllowed=y>
6. Цмоць І. Г. Паралельні алгоритми та НВІС-структури для медіанної фільтрації зображень в реальному часі / І. Г. Цмоць, І. В. Ігнатєв, А. Р. Боднар // Збірник наукових праць. Інститут проблем моделювання в енергетиці ім. Г. Є. Пухова. – Київ. – 2016
7. Раскрашиваем чёрно-белую фотографию с помощью нейросети из 100 строк кода/ [Електронний ресурс] – Режим доступу <https://habrahabr.ru/company/nixsolutions/blog/342388/>
8. Сверточная нейронная сеть, часть 2: обучение алгоритмом обратного распространения ошибки / [Електронний ресурс] – Режим доступу <https://habr.com/post/348028/>

АНАЛІЗ ПІДХОДІВ ДО ВИРІШЕННЯ ПРОБЛЕМ ВІДОБРАЖЕННЯ ОБ'ЄКТНО-ОРІЄНТОВАНОЇ МОДЕЛІ В РЕЛЯЦІЙНУ СТРУКТУРУ

Савчук Тамара, Давидов Сергій

Вінницький національний технічний університет

Анотація

За результатами проведеного аналізу було виявлено основні проблеми відображення об'єктно-орієнтованої моделі в реляційну структуру та систематизовано підходи до їх вирішення.

Abstract

According to the results of the analysis, the main problems of mapping the object-oriented model to the relational structure were identified and the approaches to their solution were systematized.

Вступ

Ключовим сутностями об'єктно-орієнтованої моделі є класи, які описують атрибути об'єктів (екземплярів), і міжкласові асоціації, що визначають можливість зв'язку між конкретними екземплярами. Саме ці сутності розглядаються як ключові, оскільки реляційна база даних, в якій об'єкти будуть зберігатись, не здатна природним чином підтримувати їх поведінку. Тобто зберігаються атрибути та зв'язки, а не методи примірників і не повідомлення, якими вони обмінюються. Таким чином, актуальним є проведення аналізу підходів до вирішення проблем відображення об'єктно-орієнтованої моделі в реляційну структуру [1].

При збереженні об'єктно-орієнтованої моделі в реляційну структуру виникає конфлікт між двома рівнями системи бази даних, оскільки, незважаючи на деяку схожість концепцій об'єктно-орієнтованої і реляційної методологій, система не здатна природним для себе шляхом звертатися до бази даних [1].

Для коректного відображення об'єктно-орієнтованої моделі на ієрархічну структуру потрібно визначитись з рішенням проблем об'єктно-реляційного відображення [2]:

- 1) ідентифікація об'єктів;
- 2) збереження окремого атрибута;
- 3) збереження масивів;
- 4) збереження посилань і зв'язків між об'єктами;
- 5) відображення класу;
- 6) відображення дерева успадкування;

Однозначно ідентифікувати об'єкт в додатку і його дані в реляційній таблиці є ключовим моментом в організації роботи з об'єктно-орієнтованою моделлю даних. Розрізняються два види ідентифікаторів: Об'єктні Ідентифікатори в прикладній програмі (OID) і Унікальні Об'єктні Ідентифікатори Збережених Об'єктів у базах даних (БД) (POID). POID грає роль не тільки ключа в таблиці даного класу, але він також використовується в якості посилання на ці об'єкти з боку інших класів у відповідних таблицях. Найкращим загальновизнаним підходом ідентифікації об'єктів в реляційну структуру є організація POID у вигляді пари цілих чисел – ідентифікатора класу об'єкта і ідентифікатора примірника самого об'єкта в рамках даного класу. Даний підхід дозволяє,

окрім вирішення основної задачі, по унікальній ідентифікації об'єкта вирішувати ще одну важливу задачу – визначати клас об'єкту [3]..

Базовою концепцією у рішенні проблеми збереження окремого атрибуту є збереження атрибуту класу у стовбцях реляційних таблиць. Для збереження значень атрибутів конкретного класу необхідно забезпечити доступ до значень цих атрибутів. При інкапсуляції об'єкта існує два загальних методи доступу: прямий доступ до атрибутів та доступ за допомогою спеціальних методів. При прямому доступі для зберігання даних певного атрибута класу використовується певний стовпець реляційної таблиці, при цьому не потрібно ніяких перетворень і дані передаються безпосередніми викликами відповідних методів [4], що є важливим при збереженні окремого атрибуту з об'єктно-орієнтованої моделі у реляційну структуру.

Для вирішення проблеми збереження масивів доцільно використовувати спосіб перетворення в двійковий потік. Дане перетворення здійснюється з використанням механізму перетворення даних об'єкта в бінарний потік. Переведення в двійковий потік неможливо, якщо внутрішні дані масиву використовуються для запитів до бази даних. Рішенням для зберігання внутрішніх елементів масиву може служити утворення окремих таблиць для масивів кожного з елементарних типів. Якщо в запитах до БД не використовується навігація по конкретних елементах, цілком доцільно використовувати спосіб перетворення в двійковий потік [5] при відображенні масивів у реляційній структурі.

При відображенні об'єктних посилань і зв'язків виникають проблеми їх збереження у реляційній структурі. Сама парадигма об'єктно-орієнтованої бази даних забезпечує навігацію по внутрішній структурі об'єктів, тому перетворення у двійковий потік не підходить для збереження двікових посилань і зв'язків. Для зв'язків потрібно забезпечити двосторонню здатність до навігації. Ключовим моментом у відображенні об'єктів на реляційні таблиці є представлення посилання на будь-який об'єкт у вигляді пари цілих чисел. Таким чином, атрибут, який є односторонньою посиланням, представляється в реляційних системах управління БД (РСУБД) двома стовпчиками, в які записуються відповідні ідентифікатори потрібного об'єкту-мети. Загальним правилом для відображення зв'язків між об'єктами в реляційній базі даних є опис реляційних зовнішніх ключів (foreign key) для забезпечення цілісності даних [6].

Найпростішим способом організації відображення класів у реляційні таблиці є відображення (TABLE mapping). При цьому, атрибути одного класу зберігаються в окремій таблиці, де відсутні зайві атрибути, що не відносяться до класу, який розглядається. Іншим способом відображення класу є метод підмножини (SUBSET mapping), коли для зберігання даних певного класу в реляційній таблиці використовується тільки частина полів. Серед способів організації відображення класів у реляційній таблиці виділяють метод надмножини (SUPERSET mapping), що передбачає збереження тільки частини необхідної для даного класу інформації в окремій таблиці СУБД, тобто збереження даних класу в кількох таблицях [7].

При відображенні дерева успадкування існує проблема визначення стратегій таблиць для збереження атрибутів кожного екземпляру класу. Для вирішення означеної проблеми використовується три варіанти стратегії відображення в РСУБД ієрархії успадкування класів:

- 1) Відображення з фільтрацією, що полягає в підтримці однієї глобальної таблиці для кожної ієрархії класів. Спочатку в таблицю потрапляють всі атрибути кореневого класу, а потім для кожного нового спадкоємця в таблицю додаються специфічні для цього спадкоємця атрибути.

- 2) Горизонтальне відображення, яке розбиває глобальну таблицю ієрархії на кілька таблиць. При цьому, в кожній такій таблиці будуть знаходитися всі атрибути конкретного

класу, в тому числі і успадковані.

3) Вертикальне відображення, що відображує ієрархію спадкування найбільш природним чином. Для кожного класу визначається окрема таблиця, в якій зберігаються тільки специфічні для даного класу атрибути, а між таблицями в ієрархії визначаються зовнішні ключі, за якими в подальшому забезпечується їх зв'язок (join) для маніпулювання даними [8].

Таким чином, було виявлено основні проблеми відображення об'єктно-орієнтованої моделі в реляційну структуру та систематизовано підходи до їх вирішення.

Список використаних джерел:

1. Проблема отображения объектной модели в хранимую реляционную структуру. [Електронний ресурс]. – Режим доступу: <http://www.ict.nsc.ru/ws/YM2002/4752/>
2. Способы отображения объектов в реляционных базах данных. [Електронний ресурс]. – Режим доступу: <https://studfiles.net/preview/895257/>
3. Khoshafian S. Object Identity // Copeland G. OOPSLA Conference, 1986.
4. Khoshafian, Franklin, Carey. Storage management for persistent complex objects / Information Systems, vol.15, no.3, p. 303-320, 1990.
5. Kent W. A rigorous model of object reference, identity and existence / JOOP June, 1991.
6. Martin Rennhackkamp. Extending Relational Databases / DBMS Magazine, December 1997
7. К.В. Антипин, В.В. Рубанов. Проблемы организации объектно-ориентированного доступа к реляционным базам данных / Труды Института Системного Программирования, вып. 2. 2000 г.
8. Khoshafian, Franklin, Carey. Storage management for persistent complex objects / Information Systems, vol.15, no.3, p. 303-320, 1990.

ПІДХІД ДО АНАЛІЗУ МАРКЕТИНГОВОЇ ДІЯЛЬНОСТІ В АГРОПРОМИСЛОВОМУ КОМПЛЕКСІ

Савчук Тамара, Верховсь Дмитро

Вінницький національний технічний університет

Анотація

Запропоновано підхід до аналізу маркетингової діяльності в агропромисловому комплексі, що передбачає вибір одного з множини рішень X області Ω допустимих значень з урахуванням коефіцієнта важливості вектора локальних критеріїв, а також може бути використаний для визначення маркетингової політики агропромислового комплексу.

Abstract

The approach to the analysis of marketing activity in the agroindustrial complex is proposed, which suggests the choice of one of the plurality of solutions of the X domain Ω of admissible values, taking into account the coefficient of importance of the vector of local criteria and can be used to determine the marketing policy of the agroindustrial complex.

Вступ

Оскільки для організації оперативної роботи, менеджери агропромислових комплексів повинні аналізувати ринок, швидко реагувати на погодні умови, досліджувати попит на різні види сільськогосподарської продукції, прораховувати ризики та рентабельність прийнятих рішень та на підставі цих даних розроблять маркетингову політику, актуальною є задача використання для управління в означеній сфері інформаційних інтелектуальних технологій [1, 2].

При цьому, управлінські рішення, що приймаються менеджером на підставі аналізу під впливом факторів невизначеності, характерних для сільського господарства, що є зоною ризикового виробництва, можуть призвести до нестійкого розвитку та функціонування економіки. На сільське господарство, як і на будь-яку іншу галузь економіки, має вплив нестабільність цінової політики, коливання попиту та пропозиції, невизначеність реалізаційних цін та витрат на ресурси та інше. Одним із засобів прийняття управлінських рішень з урахуванням комплексу факторів невизначеності є побудова стохастичних моделей [3].

Задача аналізу маркетингової діяльності в агропромисловому комплексі в умовах невизначеності зводиться до вибору одного з множини рішень X області Ω допустимих значень. При цьому кожне з вибраних рішень приймається з урахуванням сукупності критеріїв, як вектора локальних критеріїв $K (k_1, k_2, \dots, k_n)$, які можуть відрізнятися коефіцієнтами важливості, поданими відповідним вектором коефіцієнтів важливості локальних критеріїв $V (v_1, v_2, \dots, v_n)$. Наприклад, для логістичного критерію, більше значення коефіцієнту важливості будуть мати дані про розташування підприємства (віддаленість), способу доставки. Кожна локальна мета прийнятого рішення визначається вектором локальних критеріїв з відповідними коефіцієнтами важливості, а сума коефіцієнтів важливості локальних критеріїв, взятих до уваги, $\sum_{l=1}^n v_l = 1, l = 1, n$.

При цьому, область Ω допустимої множини рішень X може бути розбита на дві непересічні множини: $\Omega (\Omega_x^c, \Omega_x^k)$, де Ω_x^c – область згоди, в якій якість рішення про доцільність вибору може бути покращена одночасно за всіма локальними критеріями вектору локальних критеріїв, або без зниження рівня за будь-яким з них; Ω_x^k – область компромісів, в якій поліпшення якості рішення за одним локальним критерієм призводить до погіршення якості рішення про доцільність вже обраного рішення.

Оптимальне рішення може належати тільки області компромісів в області Ω допустимих рішень, тому що область згоди рішення Ω_x^c про доцільність вибору може і має бути покращена з урахуванням коефіцієнтів важливості обраних локальних критеріїв.

Розглянемо приклад прийняття рішення менеджером про збут товару, в якому в якості вектора локальних критеріїв виступатиме $K(k_1, k_2, k_3, k_4, k_5, k_6)$, де k_1 - область, k_2 - тип підприємства, k_3 - ціна, k_4 - вид оплати, k_5 - обсяг товару, k_6 - спосіб доставки) з відповідним вектором важливості локальних критеріїв $V(v_1, v_2, v_3, v_4, v_5, v_6)$. Тоді, область згоди Ω_x^c та область компромісів Ω_x^k визначаються парами (k_i, v_i) , де i – номер k_i -го локального критерію з коефіцієнтом важливості v_i . Саме з області компромісів менеджер обирає рішення, що є доцільним. Задача вибору рішення з області Ω може бути розв'язана як задача лінійного програмування при визначеній функції локальної мети. Нехай, локальні критерії мають значення, що представлені у таблиці 1. При цьому, з урахуванням важливості локальних критеріїв, область допустимих значень Ω множини рішень X розбита на область згоди Ω_x^c та область компромісів Ω_x^k за критеріями k_1 та k_3 , як показано на рисунку 1.

Таблиця 1 – Локальні критерії вибору рішення

Область	Тип підприємства	Ціна	Доставка	Оплата	Кількість
A	Господарство	1500	Самовивіз	Безготівковий	500 т
B	Елеватор	1450	Потяг	Готівка, гривня	150 т
C	Ферма	1800	Самовивіз	Готівка, валюта	10 т
D	Порт	1400	Потяг	Безготівковий	1500 т

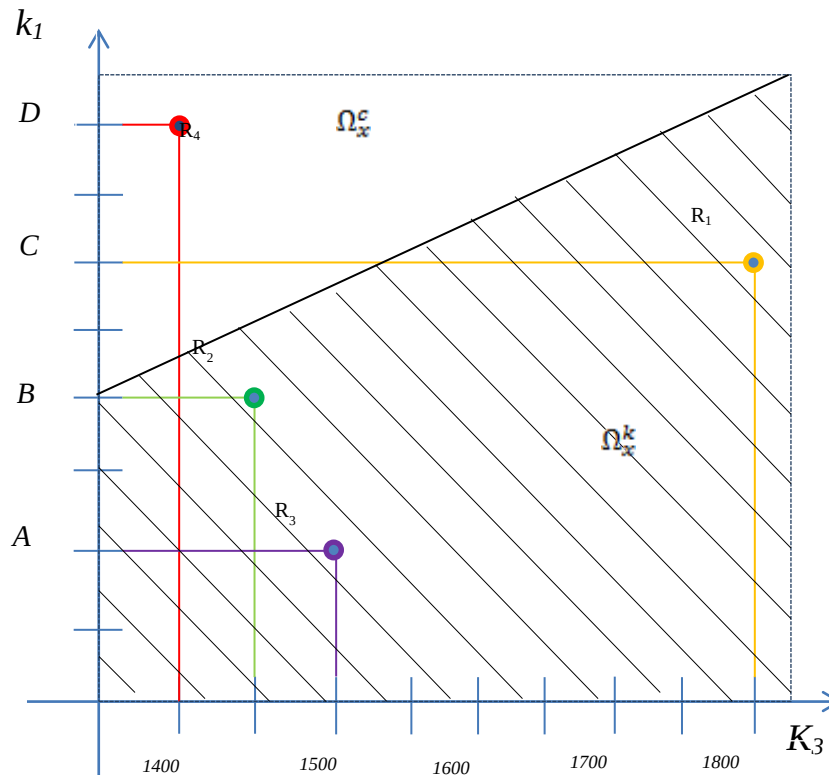


Рисунок 1 – Область допустимих значень Ω_x^c розбита за критеріями k_1 та k_3

На рисунку 1 зображена область допустимих значень Ω розбита за критеріями k_1 та k_3 , а R_1, R_2, R_3, R_4 є рішеннями, які може прийняти менеджер з урахуванням важливості локальних критеріїв V . У прикладі локальні критерії однаково важливі ($k_1 = k_3 = 0,5$). Зміна значення коефіцієнта важливості (наприклад, ціни (k_3)) приведе до переміщення точок-рішень R_1, R_2 , та R_3 в області компромісів Ω_x^k по вертикалі або по горизонталі. Рішення, що буде ближчим до визначеної менеджером границі області компромісів, і буде рекомендованим.

Таким чином, запропонований підхід до аналізу маркетингової діяльності в агропромисловому комплексі передбачає вибір одного з множини рішень X області Ω допустимих значень з урахуванням коефіцієнта важливості вектора локальних критеріїв, а також може бути використаний для визначення маркетингової політики агропромислового комплексу.

Список використаних джерел:

1. Кіреєва Е.А. – Маркетингова діяльність підприємств [Електронний ресурс] Тип доступу http://www.confcontact.com/20111222/3_kireeva.php
2. Воробйов Є.М. – Агропромисловий комплекс України [Електронний ресурс] – Тип доступу <https://www.crbc.ua/rus/tag/agropromyshlennyy-kompleks>
3. Т.О. Савчук. Використання кластерного аналізу для вирішення задач цільового маркетингу/ Т.О. Савчук, Р.А. Луженецький / Вимірювальна та обчислювальна техніка в технологічних процесах. Міжнародний науково-технічний журнал - Хмельницький, 2011. - №2, 2011. – С. 144-148. - ISSN 2219-9365

ІНТЕЛЕКТУАЛЬНИЙ МОДУЛЬ МОНІТОРИНГУ ВИКОНАННЯ ЗАВДАНЬ

Савчук Тамара, Кміть Владислав

Вінницький національний технічний університет

Анотація

У даній роботі запропоновано інтелектуальний модуль моніторингу виконання завдань з використанням web-технологій, що здатен забезпечити безкоштовну реєстрацію та користування програмним засобом та орієнтується на організації та компанії, незалежно від кількості персоналу. Програмний засіб здатний, на підставі аналізу терміну виконання завдання, надавати рекомендації щодо вчасного виконання поставлених задач.

Abstract

In this work, the intellectual module for monitoring tasks implementation using web-technologies is proposed that can provide free registration and use of the software and orientate on the organization and the company, regardless of the number of personnel. The software can, on the basis of analysis of the deadline for the task, provide advice on the timely implementation of the tasks.

На сьогоднішній час сучасному керівнику приходить контролювати виконання багатьох задач, що виконуються одночасно. Це означає необхідність моніторингу стану виконання завдання його підлеглими. Тому, актуально є задача створення автоматизованого засобу моніторингу виконання завдань, як зі стаціонарного комп'ютера так і з використанням сучасних web-технологій.

Моніторинг [1] виконання завдань дає можливість вчасно ліквідувати причини відхилення від запланованих термінів або зрив їх виконання.

Серед сучасних засобів моніторингу виконання завдань особливої уваги заслуговують: «LeaderTask», «Стаховець», «IP.Manager», «TimeTracker», «Сунтека», для яких характерним є обов'язкова наявність плати за реєстрацію та користування, відсутність функції аналізу терміну виконання завдання, а також орієнтація на потужні організації та компанії з кількістю користувачів не менше 100, оскільки при цьому створюється локальне середовище спілкування.

Таким чином, актуальною є задача створення модулю моніторингу виконання завдань з використанням web-технологій, здатного, на підставі аналізу терміну виконання завдання, надавати рекомендації виконавцям щодо вчасного представлення результатів роботи.

Виконання поставленої задачі передбачає створення програмного засобу, що виконує функцію моніторингу термінів виконання як завдання в цілому, так і окремих його етапів, означених керівником проекту. При цьому, у функції означеного інтелектуального модуля входить відправка та отримання оповіщень про завдання, які потрібно виконати у визначений період з вказанням формату представлення результатів роботи. Такі оповіщення можуть приходити на клієнтський обліковий запис Telegram [3]. При необхідності, користувач може приєднати до свого облікового запису Telegram свої облікові записи Viber та Skype. Оповіщення будуть приходити на пристрої, де встановлений і приєднаний до облікового запису клієнт Telegram, а також клієнти Viber та Skype. Отримувати оповіщення зможуть зареєстровані у Telegram користувачі.

Для розробки інтелектуального модулю використано технологію Microsoft ASP.NET Core та сервер бази даних MS SQL Server. Сервер використовує Microsoft Task Scheduler для планування відправлень оповіщень кожному користувачеві. Для очікування завершення реєстрації користувача, а саме підтвердження контактних даних користувача за допомогою Telegram, використовується SignalR сервер [4]. Для відправлення оповіщень користувачам використовуються створені служби «Гарантованого доставлення оповіщень». Всі події про виконання та помилки

відправлення оповішень записуються в базу даних. Для запобігання десинхронізації служб використовується cache сервер Redis.

Загальний алгоритм функціонування запропонованого інтелектуального модулю включатиме такі кроки:

1. Створення задачі для оповіщення вибраних користувачів.
2. Додавання задачі в чергу на опрацювання за допомогою Windows Task Scheduler.
3. Виконання запиту до служб доставки оповішень при досягненні черги Windows Task Scheduler.
4. Виконання синхронізації з Redis-сервером і відправлення оповіщення. При цьому, після завершення відправлення оповіщення, в базу даних добавляються відповідні записи про успішність відправлення та виконується повторна синхронізація з метою запобігання повторного відправлення оповіщення.
5. Завершення відправлення оповішень на пристрої користувачів через мережі Telegram, Viber, Skype.
6. Формування висновку про ступінь повноти виконання роботи в межах встановленого deadline.

Діаграма станів моніторингу виконання завдань представлена на рисунку 1.

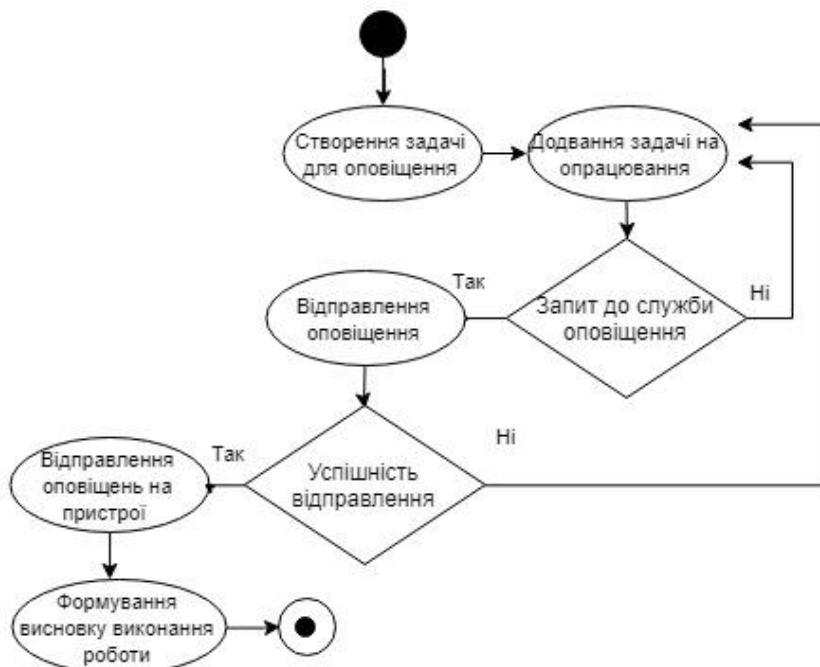


Рисунок 1 - Діаграма станів моніторингу виконання завдань

Отже, запропонований інтелектуальний модуль моніторингу виконання завдань з використанням web-технологій, забезпечує безкоштовну реєстрацію та користування програмним засобом, орієнтується на організації та компанії незалежно від кількості персоналу. Програмний засіб здатний, на підставі аналізу терміну виконання завдання, надавати рекомендації щодо вчасного виконання поставлених задач.

Список використаних джерел:

1. Monitoring in science and technology [Електронний ресурс]. – Режим доступу: – <https://en.wikipedia.org/wiki/Monitoring>
2. Моніторинг та контроль на підприємствах [Електронний ресурс]. – Режим доступу: – <https://port-u.ru/osushkcontrolya>
3. API Telegram [Електронний ресурс]. – Режим доступу: – <https://core.telegram.org/>
4. Microsoft Task Scheduler [Електронний ресурс]. – Режим доступу: – [https://msdn.microsoft.com/ru/library/windows/desktop/aa446802\(v=vs.85\).aspx](https://msdn.microsoft.com/ru/library/windows/desktop/aa446802(v=vs.85).aspx)

ВЕБ-ОРІЄНТОВАНА ПРОГРАМНА ПЛАТФОРМА ДЛЯ СТВОРЕННЯ ЕКСПЕРТНИХ СИСТЕМ «GIMET»

Яровий Андрій, Маначинський Олексій, Супрун Роман, Попова Інна

Вінницький національний технічний університет

Анотація

У ході досліджень розроблено веб-орієнтовану платформу для створення експертних систем. Здійснено експериментальні дослідження її роботи у сфері тестування програмного забезпечення. Відзначено перспективи подальшого практичного застосування даної розробки.

Abstract

The web-based platform for the creation of expert systems has been developed in the given researches. Experimental researches of its work in the field of software testing are carried out. The prospects for further practical application of this development are noted.

Вступ

На сучасному етапі розвитку інформаційних технологій все більше спостерігається чітка орієнтація на розвиток та застосування технологій штучного інтелекту в зв'язку з їх економічною ефективністю в різноманітних галузях діяльності людини. На даний момент застосовуються сотні типів прикладних програм інформаційних систем різного призначення і різної проблемної орієнтації, серед яких значне місце посідають експертні системи [1, 2, 3]. Відповідно до вищевказаного, можна зробити висновок, що експертні системи (ЕС) репрезентують стратегічно важливу, конкурентну технологію систем штучного інтелекту [4, 5].

Разом з тим, аналіз ринку програмних продуктів переконливо свідчить про чітку тенденцію до значного поширення веб-орієнтованих засобів як складних та масштабних програмних комплексів, що пов'язано із стрімким розвитком технологій, практичністю та економічною доцільністю їх застосування, ефективним застосуванням ресурсів.

Зважаючи на вищевказане, актуальною є задача використання сучасних програмних технологій у сфері розробки спеціалізованих експертних систем, зокрема, розробки веб-орієнтованої програмної платформи для створення ЕС [6], що забезпечить пришвидшення процесу створення ЕС, надійність функціонування, зручність для користувача, тощо.

Метою досліджень є підвищення ефективності роботи експертів, інженерів зі знань та програмістів при розробці спеціалізованих ЕС, а також користувачів при використанні ЕС.

Основна частина

Основними модулями веб-орієнтованої платформи для створення експертних систем «GIMET» є такі: модуль авторизації, модуль логічного введення-виведення, модуль створення та наповнення бази знань, сховище баз знань, модуль консультації, інтерфейс користувача (безпосередньо графічний інтерфейс).

Модуль авторизації відповідає за створення облікового запису користувача його особистого кабінету та можливість користування системою відповідно до отриманих повноважень (рольовий підхід).

Модуль консультації відповідає за створення консультаційної сесії між користувачем та веб-ресурсом із спеціалізованою експертною системою.

Головна сторінка веб-орієнтованої платформи для створення експертних систем відрображена на рис. 1.

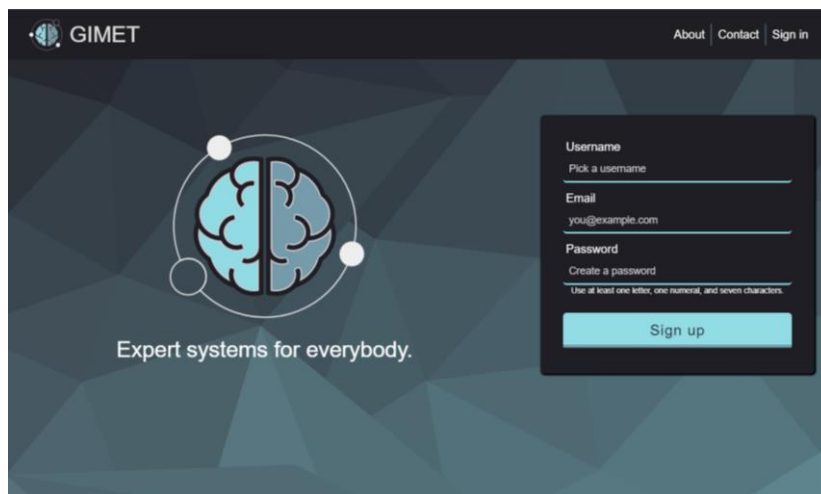


Рисунок 1 - Головна сторінка веб-орієнтованої платформи для створення експертних систем «GIMET»

В даній платформі застосовано семантичну, а також продукційну моделі подання знань. Доцільність використання семантичної мережі як моделі є можливість глибокого представлення знань у вигляді орієнтованого графа, вершини якого відповідають об'єктам предметної області, а ребра задають відношення між ними. Об'єктами, відповідно, можуть бути поняття, події, властивості, процеси. Доцільність використання продукційної моделі подання знань обґрунтовано її гнучкістю та модульністю, що є надзвичайно важливим фактором в окремих предметних областях.

База знань формується в персональному кабінеті кожного користувача та може бути модифікована за його бажанням. Приклад створення бази знань (БЗ) в кабінеті користувача зображено на рис. 2 (а,б).

а)

б)

Рисунок 2 – Приклад розробки БЗ: а) початковий екран; б) робота із наповненням БЗ

Програмну реалізацію веб-орієнтованої програмної платформи для створення ЕС виконано на мові JavaScript у середовищі розробки WebStorm 2017. Також використовувались такі додаткові технології як: Node.js, React.js, Redux та Webpack.

Веб-орієнтована платформа для створення ЕС працює на сучасних ПК, портативних та мобільних пристроях під різними ОС (Windows, MacOS, Linux, Android, iOS та ін.).

В процесі тестування розроблено три різноманітних спеціалізованих ЕС у різних предметних областях (діагностування несправностей ПК, діагностування цифрової техніки, консультування при тестуванні програмних продуктів).

Найбільш перспективним на думку авторів є розвиток даної розробки у сфері програмної інженерії, зокрема при наданні консультацій щодо процесу тестування ПЗ, що викликає інтерес та схвальні відгуки представників ІТ-компаній.

Спільно із експертами однієї із ІТ-компаній, що підтримує дану розробку, у веб-орієнтованій платформі для створення експертних систем «GIMET» реалізовано початковий варіант ЕС для консультування молодих фахівців-тестувальників із невеликим досвідом роботи із тестування програмних продуктів. Здійснено експериментальні дослідження із апробації розробки у даній специфічній предметній області, фрагмент яких наведено на рис. 3.

Рисунок 3 – Екранна форма із прикладом роботи ЕС

Експериментальні дослідження підтвердили коректність роботи ЕС та перспективність практичного застосування даної розробки. У подальших дослідженнях планується розширити впровадження моделей подання знань.

Список використаних джерел:

1. Яровий А.А. Експертні системи. Частина 2 : навчальний посібник / Яровий А.А., Арсенюк І.Р., Месюра В.І. – Вінниця : ВНТУ, 2017. – 106 с.
2. Месюра В.І. Експертні системи. Частина 1. Навчальний посібник. / Месюра В.І., Яровий А.А., Арсенюк І.Р. – Вінниця: ВНТУ, 2006. – 114 с.
3. Свідоцтво про реєстрацію авторського права на твір № 24444. Комп'ютерна програма "Оболонка експертної системи продукційного типу для підтримки процесу прийняття рішень "Decision Support Expert:Shell" / Яровий А.А., Яровий А.М., Малик Н.О. Дата реєстрації ДДІВ України 13.05.2008.
4. Дж.Ф. Люгер Искусственный интеллект: стратегии и методы решения сложных проблем. 4-е издание: Пер. с англ. / Дж.Ф. Люгер – М.: ИД «Вильямс», 2005. – 864 с.
5. Федорчук Є. Н. Програмування систем штучного інтелекту. Експертні системи. / Федорчук Є. Н. – Львів: Видавництво Львівської політехніки, 2012. – 168 с.
6. Триус Ю. В. Web-орієнтована консультаційна експертна система з методів оптимізації / Ю.В. Триус, М.О. Манько // Вісник Черкаського університету. Серія: Прикладна математика. Інформатика. – 2014. – № 18. – С. 99-114.

ДОСЛІДЖЕННЯ ТА ПОРІВНЯЛЬНИЙ АНАЛІЗ АЛГОРИТМІВ ЗНАХОДЖЕННЯ ОПТИМАЛЬНОГО ШЛЯХУ

Петришин Сергій, Решетник Вікторія

Вінницький національний технічний університет

Анотація

Розглянуто алгоритми, що знаходять найоптимальніший шлях з урахуванням особливостей прохідності місцевості. Описано методи, які умовно можна розділити на наступні класи: алгоритми пошуку найкоротшого шляху; алгоритми пошуку субоптимального шляху.

Ключові слова: пошук шляху, алгоритм Дейкстри, алгоритм A*.

Abstract

The algorithms providing one of the possible variants of a way from one point to another taking into account the peculiarities of the passability of the area are considered. Described methods that can be conventionally divided into the following classes: algorithms for finding the shortest path; algorithms for finding suboptimal paths.

Keywords: path search, Dijkstra algorithm, A* algorithm.

Вступ

При створенні симуляторів, що мають перемішувати різні типи об'єктів по великих територіях з урахуванням поточної обстановки, виникають проблеми з вибором алгоритму пошуку оптимального шляху, так як на його використання накладаються обмеження, викликані такими факторами як великий обсяг даних реальних карт місцевості; складність уявлення ландшафту та ін. Оптимальним рішенням може виявитися як пряма, так і ламана лінія.

Головна проблема задачі пошуку шляху заключається в тому, що не існує універсального алгоритму її вирішення.

Результати дослідження

Перебірні алгоритми по суті своїй є алгоритмами пошуку, як правило, пошуку оптимального рішення. При цьому рішення конструюється поступово. В цьому випадку зазвичай говорять про перебір вершин дерева варіантів [1]. Вершинами такого графа будуть проміжні або кінцеві варіанти, а ребра будуть вказувати шляхи побудови варіантів рішення.

Хвильовий алгоритм Лі належать до класу перебірних та складається з двох етапів:

- поширення хвилі;
- зворотній хід [2].

Поширення хвилі і є власне пошук в ширину, при якому клітини позначаються номером кроку методу, на якому клітина відвідується. При зворотному ході, починаючи з кінцевої вершини, йде відновлення шляху, по якому в неї потрапили шляхом включення в нього клітин з мінімальною позначкою. Особливістю алгоритму Лі є те, що відновлення починається з кінця (з початку воно часто неможливо) [3].

Граф представляє собою сукупність не пустої множини вершин і ребер (наборів пар вершин). Дві вершини на графі сусідні, якщо вони з'єднуються спільним ребром. Шлях в неорієнтованому графі представляє собою послідовність вершин $P = (v_1, v_2, \dots, v_n) \in V \times V \times \dots \times V$, таких, що v_i суміжна з v_{i+1} для $1 \leq i < n$. Такий шлях P називається шляхом довжиною n з вершини v_1 в v_n (i вказує на номер вершини шляху і не має ніякого відношення до нумерації вершин на графі) [4].

Для вирішення вказаної задачі можна використовувати алгоритм Дейкстри. Він знаходить найкоротшу відстань від однієї вершини графа до всіх інших. Алгоритм

Дейкстри придуманий нідерландським вченим Едсгер Дейкстрой в 1959 році [5].

Складність алгоритму складає $O(n^2 + m)$, де n – кількість вершин і m – кількість ребер.

Недоліком алгоритму є те, що він не завжди працює з ребрами при від'ємному значенні ребер [6].

Алгоритм Флойда-Уоршелла був опублікований Робертом Флойдом і Стівеном Уоршеллом в 1962 році. Він є легшим у реалізації програми у порівнянні з алгоритмом Дейкстри. Алгоритм динамічного програмування Флойда-Уоршелла служить для визначення найкоротших шляхів між усіма парами вершин графа. Даний алгоритм дуже простий у освоєнні, але у нього дуже низька швидкість роботи і в ньому не передбачено розрахунок ребер з негативними вагами.

Мета алгоритму - знаходження найкоротшого шляху між усіма вершинами графа [7].

Метод Флойда базується на тому факті, що в графі з позитивними вагами будь-якого неелементарного ребра (що містить більше 1 ребра), короткий шлях складається з інших найкоротших шляхів.

Дано матрицю, яка заповнюється вагами ребер для кожної з вершин. Після цього проводиться ітерація кожної вершини, де порівнюється вага ребер між вершинами А і Б, через вершину В. Найкоротшим шляхом між А і Б є мінімальне значення з цих варіантів.

Цей алгоритм більш загальний порівняно з алгоритмом Дейкстри, так як він знаходить найкоротші шляхи між будь-якими двома вершинами графа.

Перегавою алгоритму є його простота реалізації, слабкість – в складності алгоритму. Вона дорівнює $O(n^3)$, де n – кількість вершин графа [8].

Алгоритм бектрекінгу був розроблений багатьма дослідниками ще до формального опису. Метою цього алгоритму не є знаходження найкоротшого шляху, а знаходження всіх можливих варіантів шляхів від вершини А до вершини Б.

Складність алгоритму $O(n * m)$, де n – кількість вершин графа. Алгоритм ефективний тим, що всі можливі варіанти можуть бути збережені в структурах даних і легко можуть бути використані в подальших розрахунках у програмі [9].

Перебірні алгоритми по своїй суті є алгоритмами пошуку, як правило, пошуку оптимального рішення. При цьому рішення конструюється поступово. В цьому випадку звичайно говорять про перебір вершин дерева варіантів. Для прискорення перебору з поверненням обчислень завжди намагаються організувати так, щоб була можливість якомога відмінити недоречні варіанти [10].

Алгоритм пошуку A^* належить до евристичних алгоритмів пошуку. Він використовується для пошуку найкоротшого шляху між двома вершинами графу з додатніми вагами ребер. Алгоритм використовує допоміжну функцію (евристику), аби скеровувати напрям пошуку та скорочувати його тривалість [11]. Основним недоліком алгоритму A^* є потреба в пам'яті для збереження всіх відомих та досліджених вершин. Через це алгоритм A^* непридатний для багатьох задач [12].

Однією з основних проблем алгоритму A^* є те, що одержані за його допомогою шляхи не виглядають реалістичними. Ця проблема вирішується в алгоритмі Θ^* . Ключовий момент, який відрізняє ці два алгоритми, в тому, що Θ^* дозволяє в якості «предка» для кожної вершини вибрати будь-яку вершину, на відміну від A^* , де «предком» може бути тільки найближчий видимий сусід. Якщо потрібно отримати найбільш реалістичний субоптимальний шлях, рекомендується використовувати алгоритм Θ^* [13].

Висновки

Було розглянуто алгоритми, які використовуються для знаходження оптимального шляху на географічних картах, а саме: алгоритм Дейкстри, алгоритм Флойда-Уоршелла, алгоритм бектрекінгу, алгоритм A^* та алгоритм Θ^* . Також було проведено короткий

огляд перебірних алгоритмів, але вони не підходять для вирішення поставленої задачі через великі затрати пам'яті.

У загальному випадку необхідно розробляти систему алгоритмів. Так як витрати на звернення на ландшафт являються критичними, то будемо використовувати наступну комбінацію алгоритмів:

- алгоритм A * для отримання маршруту;
- видалимо точки, що лежать на одній прямій;
- застосуємо алгоритм перевірки наявності шляху по прямій.

Список використаних джерел:

1. Cook W. J. In Pursuit of the Traveling Salesman: Mathematics at the Limits of Computation/ W. J. Cook. – Princeton University Press, 2012. – 254 p.
2. Applegate D.L., Bixby R.E., Chvátal V., Cook W.J. The Traveling Salesman Problem. Princeton University Press, 2007. – 347 p.
3. Ананий Левитин, Игорь Красиков. Алгоритмы. Введение в разработку и анализ/ Левитин А., Красиков И. – Вильямс, 2006. – 576 с. – ISBN 5-8459-0987-2, 0-201-74395-7.
4. Кормен Т., Лейзерсон Ч., Ривест Р., Штайн К. Алгоритмы. Построение и анализ. Москва, Вильямс, 2005.
5. Botea A., Muller M., Schaeffer J. Near Optimal Hierarchical Path-Finding. Journal of Game Development, 2004, vol. 1, issue 1, pp. 7–28.
6. Daniel K., Nash A., Koenig S., Felner A. Theta*: Any-Angle Path Planning on Grids. Journal of Artificial Intelligence Research, 2010, vol. 39, pp. 533–579.
7. Коробицын В.В., Фролова Ю.В. Моделирование автомобильного потока на перекрестке и определение оптимальных параметров управления сигналами светофора: журнал. Выпуск №2(14), журнал «Математические структуры и моделирование» — 2004 г., — вып. 14, — с. 34—36
8. Седжвик Р. Алгоритмы на Java: учеб. пособие. Вильямс, 2012. — 575 с.
9. Сундетов р.н., есламгалиев т.н. обоснование выбора алгоритма поиска оптимального пути с расчетом показателей светофора в городской сети // естественные и математические науки в современном мире: сб. Ст. По матер. XXX междунар. Науч.-практ. Конф. № 5(29). – новосибирск: сибак, 2015.
10. Семакин, И.Г. Основы алгоритмизации и программирования: Учебник для студ. учреждений сред. проф. образования / И.Г. Семакин, А.П. Шестаков. - М.: ИЦ Академия, 2013. - 304 с.
11. Крупский, В.Н. Математическая логика и теория алгоритмов: Учебное пособие для студентов учреждений высшего проф. образования / В.Н. Крупский, В.Е. Плиско. - М.: ИЦ Академия, 2013. - 416 с.
12. Игошин, В.И. Теория алгоритмов: Учебное пособие / В.И. Игошин. - М.: ИНФРА-М, 2013. - 318 с.
13. Канцедал, С.А. Алгоритмизация и программирование : Учебное пособие / С.А. Канцедал. - М.: ИД ФОРУМ, НИЦ ИНФРА-М, 2013. - 352 с.

ОЦІНКА ОСНОВНИХ МЕТОДІВ ІНТЕЛЕКТУАЛЬНОГО АНАЛІЗУ ДАНИХ ДЛЯ ЗАДАЧІ ПІДБОРУ ПОКУПОК

Петришин Сергій, Замковий Олександр

Вінницький національний технічний університет

Анотація

Розкрито поняття «інтелектуального аналізу даних». Розглянуто алгоритм дерева прийняття рішень, алгоритм Байєса, алгоритм лінійної регресії. Досліджено переваги та недоліки алгоритмів. Обрано найдоцільніший алгоритм для розв'язання задачі інтелектуального підбору покупок.

Abstract

Disclosed the concept of data mining. The decision tree algorithm, Bayes algorithm, linear regression algorithm are considered. The advantages and disadvantages of algorithms are explored. The most suitable algorithm for the smart purchasing task is chosen.

Вступ

В наш час набирає популярність система «розумний» будинок. Одним зі складових такої системи може бути «розумний» холодильник, який може перевіряти наявність певних продуктів. Завдяки впровадженню системи інтелектуального підбору покупок, «розумний» холодильник може складати список покупок, та замовляти їх через мережу Інтернет. Завдяки цій системі власники «розумного» холодильника завжди будуть мати перелік продуктів, які звикли споживати.

Оцінка основних методів даних для задачі підбору покупок

Основними методами для інтелектуального аналізу даних для задачі підбору покупок є

- дерево прийняття рішень;
- спрощений алгоритм Баєса;
- алгоритм лінійної регресії.

Дерево прийняття рішень — використовується в галузі статистики та аналізу даних для прогнозних моделей. Структура дерева містить такі елементи: «листя» і «гілки». На ребрах («гілках») дерева прийняття рішення записані атрибути, від яких залежить цільова функція, в «листі» записані значення цільової функції, а в інших вузлах — атрибути, за якими розрізняються випадки[1]. Щоб класифікувати новий випадок, треба спуститися по дереву до листа і видати відповідне значення. Подібні дерева рішень широко використовуються в інтелектуальному аналізі даних для задачі підбору покупок. Мета полягає в тому, щоб створити модель, яка прогнозує значення цільової змінної на основі декількох змінних на вході. Кожен лист являє собою значення цільової змінної, зміненої в ході руху від кореня по листа. Кожен внутрішній вузол відповідає одній з вхідних змінних. Дерево може бути також «вивчено» поділом вихідних наборів змінних на підмножини, що засновані на тестуванні значень атрибутів. Це процес, який повторюється на кожній з отриманих підмножин. Рекурсія завершується тоді, коли підмножина в вузлі має ті ж значення цільової змінної, таким чином, воно не додає цінності для прогнозування. Процес, що йде «згори донизу», індукція дерев рішень (TDIDT), є прикладом поглинаючого «жадібного» алгоритму, і на сьогодні є найбільш поширеною стратегією дерев рішень для даних, але це не єдина можлива стратегія. В інтелектуальному аналізі даних, для розв'язання задачі підбору покупок, дерева рішень можуть бути використані як математичні та обчислювальні методи, щоб допомогти

описати, класифікувати і узагальнити набір даних, які можуть бути записані таким чином:

$$(x, Y) = (x_1, x_2, x_3 \dots x_k, Y)$$

Залежна змінна Y є цільовою змінною, яку необхідно проаналізувати, класифікувати й узагальнити. Вектор x складається з вхідних змінних x_1, x_2, x_3 тощо, які використовуються для виконання цього завдання[1].

Спрощений алгоритм Байеса є алгоритмом класифікації, на підставі теореми Байеса і використовується в прогнозуючому моделюванні. Слово «спрощений» в його назві вказує на те, що алгоритм використовує методи Байеса, але не враховує можливі залежності. Даний алгоритм вимагає меншої кількості обчислень, ніж інші алгоритми, і може бути використаним для швидкого формування моделей інтелектуального аналізу даних для виявлення відносин між вхідними і прогнозованими стовпцями, також цей алгоритм підходить для розв'язання задачі підбору покупок.

Абстрактно імовірнісна модель для класифікатора — це умовна модель

$$p(C | F_1, \dots, F_n)$$

над залежною змінною класу C з малою кількістю результатів або класів, залежна від кількох змінних $F_1, \dots, F_n$ [2]. Проблема полягає в тому, що коли кількість властивостей n , тобто кількість можливих комбінацій покупок, дуже велика або коли властивість може приймати велику кількість значень, тоді будувати таку модель на імовірнісних таблицях стає неможливо. Тому ми переформулюємо модель, щоб зробити її такою, яка легко піддається обробці.

Використовуючи теорему Баєса, запишемо

$$p(C | F_1, \dots, F_n) = p(C)p(F_1, \dots, F_n | C) / p(F_1, \dots, F_n) .$$

На практиці цікавий лише чисельник цього дробу, так як знаменник не залежить від C і значення властивостей дані, так що знаменник — константа[2]. Цей алгоритм можна використовувати для початкового дослідження даних, а потім застосувати результати для створення додаткових моделей інтелектуального аналізу з іншими алгоритмами, які вимагають більшої кількості обчислень і є більш точними, що в кінцевому рахунку приведе до розв'язання задачі підбору покупок.

Алгоритм лінійної регресії є різновидом алгоритму дерева прийняття рішень, що допомагає розрахувати лінійну зв'язок між залежною і незалежною змінною, а потім використовувати цей зв'язок при прогнозуванні, або ж підборі покупок. При виборі алгоритму лінійної регресії викликається особливий варіант алгоритму дерева прийняття рішень з параметрами, які обмежують поведінку алгоритму і вимагають використання певних типів даних на вході. Більш того, в моделі лінійної регресії для обчислення зв'язків при початковому проході використовується весь набір даних; тоді як в стандартній моделі дерева прийняття рішення дані багаторазово розбиваються на менші підмножини або дерева[3].

У ході оцінювання методів інтелектуального аналізу даних для задачі підбору покупок було розглянуто такі методи, як дерево прийняття рішень, спрощений алгоритм Баєса, алгоритм лінійної регресії. Оскільки покупки зазвичай пов'язані між собою, то для задачі підбору покупок доцільно використовувати алгоритм дерева прийняття рішень в комбінації з спрощеним алгоритмом Баєса, оскільки це забезпечить можливість перегляду значення цільової функції з додаванням нових параметрів, та зміною уже існуючих параметрів.

Список використаних джерел:

1. Дерево прийняття рішень - <http://stud.com.ua/31896/menedzhment>.
2. Левитин А. Алгоритмы. Введение в разработку и анализ. Вильямс, 2006. Р. 160.
3. Алгоритм лінійної регресії — [Електронний ресурс]. — Режим доступу: [https://msdn.microsoft.com/ru-ru/library/ms174824\(v=sql.120\).aspx](https://msdn.microsoft.com/ru-ru/library/ms174824(v=sql.120).aspx)



ОДИНАДЦЯТА МІЖНАРОДНА КОНФЕРЕНЦІЯ
ІОН - 2018
ІНТЕРНЕТ-ОСВІТА-НАУКА-2018



**СЕКЦІЯ В. КОМП'ЮТЕРНІ МЕРЕЖЕВІ
ТЕХНОЛОГІЇ**



THE ELEVENTH INTERNATIONAL
CONFERENCE
IES-2018
INTERNET-EDUCATION-SCIENCE - 2018



**SECTION B. COMPUTER NETWORK
TECHNOLOGIES**



ОДИННАДЦАТАЯ МЕЖДУНАРОДНАЯ
КОНФЕРЕНЦИЯ
ИОН-2018
ИНТЕРНЕТ– ОБРАЗОВАНИЕ – НАУКА 2018



**СЕКЦІЯ В. КОМП'ЮТЕРНІ МЕРЕЖЕВІ
ТЕХНОЛОГІЇ**



ОПТИМІЗАЦІЯ ПОТОКІВ У БАГАТОПОЛЮСНІЙ МЕРЕЖІ

Тихонова Олена

ОНАЗ ім. О.С. Попова

Анотація

Розглядається задача пошуку максимального потоку у багатополісній транспортній мережі та відповідного розподілу його складових по комунікаційних каналах. Введені поняття "триджету" та "триплету" як структурних елементів графу мережі. Узагальнений алгоритм оптимального розподілу потоків проілюстровано на прикладі повнозв'язного триполісного мережевого фракталу з шести вузлів.

Abstract

The maxflow task is considered in multi-pole transport network as well as the corresponding flows distribution over communication channels. The concepts of "triget" and "triplet" are introduced as structural elements of the network graph. A generalized algorithm of optimal flows distribution is illustrated by the case of a six-node fully connected three-pole network fractal.

Вступ

Сучасні телекомунікаційні мережі стикаються зі зростаючим попитом на послуги Інтернет. Поряд з удосконаленням телекомунікаційного обладнання і технологій, оптимізація використання наявної мережевої інфраструктури дозволяє додатково підвищити доходи постачальників телекомунікаційних послуг та доступність послуг для споживача. Зокрема, це надає можливість збільшити кількість задоволених вимог на обслуговування мережею за існуючої пропускної здатності комунікаційних каналів. Тому актуальною є задача пошуку максимального потоку у транспортній мережі, а також конкретного розподілу загального максимального потоку по транспортній інфраструктурі.

Традиційний підхід до вирішення задачі про максимальний потік передбачає існування двох виділених вузлів мережі, один з яких - джерело потоку, а інший - його кінцева точка [1]. Також відомі узагальнення задачі максимального потоку для багатополісного орієнтованого графа, наприклад графа двосторонньої структури з декількома витоками та декількома стоками [2], або для багатополісного направленного збалансованого графа [3]. В роботі [4] авторами зазначено, що загальноприйняті графові моделі не в повній мірі відображують сучасні мережеві технології; наприклад, відоме представлення зв'язку між двома мережевими вузлами направленим або неорієнтованим «ребром» мережевого графа (з фіксованою вагою у кожному напрямку) не враховує здатність гнучкої реконфігурації сучасних оптичних систем зв'язку. У зв'язку з цим, в роботі [4] була запропонована розширена постановка задачі про максимальний потік для багатополісної відкритої вільно-орієнтованої транспортної мережі, де фіксованою залишається лише загальна потужність зв'язку між кожною парою вузлів, а її співвідношення у прямому та зворотному напрямках може змінюватись в залежності від поточних потреб мережі. Метою даної роботи є побудова алгоритму оптимального розподілу потоків багатополісної мережі за критерієм максимізації загального сумарного потоку та з урахуванням вільної орієнтації каналів зв'язку.

Запропонований узагальнений алгоритм полягає в поетапному накопиченні значення максимального потоку на зростаючих логічних відстанях між всіма полюсами мережі; при подібній декомпозиції вихідного графу мережі утворюються типові структурні елементи, названі "триджет" та "триплет", для яких вже вважається відомим попередньо розроблений метод розрахунку максимального потоку.

Розрахунок максимального потоку для структурних елементів графу

Як відомо з теорії графів, вузол з трьома ребрами є мінімальним структурним «примітивом», за допомогою якого можна утворити складний неорієнтований граф довільної топології [5]. Даний примітив запропоновано визначати як "триджет", рис. 1.

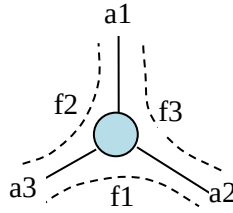


Рисунок 1 – Структурний елемент типу "триджет"

Через відкриті ребра триджету $a1$, $a2$, $a3$ циркулюють три зовнішніх потоки: $f1$, $f2$, $f3$. Повний потік триджету, за визначенням, дорівнює сумі $f_{\Sigma} = f1 + f2 + f3$. В роботі [6] обґрунтовано алгоритм розрахунку максимальної величини $f_{\Sigma \max}$ і відповідних $f1$, $f2$ та $f3$, який залежить від співвідношення ваги відкритих ребер $a1$, $a2$, $a3$ наступним чином.

1. Якщо вага жодного з відкритих ребер $a1$, $a2$, $a3$ не перевищує ваги двох інших (тобто виконується правило трикутника):

$$\begin{aligned} f_{\Sigma \max} &= (a1 + a2 + a3) / 2, \\ f1 &= (a2 + a3 - a1) / 2, \\ f2 &= (a1 + a3 - a2) / 2, \\ f3 &= (a1 + a2 - a3) / 2. \end{aligned} \quad (1)$$

2. Якщо правило трикутника не виконується, максимальний потік $f_{\Sigma \max}$ дорівнює:

$$f_{\Sigma \max} = (a1 + a2 + a3) - \max(a1, a2, a3), \quad (2)$$

а складові максимального потоку проходять по двом ребрам мінімальної сумарної ємності, які відіграють роль мінімального розрізу на триджеті.

Визначений вище базовий структурний елемент триджет на рис.1 застосуємо для аналізу потоків у відкритому зваженому вільно-орієнтованому графі більш складної топології. Структурний фрейм наступного (другого) рівня, який запропоновано визначати як "триплет", побудуємо шляхом об'єднання трьох триджетів, рис. 2.

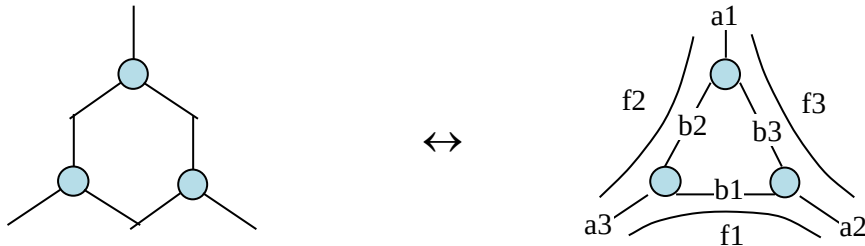


Рисунок 2 – Структурний елемент типу "триплет"

Алгоритм пошуку максимального потоку для триплету полягає у наступному.

1. Якщо жодне з внутрішніх ребер триплету $b1$, $b2$, $b3$ не є вузьким місцем для відповідних потоків $f1$, $f2$ та $f3$, то максимальний потік та його складові розраховується як у триджеті, тобто за формулами (1), (2).

2. Якщо усі внутрішні ребра триплету є вузькими місцями, тобто обмежують відповідні потоки $f1$, $f2$ та $f3$, то максимальний потік дорівнює мінімальному "внутрішньому" перетину $f_{\Sigma \max} = b1 + b2 + b3$, а складові максимального потоку дорівнюватимуть вагам обмежуючих ребер $f1 = b1$; $f2 = b2$; $f3 = b3$.

3. У випадках, якщо одне або два внутрішні ребра з ($b1$, $b2$, $b3$) є вузьким місцем для відповідних потоків $f1$, $f2$ та $f3$ (рис. 3):

- дані потоки приймаються рівними вагам обмежуючих внутрішніх ребер триплету;

- обчислюється остаточної граф триплету;

3.1) якщо триплет містить одне обмежуюче внутрішнє ребро, наприклад b_1 (рис. 3-а), максимальний потік становить $f_{\Sigma \max} = b_1 + \min\{a_1, \min(b_2, a_3 - b_1) + \min(b_3, a_2 - b_1)\}$. При цьому потоки f_1, f_2 можуть розподілятися довільним чином в межах не перевищення пропускної здатності ребер графу;

3.2) якщо триплет містить два обмежуючих внутрішніх ребра, наприклад b_1 та b_2 (рис. 3-б), очевидно що $f_3 = \min\{a_1 - b_2, b_3, a_2 - b_1\}$, а максимальний потік становить $f_{\Sigma \max} = b_1 + b_2 + \min\{a_1 - b_2, b_3, a_2 - b_1\}$.

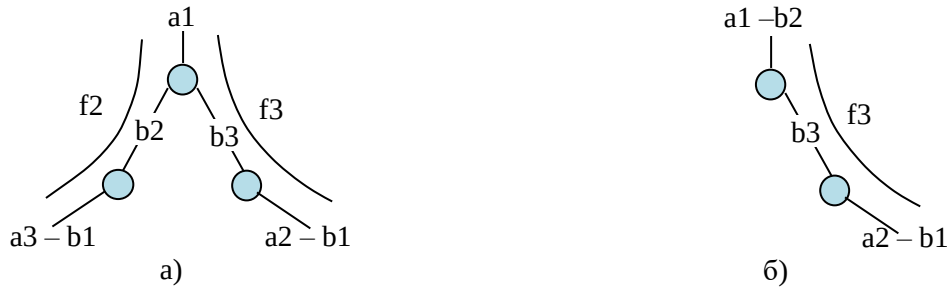


Рисунок 3 – Остаточний граф триплету: а) з двома обмежуючими ребрами; б) з одним обмежуючим ребром

Запропонований алгоритм розраховує максимальний потік триджету та його складові з точністю до 3-крокових потоків. Застосовуючи принцип масштабування триджетів і триплетів, можна конструювати все більш складні топології графу. Структурний елемент наступного (третього) рівня будемо називати "фракталом". В даній роботі створена комп'ютерна програма на мові Python, яка реалізує узагальнений алгоритм пошуку максимального потоку для повнозв'язного триполюсного мережевого фракталу з шести вузлів.

Висновки

На основі розширеної постановки задачі про максимальний потік для багатопольової відкритої неорієнтованої транспортної мережі, розроблено узагальнений алгоритм пошуку максимального потоку, який полягає у декомпозиції вихідного графу мережі на спрощені типові структурні елементи. Визначено структурні елементи "триджет" та "триплет", для яких розроблено алгоритми розрахунку максимального потоку. Створено комп'ютерну програму, яка реалізує узагальнений алгоритм для повнозв'язного триполюсного мережевого фракталу з шести вузлів.

Список використаних джерел:

1. Ford L.R. Flows in Networks / L.R.Ford, D.R.Fulkerson // A report prepared for United States air force project RAND. – 1962. – 332 p.
2. Bela Bollobas. Modern Graph Theory. – New York: Springer Science & Business Media, 1998. – 394 p.
3. Christian Fremuth-Paeger. Balanced Network Flows. I. A Unifying Framework for Design and Analysis of Matching Algorithms / Christian Fremuth-Paeger, Dieter Jungnickel // Networks. – 1999. – vol.3, issue 1. – p.1-28.
4. Tykhonova O.V. The maxflow problem statement for multi-pole software defined network / O.V.Tykhonova, V.I.Tikhonov // матеріали XVII міжнародної НТК ВОТТІ-17-2017 (08-13 червня 2017 р.). – Одеса: ОНАЗ ім. О.С.Попова, 2017. – с. 161-164.
5. Vasudev C. Graph Theory with Applications. – New Age International, 2006. – 466 p.
6. Тихонова Е.В. Обобщенный алгоритм расчета максимального потока для многополюсной транспортной сети: матеріали 72-ї НТК професорсько-викладацького складу, науковців, аспірантів та студентів (Одеса, 13-15 грудня 2017 р.). – О.: ОНАЗ ім. О.С.Попова, 2017. – с. 69-72.

АНАЛІЗ МЕТОДІВ ЗАХИСТУ ПЕРЕДАВАНОЇ ІНФОРМАЦІЇ В КАНАЛІ ЗВ'ЯЗКУ

Кільдишев Віталій, Тіхонов Андрій

ОНАЗ ім. О.С. Попова

Анотація

В роботі розглядаються питання захисту каналів телекомунікаційного зв'язку від природних завад і штучних загроз, а також базові принципи захисту каналів зв'язку. Визначено деякі умови для побудови надійного алгоритму шифрування даних. Розглянуто залежність між фізичною швидкістю передачі символів та швидкістю передачі корисної інформації при збільшенні надмірності шифрування. Проаналізовано особливості передачі і шифрування даних у каналах з квантовими ефектами.

Abstract

This paper is focused on the issues of telecommunication channels protection from the natural influences and artificial threats, as well as basic principles of communication channels protection. Some conditions for constructing a reliable data encryption algorithm are defined. The dependence is considered between the physical rate of symbols transmission and the speed of the useful information transfer while increase of encryption redundancy. The features are analyzed of data transmission and encryption in channels with quantum effects.

Вступ

Захист каналів зв'язку займає важливе місце в загальній системі інформаційної безпеки. У даній роботі розглядається поняття «канал зв'язку» як телекомунікаційної підсистеми, утвореної двома цифровими приймачами, з'єднаними фізичною лінією зв'язку, на яку можуть впливати різного роду природні (ненавмисні) і штучні (навмисні) перешкоди, а також може мати місце пасивний та/або активний несанкціонований доступ. У каналі зв'язку існує безліч різних типів загроз, і в залежності від кожного з них розробляються специфічні методи боротьби з ними [1–4].

Принципи захисту інформації в каналі зв'язку

Основною одиницею прийому-передачі даних на каналному рівні є символи або блоки символів. Найпростішим символом передачі даних є біт. Сучасні телекомунікаційні системи використовують більші символи, що містять від 2 до 64 біт і більше. Головна мета боротьби з природними перешкодами в каналі зв'язку - це підвищення достовірності інформації що передається, тобто обмеження ймовірності прийому помилкового символу. Для цього застосовують т.зв. надлишкове кодування, при якому на передавальній стороні змістовні блоки символів відображаються в розширені блоки передачі, аналіз яких на приймальній стороні каналу дозволяє виявити або виправити помилки певних типів.

Для захисту інформації в каналі зв'язку від несанкціонованого доступу типу «прослуховування» використовують різні методи криптографії (шифрування даних): заміна (підстановка) символів, перестановка, аналітичні перетворення шифрованих даних та інші. Поширений метод шифрування - це заміна переданих символів на символи з того ж самого алфавіту, здійснювана по секретним таблицям шифрування. На основі цього методу можна побудувати алгоритм, який в принципі не піддається дешифруванню при відсутності таблиці шифрування. Для цього достатньо, щоб множина символів підстановки утворювала випадкову послідовність довжиною не менше переданого повідомлення (з однаковою ймовірністю всіх символів підстановки і незалежністю між будь-якою парою символів підстановки). Обмеження такого методу шифрування

обумовлені технічними можливостями створення, обміну та зберігання таблиць шифрування великих розмірів.

Підвищення швидкості передачі і зменшення енергії на одиницю інформації в оптичних каналах обумовлює появу квантових ефектів, пов'язаних з нечіткою ідентифікацією прийнятих символів. З точки зору детектора сигналу, один і той символ (наприклад, один біт), що генерується на передавальній стороні каналу, може перебувати в двох станах (нуль і одиниця). При цьому відносні частоти появи нулів і одиниць наближаються до можливостям їх появи. Однак при однаковій фізичній швидкості передавання символів, збільшення надмірності переданих блоків символів призводить до зниження кількості корисної інформації. При цьому зменшується ймовірність помилок; це, в свою чергу, дозволяє збільшити фізичну швидкість передачі. В результаті взаємного впливу цих факторів може бути досягнуто загальне підвищення ефективності передавання корисної інформації.

Властивості каналу зв'язку з квантовими ефектами визначаються матрицею ймовірностей $P_{i,k} = p(i,k)$, де i - значення переданого символу, j - значення прийнятого символу. Ця матриця є чутливою до змін фізичних властивостей каналу, наприклад, при несанкціонованому доступі до каналу матриця зміниться в тій чи іншій мірі. Дана матриця є унікальною характеристикою каналу зв'язку, яка може бути досліджена в метрологічному експерименті, а далі використана для детектування сигналів та виявлення несанкціонованого доступу. Квантові методи у криптографії поки що знаходяться у стадії активного розвитку. Однією з основних проблем у квантовій криптографії є підвищення швидкості передачі даних на великі відстані.

Висновки

В каналах зв'язку мають місце як природні, так і штучні перешкоди і впливи. Для боротьби з природними завадами використовують методи завадостійкого кодування з детектуванням та виправленням помилок. Боротьба зі штучними впливами здійснюється різними методами, зокрема шифруванням даних, а також застосуванням квантових принципів, чутливих до несанкціонованого доступу. Квантові методи у криптографії знаходяться у стадії активного розвитку. Однією з актуальних задач квантової криптографії є збільшення швидкодії квантових каналів зв'язку.

Список використаних джерел:

- 1.Защита каналов связи. – Режим доступа : http://www.bezpeka.com/files/lib_ru/book-domarev03/ch_14.pdf.
- 2.Ємельянов С.О. Систематизація методів та засобів технічного захисту інформації в телефонних каналах та лініях зв'язку / С.О. Ємельянов // Сучасна спеціальна техніка. – 2011. – № 2 (25). – с. 128–132.
- 3.Гончарова Л.Л. Основи захисту інформації в телекомунікаційних та комп'ютерних мережах / Л.Л. Гончарова, А.Д. Возненко, О.І. Стасюк, Ю.О. Коваль. – 2013. – Режим доступа : http://lib.detut.edu.ua/files/Nauk_trud_vukladahiv/Fakultet%20Infrastruktur_guxomuy_sklad%20%E2%80%9D/Kafedra_tel_texn_avtomatuka/nauk_trud_voznenko.pdf.
- 4.Васіліу Є.В. Методи підвищення криптографічної стійкості та збільшення інформаційної місткості протоколів квантової криптографії / Є.В. Васіліу // Автореферат дисертації на здобуття наукового ступеня доктора технічних наук. – 2011.

УДК 004.2

АРХІТЕКТУРА ВЕБ-СЕРВЕРА З БАГАТОПРОЦЕСОВИМ АСИМЕТРИЧНИМ КЕРУВАННЯМ ПОДІЯМИ

Савчук Тамара, Горобець Юрій

Вінницький національний технічний університет

Анотація

В даній доповіді запропоновано архітектуру веб-сервера, який використовує багатопроцесове асиметричне керування подіями, оцінено її продуктивність на різних робочих навантаженнях і швидкодію порівняно з іншими серверними архітектурами.

Abstract

This report presents a web-server architecture, that uses multi-process asymmetric event management, evaluates its performance across different workloads, and performs faster than other server architectures.

Продуктивність веб-серверів відіграє ключову роль у задоволенні потреб великої та зростаючої спільноти веб-користувачів. Портативні високопродуктивні веб-сервери знижують вартість обладнання для задоволення попиту на певну послугу і забезпечують гнучкість у зміні апаратних платформ та операційних систем на основі витрат й доступності [1].

Веб-сервери покладаються на кешування часто запитуваних сторінок в основній пам'яті для досягнення пропускнуєї спроможності у тисячі запитів в секунду, незважаючи на довгу латентність операцій з дисками. Оскільки розмір даних, які розміщені в Інтернеті є потужними, робочі навантаження зазвичай перевищують ємність основної пам'яті сервера.

Таким чином, високопродуктивний веб-сервер повинен мати таку архітектуру, щоб він зміг перекривати запити для кешування вмісту з одночасною операцією на диску, яка отримує запитуваний вміст, що в даний момент не є кешованим в основній пам'яті. Веб-сервери використовують різні підходи для досягнення такої паралельності. Сервери, що використовують Single Processing Event Driven (SPED), не є ефективними у використанні [1].

SPED може забезпечити відмінну продуктивність для кешованих навантажень, де більшість запитуваного вмісту можна утримувати в основній пам'яті. На робочих навантаженнях, що перевищують ємність кеш-пам'яті сервера, сервери з багатопроцесорними (MP) або багатопоточними (MT) архітектурами, як правило, ефективніше у продуктивності і швидкодії [1, 2].

Використання багатопроцесового асиметричного керування подіями (AMPED - asymmetric multi-process eventdriven) у архітектурі веб-сервера дозволить сумістити продуктивність і швидкодію MP та MT архітектур, і також перевищити її на динамічних робочих навантаженнях при легкій портативності завдяки використанню стандартного API.

Архітектура AMPED працює як одиночний процес, керований подіями. При запиті дані кешуються і використовують ті самі алгоритми, що MP- та MT-архітектури при запиті даних з диска [3].

Продуктивність архітектури AMPED є не меншою за продуктивність серверів на архітектурі SPED при роботі з кешованими даними, але вищою продуктивності серверів на архітектурах MP і MT під час динамічних робочих навантажень [3, 4].

Результати аналізу порівняння продуктивності архітектури AMPED з продуктивністю інших серверних архітектур при реалізації з однаковою кодовою базою

наведено на рисунках 2, 3. В першому експерименті (рисунок 2) набір клієнтів повторно запитує один і той же файл, обсяг якого змінюється в кожному тесті.

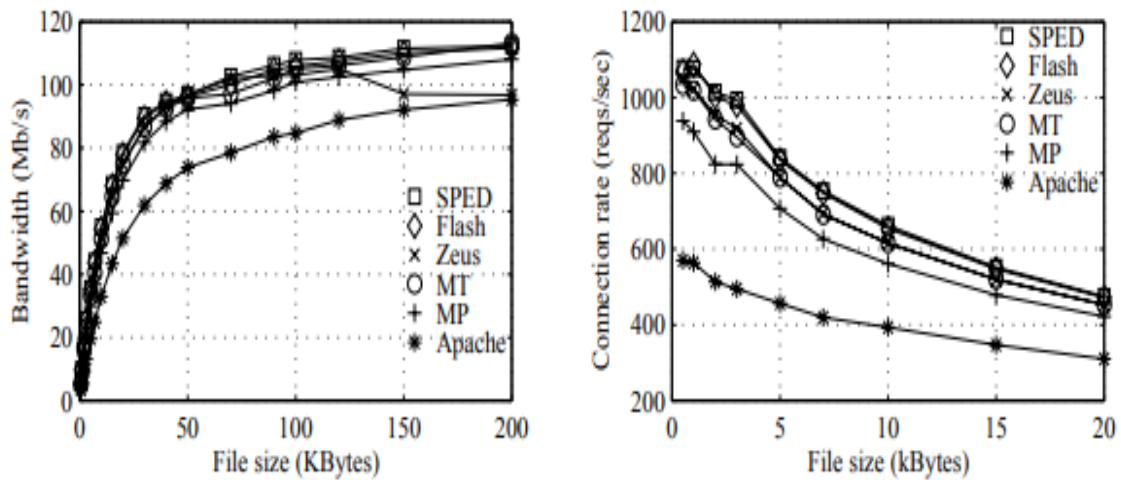


Рисунок 2 – Результати порівняння серверних архітектур за: а) пропускною здатністю; б) кількістю запитів.

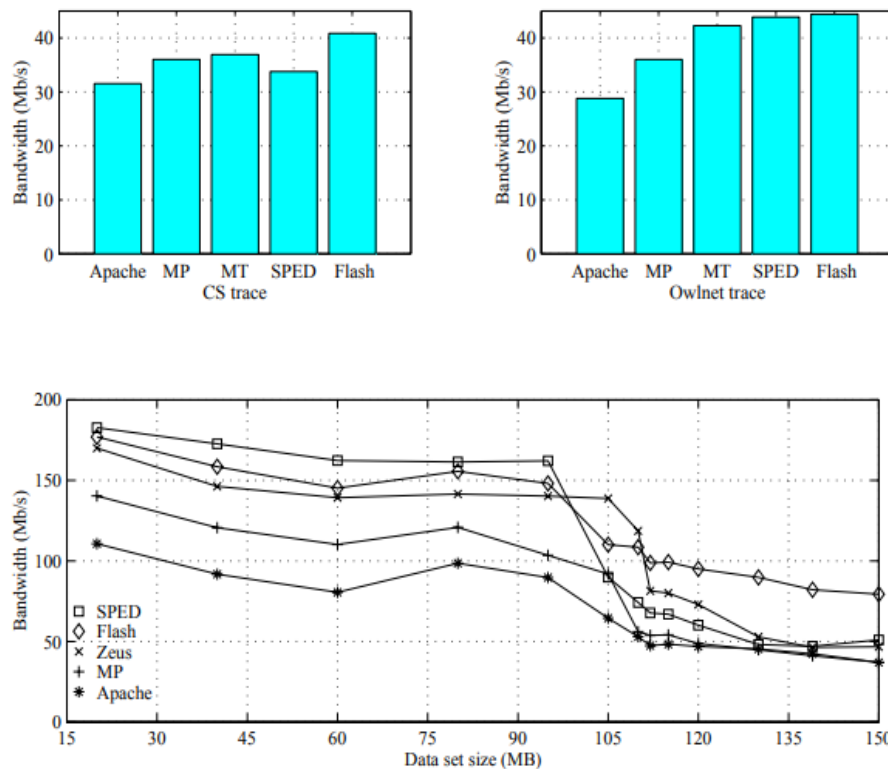


Рисунок 3 – Результати порівняння архітектур на робочих навантаженнях за: а) пропускною здатністю; б) обсягом даних

Як видно, продуктивність серверу з архітектурою AMPED не нижче продуктивності інших архітектур в широкому діапазоні реалістичних робочих навантажень, а також перевищує продуктивність веб-серверу Zeus [5] на 30%, і продуктивність Apache [6] на 50% на реальних робочих навантаженнях

В другому експерименті (рисунок 3) було проаналізовано залежність швидкодії різних веб-серверів при реальних навантаженнях від обсягу даних. Для виконання цього експерименту було використано тротлінг вхідної шини для тестування архітектури серверів Zeus, Apache, MP, SPED на різних значеннях параметрів інтернет з'єднання (пропускна здатність) для подальшого пошуку залежностей. Виявлено, що використання архітектури AMPED є доцільним, коли обсяг даних перевищує 135 МБ, що дає можливість роботи з Big Data. Як видно з рисунку 3, збільшення обсягу даних знижує продуктивність роботи на серверних архітектурах SPED, MP, Apache, Zeus. Отже, AMPED архітектура не зменшує продуктивність серверів, які використовують архітектуру SPED на кешованих робочих навантаженнях, а також серверів MP і MT на динамічних навантаженнях. При цьому, серверна архітектура AMPED забезпечує більшу швидкодію при обробках запитів з великим обсягом даних та використовує тільки стандартні API-інтерфейси, доступні в сучасних операційних системах, а тому легко переноситься.

Список використаних джерел:

- 1.M. F. Arlitt and C. L. Williamson. Web Server Workload Characterization: The Search for Invariants. In Proceedings of the ACM SIGMETRICS '96 Conference, pages 126–137, Philadelphia, PA, Apr. 1996.
- 2.M. J. Feeley, W. E. Morgan, F. H. Pighin, A. R. Karlin, H. M. Levy, and C. A. Thekkath. Implementing global memory management in a workstation cluster. In Proceedings of the Fifteenth ACM Symposium on Operating System Principles, Copper Mountain, CO, Dec. 1995.
- 3.Y. Hu, A. Nanda, and Q. Yang. Measurement, analysis and performance improvement of the Apache web server. In Proceedings of the 18th IEEE International Performance, Computing and Communications Conference (IPCCC'99), February 1999.
- 4.J. Liedtke, V. Panteleenko, T. Jaeger, and N. Islam. High-performance caching with the Lava hit-server. In Proceedings of the USENIX 1998 Annual Technical Conference, New Orleans, LA, June 1998.
- 5.Zeus Technology Limited. Zeus Web Server. <http://www.zeus.co.uk>
- 6.Apache. <http://www.apache.org>



ОДИНАДЦЯТА МІЖНАРОДНА КОНФЕРЕНЦІЯ
ІОН - 2018
ІНТЕРНЕТ-ОСВІТА-НАУКА-2018



СЕКЦІЯ С. КОМП'ЮТЕРНА ІНЖЕНЕРІЯ



THE ELEVENTH INTERNATIONAL
CONFERENCE
IES-2018
INTERNET-EDUCATION-SCIENCE - 2018



SECTION C. COMPUTER ENGINEERING



ОДИННАДЦАТАЯ МЕЖДУНАРОДНАЯ
КОНФЕРЕНЦИЯ

ІОН-2018
ІНТЕРНЕТ– ОБРАЗОВАНИЕ – НАУКА 2018



СЕКЦІЯ С. КОМП'ЮТЕРНА ІНЖЕНЕРІЯ



ЯК ДОЛУЧИТИСЬ ДО INTERNET OF THINGS

Цирульник Сергій¹, Роптанов Володимир²

¹Вінницький технічний коледж

²Вінницький національний технічний університет

Анотація

Описано підходи до розробки недорогих, але ефективних пристроїв для «Інтернету речей» на основі популярних налагоджувальних плат з використанням модулів Bluetooth та Wi-Fi ESP8266. Розглянуто безкоштовні систем розробки та використання мобільних графічних інтерфейсів для управління пристроями IoT зі смартфона або планшета.

Abstract

The described approaches to the development of inexpensive but effective devices for the "Internet of things" based on the popular debugging boards with modules Bluetooth and Wi-Fi ESP8266. Reviewed free systems the development and use of mobile graphical interfaces to control IoT devices from your smartphone or tablet.

Вступ

«Інтернет речей» (Internet of Things, IoT) вже став частиною нашого життя. Багато хто з нас використовують розумні термометри для моніторингу температури житлових приміщень та WiFi розетки.

«Інтернет речей» – це взаємозв'язок унікально ідентифікованих вбудованих обчислювальних приладів з інтернет-інфраструктурою [1]. IoT це концепція забезпечення інноваційного зв'язку, такий як Bluetooth Smart (Hi-Fi) або Wi-Fi, при використанні якої виконується підключення до інфраструктури Інтернету.

Підключення приладів до мережі Інтернет надає нові можливості як споживачам, так і виробникам. Споживачі можуть контролювати свої витрати й керувати часом, а виробники – контролювати роботу пристроїв, простіше вирішувати питання його обслуговування, а також пропонувати нові структури, що приносять дохід..

Основна частина

Сучасні смартфони поставляються з вбудованим Bluetooth Smart, що забезпечує миттєвий доступ до Інтернету та спрощене створення пари з приладом. Додаток смартфона може стежити за потребами користувачів та керувати передачею даних до пристрою і від нього. WiFi є ще одним способом підключення приладів до IoT, що забезпечує постійний канал для передачі даних з давачів.

Бездротові пристрої для «Інтернету речей» повинні задовольняти таким вимогам: мінімальне енергоспоживання, простота та надійність роботи; безпека підключення, сумісність з більшістю смартфонів, планшетів, ноутбуків; можливість масштабування без значних додаткових витрат; дотримання міжнародних стандартів.

Будь-який домашній розробник мікроелектроніки використовує контролери Arduino (UNO, Micro, Nano, Mini, Mega), ESP8266 (WeMos D1, WeMos D1 mini NodeMCU), AirBoard, ChipKIT (UNO32, DP32, uC32, Max32) [2, 3, 4]. Для зв'язку між контролером та мобільним пристроєм можна скористатися Bluetooth HC-05, HC-06, WiFi ESP8266, Ethernet Shield W5100. Однак, рано чи пізно виникає необхідність управління власноруч створеним пристроєм за допомогою пульта, яким буде зручно перемикаати режими роботи або ж просто переглядати поточний стан. Для створення свого пристрою IOT пропонуються кілька безкоштовних систем розробки та використання мобільних графічних інтерфейсів для управління контролерами зі смартфона або планшета: Blynk, Cayenne, RemoteXY, Virtuino [5, 6].

Blynk – додаток для мобільного пристрою (рис. 1, а), що дозволяє у формі графічного конструктора створювати повнофункціональні додатки для зв'язку їх з пристроями на платформі Arduino, ESP8266, Raspberry Pi. Особливістю Blynk є простота, з якою створюється як сам додаток, так і те, як реалізується зв'язок з програмним кодом пристрою. Для початку роботи користувач встановлює додаток Blynk на телефон або планшет. Далі, розміщає такі елементи, як кнопки, слайдери, перемикачі, лампочки, графобудівники. Кожен елемент може бути прив'язаний до виводів фізичного або віртуального пристрою. На стороні пристрою достатньо лише під'єднати бібліотеку, налаштувати зв'язок між вихідним кодом та реєстраційним кодом встановленого додатка, помістити в цикл обробник подій.



Рисунок 1 – Інтерфейс користувача: а) Blynk, б) Cayenne

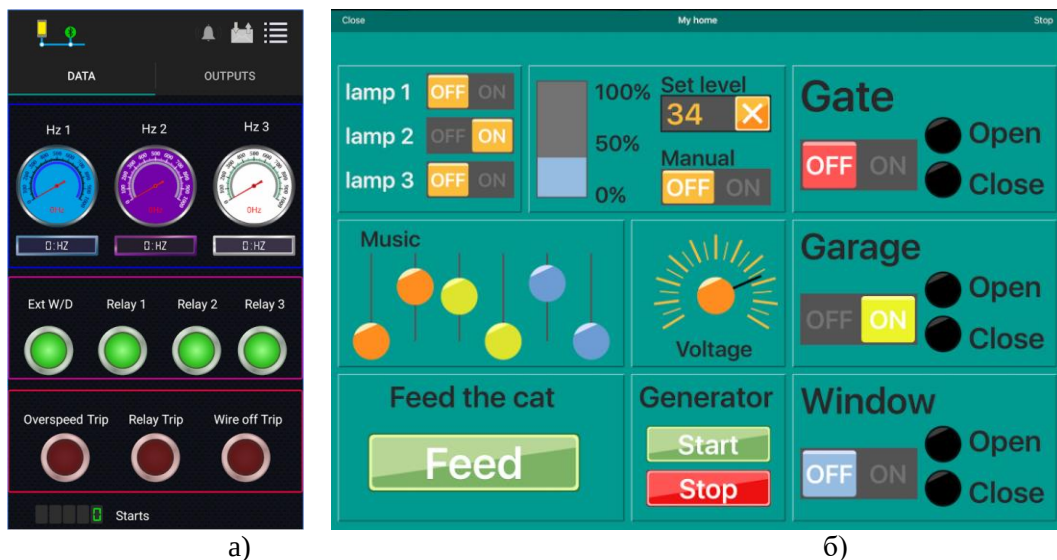


Рисунок 2 – Інтерфейс користувача: а) Virtuino, б) RemoteXY

Сауенне передбачає підхід з мінімальною кількістю програмування на стороні пристрою клієнта. Сауенне крім мобільного додатку пропонує і повнофункціональну панель управління на своєму Web-сайті. В додатку або через веб-браузер, користувач створює проект (рис. 1, б), додає кнопки, слайдери, регулятори, лампочки, шкали, які можна прив'язати до віртуальних або реальних виводів контролера. Додатково у Сауенне є механізм тригерів та подій. Тригери обробляють події, які одержує від пристрою.

Модель подій спирається на розклад за календарем. Зв'язок контролера та програми здійснюється шляхом додавання невеликих фрагментів програмного коду.

Virtuino (рис. 2, а) та RemoteXY (рис. 2, б) передбачає використання тільки мобільного додатку для створення інтерфейсу користувача. Як і Cayenne з Blynk, Virtuino та RemoteXY використовують технологію додатка в додатку. Це означає, що додаток залишається в «пісочниці» і не може існувати окремо від середовища розробки. Virtuino і RemoteXY не використовують проміжний сервер. Blynk і Cayenne використовують серверну частину та працюють тільки через неї. Не можна звернутися до пристрою без підключення до інтернету. У Virtuino та RemoteXY розробник може піти двома шляхами. По-перше, він може скористатися сервісом ThingSpeak (Virtuino) або Cloud.remotexy (RemoteXY) як проміжний сервер. По-друге, комунікація між додатком та пристроєм здійснюється за допомогою веб-сервера, піднятого на самому пристрої. Доступ ззовні локальної мережі до вашого пристрою буде неможливий.

У сервісі RemoteXY інтерфейс користувача створюється на сайті, генерується вихідний код для Arduino IDE. Структура інтерфейсу зберігається в контролері. При підключенні немає ніякої взаємодії з іншими серверами для того щоб завантажити інтерфейс. Структура інтерфейсу (рис. 2, б) завантажується в мобільний додаток з контролера. З одного мобільного додатка можна керувати всіма своїми пристроями. Кількість пристроїв не обмежена. Таблиці і рисунки нумеруються тільки тоді, коли на них є посилання в тексті. Формули повинні бути набраними в редакторі Microsoft Equation 3.0 відділеними від тексту.

Висновки

Internet of Things – це ідея, згідно з якою всі пристрої навколо нас підключені до Інтернету і спілкуються не тільки з нами, але й один з одним. Очікується, що до 2020 року в Мережу вийдуть близько 50 мільярдів пристроїв.

У продажу фірмові налагоджувальні плати реалізуються, як правило, за мінімальною ціною з низьким рівнем рентабельності. В електроніці для першого знайомства з новим технічним напрямком використовують простий, але ефективний спосіб. Користувачеві пропонується оцінити всі переваги нового виробу випробувавши в роботі його функціонально закінчений прототип. Вхідження до Internet of Things досить простий. Необхідно вибрати апаратну платформу, середовище розробки та створити графічний інтерфейс для свого пристрою.

Судячи за масштабами та темпами розвитку нових технологій, embedded фахівці та програмісти вбудованих систем на найближче десятиліття без роботи не залишаться.

Список використаних джерел:

- 1.Шварц М. Интернет вещей с ESP8266: Пер. с англ./М. Шварц. — СПб: БХВ-Петербург, 2018. – 192 с. – ISBN 978-5-9775-3867-1
- 2.Цирульник С. М. Візуальне програмування засобами MODKIT/ С. М. Цирульник, В. М. Ткчук// Збірник матеріалів МНПК «Зимові наукові читання», 1 частина. – К.: Центр наукових публікацій. – 2016. – с. 122-127
- 3.Рюмик С. М. 1000 и одна микронтроллерная схема. Вып. 4 / С. М. Рюмик. – М.: ДМК-Пресс, 2017. - 336 с. – ISBN 978-5-97060-565-3
- 4.Алексеев В. Модули Bluetooth, Wi-Fi и NFC производства u-box для «Интернета вещей». Часть2. Совмещенные Wi-Fi / Bluetooth – модули. В. Алексеев // Chip news Украина. Инженерная микроэлектроника. – 2015. – №10. – С. 28-34.
- 5.Петин В. А. Создание умного дома на базе Arduino / В. А. Петин. – М.: ДМК Пресс, 2018. – 180 с.– ISBN 978-5-97060-620-9
- 6.Феномен Blynk и его альтернативы [Електроний ресурс]. – Режим доступа: <https://blog.kvv213.com/2017/02/phenomen-blynk-i-ego-al-ternativy>. – Загл. з екрана. – Мова російська.

ПРИМЕР ПАРАЛЛЕЛЬНОГО УПРАВЛЕНИЯ В ЗАДАЧЕ КОЛЛЕКТИВНОГО ВЗАИМОДЕЙСТВИЯ ГРУППЫ РОБОТОВ

Абабий Виктор, Судачевски Виорика, Мунтяну Сильвия, Абабий Константин, Самоил Ион

Технический Университет Р. Молдова, Департамент Информатики и Системной Инженерии

Аннотация

В данной работе представлен пример синхронизации и параллельного управления в задаче коллективного взаимодействия группы роботов. Алгоритм управления основан на параллельную обработку данных и генерации сигналов для воздействия на группу роботов. Для функционального моделирования системы управления используются сети Петри, модель которых в дальнейшем используется для синтеза самой системы параллельной обработки данных и управления.

Abstract

In this paper, we present an example of synchronization and parallel control in the task of collective interaction of a group of robots. The control algorithm is based on parallel processing of data and generation of signals for impact on a group of robots. For the functional modeling of the control system, Petri nets are used, the model of which is subsequently used to synthesize the system of parallel data processing and control.

Введение

Управление коллективными роботами, это явный пример разработки систем для обработки и анализа распределенных данных [1], так как эти вычислительные структуры должны обеспечивать такие важные характеристики, для систем управления, как: надежность, отказоустойчивость, гибкость, адаптивность, согласованность, сотрудничество и взаимодействие [2].

Поведение коллективных роботов было вдохновлено поведением живых существ, такие как насекомые, птицы и др. [3, 4], где каждое существо решает часть общей задачи.

Целью данных исследований является проектирование системы для параллельного управления коллективными роботами при выполнении конкурирующих операций.

Выбор модели параллельной обработки данных для управления коллективными роботами

Для обеспечения желаемой производительности, при управлении коллективными роботами (КР), необходимо использование двух типов вычислительных архитектур (ВА), такие как: распределенные и параллельные.

Распределенные вычислительные архитектуры (РВА) [19] реализованы на базе вычислительных сетей, которые обеспечивают: высокую производительность при решении сложных задач; хранение и обработку больших объемов данных; расширяемость, отказоустойчивость и надежность системы в целом.

Параллельные вычислительные архитектуры (ПВА) [20] реализованы на базе многопроцессорных или микроконтроллерных систем с потоковой обработкой данных. Для выбора модели параллельной обработки данных были анализированы такие модели как: **SISD** (Single Instruction stream, Single Data stream), **MISD** (Multiple Instruction stream, Single Data stream), **SIMD** (Single Instruction stream, Multiple Data stream), и **MIMD** (Multiple Instruction stream, Multiple Data stream). В результате анализа была выбрана модель **MIMD**.

В качестве примера РВА и ПВА можно привести ВА много-агентных систем, которые описаны в работах [5-8]. В данных системах, как и при управлении КР, общая задача распределена на множество ВА, каждая из которых решает свою под-задачу.

Моделирование параллельных процессов обработки данных для управления коллективными роботами

Эффективность управления КР определяется точностью синхронизации процессов обмена данными, их обработки и воздействия на исполнительные устройства. Наиболее эффективным методом выявления конфликтов при передаче и обработке данных является моделирование на базе сетей Петри [9, 21].

Сети Петри это математический аппарат для моделирования динамических дискретных систем. Сеть Петри $PN=(P, T, F, M0)$ представляет собой двудольный ориентированный мультиграф, состоящий из вершин двух типов: позиций $P=\{p1, p2, ..., pn\}$ и переходов $T=\{t1, t2, ..., tm\}$, соединённых между собой дугами $F \subseteq (P \times T) \cup (T \times P)$. Вершины одного типа не могут быть соединены непосредственно. В позициях могут размещаться метки (маркеры) M , способные перемещаться по сети синхронизируемые событиями. $M0$ – это исходное состояние сети Петри. Событием называют срабатывание перехода, при котором метки из входных позиций этого перехода перемещаются в выходные позиции. События происходят мгновенно, либо одновременно, при выполнении некоторых условий.

Синтез структурной схемы

Структурная схема системы параллельной обработки данных для управления КР представлена на Рисунке 1, где: **PC** – ЭВМ с программным обеспечением: для моделирования на базе сетей Петри (**VPNP** [14]), для компиляции модели сети Петри в код конфигурации **FPGA** (**HPNC** [10-13, 22]), и для проектирования и конфигурации устройств **FPGA** (**Quartus –II** [15]); **FPGA** – блок параллельной обработки данных и генерации сигналов синхронизации; **AD** – распределенное вычислительное устройство на базе **Arduino UNO**; **RM** – роботы манипуляторы **Arduino Braccio Robotic Arm** [17], которые выполняют параллельные действия в области **Workspace**.

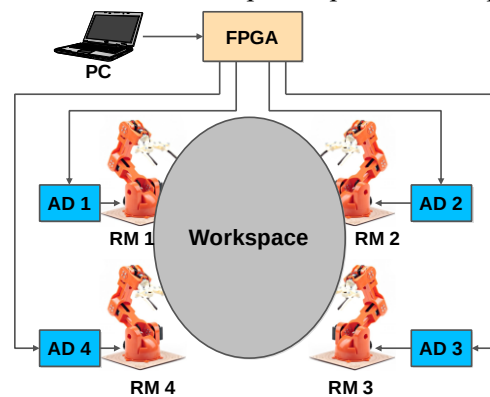


Рисунок 1 – Структурная схема системы параллельной обработки данных для управления коллективными роботами

Функциональная модель системы управления

Функциональная модель системы параллельной обработки данных для управления коллективными роботами представлена на Рисунке 2, где: **FPGA DE0** – блок параллельной обработки данных на базе **FPGA Altera Cyclone IV** [16]; **Module 1...4** – модули для управления роботами манипуляторов на базе **Arduino Braccio Robotic Arm**. Каждый модуль состоит из: **AU** - устройства **Arduino Uno** [18]; **DRV** – драйвера для управления двигателями **SV**.

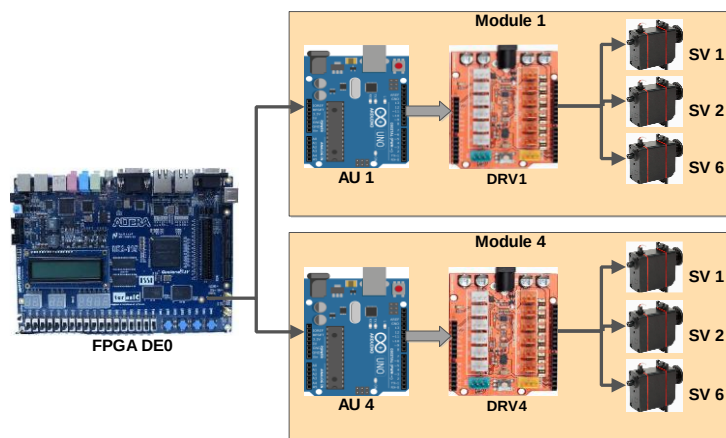


Рисунок 2 – Функциональная модель системы параллельной обработки данных для управления коллективными роботами

Пример моделирования системы управления

Моделирование системы параллельной обработки данных для управления коллективными роботами выполнено на базе программного приложения *VPNP* [14]. Результат моделирования для взаимодействия 4 роботов манипуляторов (**BR1**, **BR2**, **BR3**, **BR4**) представлен на Рисунке 3.

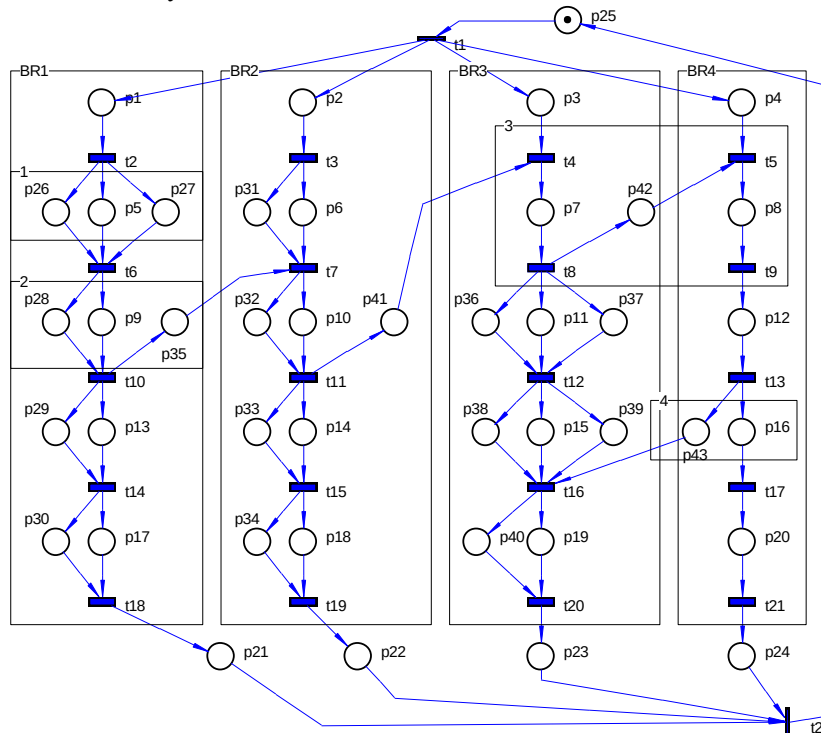


Рисунок 3 – Результат моделирования для взаимодействия 4 роботов манипуляторов

Позиция **P25** определяет готовность системы к началу нового цикла управления. Позиции **P1**, **P2**, **P3** и **P4** это параллельно выполняемые операции всеми манипуляторами. Блок операций **1** (**P6**, **P26**, **P27**) указывают на одновременное включение 3 двигателей для манипулятора **BR1**. Блок операций **2** содержит 2 позиции (**P9**, **P28**) для включения 2 двигателей для манипулятора **BR1** и позицию **P35** для синхронизации операции манипулятора **BR2**. Блок **3** и **4** указывают на взаимную синхронизацию между манипуляторами **BR3** и **BR4** (через позицию **P42**), и **BR4** и **BR3** (через позицию **P43**).

Синтез системы параллельной обработки данных для управления коллективными роботами основано на применении аппаратных сетей Петри [10-13, 22], которые реализованы на базе ИС *FPGA* [15] (Комплекс разработки *DE0* [16]).

Список использованных источников:

1. A. Bröring, et al., „New generation sensor web enablement,” *Sensors*, 11, 2011, pp. 2652-2699. ISSN: 1424-8220. [Available from: doi:10.3390/s110302652].
2. Gaston Lefranc, „Colony of Robots: New Challenge,” In: *Int. J. Of Computers, Communications & Control*, Vol. III(2008), Suppl. Issue: Proceedings of ICCCC-2008, pp.92-107, ISSN: 1841-9836, E-ISSN: 1841-9844.
3. C. Ampatzis, „On the Evolution of Autonomous Time-based Decision-making and Communication in Collective Robotics,” PhD thesis, IRIDIA, Université Libre de Bruxelles, Belgium, 2008.

4. G. Beni, „From swarm intelligence to swarm robotics,” In: Swarm Robotics, volume 3342 of Lecture Notes in Computer Science, pp. 1–9, Springer, Berlin, Heidelberg, 2005.
5. Gh. Safonov, V. Ababii, V. Sudacevski, „Analysis of distributed computing architectures for synthesis of multi-agent systems,” In: European Applied Sciences Journal, № 9, 2016 (September), pp. 34-37, ISSN: 2195-2183.
6. V. Ababii, V. Sudacevski, Gh. Safonov, „Designing a Collective Agent for synthesis of Adaptive Decision-Making Systems,” In: Sciences of Europe (Praha, Czech Republic), Vol 1, No 17(17), 2017, pp. 70-75, ISSN: 3162-2364.
7. V. Ababii, V. Sudacevski, D. Bordian, A. Raschipkin, „Sistem pentru comanda unei colonii de roboți mobili în baza modelelor de rețele neuronale,” In: Proceedings of the 9th International Conference on Microelectronics and Computer Science & The 6th Conference of Physicists of Moldova, Chișinău, Moldova, October 19-21, 2017. pp. 288-290, ISBN: 978-9975-4264-8-0.
8. В. Абабий, В. Судачевски, М. Подубный, Г. Сафонов, Е. Негарэ, „Система коллективного принятия решений на базе пространственно-распределенных ВУ,” In: The Tenth International Scientific-Practical Conference Internet-Education-Science IES-2016, Ukraine, Vinnytsia, VNTU, 11-14 October, 2016, pp. 20-22, ISBN: 978-9666-641-646-2.
9. J.L. Peterson, „Petri Net Theory and the Modeling of Systems,” Prentice-Hall, 1981.
10. V. Sudacevski, V. Ababii, „Modelling and Synthesis of Real-Time Control Systems Based on Hardware Timed Petri Nets,” In: Buletinul Institutului Politehnic Din Iași, Publicat de Universitatea Tehnică „Gheorghe Asachi” din Iași, Secția „Electrotehnică. Energetică. Electronică”, Tomul LIX (LXIII), Fasc. 4, 2013, pp. 161-172.
11. V. Sudacevski, V. Ababii, E. Gutuleac, M. Podubnii, „Sinteza procesoarelor specializate în baza rețelelor Petri hardware funcțional interpretate,” In: Meridian Ingineresc Nr. 3, 2015. pp.117-123, ISSN: 1683-853X.
12. V. Ababii, V. Sudacevski, M. Podubnii, I. Cojuhari, „Real-time reconfiguration of distributed control system based on hard Petri nets,” In: International Conference on DEVELOPMENT AND APPLICATION SYSTEMS 12th Edition, May 15-17, 2014, Suceava, ROMANIA, pp. 21-24, ISSN: 1844-5039.
13. V. Sudacevski, V. Ababii, M. Podubnii, „A Synthesis Method for Reconfigurable Embedded Processors,” In: The 13th International Conference on DEVELOPMENT AND APPLICATION SYSTEMS, Suceava, Romania, May 19-21, 2016, IEEE Catalog Number: CFP1665Y-DVD, pp. 184-188, ISBN: 978-1-5090-1992-2.
14. E. Guțuleac, C. Boșneaga, A. Railean, „VPNP-Software tool for modeling and performance evaluation using generalized stochastic Petri nets,” In: Proceedings of the 6-th International Conference on DAS-2002, 23-25 May 2002, Suceava, România, p. 243-248, ISBN 973-98670-9-X.
15. <https://www.altera.com> [Электронный ресурс. Доступ: 25.03.2018].
16. <http://www.terasic.com.tw> [Электронный ресурс. Доступ: 25.03.2018].
17. <https://www.robotshop.com/en/arduino-braccio-robotic-arm.html> [Электронный ресурс. Доступ: 25.03.2018].
18. <https://store.arduino.cc/usa/arduino-uno-rev3> [Электронный ресурс. Доступ: 25.03.2018].
19. G. Moldovan, I. Dzițac, „Sisteme distribuite – Modele matematice,” Oradea, Editura Universității Agora, 170p., 2006, ISBN: 973-88205-0-2.
20. Blaise Barney, „Introduction to Parallel Computing,” [Электронный ресурс. Доступ: 25.03.2018; https://computing.llnl.gov/tutorials/parallel_comp/].
21. O. Păstrăvanu, M. Matcovschi, C. Mahulea, „Aplicații ale rețelelor Petri în studierea sistemelor cu evenimente discrete,” Iași, Editura Gheorghe Asachi, 2002, 256p., ISBN: 973-8292-86-7.
22. V. Sudacevski, Sinteza structurilor de procesare concurentă a datelor. Teza de doctor în tehnică (In Eng.: Synthesis of structures for parallel data processing. Doctoral thesis). UTM, Chișinău 2009, 167 p.

УДК 004.7:519.2

МЕТОД ВДОСКОНАЛЕННЯ ОДНОШЛЯХОВИХ ПРОТОКОЛІВ ДИНАМІЧНОЇ МАРШРУТИЗАЦІЇ

Шевчук Катерина, Захарченко Сергій

Вінницький національний технічний університет

Анотація

Розглядаються сучасні протоколи динамічної маршрутизації, принцип їх функціонування та способи призначення метрики зв'язків. Визначено, що більшість з них є одношляховими, обирають один маршрут з мінімальною метрикою або здійснюють балансування між маршрутами з однаковою метрикою.

Як результат функціонування мережі у такий спосіб спричиняє максимальне використання знайденого найкращого або альтернативного шляху, їх перевантаження, в той час як інші вузли (ресурси) мережі перебуватимуть в стані очікування (не задіяні при передачі трафіку). Впроваджувати зміни безпосередньо до протоколу динамічної маршрутизації є не доцільним, оскільки схожа ситуація існує серед всіх одношляхових протоколів, тому існує необхідність знайти універсальне рішення. Це можливо здійснити через структурні зміни в мережі, а саме модифікацію процесу маршрутизації, скомбінувавши найкращі особливості розподіленого та централізованого способів маршрутизації.

Abstract

The modern protocols of dynamic routing, the principle of their functioning and methods of assigning the link metric are considered. It is determined that most of them are one-way, choose one route with a minimum metric or perform balancing between routes with the same metric.

As a result, the network operation in this way causes the maximum use of the best or alternative path found, their overload, while other nodes (resources) of the network will be in standby (not involved in the transmission of traffic). Implementing the changes directly to the dynamic routing protocol is not feasible, since a similar situation exists among all one-way protocols, so there is a need to find a universal solution. This is possible through structural changes in the network, namely, the modification of the routing process, combining the best features of distributed and centralized routing methods.

Вступ

Необхідність забезпечення якісного обслуговування сучасного трафіку, що передається через IP-мережі, обумовлені високими вимогами до ефективності передачі пакетів даних від відправника до отримувача. Після активізації та налаштування динамічної маршрутизації за одним з протоколів, інформація про маршрути оновлюється автоматично після отримання нової інформації про маршрути. Маршрутизатори обмінюються повідомленнями про зміни у топології мережі.

Дослідження присвячене підвищенню якості передачі трафіку, шляхом рівномірного розподілу трафіку, зменшення затримки передавання трафіку за допомогою модифікації процесу маршрутизації без внесення змін в протоколи маршрутизації.

Для вирішення практичних проблем необхідно проаналізувати протоколи динамічної маршрутизації, їх функціональні особливості, основні переваги та недоліки, з метою визначення ймовірних негативних явищ в мережі та методи впливу на них, способи маршрутизації та різновиди протоколів за кількістю маршрутів.

Протокол маршрутизації (RIP) є дистанційно-векторним, має обмежені знання про мережу, використовує механізм підрахунку переходів, щоб знайти оптимальний шлях для маршрутизації пакетів, оновлює інші маршрутизатори, транслюючи всю таблицю маршрутизації до всіх маршрутизаторів кожні 30 секунд.[1] Virізняється простотою та легкою конфігурацією, проте його недоліками є повільний час конвергенції (оновлення) та обмеження масштабованості, тому цей протокол найкраще працює для малих мереж з

більш стабільною роботою, не враховує пропускних здатностей каналів, не підтримує кілька шляхів для одного маршруту, тобто є одношляховим.[1]

(OSPF) - це протокол внутрішнього шлюзу (IGP), заснований на технології відстеження стану каналу (link-state technology) та пошуку найкоротшого шляху. Цей протокол здійснює маршрутизацію пакетів, збираючи інформацію про стан зв'язків з сусідніх маршрутизаторів і на підставі отриманої інформації будує карту мережі. [1]

Перевагами передачі трафіку з протоколом OSPF, зміни топології мережі виявляються дуже швидко, багато параметрів для налаштування, що проявляється в гнучкості та надійності, відрізняється простою практичної реалізації алгоритму.

Головною проблемою протоколу OSPF є те, що при використанні алгоритму Дейкстри, IP-мережа не захищена від перевантажень, необхідно застосувати додаткові методів щодо зниження ймовірності перевантаження по найкоротшому шляху.

EIGRP покращений протокол маршрутизації внутрішнього шлюзу - дистанційно-векторний протокол динамічної маршрутизації, що був оптимізований для зменшення нестабільності протоколу після змін топології мережі, уникнення проблеми зациклення маршруту та більш ефективного і економного використання потужностей маршрутизатора. [2] Маршрутизатори обмінюються інформацією про маршрути після встановлення з'єднання, після чого надсилаються лише часткові оновлення. Оновлення на основі потреб є перевагою перед іншими протоколами (RIP та OSPF), оскільки це зменшує трафік між маршрутизаторами і, отже, економить пропускну здатність. Метрика, яка використовується для пошуку оптимального шляху, розраховується за допомогою змінної пропускної здатності, навантаження, затримки та надійності.

За способом маршрутизації мережі бувають з централізованою, децентралізованою та гібридною маршрутизацією.

Централізована маршрутизація реалізується за принципом вибору напрямку руху для кожного пакету центром управління мережею, а мережеві вузли лише сприймають та реалізують результати вирішення задачі маршрутизації. Перевагами такого способу є можливість обрати вузли прості за структурою, оскільки вони приймають мінімальну участь в процесі маршрутизації. Однак при збільшенні кількості вузлів зростає складність організації централізованого керування мережі передачі даних.

Розподілена або децентралізована маршрутизація виконується через розподіл функцій керування мережею між її вузлами. На основі збереженої керуючої інформації, кожен вузол самостійно визначає напрямок передачі пакетів. Це підвищує структурну складність вузлів, однак мережа відзначається вищим рівнем працездатності, оскільки вихід з ладу будь-якого вузла не впливає на роботу мережі загалом. [3]

Змішана маршрутизація характеризується співвідношенням реалізованих принципів централізованої та розподіленої маршрутизації (наприклад, гібридна адаптивна маршрутизація). Адаптивна маршрутизація передбачає пристосування алгоритму маршрутизації до реального стану мережі. Недоліком методів адаптивної маршрутизації є складність прогнозування стану мережі.

За наявністю використання декількох маршрутів до одного адресата протоколи маршрутизації поділяють на:

- одношляхові (англ. single-path) – при встановленні з'єднання між маршрутизаторами та ознайомлення з топологією мережі, заносять до таблиці маршрутизації дані про єдиний оптимальний маршрут. Недоліком є нерівномірне навантаження мережі через максимальне завантаження оптимального маршруту.

- багатошляхові (англ. multi-path) – вирізняються визначенням декількох оптимальних шляхів та занесення їх до таблиці маршрутизації. [4] У випадку блокування основного маршруту, з таблиць маршрутизації зчитується інформація про додаткові маршрути без повторного визначення оптимальних шляхів. При перевантаженні основного маршруту, багатошляхові протоколи маршрутизації мають можливість перерозподіляти навантаження на резервні шляхи.

Для вирішення проблеми одношляхових протоколів маршрутизації пропонується здійснити структурні зміни в мережі, а саме модифікацію процесу маршрутизації шляхом впровадження в мережу централізованого контролера маршрутизації (рис. 1). Від всіх маршрутизаторів періодично надходитиме інформація про їх функціональний стан. Контролер проводить аналіз, надсилає запити до маршрутизаторів та при виникненні потреби через протокол SNMP вносить зміни в параметри маршрутизатора з подальшою зміною таблиць маршрутизації. В свою чергу маршрутизатори при виникненні небажаних подій, аналогічним способом надсилають інформаційне повідомлення про це.

Скомбінувавши найкращі особливості розподіленого та централізованого способів маршрутизації, як результат отримуємо мережу, в якій розподіл трафіку можливий по багатьом оптимальним маршрутам та ймовірний вихід з ладу центрального контролера не позбавляє мережу працездатності, вона продовжує роботу в звичайному режимі з розподіленим способом маршрутизації.

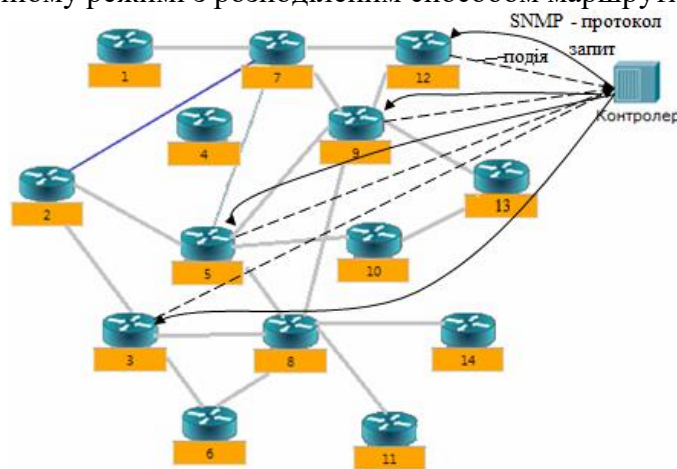


Рисунок 1 – Стан мережі після модифікації процесу маршрутизації

Висновок

Поруч з значними перевагами всіх протоколів динамічної маршрутизації, стає очевидно, що всі вони здійснюють пошук одного найкращого маршруту з мінімальною метрикою, тобто є одношляховими, або здійснюються балансування маршрутів у мережі з однаковою метрикою, що спричиняє максимальне використання знайденого найкращого або альтернативного шляху, їх перевантаження.

Виправити ситуацію через впровадження змін до самого протоколу є не доцільним, оскільки ця проблематика спостерігається у всіх протоколах динамічної маршрутизації, тому всеохоплюючим рішенням буде саме модифікація процесу маршрутизації без внесення змін в сам протокол маршрутизації. Такий варіант впливу дозволить універсально для всіх протоколів динамічної маршрутизації зменшити затримку передачі трафіку та збалансувати навантаження на мережу.

Список використаних джерел:

1. Олифер В., Олифер Н. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 5-е изд. – СПб.: Питер, 2016. – 992 с.
2. Таненбаум Э., Уэзеролл Д. Компьютерные сети. – 5-е изд. – СПб.: Питер, 2012. – 960 с.
3. Невдяев Л.М. Телекоммуникационные технологии. Англо-русский толковый словарь-справочник. Под редакцией Ю.М. Горностаева. Москва, 2002.
4. Кулаков Ю.А., Левчук А.В. Многопутевая маршрутизация в беспроводных сетях // Электроника и системы управления - М.: НАУ.2010 - № 4 (26) 2010. – с. 142-147.

ОСОБЛИВОСТІ ПОБУДОВИ БЛОКІВ ДЕКОДУВАННЯ ДЛЯ ТРС-ДЕКОДЕРУ

Крайник Ярослав, Перов Владислав

Чорноморський національний університет імені Петра Могили

Анотація

У даній роботі представлені особливості побудови деяких блоків реконфігурованого декодери Turbo-Product-кодів. Досліджені та розроблені блоки дозволяють організувати обробку кодових слів для різних кодів, тому декодер, що використовує такі блоки може виконувати декодування різних кодів без необхідності перепрограмування.

Abstract

This paper presents peculiarities of construction of decoding blocks for reconfigurable decoder of Turbo-Product codes. The main attention is devoted to the block of minimum search that is further used for test vector generation. The investigated blocks allow organizing codewords processing for different codes without reprogramming.

Вступ

Декодування Turbo-Product-кодів (англ. TP-codes – ТРС) є важливою складовою побудови інформаційних систем, що базуються на різних стандартах передачі даних (Wi-Fi, DVB-S2 та ін.). Такі системи можуть використовувати програмовні логічні інтегральні схеми (ПЛІС) для реалізації основних функцій по декодуванню. Реконфігуровний декодер на базі ПЛІС повинен проводити обробку кодів різної довжини без необхідності додаткового перепрограмування. Це дозволяє змінювати налаштування без необхідності проведення складних маніпуляцій, пов'язаних з даним процесом, завдяки чому сигнал може оброблюватись постійно, і можливим є збільшення пропускну здатності при використанні динамічних протоколів взаємодії. Саме тому проблема побудови реконфігурованого декодери є актуальною.

Декодування ТРС-кодів часто базується на алгоритмі Чейза [1] та використовує деякі стадії, що запропоновані у цьому алгоритмі. Важливим моментом у побудові декодерів з використанням даного алгоритму є пошук заданої кількості позицій, що містять мінімальні абсолютні значення у кодовому слові.

Основна частина

У роботі [2] представлена структура для пошуку трьох мінімальних значень у векторів кодового слова для коду, що має довжину 32 біти. Така структура використовується лише для декодування одного коду – (32, 26). У той час, як подача значень на інші коди або неможлива через недостатню кількість входів, або через може призвести до некоректних результатів.

Дана робота є продовження робіт [3, 4], у яких представлений повний алгоритм декодування ТРС-кодів, що використовує стадії алгоритму Чейза, а також представлена архітектура декодери на базі ПЛІС, яка враховує апаратні особливості цільової платформи для реалізації.

Для пошуку одного мінімуму може використовуватись каскад, який складається з блоків, представлених на рис. 1. Такий блок надає можливість у кінцевому результаті отримати одне значення та позицію, які дійсно є мінімальним (гарантовано не є більшими за інші значення у кодовому слові). Проте, у ході декодування ТРС-кодів необхідно знайти декілька мінімальних значень. Тому необхідно є організація кількох паралельних каскадів.

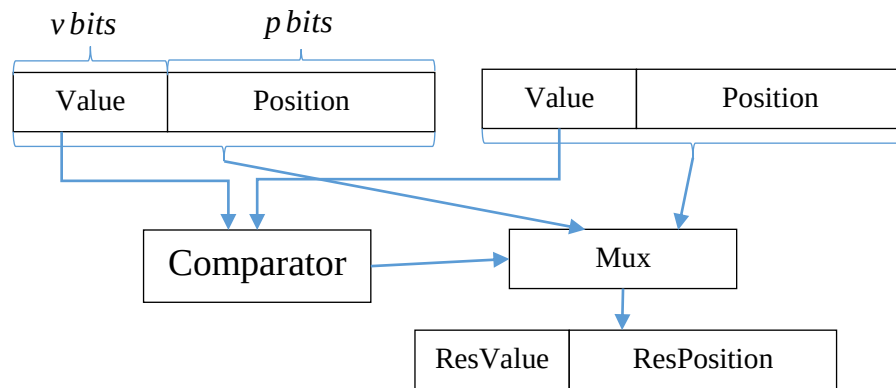


Рисунок 1 – Простий блок для організації каскаду пошуку одиничного мінімуму

Особливістю каскаду блоків порівняння є те, що значення, яке виявилось меншим з двох не відкидається одразу, а подається на вхід паралельного каскаду. Це забезпечує можливість, що обидва вхідні значення, подані на вхід такого елементу, у результаті можуть бути обрані в якості кінцевих мінімумів. Якби одне зі значень відкидалось одразу, то, за умови порівняння двох мінімумів, один з них був би втрачений і позиція мінімуму була б обчислена некоректно. Організація паралельного каскаду надає можливість відкинутому значенню пройти по паралельній гілці та потрапити до числа мінімумів. Значення, які подаються на вхід блоку є комбінацією з самого значення та його індексу. Під значення відводиться фіксована довжина, яка дорівнює v бітам, так само, як і під значення індексу, довжина якого має складати p біт. Для роботи такого каскаду необхідним є інший тип блоків, наведений на рис. 2.

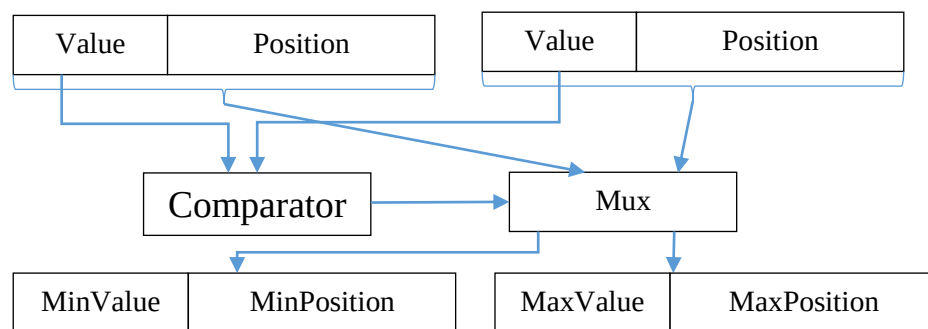


Рисунок 2 – Блок порівняння з двома виходами для організації паралельного каскаду

На відміну від попереднього блоку у даному випадку мультиплексор має два виходи. Один з них призначений для того, щоб обрати мінімальне значення. У випадку рівності значень перевага надається значенню з меншим індексом. На інший вихід подається значення, яке не було обране в якості мінімального.

На обох попередніх рисунках блоки представлені у вигляді регістрів. Також їх можна представити як блоки з відповідною кількістю входів та виходів, оскільки регістри можна розглядати як окремі компоненти, які використовуються для зв'язування блоків комбінаційної логіки.

Іншим важливим моментом у роботі блоку пошуку мінімумів є можливість обробки вхідних даних з різною довжиною кодового слова. Для цього на вхідні регістри, індекси яких перевищують довжину кодового слова, подається значення, яке відображає

максимальне абсолютне значення у системі. Також необхідно забезпечити, щоб усі результуючі значення позицій мінімумів входили до діапазону, що визначається довжиною коду – $[0, n - 1]$.

У випадку, коли значення поза діапазоном не були відсіяні (це можливо, наприклад, коли усі вхідні значення однакові або для деяких варіантів кодових слів), перевага має надаватись значенням з меншим індексом.

Послідовне з'єднання вищенаведених блоків у каскад з кількома рівнями дозволить однозначно визначити мінімальний елемент з найменшим індексом (за умови рівності значень). Проте, для роботи алгоритму на основі генерації списку тестових векторів одного значення недостатньо, тому, такі рівні можуть повторюватись лише до певного моменту, коли буде виділена певна кількість значень, серед яких і необхідно обрати кінцевий набір значень. Для цього, по аналогії з попередньою стадією, коли був визначений один мінімум, організуються блоки, які отримають на вхід результат блоків, які виконують пошук одиничного мінімуму у заданому наборі значень. У ході обробки використовуються обидва типи блоків.

У випадку, коли значення поза діапазоном не були відсіяні (це можливо, наприклад, коли усі вхідні значення однакові або для деяких варіантів кодових слів), перевага має надаватись значенням з меншим індексом.

У даній роботі описані особливості побудови блоків декодування ТР-декодеру, зокрема, блоків пошуку мінімумів. Розроблений блок призначений для використання у реконфігурованому декодері, який здатен проводити обробку різних кодів без необхідності перепрограмування пристрою (цільової платформи для реалізації є ПЛІС). Основна ідея його реалізації полягає у організації паралельного каскаду, що дозволяє значенням, які були відкинуті на одній з початкових стадій, потрапити до заданої кількості мінімальних значень. У каскаді використовуються два типи блоків, коректне з'єднання яких і забезпечує необхідну функціональність. На основі запропонованих у даній роботі положень реалізований декодер, який дозволяє проводити обробку кодових слів довжиною до 128 біт включно. Даний декодер реалізований на базі ПЛІС фірми Altera, яка надана для проведення тестування фірмою «Віаком» (м. Київ) мовою схемотехнічного опису VHDL.

Список використаних джерел:

1. Chase D. "A class of algorithms for decoding block codes with channel measurement information," IEEE Trans. Inform. Theory, vol IT-18, pp. 170–182, Jan. 1972.
2. Leroux C. Turbo-Product code decoder without interleaving resource: From parallelism exploration to high efficiency architecture / C. Leroux, C. Jegou, P. Adde, D. Gupta, M. Jezequel / Journal of Signal Processing Systems, Springer. – 2011, 64 (1). – pp.17-29.
3. Krainyk Y. Low-complexity high-speed soft-hard decoding for turbo-product codes / Y. Krainyk, V. Perov, M. Musiyenko – 2017 IEEE 37th International Conference on Electronics and Nanotechnology (ELNANO), 2017. – Kyiv, 2017. - pp. 471-474.
4. Krainyk Y. Hardware-Oriented Turbo-Product Codes Decoder Architecture / Krainyk Y., Perov V., Musiyenko M., Davydenko Ye. // Conference Proceedings of IEEE IDAACS-2017. - Bucharest, 2017. -pp. 151-154.

НАКОПИЧУВАЧІ ЕНЕРГІЇ ВІБРАЦІЇ ІoT-ПРИСТРОЇВ НА ОСНОВІ КОНСОЛЬНИХ П'ЄЗОЕЛЕМЕНТІВ

Мусієнко Максим, Корецька Олександра

Чорноморський національний університет імені Петра Могили

Анотація

В роботі розглянуті консольні п'єзоелектричні накопичувачі енергії вібрації. Досліджено використання біморфних та триморфних елементів, проведено експериментальні дослідження, отримані рекомендації щодо кількості використання п'єзоелементів та виконання консольних конструкцій.

Abstract

The console piezoelectric vibration energy storage devices are described in this paper. Using of bimorph and trimorph elements has been investigated, experimental studies have been carried out, recommendations on the number of use of piezoelements and the implementation of cantilever designs have been obtained.

Все більш поширене застосування ІoT пристроїв в житті людини вимагає розробки ефективних засобів живлення таких систем. Враховуючи те, що такі пристрої будуються на застосуванні мікроконтролерних пристроїв з низьким споживанням енергії, рішенням може бути використання альтернативних джерел енергії. Одним із таких джерел, що розглядається в роботі є вібрація, енергія від якої отримується завдяки застосуванню п'єзоелектричних перетворювачів.

У разі розробки систем збору енергії від вібрації найбільш прийнятним є використання п'єзоелементів, як перетворювачів механічних коливань в електричну енергію [1]. Найбільш придатним для вирішення зазначеного завдання є використання консольних п'єзоперетворювачів, коли вібрація пристрою призводить до коливань вільного кінця консольного елемента, де і закріплений п'єзоелектричний перетворювач. Розміри таких коливань становлять доли міліметра [2] і цілком задовольняють умовам неруйнування кераміки і необхідного впливу на п'єзоелемент.

При побудові консольних п'єзоперетворювачів важливим питанням є розробка модуля накопичення і контролю заряду, який підключається безпосередньо до виходу п'єзоперетворювача.

Одним з таких рішень є використання перетворювачів Volture з платами накопичення енергії [2]. Незважаючи на деякі позитивні фактори, недоліком зазначеного рішення є порівняно низька чутливість п'єзоелементів, яка характеризується використанням в конструкції мономорфних п'єзоперетворювачів.

Метою роботи є підвищення рівня накопичення енергії вібрації за рахунок розробки конструкції консольних п'єзоелектричних перетворювачів вібрації в електричну енергію з підвищеним рівнем накопичення енергії.

Як відомо, найбільшу чутливість мають п'єзоперетворювачі в біморфному чи триморфному виконанні, коли поєднується використання п'єзоелемента з металевою пластиною. В разі використання асиметричних біморфних п'єзоперетворювачів чутливість збільшується у 10-20 разів у порівнянні з використанням мономорфних елементів [1].

Враховуючи складність теоретичних досліджень п'єзокерамічних перетворювачів, тим більше у поліморфному виконанні, в роботі більшість результатів отримано завдяки експериментальним дослідженням.

При розробці експериментального стенда були розглянуті та враховані наступні питання: вибір типу п'єзоелементів; металевих пластин; конструкцій консольних

поліморфних п'єзоперетворювачів; схеми накопичувача енергії; імітації механічного впливу; побудова лабораторного стенду.

Конструкція експериментальної установки показана на рис. 1.



Рисунок 1 - Конструкція експериментальної установки

За допомогою установки були досліджені різні варіанти виконання конструкції консольних п'єзоперетворювачів накопичення енергії вібрації: біморфні та триморфні, різні схеми під'єднання п'єзоелементів, їх кількість та тип. В результаті проведених експериментів з'ясовано, що найбільшу енергоефективність мають конструкції з двома біморфними п'єзоелементами, що закріплені на протилежних сторонах металевої пластини. Серед розглянутих біморфних п'єзоелементів найбільшу чутливість мають елементи 7BV-20-6C.

Висновки. В роботі розглянуті консольні п'єзоелектричні накопичувачі енергії, а саме – питання конструктивного виконання таких елементів для збільшення чутливості перетворювачів. Досліджено використання біморфних та триморфних елементів, проведено експериментальні дослідження, отримані рекомендації щодо кількості використання п'єзоелементів та виконання консольних конструкцій. В результаті проведених експериментів з'ясовано, що найбільшу енергоефективність мають конструкції з двома біморфними п'єзоелементами, що закріплені на протилежних сторонах металевої пластини.

Список використаних джерел:

1. Шарапов В.М. Мусиенко М.П., Шарапова Е.В. Пьезоэлектрические датчики : монография / Под ред. В.М.Шарапова. – Москва: Техносфера, 2006. - 632 с. – ISBN 5-94836-100-4.
2. Бугаев В.И. Сборщики энергии вибраций от Mide Technology приходят на смену батарейкам / В.И.Бугаев, В.А.Дидук, М.П.Мусиенко // Новости электроники. Москва. – № 7(141). 2015. С. 23 – 27.. – Львів : ВЦ ЛНУ ім. І. Франка, 2007. – 584 с.



ОДИНАДЦЯТА МІЖНАРОДНА КОНФЕРЕНЦІЯ
ІОН - 2018
ІНТЕРНЕТ-ОСВІТА-НАУКА-2018



СЕКЦІЯ D. МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ



THE ELEVENTH INTERNATIONAL
CONFERENCE
IES-2018
INTERNET-EDUCATION-SCIENCE - 2018



SECTION D. MATHEMATICAL MODELING



ОДИНАДЦАТАЯ МЕЖДУНАРОДНАЯ
КОНФЕРЕНЦИЯ
ИОН-2018
ИНТЕРНЕТ– ОБРАЗОВАНИЕ – НАУКА 2018



**СЕКЦІЯ D. МАТЕМАТИЧЕСКОЕ
МОДЕЛИРОВАНИЕ**



О ПАРАМЕТРИЗАЦИИ ИНТЕРПРЕТАЦИЙ МНОГООБРАЗИЙ

Мамедов Октай, Мехтиев Хиджран

Бакинский Государственный Университет

Аннотация

В данной работе рассматривается некоторая параметризация семейства локальных интерпретаций многообразий и одно обобщение почти-единодушных термов.

Abstract

Here we consider some parameterization of local interpretations of varieties and a generalization of near unanimity terms.

Многообразие есть класс однотипных алгебр, определяемый некоторым множеством тождеств; например, группы, кольца, модули над фиксированным кольцом, решётки, булевы алгебры. Многообразие можно охарактеризовать и как класс алгебр, замкнутый относительно взятия гомоморфных образов, подалгебр и прямых произведений. Хорошо известно, что все алгебры в многообразии групп, колец, модулей обладают перестановочными конгруэнциями, т.е. реляционное произведение конгруэнций коммутативно. Ещё Дедекиндом было показано, что перестановочность влечет модулярность решеток конгруэнций. А.И.Мальцев доказал, что все алгебры многообразия имеют перестановочные конгруэнции тогда и только тогда, когда существует терм $p(x, y, z)$ удовлетворяющий тождествам $p(x, z, z) = x$ и $p(x, x, z) = z$. Этот терм называется термом Мальцева и условия такого типа (т.е. существование термов, удовлетворяющих некоторым тождествам или импликациям) называются мальцевскими. Мы будем рассматривать многообразия с хотя бы одной индивидуальной константой (при этом не требуется её вхождение в сигнатуру). Для сравнения взаимных «сил» многообразий удобным оказалось понятие (глобальной) интерпретации многообразий, введённое У.Нейманом. Возникающая при этом решётка (носителем которой является класс) $\mathcal{L}$ интерпретаций широко изучалась Гарсией и Тейлором [3]; мальцевские условия оказались фильтрами этой решётки. Локальная интерпретация, рассмотренная Я.Мыцельским, также привела к решётке (носителем которой является множество) эквациональных глав $\mathcal{LEC}$ [4]. Здесь мы связываем эти две интерпретации (решётки $\mathcal{L}$ и $\mathcal{LEC}$) некоторой параметризацией; что можно рассматривать как ответ на один вопрос Мыцельского ([3], стр.120). В конце работы рассмотрено некоторое обобщение широко известных почти единодушных термов и установлены ряд их свойств. Сведения по универсальной алгебре можно найти в [2].

Пусть $\mathcal{V}$ есть многообразие типа τ . Если типа τ' содержится в τ , $\tau' \subseteq \tau$, то можно образовать редукт $\mathcal{V}'$ (типа τ') многообразия $\mathcal{V}$ так: $\mathcal{V}' = \text{var}(\mathcal{A}|_{\tau'} : \mathcal{A} \in \mathcal{V})$.

Определение Для многообразий $\mathcal{V}$ и $\mathcal{U}$ (возможно, разнотипных) и для неконечного кардинала k $\mathcal{U}$ редукт- k -локально интерпретируемо в $\mathcal{V}$ (это обозначаем так: $\mathcal{U} \trianglelefteq_k \mathcal{V}$), если любой редукт $\mathcal{U}'$ с типом мощности $< k$ интерпретируемо (в обычном, т.е. глобальном смысле) в $\mathcal{V}$.

Отношение $\trianglelefteq_k$ является квазипорядком на классе всех многообразий. Так как пересечение любого квазипорядка со своим обращением является эквивалентностью, то $\trianglelefteq_k$ определяет частичный порядок $\leq_k$ на семействе всех классов эквивалентности. Таким образом, если положить $\mathcal{U} \bowtie_k \mathcal{V} \Leftrightarrow \mathcal{U} \trianglelefteq_k \mathcal{V} \text{ \& } \mathcal{V} \trianglelefteq_k \mathcal{U}$, то $\bowtie_k$ будет эквивалентностью на классе всех многообразий и $\leq_k$ есть частичный порядок на классах $\bowtie_k$ -эквивалентности. Класс $\bowtie_k$ -эквивалентности, содержащий $\mathcal{U}$, обозначим $[\mathcal{U}]_{\bowtie_k}$ и назовём его эквациональной k -строфой многообразия $\mathcal{U}$. Запись $[\mathcal{U}]_{\bowtie_k} \leq_k [\mathcal{V}]_{\bowtie_k}$ означает в частности, что

$\mathcal{U} \sqsubseteq_k \mathcal{V}$. Семейство всех этих классов $\mathbb{M}_k$ -эквивалентности обозначим $\mathbf{LEkV}$; итак, $\mathbf{LEkV} = ([\mathcal{U}]_{\mathbb{M}_k} : \mathcal{U} \text{ есть многообразие})$. Пусть α - произвольная k -строфа, задаваемая многообразием $\mathcal{U}$; т.е. $\alpha = [\mathcal{U}]_{\mathbb{M}_k}$. Рассмотрим семейство всех редуктов многообразия $\mathcal{U}$, мощности типов которых $< k$. Это семейство однозначно определяет строфу α . Всякое многообразие этого семейства интерпретируемо в $\mathcal{U}$ и каждое такое многообразие имеет тип мощности $< k$. При ОКГ различных таких многообразий $\leq k$. Тогда дизъюнктивное объединение этих многообразий имеет тип мощности $\leq 2^k$ и оно редукт k -локально интерпретируемо в $\mathcal{U}$ и наоборот. Итак, эквациональная k -строфа многообразия $\mathcal{U}$ имеет представитель с типом мощности $\leq 2^k$ и поэтому $|\mathbf{LEkV}| \leq 2^{2^k}$. Легко понять, множество $\mathbf{LEkV}$, частично упорядоченное отношением $\leq_k$, имеет нуль $\mathbf{0} = [x = x]_{\mathbb{M}_k}$ (эквациональная k -строфа многообразия всех множеств) и единицу $\mathbf{1} = [x = y]_{\mathbb{M}_k}$ (эквациональная k -строфа тривиального многообразия).

Теорема Для любого кардинала k частично упорядоченное множество

$$\mathbf{LEkV} = \langle \mathbf{LEkV}, \leq_k \rangle$$

является полной решёткой, в которой для сигнатурно разъединённых многообразий $\mathcal{U}$ и $\mathcal{V}$ типов τ и, соответственно, σ , пересечение определяется так: $[\mathcal{U}]_{\mathbb{M}_k} \wedge [\mathcal{V}]_{\mathbb{M}_k} = [\mathcal{W}]_{\mathbb{M}_k}$, где $\mathcal{W}$ имеет тип $\tau \cup \sigma \cup \{\cdot\}$ и задаётся тождествами (прямоугольная связка $\mathcal{U}$ и $\mathcal{V}$):

- 1) $x \cdot x = x$,
- 2) $(x \cdot y) \cdot (u \cdot v) = x \cdot v$,
- 3) $f(x_1 \cdot y_1, \dots, x_m \cdot y_m) = f(x_1, \dots, x_m)$,
- 4) $g(x_1 \cdot y_1, \dots, x_n \cdot y_n) = g(y_1, \dots, y_n)$,
- 5) $s \cdot y = t \cdot y$,
- 6) $x \cdot u = x \cdot v$,

где $f \in \tau$, $g \in \sigma$, $s = t$ пробегает по всем тождествам $\mathcal{U}$ и $u = v$ пробегает по всем тождествам $\mathcal{V}$.

Доказательство. Пусть $\{\mathcal{V}_i : i \in I\}$ некоторое множество многообразий, причём каждое $\mathcal{V}_i$ имеет тип τ_i и систему тождеств Σ_i . Рассмотрим дизъюнктивное разъединение типов τ_i^0 и соответствующие им системы тождеств Σ_i^0 . Пусть $\coprod\{\mathcal{V}_i : i \in I\}$ есть многообразие типа $\cup\{\tau_i^0 : i \in I\}$ с системой тождеств $\cup\{\Sigma_i^0 : i \in I\}$. Тогда понятно, что эквациональная k -строфа многообразия $\coprod\{\mathcal{V}_i : i \in I\}$ есть $\vee\{[\mathcal{V}_i]_{\mathbb{M}_k} : i \in I\}$. Кроме того, как отмечено выше, в частично упорядоченном множестве $\langle \mathbf{LEkV}, \leq_k \rangle$ есть нуль и единица; это устанавливает полноту решётки $\mathbf{LEkV}$. Сначала докажем, что $\mathcal{W}$ редукт- k -локально интерпретируемо в $\mathcal{U}$ и в $\mathcal{V}$; затем покажем, что если некоторое многообразие $\mathcal{Z}$ редукт- k -локально интерпретируемо и в $\mathcal{U}$ и в $\mathcal{V}$, то $\mathcal{Z}$ редукт- k -локально интерпретируемо в $\mathcal{W}$.

Для доказательства первого утверждения достаточно проинтерпретировать операцию $\cdot$ как проекцию $\pi_2^0(x, y) = x$, все операции $g \in \sigma$ как одну и ту же константу многообразия $\mathcal{U}$, а все операции $f \in \tau$ как те же самые операции в $\mathcal{U}$. Отсюда видно, что $\mathcal{W}$ будет редукт- k -локально интерпретируемо в $\mathcal{U}$. Точно так же, беря вместо π_2^0 проекцию $\pi_2^1(x, y) = y$, получаем интерпретируемость $\mathcal{W}$ в $\mathcal{V}$.

Докажем второе утверждение. Рассмотрим редукт $\mathcal{Z}'$ многообразия $\mathcal{Z}$ такой, что $|\text{тип}(\mathcal{Z}')| < k$. По условию, $\mathcal{Z}'$ интерпретируемо и в $\mathcal{U}$ и в $\mathcal{V}$. Пусть h есть некоторая операция многообразия $\mathcal{Z}'$. Положим $h_0 = h_{\mathcal{U}} \cdot h_{\mathcal{V}}$, где $h_{\mathcal{U}}$ и $h_{\mathcal{V}}$ есть интерпретация h в операциях, соответственно, $\mathcal{U}$ и $\mathcal{V}$. Тогда семейство $\{h_0 : h \text{ есть операция } \mathcal{Z}'\}$ определяет интерпретацию $\mathcal{Z}'$ в $\mathcal{U}$. Надо проверить, что для любого терма t в языке $\mathcal{Z}'$ $t_0 = t_{\mathcal{U}} \cdot t_{\mathcal{V}}$.

Это показывается обычной индукцией по длине терма: если t переменная, то тождество 1) обеспечивает справедливость равенства $t_0 = t_u \cdot t_v$; если же $t = f(t^1, \dots, t^r)$, то

$$\begin{aligned} t_0 &= f_0(t_0^1, \dots, t_0^r) = f_u(t_u^1 \cdot t_v^1, \dots, t_u^r \cdot t_v^r) \cdot f_v(t_u^1 \cdot t_v^1, \dots, t_u^r \cdot t_v^r) = \\ &= f_u(t_u^1, \dots, t_u^r) \cdot f_v(t_v^1, \dots, t_v^r) = t_u \cdot t_v. \end{aligned}$$

Предположим теперь, что $t = t'$ есть некоторое тождество многообразия $\mathcal{Z}'$. Так как $\mathcal{Z}'$ интерпретируемо и в $\mathcal{U}$ и в $\mathcal{V}$, то $t_u = t'_u$ является тождеством многообразия $\mathcal{U}$, а $t_v = t'_v$ является тождеством многообразия $\mathcal{V}$. Из тождеств 5) и 6) вытекает, что $t_u \cdot y = t'_u \cdot y$ и $x \cdot t_v = x \cdot t'_v$. Тогда $t_u \cdot t_v = (t_u \cdot y) \cdot (x \cdot t_v) = (t'_u \cdot y) \cdot (x \cdot t'_v) = t'_u \cdot t'_v$.

С другой стороны $t_u \cdot t_v$ равно t_0 (т.е. интерпретации терма t в $\mathcal{U}$), и $t'_u \cdot t'_v = t'_0$. Итак многообразию $\mathcal{W}$ удовлетворяет тождеству $t_0 = t'_0$ и теорема доказана.

Предложение Всякое конечнобазированное многообразие конечного типа является компактным элементом решётки $\mathcal{LEKV}$.

Доказательство Пусть конечнобазированное $\mathcal{V}$ имеет конечный тип и пусть

$$[\mathcal{V}]_{\aleph_k} \leq V\{[\mathcal{V}_i]_{\aleph_k} : i \in I\}.$$

Так как $V\{[\mathcal{V}_i]_{\aleph_k} : i \in I\} = [\coprod\{\mathcal{V}_i : i \in I\}]_{\aleph_k}$, то конечный тип многообразия $\mathcal{V}$ можно проинтерпретировать в не более чем конечном числе многообразий $\mathcal{V}_i$. Теперь дизъюнктивное объединение этого конечного числа многообразий даёт требуемое конечное подпокрытие для $[\mathcal{V}]_{\aleph_k}$.

По теореме в сигнатуру пересечения добавляется лишь одна бинарная операция; поэтому верно

Предложение Пересечение компактных элементов решётки $\mathcal{LEKV}$ является компактным элементом.

Предложение В решётке $\mathcal{LEKV}$ есть скачки; в частности, на вершине есть скачок.

Доказательство Рассмотрим любую компактную эквациональную k -строфу α . Объединение некоторой максимальной цепи строф, строго меньших α , опять будет строго меньше α . Поскольку в дизъюнктивном объединении многообразий всегда выполняется некоторое нетривиальное тождество, то и на вершине решетки $\mathcal{LEKV}$ есть скачок:

$$V\{\alpha \in \mathcal{LEKV} : \alpha <_k \mathbf{1}\} <_k \mathbf{1}.$$

Предложение В решётке $\mathcal{LEKV}$ для любых $\alpha, \beta >_k \mathbf{0}$ имеем: $\alpha \wedge \beta >_k \mathbf{0}$.

Доказательство. В противном случае новая бинарная операция $\{\cdot\}$ из условия теоремы 1 должна быть проинтерпретирована либо как проекция, либо же некоторой константой, что невозможно.

В ([3]), в решётке $\mathcal{L}$ интерпретационный тип многообразия всех алгебр с одной константой обозначено через $\mathcal{C}$.

Предложение Для любого k существует гомоморфизм из интервала $[\mathcal{C}, \mathbf{1}]$ решётки $\mathcal{L}$ на решётку $\mathcal{LEKV}$.

Доказательство Для доказательства сопоставим каждому многообразию $\mathcal{V}$ его эквациональную k -строфу $[\mathcal{V}]_{\aleph_k}$. Это отображение сюръективно и сохраняет решёточные операции.

Заметим также, что в решётке $\mathcal{LEKV}$ семейство всех таких многообразий $\mathcal{V}$, что мощность типа $\mathcal{V}$ меньше k , является «обобщенно» компактным в том смысле, что если супремум некоторого семейства покрывает $\mathcal{V}$, то существует подсемейство мощности меньше k , которое также покрывает $\mathcal{V}$. Кроме того, эти «обобщенно» компактные элементы сами образуют подрешётку.

В завершении рассмотрим некоторое обобщение почти-единодушных термов, введённых в [1]. Пусть A произвольная алгебра и $n > 2k > 0$. Терм $t(x_0, \dots, x_{n-1})$ назовём k -почти-единодушным для A , если A удовлетворяет следующим тождествам:

$$\{x = t(\varphi(0), \dots, \varphi(n-1)) \mid \forall \varphi \in \{x, y\}^n \ \& \ 0 \leq |\varphi^{-1}(y)| \leq k\};$$

таким образом, не более k аргументных мест заполнены y -ами, а все остальные места заполнены x -ами. При $k = 1$ получаем обычный почти единодушный терм. Терм t есть k -почти-единодушный терм для многообразия $\mathcal{V}$, если он является k -почти-единодушным для каждой алгебры из $\mathcal{V}$. Пусть $\mathcal{E}_{n,k}$ обозначает многообразие всех алгебр с одной-единственной n -арной операцией t , удовлетворяющей указанным тождествам. Очевидно, каждый n -арный k -почти-единодушный терм является $(k-1)$ -почти-единодушным термом; в частности каждый k -почти-единодушный терм является почти-единодушным термом. Следовательно $\mathcal{E}_{n,k}$ является конгруэнц-дистрибутивным многообразием. Например, для многообразия решёток 5-арный терм

$$t(x, y, z, t, u) := (x \vee y \vee z) \wedge (x \vee y \vee t) \wedge (x \vee y \vee u) \wedge (x \vee z \vee t) \wedge (x \vee z \vee u) \wedge \\ (x \vee t \vee u) \wedge (y \vee z \vee t) \wedge (y \vee z \vee u) \wedge (y \vee t \vee u) \wedge (z \vee t \vee u)$$

является 2-почти-единодушным и потому $\mathcal{E}_{5,2}$ интерпретируемо в многообразии всех решёток.

Точно также как в [6], теорема 1.2, можно показать, что мальцевское семейство (идемпотентных) многообразий, обладающих k -почти-единодушным термом, является робастным, т.е. если $\mathcal{V}$ и $\mathcal{W}$ однотипные идемпотентные многообразия, обладающие k -почти-единодушными термами арностей n и, соответственно, m , то $H(\mathcal{V} \circ \mathcal{W})$ (многообразие, порождённое мальцевским произведением) также обладает k -почти-единодушным термом (арности nm ; более того, так же, как в [5], теорема 2.2, (легко проверить, что) арности $n + m - 1$). Согласно [7], в решётке интерпретаций $\mathcal{L}$ фильтр многообразий, обладающих почти-единодушным термом, является пересечением двух больших фильтров. Нетрудно проверить этот результат для многообразий, обладающих k -почти-единодушным термом. Таким образом, многообразие $\mathcal{V}$ имеет n -арный k -почти-единодушный терм тогда и только тогда, когда $\mathcal{E}_{n,k} \leq \mathcal{V}$. Так же, как в [7] легко показать, что $\mathcal{E}_{n+1,k} < \mathcal{E}_{n,k}$, т.е. фильтр $\mathcal{E}_{\omega,k}$ всех многообразий, обладающих k -почти-единодушными термами не является главным фильтром в $\mathcal{L}$. Более того, $\mathcal{E}_{\omega,k}$ является разложимым фильтром в $\mathcal{L}$ (конечно, $\mathcal{E}_{\omega,k}$ содержится в фильтре всех конгруэнц-дистрибутивных многообразий). Сформулируем эти факты в виде теоремы.

Теорема. Мальцевское семейство всех многообразий, обладающих k -почти-единодушным термом является робастным. Кроме того, фильтр $\mathcal{E}_{\omega,k}$ всех многообразий, обладающих k -почти-единодушными термами является разложимым (в пересечение) фильтром в $\mathcal{L}$.

Список использованных источников:

1. Baker K.A., Pixley A.F. Polynomial interpolation and the Chinese remainder theorem for algebraic systems// Math. Z., 1975, 143, p. 165-174.
2. Bergman C. Universal Algebra. London: CRC Press, 2012, xii+306p.
3. Garcia O.C., Taylor W. The lattice of interpretability types of varieties. Memoirs of the Amer. Math. Soc., No 305, Providence, R.I., 1984, vi+125p.
4. Mycielski J., Taylor W. Remarks and problems on a lattice of equational chapters// Algebra Univers., 1986, 23, p. 24-31.
5. Campanella M., Conley S., Valeriote M. Preserving near unanimity terms under products// Algebra Univers. 2016, 76, p. 293-300.
6. Freese R., McKenzie R. Maltsev families of varieties closed under join or Maltsev product // Algebra Univers. 2017, 77, p. 29-50.
7. Sequeira L. Near-unanimity is decomposable// Algebra Univers. 2003, 50, p. 157-164.

МУРАШИНИЙ АЛГОРИТМ КЛАСТЕРИЗАЦІЇ

Горносталь Олександр, Дорогий Ярослав

Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»

Анотація

В роботі розглянуто питання створення алгоритму кластеризації на базі мурашиних колоній для задачі розпізнавання мови. Створений алгоритм інтегрований в аудіовізуальну систему розпізнавання мови і протестований в шести режимах розпізнавання.

Abstract

The paper considers the problem of creating an algorithm for clustering based on ant colonies for the problem of speech recognition. The created algorithm is integrated into the audio-visual speech recognition system and tested in six modes of recognition.

Вступ

Даний алгоритм використовується для вирішення проблем оптимізації. Наприклад, його активно застосовують для вирішення:

- задачі комівояжера [1];
- задачі кластеризації даних [2-3];
- задачі текстового пошуку [4-5].

Мурашиний алгоритм кластеризації

Алгоритм можна пояснити наступними 4-ма правилами:

1. Мурахи шукають їжу і різні шляхи для її пошуку.
2. Кожна мураха виділяє феромон.
3. Мурах приналежить феромон, тому шляхи з більшою кількістю феромону є більш інтенсивними.
4. Феромон з часом випаровується. Відповідно, падає інтенсивність шляхів з меншою кількістю феромону.

Алгоритм складається з наступних кроків:

1. Визначається початкова кількість феромону для кожного елементу таблиці феромонів за формулою 1:

$$\tau_0 = \frac{f_{fit}(S_{best})}{N} \quad (1)$$

де

f_{fit} - фітнес-функція;

S_{best} - найкращий розв'язок;

N - розмірність задачі.

2. Обчислюється ймовірнісна функція вибору того чи іншого шляху пошуку (2):

$$P_k(r,s) = \left\{ \frac{[\tau(r,s)]^\alpha \cdot [\eta(r,s)]^\beta}{\sum_{\mu \in J_k(\tau)} [\tau(r,s)]^\alpha \cdot [\eta(r,s)]^\beta} \right\} \quad (2)$$

де

$P_k(r,s)$ - ймовірність пересування мурахи k з точки r в точку s ;

$\tau(r,s)$ - кількість феромону на шляху;

$\eta(r, s)$ - фітнес-функція пересування шляхом;

α, β - коефіцієнти, що залежать від типу конкретної задачі;

$J_k(r)$ - множина точок пересування та r - остання точку, яку відвідала мураха.

3. Обчислюються нові локальні значення таблиці феромонів, що запобігає руху мурах одними і тими ж шляхами (3):

$$\tau(r, s) = (1 - \sigma) \cdot \tau(r, s) + \sigma \cdot \tau_0 \quad (3)$$

де

σ - локальний коефіцієнт оновлення.

4. Обчислюються нові глобальні значення таблиці феромонів (4):

$$\tau(r, s) = (1 - \rho) \cdot \tau(r, s) + \rho \cdot \Delta\tau(r, s) \quad (4)$$

де

ρ - глобальний коефіцієнт оновлення;

$$\Delta\tau(r, s) = \begin{cases} f_{fit}(S_{best}) & \text{if } (r, s) \in S_{best} \\ 0 & \text{otherwise} \end{cases} \quad (5)$$

Кластеризація – процес поділу об'єктів або даних на класи за якимось критерієм. В якості критерію виступає значення відстані між об'єктами, яке розраховується відповідно до обраного типу цієї відстані: Евклідова, Махаланобіса або відстань міських кварталів Мінковського. Центри кластерів є змінними, відносно яких приймається рішення і які можна отримати шляхом мінімізації Евклідової відстані між всіма елементами навчальної вибірки. Мета кластеризації – мінімізація суми відстаней міських кварталів за всіма N зразками тренувальної вибірки і віднесення їх до одного з K кластерів. Тобто, маємо (6):

$$D(x_i, c_k) = \sum_k \sum_{i=1}^N (x_i - c_k) \quad (6)$$

де

N - кількість зразків мови;

K - кількість кластерів.

Центри кластерів обчислюються за формулою (7):

$$c_k = \sum_{i \in c_k} \frac{x_i}{n_k} \quad (7)$$

Цільова функція для зразка i обчислюється за формулою (8):

$$G_i = \frac{1}{S_{tr}} \sum_{j=1}^{S_{tr}} d(x_j, m_i) \quad (8)$$

де

S_{tr} - кількість зразків мови в навчальній вибірці;

m_i - клас, до якого належить зразок вибірки.

Експериментальні дослідження

Запропонований алгоритм використаний для покращення роботи аудіовізуальної система розпізнавання, представленої в [6]. Побудована система була протестована на базі цифр від 0 до 9. Кожна цифра в базі даних повторюється десять разів кожним з десяти мовців. Для кожного оратора дев'ять прикладів кожної цифри використано для навчання, а приклад, що залишився, використано для тестування.

Усереднені результати розпізнавання для шести режимів розпізнавання представлені в таблиці 1. Режими розпізнавання наступні:

- тільки аудіо;
- тільки аудіо з використанням мурашиного алгоритму кластеризації;
- тільки відео;
- тільки відео з використанням мурашиного алгоритму кластеризації;
- аудіовізуальне розпізнавання;

– аудіовізуальне розпізнавання з використанням мурашиного алгоритму кластеризації.

Таблиця 1 – Усереднені результати розпізнавання

Класифікатор	Результат розпізнавання
ПММ (тільки аудіо)	92%
ПММ (тільки аудіо) + МАК	93%
ПММ (тільки відео)	51%
ПММ (тільки відео) + МАК	57%
ЗПММ (аудіовізуальна система)	98%
ЗПММ + МАК	98,5%

Висновки

Для режиму розпізнавання мови «лише аудіо» вектори акустичного спостереження (15 MFCC коефіцієнтів, які визначені з вікна 20 мс) моделюються з використанням ПММ. Для розпізнавання в режимі «аудіо-відео» використана ЗПММ з п'ятьма станами для зв'язаних вузлів як в аудіо-, так і в відеопотоках, без зворотних переходів і трьома змішуваннями на кожний стан. Експериментальні результати показали, що рівень розпізнавання аудіовізуальної мови на основі ЗПММ з використанням МАК збільшується на 43,5% щодо розпізнавання мови в режимі «тільки аудіо». У порівнянні з багатопотоковою ПММ [7] запропонований варіант ЗПММ для аудіовізуальної системи розпізнавання показує кращі результати.

Список використаних джерел:

1. Coello C.A. Evolutionary algorithms for solving multi-objective problems [Текст] / C.A.Coello and others // Springer, 2007.
2. Lumer E.D. Diversity and adaptation in populations of clustering ants [Текст] / E. D. Lumer and B. Faieta // Proceedings of the third international conference on Simulation of adaptive behavior: from animals to animats 3: from animals to animats 3. – MIT Press, 1994.
3. Tsai C.F. ACODF: a novel data clustering approach for data mining in large databases [Текст] / C. F. Tsai, et al. // Journal of Systems and Software. – 2004. – Vol. 73, Is. 1. – pp. 133-145.
4. Handl J. Improved ant-based clustering and sorting in a document retrieval interface [Текст] / J. Handl and B. Meyer // Parallel Problem Solving from Nature—PPSN VII. Springer Berlin Heidelberg, 2002. – pp. 913-923.
5. Hoe K.M. Homogeneous ants for web document similarity modeling and categorization [Текст] / K. M. Hoe, et al. // Ant Algorithms, Springer Berlin Heidelberg, 2002. – pp. 256-261.
6. Горносталь А.Н. Розробка аудіовізуальної системи розпізнавання мови [Текст] / А.Н.Горносталь, Я.Ю.Дорогий // Scientific Journal «Science Rise». – 2017. - №12(41). – с. 42-47.
7. Neti C. Audio-visual speech recognition [Текст] : Final Workshop 2000 Report, Center for Language and Speech Processing / C. Neti, G. Potamianos, J. Luetttin et al. // The Johns Hopkins University, Baltimore. – 2000.

STUDY OF COEFFICIENTS OF RHEUMATOID ARTHRITIS MODEL

Odisharia, Kakhaber

St.Andrewthe First-Call Georgian University of the Patriarchate of Georgia, Tbilisi, Georgia

Abstract

Mathematical models of diseases caused by immune disorders allow to solve specific questions related to the disease immune dynamics and choice of relevant treatment. Here we consider the model of rheumatoid arthritis and discuss the evaluation of the coefficients of the model of their influence on the solution.

Анотация

Математические модели, описывающие болезни вызванные иммунным нарушениями, позволяют решать конкретные вопросы, связанные с динамикой болезни и выбора соответствующего лечения. Здесь мы рассматриваем модель ревматоидного артрита и обсуждаем вопросы оценки коэффициентов модели их влияния на решение.

Introduction

The model based investigation of diseases is a complex and evolving field. We have introduced new mathematical model of immune mediated disorders [4]. The model describes progression of rheumatoid arthritis and the effect of treatment.

Rheumatoid arthritis is a systematic autoimmune disease characterized by inflammation of the joints, bone loss and cracking cartilage tissue [1, 2]. The disease is caused by violation of balance between B, regulatory T and helper T lymphocytes that are subset of blood cells. In rheumatoid arthritis B lymphocytes goes beyond the norm and along with T helper cells produces antibodies to the cell of the cartilage resulting in its structural destruction [3]. Regulatory T cells due to their reduced quantities fail to suppress B cells. The immune system fails to properly distinguish between “self” and “non-self” and attacks part of the body inducing strong inflammatory response against self-substances.

Mathematical model

Now we improve the model by adding treatment component. We concede “Tocilizumab” as drug for treatment. Mathematical model of rheumatoid arthritis with drug therapy is given below:

$$\frac{dJ(t)}{dt} = -a_1 J(t)(B(t) - B^{norm}) \quad (1)$$

$$\frac{dB(t)}{dt} = r_1 B(t)(1 - b_1 B(t)) + c_1 B(t)T_h(t) - d_1 B(t)T_{reg}(t) \quad (2)$$

$$\frac{dT_h(t)}{dt} = r_2 T_h(t)(1 - b_2 T_h(t)) - k_1(1 - e^{-m_1 u(t)})T_h - k_2(1 - e^{-m_2 u(t)})T_h \quad (3)$$

$$\frac{dT_{reg}(t)}{dt} = s_2 - d_2 T_{reg}(t) + k_2(1 - e^{-m_2 u(t)})T_h \quad (4)$$

$$\frac{du(t)}{dt} = -d_3 u(t) \quad (5)$$

$J(t)$ denotes cartilage cell population at time t moment, $B(t)$ – B cell population at time t , $T_h(t)$ and $T_{reg}(t)$ – helper and regulatory T cells population, accordingly. Equations (1) and (2) are the same as for model without drug therapy. In equation (3) and (4) drug component is added. Equation (5) determines amount of the drug in the blood at time t . Drug action is the following: drug affects helper T and regulatory T cells. It kills part of helper T cells and turns other part of helper T cells into regulatory T cells. As a result, population of helper T cells is

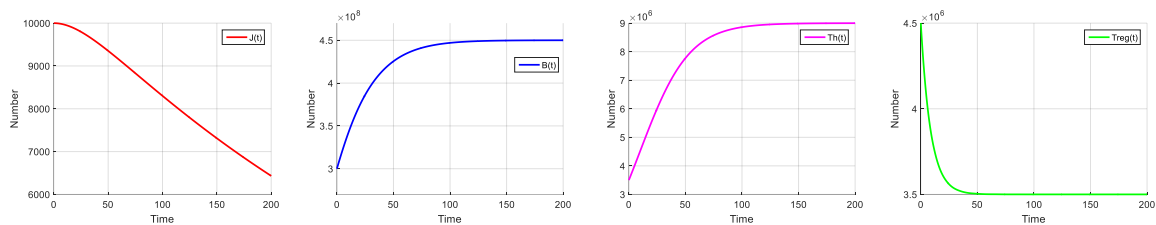
decreased and population of regulatory T cells is increased. After a certain period B lymphocytes should start to decrease. The next assumptions are made about the drug:

1. The drug is completely eliminated (metabolism and excretion) from the blood.
2. The drug is directly administrated by an intravenous injection and is immediately completely distributed into the blood stream.
3. Amount of the drug in the blood after injection is given by exponential reduce model pattern: equation (5).
4. Fractional cells kill for an amount of drug u is given by exponential model

$$F(u) = k(1 - e^{-mu})$$

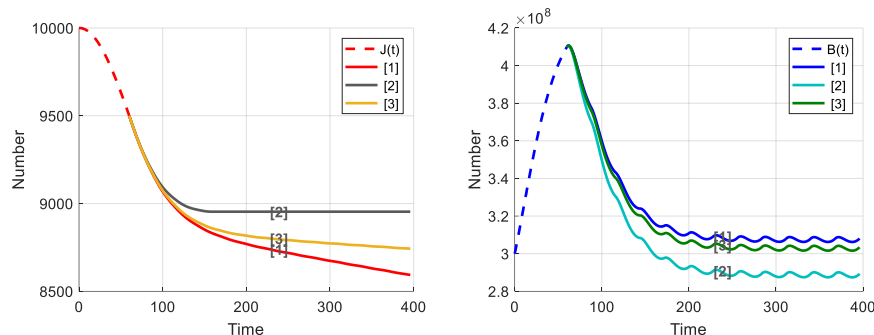
Coefficients of the model

The model contains several coefficients and their value may vary for different patients. So, it is important to choose correct values of these coefficients. Coefficient a_1 determines the rate of cartilage destruction. For healthy patient $B(t) = B_{norm}$ and a_1 may be ignored. r_1 and r_2 are cell amount rate and $1/b_1$ and $1/b_2$ are cells carrying capacity. s_2 denotes constant source of regulatory T cells and d_2 is death rate of regulatory T cells. c_1 and d_1 are rates of which B cells are stimulated to be produced by helper T cells and suppressed by regulatory T cells, accordingly [4]. These coefficients may be estimated if we have at least two clinical analysis of patient blood, taken in some time intervals. These analyzes should measure B lymphocytes, helper and regulatory T cell amounts, and estimate also cartilage size. We normalize size of the cartilage and normal size is assumed to be 10000 units. These values maybe measured at different time points. Figure 1 represents behavior of these 4 cells in case when at 100th day B lymphocytes value is $450 \cdot 10^6$, at 160th day helper T cells value is $9 \cdot 10^6$, regulatory T cells value is $3.5 \cdot 10^6$ at 50th day, and cartilage value is 7500 at 140th day. The next figure represents behavior of model functions ($J, B, Th, Treg$) under the conditions described above.

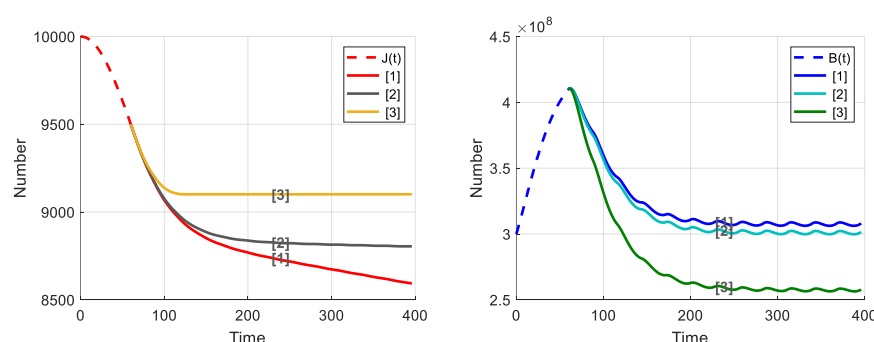


From these graphs, the condition of the cartilage may be presumed in 200 days. It is assumed that at initial time ($t=0$) all indicators were normal. Note that this figure is obtained from model that doesn't include treatment component. All coefficients of the model are calculated automatically based on the results of clinical analyzes.

Introduction of the drug component added another four coefficients (k_1, k_2, m_1, m_2) to the model. Correct selection of them is also very important. k_1 and k_2 denote fractional rate of killed and transformed by drug (Tocilizumab) helper T lymphocytes. The next figure shows effect of these coefficients on the progress of treatment. Dashed lines are values before drug treatment is started (60 days). Three different cases are considered: graph 1 represents case $k_1 = 0.005, k_2 = 0.025$, for graph 2 $k_1 = 0.005, k_2 = 0.03$ and for graph 3 - $k_1 = 0.007, k_2 = 0.025$. Here $m_1 = 1, m_2 = 1$



Coefficients m_1 and m_2 can be regarded as a scaling factor, and they can be included in the function u . Therefore, their values often are taken as 1. Figures below show effect of m_1 and m_2 . For graph 1 $m_1 = 1, m_2 = 1$, for graph 2 – $m_1 = 2, m_2 = 1$, for graph 3 – $m_1 = 1, m_2 = 2$. Here $k_1 = 0.005, k_2 = 0.025$.



Another coefficient is introduced in equation (5). Coefficient d_3 can be calculated from half-life period (τ) of the drug: $d_3 = -\ln(0.5)/\tau$. The above results were obtained on condition that the drug disintegration time was 13 days, and the treatment of the disease started on the 60th day

Acknowledgments

I thank professor of Tbilisi State Medical University Nona Janikashvili as inspirer of these study and for helping me to understand the biological mechanisms of immune diseases.

References:

1. Bellucci E, Terenzi R, La Paglia GM, Gentileschi S, Tripoli A, Tani C, Alunno A. One year in review 2016: pathogenesis of rheumatoid arthritis. // Clin. Exp. Rheumatol., Sep-Oct, 2016, Vol. 34(5), pp.793-801.
2. Ferro F, Elefante E, Luciano N, Talarico R, Todoerti M. One year in review 2017: novelties in the treatment of rheumatoid arthritis. // Clin. Exp. Rheumatol. 2017 Sep-Oct; Vol.35(5), pp.721-734.
3. Edwards JC, Cambridge G. B-cell targeting in rheumatoid arthritis and other autoimmune diseases. // Nat. Rev. Immunol., May, 2006, Vol.6(5), pp.394-403.
4. K.Odisharia, V.Odisharia, P.Tsereteli, N.Janikashvili Implementation of the Mathematical Model of Rheumatoid Arthritis // Reports of Enlarged Seminars of I.Vekua Institute of Applied Mathematics, Vol.31, 2017, pp.107-110

ПРИМЕНЕНИЕ ПАКЕТА GEOGEBRA ПРИ ПОСТРОЕНИИ ТРАЕКТОРИЙ МЕЖПЛАНЕТНЫХ ПОЛЕТОВ КОСМИЧЕСКИХ АППАРАТОВ

Кузнецов Юрий¹, Столяревская Алла²

¹Национальный аэрокосмический университет «Харьковский авиационный институт» имени Н.Е. Жуковского, Харьков, Украина

²Международный Соломонов университет, Харьков, Украина

Аннотация

В работе предлагается подход к применению пакета GeoGebra для отображения траекторий полета космических аппаратов при межпланетных миссиях. Результаты представлены на примере построения траектории перелета с круговой околоземной орбиты на круговую окололунную орбиту и обратно.

Abstract

The approach for the use of the GeoGebra package for displaying flight trajectories of spacecraft during interplanetary missions is proposed. The results are presented on the example of constructing a flight path from a circular near-earth orbit to a circular near-moon orbit and back.

Введение

Геометрические возможности пакета GeoGebra для изображения орбит планет в курсах изучения астрономии или для визуализации траекторий космических аппаратов (КА) при изучении околоземных орбитальных маневров описывались в ряде публикаций [1, 2]. В настоящей работе пакет применяется для представления траектории КА при выполнении полета на Луну и обратного перелета.

Постановка задачи

Движение КА как материальной точки в гравитационных полях планет для задачи 4-х тел (Солнце, Земля, Луна, КА) описывается во 2-й экваториальной системе координат (2ЭСК) уравнениями следующего вида [3]

$$\ddot{\vec{r}} = -\frac{\mu_E}{|\vec{r}|^3} \cdot \vec{r} + \vec{a}_L + \vec{a}_S,$$

где $\vec{r}$ – радиус-вектор КА в 2ЭСК; $\dot{\vec{r}} = \vec{V}$ – линейная скорость КА; μ_E – гравитационный параметр Земли; $\vec{a}_L$, $\vec{a}_S$ – ускорения, создаваемые полями Луны и Солнца.

Зададим начальные условия $\vec{r}(0) = \vec{r}_0$, $\vec{V}(0) = \vec{V}_0$, конечные условия $\vec{r}(T_k) \in R(T_k)$, $\vec{V}(T_k) \in V(T_k)$, где T_k – длительность перелета; $R(T_k), V(T_k)$ – множества допустимых конечных значений радиуса-вектора и линейной скорости КА.

Функционал качества многокритериальной оптимизационной задачи запишем в виде:

$$I = a_1 I_1 + a_2 I_2 + a_3 I_3 \rightarrow \min,$$

где $I_1 = \sum_{i=1}^N |\Delta V_i|$ – функционал расхода топлива; $\Delta V_i (i=1,2,3,4)$ – величина импульсов скорости КА; $I_2 = T_k$ – функционал времени перелета; $I_3 = H_{OP} - H_{OP}^* = \delta$ – функционал точности; $H_{OP} = r_M^\pi - R_M$ – высота окололунной орбиты КА; r_M^π – минимальный радиус-вектор КА относительно центра Луны; R_M – радиус Луны; H_{OP}^* – требуемая высота окололунной орбиты КА; $a_i (i=1, 2, 3)$ – весовые коэффициенты. Должны выполняться

условия $H_{OP}^{\min} \leq H_{OP} \leq H_{OP}^{\max}$ и $|\delta| \leq \varepsilon$, где $H_{OP}^{\max}, H_{OP}^{\min}$ – максимальная и минимальная высоты орбит прилета КА к Луне; ε – допустимая погрешность реализации окололунной орбиты.

Требуется определить величины и направления импульсов изменения линейной скорости КА, формирующих квазиоптимальную траекторию перелета с круговой околоземной орбиты на круговую окололунную орбиту и обратно.

Методика и результаты решения задачи

Сделаем ряд предположений: 1) КА – материальная точка; 2) гравитационные поля планет считаем центральными; 3) применим импульсную теорию орбитальных маневров, т.е. изменения линейной скорости КА ΔV_i происходят мгновенно; 4) считаем, что плоскость орбиты КА лежит в плоскости орбиты Луны (компланарный перелет).

Будем искать квазиоптимальные решения приближенным методом, основанном на теории невозмущенного движения, орбитальных маневров Цандера-Хомана, методе сфер влияния и с учетом принятых упрощающих предположений [3]. Из множества всех возможных траекторий полета к Луне остановимся на траектории Кондратюка. Она больше всех отвечает условию $I_1 \rightarrow \min$, так как использует гравитационное поле Луны как притягивающего центра. Кроме того, она апробирована астронавтами США в программе «Аполлон» [4].

Перелет по траектории Кондратюка предполагает выдачу первого импульса величиной и по направлению, обеспечивающих полет КА по эллиптической траектории и попадание КА в область сферы влияния Луны. Под влиянием гравитационного поля Луны траектория полета КА изменится на гиперболическую. При пролете на минимальном расстоянии от поверхности Луны необходимо выдать тормозной импульс, в результате чего КА перейдет на окололунную орбиту, близкую к круговой.

При возврате на Землю циклограмма выдачи импульсов на изменение линейной скорости КА симметрично повторяется.

Импульс приращения скорости ΔV_1 вычислим по формуле [3]

$$\Delta V_1 = V_0 \cdot \left(\sqrt{\frac{2R_1}{r_E + R_1}} - 1 \right),$$

где $V_0 = \sqrt{\frac{\mu_E}{r_E}}$ – скорость КА на околоземной орбите высотой H_0 ; $r_E = R_E + H_0$ – радиус-вектор КА; R_E – средний радиус Земли; $\mu_E = 398602,4415 \text{ км}^3/\text{с}^2$ – гравитационный параметр Земли; $R_1 = a - r_{MS} + \Delta r_{MS}$ – апогей эллиптического участка перелетной орбиты к Луне; a – среднее расстояние от Земли до Луны; r_{MS} – радиус сферы влияния Луны; Δr_{MS} – допуск на апогей эллиптической орбиты.

Для $H_0 = 300 \text{ км}$, $R_E = 6371 \text{ км}$, $a = 384400 \text{ км}$, $r_{MS} = 66421 \text{ км}$ получим $V_0 = 7,730 \text{ км/с}$ и $\Delta V_1 = 3,089 \text{ км/с}$. Следует уточнить момент времени выдачи импульса ΔV_1 с учетом прогноза движения Луны по орбите за время перелета T_k , которое в соответствии с третьим законом Кеплера вычисляется по формуле:

$$T_k = \frac{\pi}{2\sqrt{2\mu_E}} \cdot (r_E + R_1)^{3/2},$$

и составит около 3,8 суток. При этом угловое смещение Луны α_L за это время перелета при линейной скорости движения ее по орбите 1,02 км/с составит около 49,5 град.

Для определения направления отлетного импульса ΔV_1 воспользуемся матрицей М перехода от 2ЭСК к подвижной орбитальной системе координат (ОСК) с началом в центре масс КА [3]:

$$M = \begin{bmatrix} \cos u \cos \Omega - \sin u \cos i \sin \Omega & \sin \Omega \cos u + \cos \Omega \sin u \cos i & \sin u \sin i \\ -\sin \Omega \cos u \cos i - \cos \Omega \sin u & \cos \Omega \cos u \cos i - \sin \Omega \sin u & \cos u \sin i \\ \sin \Omega \sin i & -\cos \Omega \sin i & \cos i \end{bmatrix},$$

где Ω – долгота восходящего узла орбиты КА; i – наклонение; $u = u_L - \pi + \alpha_L$ – аргумент широты КА в момент выдачи импульса; u_L – аргумент широты Луны.

Тогда, если $\Delta \vec{V}_1 = [0, \Delta V_1, 0]^T$ – вектор импульса скорости в подвижной ОСК, то элементы второй строки матрицы M являются проекциями орта направления первого импульса скорости на оси 2ЭСК:

$$\Delta \vec{V}_{12\text{ЭСК}} = M^T \cdot \Delta \vec{V}_1 = \Delta V_1 \cdot \begin{bmatrix} -\sin \Omega \cos u \cos i - \cos \Omega \sin u \\ \cos \Omega \cos u \cos i - \sin \Omega \sin u \\ \cos u \sin i \end{bmatrix}.$$

В примере перелета «Земля-Луна-Земля» для приведенных выше исходных данных построена траектория Кондратюка. На рис. 1 показаны этапы ее построения.

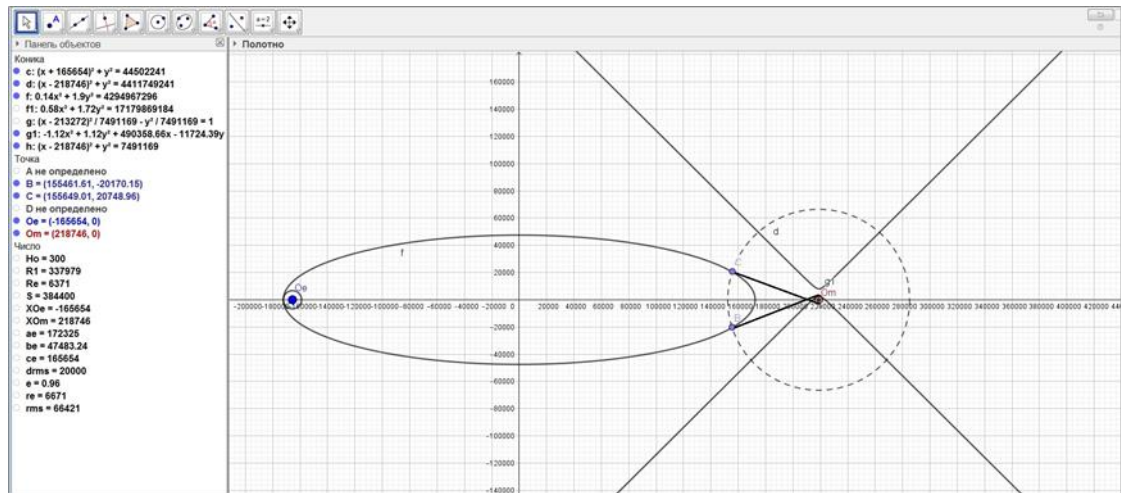


Рисунок 1 – Построение траектория Кондратюка

Список использованных источников:

1. Tortosa L. Some geometric models of ancient astronomy with Geogebra. – Date: July 25, 2016 [Electronic resource] // The access mode: <https://ggijro.files.wordpress.com/2011/07/article-7.pdf>.
2. Kuznyetsov Yu. Modeling the Spacecraft Orbital Maneuvers with Using GeoGebra for Visualization / Yu. Kuznyetsov, A. Stolyarevskaya // Proceedings of the International Scientific-Practical Conference Internet-Education-Science IES-2016. – Pp. 104-105.
3. Александров Ю.В. Введение в космонавтику: Учебное пособие / Ю.В. Александров. – Х.: ХНУ им. В.Н. Каразина, 2009. – 144 с. – ISBN 978-966-623-556-8.
4. Кондратюк Ю.В. Завоевание межпланетных пространств. 2-ое изд. / Под ред. П.И. Иванова / Ю.В. Кондратюк. – М.: Оборонгиз, 1947. – 76 с. [Электронный ресурс] // Режим доступа: http://az.lib.ru/k/kondratjuk_j_w/text_1929_zavoevanie.shtml.

РАЗРАБОТКА МАТЕМАТИЧЕСКОЙ МОДЕЛИ МНОГОКАНАЛЬНОЙ СИСТЕМЫ МАССОВОГО ОБСЛУЖИВАНИЯ СО МНОГИМИ СОСТОЯНИЯМИ ФУНКЦИОНИРОВАНИЯ

Рамаз Шамугия^{1,2}

¹ Сухумский физико-технический институт им. И.Векуа

² Сухумский государственный университет

Аннотация

Целью настоящей работы является создание наиболее обобщенной по сравнению с известными в литературе, аналитической модели сложной технической обслуживающей системы, состоящей из некоторого заранее определенного количества идентичных в надежностном понимании обслуживающих устройств, которые подвержены случайным отказам и восстановлением, и в которую в случайные моменты времени поступают на обслуживание требования, времена обслуживания которых также являются случайными. Согласно намеченной цели, в предлагаемой работе разработана конкретная аналитическая модель многоканальной системы массового обслуживания с ненадежными обслуживающими устройствами, в которой потоки отказов обслуживающих устройств и потоки поступающих требований, подчинены пуассоновским, а потоки восстановлений отказавших устройств и потоки обслуживаний поступающих требований-экспоненциальным законам распределения вероятностей. Случайный процесс переходов системы при этом является Марковским процессом с непрерывным временем и дискретными состояниями. Получены соотношения связывающие основные параметры и выходные характеристики систем указанного типа.

Abstract

The work deals with the development of analytical model of multichannel technical queuing system with unreliable servers and input memory where server failure flows and incoming request flows comply with Poissonian laws, while the flows of failed facilities repairs and flows of incoming requests comply with exponential laws of probability distribution. Random process of system change-over is a Markovian process with continuous time and discrete states. Relations binding basic parameters and output characteristics of the system indicated are obtained as probabilities of system staying in the given moment in one of the possible states. The proposed model is the most generalized compared to some models known in literature which could be considered as special cases of the considered model.

Введение

Благодаря структурной, временной и функциональной избыточностям, сложные технологические системы обладают многими работоспособными состояниями. В отличие от систем обладающих лишь двумя возможными состояниями (работоспособными и неработоспособными), для таких систем (multi-state systems) практически невозможно определить общепринятое понятие отказа. Поэтому для систем со многими состояниями вместо надежности вводится понятие технической эффективности, оценка которого производится с помощью выбранных показателей эффективности, зависящих от случайных факторов и учитывающих влияния их последствий на качество функционирования системы. Методологической основой существующих методов оценки и исследования эффективности функционирования сложных технологических систем со многими состояниями, служит концепция системного подхода. Эта концепция в данном случае проявляется в том, что показатель эффективности рассматривается как функционал от процесса функционирования системы.

В рамках указанного подхода, оценка эффективности функционирования сложных систем основывается на использовании модели процесса изменения работоспособности элементов системы. Ее сущность заключается в следующем: формально каждый элемент

системы в любой момент времени может находиться в одном из возможных состояний, каждое из которых характеризуется определенным уровнем работоспособности. Совокупность состояний элементов в произвольный момент времени однозначно определяет состояние системы. С течением времени, под влиянием внешних и внутренних случайных факторов, элементы системы переходят из одного состояния в другое. В результате происходит последовательная смена состояний системы в целом. Случайный многомерный процесс рассматривается как формализованный процесс изменения работоспособности элементов системы и описывает ее поведение во времени. Каждой реализации процесса соответствует определенная траектория в пространстве состояний системы.

Постановка задачи моделирования

Предлагаемая модель разработана с учетом следующих предположений:

- переходы системы между различными состояниями осуществляются под совместным воздействием нескольких случайных процессов-процессов поступления и обслуживания требований, а также процессов отказов и восстановлений обслуживающих устройств;
- техническая система массового обслуживания состоит из n одинаковых обслуживающих устройств;
- обслуживающие устройства подвержены устойчивым отказам, которые подчинены пуассоновскому закону распределения вероятностей с параметром α ;
- случайный процесс восстановления отказавших устройств описывается экспоненциальным законом распределения вероятностей с параметром μ ;
- в систему, на обслуживание поступает пуассоновский поток требований с интенсивностью равной λ ;
- обслуживание поступающих требований происходит по экспоненциальному закону с параметром β ;
- в системе предусмотрен входной накопитель для тех требований, которые поступают в течении промежутка времени, когда, все i исправные приборы заняты обслуживанием ранее поступивших заявок;
- длина очереди равна $k-l$, где k -общее количество требований находящихся в системе в рассматриваемый момент времени, а l -количество обслуживаемых на данный момент времени требований ($l=\overline{0, i}$), где i - количество исправно работающих к тому же моменту времени обслуживающих приборов;

Для описания процесса функционирования системы во времени, введем специальные вероятностные функции $R_{i,n-l}^{l,k-l}(t)$ и $P_{i,n-l}^{l,k-l}(t)$ описывающие процесс переходов системы в различные состояния, в зависимости от причин вызывающих эти переходы - отказы и восстановления обслуживающих устройств или поступление и обслуживание требований.

Введенные функции определяются следующим образом:

$R_{i,n-l}^{l,k-l}(t)$ -вероятность события, при котором в момент времени t система будет находиться в состоянии с i исправными и $n-i$ неисправными приборами, и при этом, общее количество требований находящихся в системе будет равно k , из которых количество находящихся на обслуживании требований будет равно l , а количество находящихся в очереди – $(k-l)$. Данная вероятность описывает процесс изменения состояний системы при фиксированных значениях верхних индексов, т.е. показателей поступления и обслуживания требований – l и $(k-l)$.

$P_{i,n-l}^{l,k-l}(t)$ – вероятность события, при котором в момент времени t система будет находиться в состоянии с i исправными и $n-i$ неисправными приборами, и при этом,

общее количество требований находящихся в системе будет равно k , из которых количество находящихся на обслуживании требований будут равно l , а количество находящихся в очереди требований – $(k-l)$. Данная вероятность описывает процесс изменения состояний системы при фиксированных значениях нижних индексов, т.е. надежности показателей системы-отказов и восстановлений обслуживающих устройств l и $n-i$.

$H_{i,n-i}^{l,k-l}(t)$ – вероятность события, при котором в момент времени t система будет находиться в состоянии с i исправными и $n-i$ – неисправными приборами, и при этом, общее количество требований находящихся в системе будет равно k , из которых количество находящихся на обслуживании требований будут равно l , а количество находящихся в очереди требований – $(k-l)$. Данная вероятность описывает процесс изменения состояний системы, при непрерывно меняющихся в процессе функционирования верхних и нижних индексах – $i, l, k, n-i$.

$$H_{i,n-i}^{l,k-l}(t) = R_{i,n-i}^{l,k-l}(t) * P_{i,n-i}^{l,k-l}(t); \quad k=0, \infty, \quad n=0, \infty, \quad i=0, n-1, \quad l=0, k-1$$

Рассматривая возможные изменения состояний системы в бесконечно малом интервале времени $(t, t+\Delta t)$, на основе вероятностных рассуждений, записываются системы разностных уравнений, описывающих процесс функционирования системы во времени в предположении фиксированных значений, то верхних (i и n), то нижних (l и k) индексов соответствующих функций $R_{i,n-i}^{l,k-l}(t)$ и $P_{i,n-i}^{l,k-l}(t)$.

Из полученных уравнений путем преехода к пределу при $\Delta t \rightarrow 0$, получим рекуррентные дифференциальные уравнения вида:

$$\frac{dR_{0,n-i}^{l,k-l}(t)}{dt} = a_{0,n-i}^{l,k-l} R_{0,n-i}^{l,k-l}(t) + a_{1,n-i}^{l,k-l} R_{1,n-i}^{l,k-l}(t) + Q_{0,n-i}^{l,k-l}(t); \quad \text{при } i=0; \quad (1)$$

$$\frac{dR_{i,n-i}^{l,k-l}(t)}{dt} = a_{i,n-i}^{l,k-l} R_{i,n-i}^{l,k-l}(t) + a_{i-1,n-i}^{l,k-l} R_{i-1,n-i}^{l,k-l}(t) + a_{i+1,n-i}^{l,k-l} R_{i+1,n-i}^{l,k-l}(t) + Q_{i,n-i}^{l,k-l}(t); \quad (2)$$

при $1 \leq i \leq n$

$$\text{где } Q_{i,n-i}^{l,k-l}(t) = b_{i,n-i}^{l-1,k-l} P_{i,n-i}^{l-1,k-l}(t) + b_{i,n-i}^{l+1,k-l} P_{i,n-i}^{l+1,k-l}(t); \quad (3)$$

$$\frac{dP_{i,n-i}^{0,k-l}(t)}{dt} = b_{i,n-i}^{0,k-l} P_{i,n-i}^{0,k-l}(t) + b_{i,n-i}^{1,k-l} P_{i,n-i}^{1,k-l}(t), \quad \text{при } l=0; \quad (4)$$

$$\frac{dP_{i,n-i}^{l,k-l}(t)}{dt} = b_{i,n-i}^{l,k-l} P_{i,n-i}^{l,k-l}(t) + b_{i,n-i}^{l-1,k-l} P_{i,n-i}^{l-1,k-l}(t) + b_{i,n-i}^{l+1,k-l} P_{i,n-i}^{l+1,k-l}(t); \quad (5)$$

при $1 \leq l \leq k$

После несложных преобразований с использованием метода Лапласа-Стилтьеса, уравнения (1) - (5) преобразуются в неоднородные системы алгебраических уравнений, которые довольно просто решаются с помощью формул Крамера относительно $R_{i,n-i}^{l,k-l}(s)$ и $P_{i,n-i}^{l,k-l}(s)$:

Ниже в качестве примера приведено решение системы уравнений относительно $P_{i,n-i}^{l,k-l}(s)$ с помощью формул Крамера, которое имеет следующем вид:

$$P_{i,n-i}^{l,k-l}(s) = \Delta_{i,n-i}^{l,k-l}(s) / \Delta^{l,k-l}(s), \quad \text{при } 1 \leq i \leq n, \quad \text{где} \quad (6)$$

$$\Delta^{l,k-l}(s) = \begin{bmatrix} [s - b_{i,n-i}^{1,k-l}(s)] & b_{i,n-i}^{0,k-l}(s) \cdots & b_{i,n-i}^{2,k-l}(s) \\ \vdots & \vdots & \vdots \\ [s - b_{i,n-i}^{k-1,k-l}(s)] & b_{i,n-i}^{k-2,k-l}(s) \cdots & b_{i,n-i}^{k,0}(s) \end{bmatrix} \quad (7)$$

главный определитель соответствующей системы, а $\Delta_{\delta}^{l,k-l}(s)$, определители получаемые подстановкой значений правой части $(1/s)$ системы уравнений в δ -ый столбец матрицы. Здесь: $\delta=1-3$ номера столбцов матрицы. Аналогичным образом записываются решения системы уравнений относительно $R_{l,n-l}^{l,k-l}(s)$.

С помощью найденных вероятностей состояний, можно определить различные показатели надежности и эффективности рассмотренной системы.

Выводы

Результаты полученные в данной работе, представляют собой некоторое обобщение уже известных в литературе результатов. Они позволяют вычислять вероятности возможных состояний описанной выше системы, через которые можно будет выразить другие важные показатели надежности и эффективности функционирования таких систем.

Результаты работы могут быть применены при анализе и синтезе таких сложных технических систем, какими являются системы передачи данных, системы сотовой связи, компьютерные и коммуникационные сети, гибкие производственные линии, автоматизированные системы управления, а также другие сложные технические и технологические системы используемые как в гражданских, так и в военных целях. Они могут быть использованы при оценке заданных, или обеспечении требуемых уровней надежности, производительности и эффективности функционирования сложных технических систем, как на этапе эксплуатации, так и на этапе проектирования.

Список использованных источников:

1. Гнеденко Б.В., Коваленко И.Н. Введение в теорию массового обслуживания. М.: Наука, 1987.
2. Барзилович Е.Ю., Беляев Ю.К., Каштанов И.Н. и др. Вопросы математической теории надежности. М.: Радио и связь, 1983
3. Саати Т.Л. Элементы теории массового обслуживания и ее приложения. М.: Сов. радио 1971.
4. Черкесов Г.Н. Надежность технических систем с временной избыточностью. М.: Сов. радио, 1974.
5. Shamugia, R. (2014) On One Model of Multichannel Queuing System with Unreliable Repairable Servers and Input Memory. *Int'l J. of Communications, Network and System Sciences*, 7, 279-285. doi: 10.4236/ijcns.2014.78030.
6. Shamugia, R. (2014) On One Model of Complex Technical Queuing System with Unreliable Devices and with Time Redundancy. *Int'l J. of Communications, Network and System Sciences*, 7, 257-264. doi: 10.4236/ijcns.2014.78028.
7. Shamugia, R.R. (2015) On One Analytical Model of a Probability Estimation of Quality and Efficiency of Functioning of Complex Technical Queuing Systems. *Int. J. Communications, Network and System Sciences*, 8, 295-303. <http://dx.doi.org/10.4236/ijcns.2015.88029>

MATHEMATICAL AND COMPUTER MODELING OF POLITICAL ELECTIONS

Temur Chilachava, Leila Sulava

Sokhumi State University

Abstract

In this paper, we have modeled the dynamics of an election process in the case of the transformation of bipartisan (the ruling party and one opposition party) election into three-party (ruling and two opposition parties) election during the inter-election period. Special case is considered.

In the particular case, with the zero demographic factor of all three political parties, and also with some relation between the variable coefficients of the model in the time segment $[0, T_1]$ and the constancy of the model coefficients in the time interval (T_1, T) , exact analytic solutions are found.

For computer modeling of the process of transformation of bipartisan elections into three-party, in general, the model coefficients are taken as variable time functions. Also, the process of the appearance of a new party in the period between two elections (in many countries this period is $T = 4$ years = 1460 days) is considered after 400, 800 and 1200 days from the date of previous elections. To analyze the results obtained, the case $T_1 = 400$ days is taken. It should be specially noted that with some selection of the variable coefficients of the model (for example, when the coefficient of attracting supporters for the emerging second opposition party significantly exceeds the coefficients of attracting the other two parties), in the time interval (T_1, T) there is an effect of an increase and a subsequent decrease in the number of supporters of the first opposition and the ruling party, i.e. the functions have a stationary points.

Аннотация

В этой статье мы моделировали динамику избирательного процесса в случае трансформации двухпартийной (правящей партии и одной оппозиционной партии) выборов в трехсторонние (правящие и две оппозиционные партии) выборы в межвыборный период.

В частном случае с нулевым демографическим фактором всех трех политических партий, а также с некоторой зависимостью между переменными коэффициентами модели в сегменте времени $[0, T_1]$ и постоянством коэффициентов модели во временном интервале (T_1, T) найдены точные аналитические решения.

Для компьютерного моделирования процесса трансформации двухпартийных выборов в трехпартийные, в общем, коэффициенты модели принимаются как переменные функции времени. Кроме того, процесс появления новой партии в период между двумя выборами (во многих странах этот период составляет $T = 4$ года = 1460 дней) рассматривается после 400, 800 и 1200 дней с даты предыдущих выборов. Для анализа полученных результатов был взят случай $T_1 = 400$ дней. Следует особо отметить, что при некотором выборе переменных коэффициентов модели (например, когда коэффициент притяжения сторонников для новой второй оппозиционной партии значительно превышает коэффициенты притяжения двух других сторон), в интервале времени (T_1, T) наблюдается эффект увеличения и последующего уменьшения числа сторонников первой оппозиции и правящей партии, т. е. функции имеют стационарные точки.

Introduction

Mathematical and computer modeling has been widely recognized in such disciplines as sociology, economics, history, political science and others [1,2]. Of great interest is mathematical modeling of political elections. Many scientists deal with this topic. In most cases, stochastic models of political elections are proposed, which involve an analysis of the statistics of elections already held [3,4]. Extremely important is the creation of a mathematical model, which would give an opportunity to define the dynamics of change in the number of supporters of different political subjects during the election period and a possible forecast of the election results. In [5] is proposed the nonlinear mathematical model with variable coefficients in the case of three-party elections, that describes the dynamics of the quantitative change of the votes

of the progovernment and two opposition parties from election to election. In the particular case obtained exact analytical solutions.

1. General mathematical model of transformation of two-party elections to three-party elections

We will consider the general mathematical model of transformation of two-party elections to three-party elections, from the accounting of demographic factor of elections which we have an appearance:

$$\begin{cases} \frac{dN_1(t)}{dt} = (\alpha_1(t) - \alpha_2(t))N_1(t)N_2(t) + (\alpha_1(t) - \alpha_3(t))N_1(t)N_3(t) - F_1(N_1(t), t) + \gamma_1(t)N_1(t) \\ \frac{dN_2(t)}{dt} = (\alpha_2(t) - \alpha_1(t))N_1(t)N_2(t) + (\alpha_2(t) - \alpha_3(t))N_2(t)N_3(t) - F_2(N_2(t), t) + \gamma_2(t)N_2(t) \\ \frac{dN_3(t)}{dt} = (\alpha_3(t) - \alpha_1(t))N_1(t)N_3(t) + (\alpha_3(t) - \alpha_2(t))N_2(t)N_3(t) + F_1(N_1(t), t) + F_2(N_2(t), t) + \gamma_3(t)N_3(t) \end{cases} \quad (1.1)$$

$$t \in (0, T],$$

$$N_1(0) = N_{10}, N_2(0) = 0, N_3(0) = N_{30}, N_{30} > N_{10} \quad (1.2)$$

$$N_2(t) \equiv 0, F_2(N_2(t), t) \equiv 0, t \in [0, T_1], T_1 < T, N_2(T_1) = N_{20} > 0$$

In this nonlinear mathematical model(1.1), (1.2) all coefficients are variables and demographic factors are taken into consideration. Equations (1.1) is defined in the interval $t \in (0, T]$, and initial conditions (of Cauchy) $t = 0$ moment of time. We look for the solution of the Cauchy problem on the segment $t \in [0, T]$ in the class of continuous differentiable functions

$N_1(t), N_2(t), N_3[t] \in C^1[0, T]$. In a nonlinear system of differential equations (1.1):

$N_1(t), N_2(t), N_3(t)$ – are the numbers of supports of two opposition and one ruling party $N_3(t)$ at time t ; $t = 0$ – is the time of previous elections, when one of the parties $N_3(t)$ won the elections and became the ruling party; $t = T$ – is the time of the following elections (in many cases $T = 4$ years or 1460 days); $t = T_1$ ($0 < T_1 < T$) – time-point, when to political arena there is the second opposition party; $\alpha_1(t), \alpha_2(t), \alpha_3(t)$ – are the coefficients of attracting votes by the first and second opposition party and the ruling party at time t . They largely depend on the action programs, as well as financial, technological and informational capacities of the political parties; $F_1(N_1(t), t), F_2(N_2(t), t)$ – are the continuous positive functions, that define the scale of used administrative resources; $\gamma_1(t), \gamma_2(t), \gamma_3(t)$ – are the coefficients that describe demographic changes of the parties.

2.A special case with zero demographic factor and variable coefficient of elections

We will consider a special case when the functions characterizing use of administrative resources are linear concerning the first variables, demographic factors of elections of all three parties are equal to zero

$$F_1(N_1(t), t) = \beta_1(t)N_1(t), F_2(N_2(t), t) = \beta_2(t)N_2(t), \quad (2.1)$$

Taking into account (2.1), (1.1) and (1.2) will correspond in the following look

$$\begin{cases} \frac{dN_1(t)}{dt} = (\alpha_1(t) - \alpha_3(t))N_1(t)N_3(t) - \beta_1(t)N_1(t) + \gamma_1(t)N_1(t) \\ \frac{dN_3(t)}{dt} = (\alpha_3(t) - \alpha_1(t))N_1(t)N_3(t) + \beta_1(t)N_1(t) + \gamma_3(t)N_3(t) \end{cases} \quad (2.2)$$

$$t \in (0, T_1] \quad N_1(0) = N_{10}, \quad N_3(0) = N_{30}, \quad N_{30} > N_{10}$$

$$\begin{cases} \frac{dN_1(t)}{dt} = (\alpha_{11}(t) - \alpha_{31}(t))N_1(t)N_3(t) + (\alpha_{11}(t) - \alpha_2(t))N_1(t)N_2(t) - \beta_{11}(t)N_1(t) + \gamma_1(t)N_1(t) \\ \frac{dN_2(t)}{dt} = (-\alpha_{11}(t) + \alpha_2(t))N_1(t)N_2(t) + (\alpha_2(t) - \alpha_{31}(t))N_3(t)N_2(t) - \beta_2(t)N_2(t) + \gamma_2(t)N_2(t) \\ \frac{dN_3(t)}{dt} = (-\alpha_{11}(t) + \alpha_{31}(t))N_1(t)N_3(t) + (-\alpha_2(t) + \alpha_{31}(t))N_3(t)N_2(t) + \beta_{11}(t)N_1(t) + \beta_2(t)N_2(t) + \gamma_3(t)N_3(t) \end{cases}$$

$$t \in (T_1, T] \quad N_1(T_1) = N_{11}, \quad N_2(T_1) = N_{20} > 0, \quad N_3(T_1) = N_{31} \quad (2.3)$$

Thus, we get the two Cauchy problem (2.2), (2.3).

Consider the case, when

$$\gamma_1(t) = \gamma_2(t) = \gamma_3(t) \equiv 0 \quad t \in [0_1, T] \quad (2.4)$$

Then the exact solution of the Cauchy problem (2.3) has the form

$$\begin{cases} N_1(t) = \frac{\frac{(\alpha_{11} - \alpha_{31})c - \beta_{11}}{\alpha_{11} - \alpha_{31} + p(\alpha_2 - \alpha_{31})} N_{11} \exp\{[(\alpha_{11} - \alpha_{31})c - \beta_{11}](t - T_1)\}}{(\alpha_{11} - \alpha_{31})c - \beta_{11} + N_{11} \exp\{[(\alpha_{11} - \alpha_{31})c - \beta_{11}](t - T_1)\} - N_{11}} \\ N_2(t) = pN_1(t) \\ N_3(t) = c - (p+1)N_1(t) \end{cases} \quad (2.5)$$

$$t \in [T_1, T]$$

3. Computer modeling

For the computer simulation of the process of transforming bipartisan elections into three-party elections in the general case (1.1), the model coefficients are taken as variable time functions. The process of entering the new opposition party's political arena in the period between the two elections for definiteness was considered after 400, 800 and 1200 days from the date of the previous elections. For a specific numerical count, the coefficients of the model are taken as exponentially increasing functions, although in the sequel can be considered other cases. For clarity, with a numerical calculation, the number of voters was chosen by the example of two countries - Georgia and Australia. It should be specially noted that with some selection of the variable coefficients of the model (for example, when the coefficient of attracting supporters for the emerging second opposition party significantly exceeds the coefficients of attracting the other two parties), in the time interval (T_1, T) there is an effect of an increase and a subsequent decrease in the number of supporters of the first opposition and the ruling party,

i.e. the functions $N_1(t)$ and $N_3(t)$, $t \in (T_1, T)$, have a stationary point $t^* \in (T_1, T)$, where $N_1'(t^*) = 0$ and stationary point $t^{**} \in (T_1, T)$, where $N_3'(t^{**}) = 0$ (Fig. 1).

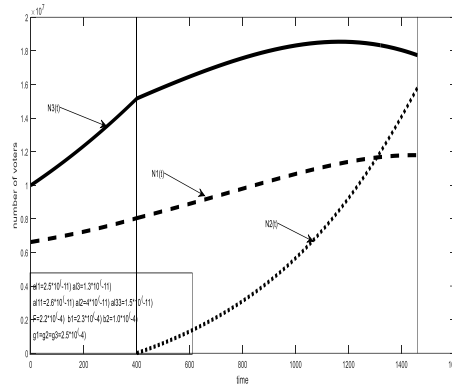


Fig 1.

Conclusions

The paper considers a nonlinear mathematical model of the transition of bipartisan elections to three-party elections, when in the period between elections to the political arena the second opposition party stands. In the case, with the zero demographic factor of all three batches, and also with some relation between the variable coefficients of the model in the segment $[0, T_1]$ and the constancy of the model coefficients in the interval (T_1, T) , exact solutions are found. In the case of variability of all coefficients of the model, numerous computer calculations are performed, in which, depending on the choice of variable coefficients and initial data, different election results are obtained. The results of the numerical account can be used by both the ruling and opposition parties to achieve their goals.

References

1. Chilachava T.I., Dzidziguri Ts.D. Mathematical modeling. Tbilisi, Inovacia, 2008.
2. Chilachava T.I., Kereselidze N.G. Continuous linear mathematical model of preventive information warfare. Sokhumi State University Proceedings, Mathematics and Computer Sciences, 2009, № VII, pp.113 – 141.
3. Belenky A., King D.A mathematical model for estimating the potential margin of state undecided voters for a candidate in a US Federal election, Mathematical Computer Modeling, 2007, 45, pp. 585 -593.
4. Boccara N.. Voters' Fickleness: A Mathematical Model. Int. J. Modern Phys. C, 2010, 21(2), pp.149-158.
5. Chilachava T.I., Sulava L.O. Mathematical and computer modeling of three-party elections. Georgian Electronic Scientific Journal: Computer Science and Telecommunications 2016, № 2 (48), pp. 59-72.

TENSOR MODELING OF A QUANTUM SYSTEM

Tikhonov Victor

A.S. Popov ONAT

Abstract

The issues of geometric tensor modeling of a quantum system considered. The quantum system understood as an ensemble of distinguished entities which are bound by the complex wave function of a local-point. The set of local points forms the definition area for the wave function; this area is organized in a closed compact and everywhere continuous topological space embracing the time/space independent coordinates. An interpretation of a tensor model of quantum system presented in terms of information network.

Анотація

Розглянуто питання геометричного тензорного моделювання квантової системи. Квантова система розуміється як ансамбль виділених сутностей, пов'язаних комплексною хвильовою функцією від локальної точки. Набір локальних точок утворює область визначення для хвильової функції; ця область організована у замкнутий компактний і скрізь безперервний топологічний простір, що охоплює незалежні координати часу/простору. Наведена інтерпретація тензорної моделі квантової системи в термінах інформаційної мережі.

Introduction

Classical system theories such as “General systems theory” ([1], 1968) and “Open systems theory” ([2], 2008) are being challenged recently by quantum system theory, primarily because of that classic system approach assumes systems to be a whole in a single scalability ([3], 2014). The quantum system theory takes its beginning from 1900–1925; it was rather a set of heuristic amendments and additions to classical mechanics ([4], 1967), which is now understood as semi-classical approximation [5] to modern quantum mechanics ([6], 2014). The basic concepts and methods of open quantum systems presented in [7, 2003]. The quantum system methodology is closely related to measurement problem; this view promises emergence of truly nanotechnologies that rely on the counter-intuitive properties of individual objects and can often outperform conventional decisions ([8], 2010). Nowadays, the quantum theory goes beyond physics and is increasingly used in various engineering tasks ([9], 2012). The modern directions of tiny-system modeling are quantum linear systems theory ([10], 2016) and linear dynamical quantum systems intended for communications and control ([11], 2017). However, the methodology of quantum systems analysis is not yet enough transparent and popular among the specialists of network engineering, particular with respect to apparatus of tensor algebra. *This work aims to formulate the core principles of quantum tensor analysis in terms of network applications.*

1. The “quantum system” characteristics

Consider the principal distinctive features of a quantum system (QS) in comparison with traditional conservative-continuum systems (CS); among them we will focus the three following characteristics: openness, indeterminacy, scalability.

The QS-openness means that classic hypothesis of the so called “conservative object” (which is closed and isolated from external disturbances) does not correspond to modern concepts of subtle interactions at the weak energies level. Moreover, the object interaction with the outer environment is the most interesting aspect of system analysis, where the system is constituted by at least two counteracting entities: the object of study (O) and the subject of research (S). The subject could be an individual person as it is (or, maybe provided by special instruments). So, we say that $QS = "O/S"$.

From this premise, the only way to comprehensively investigate a smart object is an accurate interaction between the object O and subject S. This interaction affects the object, and therefore, one can't observe the object as it is (without our impact). Only object disturbed states can be observed, and these states triggered by the concrete subject. Thus, the QS triggered behavior is non-fully objective (instead, it depends on a subject to some extent). The QS-openness causes the so called O/S-uncertainty dualism as a part of general QS-uncertainty. The system openness is not an exclusive privilege of quantum physics and elementary particles models. In modern IT-world one cannot imagine any cognitive activity beyond the tight communication with information environment. Towards system openness paradigm, we note that classic graph theory does not accentuate the open graph as network model. Again, many math textbooks and manuals for university students still based on the closed one-layer set theory of Cantor (suffering known logical contradictions).

The QS- indeterminacy means that contrary to the classical idea of complete matter observability, stochastic approximation is presumed for object particles behavior description. From this premise, one cannot exactly observe and control the QS-entity everywhere and any moment, or expect to find an absolute optimal decision. Everything is stochastically uncertain and approximate; everywhere the noise of indeterminacy is present. The stochastic character of QS is caused by the huge number of various factors of influence on the object of observation, which lead to exponent complexity growth of the QS-model. In general case, one may hope to estimate the probability of distinct particles appearance while regular experiments, along with the probability distribution of particle's coupling. The probability distribution is formalized by the so called wave function $\psi(x)$ which is normalized as $\|\psi(x)\|=1$. Here $x \in X$ is the set of points as definition area for wave function; this area is organized in a closed compact and everywhere continuous topological space embracing the time/space independent coordinates.

The square of wave function determines the probability distribution for particles coupling: $\rho(k,n)_x = [\psi(x)]^2 = \psi(x) \cdot \psi^*(x)$. The $\rho(k,n)_x$ is an Hermitian matrix, which diagonal elements $\rho(n,n)_x$ are real numbers; these numbers determine the proper degree of freedom for each particle. In case of symmetric coupling the $\rho(k,n)_x$ is a real symmetric matrix. The wave function admits geometric presentation in the form tensor operator. A case study of wave function could be normalized data flow distribution among the nodes of an open telecommunication network.

The QS-scalability means that modeling a complex object performed as multilayered dually opened formal system, which elements are scaled unlimitedly from above and below, in order to keep an overall system complexity at any layer. Thus, the whole complex object or system of low case level evolves to an utterly small primitive while going up to higher level of formalism. The total number of basic primitives at any hierarchy layer remains approximately even, though the primitives decisively change their essence and behavior. The greater system primitives are (towards observing subject), the more predictable and deterministic behavior shows the system. Instead, the less particles of matter investigated, the more stochastic and uncertain model of QS results.

2. Geometric tensor model of a quantum system

Visual thinking with geometric images is a powerful tool of the person's intellectual activity, including the understanding of complex objects and systems. A convenient form of representing geometric images is the classical tensor analysis, where the set of interacting objects is mapped onto the set of vectors in a local Euclidian space (real or complex). The simple case of vector presentation is a real positive symmetric matrix R which is interpreted as scalar product of a vector set (Riemann metric tensor): $R(k,n) = \{\vec{V}_k \times \vec{V}_n\}$. In this case, a real matrix A exists that $A \cdot A^T = R(k,n)$, or $A = \sqrt{R(k,n)}$.

Matrix A presents the normal coordinates of vectors V_k in a real Euclidian space with the orthonormal basis $\vec{E} = \{\vec{e}_k\}$. Under certain conditions, the wave function square $H = [\psi(x)]^2$ has a form of Hermitian matrix H ; however, it is not obligatory positive (i.e. some eigen values λ_k of H could be negative or zero). Because of that, a special technique needed to map the wave function $\psi(x)$ onto the linear system of vectors. If no zero eigen values (but diverse signs of eigen values shown) then a particular case of complex Euclidian space can be used for vector presentation (e.g. complex bundle of Euclidean space). If some zero eigen values appeared, then reduced form of linear system applied (less number of vectors presenting the wave function).

A lot of network tasks can be formulated in terms of related wave functions and their tensor presentation. Among those study cases are: the matrix of network nodes connectivity; the matrix of the shortest paths between the network nodes; the matrix of data flows between the open network poles etc.

Conclusion

The quantum system theory emerged on demand of new experimental facts in chemistry and physics of elementary particles. However, today this theory has gone far beyond this framework and finds its application in many fields of science and technology, including in the field of telecommunications, computer engineering and information systems.

References:

1. Ludwig von Bertalanffy, General System Theory, George Braziller New York, 1968, – 289 pp. Available at https://monoskop.org/images/7/77/Von_Bertalanffy_Ludwig_General_System_Theory_1968.pdf.
2. Shay D., Open systems in practice and theory: the social construction of participatory information networks. 2008. Available at <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.453.503&rep=rep1&type=pdf>.
3. Boje D., Quantum Systemicity Theory, 2014. – Available at https://business.nmsu.edu/~dboje/655/quantum_systems_theory.htm.
4. Haar D., The old quantum theory, Pergamon Press Ltd., Oxford, 1967. – Available at http://users.physik.fu-berlin.de/~kleinert/files/eins_lq.pdf.
5. Semi-classical approximation. Encyclopedia of Mathematics. URL: https://www.encyclopediaofmath.org/index.php?title=Semi-classical_approximation.
6. Sakurai J., Napolitano J., 2014. Modern Quantum Mechanics. 2-nd edition, Pearson education Ltd., 2014. – Available at <https://www.amazon.com/Modern-Quantum-Mechanics-Pearson-International-ebook/dp/B00IZ0G4BG>.
7. Breuer H., Petruccione F., Concepts and methods in the theory of open quantum systems, 2003. – Available at <https://arxiv.org/pdf/quant-ph/0302047.pdf>.
8. Wiseman H., Milburn G., Quantum Measurement and Control. Cambridge University Press, 2010. – 460 pp. Preface available at http://assets.cambridge.org/97805218/04424/frontmatter/9780521804424_frontmatter.pdf.
9. Miller D., Quantum Mechanics for Scientists and Engineers 1st Edition, Kindle Edition, 5-th printing, 2012. – <https://www.amazon.com/Quantum-Mechanics-Scientists-Engineers-Miller-ebook/dp/B00444400Y>.
10. Petersen J., Quantum Linear Systems Theory, 2016. – Available at <https://arxiv.org/pdf/1603.04950.pdf>.
11. Nurdin H.I., Yamamoto N., Linear dynamical quantum systems, Communications and control engineering, 2017. – Available at file:///C:/Users/User/Downloads/9783319551999-c2.pdf.

РОЗПІЗНАВАННЯ ПРИХОВАНИХ MISTY-ПОДІБНИХ ПЕРЕТВОРЕНЬ

Оксьоненко Максим, Яковлев Серій

Фізико-технічний інститут, КПП ім. Ігоря Сікорського

Анотація

В роботі розглянуто новий запропонований підхід до виявлення прихованих структур у таблично заданих S-блоках, який використовує так звану індикаторну матрицю високого порядку (HDIM-матрицю). Показано, що S-блоки, побудовані на основі схеми MISTY, при певних обмеженнях на кількість раундів та степінь раундової функції мають чіткі шаблони у HDIM-матриці, що може бути виявлено під час незалежного відновлення внутрішньої структури.

Abstract

We considered new proposed method for hidden structure detection in tabular S-boxes, which uses so-called High-Degree Indicator Matrix (HDIM). We show that S-boxes based on the MISTY scheme have strong patterns under certain restrictions, what can be detected during recovering of the internal structure.

Вступ

У роботі [2] запропонували метод визначення прихованої структури схеми Фейстеля у S-блоках за допомогою аналізу так званої HDIM-матриці. Зокрема, виявилось, що при деяких обмеженнях на степінь раундової функції схеми Фейстеля та кількість раундів, великі фрагменти HDIM-матриці залишаються нульовими. Схема блокового шифрування MISTY [3] є аналогом схеми Фейстеля, яка, втім, може більш ефективно обчислюватись за рахунок паралелізації обчислень сусідніх раундів, що є привабливою властивістю для ефективних реалізацій алгоритмів шифрування у малопотужних пристроях. У даній роботі наводяться знайдені особливості HDIM-матриць схем MISTY, що також дозволяє шукати приховані структури у таблично заданих S-блоках.

Необхідні терміни та визначення

Введемо необхідні для викладення результатів терміни та поняття [1].

Нехай $F_2 = \{0, 1\}$, $F_2^n = \{0, 1\}^n$. Одновимірна булева функція – це довільне відображення з множини F_2^n в множину F_2 . Багатовимірна (векторна) булева функція – довільне відображення з F_2^n у F_2^m . Кожна m -вимірна булева функція F може бути представлена у вигляді вектору одновимірних координатних функцій: $F = (f_0, \dots, f_{m-1})$.

Позначимо також через e_i двійковий вектор, у якого i -та координата дорівнює 1, а всі інші – нульові.

Кожна булева функція може бути однозначно представлена канонічним поліномом над F_2 у вигляді так званої алгебраїчної нормально форми (АНФ). Алгебраїчна степінь $\deg(f)$ булевої функції f дорівнює найбільшій кількості змінних у термах її АНФ. Степінь багатовимірної функції дорівнює максимальній степені її координатних функцій.

Нехай F – n -вимірна булева функція від n змінних. Індикаторна матриця високих порядків функції F , або просто HDIM-матриця (High-Degree Indicator matrix, HDIM [2])

$\hat{H}(F)$ – двійкова матриця розмірності $n \times n$, елементи якої визначаються як

$$\hat{H}(F)[i, j] = \bigoplus_x (e_i \cdot F(x)) \cdot (e_j \cdot x) = \bigoplus_x (e_j \cdot x) \cdot f_i(x).$$

Коефіцієнти матриці $\hat{H}(F)$ показують присутність доданку степеня $n-1$, який не містить змінної x_j , в АНФ координатної функції f_i .

Схема MISTY – ітеративна схема блокового шифрування, яка перетворює блоки довжини $2n$ у блоки довжини $2n$, один раунд шифрування якої має вид $F_k(x, y) = (y, y \oplus f_k(x))$, де $x, y \in F_2^n$, f – бієктивна раундова функція. Для побудови S-блоків використовуються схеми блокового шифрування малого розміру з константно заданими ключами (наприклад, нульовими).

Розпізнавання прихованих MISTY-подібних перетворень

Нехай E $2n$ -бітова схема MISTY ($n > 2$) із непарною кількістю раундів і раундовою функцією f , причому $\deg(f) = d$, $\deg(f^{-1}) = \tilde{d}$. Одержані результати подамо у вигляді двох таких теорем.

Теорема 1. За виконання таких умов:

- 1) при $r = 4l + 3$: $d^{l+1} + \tilde{d}^{2l+1} < 2n$;
- 2) при $r = 4l + 1$: $d^l + \tilde{d}^{2l} < 2n$;

завжди маємо $\hat{H}(F)[i, j] = 0$ при довільному $0 \leq i < n$ та довільному j .

Теорема 2. За виконання таких умов:

- 1) при $r = 4l + 3$: $d^l + \tilde{d}^{2l+1} < 2n$;
- 2) при $r = 4l + 1$: $d^l + \tilde{d}^{2l} < 2n$;

завжди маємо $\hat{H}(F)[i, j] = 0$ при довільному $i \geq n$ та довільному j .

З теорем випливає, що уся ліва або уся права частина HDIM-матриці буде заповнена нулями при виконанні зазначених умов. Таким чином, при невеликій кількості раундів (та виконання умов) уся HDIM-матриця схеми MISTY є нульовою. При більшій кількості раундів гарантовано занулюватись може лише права половина; при порушенні наведених умов поведінка елементів HDIM-матриці невідома. Одержані результати узагальнюються на парну кількість раундів (але із більш складними умовами).

Отже, одержані результати дозволяють на перших кроках аналізу визначати, чи має таблично заданий S-блок приховану структуру MISTY-подібного перетворення.

Висновки

У даній роботі розглянуто нещодавно запропонований метод виявлення прихованих структур у таблично заданих S-блоках за допомогою так званої індикаторної матриці високих порядків (HDIM-матриці). Показано, що перетворення зі структурою схеми MISTY мають певні особливості у HDIM-матриці, які можуть бути виявлені. Сформульовано умови, за яких зазначені особливості мають місце. Порушення цих умов при побудові S-блоку дозволяє захиститись від даного методу аналізу.

Список використаних джерел:

1. C. Carlet. Boolean functions for cryptography and error correcting codes [електронний ресурс]. – 2006. – Режим доступу: <http://www.math.univ-paris13.fr/~carlet/chap-fcts-Bool-corr.pdf>
2. L. Perrin, A. Udovenko. Algebraic Insights into the Secret Feistel Network (Full Version) [електронний ресурс]. – 2016. – Режим доступу: <http://eprint.iacr.org/2016/398>.
3. Matsui M. On a Structure of Block Ciphers with Provable Security against Differential and Linear Analysis // IEICE Trans. Fundamentals. – Vol. E82-A. – #1. – 1999. – pp. 117-122.

ОЦЕНКА ЭКСПЛУАТАЦИОННОГО СОСТОЯНИЯ ОБЪЕКТОВ ВОЕННО-ГРАЖДАНСКОГО НАЗНАЧЕНИЯ В УСЛОВИЯХ НЕОПРЕДЕЛЕННОСТИ

Швед Алена, Давыденко Евгений

Черноморский национальный университет имени Петра Могилы

Аннотация

Предложена процедура агрегирования индивидуальных оценок экспертов и построения результирующего ранжирования при решении задачи оценки эксплуатационного состояния объектов военно-гражданского назначения в условиях неопределенности, неточности и нечеткости исходных данных

Abstract

The procedure of aggregation of individual experts' assessments (judgments) and constructing the resulting ranking in solving problems of assessing the operational status of civil-military objects under uncertainty, inaccuracy and fuzziness of the initial data is proposed

Автоматизация процесса планирования, синтеза и принятия эффективных (оптимальных) стратегических решений военно-гражданского назначения направлена на укрепление национальной безопасности и обороны, поскольку от своевременного прогнозирования и принятия эффективных и обоснованных решений со стороны руководства при решении информационно-коммуникационных, логистических и управленческих задач, зависит сохранение жизни, как военнослужащих, так и технических средств, задействованных в ходе проведения военно-гражданских операций. В связи с этим особое значение приобретает задача оценки эксплуатационного состояния объектов военно-гражданского назначения.

Процесс принятия решений в быстро меняющихся условиях при ограниченности времени и ресурсов представляет собой неотъемлемую и ответственную функцию управления, и очень часто осуществляется в условиях неопределенности различного рода, которая характеризуется наличием неполноты, неточности, противоречивости, нечеткости входных данных.

Математическим аппаратом, позволяющим корректно оперировать с такого рода неопределенностями, является теория интуиционистских нечетких множеств.

Интуиционистским нечетким множеством (ИНМ) называют множество вида [1]:

$$A = \{(x, \mu_A(x), \nu_A(x)) \mid x \in X\},$$

где $X = \{x_i \mid i = 1, n\}$ – конечное множество элементов; $\mu_A : X \rightarrow [0, 1]$ – функция принадлежности произвольного элемента $x \in X$ к интуиционистскому нечеткому множеству A ; $\nu_A : X \rightarrow [0, 1]$ – функция непринадлежности $x \in X$ к интуиционистскому нечеткому множеству A ; функции μ_A , ν_A удовлетворяют условию $0 \leq \mu_A(x) + \nu_A(x) \leq 1$, $x \in X$.

Пусть имеется исходное множество вариантов (альтернатив) $A = \{A_i \mid i = \overline{1, n}\}$ и группа экспертов $E = \{E_j \mid j = \overline{1, m}\}$, выполняющих экспертизу. Результаты экспертного опроса в виде совокупности индивидуальных экспертных оценок можно представить в форме матрицы $B = [b_{ij}]_{n \times m}$, где $b_{ij} = (\mu_j^{(i)}, \nu_j^{(i)})$ – интуиционистские нечеткие числа, представляющие оценку j -м экспертом i -го варианта (альтернативы).

Задача состоит в получении результирующей ранжировки исследуемых объектов (военно-технического имущества: зданий, сооружений, технических средств и т.д.), отражающей коллективное мнение группы экспертов. Ранжирование вариантов осуществляется по потенциальному ущербу и значимости объекта, что позволяет рационально распределить имеющиеся ресурсы при планировании предупредительных мероприятий и проведения ремонтных работ, повышающих эксплуатационную надежность и стабильность работы объектов военно-гражданского назначения.

Для решения указанной задачи, можно использовать подход, состоящий в следующем.

На первом этапе вычисляются значения вектора приоритетов альтернатив. Для каждого эксперта E_j будет сформирован вектор весовых коэффициентов альтернатив

$\Omega_j = \{\omega_i^{(j)} \mid i = \overline{1, n}\}$, элементы которого вычисляются в соответствии с выражением:

$$\omega_i^{(j)} = \frac{\mu_i^{(j)} / (\mu_i^{(j)} + v_i^{(j)})}{\sum_{j=1}^m (\mu_i^{(j)} / (\mu_i^{(j)} + v_i^{(j)}))}, \quad \sum_{j=1}^m \omega_j^{(i)} = 1, \quad \omega_j^{(i)} \in [0, 1].$$

Далее рассчитываются значения вектора приоритетов альтернатив, на основе полученных оценок $\Omega_j = \{\omega_i^{(j)} \mid i = \overline{1, n}, j = \overline{1, m}\}$. Агрегированные весовые коэффициенты альтернатив рассчитываются на основе нечеткой оценки взвешенного среднего (IFWA) [2, 3]:

$$w_i = IFWA_{\omega_i^{(j)}}(b_{i1}, b_{i2}, \dots, b_{im}) = \omega_i^{(1)} b_{i1} \oplus \dots \oplus \omega_i^{(j)} b_{ij} \oplus \dots \oplus \omega_i^{(m)} b_{im}, \quad \sum_{i=1}^n w_i = 1, \quad w_i \in [0, 1].$$

где $\omega_i^{(j)}$ – весовой коэффициент i -го варианта, полученный на основе оценок j -го эксперта; $b_{ij} = (\mu_i^{(j)}, v_i^{(j)})$ – оценка j -м экспертом i -го варианта в виде ИНЧ.

В конце указанной процедуры будет получен вектор $W = \{w_i \mid i = \overline{1, n}\}$, $w_i = (\mu_i, v_i)$, значения которого соответствуют весовым коэффициентам рассматриваемых вариантов (альтернатив).

На втором этапе выполняется построение итоговой ранжировки вариантов (альтернатив). Для сравнения двух интуиционистских нечетких чисел в работе предложено использовать меры возможности [4, 5].

В работе предложена методика мониторинга эксплуатационного состояния объектов военно-гражданского назначения в условиях неопределенности и нечеткости исходных данных, применение которой позволит повысить эффективность безаварийной непрерывной эксплуатации объектов военно-гражданского назначения.

Список использованных источников:

1. Atanassov, K. T. Intuitionistic fuzzy sets [Text] / K.T. Atanassov // Fuzzy Sets Syst. – 1986. – Vol. 20, № 1. – P. 87–96
2. Xu, Z. Intuitionistic fuzzy aggregation operators [Text] / Z. Xu // IEEE Transactions on Fuzzy Systems. – 2007. – Vol. 15, № 6. – P. 1179–1187
3. Xu, Z. Some geometric aggregation operators based on intuitionistic fuzzy sets [Text] / Z. Xu and R. R. Yager // International Journal of General Systems. – 2006. – Vol. 35, № 4. – P. 417–433
4. Facchinetti, G. Note on ranking fuzzy triangular numbers [Text] / G. Facchinetti, R. G. Ricci, and S. Muzzioli // International Journal of Intelligent Systems. – 1998. – Vol. 13, № 7. – P. 613–622.
5. Wei C.-P. Possibility degree method for ranking intuitionistic fuzzy numbers [Text] / C.-P. Wei and X. Tang // Journal of Systems Engineering. – 2003. – Vol. 18. – P. 67–70

УЗАГАЛЬНЕНА МОДЕЛЬ ОПТИМАЛЬНОГО РОЗВИТКУ ЕКОЛОГІЗОВАНИХ ВИРОБНИЦТВ

Боровська Таїса, Гришин Дмитро, Северілов Павел, Спрут Іван

Вінницький національний технічний університет

Анотація

Виконано системний аналіз об'єктів класу «екологізоване виробництво», а саме: класифікацію, формування ресурсних зв'язків, функцій «витрати, випуск» і параметризованих моделей ефективності проекту. Виконано аналіз ресурсних структур зв'язків підсистем та їх параметризація – для отримання узагальненої моделі системи. Згідно з методикою оптимального агрегування виконано відображення ресурсної структури системи в бінарне дерево оптимального агрегування. Виконана розробка інформаційного забезпечення для системи управління комплексом біопереробки на етапах від укладення контракту до запуску виробництва. Виконано моделювання системи управління та підсистем інформаційного забезпечення.

Abstract

Performed systems analysis class objects greening production: classification of productions, the formation of resource links, cost functions, output and parameterized models of project efficiency. Analysis of resource structures links subsystems and their parameterization in order to obtain a generalized model of the system. In accordance with the methodology of optimal aggregation mapped resource system structure in binary tree optimal aggregation. Developed informational support for complex control system for the bioconversion from contract before starting production. Modeling control systems and information management subsystem.

Вступ

Сучасні виробничі системи функціонують в умовах хаотичної глобалізації. Для виживання в оточенні конкурентів, постачальників, покупців необхідно, з одного боку, прогнозувати майбутнє і планувати стійкий оптимальний розвиток. З іншого боку, виробнича система повинна швидко і оптимально реагувати на непрогнозовані погодні, ринкові, інноваційні та екологічні збурення. Високі технології, автоматизація на базі «оцифровування» всіх аспектів діяльності виробничої системи дозволяє реалізувати ефективне управління. На цьому шляху дві цивілізаційні перепони: падіння якості програмних продуктів і математичного забезпечення. Приклад щодо математики: у Франції втратилась висока наука – вчені емігрували в США, в Германії втратилась мова науки – дисертації пишуть тільки англійською. Дана робота є частиною досить широких досліджень в області соціо-техніко-екологізованих систем (СТЕС) [1, 2].

Проблемою даного дослідження є розробка методів аналізу і синтезу незалежних від розмірності та математичної специфіки моделі об'єкту (випукла, не випукла, гаусівська, негаусівська ...). Для вирішення проблеми необхідно поставити і вирішити такі задачі: – параметризація функцій виробництва і розвитку за технологічними і ціновими параметрами; – параметризація типових ресурсних структур екологізованих систем – зворотних зв'язків та ін.

Аналіз об'єктів управління

Розглянемо один з реальних прикладів екологізованих виробництв. На рис. 1 подано альтернативні схеми виробництва. Альтернатива А1: на базі неперервно виробленої цукросировини функціонують два окремих підприємства – цукрозавод і спиртозавод. Відходи виробництв утилізуються зовнішнім середовищем. Альтернатива А2 – спиртозавод працює на відходах цукрозаводу, відходи виробництва переробляються

в біореакторах, головний продукт яких – біогумус. Альтернатива A2 потенційно краща за A1.

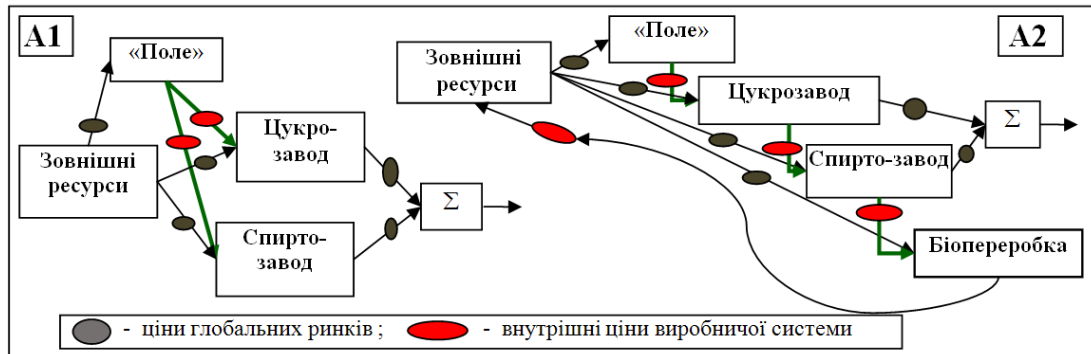


Рисунок 1 – Альтернативні структури і технології агросистеми

Теоретичні основи: параметризація операторів оптимального агрегування

Згадаємо, який шлях вдосконалень і розвитку пройшли автомобілі, двигуни. Сучасні технології та обладнання екологізованої переробки знаходяться на початковій стадії подібного розвитку, успіхи в значній мірі є просто рекламою за кошти, що виділяються на розвиток «зелених технологій». Проблеми обґрунтування «зелених» проектів не вирішуються засобами ефективного менеджменту та інформаційних технологій. Потрібні принципово нові математичні моделі і методи, зокрема, методи оптимального агрегування. Типові елементи в програмуванні – "функція користувача" і функція користувача з параметрами. В даній роботі використовується параметризація операндів оптимального агрегування і операторів. На рис. 2 подано базові варіанти параметризованого оптимального агрегування.

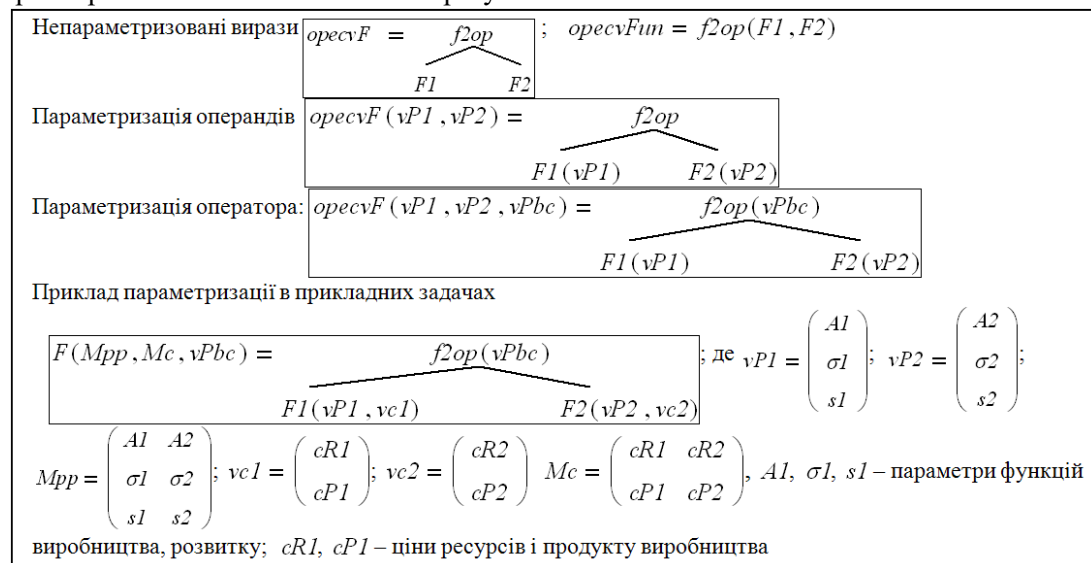


Рисунок 2 – Параметризація в алгебрі оптимального агрегування

На рис. 3 – приклад застосування методики параметризованих операндів і операторів. Для кожної підсистеми подані ресурсні зв'язки і оптимальні еквівалентні функції виробництва з параметрами технологічними і ціновими. На базі цієї схеми побудоване бінарне дерево оптимального агрегування і виконане оптимальне агрегування системи. На рис. 4 подано схему оптимального агрегування і результати відповідних бінарних операцій: $f14(X14, Mp14)$, $f23(X23, Mp23)$, $fs(Xs, Mps4)$. В цих виразах $X1s$, $X2s$, $X14$, $X23$, Xs – обсяги ресурсів для відповідних підсистем, на рис. 2 ці змінні у виразах не подані – це допускає синтаксис програмного середовища.

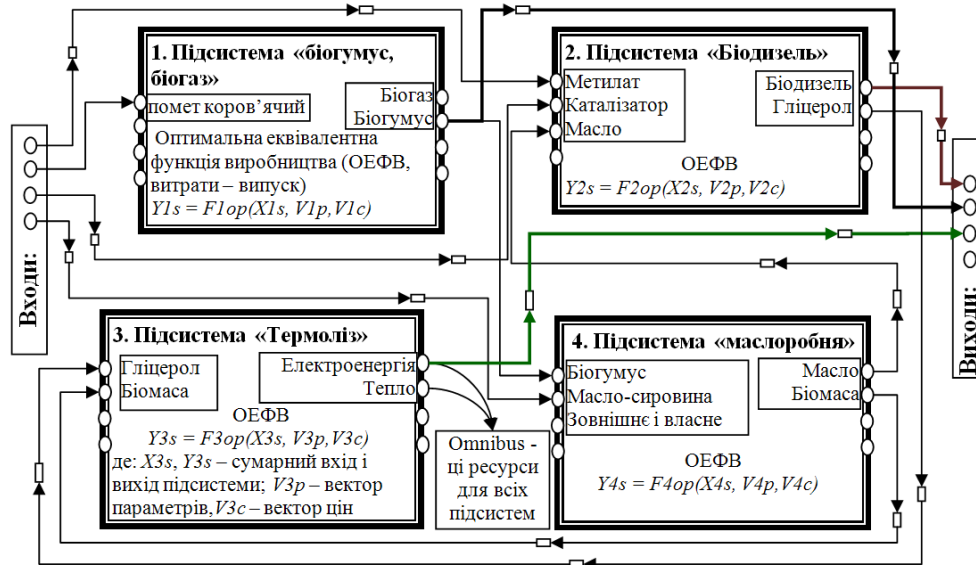


Рисунок 3 – Специфікація і параметризація ресурсних зв'язків екологізованої виробничої системи. Приклад

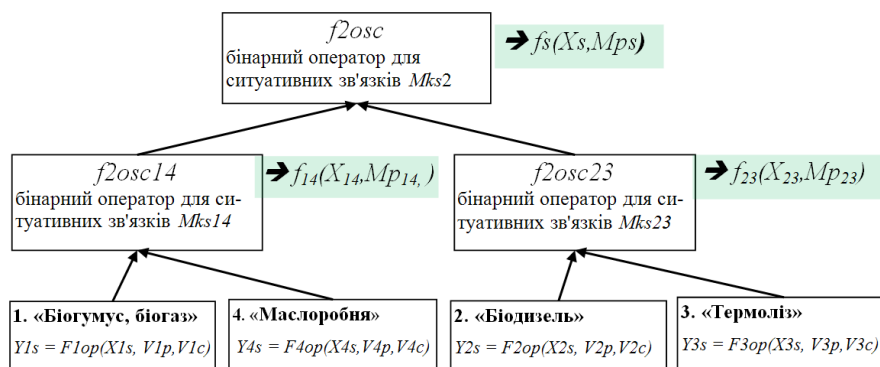


Рисунок 4 – Схема оптимального агрегування екологізованої виробничої системи (рис. 3). Приклад

Висновки

На базі аналізу стану і практики сучасних екологізованих систем виявлена актуальна проблема відсутності ефективних методів аналізу і синтезу незалежних від розмірності та математичної специфіки моделі об'єкта. Рішення проблеми отримане на базі методології оптимального агрегування. Вирішена задача параметризації бінарного оператора оптимального агрегування і параметризації операндів – функцій виробництва і розвитку. Проаналізовано рід існуючих проектів, де може бути застосоване отримане рішення. Напрями застосування – обґрунтування ефективності і ризиків проектів побудови екологізованих систем.

Список використаних джерел:

- 1.Боровська Т. М. Метод оптимального агрегування в оптимізаційних задачах: монографія / Т. М. Боровська, І. С. Колесник, В. А. Северілов. – Вінниця: УНІВЕРСУМ–Вінниця, 2009. – 229 с. – ISBN 978–966–641–285–3.
- 2.Боровська Т. М. Моделювання і оптимізація процесів розвитку виробничих систем з урахуванням використання зовнішніх ресурсів та ефектів освоєння: монографія / [Т. М. Боровська, С. П. Бадьора, В. А. Северілов, П. В. Северілов]; за заг. ред. Т. М. Боровської. – Вінниця: ВНТУ, 2009. – 255 с. – ISBN 978–966–641–312–6.

АТАКА ЗБОЇВ НА ARX-КРИПТОСИСТЕМУ HIGHT ТА ЇЇ ЕФЕКТИВНІСТЬ

Блинов Сергій, Яковлев Сергій

Фізико-технічний інститут, КПІ ім. Ігоря Сікорського

Анотація

Запропоновано атаку збоїв на блоковий шифр HIGHT, яка використовує модель фіксованого збою. Експериментально показано, що поведінка збоїв у даному шифрі носить нерівномірний характер, що не дозволяє використовувати наявний статистичний апарат для відновлення ключів, однак певні особливості розподілу збоїв дозволяють суттєво звужити множину можливих значень, а за повторення атаки – повністю відновити ключ шифрування.

Abstract

We propose a fault attack on HIGHT cipher based on fixed faults model. We experimentally show that faults inside this cipher are non-uniform, so one cannot use an existing statistical methods for key recovery. However, some properties of fault distribution allow to significantly reduce a set of possible keys (up to full recover with attack repeating).

Вступ

Розвиток алгоритмів «легкої» криптографії (англ. lightweight cryptography), призначених для використання у малопотужних пристроях, зазвичай вимагає економії на усіх обчислювальних ресурсах; тому в рамках даного напрямку широкого розвитку набули так звані ARX-криптосистеми (від англ. Add-Rotation-XOR) – алгоритми, які для обчислення використовують лише операції модульного та побітового додавання, а також циклічного зсуву двійкових векторів. Використання простих перетворень, які доступні на рівні базових інструкцій процесорів, суттєво пришвидшує шифрування даних, водночас достатній рівень захисту забезпечується за рахунок комбінування різних алгебраїчних операцій.

Атаки за побічними каналами напрямлені не на власне криптоалгоритми, а на їх реалізації у певних обчислювальних середовищах. Вони поділяються на пасивні, які одержують інформацію з побічних каналів (час виконання, споживана потужність тощо) та активні, які втручаються у роботу пристроїв та вносять збої у процес шифрування. Такі атаки є критичними для малопотужних пристроїв через обмеженість ресурсів, які можна виділити для захисту. Тому для алгоритмів легкої криптографії необхідно проводити обов'язковий аналіз стійкості до атак за побічними каналами.

Дана робота присвячена модельному дослідженню стійкості ARX-криптосистеми HIGHT до атак збоїв. Розглядаються поширені моделі зловмисника та різні сценарії проведення атаки, ефективність яких перевіряється експериментально.

Необхідні теоретичні відомості

Шифр HIGHT є блоковим шифром з ARX-дизайном, розробленим Корейською агенцією національної безпеки [1] та стандартизованим ISO [2]. Він перетворює 64-бітовий блок даних за допомогою 128-бітового ключа, виконуючи 32 раунди шифрування. Далі будуть використовуватись такі позначення.

Відкритий текст та шифротекст розглядаються як конкатенація восьми байтів і позначаються відповідно $P = P_0 \parallel \dots \parallel P_6 \parallel P_7$ та $C = C_0 \parallel \dots \parallel C_6 \parallel C_7$. Проміжні значення представлені аналогічно: $X_i = X_{i,0} \parallel \dots \parallel X_{i,6} \parallel X_{i,7}$ для $i = 0, \dots, 31$. Ключ шифрування (masterKey) розглядається як конкатенація 16 байтів, з яких генеруються вісім забілюючих ключів WK та 128 раундових ключі SK.

Раундове перетворення визначається такими співвідношеннями:

$$X_{i+1,j-1} = X_{i,j} \oplus (f_0(X_{i,j+1}) + SK_{i,j+1}), j=0,4;$$

$$X_{i+1,j-1} = X_{i,j} + (f_1(X_{i,j+1}) \oplus SK_{i,j+1}); j=2,6.$$

де f_0 та f_1 – певні перетворення (див. детальніше [1]). Схема раундової функції наведена на рис. 1. На початку та наприкінці шифрування окремі чотири байти вхідного тексту та, відповідно, шифротексту додатково забілюються ключами WK.

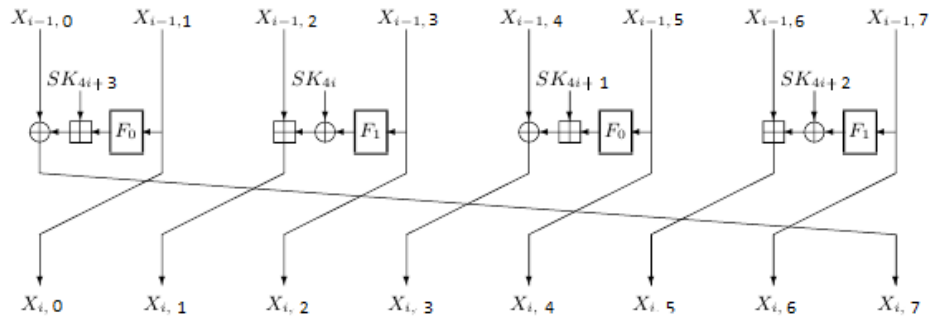


Рисунок 1 – Раундове перетворення шифру NIGHT

Блокова структура раундової функції спрощує аналіз, оскільки в цьому випадку можна перебирати раундові ключі окремо, по кожному з яких є відносно невелика кількість варіантів.

Загальна схема атаки

Основні принципи диференціальних атак збоїв для фейстель-подібних схем були сформульовані Біхамом та Шаміром [3] та в подальшому покращені Рівайном [4] при побудові атаки на шифр DES. Аналітик має доступ до шифруючого пристрою і використовує коректні та пошкоджені під час шифрування шифротексти від одного відкритого тексту, знання якого при цьому не вимагається. На основі одержаного статистичного матеріалу будуються розпізнавачі для правильних значень раундових ключів, які після цього вже знаходяться (зазвичай, перебором).

Для атаки на шифр NIGHT розглядається модель із фіксованим збоєм: аналітик може спотворювати один байт проміжного шифротексту, позиція якого йому відома, але невідоме спотворене значення. Порівняння коректних та збитих шифротекстів у 0, 2, 4 та 6 байтах шифротексту дає змогу відновити правильні значення ключів забілювання та раундових ключів за допомогою функцій розпізнавання

$$g^j(WK, SK) = (\overline{C_j} \oplus (f_0(\overline{C_{j+1}} \oplus WK) + SK)) \oplus (C_j \oplus (f_0(C_{j+1} \oplus WK) + SK)), j = 0,4,$$

$$g^j(WK, SK) = (\overline{C_j} - (f_1(\overline{C_{j+1}} - WK) \oplus SK)) \oplus (C_j - (f_1(C_{j+1} - WK) \oplus SK)), j = 2,6,$$

які отримано з аналітичного виду останнього раунду шифрування (тут C – правильний шифротекст, $\overline{C}$ – збитий шифротекст). Для правильних значень ключів поведінка функцій розпізнавання очікується суттєво нерівноімовірною, а для неправильних – значно ближчою до рівноімовірного.

Опишемо покроково алгоритм атаки.

1) Згенерувати N шифротекстів та N відповідних збитих шифротекстів. Збиті шифротексти одержуються за рахунок одного спотвореного байту проміжного шифротексту із фіксованою позицією (номер раунду, номер байту у блоці).

2) Для кожного кандидата у пару ключів (WK, SK) обчислити вибіркового розподіл значень функцій розпізнавання g^j

3) Перевірити, чи має g^j очікуваний розподіл. Якщо так, то даний кандидат є правильною парою ключів.

Оскільки на практиці теоретичний розподіл функцій g^j фактично невідомий, оскільки залежить від характеру збою та внутрішньої структури шифру (його пошук становить окрему цікаву задачу), то для кожного байту будемо перевіряти евклідову відстань до рівномірного розподілу:

$$d(WK, SK) = \sum_{x=0}^{256} \left(\frac{\#(g^j(WK, SK) = x)}{N} - \frac{1}{256} \right)^2$$

Експериментальні результати

Для проведення експериментів було реалізовано модель шифру із відповідними функціями збоїв та розпізнавання (використовувалась мова Java, ключі, тексти та збої генерувались за допомогою класу SecureRandom). Описаний сценарій атаки перевірено на 1000 випадкових ключах шифрування, для кожного з яких генерувалось 1000 пар випадкових правильних та збитих шифротекстів.

Виявилось, що навіть через лавинні ефекти, тобто змішування спотворених байтів між собою під час шифрування, розподіл функцій розпізнавання не був настільки нерівномірним, щоб гарантувати для правильних значень раундових ключів максимальну евклідову відстань від рівномірного розподілу. Однак для правильних кандидатів евклідова відстань знаходилась у діапазоні $0.00090 < d(WK, SK) < 0.00110$. Експериментально встановлено, що використовуючи дане обмеження, можна за допомогою одного збою щонайменше втричі зменшити кількість кандидатів; відповідно, при послідовному повторенні атаки з декількома різними збоями (приблизно 10-16 повторів) можна відновити правильні раундові ключі або звужити множину їх можливих значень, після якої відновлення ключа шифрування можна виконати безпосередньо перебором.

Відповідно, для захисту від атак збоїв реалізації шифру HIGHT повинні контролювати коректність обчислень щонайменше на 16 останніх раундах шифрування.

Висновки

У даній роботі було запропоновано атаку збоїв на шифр HIGHT, яка використовує байтові випадкові помилки у внутрішніх раундах шифрування. Обрана модель є не дуже жорсткою для аналітика, проте дозволяє ефективно зменшувати множину значень ключа шифрування. Експериментально встановлено, що байтові збої у шифрі HIGHT носять нерівномірний характер, що не дає змогу перенести атаку Рівайна на даний шифр; однак аналіз цього розподілу дозволяє суттєво зменшувати кількість кандидатів у правильні ключі. Описаний сценарій атаки дозволяє за рахунок 10-16 повторних запусків відновити ключ шифрування.

Список використаних джерел:

1. Hong D. et al. HIGHT: A New Block Cipher Suitable for Low-Resource Device. // Proceedings of CHES 2006. – LNCS. – vol. 4249. – Springer, 2006. – pp. 46-59.
2. Information technology – Security techniques – Encryption – Part 3: Block ciphers. ISO/IEC 18033-3.
3. Biham E., Shamir A. Differential fault analysis of secret key cryptosystems // Proceedings of CRYPTO'97. – LNCS. – vol.1294. – Springer, 1997. – pp. 513-525.
4. Rivain M. Differential Fault Analysis on DES Middle Rounds // Proceedings of CHES 2009. – LNCS. – vol. 5747. – Springer, 2009. – pp. 457-469.

СТІЙКІСТЬ ШИФРУ AES ДО ДИФЕРЕНЦІАЛЬНОГО КРИПТОАНАЛІЗУ ВІДНОСНО АЛЬТЕРНАТИВНИХ АЛГЕБРАЇЧНИХ ОПЕРАЦІЙ

Сергеев Станіслав, Яковлев Сергій

Фізико-технічний інститут, КПІ ім. Ігоря Сікорського

Анотація

Досліджується стійкість блокового шифру AES до диференціального криптоаналізу, який використовує побудовані спеціальним чином алгебраїчні операції, альтернативні операції побітового додавання у скінченному полі характеристики 2. Розглянуто 64 альтернативні операції та показано, що відносно майже всіх таких операцій гарантована стійкість шифру AES до диференціального криптоаналізу знижується.

Abstract

We study a security of AES cipher against differential cryptanalysis with respect to specific operations, which are similar to bitwise addition (XOR) in finite Galois field of characteristics 2. We consider 64 of such operations and show that AES guaranteed security against differential cryptanalysis in almost all cases is lowered.

Вступ

Диференціальний криптоаналіз є одним з найпотужніших методів криптоаналізу блокових шифрів; стійкість до диференціального криптоаналізу наразі є необхідною умовою для усіх алгоритмів шифрування. Для національного стандарту шифрування США, шифру AES [1], теоретична та практична стійкість до диференціального аналізу відносно операції побітового додавання була забезпечена параметрами S-блоків та раундового лінійного перетворення [2].

У роботі [3] було запропоновано новий підхід до диференціального криптоаналізу SP-мереж, в якому замість побітового додавання розглядаються спеціальні алгебраїчні операції на множині двійкових векторів. У даній роботі буде проведено аналіз стійкості шифру AES до диференціального криптоаналізу відносно деяких з таких операцій.

Необхідні терміни та визначення

У подальшому використовуються такі терміни та позначення.

Нехай $V_n = \{0,1\}^n$ – векторний простір всіх бітових векторів довжини n . На множині V_n визначено дві операції $\circ, +$, кожна з яких задає структуру абелевої групи.

Диференціалом булевої функції $f: V_n \rightarrow V_n$ відносно операцій $(\circ, +)$ (або просто $(\circ, +)$ -диференціалом) називається довільна пара двійкових векторів (a, b) .

Імовірність $(\circ, +)$ -диференціала (a, b) булевої функції f (або просто диференціальна імовірність) визначається за формулою

$$d_{\circ,+}^f(a, b) = \frac{1}{2^n} \sum_x [f(x \circ a) + (f(x))^{-1} = b],$$

де $[A]$ – індикатор події A (1, якщо A виконується, та 0, якщо ні), а через $(f(x))^{-1}$ позначено елемент, обернений до $f(x)$ відносно операції $+$. Позначимо також

$MDP_{\circ,+}^f(f) = \max_{a \neq 0, b} d_{\circ,+}^f(a, b)$ – максимум диференціальної імовірності функції f .

Для шифруючих перетворень (булевих функцій, параметризованих ключами) диференціальні імовірності розглядаються усереднено за усіма ключами. У цьому

випадку усереднена величина MDP є основним параметром стійкості до диференціального криптоаналізу, оскільки складність проведення атаки буде обернено пропорційна до неї; відповідно, чим більшою є MDP , тим менш стійким є шифр, та навпаки.

Блоковий шифр AES [1] побудовано на основі структури SP-мережі. Він складається з декількох раундів шифрування (від 10 до 14), на кожному з яких виконується нелінійна заміна байтів стану (процедура SubBytes) та лінійне перемішування байтів стану (процедури ShiftRows та MixColumns). S-блок s для процедури SubBytes було підібрано таким чином, щоб його MDP відносно операції побітового додавання $\oplus$ був мінімально можливий: $4/256$. Процедура MixColumns побудована як множення векторів із байтів стану на спеціальну матрицю, при цьому всі операції виконуються у скінченному полі $GF(256)$.

Теоретична стійкість шифру AES була доведена у [2], де показано, що складність будь-якої диференціальної атаки на AES буде щонайменше 2^{96} операцій шифрування. В подальшому ці оцінки були ще покращені.

Альтернативні операції для диференціального криптоаналізу

У [3] було запропоновано провадити диференціальний криптоаналіз SP-мереж відносно спеціально побудованих операцій, які зберігають деякі властивості операції побітового додавання. Головна ідея полягає у виборі таких операцій, відносно яких процедура MixColumns залишається лінійною. Якщо при цьому диференціальні імовірності S-блоків відносно таких операцій збільшуються, то загальна аналітична оцінка стійкості шифру до диференціального криптоаналізу знижується – відповідно, знижується й рівень безпеки шифру.

Будемо позначати через $\circ$ довільну операцію із описаними вище властивостями. Методика побудови таких операцій наведена у [4] та більш детально – у [3].

Диференціальний криптоаналіз відносно операції $\circ$ може провадитись у двох можливих сценаріях.

1) За припущення, що раундові ключі шифрування k відносяться до множини так званих «слабких» ключів, тобто для довільного вектору x виконується рівність $x \circ k = x \oplus k$. У даному випадку стійкість до диференціального криптоаналізу буде визначатись величиною $MDP_{\circ}(s)$.

У [3] показано, що множина слабких ключів $W_{\circ} = \{k \mid \forall x : x \circ k = x \oplus k\}$ утворює лінійний підпростір простору V_n ; більш того, розмірність цього простору $d = \dim(W_{\circ})$ задовольняє нерівностям $2 - (n \bmod 2) \leq d = \dim(W_{\circ}) \leq n - 2$. Відповідно, чим більша розмірність у $W_{\circ}$, тим більше імовірність потрапити на слабкі ключі.

2) Для довільних ключів із збереженням операції $\oplus$ у ключовому суматорі. У даному випадку стійкість шифру до диференціального криптоаналізу буде визначатись величиною $MDP_{\oplus, \circ}(s)$.

Експерименти

Для оцінювання стійкості шифру AES до диференціального криптоаналізу нами був побудований ряд альтернативних операцій із наведеними вище властивостями. Для аналізу обирались операції із максимально можливим простором слабких ключів. Оскільки для S-блоку шифру AES маємо $n = 8$, тому максимальна можлива розмірність простору слабких ключів $W_{\circ}$ $d = 6$. У [5] показано, що існує лише 64 операції, які задовольняють цій вимозі.

Для кожної з побудованих операцій були обчислені значення $MDP_{\oplus, \circ}(s)$ та $MDP_{\circ, \oplus}(s)$ S-блоку шифру AES, які порівнювались із значенням $MDP_{\oplus, \oplus}(s) = 0,015625$.

Одержано такі результати:

1. Величина $MDP_{\oplus, \circ}(s)$ відносно 63-х операцій дорівнює $6/256 = 0,0234375$.
2. Величина $MDP_{\oplus, \circ}(s)$ відносно однієї операції дорівнює $4/256 = 0,015625$.
3. Величина $MDP_{\circ, \oplus}(s)$ відносно 55-ти операцій дорівнює $8/256 = 0,03125$.
4. Величина $MDP_{\circ, \oplus}(s)$ відносно 8-ми операцій дорівнює $10/256 = 0,0390625$.
5. Величина $MDP_{\circ, \oplus}(s)$ відносно однієї операції дорівнює $4/256 = 0,015625$.

Отже, бачимо, що лише для однієї операції максимальна диференціальна імовірність не збільшується (власне, ця операція є побітовим додаванням $\oplus$). Відносно всіх інших операцій маємо збільшення значення MDP щонайменше у півтори рази. Відповідно, при другому сценарію проведення аналізу складність проведення диференціальної атаки (теоретична оцінка стійкості згідно [2]) становить щонайменше $(6/256)^{-16} \approx 2^{86}$ операцій шифрування, що на 10 порядків менше за попередні оцінки. За першим сценарієм оцінка повинна складати $(10/256)^{-16} \approx 2^{75}$ операцій шифрування, однак дана оцінка буде виконуватись лише за умови, що всі раундові ключі будуть слабкими; імовірність такої події потрібно оцінювати окремо, з урахуванням процедури генерування раундових ключів.

Висновки

У даній роботі було розглянуто нещодавно запропонований підхід до проведення диференціального криптоаналізу SP-мереж за допомогою алгебраїчних операцій спеціального виду. Було побудовано 64 такі операції для поля $GF(256)$ із найбільш прийнятними криптографічними параметрами, після чого було оцінено величини диференціальних імовірностей S-блоку шифру AES відносно даних операцій. Показано, що для деяких операцій гарантована стійкість шифру AES до диференціального криптоаналізу зменшується щонайменше на 10 порядків (тобто у тисячу разів). Хоча такі уточнені оцінки стійкості все одно гарантують стійкість AES, результати дослідження говорять про необхідність ретельного аналізу захищеності алгоритмів шифрування відносно різних модифікацій диференціального криптоаналізу та формулювання відповідних вимог до складових шифрів, зокрема, S-блоків.

Список використаних джерел:

1. Advanced Encryption Standard. [електронний ресурс]. – Режим доступу : <http://csrc.nist.gov/archive/aes>
2. Park S. Improving the upper bound on the maximum differential and the maximum linear hull probability for the SPN structures and AES / S. Park, J. Sung, S. Lee, J. Lim // Fast Software Encryption. – FSE'03, Proceedings. – Springer Verlag, 2003. – P. 247 – 260.
3. Blondeau C. Differential Attacks: Using Alternative Operations [електронний ресурс] / C. Blondeau, R. Civino, M. Sala. – Режим доступу : <https://eprint.iacr.org/2017/610.pdf>
4. Calderini M. Elementary abelian regular subgroups as hidden sums for cryptographic trapdoors [електронний ресурс] / M. Calderini, M. Sala. – Режим доступу : <https://arxiv.org/pdf/1702.00581.pdf>
5. Сергеев С.О. Використання альтернативних алгебраїчних операцій для диференціального криптоаналізу SP-мереж // Матеріали конференції «Теоретичні і прикладні проблеми фізики, математики та інформатики» (м. Київ, 26-27 квітня 2018 р.). – Том 2. – К.: ВПІ ВПК «Політехніка», 2018. – С. 75-77.

УДК 519.876.2

МЕТОДИ УПРАВЛІННЯ ПІДПРИЄМСТВОМ НА БАЗІ ІМІТАЦІЙНИХ МОДЕЛЕЙ КЛАСУ «ОДИН НА ФОНІ ВСІХ»

Боровська Таїса, Волошин Костянтин, Станіславський Іван, Вернигора Інна

Вінницький національний технічний університет

Анотація

Розглядається комплекс математичних моделей класу «виробники, продукти виробництва», призначений для досліджень проблеми управління окремим підприємством в оточенні інших виробників і користувачів певного сегменту виробництва і ринку. Виконано розробку модулів стратегій управління підприємством – пропорційна, ризикова, кредитна і оптимальна на базі оптимального агрегування. В склад комплексу входить модуль генерації невизначеностей і збурень з довільними розподілами ймовірностей, а також моделі виробництва і ринку. Розроблено інтерфейс введення і аналізу параметрів системи виробників. Програмна система обчислює процеси функціонування, і розвитку, і статистику віртуальної реальності.

Abstract

Addresses the complex mathematical models of the class "producers, food production, designed to study problems in the management of private enterprise in the active surrounded by other producers and users of some production and market segment. Modules developed enterprise management strategies-proportional risk, credit and optimum based on optimal aggregation. The complex includes a module for generating ambiguities and disturbances with arbitrary distributions, as well as models of production and market. Input interface and analysis processes. Software system calculates the functioning and development of processes and statistics.

Вступ

Оптимальне управління виробничою системою – необхідна умова її стійкого функціонування і розвитку. Відомі фундаментальні рішення щодо оптимального управління поточним і кінцевим станом проблематичні для практичної реалізації через високу розмірність, суттєві нелінійності, стохастичність і активність зовнішнього оточення. Головними трендами у виробництві вважаються висока динамічність технологічних операцій і проблемність фінансового сервісу. В епоху «хмарних» інформаційних технологій фінансові транзакції виконуються за 2-3 місяці, біржові ціни є чисто спекулятивними реаліями. Найбільш хибним фактором глобалізації є руйнування соціумів: – те, що виробляється в одному регіоні використовується в іншому, розриваються регіональні зв'язки «школа, університет, виробництво». В даній роботі подані моделі і методи управління сучасною виробничою системою, що може стійко розвиватись в будь якому оточенні як цілісна виробнича система. Ця робота – частина комплексу «розробок і досліджень»: ефективна математична модель складної системи є більш ефективним засобом продукування інтелектуальної продукції ніж реальна система. Причина – виконання експериментів, неможливих в реальній системі і швидке дослідження тривалих процесів, швидке отримання статистики віртуальної реальності.

Проблемою є створення комплексу робочих моделей для пошуку і дослідження ефективних стратегій функціонування і розвитку для окремого виробника і системи «виробники, продукти» (NM-системи) в цілому. Нові задачі, що необхідно вирішити для рішення поставленої проблеми: – розробити параметризовану математичну модель оптимального агрегування паралельних структур з можливістю налаштування на специфіку довільних галузей виробництва; – розробити математичну модель оптимального агрегування структур «виробництво, розвиток»; – розробити математичну модель «оптимальні кредитні стратегії виробника в активному оточенні»; – модифікувати інтерфейс програмної системи імітаційного моделювання NM-систем для розширеного

вибору альтернатив стратегій управління і формування структур NM-систем. В даній роботі в якості прототипів використовуються власні розробки [1–2]: – базова модель «динаміка системи N виробників певного сегменту виробництва з M продуктами (NM-система) і розширена модель NMK-система: «виробники, продукти, користувачі». Очікувані результати розробки: комплекс моделей і програмних модулів прогнозування стану системи виробників, що використовують різні стратегії управління.

Концепція розробки

Концепція моделі «один на фоні всіх» [1, 2]: певне підприємство на ринку M продуктів має задовільну програму імітаційного моделювання деякого сегменту виробництва з N виробників, що виробляють M видів виробів. Топ менеджер підприємства бажає виконати наближене до реальності тестування нових правил (стратегій) управління на своєму підприємстві з урахуванням («на фоні») дій інших виробників (конкурентів) і користувачів. В класичних моделях зовнішнє оточення імітувалися детермінованими і стохастичними функціями дій – коливань попиту, цін та ін. Сьогодні можливо генерувати такі збурення програмними модулями «породжуючих механізмів». Більшість «породжуючих механізмів» стохастичні. В програмі моделювання це відображується і дозволяє відобразити досить адекватно стохастичність і набирати «статистику віртуальної реальності». Одна з наукових задач роботи є порівняльне дослідження існуючих методів управління виробництвом на базі існуючих АСУП і систем управління з імітаційною моделлю-предиктором: генератором «віртуальної реальності». На нашій імітаційній моделі можна досліджувати такі ситуації: – «я и найближчий конкурент», «у мене інша стратегія, ніж у всіх», «моя стратегія краща, але як швидко мене доженуть». Під запропоновану концепцію розроблена схема системи управління виробництвом з імітаційною моделлю «елемента» в «системі» (рис. 1).

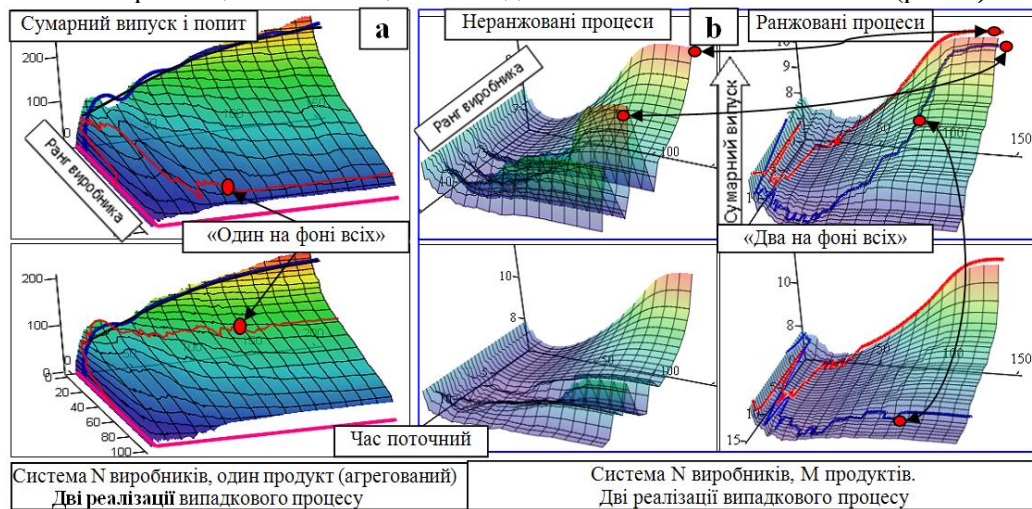


Рисунок 1 – Приклади моделювання систем класу «виробники, продукти». Динаміка відновлення після спаду

Базові імітаційні моделі

На рис. 1а подано дві реалізації процесу функціонування системи «N виробників, один продукт». По осях 3D графіка – час, темп випуску, ранг виробника. Сітка на 3D графіку: – послідовність рангових розподілів, і – послідовність ліній рівня темпу випуску. Разом з 3D графіком подано графіки динаміки сумарного випуску і сумарного попиту. На 3D графік «накладено» послідовність станів (темп випуску, ранг за темпом випуску). На рис. 1б подано дві реалізації випадкового процесу функціонування системи «N виробників, M продуктів». Ми починаємо не з математичних моделей, а з візуального подання результатів моделювання тому, що це єдиний шлях ефективного розуміння

нелінійних, нестационарних, стохастичних виробничих систем. Це стосується і моделювання невизначеностей і збурень. На рис. 2 подано статистику процесів на рис. 1.

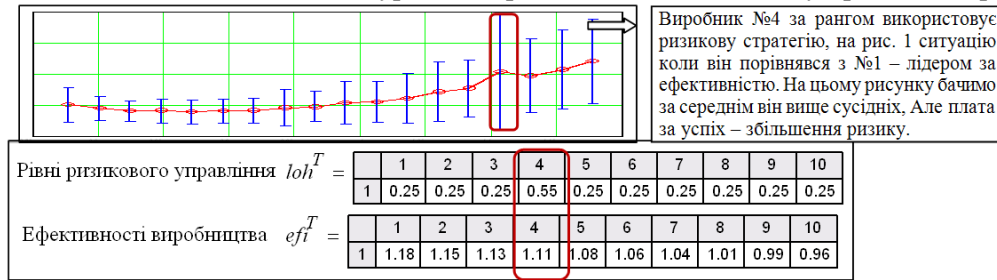


Рисунок 2 – Статистичний аналіз системи виробників. Ситуація – розподіл нових обмежених ринків

Розглянули комплекс «інструментів» для досліджень на імітаційних моделях. Вважається «самоочевидною» неможливість ставити експерименти на реальних системах. В рамках класичних моделей і методів неможливо побудувати адекватні моделі нелінійної, нестационарної і стохастичної реальності. Однак, ресурсний підхід, методологія оптимального агрегування дозволяють конструювати адекватні моделі реальних об'єктів тому, що знімають (а не вирішують) проблеми довільних нелінійностей і пошуку в багатовимірному фазовому просторі.

Альтернативні стратегії для виробника в активному середовищі

Конкретні завдання в даній роботі – розробка програмних модулів для реалізації альтернативних методів управління сучасною виробничою системою в активному оточенні інших виробників і користувачів. Показано можливість такої розробки на двох прикладах: – «стратегії «пропорційного управління» і «ризикові стратегії». В практиці такі стратегії застосовуються на суто емпіричному рівні. Природне питання: чи можливо створити кращі за показниками ефективності і живучості стратегії. На базі попередніх досліджень відібрані і розроблені робочі математичні моделі: – управління розподілом ресурсів між підсистемами на базі методів оптимального агрегування; – управління з використанням крім власних ресурсів – кредитів.

Висновки

Поставлена і вирішена задача розробки оптимальних стратегій управління виробника в середовищі конкурентів і користувачів. Сьогодні такі задачі вирішуються на базі рецептурно-емпіричних методів ефективного менеджменту. Причина такого стану науки освіти – висока складність сучасних виробництв і систем виробників. Використання методології оптимального агрегування усуває проблеми стохастичності, нелінійності і розмірності. Розробка потенційно дозволяє скоротити витрати ресурсів і часу на тестування і відлагодження нового обладнання, нових методів збирання і обробки даних і нових методів управління за рахунок імітаційних моделей без спрощень – лінеаризації, редукції та ін. Розробка перейшла в стан тестування «віртуальної реальності».

Список використаних джерел:

- 1.Боровська Т. М. Метод оптимального агрегування в оптимізаційних задачах: монографія / Т. М. Боровська, І. С. Колесник, В. А. Северілов. – Вінниця: УНІВЕРСУМ–Вінниця, 2009. – 229 с. – ISBN 978–966–641–285–3.
- 2.Боровська Т. М. Моделювання і оптимізація процесів розвитку виробничих систем з урахуванням використання зовнішніх ресурсів та ефектів освоєння: монографія / [Т. М. Боровська, С. П. Бадьора, В. А. Северілов, П. В. Северілов]; за заг. ред. Т. М. Боровської. – Вінниця: ВНТУ, 2009. – 255 с. – ISBN 978–966–641–312–6.

УЗАГАЛЬНЕНІ МОДЕЛІ ОПТИМАЛЬНОГО УПРАВЛІННЯ СИСТЕМАМИ МАСОВОГО ОБСЛУГОВУВАННЯ

Боровська Таїса, Колесник Ірина, Загородонець Аліна, Недоснований Олександр

Вінницький національний технічний університет

Анотація

Запропоновано новий підхід до сучасних типових систем виробництва продуктів і послуг з комп'ютерною системою управління. Суть новизни: розширення комп'ютерної моделі об'єкта управління – мегазавода, логістичного центру та ін. до системи спеціалізованих моделей, що складаються з моделі динаміки системи в контурі оперативного управління, моделі-предиктора в контурі стратегічного управління, моделі активного оточення – множини користувачів продуктів і послуг і конкурентів, а також моделі-спостерігача стану об'єкта і зовнішнього оточення. Використання методології оптимального агрегування дозволило зняти проблеми розмірності. Наведено приклади оптимізації та моделювання процесів функціонування і розвитку.

Abstract

A new approach to modern typical systems of production of products and services with a computer control system is proposed. The essence of novelty: expansion of the computer model of the control object – mega-plant, logistics center, etc. to the system of specialized models consisting of the model of the dynamics of the system in the operational control circuit, the predictor model in the strategic control circuit, the model of the active environment – the set of users of products and services and competitors, as well as the observer model of the state of the object and the external environment. The use of the optimal aggregation methodology allowed us to eliminate dimensional problems. Examples of optimization and modeling of processes of operation and development are presented.

Вступ

Загально визнаним методом вирішення складних проблем аналізу, оптимізації та проектування систем управління виробництвом і технологічних процесів є моделювання. Розвитку напряду сприяє зростання ефективності програмно-апаратних засобів комп'ютерних систем. Переваги моделювання: динамічна візуалізація стану організаційних, технологічних і економічних підсистем; відсутність математичних обмежень на типи залежностей між параметрами імітаційної моделі та зовнішнього стану середовища; можливість дослідження динаміки взаємодії в просторі й часі системи; можливість описувати поведінку компонент складної системи досить докладно; висока потенційна адекватність моделі і об'єкта складної системи; широка можливість застосування альтернативних математичних моделей. Початок застосування імітаційного моделювання у виробництвах – 70-80 роки, тоді пропонувалися моделі поточного і оперативного виробничого планування на базі імітаційного моделювання процесів функціонування комп'ютерних систем (КС) на базі детермінованих і переважно лінійних моделей, що відтворювали процеси виконання планових замовлень. Тепер в основі КС залишились ці розробки, непридатні для оновлень. Це дійсно глобальна проблема: повної заміни базових математичних моделей, новими вже існуючими і ще не створеними.

Імітаційне моделювання і аналіз чутливості дозволяють в результаті моделювання отримати більш адекватні реальності планові рішення, а також отримувати відповіді на питання типу “що буде якщо”, а також – приймати остаточні рішення на базі емпіричного досвіду. Однак в цьому напрямі є важливий аспект: «що кого відображує»: модель натуральну систему, чи навпаки, – натуральна система є відображення. На виробничих системах витратно і неефективно ставити експерименти. Це потрібно виконувати на моделях. Проблема – конструювання моделей великих систем для досліджень. Програми

для управління виробничими системами повинні бути зробленими «для саме цього виробництва», і одночасно універсальними. В даній розробці використовується методологія оптимального агрегування, розглядаються тільки «раціональні ресурсні структури» [1, 2]. Виробнича система вважається раціональною, якщо для кожної підсистеми виконується умова: при виділенні підсистеми додаткового ресурсу, стан інших підсистем, як мінімум не погіршується. Нераціональні виробничі системи неможливо оптимізувати.

Мета даної роботи – аналіз і вибір структур і математичних моделей для інтегрованих комплексів «об’єкт управління, комп’ютерна система». Для досягнення мети необхідно вирішити наступні задачі: проаналізувати і систематизувати типові задачі сучасних об’єктів управління – виробничих, логістичних систем, систем масового обслуговування та ін.; проаналізувати і систематизувати альтернативні структури комп’ютерних систем; розробити структуру програмного забезпечення, що ефективно поєднає рішення задач самоконтролю і типових задач об’єкта управління; виконати імітаційне моделювання роботи КС.

Моделеорієнтовані структури сучасних КС виробництва і обслуговування

На основі вивчення інформаційних джерел різних рівнів – від наукових до рекламних фільмів передових підприємств, побудована схема сучасного підприємства як «природоподібного» утворення, що стійко і оптимально функціонує і розвивається. На рис. 1 подано основні елементи і зв’язки схеми системи виробництва, обслуговування. Всі блоки на рис. 1 – реалізовані власними робочими моделями і пройшли тестування.

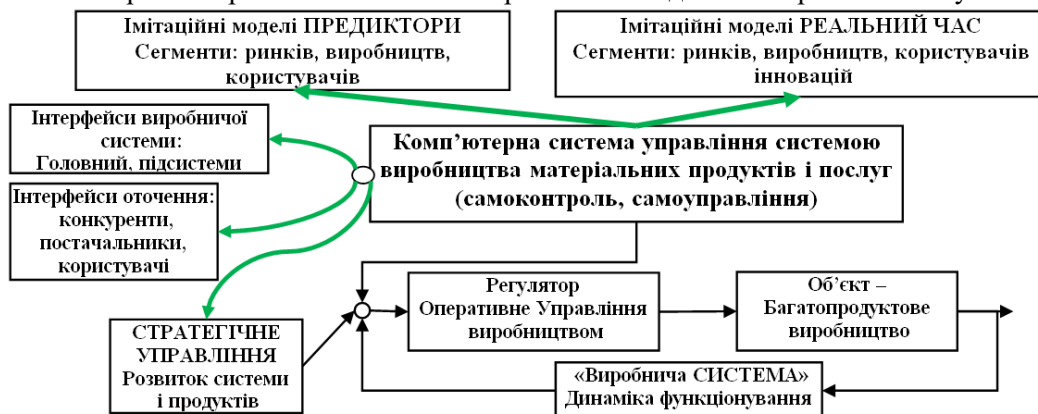


Рисунок 1 – Типова схема сучасної виробничої системи з інтегрованою комп’ютерною системою управління імітаційної моделі «виробники, продукти, користувачі»

На рис. 2 подано приклад видачі блока «модель-предиктор».

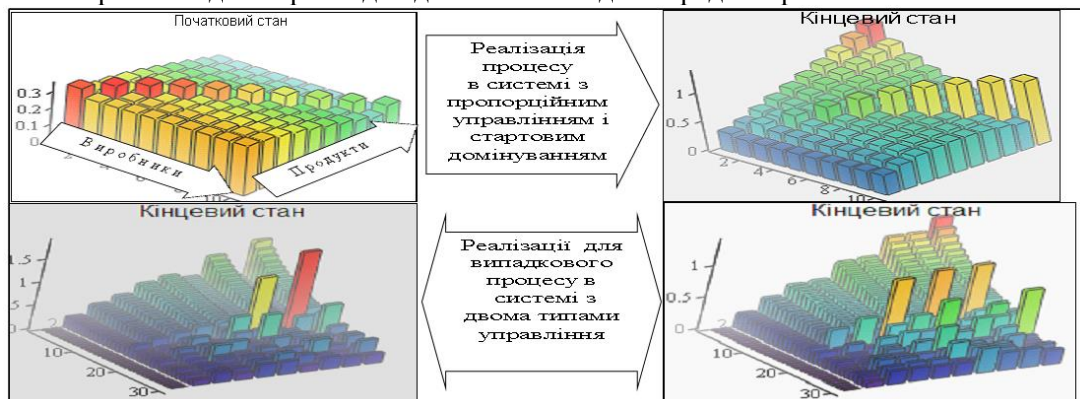


Рисунок 2 – Приклад результатів імітаційного моделювання системи виробників

Модель має декілька форм видачі – частотні характеристики, перехідні процеси в системі та для окремих виробників. Зміст прикладу на рис. 2: розглядається система «10 виробників, 10 продуктів». В початковому стані виробники і продукти ранжовані за ефективністю і обсягом ринку. Кожен виробник представлений рядком стовпців, величина стовпця – ринкова позиції даного виробника по даному продукту. Подано два стани системи – початковий і прогноз на заданий період. Сценарії моделювання: – кожен виробник є лідером у виробництві одного продукту, результат відповідає емпіричному правилу про важкість входу на зайнятий ринок: бачимо два тренди лідерів за ефективністю, і лідерів по окремому продукту; – маємо дві підмножини виробників: ефективні використовують класичну стратегію, менш ефективні використовують ризикову стратегію. Подано дві реалізації випадкового процесу. Висновок для спеціаліста користувача даного програмного продукту: – ризик може вивести аутсайдера в лідери. На рис. 3 подано приклад тестування роботи блока оперативного управління певного виробника. Для тестування вибрано вхід «послідовність інтервалів постійного навантаження з випадковими амплітудою і тривалостями.

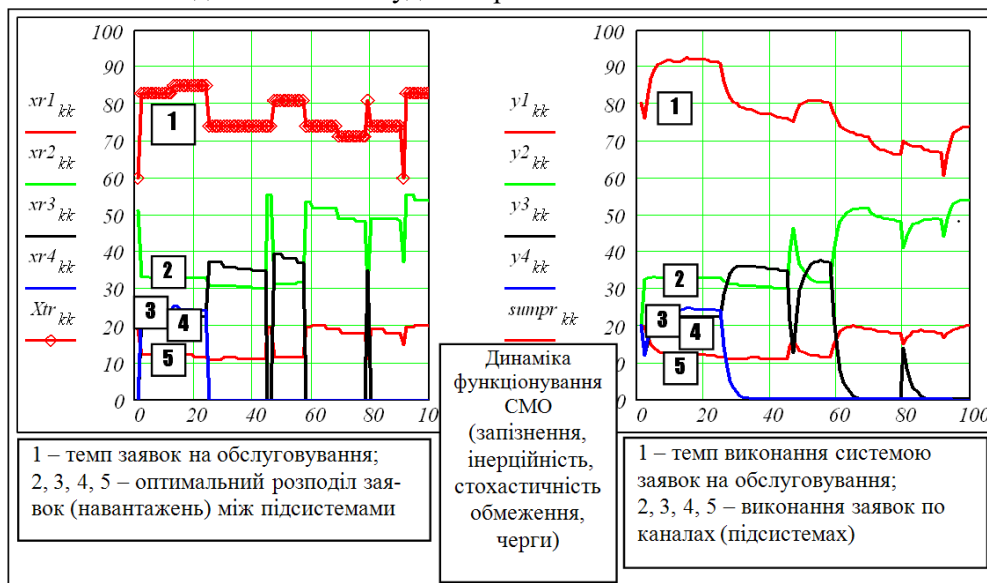


Рисунок 3 – Моделювання процесів обслуговування в багатоканальній СМО. Приклад

Висновки

В роботі поставлена мета – проаналізувати і вибрати структури і математичні моделі для інтегрованих комплексів «об'єкт управління, комп'ютерна система», поставлені відповідні задачі. За результатами дослідження вибрана модеорієнтована структура управління з математичними моделями, що забезпечують оперативне і стратегічне управління. За рахунок вибору і використання методології оптимального управління система не має обмежень щодо класів функцій обслуговування і розподілів ймовірностей. Наведені приклади імітаційного моделювання.

Список використаних джерел:

- 1.Боровська Т. М. Метод оптимального агрегування в оптимізаційних задачах: монографія / Т. М. Боровська, І. С. Колесник, В. А. Северілов. – Вінниця: УНІВЕРСУМ–Вінниця, 2009. – 229 с. – ISBN 978–966–641–285–3.
- 2.Боровська Т. М. Моделювання і оптимізація процесів розвитку виробничих систем з урахуванням використання зовнішніх ресурсів та ефектів освоєння: монографія / [Т. М. Боровська, С. П. Бадьора, В. А. Северілов, П. В. Северілов]; за заг. ред. Т. М. Боровської. – Вінниця: ВНТУ, 2009. – 255 с. – ISBN 978–966–641–312–6.

УДК 004.056.55

ЗАСТОСУВАННЯ БІКЛІК-АНАЛІЗУ ДО ШИФРУ КАЛИНА ТА ЙОГО МОДИФІКАЦІЙ

Ломаченко Ігор

Фізико-технічний інститут, Київський політехнічний інститут імені Ігоря Сікорського

Анотація

В даній роботі буде розглядатись відносно новий метод криптоаналізу, відомий як біклік-аналіз, у застосуванні до українського стандарту шифрування ДСТУ 7624:2014 (шифру Калина).

Для оригінального шифру було обґрунтовано його стійкість до біклік-аналізу. Для модифікацій шифру було одержано чисельні оцінки стійкості та показано захищеність від біклік-атак навіть для послаблених версій шифру.

Abstract

In this work we apply a recent method of cryptanalysis, known as biclique-analysis, to Ukrainian encryption standard DSTU 7624:2014 (Kalyna cipher).

We show that the original cipher is secure against biclique-analysis. For the modifications of the original cipher we estimate the security and show that even weakened version of cipher are secure against biclique-analysis.

Вступ

Не зважаючи на те, що біклік-аналіз виник досить недавно, в останні роки з'явилося багато робіт на цю тематику [1, 3, 4], в яких пропонувались методи вдосконалення самого аналізу, або наводились шляхи його застосування для побудови атак на існуючі шифри. Таким чином, можна сказати, що в даний момент активно розбудовується загальна методика біклік-аналізу та формуються нові підходи, що дадуть опору для нових ідей та відкриттів. Отже, отримання результатів застосування біклік-аналізу до конкретних шифрів є актуальною задачею.

З 2015 року в Україні діє новий національний стандарт шифрування ДСТУ 7624:2014 (шифр Калина) [2]. Дана робота присвячена дослідженню можливості застосування біклік-аналізу до шифру Калина.

Загальні відомості біклік-аналізу

Біклік-аналіз аналізу базується на принципі «Зустріч посередині» (англ. «Meet-in-the-middle»). Шифр E розбивається у композицію двох функцій g_1 та g_2 : $E = g_2 \circ g_1$.

Аналітик вибирає розбиття простору ключів на групи розміру 2^d , які представляються у вигляді матриць $K[i, j]$ розміру $2^d \times 2^d$. Для деякої пари відкритий текст — шифротекст (P, C) , отриманої на невідомому секретному ключі K_{secret} , аналітик обчислює 2^d значень $\vec{v}$ із P за допомогою перетворення g_1 та 2^d значень $\vec{v}$ з C :

$$\begin{aligned} P &\xrightarrow{K[i, \cdot]} \vec{v}, \\ \vec{v} &\xleftarrow{K[\cdot, j]} C. \end{aligned}$$

Пари, для яких $\vec{v} = \vec{v}$ формують кандидата в ключі $K[i, j]$. Позначимо через v одержане однакове проміжне значення.

Очікувана кількість кандидатів в ключі залежить від бітового розміру змінної $|v|$ та отримується за формулою $2^{2d-|v|}$. Для $|v|$, близьких до d або більших, атака має

перевагу над атаками повного перебору порядку 2^d , так як вона перевіряє 2^{2d} ключів менш ніж за 2^d викликів шифру.

Базова атака «зустріч посередині» має обмежене застосування у криптоаналізі блокових шифрів, так як внутрішня змінна v із зазначеними властивостями може бути знайдена лише для малої кількості раундів шифрування. Саме для подолання цієї перешкоди і застосовується концепція біклік [1].

Нехай f є під шифром, який відображує внутрішній стан S в шифртекст C : $f_K(S) = C$. f пов'язує 2^d внутрішніх станів $\{S_j\}$ з 2^d шифротекстами $\{C_i\}$ із урахуванням 2^{2d} ключів $\{K[i, j]\}$.

Триплет $\{\{C_i\}, \{S_j\}, \{K[i, j]\}\}$ називається d -вимірною біклікою, якщо виконується така умова:

$$C_i = f_{K[i, j]}(S_j)$$

для усіх $i, j \in \{0, \dots, 2^d - 1\}$. Інакше кажучи, в бікліці ключ $K[i, j]$ відображає внутрішній стан S_j в шифртекст C_i і навпаки.

Застосування біклік-аналізу до шифру Калина

Національний стандарт шифрування ДСТУ 7624:2014 (шифр Калина) [2] побудовано на основі структури SP-мережі. Він складається з декількох раундів шифрування (від 10 до 18), на кожному з яких виконується нелінійна заміна байтів стану (процедура SubBytes) та лінійне перемішування байтів стану (процедури ShiftRows та MixColumns). Стандарт підтримує різну довжину блоку: 128, 256, 512 бітів; відповідні варіанти алгоритму шифрування ми будемо позначати як Калина-128, Калина-256 та Калина-512.

Для проведення біклік-аналізу в першу чергу необхідно дослідити лавинні ефекти процедури шифрування та схеми генерації раундових ключів. На рисунку 1 схематично зображено зміни у байтах раундових ключів при їх генеруванні у шифрі Калина-512 з двох ключів шифрування, які відрізняються лише значенням першого байту.



Рисунок 1 — Лавинні ефекти при генеруванні раундових ключів шифру Калина-512

Як видно з рисунку, різниця лише в одному байті ключа шифрування дає непередбачувані зміни у всіх байтах раундових ключів при генеруванні. Аналогічні властивості мають місце для шифрів Калина-128 та Калина-256. З цього випливає, що бікліка, необхідна для здійснення атаки за методикою, наведеною у [1], не може бути побудована. Таким чином, атака на основі біклік на шифр Калина неможлива за рахунок особливостей ключового розкладу.

Застосування біклік-аналізу до модифікованого шифру Калина*

Розглянемо послаблені версії шифру Калина, що будуть містити такі модифікації.

1. Заміна схеми генерування раундових ключів шифру Калина на схему генерування раундових ключів, аналогічну шифру AES. Оскільки Калина є AES-подібним шифром, для неї легко адаптується схема генерування раундових ключів AES.

2. Замішування ключа за допомогою операції XOR. Шифр Калина застосовує для замішування ключа операції XOR та додавання за модулем. Дана модифікація замінює додавання за модулем на XOR, забезпечуючи замішування ключа завжди однією і тією ж

операцією.

3. Вилучення MixColumns з останнього раунду шифрування. Дана модифікація залишає в останньому раунді шифрування, окрім додавання з ключем, лише операції SubBytes та ShiftRows.

Будемо позначати через Калина* шифр Калина із зазначеними модифікаціями.

Для шифру Калина*-512 було побудоване розбиття ключового простору на 2^{496} груп по 2^{16} елементів в кожній. Також була побудована трьохраундова бібліка зі спорідненими ключовими диференціалами (див. [1]). Таким чином, співпадіння перевірялись після 15 раундів шифрування.

Для шифру Калина*-256 було побудоване розбиття ключового простору на 2^{240} груп по 2^{16} елементів в кожній. Була побудована трьохраундова бібліка зі спорідненими ключовими диференціалами. Співпадіння перевірялись після 11 раундів шифрування.

До шифру Калина*-128 навіть після модифікацій не вдалось застосувати атаку на основі біблік в чистому вигляді, так як «вузька» форма матриці (2 стовпчики по 8 байтів) унеможливує побудову бібліки, необхідної для проведення атаки.

Оцінки складності побудованих атак на основі біблік для модифікованих шифрів Калина* наведено у таблиці 1.

Таблиця 1 — Оцінки складності атак на розглянуті шифри

Назва шифру	Оцінка складності атаки
Калина*-512	$2^{511.81}$
Калина*-256	$2^{255.7682}$
Калина*-128	Атака неможлива через специфіку форми матриці

Висновки

У даній роботі була досліджена можливість застосування аналізу на основі біблік до національного стандарту шифрування України — шифру Калина. Для оригінального шифру Калина було обґрунтовано неможливість його безпосереднього біблік-аналізу за допомогою існуючих методик. Для модифікацій шифру Калина з різними розмірами блоків було застосовано підходи та методи біблік-аналізу, отримано чисельні оцінки стійкості.

З одержаних результатів випливає, що оригінальний шифр Калина є стійким до атак на основі біблік, так як навіть атаки на послаблені версії шифру мають дуже велику складність. Така стійкість забезпечується перемішувочними властивостями шифру, великою кількістю раундів, специфікою розміру матриці ключів та особливостями схеми генерування ключів.

Список використаних джерел:

1. Bogdanov A. Biclique cryptanalysis of the full AES / A. Bogdanov, D. Khovratovich, C. Rechberger // Proceedings of ASIACRYPT'11. — LSCN. — vol 7073. — Springer, 2011. — P. 344–371.

2. Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення: ДСТУ 7624:2014. — К.: Держспоживстандарт України, 2015. — 238 с.

3. Khovratovich D. Bicliques for preimages: Attacks on Skein-512 and the SHA-2 family [електронний ресурс] / D. Khovratovich, C. Rechberger, A. Savelieva. — Режим доступу: <http://eprint.iacr.org/2011/286.pdf>

4. Mala H. Biclique cryptanalysis of the block cipher Square [електронний ресурс] / H. Mala — Режим доступу: <http://eprint.iacr.org/2011/500.pdf>

РОЗРОБКА ОПТИМАЛЬНОЇ СИСТЕМИ МАСОВОГО ОБСЛУГОВУВАННЯ З ІДЕНТИФІКАТОРОМ СТАНУ ТА ЗОВНІШНЬОГО ОТОЧЕННЯ

Боровська Таїса, Кольцов Владислав, Кушнір Андрій, Северілов Віктор

Вінницький національний технічний університет

Анотація

Розроблена автоматизована система оптимального управління багатооб'єктними, багатоканальними, багатофазними системами масового обслуговування. Система будується на базі методології оптимального агрегування, згідно з якою складна система відображується в ієрархію підсистем. Модель кожної підсистеми має три компоненти – оптимальна еквівалентна функція класу «витрати, випуск», математична модель динаміки підсистеми і спостерігач стану і параметрів підсистеми. Розроблені математичні моделі цих компонентів, виконано тестування програмних модулів для підсистем і програми оптимізації і моделювання системи масового обслуговування в цілому.

Abstract

The automated system for optimal control of a multi-object, multi-channel and multiphase queuing system is developed. The system is developed on the basis of the methodology of optimal aggregation, according to which a complex system is mapped into the optimal equivalent production function. The models of the system and subsystems are represented by three components: - the optimal equivalent function of the class "costs, output", - the mathematical model of the dynamics of the system, and the mathematical model of the observer of the state and parameters. Mathematical models of these components have been developed, testing of program modules for subsystems and optimization program and modeling of the queuing system as a whole has been carried out.

Вступ

Розвиток виробництв взагалі та інформаційно-обчислювальних систем, зокрема, змінив функції і технології виконання функцій об'єктів класу «СМО». Тепер повинні відповідно змінитись моделі і методи наукового забезпечення СМО. Це стосується практики і теорії систем масового обслуговування. В США замість терміна «СМО» використовується «теорія черг». Це наслідок бурхливого розвитку телефонізації та автомобілізації. Однак, ще тоді прогресивні вчені вважали, що мета СМО не аналізи черг, а створення систем без черг. Сьогодні найскладніші системи обслуговування в автопромі, де домінуючі технології забезпечення процесу виробництва – «постачання точно в строк», а черги – малі, але перспективні неприємності. Згідно теорії СМО існують багатоканальні, багатофазні СМО. Неважко додати ще багатооб'єктність – аналог «багатопродуктовості». На рис. 1 подано концепцію побудови узагальненої моделі СМО. База концепції достатньо обґрунтована і напрацьована [1, 2]. Перший крок в розробці – оптимальне агрегування, результат якого – отримання оптимальної еквівалентної функції виробництва (ОЕФВ) послуг, параметризованої. Другий крок – побудова системи моделей динаміки системи масового обслуговування і її підсистем. Третій крок – побудова відповідної моделі спостерігача. Оптимальна з точки зору управління СМО – одноканальна, однофазна. Об'єкту обслуговування теж зручно, коли послуга відноситься до класу «все включено».

Тепер можемо сформулювати «центральну проблему управління СМО – розподілених і стохастичних. Необхідно створити оптимальну адаптивну систему управління СМО як цілісним об'єктом, з одним входом – це наявні ресурси і потрібний обсяг обслуговування, з одним виходом – сумарним ефектом (доходом, прибутком, обсягом обслуговування).

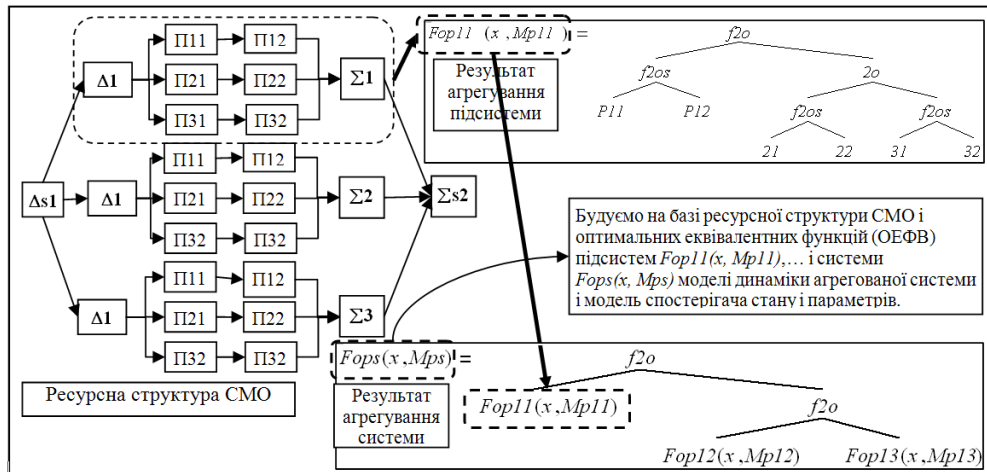


Рисунок 1 – Концепція узагальненої моделі СМО

Обґрунтування вибору

Вибираємо ресурсне управління: розподіл потоків заявок на обслуговування і відповідних ресурсів між підсистемами СМО – каналами обслуговування. Вибираємо для управління СМО методологію оптимального агрегування [1, 2]. Методи оптимального агрегування призначені для оптимізації систем класу «витрати, випуск», до якого відносяться системи виробництва матеріальних та інтелектуальних продуктів та послуг. Тобто і СМО відносяться до класу виробничих систем. Суть методів оптимального агрегування. Довільна ресурсна структура виробничої системи може бути ізоморфно відображена в бінарне дерево оптимального агрегування. В середовищах математичних пакетів бінарне дерево – це формула в структурному виді для рішення задачі оптимального розподілу ресурсів між всіма підсистемами. Результат оптимізації – не точечне рішення, а оптимальна еквівалентна функція «витрати випуск» системи (ОЕФВ). Результат оптимізації (операнд результату агрегування) – матриця, яка крім ОЕФВ містить оптимальні рішення для всіх підсистем. При оптимальному агрегуванні обчислюються оптимальні управління для системи в цілому і для всіх підсистем. Переваги методів оптимального агрегування. Обмеження математичні на функції «витрати, випуск» - тільки нестрога монотонність. Ці функції можуть бути розривними, ступінчастими, стохастичними. В існуючих методах обмеження - це випуклість, неперервність та ін.

Приклади практичної реалізації

Напрямок даної роботи – фундаментальний, він не має близьких аналогів. Його специфіка – результативність і корисність тільки в програмному середовищі. Чи не є концепція на рис. 1 неконструктивною абстракцією без інтерпретацій? В методології оптимального агрегування це перевіряється створенням відповідних програм. Запропонована концепція побудови узагальненої СМО потребує ефективних модулів динаміки для підсистем, без типових обмежень на класи нелінійностей. На рис. 2 подано приклад оператора переходу між станами для довільних СМО – один з багатьох [1, 2]. Вся специфіка і складність об'єкта «упакована» в підпрограмах. В підсумку (нижній рядок) отримуємо «псевдо-одновимірне різницеве рівняння». Це зручно користувачеві для розуміння, і головній програмі для виконання.

На рис. 3 подано схему операцій, результатом якої є оптимальна адаптивна система управління виробництвом. Схема складається з: послідовності агрегувань; бінарного дерева оптимального агрегування, що є рішенням задачі нелінійного програмування; послідовності однорівневих оптимальних агрегувань; отримання моделей динаміки об'єктів і спостерігачів.

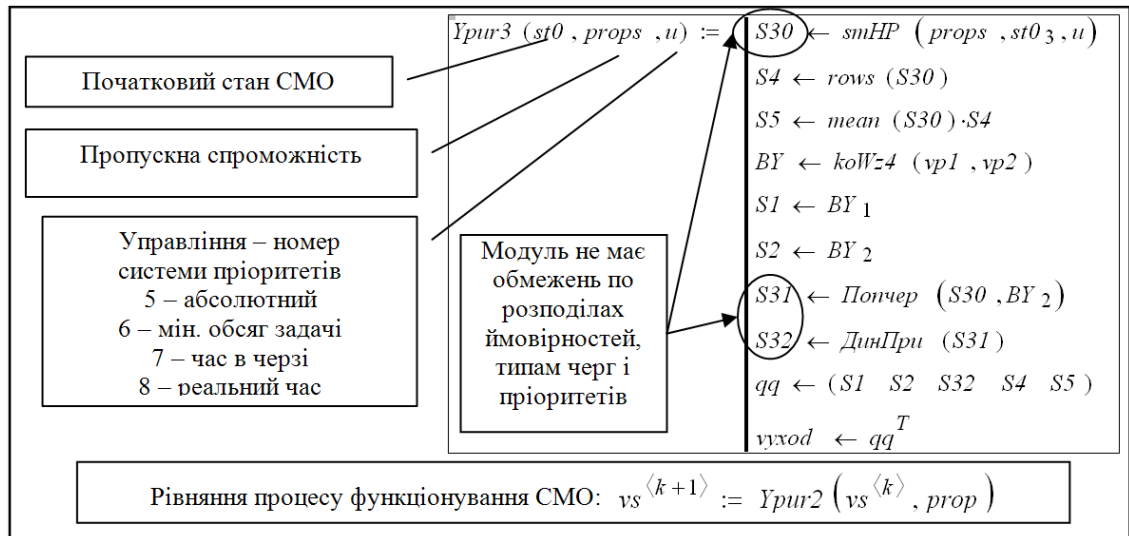


Рисунок 2 – Модуль «оператор переходу між станами СМО». Приклад

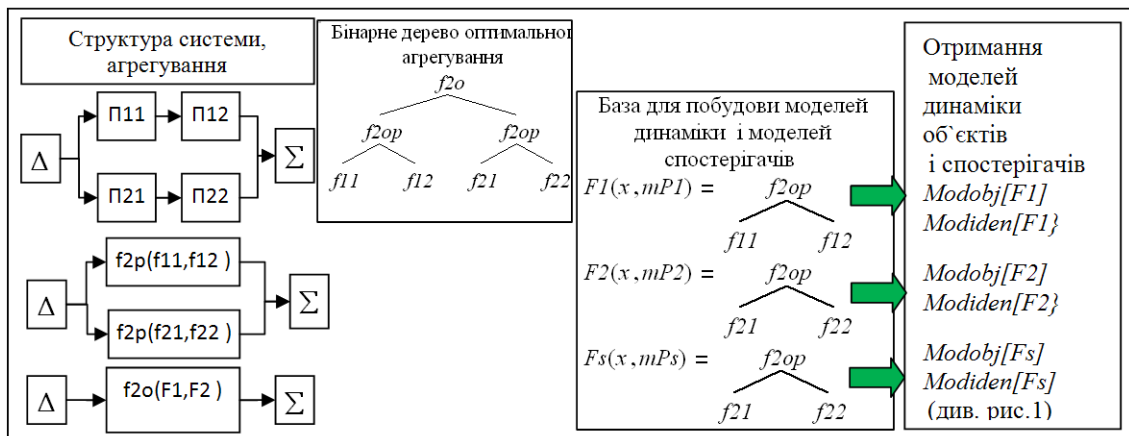


Рисунок 3 – Схема формування системи спостерігачів оптимально агрегованої СМО

Висновки

Поставлена складна задача оптимального адаптивного управління для багатоканальних і багатофазних СМО без обмежень на розмірність об'єкта, на клас функцій обслуговування і розподіли ймовірностей потоків заявок. Запропоновано, обґрунтовано і реалізується нове рішення на базі методології оптимального агрегування. Параметризація рішення задачі оптимального агрегування дозволяє реалізувати адаптацію управління до зміни розподілів ймовірностей вхідних потоків заявок. Виконане тестування модулів.

Список використаних джерел:

1. Боровська Т. М. Метод оптимального агрегування в оптимізаційних задачах: монографія / Т. М. Боровська, І. С. Колесник, В. А. Северілов. – Вінниця: УНІВЕРСУМ–Вінниця, 2009. – 229 с. – ISBN 978–966–641–285–3.
2. Боровська Т. М. Моделювання і оптимізація процесів розвитку виробничих систем з урахуванням використання зовнішніх ресурсів та ефектів освоєння: монографія / [Т. М. Боровська, С. П. Бадьора, В. А. Северілов, П. В. Северілов]; за заг. ред. Т. М. Боровської. – Вінниця: ВНТУ, 2009. – 255 с. – ISBN 978–966–641–312–6.

НАВЧАЛЬНИЙ ДОДАТОК ДЛЯ ДОСЛІДЖЕННЯ ГОРБКОВОГО АЛГОРИТМУ

Сілагін Олексій, Лученко Микола, Поліщук Богдан

Вінницький національний технічний університет

Анотація

Запропонований матеріал описує процес створення навчального додатку для дослідження Горбкового алгоритму. Цей алгоритм застосовується при створенні реалістичних 3-D ландшафтів та терраморфінгу засобами фрактальної графіки. Може бути використаний при вивченні розділу «Фрактальна графіка» дисципліни «Комп'ютерна графіка», а також при створенні програмних засобів «віртуальної реальності».

Abstract

The proposed material describes the process of creating a training appendix for the study of Gorbkov algorithm. This algorithm is used to create realistic 3-D landscapes and terramorphing with fractal graphing tools. It can be used in the study of the section "Fractal graphics" of the discipline "Computer Graphics", as well as when creating software "virtual reality"..

Вступ

Поява фрактальної графіки в свій час відкрила цілу галузь, пов'язану зі створенням реалістичних 3-D сцен та ландшафтів для різних застосувань, пов'язаних зі створенням «віртуальної реальності», таких як комп'ютерні ігри, комп'ютерна анімація та кінематографія, автоматизоване навчання та проектування і т.д. Серед засобів створення «віртуальної реальності» потрібно відмітити такі базові алгоритми, як «Шум Перліна» або Горбковий алгоритм, численні модифікації яких дають можливість імітувати поверхню потоку води, виверження вулканів, гірські ландшафти та інше. Для дослідження можливостей цих алгоритмів, а також для створення та апробації подібних модифікацій пропонується створений навчальний додаток.

Реалізація базового горбкового алгоритма

Це досить простий ітераційний алгоритм, що використовує декілька вхідних параметрів [1]. Алгоритм викладений в наступних кроках:

- створюється двомірний масив та ініціалізується нульовим рівнем (заповнюється всі осередки нулями);
- береться випадкова точка на ландшафті або біля його меж (за межами), а також береться випадковий радіус в заздалегідь заданих межах. Вибір цих меж впливає на вигляд ландшафту, - або він буде пологим, або скелястим;
- у вибраній точці "піднімаємо" горб заданого радіусу;
- повертаємось до другого кроку і так далі до вибраної кількості кроків, від нього потім залежатиме зовнішній вигляд нашого ландшафту;
- проводиться нормалізація ландшафту;
- проводиться "долинізацію" ландшафту.

Генерація горба

Фактично горб - це в нашому випадку половина параболоїда, чим більше радіус - тим більше горб (і вище). Математично це схоже на перевернуту параболу, що описується формулою (1):

$$z = r^2 - ((x_2 - x_1)^2 + (y_2 - y_1)^2) \quad (1)$$

тут (x_1, y_1) - задана точка, r - вибраний радіус, (x_2, y_2) - висота горба.

Щоб згенерувати ландшафт повністю необхідно побудувати безліч таких горбів. Але є ще дві речі на яких необхідно звернути увагу. Перше - необхідно ігнорувати негативні значення висоти горба. Друге - при генерації подальших горбів краще додавати набутого значення для даного горба до вже існуючих значень. Це дозволяє побудувати більш правдоподібніший ландшафт.

Нормалізація Ландшафту

При генерації значень для ландшафту потрібно враховували виходи цих значень за деякі межі (наприклад - якщо потім ландшафт зберігатиметься в монохромній картинці, то необхідно, щоб всі значення знаходилися в межі від 0 до 256). Для цього необхідно провести нормалізацію значень. Математично нормалізація - це процес набуття значень з одних меж, і переклад його в інші межі.

Для нормалізації проводяться наступні дії:

Аналізуються значення елементів всього масиву і запам'ятовуються найбільше і найменше значення;

Для кожного елемента масиву проводиться нормалізація в межі від 0 до 1 за формулою (2):

$$Z_{\text{norm}} = (z - z_{\text{min}}) / (z_{\text{max}} - z_{\text{min}}) \quad (2)$$

Після цього ландшафт нормалізований і до нього може бути застосована «долинізація» [2].

"Долинізація" ландшафту

Взагалі кажучи, даний ландшафт вже можна використовувати, але, якщо придивитися, то в ньому достатньо мало долин. Схили горбів надмірно круті, хочеться зробити їх пологішими. У цьому допоможе попередній крок – нормалізація. Всі значення у нас зараз знаходяться в межах від 0 до 1. Ідея "долинізації" полягає в наступному - узяти від кожного значення квадратний корінь. Це більшою мірою впливає на середні значення, практично не зачіпаючи мінімумів і максимумів..

Висновки

З використанням описаного алгоритму та графічних бібліотек OpenGL та DirectX, а також візуальної компонентної бібліотеки GLScene(із додатком ігрового ядра), досить легко будувати реалістичні 3-D ландшафти, що може бути використано в учбовому процесі при дослідженні модифікацій горбкового алгоритма.

Список використаних джерел:

1. Сайт 3D Accelerator. Стаття Генерація трехмерных ландшафтов. Режим доступу: <http://www.3daccelerator.com.ua/articles.html>
2. Сайт Введение в компьютерную графику. Визуализация природных явлений. Режим доступу: http://graphicon.ru/oldgr/courses/cg02b/assigns/hw-5/hw5_cld.htm
3. І. Арсенюк, О.Сілагін, С.Кукунін. Застосування апарату нечіткої логіки для оцінки якості графічних растрових зображень. // Збірник праць Дев'ятої Міжнародної науково практичної конференції «Інтернет-Освіта-Наука» (ІОН-2014). – Вінниця: ВНТУ, 2014. – С. 223 – 225.

THE MATHEMATICS OF HARMONY. FROM EUCLID TO CONTEMPORARY MATHEMATICS, COMPUTER SCIENCE AND MODERN MATHEMATICAL EDUCATION

Alexey Stakhov

Computer firm "FibTech"

Abstract

One may wonder what place in the general theory of mathematics is occupied by Mathematics of Harmony created by Prof. Stakhov? It seems to me, that in the last centuries, as Nikolay Lobachevsky said, "mathematicians turned all their attention to the Advanced Parts of Analytics, neglecting the origins of Mathematics and not willing to dig the field that already been harvested by them and left behind." As a result, this created a gap between "Elementary Mathematics" - basis of modern mathematical education, and "Advanced Mathematics". In my opinion, the Mathematics of Harmony developed by Prof. Stakhov fills up that gap. I.e., "Mathematics of Harmony" is a big theoretical contribution, first of all to the development of "Elementary Mathematics" and as such should be considered of great importance for mathematical education.

From Academician Mitropolsky's commentary on the scientific research of Ukrainian scientist Alexey Stakhov.

The present speech is based on author's book "The Mathematics of Harmony. From Euclid to Contemporary Mathematics and Computer Science" (World Scientific, 2009) [1] and other newest author's publications in the "World Scientific" [2,3] and the International Journals "Chaos, Solitons and Fractals", "Congressus Numerantium", "The Computer Journal", "Applied Mathematics", "British Journal of Mathematics and Computer Science" [4-27].

The main goal of the speech is to discuss author's experience in teaching of the course "Mathematics of Harmony and Golden Section" for students of the Mathematics and Physics Faculty of the Vinnitsia Pedagogical University (2001-2002 academic year). Abramchuk's article [28] is the beginning of this discussion.

The author submits the following questions for discussion:

1. Pythagorean MATHEM's as the most important parts of mathematics
2. The "Golden" Section and Platonic Solids in Euclid's Elements
3. Proclus hypothesis as new view on Euclid's Elements
4. Turing phyllotaxis
5. The mine motives of the American mathematicians for the creation of modern theory of Fibonacci numbers
6. Binet formulas and the "golden" hyperbolic Fibonacci and Lucas functions as the basis for Bodnar's geometry of phyllotaxis as continuation of Turing phyllotaxis
7. Gazale formulas and Spinadel "metallic" proportions as the basis of the hyperbolic lambda functions
8. The "Golden" Non-Euclidean geometry and new challenge for theoretical natural sciences
9. The numeral systems with irrational bases as the fundamentals of new computer science and digital metrology for mission-critical applications
10. Program of the course "Mathematics of Harmony and Golden Section" [29]

References:

1. Alexey Stakhov. Assisted by Scott Olsen. "The Mathematics of Harmony. From Euclid to Contemporary Mathematics and Computer Science", World Scientific, 2009

2. Alexey Stakhov, Samuil Aranson. Assisted by Scott Olsen. The “Golden” Non-Euclidean Geometry: Hilbert’s Fourth Problem, “Golden” Dynamical Systems, and the Fine-Structure Constant, World Scientific, 2016.
3. Alexey Stakhov. Numeral Systems with Irrational Bases for Mission-Critical Applications. World Scientific, 2016
4. Stakhov A.P. The Golden Section in the Measurement Theory, Computers & Mathematics with Applications, 1989, Vol. 17, No 4-6, 613-638
5. Stakhov A.P. The Golden Section and Modern Harmony Mathematics. Applications of Fibonacci Numbers, Kluwer Academic Publishers, Vol. 7, 1998. 393 – 399
6. Stakhov A.P. Brousentsov’s ternary principle, Bergman’s number system and ternary mirror-symmetrical arithmetic // The Computer Journal, 2002, Vol. 45, No. 2, 221-236.
7. Стахов А.П. Обобщенные золотые сечения и новый подход к геометрическому определению числа. // Украинский математический журнал, 2004, Vol. 56, No. 8, 1143-1150.
8. Стахов А.П. Золотое сечение, священная геометрия и математика гармонии. Метафизика. Век XXI. Сборник трудов. Москва: Бином, 2006. – 174-215
9. Stakhov A., Rozin B. On a new class of hyperbolic function // Chaos, Solitons & Fractals, 2005, Vol. 23, Issue 2, 379-389. <http://www.trinitas.ru/rus/doc/0232/004a/02321042.htm>
10. Stakhov A.P. Fundamentals of a new kind of Mathematics based on the Golden Section // Chaos, Solitons & Fractals 2006, Vol. 27, Issue 5, 1124-1146. <http://www.trinitas.ru/rus/doc/0232/004a/02320042.htm>
11. Stakhov AP. The generalized golden proportions, a new theory of real numbers, and ternary mirror-symmetrical arithmetic // Chaos, Solitons & Fractals, 2007, Vol. 33, Issue 2, 315-334. <http://www.trinitas.ru/rus/doc/0232/004a/02321043.htm>
12. Stakhov A.P. The Generalized Principle of the Golden Section and its applications in mathematics, science, and engineering // Chaos, Solitons & Fractals, 2005, Vol. 26, Issue 2, 263-289. <http://www.trinitas.ru/rus/doc/0232/004a/02320043.htm>
13. А.П. Стахов, Три «ключевые» проблемы математики на этапе ее зарождения и новые направления в развитии математики, теоретической физики и информатики // «Академия Тринитаризма», М., Эл № 77-6567, публ.14135, 12.01.2007 <http://www.trinitas.ru/rus/doc/0232/004a/02321064.htm>
14. Stakhov A.P. Gazale formulas, a new class of the hyperbolic Fibonacci and Lucas functions, and the improved method of the “golden” cryptography // Moscow: Academy of Trinitarism, № 77-6567, publication 14098, 21.12.2006 <http://www.trinitas.ru/rus/doc/0232/004a/02321063.htm>
15. Stakhov A.P. The Mathematics of Harmony: Clarifying the Origins and Development of Mathematics // Congressus Numerantium, 193, 2008, 5-48.
16. Stakhov A.P., Aranson S.Ch. “Golden” Fibonacci Goniometry, Fibonacci-Lorentz Transformations, and Hilbert’s Fourth Problem // Congressus Numerantium, 193, 2008, 119-156.
17. Stakhov A.P., Aranson S.Ch. Hyperbolic Fibonacci and Lucas Functions, “Golden” Fibonacci Goniometry, Bodnar’s Geometry, and Hilbert’s Fourth Problem. Part I. Hyperbolic Fibonacci and Lucas Functions and “Golden” Fibonacci Goniometry. Applied Mathematics. 2011, No 2.
18. Stakhov A.P., Aranson S.Ch. Hyperbolic Fibonacci and Lucas Functions, “Golden” Fibonacci Goniometry, Bodnar’s Geometry, and Hilbert’s Fourth Problem. Part II. A New Geometric Theory of Phyllotaxis (Bodnar’s Geometry. Applied Mathematics. 2011, No 3.

19. Stakhov A.P., Aranson S.Ch. Hyperbolic Fibonacci and Lucas Functions, "Golden" Fibonacci Goniometry, Bodnar's Geometry, and Hilbert's Fourth Problem. Part III. An Original Solution of Hilbert's Fourth Problem. Applied Mathematics. 2011, No 4.
20. Alexey Stakhov. A History, the Main Mathematical Results and Applications for the Mathematics of Harmony. Applied Mathematics, 2014, 5, 363-387
<http://www.scirp.org/journal/PaperInformation.aspx?PaperID=42742>
[file:///C:/Users/Alexey/Downloads/AM_2014021110492376%20\(12\).pdf](file:///C:/Users/Alexey/Downloads/AM_2014021110492376%20(12).pdf)
21. Alexey Stakhov. The Mathematics of Harmony. Proclus' Hypothesis and New View on Euclid's Elements and History of Mathematics Starting since Euclid. Applied Mathematics, Dec 2014, 5
[file:///C:/Users/Alexey/Downloads/AM_2014120110525820%20\(1\).pdf](file:///C:/Users/Alexey/Downloads/AM_2014120110525820%20(1).pdf)
http://www.scirp.org/Journal/Home.aspx?IssueID=5748#.Vii0I9KrT_w
22. Alexey Stakhov. The "Golden" Number Theory and New Properties of Natural Numbers. British Journal of Mathematics & Computer Science 11(6): 1-15, 2015, Article no.BJMCS.21385
[file:///C:/Users/Alexey/Downloads/Stakhov1162015BJMCS21385%20\(11\).pdf](file:///C:/Users/Alexey/Downloads/Stakhov1162015BJMCS21385%20(11).pdf)
<http://sciencedomain.org/review-history/11417>
23. Alexey Stakhov. Proclus Hypothesis. British Journal of Mathematics & Computer Science, 13 (6), 1-22, 2016
24. Alexey Stakhov, Samuil Aranson. Hilbert's Fourth Problem as a Possible Candidate on the MILLENNIUM PROBLEM in Geometry. British Journal of Mathematics & Computer Science, 12 (4), 1-25, 2016
25. Alexey Stakhov. Fibonacci p-codes and Codes of the Golden p-proportions: New Informational and Arithmetical Foundations of Computer Science and Digital Metrology for Mission-Critical Applications. British Journal of Mathematics & Computer Science, 17 (1), 1-49, 2016
26. Alexey Stakhov, Samuil Aranson. The Fine-Structure Constant as the Physical-Mathematical MILLENNIUM PROBLEM. Physical Science International Journal, 9 (1), 1-36, 2016.
27. Alexey Stakhov. The importance of the Golden Number for Mathematics and Computer Science: Exploration of the Bergman's system and the Stakhov's Ternary Mirror-symmetrical System (Numeral Systems with Irrational Bases). British Journal of Mathematics & Computer Science, 2016, 18(3): 1-34
28. Абрамчук В.С. Отзыв кафедры математики Винницкого государственного педагогического университета на курс лекций «Математика Гармонии и Золотого Сечения» // «Академия Тринитаризма», М., Эл № 77-6567, публ.12457, 26.09.2005
<http://www.trinitas.ru/rus/doc/0232/006a/02320006.htm>
29. Стахов А.П. Программа курса «Математика Гармонии и Золотого Сечения» для физико-математических факультетов педагогических университетов // «Академия Тринитаризма», М., Эл № 77-6567, публ.12437, 20.09.2005
<http://www.trinitas.ru/rus/doc/0232/006a/02320003.htm>



ОДИНАДЦЯТА МІЖНАРОДНА КОНФЕРЕНЦІЯ
ІОН - 2018
ІНТЕРНЕТ-ОСВІТА-НАУКА-2018



**СЕКЦІЯ Е. КОМП'ЮТЕРНІ ТЕХНОЛОГІЇ ТА
ІНТЕРНЕТ В ІНФОРМАЦІЙНОМУ
СУСПІЛЬСТВІ**



THE ELEVENTH INTERNATIONAL
CONFERENCE
IES-2018
INTERNET-EDUCATION-SCIENCE - 2018



**SECTION E. COMPUTER TECHNOLOGIES AND
THE INTERNET IN INFORMATIONAL SOCIETY**



ОДИНАДЦАТАЯ МЕЖДУНАРОДНАЯ
КОНФЕРЕНЦИЯ
ИОН-2018
ИНТЕРНЕТ– ОБРАЗОВАНИЕ – НАУКА 2018



**СЕКЦІЯ Е. КОМП'ЮТЕРНІ ТЕХНОЛОГІЇ
И ИНТЕРНЕТ В ИНФОРМАЦИОННОМ
ОБЩЕСТВЕ**



ДОСЛІДЖЕННЯ МАШИННОГО ПЕРЕКЛАДУ ЗА ДОПОМОГОЮ ПРОГРАМИ PRAGMA

Котик Ольга, Кунанець Наталія

Національний університет "Львівська політехніка"

Анотація

Ця стаття присвячена дослідженню машинного перекладу за допомогою програми Pragma. Проаналізовано останні дослідження перекладу за допомогою комп'ютерних програм, які досліджувало багато науковців. Розглянуто розвиток інформаційних технологій для процесів двомовних перекладів за допомогою програми Pragma та наведено приклад перекладу даною системою. Зроблені висновки про доцільність її використання.

Abstract

This article is devoted to the study of machine translation using the Pragma program. Recent research studies of computer programs, which many scholars have researched, are analyzed. The development of information technologies for bilingual translation processes with the help of Pragma program is considered and an example of translation by this system is given. Conclusions about expediency of its use are made.

Вступ

Процеси глобалізації сучасного світу, генерує потребу в налагодженні комунікації. В 190 країнах живе майже сім мільярдів населення Землі, які розмовляють майже 2 тисячами мов. Інформаційні технології дозволяють передати частину роботи перекладачів комп'ютерам.

Аналіз останніх досліджень

Проблеми перекладу за допомогою комп'ютерних програм досліджувало багато науковців, виділяючи у них окремі задачі. Можна виділити публікації Алекса Вэйбеля, Анісімова В., І.А. Большакова, В.В. Вороновича, Франза Джосефа Оч, Б. Лавуа, Т. Корельського, А.Л. Міщенко, Палія С.В. та інших.

Мета публікації

Проаналізувати тенденції щодо розвитку інформаційних технологій для процесів двомовних перекладів.

Історія розвитку технологій перекладу

В останні роки спостерігається чітка тенденція на розширення спектру програмних продуктів для перекладу, зокрема безкоштовних та доступних он-лайн. Такі програмні продукти потребують значної обчислювальної потужності сервера, для забезпечення високої швидкодії при перекладі великих обсягів лінгвістичних даних в реальному часі. При встановленні цих програм на комп'ютері користувача, швидкість перекладу значно знижується. Он-лайн перекладачі провідних ІТ фірм користуються не лише своєю базою даних текстів, але і порівнюють результати перекладу з текстами, наявними у Інтернеті, що покращує технологію перекладу.

Першим технології машинного перекладу застосував Ч. Беббідж, реалізуючи проект щодо розроблення механічного прототипу електронних цифрових обчислювальних машин у першій половині 19 століття. Технології ускладнювалися в середині 30-х років було запатентовано виготовлення механічних пристроїв, що забезпечували двомовний переклад текстів. Згодом майже паралельно різними дослідниками були розроблені автоматичні двомовні словники, які записувалися на перфострічці. Створений прилад містив двомовний словник, спроможний оперувати

граматичними рисами за правилом мови есперанто. Пристрій міг розділяти слова за синтаксичними функціями та логічними формами, здійснювати переклад на необхідну мову, редагувати отриманий текст.

Вперше технологію машинного перекладу на комп'ютері було запропоновано фонду Рокфеллера Уорреном Вівером. Згодом розпочалися тривалі експерименти у багатьох університетах Сполучених Штатів, і вже 7 січня 1954 р. в головному офісі IBM у Нью-Йорку вперше було здійснено публічний показ роботи системи машинного перекладу.

Впродовж 1990-х років інтенсифікувалися дослідження в цьому напрямі, ґрунтуючись на інноваційних технологіях розпізнання та синтезу мови. Від тоді засоби машинного перекладу стали доступними для широкого загалу користувачів [3].

Одним із зручних програмних продуктів, що забезпечує машинний переклад текстів є *Pragma 6.x* від компанії *Trident Software*. Програмний продукт забезпечує двомовний переклад текстів англійською, російською, німецькою і українською мовами. Дана компанія використовує власну технологію перекладу, що базується на використанні оригінальних словників (загальний і близько 100 тематичних), які містять понад 800 тис. слів і виразів[2].

Pragma є інтегрованим набором програмних компонентів, сформованим за функціонально-модульним принципом. Різні конфігурації формуються шляхом додавання потрібних модулів до опорної системи. Програмний продукт не має окремого середовища перекладу, він вбудовується як застосунок, в середовища, призначені для роботи з текстом, такі як: *Microsoft Word*, *Microsoft Outlook*, *Outlook Express*, *Internet Explorer*, *WordPad*, *Notepad*. Список підтримуваних застосунків безперервно розширюється. В список вбудованих застосунків нещодавно увійшли *OpenOffice.org* і *StarOffice*[1].

Функціонал програми дозволяє користувачу обирати напрям перекладу, задавати місце розміщення перекладеного фрагменту, наприклад у тому ж файлі, що й оригінал або створювати для збереження результатів перекладу окремий файл. Для підвищення якості перекладу користувачем налаштовується предметна область, до якої належить текст, що забезпечує використання впорядкованого набору термінологічних словників.

Розробники програмного продукту надали переваги коректорам словників. З його допомогою відбувається редагування перекладу відомих слів, формування словникових масивів нової тематики. Усі зміни накопичуються в словнику користувача, який має вищий пріоритет в порівнянні з системним. Всю накопичену користувачем в ході перекладів інформацію можна зберігати і переносити на інші комп'ютери за допомогою операцій експорту/імпорту.

Було проведено ряд експериментів, щодо перекладу текстів різної тематики. Результат одного з них, який передбачав можливість перекладу тексту українською мовою із вкрапленнями англійських запозичень, поданих латиницею слова.

Тестування відображає хороші результати, зміст тексту передається повністю. Програма коректно розпізнала додані латиницею терміни (див рис.1).

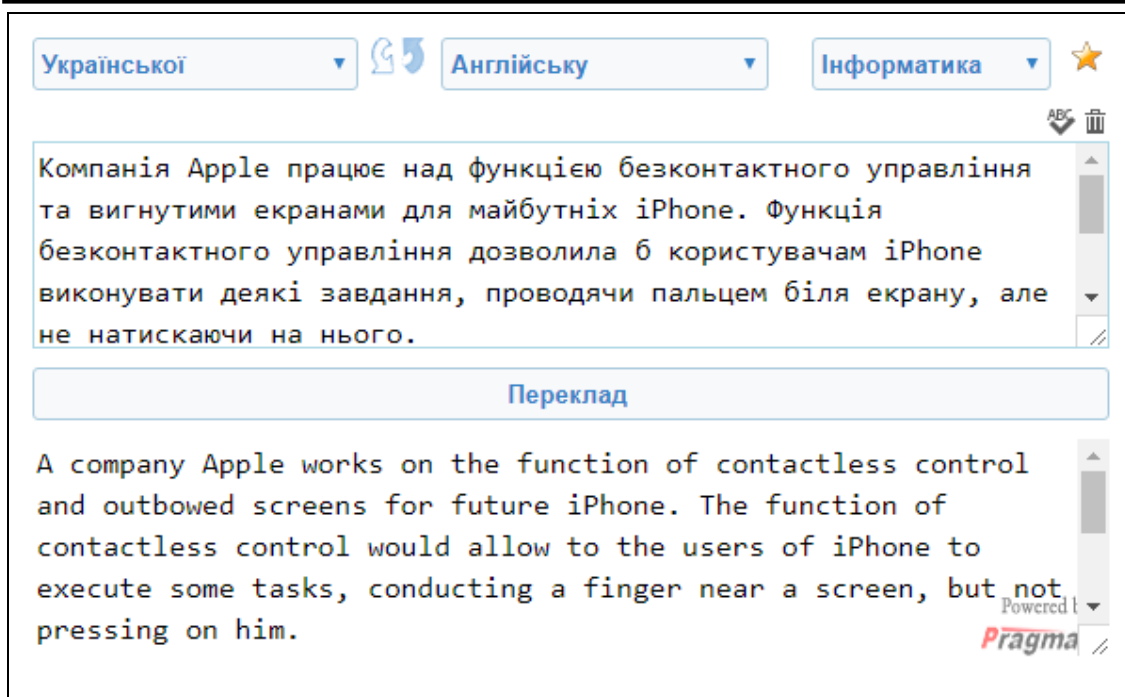


Рисунок 1 – Вікно програми Pragma з результатами перекладу

Програми машинного перекладу можна розглядати як хороший інструмент як для професійних перекладачів, так і для повсякденного використання. Для професійних перекладачів передбачається підготовка тексту, з метою подальшого редагування мовником. Для повсякденного використання досягається розуміння загального змісту тексту. Дослідження можливостей Pragma 6.x засвідчило той факт, що, незважаючи на постійне вдосконалення, програми – переклад текстів для пари мов, що належать до різних груп, може використовуватися лише як допоміжний інструмент. Досягти якісного перекладу можливо лише залучивши фахівця людину, яка наділена перекладацьким талантом.

Однак використання машинного перекладу доцільне при необхідності загального ознайомлення зі змістом науково-технічного або суспільно-політичного спрямування документу малознайомою мовою.

Список використаних джерел:

1. Pragmatichnyj perevodchik [Електронний ресурс]: Режим доступу – https://itc.ua/articles/pragmatichnyj_perevodchik_17549/
2. Комп'ютерний переклад для усіх [Електронний ресурс]: Режим доступу – <http://www.translate.ua/uk/company>
3. Hutchins, J. (1986) Machine Translation: past, present, future (Chichester : Ellis Horwood) ISBN [Електронний ресурс]: Режим доступу – <http://www.traduceme.org/profiles/blogs/history-of-machine-translation>

О НЕКОТОРЫХ АЛГОРИТМАХ РАЗМЫТИЯ ИЗОБРАЖЕНИЙ И СРАВНИТЕЛЬНЫЙ АНАЛИЗ ИХ ПРОГРАММНЫХ РЕАЛИЗАЦИЙ

Бенидзе Нана, Габисония Инга

Сухумский государственный университет, Тбилиси, Грузия

Аннотация

В данной работе проанализированы некоторые виды алгоритмов размытия, широко применяемых в компьютерной графике, методы их программной реализации на языке программирования C++, которые позволяют в ряде случаев повысить скорость работы (быстродействие) алгоритмов. А также даны эмпирические оценки при распараллеливании вычислительных процессов.

Abstract

In this paper, we analyzed some types of Blur Algorithms that are widely used in computer graphics; also methods of their software implementation in the C++ programming language, which allow in some cases to increase the speed of the algorithms. And also empirical estimates are given for Parallelizing Computational processes.

Введение

В компьютерной графике широко применяются различные виды размытия изображений. Существует большой класс разработанных алгоритмов размытия, которые применяются в графических программах. Данные алгоритмы также полезны при сжатии графических изображений, так как размытые изображения достаточно удобно сжимаемы и хорошо обрабатываемы. Поэтому данные в работе эмпирические оценки для некоторых классов алгоритмов могут быть весьма полезны в практических реализациях.

Существует достаточно большое количество алгоритмов размытия изображений, применяемых в различных графических редакторах, причем они практически постоянно совершенствуются. Несмотря на известность математической составляющей данного класса алгоритмов, при программной реализации встречается множество "подводных камней", связанных с реализацией алгоритмов на конкретном языке программирования. Интересен также вопрос о распараллеливании вычислений, так как даже для сложных алгоритмов заметные результаты с целью ускорения работы достигаются уже в случае четырехъядерных процессоров (восьмипоточные алгоритмы).

Наиболее распространенным, но не всегда наилучшим, является Алгоритм Гаусса, основанный на классическом N -мерном преобразовании Гаусса, которое имеет вид:

$$G(r) = \frac{1}{(2\pi\sigma^2)^{N/2}} e^{\frac{-r^2}{2\sigma^2}},$$

В двумерном случае можно записать в виде:

$$G(u, v) = \frac{1}{2\pi\sigma^2} e^{\frac{u^2+v^2}{2\sigma^2}},$$

где r -радиус размытия $r^2 = u^2 + v^2$, σ - стандартное отклонение распределения Гаусса. Так, в случае двух измерений этой формулой задается семейство концентрических окружностей с распределением Гаусса от центральной точки. Значение каждого из пикселей будет средне взвешенным для соседних пикселей. Исходное значение пикселя принимает наибольшее гауссово значение, а соседние пиксели

принимают меньшие значения (веса), которые зависят от расстояния до них. В практических реализациях при работе с дискретным преобразованием Гаусса в алгоритмах не учитываются те пиксели, расстояние до которых больше, чем 3σ из-за малости значений. Последнее означает достаточность расчета матрицы размером $[6\sigma] \times [6\sigma]$ для приемлемой точности приближения. Удобность применения Гауссовых преобразований в силу свойства линейной сепарабельности (т.е. свойства факторизации) вместо применения двумерной матрицы сводится к применению двух одномерных матриц по горизонтальному и вертикальному направлениям. Данный факт позволяет снизить объем вычислений до $O(n \times M \times N) + O(m \times M \times N)$ вместо $O(n \times m \times M \times N)$ для несепарабельной матрицы свертки (ядра), где M, N -размеры фильтруемого изображения, m, n -размеры ядра фильтра.

Обычно при программной реализации преобразование осуществляется над окном, состоящим из пикселя, находящегося в центре и восьми соседних обрамляющих пикселей, причем каждый из этих девяти пикселей разбивается на составляющие в цветовой модели (наиболее часто применима модель - RGB). При применении преобразования нужно нормализовать коэффициенты в диапазоне (0...255). В работе также анализируются результаты работы алгоритмов, в которых применяются рекуррентные соотношения, что заметно ускоряет процесс вычислений.

В данной работе проанализированы некоторые виды алгоритмов размытия, методы их программной реализации на C++, которые позволяют в ряде случаев повысить скорость работы (быстродействие) алгоритмов. А также даны эмпирические оценки при распараллеливании вычислительных процессов. Приведены программные коды, иллюстрирующие эти эмпирические оценки.

Список использованных источников:

1. Frederick M. Waltza and John W. V. Millerb, "An efficient algorithm for Gaussian blur using finite-state machines", a2095 Delaware Avenue, Mendota Heights, MN 55118-4801 USA bECE Department, Univ. of Michigan-Dearborn, Dearborn, MI 48128-1491 USA, SPIE Conf. on Machine Vision Systems for Inspection and Metrology VII Originally published Boston, Nov. 1998 Copyright July 1998 by F. M. Waltz.
2. Christopher Mei and Ian Reid, Department of Engineering Science University of Oxford, Modeling and Generating Complex Motion Blur for Real-time Tracking, {cmei,ian}@robots.ox.ac.uk, 2008.
3. L. HÁJEK, Gaussian blur in Matlab, <http://kfe.fjfi.cvut.cz/~hajeklu2/files/PIN3/Bonus/GaussianBlur/GBlur.m>
4. G.J. Brostow and I. Essa. Image-based motion blur for stop motion animation. In Proc. Of ACM SIGGRAPH'01, 2001.4
5. S. Cho, Y. Matsushita and S. Lee. Removing non-uniform motion blur from images. In IEEE International Conference on Computer Vision, 2007.

УДК 004.652

РОЗРОБКА ІНФОРМАЦІЙНОЇ СИСТЕМИ КОНТРОЛЮ ОБІГУ МЕДИЧНИХ ПРЕПАРАТІВ НА БАЗІ ТЕХНОЛОГІЇ БЛОКЧЕЙН

Марченко Ігор, Петров Сергій

Сумський державний університет

Анотація

Метою даної роботи є усунення головного недоліку існуючих методів контролю обігу медичних препаратів, а саме неможливості забезпечення цілісності даних та ризик порушення лікарської таємниці. В роботі запропоновано інформаційний підхід, що базується на технології блокчейн та має перевагу над існуючими методами, які використовують централізовані або розподілені сховища даних. Розроблено смарт-контракт на базі реалізації блокчейну Ethereum, який позбавлений таких недоліків як реплікація даних та можливості компрометації даних при їх передачі.

Abstract

The purpose of this research work is address the weaknesses in existing systems, such as data integrity and observing medical confidentiality in order to control prescription medicine. This research provides blockchain-based approach for storing and managing user data. This technology is better than using centralized and/or distributed databases. Prescription medicine flow was fully implemented in terms of blockchain technology as Ethereum smart-contract.

Медична галузь гостро потребує розробку та впровадження та посилення контролю обігу медичних препаратів. На даний момент для інформатизації процесів взаємодії лікаря та пацієнта в Україні запроваджується система eHealth [1], що являє собою агрегацію декількох систем менеджменту інформаційних операцій пацієнтів, між якими, на даний момент, відсутній експорт даних. Одним з недоліків системи eHealth те, що кожна лікарня власноруч обирає систему менеджменту, котрею вона буде користуватися. При зміні місця проживання, а, відповідно, і лікарні неможливо мігрувати дані пацієнта. Таким чином ми не маємо можливості контролювати ситуацію в цілому. Іншим важливим аспектом – є обов'язкова наявність персонального комп'ютера для роботи даних систем.

Законодавчо в Україні робота даних систем регулюється постановою КМУ: «Про затвердження Порядку надання послуг конфіденційного зв'язку органам державної влади та органам місцевого самоврядування, державним підприємствам, установам та організаціям», що делегує відповідальність за зберігання та цілісність інформації на компанію, що надає програмне забезпечення. Таким чином, з точки зору правового аспекту всі наведені вище системи мають ключовий недолік: у випадку компрометації доступу до бази даних, права пацієнта про нерозголошення особистої інформації та лікарську таємницю будуть порушені [2], що посилює відповідальність власників системи щодо забезпечення цілісності даних.

Серед запропонованих систем функціонал електронних рецептів знаходиться лише на стадії концепту. А для її роботи необхідна наявність персонального комп'ютеру в аптеці, та підключення її до тієї ж системи, в якій видано рецепт.

Концепція електронних рецептів є класичним підходом, що ґрунтується на простому прийомі – оцифровці існуючих інформаційних потоків, але враховуючи високу залежність людства від безпеки персональних даних вимагає використовувати принципово нові підходи в тому числі і перегляду існуючих потоків даних та процесів їх обробки. Суттєві зміни європейського законодавства що поводить радю європейського парламенту GDPR вже з травня 2018 року вимагає обов'язкового шифрування всіх персональних даних, вважаємо що конкретна вимога щодо

гарантування цілісності буде наступною. Забезпечити останнє може така технологія як блокчейн [3].

Зазначимо, що класичні паперові рецепти не забезпечують достатньої надійності та цілісності даних. Наступним кроком у розвитку підходів до зберігання даних є використання баз даних, які за ступенем розподіленості розділяють на централізовані та розподілені [4]. Головним недоліком централізованих баз даних є низька ступінь відмовостійкості, розподілені бази даних позбавлені цього недоліку. При цьому всі види класичних баз даних не можуть забезпечити достатню ступінь цілісності даних. Так, наприклад, на випадок технічного збою необхідно створювати резервні копії даних. Розвитком розподілених баз даних є технологія блокчейн, що в простому розумінні, представляє собою репліковану розподілену базу даних, записи в якій неможливо змінити. Домінуючою сферою використання блокчейну на даний час є зберігання транзакцій криптовалют.

На даний момент існує велика кількість проектів на базі блокчейну, що не пов'язані з криптовалютами:

- авторизація за допомогою блокчейну
- зберігання файлів
- документообіг
- авторство та право володіння цифровим об'єктом
- продаж коштовностей
- голосування
- онлайн ігри

Всі ці проекти з'явилися в зв'язку з необхідністю мати незалежну та надійну базу даних. При цьому відмова одного з вузлів, на якому зберігаються дані жодним чином не впливає на роботу системи в цілому.

На даний момент існує два найбільших публічних блокчейни, доступних для використання: Bitcoin та Ethereum. Головною відмінністю між ними є можливість виконувати смарт-контракти у блокчейні Ethereum [5]. Базовим елементом блокчейну є вузол з унікальною адресою. Операція зміни стану блокчейну називається – транзакція. Всі транзакції безпосередньо зберігаються в блокчейні. Зазначимо, що недоліком публічних блокчейнів є плата за транзакції, а саме - за збереження інформації та відносно низька швидкість їх виконання.

Кожен вузол може представляти собою клієнта системи, або інтерфейс що реалізує логіку взаємодії між вузлами – смарт-контракт. Якщо транзакція направлена на адресу за якою розташовано смарт-контракт будуть виконані його методи. Приклад смарт контракту наведено нижче.

pragma solidity ^0.4.0;

```
contract TestContract {  
    address owner;  
  
    function TestContract() public {  
        owner = msg.sender;  
    }  
  
    function getOwner() public constant returns (address) {  
        return owner;  
    }  
}
```

За своєю структурою смарт-контракт нагадує звичайний об'єктно-орієнтований клас з його полями, методами та модифікаторами доступу. Відмінність полягає у тому, що в

блокчейні існують операції, котрі не змінюють його внутрішній стан, а тому і не потребують оплати. Такі операції повинні бути позначені модифікатором `constant`. Контракт при створенні зберігає адресу клієнта, що його завантажив в блокчейн, а тому є його власником, а за допомогою методу `getOwner()` повертає це значення.

Розглянемо можливість використання блокчейну для реалізації системи контролю обігу медичних препаратів. Під транзакцією в термінах нашої системи будемо розуміти будь-яку взаємодію між клієнтом та блокчейном.

Використання публічного блокчейну доцільно оскільки це забезпечую децентралізацію даних та їх цілісність, при цьому необхідно мінімізувати кількість операцій, які змінюють внутрішній стан блокчейну оскільки вони потребують оплати.

Блокчейн накладає певні обмеження на зберігання даних [6], тому в ньому є сенс зберігати лише ті дані зміна яких небажана:

- факт оформлення рецепту у лікаря;
- факт видачі ліків аптекарем.

Лікар генерує транзакцію що заносить в блокчейн інформацію про те, кому і що саме він виписав. Дані транзакції неможливо сфальсифікувати, а тому при покупці медикаментів аптекар може бути впевненим в тому, що йому представлено рецепт в такому вигляді, як його виписав лікар.

Для кожного рецепту будемо зберігати адресу клієнту, якому він виданий та скільки разів можливо придбати ліки з цього рецепту. При кожному придбанні, аптекар авторизується у системі та шляхом зчитування qr-коду з екрану мобільного пристрою, за допомогою одноразового паролю, або за допомогою NFC зменшує цю кількість на одиницю. Факт цього придбання зберігається в блокчейні у вигляді транзакції.

Завдяки цьому кожен рецепт пройде ланцюг від виписки його лікарем до видачі в аптеці, що відкидає ймовірність підробки документів на видачу ліків. Окрім того, при виявленні факту неправомірних дій будь-якої сторони можливо відстежити шлях та осіб, які були при цьому задіяні.

Враховуючи всі приведені вище переваги блокчейну над класичними способами зберігання даних було вирішено використовувати реалізацію, що базується саме на ньому. Така реалізація має наступні переваги: відмовостійкість та цілісність даних. Серед недоліків даної системи виділимо низьку швидкість транзакцій в блокчейні, яка не впливає на роботу додатку.

Список використаних джерел:

1. Головна | Офіційний сайт електронної системи охорони здоров'я eHealth [Electronic resource]. URL: <https://portal.ehealth-ukraine.org/> (accessed: 01.03.2018).
2. Про затвердження Порядку надання... | від 11.10.2002 № 1519 [Electronic resource]. URL: <http://zakon0.rada.gov.ua/laws/show/1519-2002-п> (accessed: 01.03.2018).
3. Satoshi Nakamoto, Kornmesser S., Satoshi Nakamoto. Bitcoin // Wwww.Bitcoin.Org. 2008.
4. Date C.J. An Introduction to Database Systems // An Introd. to Database Syst. 1995.
5. Wood G. Ethereum: a secure decentralised generalised transaction ledger // Ethereum Proj. Yellow Pap. 2014. P. 1–32.
6. Types — Solidity 0.4.21 documentation [Electronic resource]. URL: <http://solidity.readthedocs.io/en/develop/types.html> (accessed: 06.03.2018).

APPROACH TO ARCHITECTURE DESIGN OF THE CONTENT READABILITY DETERMINATION SYSTEM

Basyuk Taras

Lviv Polytechnic National University, Lviv, Ukraine

Abstract

The role of readability of the content in the modern information space is analyzed and necessity of developing a system for its determining is shown. The description of the possible approach to architecture design of the system for determining the readability of content and formed recommendations for its design are the result of the study.

Introduction

The growth of production, consumption and accumulation of information in all sectors of human activity is the fundamental feature of civilization. All life of mankind is one way or another connected with its reception, accumulation and processing. At the same time, the Internet network has become a global repository that contains several zetabites of information, a large number of which has unstructured or inconvenient form for perception [1]. It is known that users choose the most attractive and easily readable materials in the process of information retrieval [2]. Given that, SEO optimizers should provide potential users with the maximum convenience of reading relevant texts. At the same time, it is necessary to pay attention not only to external factors (brochures, reports, charts), but also the readability of "everyday publications" should be taken into account [3]. Theoretically, the material for publication should be easily perceived and understood by the target audience of the resource users, and hence be consistent with the basic level of readability [4]. In view of this, the actual task is to create software for intellectual analysis of content in order to provide the required level of readability. In accordance with the requirements for the development of any software at the beginning of the work, it is necessary to analyze the requirements, form the models of work and carry out the construction, which is to create the architecture of the system.

Formulation of the problem

The actuality of the task of architecture design of the system for determining the readability of content is primarily due to the dynamism of the industry and increase in the volume of "digital consumption" [3]. According to studies conducted by the SEMSOCIAL resource, if in 2017, each user had about 12 gigabytes of information, in 2020 this figure will increase to 24 GB, which will require a satisfaction of the high demand for high-quality resources that are characterized by high readability.

In the case of computer design of the architecture of readability determination system, this process is associated with considerable difficulties. Technical problems (the variety of software platforms that operate in the global network), as well as problems associated with the specifics of task can be referred to their list (the set of techniques used in the definition of readability) [4].

At the same time, the stages of creating models and developing the architecture of the system are considered as one of the most difficult. Because it involves defining all the functions of the system being developed, interface links between component elements and choosing design solutions to ensure trouble-free operation.

Major research results

According to modern technology of designing, constructing the architecture of the system for content readability determining requires the adoption of the following design solutions:

system partitioning on the module; management of data warehouses; implementation of software management; management of boundary situations.

System partitioning on the module. This stage includes the allocation of a set of individual objects, subsystems that are interconnected and have well-defined interface connections with other parts of the system. They define the form of all interactions between subsystems, but do not contain connections to their internal structure. Considering this feature, each subsystem can be developed independently, which allows sharing work between developers.

Management of Data Warehouses. Internal and external data warehouses represent clear segments that separate the subsystems with defined interface connections. Since the projected system is a real-time system, non-relational databases can be used for its operation.

Implementation of software management. All interactions in the system are presented in the form of events during the operation. There are two classes of methods for managing them: external and internal. Creating a system for determining the readability of content requires designing with the use of the principles of external management applying the method of the interactive interface. The need to select objects that form an interface using REST and Ajax technologies is the feature of this type of system. The emergence of Ajax's client architectural web-style has made it possible to reformat the design of web application in order to match the architectural style of REST. This feature enables creating Ajax/REST system, which far exceeds the traditional server web applications both in terms of speed and versatility.

Management of boundary situations. It is provided during the design of the system by predicting the reaction of each object and whole system to certain external actions. The following boundary situations are allocated: initialization, termination and collapse. In order to ensure this design solution it is necessary to predict the behavior of each object and whole system in such conditions.

After conducting research on these stages, the construction of the architecture of the system takes place, which, consists of three parts for the solved task: input / output (intended for the organization of interaction); kernels (intended for the intellectual analysis of readability and providing recommendations for changing its level) and intermediate layer (designed to level the peculiarities of the use of various types of software and hardware platforms).

Conclusion

The article analyzes the current state of the Internet space and shows the increasing need to take into account readability in the process of publishing web sites. The description of the approach to designing and developing recommendations for constructing the architecture of the system for determining the readability of the content is the result of the research.

References:

1. Grappone J. Search Engine Optimization (SEO): An Hour a Day / J. Grappone. - United States: Wiley Publishing, Inc., 2013. – 435p.
2. Basyuk T. The Popularization Problem of Websites and Analysis of Competitors / T. Basyuk – In: Shakhovska N., Stepashko V. (eds) – Advances in Intelligent Systems and Computing II. CSIT 2017. Advances in Intelligent Systems and Computing, vol 689. Springer, Cham pp. 54-65. DOI:10.1007/978-3-319-70581-1_4.
3. Kennedy G. Seo: Marketing Strategies to Dominate the First Page (SEO, Social Media Marketing) / G. Kennedy, CreateSpace Independent Publishing Platform, 2016. – 122p.
4. Bailin A. Readability: Text and Context / A. Bailin, A. Grafstein – Palgrave Macmillan, 2016. – 224p.

КОМП'ЮТЕРИЗОВАНА СИСТЕМА КОНТРОЛЮ ЗНАНЬ ЧЕРЕЗ МЕРЕЖУ INTERNET

Чорний Олексій¹, Сергієнко Сергій¹, Несен Микола², Кабаченко Ірина², Титюк Валерій³

¹Кременчуцький національний університет імені Михайла Остроградського

²Кременчуцьке вище професійне училище № 7

³Криворізький національний університет

Анотація

Розглядається система тестування на основі програмного забезпечення iSpring QuizMaker з відстежуванням результатів тестування. Мета створення, це застосування у дистанційному навчанні студентів та учнів професійно-технічних училищ. Тестування здійснюється через мережу Internet. Результати тестування надсилаються на електронну пошту викладача. Експериментально встановлено, що такий підхід дозволяє оперативно отримувати результати тестування і використовувати їх в роботі, стежити за успішністю, удосконалювати при цьому тести або створювати нові за темами, які виявилися складними для розуміння.

Abstract

A testing system based on iSpring QuizMaker program providing the test results tracing is analyzed. It is aimed at the use in the distant training of university and vocational school students. Testing is carried out via the Internet. The test results are sent to the lecturer's e-mail address. It was determined by experiment that this approach makes it possible to obtain the test results quickly and use them in work, follow the students' progress, and, at the same time, improve the tests and create new ones for the subjects that turned out difficult for understanding.

Вступ. Створення системи оцінки якості освіти – одна з основних задач в сфері реформування і модернізації сучасної системи освіти. С підписанням Болонської декларації, переходом на багаторівневе утворення, введенням бально-рейтингової системи оцінки діяльності студентів в процесі навчання з різних дисциплін, зміною державних освітніх стандартів, одним з елементів системи оцінки якості стає тестування навчальних досягнень студентів.

Сучасні стандарти освіти вимагають проведення тестування з використанням новітніх інформаційних, інтерактивних і мультимедійних технологій. У цьому випадку проведення проміжного, підсумкового та рубіжного контролю знань студентів у вигляді електронного тесту в порівнянні з традиційними видами контролю відбувається більш оперативно. Робота з електронними тестами спонукає студентів до самостійного навчання і самоконтролю. Комп'ютерне тестування має не тільки контролюючими, але і навчальними функціями, тому воно відіграє важливу роль у розвитку електронних форм навчання [1].

Матеріал доповіді. В даний час існує велика кількість систем тестування з різними функціональними характеристиками. iSpring QuizMaker – це програма для створення тестів і опитувань, розроблена компанією iSpring, яка є надійним інструментом для розробки інтерактивних тестів і опитувань. Програма поєднує в собі розширені можливості по налаштуванню правил, виду, форм тестування і підрахунку балів [2].

Крім розробки тестових завдань є можливість створювати анкети і опитувальники для збору інформації без оцінювання правильності відповідей. Кожному типу оцінюваного питання відповідає питання-анкета. В режимі створення анкети є спеціальні типи питань: шкала Ликерта (оцінка ступеня згоди або незгоди з твердженням); есе (введення відповіді у вільній формі).

Тести і опитування, створені в програмі, можна легко опублікувати в будь-якій Системі Дистанційного Навчання, що підтримує стандарти SCORM або AICC, відправити електронною поштою, згенерувати у вигляді придатному для публікації в мережі інтернет

і використанні локально або просто експортувати в Word для створення паперової версії тесту. Основні особливості програми: 23 типи питань; можливість використання мультимедіа; додавання коментарів; побудова сценаріїв розгалуження; випадкова вибірка питань.

Програма має зручний, комфортний як для створення, так і для роботи учнів інтерфейс. У питаннях і відповідях можна використовувати графіку, формули, мультимедіа, Flash- анімацію. Це дозволить не тільки зробити привабливішим вашу роботу, але і поліпшити сприйняття запропонованих завдань. І водночас дозволяє створювати окремі умови проходження тесту: час проходження, прохідний бал, змінити текстову реакцію програми на правильні і не правильні відповіді і завершення всього тесту.

При завантаженні системи тестування пропонується обрати конкретний тест та ввести дані користувача (рис. 1).

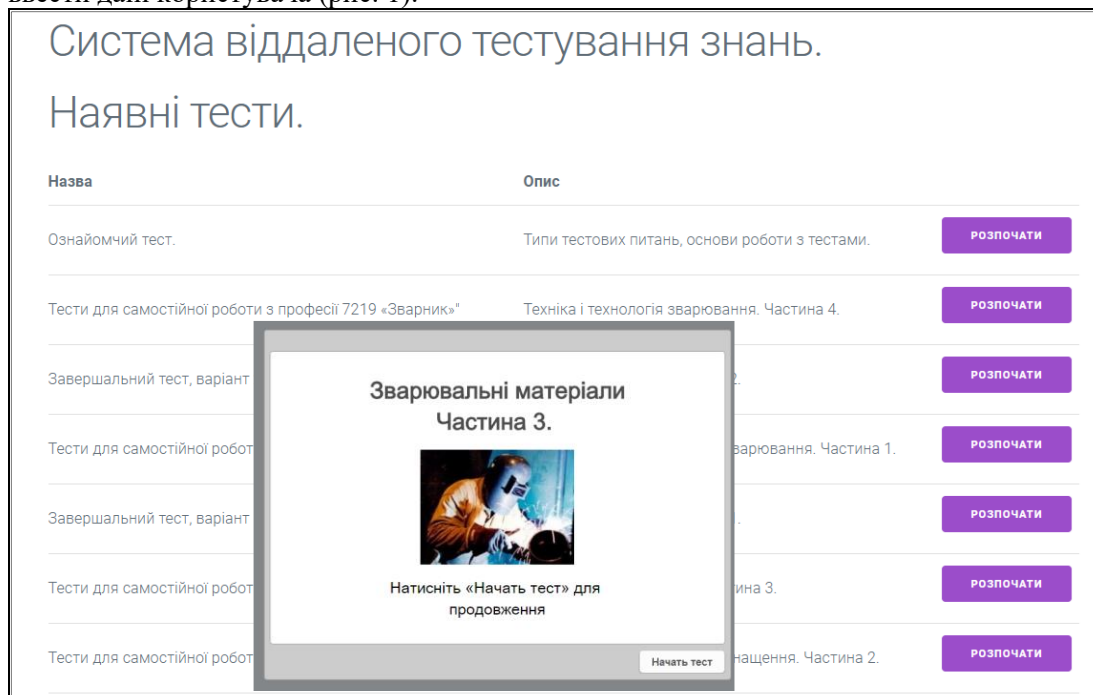


Рисунок 1 – Вікно вибору тесту і початку тестування

Система послідовно запропонує випадковим чином вибрані 24 питання з тем, що віднесені до самостійної перевірки знань і 40 питань з підсумкового тесту. Зданим є тест у якому користувач вірно відповів на 60% та більше запитань. Інформація про результати тестування автоматично передається на електронну пошту викладача та може бути роздрукована, чи навіть перенаправлена користувачеві для аналізу та вивчення тем, за якими були невірні відповіді. Інший користувач не тільки отримає інший набір запитань, а й іншу послідовність запропонованих відповідей для кожного з запитань.

На рис.2 показаний приклад відповідей учня на запитання та вдале проходження тесту з отриманими результатами.

Після проходження тестування, отримані результати автоматично пересилаються на електронну пошту викладачу, про що формується додатково повідомлення (рис. 3) та детально наводяться результати.

Таким чином реалізовано систему тестування в програмному середовищі iSpring QuizMaker з відстежуванням викладачем результатів тестування.

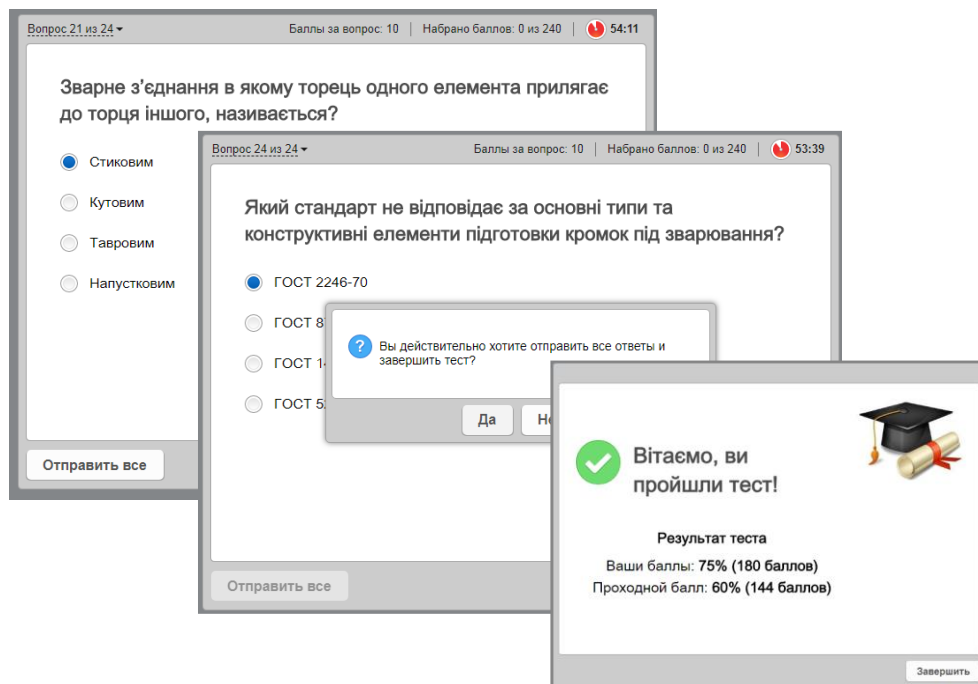


Рисунок 2 – Вигляд відповіді та завершення тесту

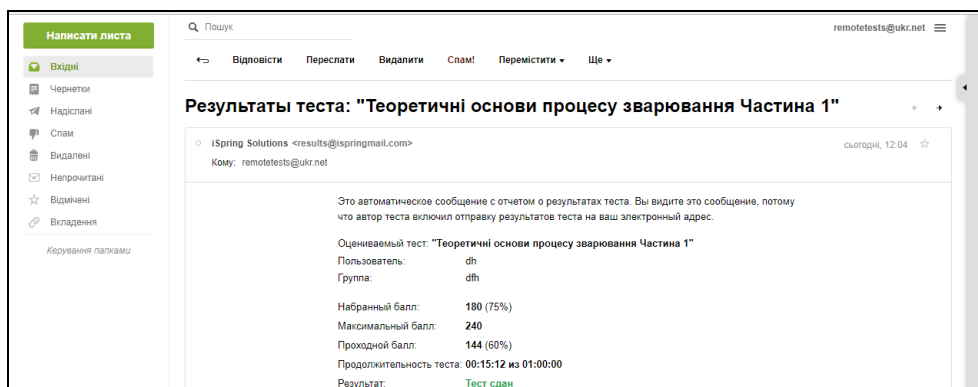


Рисунок 3 – Повідомлення на електронну пошту про файл з відповідями з тесту та результатами тестування

Висновки. Тестування на основі iSpring QuizMaker є ефективним і перевіреним на практиці методом виявлення і оцінки рівня навчальних досягнень учнів, як підсумкових, так і проміжних, закріплення і засвоєння навчального матеріалу завдяки використанню тест-тренажерів. А також дозволяє оперативно отримувати результати тестування і використовувати їх в роботі, стежити за успішністю, удосконалювати при цьому тести або створювати нові за темами, які виявилися складними для розуміння, підвищує об'єктивність перевірки знань, дозволяє визначити характер мислення об'єкта тестування, та в цілому підвищити ефективність навчального процесу.

Список використаних джерел:

1.Гороль П. К. Сучасні інформаційні засоби навчання / П. К. Гороль, Р. С. Гуревич, Л. Л. Коношевський, О. В. Шестопалюк. – Вінниця : ВДПУ імені М. Коцюбинського, 2004. – 535 с.

2.Сорочинский М.А. Реализация технологий электронного обучения на основе системы iSpring // Материалы Международного молодежного научного форума «ЛОМОНОСОВ-2015» [Электронный ресурс] – М.: МАКС Пресс, 2015.

АНАЛІЗ ЯКОСТІ ПРОГНОЗУ ПОГОДИ ПОПУЛЯРНИХ УКРАЇНСЬКИХ САЙТІВ

Козачук Андрій

CDM a/s

Анотація

Розраховано імовірність виправданості прогнозу температури та імовірність вдалого прогнозу опадів для популярних українських та іноземних веб-сайтів для двох міст. Показано, що сайти прогнозу погоди Sinoptik.ua, Gismeteo.ua та Meteoprog.ua мають схожі показники виправданості прогнозу для Вінниці. Глобальні сайти Accuweather.com та DarkSky.net мають гірші результати. Gismeteo та Accuweather найкраще прогнозують наявність опадів.

Abstract

Forecast temperature accuracy and probability of successful precipitation forecast was calculated for popular ukrainian and international web-sites for two towns. It was shown that Sinoptik.ua, Gismeteo.ua and Meteoprog.ua have similar level of the forecast accuracy for Vinnytsia. Global websites Accuweather.com and DarkSky.net have worse results. Gismeteo and Accuweather are the best in precipitation forecast.

Вступ

За допомогою мережі інтернет досить просто отримати прогноз погоди з великої кількості українських та іноземних веб-сайтів, інколи прогнози різних сайтів не співпадають. Це робить актуальною задачу порівняння якості прогнозів погоди, отриманих з популярних сайтів.

В рамках проведеного дослідження дані про прогноз погоди збиралися з наступних джерел:

- Sinoptik.ua
- Gismeteo.ua
- Meteoprog.ua
- Accuweather.com
- Darksky.net

З кожного джерела отримувався прогноз погоди для двох міст: Вінниця і Фреденсборг (Данія).

Аналіз виправданості прогнозу для досліджених сайтів

В рамках проведеного дослідження визначалась виправданість прогнозу, що дорівнює 1, якщо модуль різниці між прогнозом температури та її фактичним значення менший за 3° та 0 – у протилежному випадку [1, 2]. Детальніше методологія дослідження описана в публікації [3]. Імовірність виправданості прогнозу температури для популярних веб-сайтів наведена в таблиці 1.

Таблиця 1 – Виправданість прогнозу температури

Джерело прогнозу	Імовірність виправданості прогнозу у Вінниці, %	Імовірність виправданості прогнозу у Фреденсборзі, %
Sinoptik	72	81
Gismeteo	75	81
Meteoprog	75	83
Accuweather	46	81
DarkSky	67	82

У Вінниці найкращі результати показали Gismeteo і Meteoprog. DarkSky і особливо Accuweather мають гірші показники, вони часто завищують свої прогнози. Для Фреденсборга всі сайти показали схожі результати, з незначною перевагою у Meteoprog. В цілому прогнози для Фреденсборга значно якісніші за прогнози для Вінниці, це можна пояснити різницею у кліматі та більш щільною мережею метеостанцій.

Аналіз прогнозу опадів

В зібраних даних про фактичну погоду опади фіксувались тільки на Вінницькій метеостанції. Використовувався показник «Опади за 12 год, мм», що відповідає даним за 12-ту годину дня. Таким чином реєструвалися опади лише за першу половину доби, тому досліджувати помилки першого роду (опадів не було, хоча у прогнозі були) на основі зібраних даних неможливо. Проте можна досліджувати помилки другого роду – коли опади спостерігались, але були відсутні у прогнозі.

Було проведено аналіз середнього значення прогнозу імовірності опадів у дні, коли опади було зафіксовано та імовірність вдалого прогнозу опадів. Прогноз опадів вважався вдалим, якщо прогноз імовірності опадів на заданий день перевищує 25% і опади у цей день були зафіксовані. Розраховані значення представлені у таблиці 2.

Таблиця 2 – Середнє значення прогнозу імовірності опадів у дні коли опади спостерігались та імовірність вдалого прогнозу опадів

Джерело прогнозу	Середнє значення прогнозу імовірності опадів, %	Імовірність вдалого прогнозу опадів, %
Sinoptik	59.4	83.3
Gismeteo	-	91.6
Meteoprog	-	75
Accuweather	46.9	91.6
DarkSky	53.5	83.3

Таким чином, Sinoptik прогнозує опади з найбільшим рівнем «впевненості», а найбільший шанс не пропустити опади надають сайти Gismeteo та Accuweather.

Висновки

Популярні в Україні сайти прогнозу погоди Sinoptik.ua, Gismeteo.ua та Meteoprog.ua мають схожі показники виправданості прогнозу для Вінниці. Вони дозволяють отримати прогноз температури, що виправдовується в трьох випадках з чотирьох. Глобальні сайти Accuweather.com та DarkSky.net мають гірші результати.

Прогноз для датського міста Фреденсборг якісніший за Вінницький, при цьому усі досліджені сайти дають виправданий прогноз у трохи більше ніж 80% випадків.

Gismeteo та Accuweather найкраще прогнозують наявність опадів у Вінниці. Враховуючи те, що якість прогнозу температури в Accuweather є не дуже високою, Gismeteo є оптимальним вибором для перевірки як температури так і опадів за допомогою одного веб-сайта.

Список використаних джерел

1. Соотношения реальной температуры и прогноза Яндекс.Погоды [Електронний ресурс] – Режим доступа: <https://geektimes.ru/post/283950/>.
2. Юдин М. И. Новые методы и проблемы краткосрочного прогноза погоды // Ленинград: Гидрометеорологическое издательство, 1963. – 402 с. – Режим доступа: http://elibrary.ru/files_books/pdf/img-216184134.pdf.
3. Дослідження якості прогнозу погоди [Електронний ресурс] – Режим доступа: <https://byandriykozachuk.wordpress.com/2018/02/03/порівняння-сайтів-прогнозу-погоди>

УЯЗВИМОСТЬ NOSQL НА ПРИМЕРЕ MONGODB*Абрамова Ирина, Афанасьева Ирина*

Харьковский национальный университет Радиоэлектроники

Аннотация

В данной публикации рассматриваются вопросы незащищенности нереляционных баз данных на примере MongoDB. Многие полагают, что нереляционные базы данных имеют значительное преимущество, в сравнении с РСУБД, будь-то они являются прочнее из-за отсутствия SQL и, соответственно, связанных с ним инъекций. Тем не менее нереляционные базы данных имеют целый ряд специфических незащищенностей, как в них самих, так и в системе управления, что делает нереляционные базы данных не такими безопасными, как кажется на первый взгляд.

Abstract

This publication examines the issues of insecurity of non-relational databases using MongoDB as an example. Many believe that non-relational databases have a significant advantage, in comparison with RDBMS, whether they are stronger because of the lack of SQL and, consequently, related injections. Nevertheless, non-relational databases have a number of specific insecurities, both in themselves and in the management system, which makes non-relational databases not as secure as they seem at first glance.

Введение

Понятие NoSQL (Not Only SQL или No SQL), то есть уход от использования привычных нам уже РСУБД, получил популярность с 2009 года. На тот момент развитие web-технологий и социальных сервисов требовало нахождения новых подходов к хранению и обработке данных. Началось активное развитие и продвижение всевозможных программных решений с использованием NoSQL. Близкие по значению слова для NoSQL стали огромные объемы данных, линейная масштабируемость, кластеры, отказоустойчивость, нереляционность. Разработчики столкнулись с задачами, для которых традиционные реляционные СУБД оказались либо слишком дороги, либо недостаточно производительны. Кроме того, основателями отказа от универсальных «комбайнов» (реляционные СУБД РСУБД) в пользу специализированных решений стали молодые проекты и те, кому приходится работать в сценариях так называемых Big Data [1].

Можно допустить, что NoSQL СУБД безопасней, благодаря тому что в них отсутствуют SQL-запросы и нет возможности провести SQL-инъекцию. Частично это так, но если в запросе отсутствует SQL-код, это еще не говорит о том, что система полностью безопасна. NoSQL прикрывает лишь некоторые уязвимости, такие как SQL-инъекции, но оставляет множество других.

Привычно она состоит из трех уровней [3]:

1. Приложение;
2. API базы данных NoSQL;
3. NoSQL-СУБД.

Все вышеперечисленные уровни потенциально уязвимы. Рассмотрим с самого нижнего уровня, иначе с самой СУБД. Как и любое приложение, СУБД может быть подвластна атакам переполнения буфера или иметь незащищенную схему аутентификации. Атаковать этот уровень сложно, потому что за подобными слабыми местами следит сообщество и разработчики.

Второй уровень — API. Многие нереляционные СУБД имеют большое количество библиотек для организации доступа к данным. Большинство таких проектов имеют открытый код, но часть из них уже не поддерживаются, поэтому шанс найти уязвимость на этом уровне гораздо выше.

Высший уровень — атакуемый. Здесь нужно попытаться найти места, в которых разработчик забыл проверить входные данные. При таком обстоятельстве используется тот же подход, что и при поиске SQL-инъекций, однако в данной ситуации придется разбираться с JSON, JavaScript или чем-то подобным.

Рассмотрим слабые места нижнего уровня на основе анализа нескольких версий MongoDB [3]:

1. Незащищенное место в системе аутентификации. Стандартно БД устанавливается без пароля. Учредители MongoDB думают, что БД запускается в полностью доверенном окружении.

2. Незащищенное место в системе авторизации. Всякий созданный пользователь как принято имеет выход на чтение всей базы данных, то есть он имеет доступ ко всему, что у нас имеется.

3. Незащищенное место в системе авторизации администратора. Юзер с доступом к базе данных Admin имеет права на чтение/запись откуда/куда угодно. А т.к. стандартно нет пароля, то мы имеем доступ везде.

4. Нешифрованный текст. Все данные передаются в открытом виде, то есть они могут быть перехвачены любой MITM-атакой.

Большинство современных реляционных СУБД позволяют создавать хранимые процедуры на сервере. У MongoDB имеются аналогичные возможности, среди которых присутствует серверный JavaScript. Это позволяет исполнять почти любой код на сервере БД. С одной стороны, это даёт возможность писать алгоритмы обработки данных, но с другой — делает приложение более уязвимым.

Области применения JavaScript в MongoDB:

1. Запросы с оператором \$where.

2. Команда db.eval.

3. Функции для сохранения в базе данных. Для этого используется специальная системная коллекция system.js.

4. Map/Reduce. Это – программный фреймворк, разработанный компанией Google для параллельных вычислений над большими объемами данных.

В данной работе мы рассмотрели уязвимость РСУБД и NOSQL, можем сделать выводы, что на уровне самой БД при стандартных настройках реализации NoSQL (а именно — MongoDB) серьезно проигрывают классическим РСУБД. Однако, нужно заметить, что стандартные настройки не используются на боевых серверах, поэтому, в большинстве случаев, если уязвимость есть только при стандартных настройках, то в серьёзных проектах её не будет. А вот на уровне приложения ситуация обстоит гораздо лучше. Многие незащищенности основаны на очевидных ошибках в коде и существуют только в примерах, а на практике встретить их практически не представляется возможным.

Список использованных источников:

1. СУБД NoSQL – сильные и слабые стороны. [Электронный ресурс]. Режим доступа: <http://www.jetinfo.ru/stati/silnye-i-slabye-storony-nosql/>

2. Азбука NoSQL-инъекций. [Электронный ресурс]. Режим доступа: <https://habrahabr.ru/company/xakep/blog/143909/>

3. Mongodb - Security Weaknesses in a typical NoSQL database. [Electronic resource]. URL: <https://www.trustwave.com/Resources/SpiderLabs-Blog/Mongodb---Security-Weaknesses-in-a-typical-NoSQLdatabase/>

THE CLOSURE OF TABLE ALGEBRA OF INFINITE TABLES WITH RESPECT TO OPERATIONS OF MULTISSET TABLE ALGEBRA

Glushko Iryna

Nizhyn Mykola Gogol State University

Abstract

This article is a continuation of the works devoted to the actual problem of the development of the theoretical basis of the table databases. The question of the relationship between table algebra of infinite tables and multiset table algebra is considered. The question arises, is whether table algebra of infinite tables a subalgebra of multiset table algebra. This paper is devoted to this issue. Applying the theorem-plural and logical-algebraic methods found that this is not the case. The table algebra of infinite tables does not form subalgebra of multiset table algebra, since it is not closed in relation to some signature operations of multiset table algebra. These operations are determined.

Анотація

Дана робота є продовженням робіт, присвячених актуальній проблемі розробки теоретичної основи табличних баз даних, в якості якої виступають табличні алгебри. Досліджується питання про те, чи є таблична алгебра нескінченних таблиць підалгеброю мультимножинної табличної алгебри. Застосовуючи теоретико-множинні та логіко-алгебраїчні методи, встановлено, що таблична алгебра нескінченних таблиць не утворює підалгебру мультимножинної табличної алгебри, бо не є замкнутою відносно деяких операцій сигнатури мультимножинної табличної алгебри. У роботі встановлено, що це за операції.

Introduction

This article is a continuation of the works devoted to the actual problem of the development of the theoretical basis of the table databases. The purpose of this work is to determine is whether table algebra of infinite tables a subalgebra of multiset table algebra.

Table algebra of infinite

Table algebra of infinite tables generalizes table algebra which was suggested by Redko V., Brona J., Buy D., Poliakov S. in monograph [1]. First of all any set of tuples, in particular infinite, is understand under relation, because, as a rule, mathematical statements about standard properties of specification of relation operations remain true for infinite relations. Secondly every table correlated to a certain scheme. A table is pair, where the first component is an arbitrary set and the second component is a scheme of the table.

Let $\mathbf{A}$ be the set of attributes and $\mathbf{D}$ be the universal domain. Under the table algebra of infinite tables is understood algebra $\langle \mathbf{T}, \Omega_{P, \Xi} \rangle$, where $\mathbf{T}$ is the set of all tables, $\Omega_{P, \Xi} = \{ \cup_R, \cap_R, \setminus_R, \sigma_{p, R}, \pi_{X, R}, \otimes_{R_1, R_2}, \div_{R_2}^{R_1}, Rt_{\xi, R}, \sim_R \}$ is a signature, $p \in P, \xi \in \Xi$, $X, R, R_1, R_2 \subseteq \mathbf{A}$, P, Ξ are the sets of parameters.

An arbitrary finite set of attributes $R \subseteq \mathbf{A}$ is called scheme. The tuple of scheme R is the nominal set on pair $R, \mathbf{D}$. The projection of this nominal set for the first component is equal to R .

A table of scheme R ($R \subseteq \mathbf{A}$) is pair $\langle t, R \rangle$, where t is a set (in particular infinite) of tuples of fixed scheme R . The operations of signature $\Omega_{P, \Xi}$ are defined in [2].

Multiset table algebra

Multiset table algebra is multisets analog of the table algebra. In this case, the concept of the table is specified, using concept of the multisets (or bags).

Under multiset table algebra is understood algebra $\langle \Psi, \Omega_{P, \Xi} \rangle$, where Ψ is the set of all tables, $\Omega_{P, \Xi} = \{ \bigcup_{All}^{\Psi, R}, \bigcap_{All}^{\Psi, R}, \setminus_{All}^{\Psi, R}, \sigma_{p, R}, \pi_{X, R}, \otimes_{R_1, R_2}, Rt_{\xi, R}, \sim_R \}^{p \in P, \xi \in \Xi}_{X, R, R_1, R_2 \subseteq A}$ is a signature, P, Ξ are the sets of parameters. The operations of signature $\Omega_{P, \Xi}$ are defined in [2, 3].

The table is pair $\langle \psi, R \rangle$, where the first component ψ is an arbitrary multiset, basis of which $\Theta(\psi)$ is the set of tuples of the same scheme and the second component R is a scheme of the table. A certain scheme is also ascribed to every table and table can be infinite.

About relationship between table algebra of infinite tables and multiset table algebra

1-multisets are multisets whose range of values is the empty set or single-element set $\{1\}$. These multisets are the analogues of ordinary sets. Considering this fact the question arises, is whether table algebra of infinite tables a subalgebra of multiset table algebra. This paper is devoted to this issue. Applying the theorem-plural and logical-algebraic methods found that this is not the case. The table algebra of infinite tables does not form subalgebra of multiset table algebra, since it is not closed with respect to the union, projection and active complement.

Let's check it out at union operation. Bases of 1-multisets t_1^1 and t_2^1 are designated as $\Theta(t_1^1), \Theta(t_2^1)$ accordingly. So $\langle t_1^1, R \rangle \bigcup_{All}^R \langle t_2^1, R \rangle = \langle t_1^1 \bigcup_{All} t_2^1, R \rangle$, where $\langle t_1^1, R \rangle, \langle t_2^1, R \rangle \in T(R)$, $T(R)$ is a set of all table on scheme R .

Basis of multiset $t_1^1 \bigcup_{All} t_2^1$ of the resulting table is equal to union of bases of multisets of input tables:

$$\Theta(t_1^1 \bigcup_{All} t_2^1) = \Theta(t_1^1) \cup \Theta(t_2^1).$$

Duplicate tuples, which appear after implementation of operation, are not removed from the result. The number of duplicates is given by the following formula:

$$Occ(s, t_1^1 \bigcup_{All} t_2^1) = \begin{cases} 1, & \text{if } s \in \Theta(t_1^1) \setminus \Theta(t_2^1) \text{ or } s \in \Theta(t_2^1) \setminus \Theta(t_1^1), \\ 2, & \text{if } s \in \Theta(t_1^1) \cap \Theta(t_2^1); \end{cases}$$

where $s \in \Theta(t_1^1) \cup \Theta(t_2^1)$. As a result $t_1^1 \bigcup_{All} t_2^1$ is a multiset and it is not a 1-multiset.

Consequently, the set of all table of table algebra of infinite tables is not closed with respect to the union $\bigcup_{All}^R$. Similarly, we can show that the set of all table of table algebra of infinite tables is not closed with respect to the projection and active complement.

References:

1. Реляційні бази даних: табличні алгебри та SQL-подібні мови / В.Н. Редько, Ю.Й. Брона, Д.Б. Буй, С.А. Поляков. – Київ: Видавничий дім "Академперіодика", 2001. – 198 с. – ISBN 966-8002-00-8.
2. Буй Д.Б. Числення на розширення сигнатур табличних алгебр: монографія / Д.Б. Буй, І.М. Глушко. – Ніжин: НДУ ім. М. Гоголя, 2016. – 151 с. – ISBN 978-617-527-145-2.
3. Buy D.B. Extended of Table Algebrs: Multiset Table Algebra / D.B. Buy, I.M. Glushko // Modern scientific research and their practical application. – 2013. – Vol.J11309. – С. 41-49.
4. Glushko I. Формальна семантика агрегатних операцій мультимножинної табличної алгебри (A formal semantics of aggregate operations of multiset table algebra) / I. Glushko // Proceedings of the 9th International Conference of Programming. – Kyiv, Ukraine, May 20-22, 2014. – P.166-173.

К ВОПРОСУ О ВОСПРИЯТИИ ИНФОРМАЦИИ В ИНТЕРНЕТ-ПРОСТРАНСТВЕ

Архипова Евгения

Национальный технический университет Украины
«Киевский политехнический институт имени Игоря Сикорского»

Аннотация

В работе коротко рассматривается значение интернета в информационном обществе. Показаны позитивные и негативные стороны интернета, его влияние на сознание человека. Анализируется возможность критического восприятия информации, размещенной в интернет-пространстве.

Abstract

The paper briefly examines the meaning of the internet in the information society. Positive and negative aspects of the internet, its influence on the human mind are shown. The possibility of critical perception of information which is placed in the internet space is analyzed.

Введение

Характерной чертой информационного общества является первостепенная роль информации, которая выступает основным ресурсом развития практически сферы человеческой деятельности, главной ценностью этого общества. Успех отдельного человека во многом зависит от того, насколько хорошо он способен взаимодействовать с информацией, координировать информационные потоки, трансформировать информацию в знания, а затем использовать его для своего дальнейшего развития.

Материалы доклада

Современное общество невозможно представить без интернета, который стал его своеобразной визитной карточкой. «Спросить у Гугла», «найти в интернете», «интернет знает все» – этими фразами сегодня никого не удивишь. Интернет стал нашим незаменимым помощником, нашим другом, с которым мы «общаемся» подчас гораздо чаще, чем с реальными друзьями. Интернет-пространство открывает новые возможности для коммуникации, организации бизнеса, проведения досуга, выполнения рабочих и бытовых задач, самореализации, образования и многого другого. Интернет является практически безграничным хранилищем информации, существенно упрощает доступ к мировым информационным ресурсам. Казалось бы: полная свобода выбора, ведь в интернете информация представлена на любой вкус и для любых целей.

Однако следует отметить, что интернет не настолько прост и безобиден, как может показаться на первый взгляд, а свобода, которая якобы предоставляется пользователям интернета в вопросе выбора потребляемой ими информации, да и вообще способа использования интернета, имеет свои границы. В данной работе мы намеренно опускаем такие негативные проявления интернета, как вирусные атаки, возникновение зависимости у интернет-пользователей, интернет-мошенничество, осуществляемые по сети кибернетические атаки, сайты, распространяющие противозаконную продукцию и услуги и т.д. Остановимся лишь на возможности адекватного восприятия информации, размещенной в интернет-пространстве.

В интернете мы можем найти информацию различных видов, форм, происхождения и предназначения: позволяющую нам более качественно выполнить свою работу и дающую возможность отдохнуть; которую можно посмотреть, послушать или почитать; заставляющую думать или дающую возможность расслабиться; которая дается нам в готовом виде, которую можно видоизменять или которую мы создаем самостоятельно;

исходящую из официальных источников или неофициальных; отражающую факты, содержащую обоснованные гипотезы или голые предположения и домыслы...

В этом контексте следует упомянуть феномен информационного неравенства: тот, кто контролирует информационные потоки, способен закладывать в сознании пользователей определенные информационные предпочтения и вкусы, задавать рамки информационного восприятия, формировать мировоззрение и таким образом направлять поведение людей в желаемое русло. Эта закономерность успешно работает как в традиционных СМИ, так и в современных информационно-коммуникативных каналах. Отметим, что социальные сети являются более действенным инструментом влияния на сознание молодых людей, чем традиционные СМИ. Продвинутые интернет-пользователи уже давно усвоили, что олигархи через подвластные СМИ транслируют выгодную им информацию. Сообщения, поступающая от «друзей», имеют больший кредит доверия, поскольку ею делятся обычные пользователи интернета, у которых отсутствует личная заинтересованности. Чем большее число пользователей репостит, «лайкает» сообщение, тем сильнее подсознательная уверенность в объективности распространяемой информации, тем меньше желания ее проверять и критически переосмысливать – в общем то достаточно сомнительное желание, учитывая количество фейковых аккаунтов, проплаченных интернет-агитаторов и прискорбную привычку некоторых пользователей «раздавать лайки» не особо вчитываясь в сообщение. Вот почему интернет называют не только кладезем полезной информации, но и, например, большой информационной свалкой, содержащей большое количество недостоверной и неактуальной информации.

Обилие информации, с одной стороны, предоставляет широкие возможности выбора, но, с другой стороны, в разы усложняет процедуру отбора и верификации информации. Клонированная или слегка модифицированная информация, например сообщения-близнецы на новостных сайтах, вытесняет альтернативные версии событий, происшествий, толкований. Причем вытеснение происходит на нескольких уровнях: сначала из первых страничек результатов поисковика, а в конечном итоге, и из сознания отдельных пользователей интернета – конечно, не всех поголовно, но достаточно большой их части. Такое вытеснение имеет вполне объективные и закономерные причины: принципы работы человеческого мозга (количество информации, которая может быть критически воспринята, ограничено ее общим разнообразием, длительностью воздействия и сложностью) в совокупности с информационной перегруженностью, силой привычки, влиянием авторитетов и банальной ленью.

В интернете серьезные материалы, требующие умственного напряжения, соседствуют с такими, которые «размягчают» мозги и превращают человека в ленивого потребителя простенькой информации; новостные сообщения с соблюдением всех канонов журналистской этики конкурируют с репортажами с завуалированным или откровенным навязыванием какой-либо идеи. Как правило, выигрывают в этой борьбе сообщения более понятные, играющие на простых, базовых эмоциях, потребностях и желаниях, внешне непротиворечивые и не требующие построения сложных умозаключений. Построение умозаключений (особенно, с привлечением дополнительной информации, не содержащейся в сообщении), является сложным мыслительным процессом. Очень малое количество людей способно держать себя в постоянном напряжении, перепроверя десятки сообщений ежедневно – это требует не только большого желания, но и развитых аналитических способностей, хорошей памяти, наличия определенных умений и навыков (от элементарной компьютерной грамотности до работы с современными базами данных) и, что не менее важно, – времени.

В условиях огромного разнообразия информации и знаний человек физически не способен разобраться во всем. При желании, он может быть специалистом лишь в некоторых областях, в остальных сферах ему придется полагаться на другие авторитеты, устоявшиеся мнения, прочитанную новость, интуицию – на что угодно, кроме рационального анализа и самостоятельного осмысления информации, что способствует превращению интернета из средства информирования в средство манипулирования.

КЛАСИФІКАЦІЯ ЗАГРОЗ ДЛЯ WI-FI МЕРЕЖ

Татарчук Артем, Куперштейн Леонід, Лукічов Віталій

Вінницький національний технічний університет

Анотація

Сьогодні все більше користувачів надають перевагу бездротовим мережам Wi-Fi, що міцно посіли важливе місце в нашому житті. Тому в даній статті запропонована класифікація загроз для бездротових мереж Wi-Fi.

Abstract

Today, more and more users prefer Wi-Fi wireless networks, which have gained an important place in our lives. Therefore, this article presents the classification of threats for wireless Wi-Fi networks.

Вступ

В даний час, в Україні, у зв'язку з входженням у світовий інформаційний простір, швидкими темпами впроваджуються новітні досягнення комп'ютерних і телекомунікаційних технологій[1].

Бездротові мережі на сьогоднішній день використовуються практично у всіх сферах діяльності. Широке використання бездротових мереж обумовлено тим, що вони є зручними та мають порівняно невисоку вартість.

Розвиток Wi-Fi технологій спровокує появу нових атак і засобів несанкціонованого отримання інформації. Саме тому актуальним є складання класифікації загроз для бездротових мереж Wi-Fi.

Результат дослідження

Класифікація загроз інформаційної безпеки була створена на основі класифікації запропонованої В. Б. Щербаковим та С. А. Щербаковим [2]. Але запропонована ними класифікація базується на проектуванні архітектури інформаційної безпеки і не може в повній мірі описати множини загроз для бездротової мережі Wi-Fi. Розглянуто класифікацію Панська А.В., Резніченко В.А. [3]. Дана класифікація пропонує тільки мережеві загрози і побудувати повну систему захисту за нею не можливо. Також розглянуто класифікацію Шовкута В. А. та Флорова С. В. [4], ця класифікація розглядає тільки вразливості протоколів безпеки Wi-Fi мереж, які також не підходять для створення системи захисту.

Наведена класифікація може служити етапом в аналізі ризиків інформаційної безпеки Wi-Fi мереж, для аналізу загроз інформаційної безпеки, на її основі можна вибрати методи захисту Wi-Fi мережі.

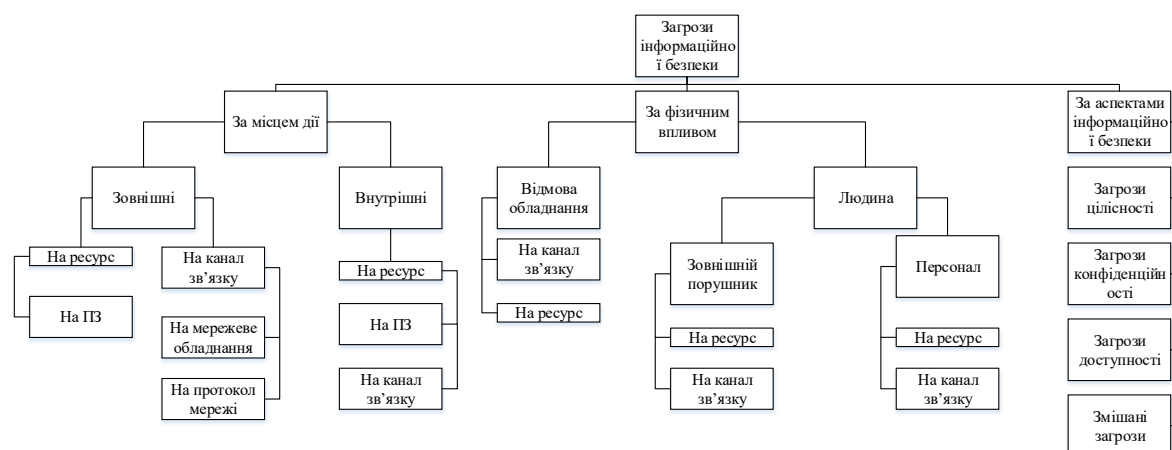
В даній статті наведено класи загроз, за якими можна розподілити конкретні загрози.

Кожен клас загроз має свій вплив: на ресурс, на програмне забезпечення та на канал зв'язку.

Під ресурсом розуміються:

- документація;
- персональні дані;
- інформація, яка знаходиться на базах даних, які пов'язані з Wi-Fi мережею;
- інша інформація, яка потрібна зловмиснику.

До основних загроз можна віднести: Dos-атаки, неправильне налаштування мережі, «випадкові асоціації» (коли ноутбук з Windows XP (досить довірливо ставиться до всіх бездротових мереж) або просто некоректно налаштований бездротовий клієнт автоматично асоціюється і підключає користувача до найближчої бездротової мережі), слабкі ключі шифрування, методи автентифікації з відомими вразливостями,



інтерференції, сканування мережі. Розвиток Wi-Fi мереж породили нові способи реалізації старих загроз, а також деякі нові, досі неможливі в провідних мережах. У всіх випадках, боротися з атакуючим стало набагато важче, тому що неможливо ні відстежити його фізичне місце розташування, ні ізолювати його від мережі. До них відносять: розвідку, імперсонацію, відмову в обслуговуванні.

Практично всі бездротові мережі в якийсь момент з'єднуються з провідними. Відповідно, будь-яка бездротова точка доступу може бути використана як плацдарм для атаки. Але це ще не все: деякі помилки в конфігурації точок доступу в поєднанні з помилками конфігурації провідної мережі можуть відкривати шляхи для витоків інформації. Найбільш поширений приклад - точки доступу, що працюють в режимі моста (Layer 2 Bridge), підключені в плоску мережу (або мережа з порушеннями сегментації VLAN) і передають в ефір ширококомовні пакети з дротового сегмента, запити ARP, DHCP, фрейми STP і т.д.

Деякі особливості функціонування бездротових мереж породжують додаткові проблеми, здатні впливати в цілому на їх доступність, продуктивність, безпеку і вартість експлуатації. Для грамотного вирішення цих проблем потрібен спеціальний інструментарій підтримки і експлуатації, спеціальні механізми адміністрування та моніторингу, не реалізовані в традиційному інструментарії управління бездротовими мережами.

Також загрозу мережевій безпеці можуть представляти природні явища і технічні пристрої, проте тільки люди (незадоволені звільнені службовці, хакери, конкуренти) проникають в мережу для навмисного отримання або знищення інформації і саме вони представляють найбільшу загрозу.

Бездротові мережі породжують нові класи ризиків і загроз, від яких неможливо захиститися традиційними засобами. Тому через особливості бездротового зв'язку, важливо контролювати не тільки безпеку інфраструктури доступу, але і стежити за користувачами, які можуть стати об'єктом атаки зловмисника або просто можуть випадково або умисно перейти з корпоративної мережі на незахищене з'єднання.

Список використаних джерел:

1. Концепція технічного захисту інформації в галузі зв'язку України. [Електронний ресурс]. – Режим доступу: <http://zakon5.rada.gov.ua/laws/show/1126-97-%D0%BF>
2. Щербаков В. Б. Безопасность беспроводных сетей: стандарт IEEE 802.11. / В. Б. Щербаков, С. А. Ермаков - Москва : РадиоСофт, 2010. - 256 с.
3. Загрози та вразливості бездротових мереж. [Електронний ресурс]. – Режим доступу: http://dSPACE.kntu.kr.ua/jspui/bitstream/123456789/5022/1/AUConferenceCyberSecurity_November2016_p146.pdf
4. Аналіз механізмів захисту та вразливостей бездротових Wi-Fi мереж. [Електронний ресурс]. – Режим доступу: <http://ir.nmu.org.ua/bitstream/handle>

NEW ASYMMETRIC ALGORITHM FOR FAST MESSAGE TRANSMISSION AND TROPICAL CRYPTOGRAPHY

Richard P. Megrelishvili

Javachishvili Tbilisi State University

Abstract

In this article we, in the literal sense, announced about the new fast numbers multiplication. With respect to the issue of relevance, we repeat, that the main advantage of the matrix one-way function is high speed operations [1]. The maximum speed is achieved with the direct multiplication of numbers [2].

As a result of ElGamal's algorithm (1985), the leading countries were able to create their state standards for digital signatures in the cryptography.

But ElGamal himself, when creating his system of direction in cryptography (1985), is based on the well-known Diffie-Hellman algorithm for the purpose of establishing a connection between the transmitting and receiving parties for a certain period of time. Similarly, we arrive in this article as in scientific works [1,2]. Similarly to ElGamal, we used Diffie-Hellman once (At a certain time period) [1] and twice in this article (In the same period of time).

The results their applications may be named as "Tropical Cryptography"[3]. But at the same time, regardless of the general algebraic values Tropical Cryptography, it is fact, that the construction of multiplicative groups, based on the our tropical operations, may be accepted as an integral part of the realization of the one-way function. Therefore, its adoption and an implementation can be associated with its recognition.

Introduction

The main goal is to achieve the high speed of the algorithm. This article is an example of words spoken. It all started in 2006, when an article was published that contains a new algorithm for single-function function. The fact is that similar algorithms, and there were only two of them, located in mathematics, specifically - in the field of number theory, have already been "snatched" by the cryptographs Diffie-Hellman and RSA. In this article we, in the literal sense, announced about the new fast numbers multiplication. With respect to the issue of relevance, we repeat, that the main advantage of the matrix one-way function is high speed operations [1]. The maximum speed is achieved with the direct multiplication of numbers [2].

The second part is intended for fast implementation algorithms.

In the remaining parts, the materials necessary for the full pre-inscription of the protection of the new One-Way function [1] and the method of Tropical Cryptography are presented [2].

The analysis showed that the matrix one-way function is broken, if it is used without a joint application with Tropical cryptography or without the use of one-way function (ie, the function is not a carrier of properties one-way function if it is applied without any special versions of, see below). Matrix function is as follows:

$$v A' = u. \quad (1)$$

Where $A' \in \tilde{A}$, a $\tilde{A}$ is a set of high power from an n -dimensional quadratic commutative matrices [1]. Along with this, $v, u \in V_n$. Where V_n vector space of dimension n (For simplicity $\tilde{A}$ and V_n is considered over the Galois field $GF(2)$). In expression (1) v and u are open (without any special versions) and A' is secret, although A - initial matrix is open with which may be formed a plurality $\tilde{A}$ (e.g., a plurality $\tilde{A}$ can be produced with degrees of matrix A). Therefore, if the expression (1) is considered as a one-way function, then it can break down in the following ways:

If the matrix set $\tilde{A}$ contains recursion (that was identified by us), then the expression (1) can easily be broken with the help Companion matrices, that is, the set of n^2 unknown can be lead to a matrix with n unknowns, for any square matrix $A' \in \tilde{A}$ can be bring to n unknown, i.e., using the equation (1) can obtain a system of n equations in n unknowns, etc. These issues have been discussed in [2-5, 6]. If the matrix of set of $\tilde{A}$ does not contain recursion (or hard to find), then the matrix one-way function can be broken with the use of the basic matrixes of $A_0, A_1, A_2, \dots, A_{n-1}$ which is not hard to get, if we know the initial matrix A .

Rapid algorithms

The main task is to quickly implement the transfer of necessary information. But for this it is necessary to implement two times for a certain time interval. It is necessary to transfer (from the transmitting X side to the receiving side of Y) secretly the particularly important mod p and d values introduced by T.ElGamal in 1985. After the implementation of secrecy, we can transmit information on an asymmetric channel: $C = M * e \pmod{p}$.

And take it to the host: $M = C * d \pmod{p}$.

Let's spread the information transfer by example. Let's assume that the corresponding parameters are: $p = 11$, message $M = 2$. To form e and d, we use the expression: $e * d = 1 \pmod{p}$. To form e, d, we consider two cases - $k = 1$ and 4. We obtain: $e_1 = 4, d_1 = 3; e_2 = 5, d_2 = 9$.

For speedy transmission of our message, choose $e = 5, d = 9$, then we get: $C = M * e = 2 * 5 = 10 \pmod{11}$.

And take it to the host: $M = C * d = 10 * 9 \pmod{11} = 2$.

On the possibility of breaking the one-way function matrix

We want to show that though (1) the matrix function is broken without additional versions, but this is exceptional function. It is special function because of its speed and therefore deserves special attention. We are convinced that the additional versions will not reduce the speed and efficiency of the entire system. It is interesting, how it is can be possible with additional means maintained the speed, the efficiency and the strength of the system? In addition, for this article we consider the ability to break of matrix one-way function, and then we will discuss the possibilities of using tropical cryptography and exponential one-way function. We'll look at how break the matrix one-way function with the use, of said, of basis matrixes (other questions, how to hack the function (1), were considered in [1-7]). We will consider breaking this function in the particular example.

Suppose, it is given the multiplicative group $\tilde{A}$ of the commutative matrices of dimension 3×3 (the group has a maximal order, $e = 2^3 - 1 = 7$):

$$A = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix}, A^2 = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix}, A^3 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \dots, A^7 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}. \quad (2)$$

Suppose, the two subjects X (Alice) and Y (Bob) can form the secure key k with matrix one-way algorithm via public channel (This algorithm is based on a matrix one-way function (1)). Then Alice selects matrix $A_1 = A^2$ as the secret matrix in (2). Bob, for his part, chooses the matrix $A_2 = A^3$, we also assume that $v = (110)$. Then our algorithm will be functioning as follows:

– Alice computes and sends to Bob the following vector:

$$u_1 = vA_1 = (011). \quad (3)$$

– Bob computes and sends to Alice the following vector:

$$u_2 = vA_2 = (111). \quad (4)$$

– Alice computes the exchanged key:

$$k_1 = u_2A_1 = (100). \quad (5)$$

– Bob computes the exchanged key:

$$k_2 = u_1A_2 = (100). \quad (6)$$

As we see $k = k_1 = k_2$ and the results are correct (The matrixes are commutative: $vA_1A_2 = vA_2A_1$). As noted above, we plan to break the algorithm by means of the basis matrix comprising a multiplicative set $\tilde{A} = \{c_0A^{2^0}, c_1A^{2^1}, \dots, c_{n-1}A^{2^{n-1}}\}$ (where $\{c_0, c_1, \dots, c_{n-1}\} \in GF(2)$). For a set of (2) we form an appropriate basis:

$$A^0 = I, A^1, A^2, \quad (7)$$

Where $A^0 = I$ is the identity matrix. In the beginning we define the matrix $A_1 = A^2$ selected by Alice. The required matrix is denoted by $A_1(x)$, then we will have:

$$A_1(x) = c_0A^0 + c_1A^1 + c_2A^2. \quad (8)$$

Since Ellis opened calculates the value of $A_1(x)$, then we have:

$$u_1 = vA_1(x) = c_0vA^0 + c_1vA^1 + c_2vA^2 = c_0w_0 + c_1w_1 + c_2w_2. \quad (9)$$

Considering (2), (3) and (9) we can determine the values of u_1 and w_0, w_1, w_2 :

$$\begin{aligned} vA^0 &= (110) A^0 = (110) = w_0, \\ vA^1 &= (110) A^1 = (001) = w_1, \\ vA^2 &= (110) A^2 = (011) = w_2, \\ u_1 &= (011). \end{aligned} \quad (10)$$

Using (9) and (10) we may form a system of equations for the coefficients c_0, c_1, c_2 :

$$\begin{aligned} 1c_0 + 0c_1 + 0c_2 &= 0, \\ 1c_0 + 0c_1 + 1c_2 &= 1, \\ 0c_0 + 1c_1 + 1c_2 &= 1. \end{aligned} \quad (11)$$

Solving the system of equations (11), we define the values of the coefficients: $c_0 = 0, c_1 = 0, c_2 = 1$. Then, from (8) we obtain the value of the ratio of the desired matrix: $A_1(x) = A^2$, i.e. get the matrix A^2 of (2). The answer is correct. (Similar we can find the matrix A_2 , chosen by Bob).

Two embodiment of the one-way matrix function

As stated above, this paper first announced two special versions of the matrix one-way function. First option, as a result of the natural development of cryptography, involves the use of new tropical arithmetic operations in cryptography. When applying was found that the new tropical operations apart from a general purpose can be thought integral part of our matrix one-way function. Therefore, if earlier, for the construction of matrices A had to use classical arithmetic operations, it is now necessary to apply our new tropical arithmetic. With new tropical operations, we must build a set of matrices $\tilde{A}$ with the properties with the same as before: high dimension and order, i.e. we should construct a multiplicative group $\tilde{A}$ that is formed by degrees of an initial matrix A of new form (of a new structure). Construction of a new matrix of $\tilde{A}$, as noted above, is already a meaningful (traditional) problem and we would not have shown any effect if there was not having contact with her. Consider the issues of the first option, that we have introduced, or questions about Tropical Cryptography. The obtained tropical operations, for simplicity, considered over the Galois field $GF(2)$. Additive operations, in this case, are the same as the classical operations:

$$0 + 0 = 0; 0 + 1 = 1; 1 + 0 = 1; 1 + 1 = 0 \quad (12)$$

But the multiplicative operations are fundamentally different from the classical operations [7]:

$$0 * 0 = 0; 0 * 1 = 1; 1 * 0 = 1; 1 * 1 = 1. \quad (13)$$

Interestingly, what feature and utility of our proposed tropical operations? Must be stated that the new operations cause so impressive effect in their application that raises another question? It is about ensuring the stability of the matrix function (1), i.e. on the solubility or insolubility of the system of equations (11), depending on what kind of arithmetic operations will be applied - the classic or offered by us? For example, in our opinion, the system of equations (11) does not have a unique solution. Matrix function (1), with tropical operations, is one-way function, it will not be broken in real time, and satisfies the conditions of stability (Under appropriate conditions, implying the proper dimension and higher order for a set of matrices A). Indeed, when using the new operations (12) and (13), a system (14) has not a unique solution (to the counterweight (11)), since by multiplication coefficients of c_0, c_1, c_2 on the w_0, w_1, w_2 will not cause the formation of null values but on the contrary, causes the formation of new unknowns (While, in the classical operations and using the Gauss method, the system (11) is rapidly soluble):

$$\begin{aligned} 1 * c_0 + 0 * c_1 + 0 * c_2 &= 0, \\ 1 * c_0 + 0 * c_1 + 1 * c_2 &= 1, \\ 0 * c_0 + 1 * c_1 + 1 * c_2 &= 1. \end{aligned} \quad (14)$$

For example, the first line of system (14) has the six unknowns, therefore, when dimension has high order (and there are used our tropical operations), the system (14) does not has a solution in real time. Therefore, our matrix one-way function according to the first embodiment ensures durability, since it is not can to break in real time (Take into account the fact that tropical group (15) is a multiplicative group and not a field). As an example we present the multiplicative group (15). For the key exchange algorithm are used: A is an Initial Matrix of (15) and the corresponding $u = vA^3$, where $v = (110)$:

$$A = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, A^2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}, A^3 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}, \dots, A^7 = A^0 = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix} \quad (15)$$

The implementation of the algorithm according to (15) does not differ from the implementation of the algorithm (3) - (6), since the main issue here - the generation of the multiplicative group of maximal order, which meets the requirements of Tropical Cryptography (12) - (13).

Interestingly than can one explain that - the second embodiment has, too, a high efficiency and durability as the first, whereas radically different from the first? In a second embodiment, with respect to the matrix of our one-way function is used a different one-way function (i.e. there is a new problem), but as a method of processing, it shows identity with the decision of other cryptography tasks, which, in our opinion, deserves attention (see. below). For example, ElGamal uses an exponential one-way function to solve their problems, but the thing is - how? He uses a one-way function periodically, for a certain length of time [8]. The similarity with our second option is a period of time for which use the function [9]. In the algorithm of ElGamal degree (exponential) one-way function is used within a certain time period, to meet the challenges of authentication and verification. We use it also within a certain time period, to resolve the problem of the stability of our matrix one-way function. For this, by using exponential one-way function occurs a key exchange via the open channel. The result of this key exchange is a secret of parameter $k = v$. In this same time period occurs the key exchange, or other operations carried out, with our algorithm. In this case, in (1) parameters v , A' are secret and only parameter u is open. This change defines the stability of one-way function (1) and also of algorithm (3) - (6), and it does not cause decrease the rate of operation.

References:

- 1.R.P.Megrelishvili, Analysis of the Matrix One-Way Function and two Variants of Its Implementation, International J. of (IJMRAE), Vol. 5, No. IV (October 2013), pp. 99-105.
- 2.R.P.Megrelishvili, Two New Versions of Numbers Fast Multiplication and Tropical Cryptography, Communications on Applied Electronics (CAE), Foundation of Computer Science FCS, New York, USA, Volume 7 – No. 8, October 2017, pp. 12-15.
- 3.R.P.Megrelishvili, New Direction in Construction of Matrix One-Way Function and Tropical Cryptography, Archil Eliashvili Institute of Control Systems of The Georgian Technical University, Proceedings, N 16, 2012, pp.244-248.
- 4.R.Megrelishvili, M.Chelidsze, K.Chelidze, "On the construction of secret and public key cryptosystems," Iv.Javakhishvili Tbilisi State University, I.Vekua Institute of Applied Mathematics, Informatics and Mechanics (AMIM), v. 11, No 2, 2006, pp.29-36.
- 5.R.Megrelishvili, A.Sikharulidze, "New matrix sets generation and the cryptosystems," Proceedings of the European Computing Conference and 3rd International Conference on Computational Intelligence, Tbilisi, Georgia, June, 26-28, 2009, pp. 253-255.
- 6.R.Megrelishvili, M.Chelidze, G.Besiashvili, "Investigation of new matrix-key function for the public cryptosystems". Proceedings of The Third International Conference, Problems of Cybernetics and Information, v.1, September, 6-8, Baku, Azerbaijan, 2010, pp. 75-78.
- 7.R.Megrelishvili, M.Chelidze, G.Besiashvili, "One-way matrix function - analogy of Diffie-Hellman protocol", Proceedings of the Seventh International Conference, IES-2010, 28 September-3 October, Vinnytsia, Ukraine, 2010, pp. 341-344.
- 8.W.P.Wardlaw, Matrix Representacion of Finite Fields, U.S. Navy, March 12, 1992, pp. 1-10, NRL/MR/5350.1-92-6953.
- 9.W.Diffie and M.E.Hellman. New Direction in Cryptography, IEEE Transaction on Information Theory, IT-22, n. 6, Nov. 1976, pp. 644-654.
10. ElGamal. "A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," IEEE Transaction on Information Theory, v. IT-31, n. 4, 1985, pp. 469-472.
11. R.I.Rivest, A.Shamir and I.M.Adleman, A Method for Obtaining Digital Signature and Public-Key Cryptosystems, Communications of the ASM, v. 21, n. 2, Feb. 1978, pp. 120-126.

NEW BLOCK ENCRYPTION ALGORITHM

Kochladze Zurab¹, Beselia Lali²

¹ Ivane Javakhishvili Tbilisi State University Faculty of Exact and Natural Sciences, Department of Computer Science

² Sokhumi State University, Faculty of Mathematics and Computer Sciences

Abstract

This paper describes a new block encryption algorithm that uses the Hill's modified algorithm for faster efficiency process. This allows us to increase the encryption and decryption speeds so as not to reduce the algorithm's resistance to cryptanalytic attacks.

Анотація

В этом документе описывается новый алгоритм шифрования блоков, который использует модифицированный алгоритм Хилла для ускорения процесса эффективности. Это позволяет увеличить скорость шифрования и дешифрования, чтобы не уменьшать устойчивость алгоритма к криптоаналитическим атакам.

Introduction

Modern block algorithms are very often very substantially different from each other [1, 2] in both, architecture and the number of operations and rounds, but the outcome of their work is always the same. The starting line is a binary string with the length of n , whose structure is defined by the open text, by the key of length k and the use of certain operations, after the multiple iterations goes back to the n length pseudo-random bit string. In fact, any block algorithm mathematically can be imagined as function of two variables

$$E : \{0,1\}^n \times \{0,1\}^k \rightarrow \{0,1\}^n,$$

where $(0,1)^l$ notes bit string of l length, and k and n values depend on the specific of encryption algorithm. In practice, this means that for each fixed $K \in \{0,1\}^k$ encryption function is a replacement on $\{0,1\}^n$ bit string [3, 4]. Obviously, the received function can't be absolutely random, since the transfer is done with the determinant algorithm. This means that any such algorithm can theoretically be broken, and it can be only computationally protected against the cryptanalytic attacks. In order to prevent an opponent with limited computational resources from breaking the algorithm, it is essential that the binary string that is encrypted by encryption algorithm, will be near with a random binary string.

As it is well known, C. Shannon in his fundamental work [5] showed that to achieve this goal it is necessary, that maximal number of open-text symbols to take part in getting one symbol of cipher-text. To achieve this goal, modern bloc ciphers use several iterations, i.e. the same block is encoded several times using different keys. Obviously, repeating the same procedure increases the encryption time. Thus, it is better that the operations used in the rounds are more effective in this regard.

Description of algorithm

In 1930, the American mathematician L.S. Hill developed the previously existing bigram and trigram ciphers and introduced a n -gram encryption using a linear algebra [6]. The essence of the algorithm is that as it is obtained in the classical cryptography, the letters of the encrypted text will be transferred to the numbers. Then these numbers are divided into vectors of length n and are multiplied to a $n \times n$ square matrix by module n , where n is the number of characters in the language on which the open text is drawn. The matrix that represents the key of this algorithm must have a reverse matrix. It is not easy to use only crypto-text to attack the

algorithm, but it is easy to attack using open-text, because the conversion is a straight line, and if the size of the matrix is $n \times n$, then only the linear n^2 equation system is needed to accurately calculate the key. Because of these reasons, the long-term algorithm was no longer used in computer cryptography, although the multiplication operation on the matrix has a very high efficiency of diffusion. In recent years the works [7,8,9,10] have been published, the authors of which are still trying to use different options of the Hill's Algorithm due to the quality.

In the articles [11,12], the author describes Hill's modified algorithm that can be used in cipher in which the encrypted block can be viewed as a matrix of the condition (for example AES standard [13]).

Description of the algorithm: the size of the block is 128 bits. Two keys are used for encryption, each of them is 128 bits long. The open text will be viewed as ASP-II codes in binary string and will be divided into 128 bit length blocks. Before the open text will enter in first round, it gathers with the 128-bit first key with the xor operation. Each round consists with three operations: multiplication on the self-reversible matrix, shifting the bytes in matrix and gathering with the round key. The result of first operation will be divided by 16 bits (16 bytes) and will be written as a square matrix (4×4). Recording from left to right and down from the top. Bytes will be transferred in decimal systems. Received matrix is multiplied by the self-reversible matrix by mod256. In received matrix, the bytes are shifted to left by strings by one byte. The bits string will be transformed into a matrix and will enter the second round matrix will be transfer on bit string and we gather it with the second key by xor operation. The gathered bits string will be transformed into a matrix and will enter the second round. After four rounds, we get an encrypted text.

References:

1. B. Schneier. Applied cryptography, John Wiley & Sons, Inc. 1996.
2. M. Mogollon. Cryptography and Security Services. Cybertech Publishing 2007
3. R. Oppilger. Contemporary Cryptography Artech House Boston/ London 2005.
4. M. Bellare, P. Rogaway. Introduction to Modern Cryptography. -UCSD CSE 207, 2005.
5. C. Shannon. Communication theory of secrecy systems. Bell System tech. J., 28, #4 (1949), 656-715.
6. Lester S. Hill. Cryptography in an algebraic alphabet. //The American Mathematical Monthly, vol.56, #6, 1929, pp. 306-312.
7. Bibhudendra Acharya, Sarojkumar Panigrahy, Saratkumar Patra, Canapsti Panda. Image Encryption Using Advanced Hill Cipher Algorithm. // International Journal of Recent Trends in Engineering, May 2009, vol.1, No.1, pp.663-667.
8. Bibhudendra Acharya, SarojkumarPanigrahy, SaratkumarPatra, and Canapsti Panda. Image Encryption Using Advanced Hill Cipher Algorithm. International Journal of Recent Trends in Engineering. Vol.1, No.1, May 2009. pp.663-667.
9. M. Farmanbar, A.G. Chefranov. Investigation of Hill Cipher Modifications Based on Permutation and Iteration. (IJCSIS) International Journal of Computer Science and Information Security. Vol.10, No9, September, 2012. pp.1-7.
10. V.U.K.Sastry, A.Varanasi and S.U. Kumar. A Modern Advanced Hill Cipher Involving a Permuted Key and Modular Arithmetic Addition Operation
11. Z. Kochladze. Modified Version of the Hill's Algorithm. GESJ: Computer Science and Telecommunication No3 (43) 2014.
12. Georgian engineering innovations, No.1 (vol.73), 2015, pp.50. In Georgian.
13. J. Daemen, V. Rijmen The Decign of Rijndael: AES – The Advanced Encryption Standard. Springer, 2002.

РОЗРОБЛЕННЯ ІННОВАЦІЙНОГО ІТ-СТАРТАПУ ПРОГРАМНОГО ПРОДУКТУ «ПОМІЧНИК СІМЕЙНОГО БЮДЖЕТУ» (“FAMILY BUDGET HELPER”)

Яремко Олег, Кунанець Наталія

Національний університет «Львівська політехніка»

Анотація

У цій роботі проаналізовано основні засади роботи організацій, призначених для пошуку й створення життєздатної бізнес-моделі, яка в подальшому допоможе підприємцю розвинути його бізнес-проект в успішну компанію. Міні-підприємства, що отримали умовну назву стартап, набувають все більшої популярності серед молодих підприємців як України, так і всього світу. Проаналізуємо підходи до створення такого стартапу в галузі інформаційних технологій.

Розроблений нами ІТ-стартап ґрунтується на створенні комп'ютерної програми для формування та моніторингу сімейного бюджету – «Помічник сімейного бюджету» (“Family budget helper”). Програма розрахована на членів однієї родини і адаптується під певного користувача.

У статті наведено цілі та стратегії розвитку, оцінювання його ризиків та сильних сторін (SWOT-аналіз) стартапу. Розраховано необхідні ресурси й можливості їхнього залучення із зовнішніх джерел, розроблено прототип ІТ-стартапу, подано особливості ІТ-стартапу, спрямованого на допомогу сім'ям саме у фінансовій сфері.

Abstract

This paper describes organizations that are dedicated to finding and creating a viable business model, which in the future should help an entrepreneur develop his product into a successful company – start-ups. These mini-enterprises are gaining popularity among young entrepreneurs both in Ukraine and around the world. So, we give an example of creating such a start-up in the field of information technology.

Our IT start-up is a computer program, which generates and checks the family budget - the “Family budget helper”. The program is made for members of one family with the ability to change the user.

In order to better understand the principles of the development and work of the “Family budget helper”, the paper provides goals and strategies of development, evaluation of its risks and strengths (SWOT-analysis). In addition, the resources and the possibilities of their attraction from external sources are considered, a prototype of this IT start-up has been developed.

The report on this IT start-up is aimed at people who are interested in cutting-edge innovative technologies and want to learn how to ease their everyday troubles with their help.

Вступ

Інформація в сучасному суспільстві, а особливо її опрацювання з допомогою інформаційних технологій, залишається на сьогодні важливим фактором підвищення ефективності діяльності людини у всіх сферах суспільства. Для удосконалення процесів ефективного опрацювання останніми роками все частіше створюють стартапи. Перевагами такого підходу є формування пропозицій щодо продуктів або сервісів, які або до цього ще не були представлені на товарному ринку, або ж наявні не задовольняють потреб споживачів, тому висувуються ідеї щодо їх вдосконалення. При цьому не виключається ситуація, що для однієї держави ідея стартапу може бути справді прогресивною та інноваційною, а для іншої – традиційною і далеко не новою. Тобто стартап – не обов'язково повинен бути глобального рівня, тут усе залежить від можливостей розробників.

Мета

Метою статті є проаналізувати IT-стартап у вигляді розробленої комп'ютерної програми призначена полегшити ведення та аналізування фінансових справ як окремої сім'ї, так і певної людини «Помічник сімейного бюджету» (“Family budget helper”).

Постановка проблеми

Відомо, що в сучасних не надто економічно вигідних умовах життя, контролювати свої прибутки та видатки є особливо важливо. Проте не всі володіють компетентностями фінансистів, або ж володіють основами фінансової грамотності, незважаючи на наявність безлічі тренінгів. Інформаційні продукти, зорієнтовані на допомогу у формуванні та моніторингу сімейного бюджету практично відсутні. Проте слід наголосити, що ця проблема є надзвичайно важливою, адже від добробуту сім'ї залежить стан добробуту в країні, у якій ця сім'я проживає. Такий стан речей генерує потребу створення програмного продукту, який допомагав би сім'ям в опрацюванні та аналізі інформації про їх сімейний бюджет, його планування, визначення тенденцій щодо його стану тощо.

Основний виклад матеріалу

Розроблений програмний продукт дозволяє користувачеві легко організовувати всю необхідну інформацію про сімейний бюджет та отримувати важливу інформацію про його фінансовий стан, надає можливість аналізу різних аспектів бюджету залежно від факторів, категорій, подій і т. п., полегшує пошук резервів, шляхів скорочення витрат тощо. Важливо, що програмою зможуть користуватися члени однієї родини, проте, завдяки опції «встановлення паролів», у них є змога надавати доступ обмеженому колу користувачів. Таким чином усувається потреба створення окремих облікових записів, що значно оптимізує роботу із такою програмою. Основним призначенням цього стартапу є формування та моніторинг сімейного бюджету завдяки ефективному алгоритму автоматизованого збору та опрацювання інформації. Програмний продукт оснащений зручним та зрозумілим інтерфейсом, що надає користувачеві доступ до важливих даних про стан його бюджету, висвітлювати зміни у будь-який момент часу.

Головні переваги розробленого програмного продукту – можливість формування, аналізу та роздруку статистичних звітів про використання сімейних фінансів за заданий період, а також спрощена технологія введення вхідних даних у програму, завдяки опції сканування товарних чеків.

Спроектований інформаційний продукт виконує наступні функції:

- аналіз структури сімейного бюджету, методики його формування та моніторингу;
- формування бази даних;
- аналіз видатків та надходжень, формування статистичних звітів[1].

Для реалізації поставленого завдання була обрана мова програмування C# з використанням .NET Framework, а саме підсистеми Windows Presentation Foundation. Основні характеристики створюваної нами програми:

- платформа: .Net Framework [2,3];
- операційна система: Windows;
- мова програмування: C#;
- засоби розроблення: Windows Presentation Foundation (WPF);
- кількісні показники: один програмний продукт;
- необхідні ресурси: стартовий капітал 60 тис. грн.

Доступом до необхідного функціоналу забезпечується через зручний інтерфейс.

Вирішено розробити цей програмний продукт у вигляді стартапу, адже початкові стадії розробки не потребували значних капіталовкладень, а, за умови успішності цього проекту, зовнішні інвестиції допоможуть перетворити первісний прототип на якісний та конкурентоспроможний IT-продукт.

Оскільки, необхідною умовою успішного проекту є бізнес-план, а в нашому разі – бізнес-план стартапу, визначемо перспективні цілі його реалізації.

З допомогою зручного інструменту менеджменту проектів S.M.A.R.T. [4] визначимо початкові цілі нашого IT-стартапу:

1. Створення якісної інноваційного програмного продукту із зручним та зрозумілим користувацьким інтерфейсом.

2. Організація ефективного маркетингу програми, який допоможе охопити 50-тисячну аудиторію користувачів за перші півроку.

3. Отримання прибутку за рахунок продажу програмного продукту вже протягом перших півроку.

4. Залучення інвестицій на розвиток функціоналу програмного продукту не пізніше, ніж через півроку від його створення.

5. Вихід на міжнародний рівень через рік після реалізації проекту.

6. Збільшення покупців за 2 рік існування програмного продукту на ринку як мінімум на чверть відносно першого року.

7. Створення мобільного додатку програмного продукту після реалізації пункту 3.

8. Синхронізація із банківськими системами після реалізації пункту 3.

9. Розширення робочого колективу на 3 рік діяльності програми для її покращення та надання супутніх послуг.

Ймовірність успішності будь-якого стартапу коливається від 0,1% до 20%. Тому дуже важливим на початковому етапі реалізації проекту із розроблення стартапу визначити стратегію, якої необхідно дотримуватися для досягнення конкурентоспроможності стартапу в умовах жорсткої ринкової конкуренції.

Оскільки ми позиціонуємо наш програмний продукт «Помічник сімейного бюджету» як інноваційний IT-стартап, вважаємо найдоцільнішою стратегією його створення - стратегію диференціації, основна мета якої довести потенційним користувачам, що пропонований продукт є унікальним і важливим для вагомого числа покупців.

Стратегія передбачає позиціонування продукту як найкращого на ринку, обґрунтування його унікальності для привабливості вибагливих покупців; наголошення на інноваційності підходу до розроблення програмного продукту та аналіз можливості створення його різноманітних модифікацій.

Висновки

Таким чином, відмінність розробленого IT-стартапу полягає не лише у тому, що створений «Помічник сімейного бюджету» покликаний швидко та ефективно забезпечувати аналіз значного обсягу інформації про сімейний бюджет, його зміни та можливості поповнення, але й у тому, що програмний продукт за мінімальних часових та матеріальних витрат забезпечує доступ до інформації сформованій спільноті користувачів. Запропонований авторами IT-стартап «Помічник сімейного бюджету» є цілком конкурентоспроможним в Україні, оскільки на вітчизняному IT ринку аналогічного якісного продукту не представлено.

Список використаних джерел:

1. Біла О.Г. Фінансове планування і прогнозування. Навчальний посібник. – Львів: Компакт, 2005. – 312 с.

2. Грицунов О.В. Інформаційні системи та технології. Навчальний посібник. – Харків: ХНАМГ, 2010. – 222 с.

3. Інформаційний ресурс Microsoft Developer Network (msdn.microsoft.com), розділ API, довідка та рекомендації, а саме такі підрозділи як: Visual C#, .NET Framework, Windows Presentation Foundation та засоби розробки.

4. Кірейцев Г.Г. Фінансовий менеджмент. Навчальний посібник. – Київ: ЦУЛ, 2002. – 496 с.

ВИКОРИСТАННЯ QR-КОДІВ В ПЛАТІЖНИХ СИСТЕМАХ

Сотнікова Альона, Сілагін Олексій

Вінницький національний технічний університет

Анотація

Розглянуто актуальність питання зчитування QR-кодів. Розглянуто основні типи інформації, що може бути закодована у QR-коді. Проаналізовано відмінності між статичними та динамічними QR-кодами. Визначено доцільність розробки системи для контролю грошових операцій з використанням технології зчитування QR-кодів.

Abstract

Considered the relevance of reading QR-codes. The main types of information that can be coded in QR-code are considered. The differences between static and dynamic QR-codes are analyzed. Determined feasibility of developing a system to monitor transactions using QR-code technology.

Вступ

На сьогоднішній день у світі на web-сайтах, сторінках блогів, у періодичних виданнях, на туристичних об'єктах, плакатах, одязі, в музеях, на сувенірах розміщені QR-коди. QR-код виконує дві функції: вміщує велику кількість інформації у невеликій картинці і дозволяє автоматично зчитувати закодовані дані. QR-код – доволі простий, зручний та інтерактивний спосіб швидкого отримання та поширення інформації.

Основні типи інформації, що може бути закодована у QR-коді

Найчастіше в QR-кодах закодована така інформація:

- Текст – в QR-коді може бути зашифрований текст різного спрямування.
- Контактні дані – візитка з QR-кодом дає можливість зчитувати персональні дані і зберігати їх у пам'яті мобільного пристрою або персонального комп'ютера.
- Номери телефонів – телефонний номер, розміщений в QR-коді, може бути набраний автоматично чи на нього може бути відправлене смс-повідомлення [1].
- URL-адреси – дозволяє відкрити веб-сторінку без введення її адреси з клавіатури.
- E-mail з темою листа – в коді можна зашифрувати ім'я отримувача і адресу електронної пошти, щоб надати користувачу змогу швидко та без зайвих зусиль відправити лист.
- Географічні координати – за допомогою QR-коду можна визначити місце розташування об'єкта на електронних картах (наприклад Google, Yandex та інші).
- Графічні файли форматів .gif, .jpg, .png, невеликого розміру.
- Адреси електронних гаманців [2].

Відмінності між статичним та динамічним QR-кодами

Статичний QR-код містить інформацію, яку було вказано на момент його генерації. Інформацію у такому коді не може бути змінено без повторної генерації вже з новими даними.

Динамічний QR-код відрізняється тим, що після його створення, інформація у ньому може бути відредагована без втручання в сам код. Динамічні коди створюють і наносять один раз, при цьому адміністратор (власник QR-коду) може змінювати інформацію та посилання, з якого буде відбуватися відображення [3].

Загальну структуру, що використовується для формування як динамічного, так і статичного QR-кодів, наведено на рисунку 1.

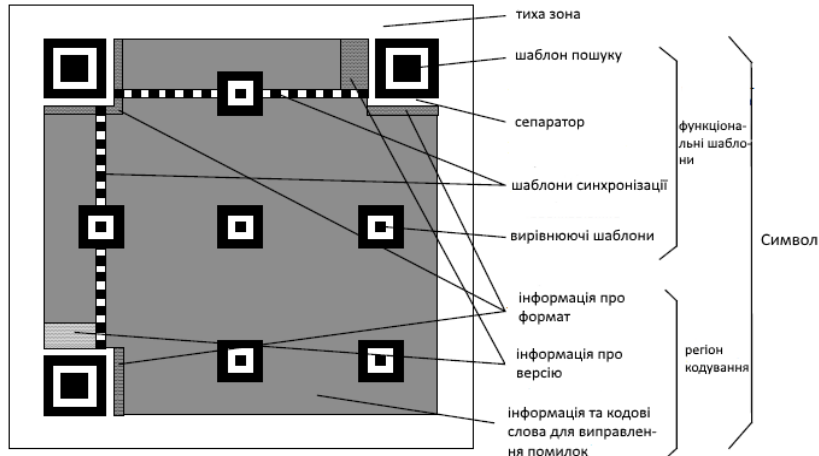


Рисунок 1 – Структура QR-коду

Використання QR-кодів в платіжних системах

Найпопулярніший і найприбутковіший варіант використання QR-кодів - індустрія платежів. Масова поява у користувачів мобільних пристроїв типу “смартфон” в кінці 2000-х років стимулювала розвиток цифрових і мобільних платежів. Поява QR-кодів спровокувала “революцію” в світі платежів, так як тепер будь-який користувач може виконати транзакцію лише завантаживши мобільний додаток [4].

Станом на кінець 2017 року Китай є лідером у впровадженні технології QR-кодів. Alipay інтегрувала платежі на основі QR-кодів в 2013 році, а WeChat послідувала її прикладу на початку 2014 року. Відповідно до даних статистики, що були наведені Alipay на конференції “Money 20/20” в Європі в квітні 2016 року, послуга мобільних платежів використовується для здійснення більш 175 мільйонів транзакцій на добу [5].

Висновки

На сьогоднішній день зростає зацікавлення в швидкому доступі до інформації. Перевагою QR-кодів є висока ймовірність розпізнавання інформації навіть у випадку його пошкодження. QR-кодування є зручним, використовується в багатьох сферах, набуває популярності і широко використовується в банківській справі та електронній комерції.

Алгоритм зчитування QR-коду планується до імплементації у систему моніторингу проведення операцій з купівлі-продажу валюти, тому надалі необхідно продовжити дослідження вже в контексті зчитування адрес електронних гаманців та генерації QR-кодів на основі цих адрес.

Список використаних джерел:

1. Вячеслав Логачев. Что несет QR-код. [Електронний ресурс]. — Режим доступу : <http://www.ridcom.ru/publications/131/>.
2. Weibing Chen «A Simple and Efficient Image Pre-processing for QR Decoder». http://www.atlantis-press.com/php/download_paper.php?id=3264
3. Мир високих технологий [Електронний ресурс]. — Режим доступу : <http://www.wht.by/blog/1567-sonicnotify-akusticheskaya-versiya-qrkodov.html>.
4. Squires, Sanford, R. Levinger, James «Efficient finder patterns and methods for application to 2d machine vision problems». http://www.wipo.int/pctdb/en/wo.jsp?wo=2006127608&IA=US2006019749&DISP_LAY=STATUS
5. Читаем QR-код [Електронний ресурс]. — Режим доступу: <http://habrahabr.ru/post/127197/>.

АНАЛІЗ МОВ НАПИСАННЯ СМАРТ КОНТРАКТІВ ІСНУЮЧИХ КРИПТОВАЛЮТ

Щербіна Євгеній, Месюра Володимир

Вінницький національний технічний університет

Анотація

Розглянуто існуючі мови написання смарт-контрактів. Розглянуто їх переваги та недоліки. Проведено аналіз існуючих вразливостей. Проведено аналіз середовища виконання (runtime) смарт-контрактів.

Abstract

Considered existing smart-contract languages. Considered their benefits and drawbacks. Analyzed existing vulnerabilities. Analyzed runtime of smart-contracts.

Вступ

На сьогоднішній день у світі дуже розповсюджений спосіб оплати з використанням електронних гаманців та готівки, переведеної у криптовалюту. Існує декілька сотень різних видів криптовалют, проте найпопулярнішою є біткоїн - електронна валюта, концепт якої був озвучений 2008 року Сатосі Накамото.

Bitcoin

Bitcoin — електронна валюта, концепт якої був озвучений 2008 року Сатосі Накамото, і представлений ним 2009 року, базується на самоопублікованому документі Сатосі Накамото. Повна капіталізація ринку біткоїнів на 5 грудня 2017 року, коли курс сягав 12 000 \$, становить 200 млрд USD. Середня ціна одного біткоїна на 30 листопада 2017 року — понад 10 000 \$.

У грудні 2017 року Bitcoin став шостою за капіталізацією валютою світу, обійшовши рубль, фунт і південнокорейську вону. 7 грудня курс досяг свого чергового максимуму в 17,7 тис. дол.. Наступний ріст до 20 тис. доларів відбувся 17 грудня, потім курс впав до 16 тис. У 2018 році курс продовжив падати. Періодично підіймаючись і падаючи на 10-20%, станом на 5 квітня 2018 року 1 Bitcoin коштує 6800 дол [1].

Ethereum

Ethereum — платформа для створення практично будь-яких децентралізованих онлайн-сервісів на базі блокчейна (Dapps), що працюють на базі смарт-контрактів. Реалізована як єдина децентралізована віртуальна машина. Ідея була втілена 30 липня 2015 року. Оскільки Ethereum сильно спрощує і здешевлює впровадження блокчейна, його впроваджують як великі гравці, такі як Microsoft, IBM, Acronis, Сбербанк, банківський консорціум R3, так і нові стартапи [2].

Огляд існуючих підходів до написання смарт-контрактів

У сучасному світі існує декілька підходів до написання смарт-контрактів. Коротко розглянемо кожен із них:

- Bitcoin (Bitcoin-Script) обмежена стекова мова програмування. В ній відсутні цикли I/O операції, дані зберігаються у двох стеках (основний/допоміжний). Bitcoin-Script є низькорівневою мовою програмування. Ведуться розробки, щодо написання транслятора з деякої JavaScript-like, c-like мови програмування у Bitcoin-Script [3].

- Ethereum (Solidity, Serpent, ...). Ethereum має дуже розвинуту систему написання смарт-контрактів. Він має свою віртуальну машину EVM (Ethereum Virtual Machine),

декілька спеціалізованих високорівневих мов програмування (Solidity, Serpent, тощо) які компілюються у байт-код для EVM. На відміну від Bitcoin-Script Solidity надає програмісту можливість працювати з регістровою пам'яттю та інші потужні можливості, але має і деякі обмеження, що були введені в цілях безпеки.

- Останній варіант - надання майже повної свободи у написанні смарт-контрактів. Програмісту надається можливість писати смарт-контракти на Rust, Java, тощо. За для безпеки увесь код смарт-контрактів має бути проаналізований програмістами перед розгортанням [4].

Огляд існуючих вразливостей у середовищах написання смарт-контрактів

- Аналіз mutability-problem у біткойн.
- Аналіз опкодів, у реалізації яких були знайдені вразливості
- Аналіз атак на смарт-контракти, наприклад DAO [5].

Аналіз вихідного коду середовищ виконання смарт-контрактів

- Проаналізувати код BitcoinScript у reference implementation Bitcoin: <https://github.com/bitcoin/bitcoin>.

- Проаналізувати package txscript в імплементації Bitcoin протоколу на мові програмування GoLang <https://github.com/btcsuite/btcd> [6].

- Проаналізувати код Go-Ethereum (<https://github.com/ethereum/go-ethereum>) - імплементації Ethereum протоколу на мові програмування GoLang.

- Проаналізувати специфікацію EVM (Ethereum Virtual Machine) та інших високорівневих мов програмування (Solidity, Serpent, тощо), що компілюються у байт-код для EVM.

- Спробувати застосувати класичні атаки (атаки, що застосовуються для продуктів, що написані на мовах програмування C/C++/Java/C#) на смарт-контракти, що реалізовані на мовах програмування Solidity, Serpent, BitcoinScript тощо [7].

Висновки

На сьогоднішній день можна виділити три основні підходи для написання смарт-контрактів, вони є результатом компромісу між функціональними можливостями і безпекою. В ході роботи ми проаналізуємо ці мови програмування та їх середовище виконання (runtime).

Список використаних джерел:

1. Види криптовалют і їх популярність [Електронний ресурс]. — Режим доступу: <https://pingblockchain.com/vidi-kriptoaljut-i-ih-populjarnist/>
2. H. Massias, X.S. Avila, and J.-J. Quisquater, "Design of a secure timestamping service with minimal trust requirements," In 20th Symposium on Information Theory in the Benelux, May 1999.
3. S. Haber, W.S. Stornetta, "Secure names for bit-strings," In Proceedings of the 4th ACM Conference on Computer and Communications Security, pages 28-35, April 1997
4. R.C. Merkle, "Protocols for public key cryptosystems," In Proc. 1980 Symposium on Security and Privacy, IEEE Computer Society, pages 122-133.
5. W. Feller, "An introduction to probability theory and its applications," 1957
6. A. Back, "Hashcash - a denial of service counter-measure," <http://www.hashcash.org/papers/hashcash.pdf>, 2002.
7. D. Bayer, S. Haber, W.S. Stornetta, "Improving the efficiency and reliability of digital time-stamping," In Sequences II: Methods in Communication, Security and Computer Science, pages 329-334, 1993

ІНТЕЛЕКТУАЛЬНИЙ МОДУЛЬ СИНХРОНІЗАЦІЇ ДАНИХ В РЕЖИМІ РЕАЛЬНОГО ЧАСУ

Михайлюк Лілія, Сілагін Олексій

Вінницький національний технічний університет

Анотація

Розглянуто актуальність задачі синхронізації даних в реальному часі. Розглянуто алгоритми синхронізації даних в реальному часі та запропоновано використання оптимістичного алгоритму.

Abstract

The relevance of the data synchronization problem in real time is considered. The algorithms of data synchronization in real time are considered, and the use of optimistic algorithm is proposed.

Вступ

Задача синхронізації даних є актуальною у зв'язку з інтенсивним розвитком цифрових технологій. З поширенням гаджетів, дана задача все частіше виникає перед пересічними користувачами, що збільшує попит на технології, що пов'язані з передачею даних.

Зі збільшенням кількості мобільних користувачів мережі з'явилася необхідність в обміні інформацією та в оперативному отриманні даних ними.

Огляд існуючих методів

Традиційно використовуються два підходи до реалізації алгоритму синхронізації об'єктів моделювання, розподілених по різних обчислювальним вузлам: консервативний і оптимістичний. Основною метою цих алгоритмів є забезпечення виконання кожним логічним процесом подій в порядку не спадання їх тимчасових міток, щоб зберегти причинно-наслідкові зв'язки.

Алгоритми синхронізації створюють упорядкування подій. Алгоритми синхронізації можна розділити на консервативні (conservative) і оптимістичні (optimistic)[1].

Кожен з цих алгоритмів має свої недоліки, наприклад: консервативний алгоритм є досить ресурсо- і часозатратним. Адже для синхронізації масивів даних, що постійно надходять, може бути затрачено досить багато часу, бо працює по протоколу «зупинися-і-чекай». Оптимістичний алгоритм дозволяє оновлювати дані дискретно. Оскільки, DeadReckoning, є найяскравішим та найрозповсюдженішим прикладом даного алгоритму. Його було обрано як основу для обробки даних в процесі синхронізації.

Консервативний алгоритм

Принципове завдання консервативного алгоритму - визначити час, коли обробка чергового події зі списку необроблених подій є «безпечним». Подія є безпечною, якщо можна гарантувати, що процес надалі не отримає від інших процесів повідомлення з меншою часовою міткою. Консервативний підхід не дозволяє обробляти подію до тих пір, поки не переконається в його безпеці. На відміну від консервативних алгоритмів, що не допускають порушення обмеження локальної каузальності, оптимістичні методи не накладають такого обмеження. Вони забезпечують відновлення правильного порядку при його порушенні.

Оптимістичний алгоритм

Загалом можна сказати, що оптимістичний алгоритм є методом синхронізації даних в режимі реального часу. Коли логічний процес отримує подію, що має тимчасову позначку меншу, ніж вже оброблені події, він виконує відкат і обробляє ці події повторно в хронологічному порядку. Відкочуючись назад, процес відновлює стан, який був до обробки подій (їхні капітали системи зберігаються) і відмовляється від повідомлень, відправлених в результаті обробки подій, які необхідно скасувати в результаті відкату.

Таким методом є DeadReckoning (DR). Він полягає в обчисленні траєкторії об'єкта (у вигляді швидкості і положення в просторі), ґрунтуючись на відомій раніше траєкторії, швидкості і часу, коли відома траєкторія була актуальною.[3]

В DeadReckoning пересування є безперервним, але його можливо оновлювати тільки дискретно. До того ж завжди існує затримка і одержувані дані є застарілими. Отже, необхідний спосіб побудови безперервної траєкторії з дискретних оновлень і передбачення майбутньої траєкторії. DeadReckoning дозволяє передбачати траєкторії об'єктів, таким чином приховуючи затримку сигналу.

Як алгоритм синхронізації, DeadReckoning – це поєднання передачі та передбачення стану. Іншими словами, кожен вузол обмінюється з іншими вузлами даними про траєкторії первинних копій і передбачає траєкторії вторинних. У централізованій архітектурі сервер виробляє передачу стану, а клієнти - передбачення.

Дані про траєкторію можуть передаватися або в кожному повідомленні, або по перевищенню порога помилки, залежно від передбачуваності траєкторії. Передбачення може бути засноване на інтерполяції або екстраполяції, залежно від необхідної точності. Під точністю розуміється точність відтворення траєкторії. Наприклад, лінійна інтерполяція забезпечує згладжену, але неточну траєкторію. Особливо це помітно, коли траєкторія змінюється хаотично[4].

Висновки

Для синхронізації даних в реальному часі доцільним є оптимістичний алгоритм. Метою дослідження є розробка інтелектуального модулю синхронізації даних за методом DeadReckoning, з урахуванням всіх принципів, на яких заснований даний метод.

Для подальших досліджень потрібно провести відповідні модифікації класичного методу для підвищення точності та ефективності розпізнавання в різних умовах.

Список використаних джерел:

1. L. Naimark and E. Foxlin. Circular data matrix fiducial system and robust image processing for a wearable vision-inertial self-tracker. In ISMAR 2002: IEEE / ACM International Symposium on Mixed and Augmented Reality, Darmstadt, Germany, Sept.
2. ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ІМІТАЦІЙНОГО МОДЕЛЮВАННЯ [Електронний ресурс]. – Електрон. дан. – http://dn.khnu.km.ua/dn/k_default.aspx?M=k0548&T=06&lng=1&st=0
3. Контроль і управління в складних системах (КУСС-2014). XII Міжнародна конференція. Тези доповідей. Вінниця, 14-16 жовтня 2014 року. — Вінниця: ВНТУ, 2014. — 222с.
4. Kryvyy R. Orthogonal placement of different overall components in plane / Rostyslav Kryvyy, Maryan Lobur, Sergiy Tkatchenko // Proc. of the X-th International Conference TCSET. — Lviv-Slavske, 2010. — P.329.

ПЕРСПЕКТИВИ ВИКОРИСТАННЯ ТЕХНОЛОГІЇ БЛОКЧЕЙН

Білик Руслан, Сілагін Олексій

Вінницький національний технічний університет

Анотація

У статті розглянуто технологію блокчейн як інноваційного інструменту. Зокрема, визначено сутність та передумови розвитку блокчейн, принципи та специфіку функціонування системи, а також схему її роботи. Особливу увагу приділено дослідженню проблеми безпеки і конфіденційності, забезпечуючи новий обчислювальний шар, де дані можуть бути безпечно оброблені та проаналізовані, залишаючись приватним. Розкрито потенційні переваги та виділено проблеми, які потрібно вирішити для ефективного використання цієї технології.

Abstract

The article considers the blockade technology as an innovative tool. In particular, the essence and background of the development of blocks, the principles and specifics of the functioning of the system, as well as the scheme of its work, are determined. Particular attention is paid to the study of security and privacy by providing a new computing layer where data can be safely processed and analyzed while remaining private. The potential advantages are highlighted and the problems that need to be resolved for effective use of this technology are highlighted.

Вступ

Перспективи використання технології блокчейн. Blockchain є новою інформаційною технологією, яка набуває розвитку та використання у багатьох галузях. Першим і найбільш відомим прикладом використання технології Blockchain є криптовалюта – Bitcoin [1]. На цей час криптовалюта перетворилась у визнаний платіжний засіб, віртуальну валюту, яку приймають великі та дрібні підприємства, корпорації та сервіси.

Результати дослідження

На сьогодні ведуть дослідження та здійснюють реалізацію низки проектів з використанням технології Blockchain у таких галузях, як охорона здоров'я, засоби масової інформації, електронне голосування, зберігання файлів, смарт-контракти, страхування, державний сектор (видача паспортів, збір податків, реєстрація земельних ділянок) та ін. [2].

Blockchain – це розподілена структура даних, яка складається з послідовності блоків, в якій кожний блок містить хеш попереднього блоку, утворюючи, як наслідок, ланцюг блоків (рисунок 1). Перший блок у ланцюжку (батьківський блок, genesis block) розглядають як окремий випадок, оскільки в нього відсутній попередній блок. Blockchain працює як розподілена база даних, яка здійснює облік усіх операцій у мережі. Операції мають відзначку часу і зберігаються у блоках, де кожен блок ідентифікується своїм криптографічним хешем. Blockchain повністю зберігається у кожному вузлі мережі. Для роботи Blockchain не потрібно довіри між вузлами мережі, оскільки будь-який вузол може самостійно перевірити, чи збігається його копія бази з копіями, які зберігаються в інших вузлах [3].

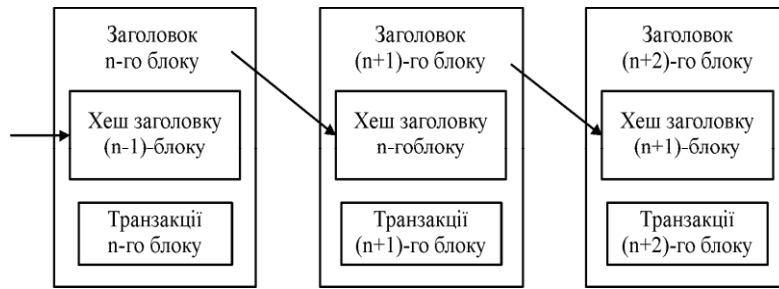


Рисунок 1 – Спрощена послідовність блоків

Принцип функціонування технології Blockchain розглянемо на прикладі криптовалюти "біткойн". Як хеш-функцію криптовалюта біткойн використовує криптографічну хеш-функцію SHA-256 [4]. Для перевірки цілісності даних у блоці використовується деревоподібне хешування (дерево Меркле), яке представляє особливу структуру даних, що містить інформацію про здійснені транзакції. Для цього з кожної транзакції обчислюється хеш, а потім з кожної пари хешів обчислюється новий хеш пари. Ця процедура повторюється доти, поки не залишиться один хеш. Якщо пара в хешу відсутня, то він переноситься на новий рівень без змін (рисунок 2).

Групу транзакцій після перевірки записують у спеціальний блок (рисунок 2). Блок складається із заголовка та списку транзакцій (Tr A, Tr B, ...). Заголовок блоку включає хеш даного блоку, хеш попереднього блоку (Previous Hash), хеш транзакцій (Merkle Root) та додаткову службову інформацію (Nonce, Timestamp). Відзначка про час (Timestamp) вказує, коли був створений блок, і надає докази того, що дані в блоці існували в певний момент часу.

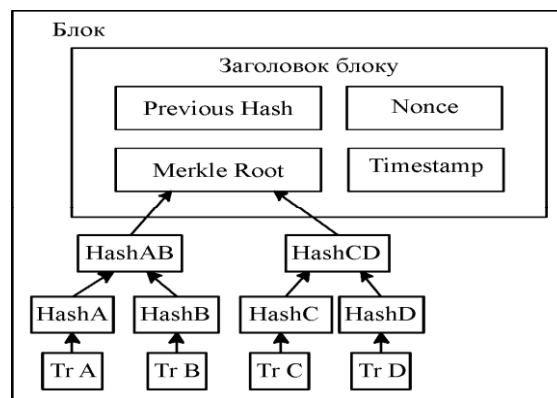


Рисунок 2 – Структура блоку

Для формування нового блоку вузла потрібні дані: хеш попереднього блоку в ланцюжку; хеш Merkle для операцій, які потрібно помістити у блок; час (Timestamp) та одноразовий код (Nonce), вибраний псевдовипадковим чином.

Для підтвердження коректності блоку потрібно обчислити хеш заголовка нового блоку, який повинен починатися із заданої кількості нулів. Дана задача відома, як доказ правильності роботи (proof-of-work), що базується на двох принципах: 1) зробити підтвердження транзакцій затратними для користувачів мережі у вигляді комп'ютерних обчислень; 2) здійснювати винагороду за допомогу у перевірці транзакцій.

Новий блок приймається іншими вузлами мережі, якщо значення хешу заголовка дорівнює або менше заданого числа, величина якого періодично змінюється. Коли результат знайдено, сформований блок розсилається іншим вузлам, які його перевіряють. Якщо перевірка пройшла успішно, то блок додається в ланцюжок і наступний блок повинен включати в себе його хеш.

Робота, яку вузли повинні виконати для створення нового блоку, вимагає багато часу та обчислювальних ресурсів. Це знижує ймовірність того, що два блоки будуть зроблені одночасно, але така ситуація все-таки можлива. Коли це відбувається, то створюється розгалуження в Blockchain. У такому випадку вузли можуть почати будувати ланцюг на різних гілках.

Обчислювальна складність перевірки транзакцій допомагає уникнути залежності від кількості вузлів у мережі, які може контролювати зловмисник. Отже, на перевірку впливає тільки загальна обчислювальна потужність вузлів. Отже, для зміни інформації в блоці зловмиснику потрібні значні обчислювальні ресурси, що робить це практично недоцільним.

Оскільки копії Blockchain зберігаються у вузлах розподіленої мережі, це робить технологію Blockchain стійкою до проблем з тимчасовим або постійним відключенням вузлів, пов'язаним із збоями обладнання або зв'язку, а також підключенням нових вузлів.

Переваги технології **Blockchain**. Переваги технології Blockchain, які забезпечують її ефективне використання у середовищі Інтернет речей [2-3]:

- 1)Blockchain є публічною розподіленою базою всіх транзакцій у мережі, яка підтримується одноранговою мережею;
- 2)мережа Blockchain стійка до збоїв, оскільки вона функціонує без єдиної точки відмови;
- 3)Blockchain є незмінною і довговічною розподіленою базою і, як тільки транзакції записані в Blockchain, вони не можуть бути змінені або видалені;
- 4)мережа Blockchain має високий ступінь масштабованості;
- 5)усі транзакції в мережі Blockchain захищені криптографічними методами;
- 6)Blockchain дає змогу пристроям здійснювати операції автономно без довіреної сторони.

Технологія Blockchain пропонує рішення проблеми безпеки і конфіденційності у середовищі Інтернет речей, забезпечуючи новий обчислювальний шар, де дані можуть бути безпечно оброблені та проаналізовані, залишаючись приватним.

Висновки

Blockchain є відносно новою концепцією з високим потенціалом, відповідно потребує додаткових досліджень для її ефективного застосування у нових галузях, таких як кіберфізичні системи та Інтернет речей

Список використаних джерел:

1. Ashton K. That Internet of Things / K. Ashton // Thing. RFID Journal, 22 July 2009. [Electronic resource]. – Mode of access <http://www.rfidjournal.com/articles/view?4986>.
- 2.Dorri, Ali. Kanhere, and Raja Jurdak / Ali Dorri, S. Salil // Blockchain in internet of things: Challenges and Solutions" *arXiv preprint arXiv:1608.05187*, 2016.
- 3.Shancang Li. The internet of things: a survey / Li Shancang, Li Da Xu, and Shanshan Zhao // Information Systems Frontiers 2015, 17.2. – Pp. 243-259.
- 4.Whitmore Andrew. The Internet of Things – A survey of topics and trends / Whitmore Andrew, Anurag Agarwal, and Li Da Xu // Information Systems Frontiers 17.2, 2015. – Pp. 261-274.

УДК 003.26.09

ПОБУДОВА АТАК НА КРИПТОСИСТЕМУ AJPS З ВИКОРИСТАННЯМ МОДЕЛІ АКТИВНОГО ЗЛОВМИСНИКА

Ядуха Дарія, Фесенко Андрій

Національний технічний університет України «Київський політехнічний інститут ім. Ігоря Сікорського»,
Фізико-технічний інститут

Анотація

Д. Агарвал та інші нещодавно запропонували нову потенційно постквантову асиметричну криптосистему AJPS, яка використовує операції за модулем числа Мерсенна. У даній роботі побудовано атаки на криптосистему AJPS, а саме атаки підміни та імітації активним криптоаналітиком.

Abstract

D. Aggarwal and other recently introduced a new potentially postquantum public-key cryptosystem based on operations by modulus of the Mersenne number. This paper describes the attacks on AJPS cryptosystem, namely the attacks of substitution and simulation by an active cryptanalyst.

Вступ

Асиметричні криптосистеми або криптосистеми з відкритим ключем - це ефективні системи криптографічного захисту даних, у яких для зашифрування даних використовують один ключ - відкритий (публічний), а для розшифрування - інший (особистий). Оскільки стійкість більшості асиметричних криптосистем ґрунтується на складності задач, розв'язування яких може значно швидше виконати квантовий комп'ютер, то є мотивація створювати криптосистеми з відкритим ключем, які будуть стійкими до атак з використанням квантового комп'ютера. Національний інститут стандартів і технологій (NIST) оголосив конкурс постквантових криптографічних алгоритмів з відкритим ключем [4], заявки на участь у якому приймали до 30 листопада 2017 року. Одним із запропонованих примітивів і є криптосистема AJPS [1]. Основною задачею даної роботи є аналіз запропонованої криптосистеми та побудова атак на неї за моделі активного зловмисника.

Опис криптосистеми AJPS

Розглянемо криптосистему AJPS [1]: нехай є відкриті параметри $M_n = 2^n - 1$ - число Мерсенна, α - параметр захищеності, заданий під час побудови криптосистеми, і h - фіксоване значення, яке задовільняє умовам $4h^2 < n$ та $C_{n-1}^{h-1} \geq 2^\alpha$. Позначимо функцію знаходження ваги Хеммінга як Ham . Нехай $HM_{n,h} = \{x : Ham(x \bmod M_n) = h\}$, тобто $HM_{n,h}$ - множина чисел, які за модулем числа Мерсенна мають вагу Хеммінга h . Числа F та G обираються незалежно та рівноймовірно з множини $HM_{n,h}$. Значення G є особистим ключем отримувача, F - таємний параметр криптосистеми. Відкритий ключ H обчислюється наступним чином: $H = \frac{F}{G} \bmod M_n$.

Криптосистема дозволяє зашифрувати один біт, тобто відкритим текстом є число $b \in \{0,1\}$. Шифротекст C обчислюється за формулою $C = (-1)^b (A \cdot H + B) \bmod M_n$, де A, B - незалежно і рівноймовірно обрані значення з множини $HM_{n,h}$. Для розшифрування спочатку обчислюється значення $d = Ham(C \cdot G \bmod M_n)$, потім біт b знаходиться наступним чином:

$$b = \begin{cases} 0, & \text{якщо } d \leq 2h^2 \\ 1, & \text{якщо } d \geq n - 2h^2 \\ \perp (\text{помилка}), & \text{інакше.} \end{cases}$$

Правильність розшифрування впливає з леми [1]:

Лема 1. Нехай $M_n = 2^n - 1$ та $A, B \in \{0, 1\}^n$, тоді виконуються наступні співвідношення:

1. $\text{Ham}(A + B \pmod{M_n}) \leq \text{Ham}(A) + \text{Ham}(B)$;
2. $\text{Ham}(A \cdot B \pmod{M_n}) \leq \text{Ham}(A) \cdot \text{Ham}(B)$;
3. Якщо $A \neq 0^n$, то $\text{Ham}(-A \pmod{M_n}) = n - \text{Ham}(A)$.

Стійкість криптосистеми AJPS ґрунтується на складності задачі ділення чисел з малою вагою Хеммінга за модулем числа Мерсенна (задача MLHRSP) [1]. Також були спроби застосувати відомі види атак, наприклад, «зустріч посередині», «вгадай і виграй» [1] та інші побудовані атаки, наприклад, «розділи та спробуй» [2] – проведені атаки показали те, що криптосистема є стійкою за умови збільшення параметру захищеності [2].

Побудова атак на криптосистему активним криптоаналітиком

Активний криптоаналітик може не лише переглядати усі шифротексти, які передаються відкритим каналом зв'язку, а також, при успішній атаці, може змінювати або підмінювати шифротекст так, що отримувач не помітить підміни. Далі розглянемо наступні атаки на криптосистему AJPS.

Твердження 1. Атака підміни з незмінним відкритим текстом є успішною для криптосистеми AJPS: маючи у розпорядженні один шифротекст C , зловмисник може обчислити шифротексти, що будуть відповідати тому ж відкритому тексту наступним чином: $C^* = C \cdot 2^z$ для довільного значення $z \in \mathbb{N}$.

Доведення. Дана атака полягає у тому, що криптоаналітик деяким чином перетворює перехвачений текст так, що при розшифруванні отримувач має той ж біт, який і мав отримати, навіть якщо криптоаналітик не втрутився. Таким чином, криптоаналітик не знає відкритий текст і не отримує про нього ніякої інформації під час атаки. Така атака матиме наступний вигляд: нехай C - справжній шифротекст і значення, яке мав би знаходити отримувач при розшифруванні: $d = \text{Ham}(C \cdot G \pmod{M_n})$. Позначимо C^* модифікований шифротекст, тоді значення, яке після успішної атаки буде знаходити отримувач для розшифрування: $d^* = \text{Ham}(C^* \cdot G \pmod{M_n})$. Нехай криптоаналітик перехватив шифротекст C . Тоді він обчислює $C^* = C \cdot 2^z$, $z \in \mathbb{N}$ і відправляє його одержувачу. Одержувач обчислює наступне:

$$d^* = \text{Ham}(C^* \cdot G \pmod{M_n}) = \text{Ham}(C \cdot 2^z \cdot G \pmod{M_n}) = \text{Ham}((C \cdot G) \cdot 2^z \pmod{M_n}).$$

Далі використовуємо відому властивість для чисел Мерсенна - множення на степінь двійки за модулем числа Мерсенна є циклічним зсувом числа [3]. Тоді у даному випадку отримуємо значення зсуву $C \cdot G$ на z позицій. А оскільки циклічний зсув ніяк не впливає на вагу Хеммінга числа, то маємо: $\text{Ham}((C \cdot G) \cdot 2^z \pmod{M_n}) = \text{Ham}(C \cdot G \pmod{M_n}) = d$. Таким чином, отримувач правильно розшифрує модифікований шифротекст.

Розглянута атака не надає можливості криптоаналітику отримати інформацію про відкритий текст або ключ та не спотворює повідомлення відправника, але якщо властивості шифротексту мають цінність, то описане твердження може бути використане із зловмисною метою.

Твердження 2. Атака імітації з обраним криптоаналітиком фіксованим відкритим текстом успішна для криптосистеми AJPS: незалежно від особистого ключа, якщо криптоаналітик відправить повідомлення C_1 таке, що $\text{Ham}(C_1 \bmod M_n) \leq 2h$, то отримувач розшифрує його як біт 0, та якщо відправить $C_2 = -C_1 \bmod M_n$, то отримувач при розшифруванні отримає біт 1.

Доведення. Дана атака заключається у тому, що криптоаналітик може відправляти деякі шифротексти отримувачу, причому знаючи, що саме отримає при розшифруванні отримувач. Тобто криптоаналітик сам обирає шифротекст так, щоб отримувач при розшифруванні отримав вигідний для криптоаналітика відкритий текст. Розглянемо два випадки: коли криптоаналітику потрібно, щоб отримувач при розшифруванні отримав біт $b=0$ та коли $b=1$.

1. Випадок $b=0$: криптоаналітик обирає довільний такий шифротекст C_1 , для якого виконується умова $\text{Ham}(C_1 \bmod M_n) \leq 2h$ та відправляє його. Тоді при розшифруванні отримувач має $d = \text{Ham}(C_1 \cdot G \bmod M_n)$ і, використовуючи лему 1, маємо:

$$d = \text{Ham}(C_1 \cdot G \bmod M_n) \leq \text{Ham}(C_1 \bmod M_n) \cdot \text{Ham}(G) = \text{Ham}(C_1 \bmod M_n) \cdot h \leq 2h^2$$

Оскільки $d \leq 2h^2$, то $b=0$.

2. Випадок $b=1$: криптоаналітик обирає шифротекст $C_2 = -C_1 \bmod M_n$, де C_1 - шифротекст з пункту 1, задовольняючий наведеним вище умовам, та відправляє його отримувачу. Тоді при розшифруванні маємо:

$$d = \text{Ham}(C_2 \cdot G \bmod M_n) = \text{Ham}(-C_1 \cdot G \bmod M_n) = n - \text{Ham}(C_1 \cdot G \bmod M_n) \geq n - 2h^2$$

Оскільки $d \geq n - 2h^2$, то $b=1$.

Отже, криптоаналітик, не знаючи особистий ключ, може відправляти шифротексти з обраним значенням біту.

Висновки

У даній роботі розглянуто побудовану нещодавно асиметричну криптосистему AJPS, одного з учасників конкурсу NIST для постквантових криптопримітивів. На відміну від більшості постквантових криптографічних алгоритмів, система AJPS використовує обчислення в кільці лишків. У роботі побудовано ефективні атаки підміни та імітації, які можуть бути використані при активній моделі зловмисника.

Список використаних джерел:

1. Divesh Aggarwal, Antoine Joux, Anupam Prakash, Miklos Santha. A New Public-Key Cryptosystem via Mersenne Numbers [Електронний ресурс]. — Режим доступу: <https://eprint.iacr.org/2017/481>.
2. Marc Beunardeau, Aisling Connolly, R'emi G'eraud, David Naccache. On the Hardness of the Mersenne Low Hamming Ratio Assumption. [Електронний ресурс]. — Режим доступу: <https://eprint.iacr.org/2017/522>.
3. Joppe W. Bos, Thorsten Kleinjung, Arjen K. Lenstra. Efficient SIMD arithmetic modulo a Mersenne number. [Електронний ресурс]. — Режим доступу: <https://eprint.iacr.org/2010/338>.
4. Post-Quantum cryptography standardization NIST [Електронний ресурс]. — Режим доступу: <https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization>

МОЩНЫЕ ФРАКТАЛЬНЫЕ МАТРИЧНЫЕ МНОЖЕСТВА ДЛЯ РЕАЛИЗАЦИИ И СТОЙКОСТИ КРИПТОГРАФИЧЕСКОГО АЛГОРИТМА

Шенгелия София

Сухумский государственный университет

Аннотация

Целью работы является создание мощных матричных множеств высокого порядка для реализации алгоритма обмена ключами по открытому каналу связи. Эта задача связана с глобальной проблемой, поскольку нет другой односторонней функции (известной и признанной), которая имеет высокую эффективность по сравнению с односторонними функциями, используемыми в асимметричных алгоритмах Диффи – Хеллмана и RSA.

Abstract

The goal of the work is to construct a set of high order strong matrixes for an open channel key exchange matrix algorithm and create a quick one-way matrix function. This issue concerns a global problem as nowadays there is no other one-way function (known and recognized), which is quicker compared to the one-way functions used in Diffie-Hellman and RSA asymmetric algorithms.

Введение

Алгоритм представляет собой оригинальный криптографический подход, особенно надо отметить его быстродействие. Для стойкости и реализации криптографического алгоритма предлагаются мощные фрактальные матричные множества [1-5].

Алгоритм обмена ключами по открытому каналу связи

Для реализации однонаправленной матричной функции задается матрица $A(n \times n)$. Для простоты изложения, матрицы рассматриваются над полем $GF(2)$. Матрица A представляет собой секретный параметр, выбранный случайным образом из множества $\hat{A}$ высокой мощности; т.е. $A \in \hat{A}$, $v \in V_n$, где V_n - векторное пространство над $GF(2)$ (v - открытый параметр). Тогда, однонаправленная матричная функция имеет следующий вид:

$$vA = u; \quad (1)$$

где

$u \in V_n$ и u – также открытый параметр.

Матричный алгоритм обмена ключами по открытому каналу осуществляется следующим образом:

- Алиса (случайно) выбирает матрицу $A_1(n \times n) \in \hat{A}$ и посылает Бобу вектор $u_1 = vA_1$, (2)

- Боб (случайно) выбирает матрицу $A_2(n \times n) \in \hat{A}$ и посылает Алисе вектор $u_2 = vA_2$, (3)

где α - n -размерный вектор (открытый), A_1 и A_2 суть (секретные) матричные ключи.

- Алиса вычисляет

$$k_1 = u_2A_1. \quad (4)$$

- Боб вычисляет

$$k_2 = u_1A_2, \quad (5)$$

где k_1 и k_2 секретные ключи. $k_1 = k_2 = k$ потому, что $k = vA_1A_2 = vA_2A_1$.

Построение исходных матриц размерности $(n \times n)$

Исследования были проведены с использованием программного обеспечения. Мы изучили мощные матричные множества размерности $n=400$ (400×400).

Порядок e , для всех матриц, равен числу Мерсенна или максимально достигаемому значению (размерность матрицы n , максимальное значение $e = 2^n - 1$). Исследования были проведены для фрактальных матричных структур (см. рис.1). Для каждой размерности $n > 1$ исходная матрица ($n \times n$) должна генерировать либо максимальное число матриц ($2^n - 1$), либо количество матриц, равное числу Мерсенна, т.е. $2^j - 1$, где $j < n$.

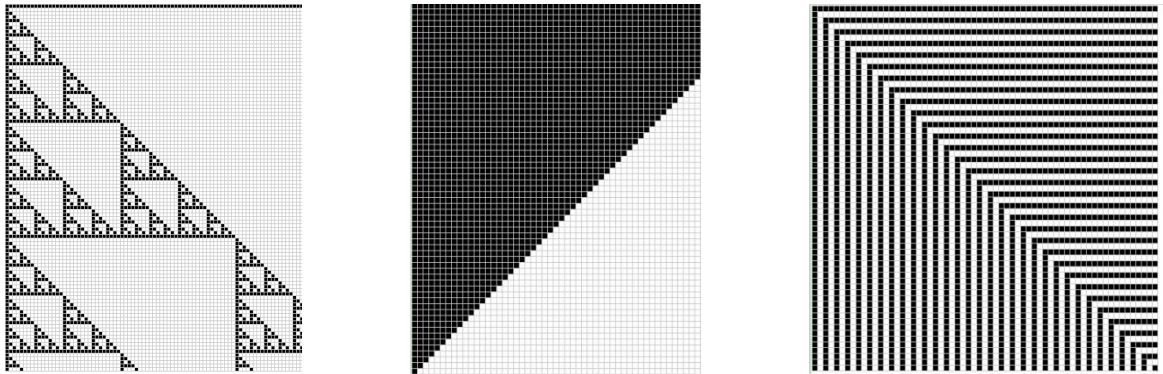


Рисунок 1 – Фрактальные структуры

Матричные структуры:

$$A = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 \end{pmatrix} \quad B = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix} \quad C = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 \end{pmatrix} \quad (6)$$

Список использованных источников:

1. R.Megrelishvili, M. Chelidze, K. Chelidze, On the construction of secret and public-key cryptosystems, Iv. Javakhishvili Tbilisi State University I.Vekua Institute of Applied Mathematics, Applied Mathematics, Informatics and Mechanics, AMIM, v.11, N2, 2006, pp. 29-36.
2. Мегрелишвили Р.П., Челидзе М.А., Бесиашвили Г.М., Джинджихадзе М.В., Построение новой однонаправленной матричной функции и ее применение в криптографии, Оптико-электронные информационно-энергетические технологии, N2 (20), 2010, с. 67-71.
3. Мегрелишвили Р., Шенгелия С.; “Оригинальная матричная однонаправленная функция и вопросы ее реализации”, System Analysis and information technologies ,Conference SAIT 2013, Ukraine, Kyiv, cc. 465-466, 2013.
4. Мегрелишвили Р., Шенгелия С.; “Фрактальные матрицы в криптографии”, System Analysis and information technologies ,Conference SAIT 2014, Ukraine, Kyiv, cc. 418-419, 2014.
5. Мегрелишвили Р., Шенгелия С., Исследование и синтез матричных структур, System Analysis and information technologies ,Conference SAIT 2017, Ukraine, Kyiv, cc. 301-302, 2017.

ПРИНЦИП ВИБОРУ ОКУЛЯРІВ ВІРТУАЛЬНОЇ РЕАЛЬНОСТІ ПРИ РОЗРОБЦІ ПРОГРАМНИХ ЗАСОБІВ

Суприган Олена, Маркіна Ірина

Вінницький національний технічний університет

Анотація

В ході проведення досліджень були визначені актуальність і ефективність застосування тих чи інших окулярів віртуальної реальності для розробки програмних засобів. Був проведений аналіз наявних технологій і їх порівняння. На основі проведених даних було отримано оптимальний пристрій для використання.

Abstract

During the research, the relevance and effectiveness of using certain head-mounted display for the development of programs with virtual reality technologies was determined. An analysis of existing technologies and their comparison was carried out. Based on the received data, an optimal device for use was obtained.

Вступ

Для найкращого відображення деталізації середовища, важливим є не тільки апаратне забезпечення самого комп'ютера, а й якість дисплею окулярів та його характеристики. Щоб людський мозок сприймав віртуальне середовище більш реальним, властивості окулярів повинні бути доволі високими, а сама гарнітура має охоплювати декілька органів відчуттів. Це забезпечується різними технологіями у самих окулярах віртуальної реальності. Дисплей і лінзи відповідають за відображення навколишнього простору, фокусуючи зображення з екрану/смартфона. Оснащення окулярів просторовими датчиками забезпечує відслідковування користувача у просторі. Серед них: акселерометр, який використовується для визначення швидкості руху та гіроскоп, який забезпечує отримання даних про зміну орієнтації у просторі [1].

Результати дослідження

Насамперед розглядається платформа під яку призначений пристрій та тип його дисплею. Для самого дисплею важливою характеристикою є роздільна здатність – визначає кількість пікселів на одиницю площі і чим більше вона, тим кращою буде деталізація навколишнього середовища, що є вкрай важливим. У випадку гарнітур віртуальної реальності число пікселів по горизонталі ділиться навпіл, оскільки зображення виводиться на дві частини дисплею для обох очей. Для динамічних ігор, наприклад шутерів, важлива частота оновлення – характеристика, яка визначає кількість оновлень зображення за секунду і чим вона більша, тим більше разів оновиться зображення. Оскільки у віртуальному просторі можна оглядати простір навколо себе на 360° при повороті голови у гарнітурі, то кут огляду дозволяє користувачу використовувати периферійний зір, коли він дивиться прямо, що посилює занурення у віртуальну реальність. І чи не найбільш істотно на відображення простору впливає час відгуку самого пристрою. При великому значенні цього параметру може виникати мерехтіння, що буде заважати при використанні гарнітури. Основні характеристики окулярів віртуальної реальності наведені у таблиці 1. При виборі основної гарнітури для розробки програмних засобів найважливішими характеристиками будуть, насамперед, роздільна здатність і час відгуку. На їх основі віддаватиметься пріоритет тому чи іншому пристрою. Вже після цього слід приймати до уваги частоту оновлення, а лише вкінці кут огляду.

Таблиця 1 – Порівняльна таблиця основних характеристик окулярів

Пристрій	Тип дисплею	Роздільна здатність	Частота оновлення	Кут огляду	Час відгуку
HTC Vive Pro	Dual AMOLED	2800 × 1600	90 Гц	110°	2 мс
Pimax	CLPL	3840 × 2160	90 Гц	200°	15 мс
Oculus Rift	OLED	2160 × 1200	95 Гц	110°	1 мс

Спочатку розглянемо роздільну здатність та час відгуку для кожного приладу. За результатами цих двох характеристик можна сказати, що хоч Pimax має і максимальну з представлених гарнітур роздільну здатність, проте має і доволі великий час відгуку, тому оптимальними приладами будуть HTC Vive Pro та Oculus Rift. Частота оновлення серед усіх трохи більша у Oculus Rift. За кутом огляду однозначно виграє Pimax.

Пропонується звернути увагу і на середовище розробки програмних засобів або ігор, де можливе використання технологій віртуальної реальності, серед яких основними є Unity та Unreal Engine 4. Після детальнішого знайомства із ними можна сказати, що в них вже є спеціальні бібліотеки та сценарії, які полегшують розробку саме під потрібні пристрої, в тому числі під HTC Vive Pro та Oculus Rift. Окрім цього враховуються і їх особливості на кшталт властивостей датчиків відслідковування або контролерів.

Не менш важливим є і дослідження кількості користувачів, які використовують той чи інший прилад. Ринок гарнітур віртуальної реальності ділять між собою Oculus Rift та HTC Vive Pro. Число користувачів Oculus Rift в серпні 2017 року збільшилось на 8,1 відсотка – і тепер становить 43,8 відсотка. Лідером залишається компанія HTC зі своєю гарнітурою віртуальної реальності Vive. Число користувачів скоротилося на 7,7 відсотка, хоча все ще становить 52,3 відсотка [2].

Отже можна сказати, що при розробці програмних засобів доцільно використовувати одну з двох гарнітур, що є лідерами ринку – Oculus Rift та HTC Vive Pro, які сумарно мають 96,1% користувачів та одночасно мають в сукупності високі характеристики. Однак гарнітура Pimax зовсім недавно введена в експлуатацію, хоча вона і має високі роздільну здатність та кут огляду, тому в перспективі має шанси на збільшення кількості користувачів, які використовують цей прилад.

Висновки

Були проведені дослідження і аналіз ефективності використання окулярів віртуальної реальності як основного пристрою, для якого буде розроблятися програмний засіб. Результати говорять про необхідність використання окулярів з найменшим часом відгуку разом з максимально можливою роздільною здатністю для кожного ока та з максимальною частотою оновлення для найкращих результатів відображення графіки. За результатами аналізу можна виділити два напрямки при використанні гарнітур для розробки програмних засобів: саме у цей час та в найближчі роки. В першому випадку доцільно використати чи HTC Vive Pro, чи Oculus Rift. В другому – основним пристроєм слід обрати Pimax, слідкуючи за апаратними оновленнями цієї гарнітури.

Список використаних джерел:

1. Steven M. LaValle. Virtual Reality : монографія / S. M. LaValle. – England: Cambridge University Press, 2017. – 380 с.
2. Сурепін С. Користувачі VR-гарнітур платформи Steam [Електронний ресурс]/ Режим доступу: https://life.ru/t/игры/1040913/kolichiestvo_polzovateliei_oculus_rift_v_steam_uvelichilos (дата звернення 26.04.2018)

ВПЛИВ КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ НА ТЕОРІЮ І ПРАКТИКУ МАРКЕТИНГУ В ІНФОРМАЦІЙНОМУ СУСПІЛЬСТВІ

Корчинська Олена

Академія праці, соціальних відносин і туризму

Анотація

Представлений матеріал характеризує зміни, які відбуваються у теорії і практики маркетингу, викликані розвитком інформаційного суспільства і широким застосуванням комп'ютерних технологій.

Обґрунтовується необхідність розглядати Інтернет-маркетинг не як різновид прямих продаж, як це було прийнято в індустріальному суспільстві, а як самостійний напрям економічної діяльності.

Abstract

The presented material characterizes changes in marketing theory and practice caused by development of information society and widely application of computer technologies.

The Internet-marketing is substantiated to be considered not as kind of direct sales but as an independent direction of economic activity.

Постановка проблеми. Зміни, які відбуваються в економіці, викликані появою і розвитком інформаційного суспільства, напряду відображаються у маркетингу, трансформуючи не тільки його форму, а й зміст. Мета даних тез – виявити і охарактеризувати ті зміни, які відбуваються у теорії і практиці маркетингу в зв'язку із широким впровадженням Інтернет-технологій.

Виклад основного матеріалу. Якщо у традиційному маркетингу Інтернет-маркетинг носить фрагментарний характер і розглядається як різновид прямих продаж, то нині, коли і сам ринок і його учасники і методи просування продукції перейшли у віртуальний простір, ситуація кардинально змінюється й Інтернет – маркетинг поступово набуває рис самостійної наукової теорії.

Хоча Інтернет – маркетинг базується на традиційному комплекс-маркетингу («4Р»), що включає товар, ціну, збут і просування, зміст і пріоритетність складових змінюється. На перше місце виходить збутова політика, яка дозволяє зробити товар доступним для максимальної кількості потенційних покупців.

Суб'єкти мережевої економіки використовують Інтернет, в першу чергу, не для комунікацій чи маркетингових досліджень, а розглядають Інтернет як окремий великий ринок, на якому існує низький вхідний бар'єр і рівні конкурентні можливості. Все інше – другорядне.

Відбулися зміни й у відношеннях між продавцем і покупцем, обумовлені тим, що Інтернет - технології дають можливість створити і підтримувати інтерактивні взаємодії учасників каналів товароруху і покупців. Комп'ютерні технології дозволяють автоматизувати збір, обробку й аналіз інформації про ринок, роблять доступним миттєвий зворотній зв'язок при збуті товару.

Торкнулися зміни і цінової політики. Оскільки у мережі Інтернет ні один постачальник не може обмежити доступ покупців до інформації про ціни і конкурентні пропозиції. Ні один посередник не може монополізувати ринок і диктувати умови поставки. Сьогодні покупці вільно обмінюються інформацією про товари між собою у соціальних мережах. Все це створює умови ідеальної конкуренції. Крім того, економія на трансакційних витратах у мережі Інтернет дає інтернет-продавцям значні переваги за ціною порівняно із традиційною торгівлею. Звісно, традиційні інструменти цінової політики (знижки, бонуси, залікові знижки тощо) застосовуються в Інтернет-маркетингу. Проте головна перевага – можливість зниження кінцевої ціни за рахунок скорочення трансакційних витрат.

Зміни відбулися і в товарній політиці. Нині товарна політика в Інтернет-маркетингу будується на визнанні того, що покупцю потрібен не великий асортимент товарів, а конкретний товар з певними характеристиками, який максимально задовольняє його потреби. Тому змінилася задача продавця – не просто пропонувати максимально широкий асортимент товарів, а й враховувати індивідуальні побажання кожного покупця. Покупець йде в Інтернет, щоб швидко й з мінімальними трансакційними витратами знайти «свій товар». Лідером електронних продаж стає не той, хто пропонує багато товарів, а той, хто може запропонувати товар індивідуального попиту.

Розвиток інформаційного суспільства і мережевої економіки значно змінили й характер маркетингових комунікацій. З інструмента інформаційного впливу на цільову аудиторію, вони перетворилися в інструмент діалогу з покупцями й контрагентами. Сьогодні Інтернет-комунікації дозволили зробити ринки збуту безмежними й індивідуально підходити до обслуговування великої кількості клієнтів. З одного боку, в Інтернеті виникли прямі комунікації із цільовою аудиторією й окремими клієнтами. З іншого боку з'явилася можливість автоматизувати ведення маркетингових баз даних й підтримувати індивідуальні контакти з партнерами й клієнтами. В результаті, маркетингові комунікації набули індивідуального характеру й автоматизувалися одночасно.

Важливою особливістю маркетингових комунікацій в мережі Інтернет є те, що покупці завдяки індивідуалізації продаж, стають повноцінними учасниками Інтернет-маркетингу. Вони здатні самостійно утворювати віртуальні співтовариства, напряму взаємодіючи з постачальниками товарів. Наприклад, досить популярним є, коли молоді мами об'єднуються в соціальних мережах для покупки оптових партій дитячих товарів.

Постійні покупці стають частиною віртуальної інфраструктури збуту, джерелом й адресатом комунікацій. Вони самі починають активно займатися інтернет-маркетингом, розповсюджуючи маркетингову інформацію, активно впливаючи на маркетингові рішення продавців.

Таким чином, застосування комп'ютерних технологій в маркетингу веде до значних змін на практиці.

На сьогоднішній день он-лайн покупки здійснює 26 відсотків населення світу, це більше половини користувачів Інтернету [1]. Щорічно зростає обсяг електронної комерції в світі. Так, у 2014 році обсяг світового ринку он-лайн покупок становив 1 трлн. 336 млрд. дол. США, у 2017 році - 2 трлн. 304 млн. За прогнозами у 2018 році обсяг даного ринку зросте до 2842 млрд. дол. США [2].

Серед країн світу за обсягами електронної торгівлі лідером є Китай. У 2016 році там було здійснено он-лайн покупок на суму 766,5 млрд. дол. США (33,7% від світового обсягу). На другому місці – США – 595,1 млрд. дол. США (26,2%), на третьому місці – Великобританія – 174,2 млрд. дол. США (7,7%) [2]. У десятку найбільш активних у сфері електронної торгівлі країн світу входить і Росія, яка знаходиться на десятому місці і на неї припадає 1 відсоток світового обсягу Інтернет-покупок. Загалом на десять країн світу припадає більше 85 % обсягу он-лайн продаж у світі. На інші країни припадає менше 15 %. Серед них і Україна, ринок електронної комерції якої у 2016 році становив лише 5,65 млрд. дол. США [3]. Разом з тим, слід зазначити, що даний ринок розвивається значними темпами, в середньому за останні роки щорічні темпи зростання перевищують 30 %.

Висновки. Таким чином, в інформаційному суспільстві комп'ютерні технології впевнено входять у практику маркетингової діяльності, перетворюючи Інтернет маркетинг із складової маркетингових комунікацій у самостійний, незалежний напрямок економічної діяльності.

Список використаних джерел:

1. Аналітичний звіт “Global B2C E-commerce Report 2016” за даними Ecommerce Foundation, GfK, Asendia, Ingenico, MarketShare, WebHelp: https://www.ecommercewiki.org/wikis/www.ecommercewiki.org/images/5/56/Global_B2C_Ecommerce_Report_2016.pdf
2. Аналітичний звіт “Retail e-commerce sales worldwide from 2014 to 2020 (in billion U.S. dollars)” міжнародного маркетингового агентства Statista (Нью-Йорк): <https://www.statista.com/statistics/379046/worldwide-retail-e-commerce-sales/>
3. Електронная коммерция (e-Commerce): тренды и прогноз развития в Украине на 2017-2018 гг.: <https://www.web-mashina.com/web-blog/ecommerce-prognoz-elektronnoy-kommercii-ukrainy-2017-2018>

ОБГРУНТУВАННЯ ДОЦІЛЬНОСТІ ВИКОРИСТАННЯ ГЛИБИННОГО НАВЧАННЯ ДЛЯ РОЗВ'ЯЗАННЯ ЗАДАЧІ РОЗПІЗНАВАННЯ НЕПРАВДИВИХ НОВИН

Гранік Михайло, Месюра Володимир

Вінницький національний технічний університет

Анотація

Метою роботи є розгляд аргументів щодо використання глибинного навчання для розв'язання задачі розпізнавання неправдивих новин. Глибинне навчання на поточний момент є «гарячою» темою досліджень у сфері штучного інтелекту, і його застосування для розглянутої задачі є надзвичайно багатообіцяючим.

Abstract

The purpose of this article is to look at the arguments regarding solving fake news problem using deep learning techniques. Deep learning is a hot topic in the world of artificial intelligence right now, and its usage for the problem mentioned above looks very promising.

Вступ

Проблема визначення неправдивих новинних текстів є надзвичайно актуальною. Щоб досягти деяких цілей, інформація у новинах може бути викривлена чи взагалі вигадана. Існує велика кількість електронних сайтів, контентом яких є практично завжди неправдиві новини. Вони навмисно публікують вигадані факти, елементи пропаганди та дезінформації під виглядом справжніх новин — часто із використанням соціальних мереж з метою підвищення трафіку та збільшення бажаного ефекту. Основна ціль таких сайтів — вплив на публічну думку з деяких аспектів життя (найчастіше за все — політичних). Такі веб сайти існують в Україні, Сполучених Штатах Америки, Німеччині, Китаї і великій кількості інших країн. Отже, неправдиві новини є глобальною проблемою, і в той же час — глобальним викликом [1].

Глибинне навчання

Глибинне навчання — це галузь машинного навчання, що ґрунтується на наборі алгоритмів, які намагаються моделювати високорівневі абстракції в даних, застосовуючи глибинний граф із декількома обробними шарами, що побудовано з кількох лінійних або нелінійних перетворень.

Глибинне навчання є частиною ширшого сімейства методів машинного навчання, що ґрунтуються на навчанні ознак даних. Спостереження (наприклад, зображення) може бути представлено багатьма способами, такими як вектор значень яскравості для пікселів, або абстрактнішим способом, як множина кромek, областей певної форми тощо. Деякі представлення є кращими за інші у спрощенні задачі навчання (наприклад, розпізнаванню облич, або виразів облич). Однією з обіцянок глибинного навчання є заміна ознак ручної роботи дієвими алгоритмами автоматичного або напівавтоматичного навчання ознак та ієрархічного виділення ознак.

Різні архітектури глибинного навчання, такі як глибинні нейронні мережі, згорткові глибинні нейронні мережі, глибинні мережі переконань та рекурентні нейронні мережі застосовувалися в таких областях, як комп'ютерне бачення, автоматичне розпізнавання мовлення, обробка природної мови, розпізнавання звуків та біоінформатика, де вони, як було показано, представляють передові результати в різноманітних задачах.

Алгоритми глибинного навчання перетворюють свої входи крізь більшу кількість шарів, ніж алгоритми поверхневого навчання. На кожному шарі сигнал перетворюється

блоком обробки, таким як штучний нейрон, параметри якого «навчаються» шляхом тренування. Ланцюг перетворень від входу до виходу є шляхом передачі довіри. Шлях передачі довіри описують потенційно причинні зв'язки між входом та виходом, і можуть мати змінну довжину. Для нейронної мережі прямого поширення довжина шляхів передачі довіри, і відтак глибина цієї мережі, є числом прихованих шарів плюс один (вихідний шар також параметризовано). Для рекурентних нейронних мереж, в яких сигнал може поширюватися через якийсь шар більше одного разу, шлях передачі довіри має потенційно необмежену довжину. Універсально узгодженого порогу глибини, що відділяв би поверхнєве навчання від глибинного, не існує, але більшість дослідників у цій галузі погоджуються, що глибинне навчання має декілька нелінійних шарів [2].

Доцільність використання глибинного навчання для розв'язання задачі розпізнавання неправдивих новин

Слід виділити такі аргументи на користь використання глибинного навчання для розв'язання задачі про визначення неправдивих новин:

- Алгоритми глибинного навчання показують хороші результати на багатьох задачах, що складно піддаються формалізації
- Алгоритми глибинного навчання добре підходять до класифікаційних задач
- Існує велика кількість задач, на яких результати рішень, що використовують глибинне навчання, переважають результати, які показує людина-експерт (у медицині тощо).
- У зв'язку з швидким розвитком апаратного забезпечення з'явилась можливість тренувати великі нейронні мережі, які будуть охоплювати велику кількість особливостей тексту.
- Популярність глибинного навчання привела до появи великої кількості зручних програмних платформ, що дозволяють швидко побудувати модель глибинного навчання та ітеративно покращувати її. Це є значним фактором для покращення точності визначення неправдивих новин [3].

Висновки

Глибинне навчання є надзвичайно перспективною технологією, що розвивається великими темпами та показала свою корисність у великій кількості прикладних задач.

Базуючись на аргументах, зазначених вище, можна зробити висновок про доцільність використання глибинного навчання для визначення неправдивих новин.

Список використаних джерел:

1. Fake news websites. [Електронний ресурс] .— Режим доступу: https://en.wikipedia.org/wiki/Fake_news_website
2. Матеріали курсу Neural networks and Deep Learning компанії DeepLearning.ai [Електронний ресурс] .— Режим доступу до матеріалів: <https://www.coursera.org/specializations/deep-learning#courses>
3. Матеріали курсу Structuring Machine Learning Projects компанії DeepLearning.ai [Електронний ресурс] .— Режим доступу до матеріалів: <https://www.coursera.org/specializations/deep-learning#courses>

DEVELOPING SPEAKING SKILLS USING THE INTERNET RESOURCES (ON THE EXAMPLE OF TED)

Teteruk Svitlana

Академія праці, соціальних відносин і туризму

Анотація

У доповіді акцентується увага на доцільності використання Інтернет-ресурсів, а саме ресурсу Ted Talk з метою поліпшення комунікативних вмінь здобувачів вищої освіти, формування їх професійно орієнтованої комунікативної компетентності, інтенсифікації висловлювання без помітних утруднень.

Аннотация

Доклад акцентирует внимание на целесообразности использования Интернет-ресурсов, а именно Ted Talk с целью улучшения коммуникативных умений студентов, формирования их профессиональной компетенции, интенсификации высказываний на иностранном языке.

According to academic research, linguists have demonstrated that there is not one single best method for everyone in all contexts, and that no one teaching method is inherently superior to the others. Also, it is not always possible – or appropriate – to apply the same methodology to all learners, who have different objectives, environments and learning needs.

It is proved that language is best learned when students are interacting with each other in groups – completing a task or learning a content or resolving real life issues - where their attention is directed towards the language itself, except when a focus on language forms is necessary. Many researchers have called into question on the importance of investigating the impact of cooperative language learning on learners' oral proficiency [1, 2, 3, 5]. To develop learners' oral proficiency, the learner has to overcome a lot of obstacles including:

- lack of interest because the topic may be unknown to a learner;
- tense atmosphere in class;
- the fear of being criticized, losing face because of making mistakes;
- lack of self-confidence and the feeling of frustration and discomfort etc;
- problematic achieving a degree of ease and a natural level of speed and rhythm etc.

Thus, teachers have to provide learners with a method of increasing the opportunities of language use. English teaching and learning have the goal of focusing students so that they are able to use English for communication and as a tool for furthering their studies [3]. Any attempt to cater more for the individual needs of students means a lot of hard work and efforts on the part of teachers in terms of the provision of material and in the general attitude and approach required. To make an option easier, it's worth using Internet resources. L. Ditkovska highlights the importance of involving video-lectures and introducing mass online-courses into classrooms. It helps get proper education, improve qualification or acquire necessary knowledge in the corresponding field and provide free access to any student.[6, C. 17].

From our experience Ted Talk is an excellent aid to self-access language work. TED is a series of informative, educational, inspiring talks that present 'Ideas worth spreading' which can be a good supplement to the topics in the classroom.

Working with this resource students can:

- focus on the structure and delivery of oral presentations;
- raise their linguistic awareness;
- perceive the overall structure of a lecture and recognize from verbal and non-verbal cues when a speaker is moving from one topic to another;
- incorporate skills in note-taking;

- perform differently according to their psychological differences and their cognitive abilities and language learning aptitude;
- improve, not only their listening skills, but also improve their pronunciation, vocabulary, grammar and writing.

It's also important for students to be aware of the characteristics of native-speaker performance in conversation. Different cultures talk about different things in their everyday life and students should develop a sense of cultural awareness and banned subjects, gestures or peculiarities of body language. Listening to Ted Talk gives students the feedback.

According to our experience different skills can be developed using the following activities:

1. prediction of the future talk by its title;
2. guessing the speaker's thoughts before listening another sentence or part;
3. highlighting important differences between written and spoken English while listening or reading transcripts;
4. practicing reproducing different weak sounds or difficult phonemes;
5. guessing the meaning of new words from context (they have transcripts for extra help);
6. analyzing grammar (verb tenses, sequencing words, discourse markers);
7. interviewing the speaker, debates, writing reviews etc. after listening activities

Thus, teachers have to provide learners with a method of increasing the opportunities of language use. The primary role of the teacher is to create the best conditions for learning. The teacher needs to play a number of roles during the lesson. When students have problems in expressing their ideas, the teacher can be involved into the assistance but should be careful not to take the initiative away from the learners. There is always a chance for the teacher to take part in discussion but without dominating the student. The teacher should be careful when and how to give feedback in speaking activity because over correction may confuse the learner and take communication process out of the activity.

Involving TED into the classroom will prove that the conversation isn't just putting into practice the grammar and vocabulary skills taught within the course. It helps enhance the speaking skills, develop the ability to produce grammatically correct, logically connected sentences that are appropriate to specific contexts. It creates a classroom environment where the atmosphere is quite informal and cheerful and students have real-life communication, authentic activities and meaningful tasks that encourage them to talk on any topic and problems. It is also related to individual goals and achievement orientation. This activity can change students' attitude towards the language and culture.

References:

1. Bondar S.I. The Principles of Consciousness in Foreign Language Learning // Цілі сталого розвитку: глобальні та національні виміри: Матеріали наук.-практ.конф. (5-6 квітня 2017р.) [заг.ред. Семігіної Т.В.] К.: АПСВТ. 2017. - 318 с. – 269 С.
2. Brown, G., Yule, G (1983). Teaching the Spoken Language. New York: Cambridge University Press.
3. Ellis, R (2003) Task-based Language Learning and Teaching. Oxford: Oxford University Press.
4. Ministry of Education, The 2006 English Curriculum, Bangkok: Ministry of Education, 2008, pp. 20.
5. Zhang, Y. (2010) Cooperative Language Learning and Foreign Language Learning. Journal of Language Teaching and Research, Vol.1, No.1, January 2010.
6. Дітковська Л. А. Масові відкриті онлайн-курси Prometheus: реалії та перспективи // Мережеве суспільство: ринок праці, суспільні відносини, роль профспілок: Збірник матеріалів круглого столу (м. Київ, 22 березня 2018 р.) [Редкол.: Т. Семігіна, О. Корчинська, В. Співак]. К.: АПСВТ. 2018. 72 с. URL: https://www.socosvita.kiev.ua/sites/default/files/Tezy_RT_22_03_%202018.pdf (дата звернення: 2.05.2018).

ІНТЕЛЕКТУАЛЬНІ ТЕХНОЛОГІЇ ІДЕНТИФІКАЦІЇ В МЕДИЦИНІ

Сілагін Олексій, Тягній Маргарита

Вінницький національний технічний університет

Анотація

Досліджується можливість застосування сучасних інтелектуальних технологій ідентифікації для створення експертних систем в медицині. Розглянуто еволюцію розвитку систем підтримки прийняття рішень та експертних систем в галузі медицини. Робиться висновок про доцільність побудови медичних експертних систем та систем підтримки прийняття рішень на основі апарату нечіткої логіки

Abstract

The possibility of using modern intelligent identification technologies for creating expert systems in medicine is explored. The evolution of the decision-making support systems and expert systems in the field of medicine is considered. The conclusion is made on the feasibility of building medical expert systems and decision support systems on the basis of the fuzzy logic apparatus.

Вступ

Галузь медицини та охорони здоров'я чи не одна з перших почала використовувати для вирішення своїх проблем інформаційні технології. Вони допомагають вирішувати багато питань у медичних процесах за допомогою ПК. Як розглядають такі процеси з погляду інформатики?

Діагностика з погляду інформатики – процес виявлення несправностей у певній системі. Несправність – це відхилення від норми. Таке трактування дає змогу з єдиних теоретичних позицій розглядати і несправність обладнання в технічних системах, і захворювання живих організмів, і будь-які природні аномалії [1].

Прогнозування – логічне виведення (передбачення) імовірних наслідків заданих ситуацій на підставі аналізу даних. Прогнозування пов'язане з моделюванням різних ситуацій, тобто створюється модель, і виведені з цієї моделі наслідки формують основу для прогнозів з імовірнісними оцінками.

Моніторинг – безперервна інтерпретація даних у реальному масштабі часу і сигналізація про вихід тих чи інших параметрів за припустимі межі.

Підтримка прийняття рішень – це сукупність процедур, що забезпечує особу, яка приймає рішення, потрібною інформацією та рекомендаціями для сформування альтернативи серед множини виборів.

Інтерпретація даних – одне з традиційних завдань для інформаційних систем. Під інтерпретацією розуміють процес визначення смислу даних, результати якого мають бути узгодженими і коректними [2].

Еволюція експертних систем

Процеси прогнозування та діагностики в медицині стали можливі для програмування вже наприкінці 60-х років ХХ сторіччя. З'явилися перші діагностичні алгоритми – програми, у яких було використано бальний принцип (підррахунок балів за отримані на запитання відповіді) кількісного оцінювання кожного симптому (запитання). Бальна діагностика – відомий метод у медицині. Певний час діагностичні програми розроблялися в цьому напрямку. Такі програми мали консультативний характер, тому що не могли забезпечити високу ймовірність встановити правильний діагноз у зв'язку з відсутністю повної інформації про стан здоров'я пацієнта (наприклад, лабораторні й інструментальні дослідження). На ПК така програма представлена у формі тестового

опитування. Мета кожного запитання – отримати інформацію про симптоми, наявні або відсутні в обстежуваного. Модуль збирання інформації побудовано за принципом діалогу – на запитання треба відповідати тільки "так" чи "ні". Ця інформація формує базу даних та обробляється програмним модулем обробки й аналізу даних, після чого на екран подається діагностичне повідомлення. Сучасні вдосконалені бальні методики використовують у скринінгових системах [3].

Досконаліші програми-тести використовують інші методики діагностики (не бальні), включаючи в модуль обробки й аналізу даних імовірісно-статистичні методи (наприклад, імовірнісний метод, що полягає в обчисленні імовірностей захворювання за формулою Баєса). Такі діагностичні програми називаються імовірнісними. Імовірність діагностики в них вища, ніж у бальних програм. Вони так само є консультативними, тому що вирішальне слово залишається за лікарем.

Згодом з'являються діагностичні програми такого рівня, у яких алгоритм встановлення діагнозу наближений до мислення лікаря, тобто вони мають такий програмний логічний апарат, що дає змогу порівняти з існуючим медичним досвідом симптоми, виявлені при обстеженні хворого, а також швидко виконати складну статистичну обробку клінічного матеріалу. Такі системи називаються експертними [3].

Якщо в імовірнісних діагностичних програмах дані оброблялися на основі бази даних, то в експертних уже присутні якісно нові бази даних, названі базами знань.

Для обробки й аналізу даних база знань використовує одну з сучасних інтелектуальних технологій підтримки прийняття рішень [4]. Це штучні нейронні мережі, генетичні алгоритми та апарат нечіткої логіки. Останній, до речі найбільш приближений до моделей, якими користуються люди при прийнятті рішень. Таким чином, до початку ХХ століття формуються різні типи напрямків автоматизованих систем діагностики захворювань і прогнозування результатів їх лікування, серед яких виділяють скринінгові та експертні системи.

Висновки

Серед трьох, незалежних одна від одної теорій технології ідентифікації та прийняття рішень - нечітких множин, нейронних мереж та генетичних алгоритмів, для задачі прогнозування динаміки захворювань, найбільш доцільним є застосування теорії нечітких множин та нечіткої логіки.

Основою створеної системи прогнозування динаміки захворювань є формування, із застосуванням методів нечіткої логіки, матричної бази знань та застосування до неї продукційної системи навчання та виводу.

Список використаних джерел:

1. Кузьмук В. В., Супруненко О. О. Роль інформаційних технологій у донозологічній оцінці стану здоров'я людини // Тезиси и доклады международной конференции "Интегративная медицина" (24-25 мая 2008 г.). – К.: Алтимед, 2008. – С. 108-109.
2. Продеус А. Н., Захрабова Е. Н. Экспертные системы в медицине / А. Н. Продеус, Е. Н. Захрабова. – К.: ВЕК+, 1998. – 320 с.
3. Сілагін О.В., Евтушенко В.В. Ідентифікація кольорових відтінків із застосуванням апарату нечіткої логіки // Збірник праць Десятої Міжнародної науково-практичної конференції «Інтернет-Освіта-Наука» (ІОН-2016). – Вінниця: ВНТУ, 2016. – С. 50 – 51.
4. І. Арсенюк, О.Сілагін, С.Кукунін. Застосування апарату нечіткої логіки для оцінки якості графічних растрових зображень. // Збірник праць Дев'ятої Міжнародної науково-практичної конференції «Інтернет-Освіта-Наука» (ІОН-2014). – Вінниця: ВНТУ, 2014. – С. 223 – 225.

ІНКЛЮЗИВНА ОСВІТА В ІНФОРМАЦІЙНОМУ ПРОСТОРІ

Гончар Лариса

Академія праці, соціальних відносин і туризму

Анотація

Охарактеризовано перспективи інклюзивної освіти в окремому вищому навчальному закладі, де студенти з особливими потребами навчаються коштом Фонду соціального захисту інвалідів. Визначено проблеми взаємодії Фонду з вищим навчальним закладом та студентами. Представлено відгуки студентів з проблемами зору, слуху та іншими проблемами щодо їхнього навчання у студентському середовищі.

Abstract

The author characterises the prospects of inclusive education in a separate higher educational institution where students with special needs are taught at a cost of Fund for Social Protection of the Disabled. The problems of interaction between the higher educational institutions, students and Fund are determined. Reviews regarding the study in the student environment of students with visual impairments, hearing impairments and other problems are presented.

Вступ

Проблемами адаптації, реабілітації та інтеграції клієнтів з інвалідністю займалися такі науковці як І. Іванова, А. Капська, К.Холостова та інші. Найбільш актуальними напрямками для дослідження за словами Л. Дітковської [1]. залишаються профорієнтація, навчання, подальше працевлаштування, а також підготовка викладачів для роботи з особами, які мають особливі потреби. Зрозуміло, що майже всі вищі навчальні заклади України мають курси дистанційного навчання для успішного навчання студентів з різними формами інвалідності. Мають місце деякі невизначені моменти інклюзивної освіти у вищому навчальному закладі, що не підлаштований (або не повністю підлаштований) під потреби людей з інвалідністю: взаємодія вищого навчального закладу з Фондом соціального захисту інвалідів, надмірна кількість документів, які подаються вперше (11 наіменувань), необхідність після кожної сесії подавати завірену копію залікової книжки та довідки навчального закладу про відсутність заборгованості, брак співробітників Фонду, які приймають документи тощо. Також, студенти мають соціальні, фізичні та психологічні проблеми у цій взаємодії.

Основні результати

5 липня 2017 року президент України підписав ухвалений 23 травня цього ж року закон «Про внесення змін до Закону України «Про освіту» [2] щодо осіб з особливими освітніми потребами до освітніх послуг». Вперше такі діти, молодь, дорослі мають змогу навчатись безкоштовно не тільки у державних, а й закладах іншої форми власності коштом, наприклад, Фонду соціального захисту інвалідів.

Дослідження проводилось у травні 2018 року. В ньому брали активну участь студенти з особливими потребами: особи з проблемами зору (2 студенти), слуху (4 студенти), з проблемами опорно-рухового апарату та іншими формами інвалідності (3 студенти). Середній вік респондентів – 38 років. 8 з 9 студентів мають вищу освіту. Одна студентка має середню спеціальну освіту. Один студент не працює і стоїть на обліку в Центрі зайнятості. Спеціальності та місця роботи: маркшейдер (безробітний шахтар); бакалавр «Фінанси» (головний спеціаліст департаменту економіки та інвестицій міської ради); бухгалтер (за фахом бухгалтер в косметичній фірмі); інженер, технолог конструктор (працює за фахом як дизайнер вишивки і клеєного малюнку на дитячих виробках для новонароджених); інженер системний аналітик (фрілансер, створення і

підтримка сайтів); менеджер (не працює); інженер-хімік-технолог (офіс-адміністратор); бухгалтер (економіст, банк «Приват»); інженер (працює масажистом).

На першому етапі дослідження зі студентами були обговорені запитання для глибокого інтерв'ю. Студентами запропоновано наступні аспекти: ваш вік, освіта, місце роботи; які переваги особисто для вас має навчання в Академії?; яким чином можна охарактеризувати рівень підтримки вашої освіти в Академії?; які позитивні моменти ви можете відмітити?; з якими труднощами ви зіткнулись під час вступу?; чи можна ваше навчання назвати інклюзивним?; що можна покращити в організації процесу навчання в Академії?

Питання віку, освіти та місць роботи нами було представлено вище. Зазначимо найбільш конструктивні відповіді щодо переваг та позитивних моментів навчання, труднощів при вступі, інклюзивності в освіті, покращання процесу навчання в Академії.

Переваги та позитивні моменти, які зазначили студенти з особливими потребами в освіті: можливість соціалізації (спілкування зі студентами та викладачами); толерантне ставлення з боку викладачів; підтримка інших студентів і надання ними допомоги (навіть у пересуванні); знаходження нових друзів, які підтримують; приклад для власних дітей, самовдосконалення; додаткова реабілітація (пристосування до життя у суспільстві); розширення професійних знань і навичок; «підняття градусу суспільної свідомості» (просвіта студентів і викладачів). Дані відповіді надали 9 із 9 студентів.

Всі студенти визначили рівень підтримки навчання в Академії як високий або достатній (8 із 9). Зазначимо, що жоден із студентів попри наявні перешкоди не скаржився на труднощі навчання в Академії.

Проблеми, що зазначили слухачі: бюрократія у Київському міському відділенні Фонду соціального захисту інвалідів (невчасна виплата навчального закладу); проблеми проходження в Комісії на підтвердження групи інвалідності (некоректні запитання типу «навіщо вам вища освіта?» тощо).

Можна резюмувати, що:

необхідна підготовка викладачів для роботи з особами, які мають особливі потреби, зокрема з людьми, які мають проблеми зі слухом і зором (так, студенти з проблемами слуху самотужки наймають послуги сурдоперекладача, а студенти з проблемами зору мають програми, що перекладають тексти у доступний для сліпої особи формат);

потрібно продовжувати пристосування навчального закладу з урахуванням безбар'єрного доступу (пандуси, туалети тощо);

налагодити більш конструктивну взаємодію вищого навчального закладу з Фондом соціального захисту інвалідів у сфері подачі документів (для того, щоб студенти з особливими потребами не витрачали зайві зусилля ні на подачу документів, ні на повторне надсилання результатів сесії);

підготувати студентів психологічно до спілкування з працівниками Фонду соціального захисту інвалідів.

Список використаних джерел:

1. Дітковська Л. А. Значення інформаційних технологій у соціальній реабілітації інвалідів // Вісник Академії праці і соціальних відносин Федерації профспілок України. К., 2008. № 1. С. 5-9.

2. Закон «Про внесення змін до Закону України «Про освіту» щодо осіб з особливими освітніми потребами до освітніх послуг» від 5 липня 2017 року. (Відомості Верховної Ради (ВВР), 2017, № 30, ст.322)

МЕРЕЖЕВИЙ ІНДИВІДУАЛІЗМ В СИСТЕМІ КОМУНІКАЦІЙ

Бондар Світлана

Академія праці, соціальних відносин і туризму

Анотація

У доповіді піднімається тема мережевого індивідуалізму у спілкуванні. Процес спілкування розглядається як соціальне явище з точок зору психології та соціології. Підкреслюється зростання індивідуалізму в усіх його проявах. Визначається роль засобів масової інформації. Відмічається процес втрати суб'єктності у спілкуванні. Ставиться дискусійне питання про переваги і недоліки новітніх форм спілкування, які базуються на мережі.

Abstract

The report deals with the theme of networking individualism in communication. The process of communication is seen as a social phenomenon from psychological and sociological points of view. The growth of individualism in all its manifestations is emphasized. The role of the media is determined. The process of loss of subjectivity in communicating is noticed. The advantages and disadvantages of the latest forms of communication based on the network are proposed to discourse.

Швидкоплинні зміни у розвитку суспільства виявились особливо виразними в останні десятиріччя. Революційні зрушення в технологічних системах призвели до революційних змін в системі спілкування між людьми.

Всепоглинаючого характеру набув новітній процес так званої «інтернетизації» комунікативного простору, безпосередніми учасниками якого, спілкуючись у мережі, стали практично всі. І саме такого типу процес спілкування, увірвавшись в життя людей, став предметом розгляду багатьох науковців, починаючи з Е.Тоффлера і М.Кастельса.

Беззаперечно, невід'ємним елементами розвитку людського суспільства є спілкування між людьми. Процес спілкування в психології розглядається як окремий вид діяльності, який відрізняється комплексністю та багатоаспектністю. Вітчизняна психологічна наука визначає основною метою міжособистісного спілкування необхідність здійснення спільної діяльності. Пояснюється це тим, що будь-яке повідомлення, яке відправляється або приймається, обов'язково проходить через «ментальний фільтр» людини – її психологічні установки, що з наукової точки зору передбачають готовність або намір сприймати майбутні події або дії певним чином [2]. І це абсолютно справедливе науково-обгрунтоване твердження, якщо йдеться про спілкування між суб'єктами - носіями вербальної передачі і трансляції історичного чи набутого досвіду, якщо йдеться про комунікативну спільноту, долученням до норм існування якої і право самого існування в ній можливе лише через приєднання, тобто через процес колективної суб'єктизації.

Комунікація - частина життєдіяльності людини і одна з фундаментальних основ існування суспільства. Мається на увазі, що суспільство - це не дві-три людини, не одна-дві держави, а зв'язки і відносини, в яких певні учасники комунікації перебувають у стосунках спілкування один з одним. На думку багатьох дослідників, комунікація - це соціальне явище, або ж соціальна комунікація, що позначає передачу інформації, ідей, емоцій за допомогою знаків, символів, - це процес, який пов'язує окремі частини соціальної системи один з одним, це механізм, за допомогою якого реалізується влада (як спроба визначити поведінку іншої людини) [1]. Іншими словами, соціальна комунікація - обмін сенсу між людьми. Цілком очевидно, що ніяке суспільство не може існувати без комунікаційних зв'язків, а комунікативна потреба - органічна (абсолютна) духовна потреба людини.

У призмі інтернет-технологій динаміка розвитку сучасного суспільства характеризується соціальною атомізацією як явищем розпаду соціальних зв'язків[4].

Головним суб'єктом глобалізації стає людина з індивідуально орієнтованою, егоїстичною свідомістю, людина-споживач і прагматик у своїх відносинах із суспільством і людьми, яка для досягнення мети йде через конкуренцію, а не кооперацію. Зростання індивідуалізму в усіх його проявах займає домінуючу тенденцію в розвитку соціальних стосунків. Отже, індивідуалізм також проявляється і в комунікативних процесах, порушуючи норми існування комунікативної спільноти, формуючи нову модель комунікабельності, яка «характеризується індивідуалізмом, що базується на мережі» [3].

Новітній комунікативний процес охоплює певні, властиві тільки йому риси, а саме:

- надзвичайні технічні можливості його супроводу;
- пасивне споживання інформації;
- безмежна дискусійна платформа;
- віртуалізована анонімність;
- симульована публічність;
- виключення із комунікативної суб'єктності.

Сучасні засоби мас-медіа здійснюють свій вплив на розвиток індивідуалізму, вони сприяють формуванню підвищеного усвідомлення власної індивідуальності. Інтернет стає потужною матеріальною базою для поширення мережевого індивідуалізму, але сам він не створює модель мережевого індивідуалізму.

Завдяки таким змінам кожна особистість здатна створювати образ себе, і навіть кілька образів. Віртуальне спілкування дозволяє людині відійти від стандартів, відкрито висловлювати свої думки, переборювати бар'єри спілкування, одній і тій же людині по-різному позиціонувати себе через «аватарство». Мережевий індивідуалізм виявляється в тому, що спілкування втрачає суб'єктність: люди створюють «ніки (від англ. nickname - прізвисько)» і спілкуються не з людьми, а з «ніками», перебуваючи в реальному часі в «чаті» (chat - розмова) -ресурсі Інтернет, в якому за допомогою програм і скриптів реалізована можливість одночасного спілкування великої кількості користувачів, через вікно, в якому відсутня змога бачити реального співбесідника. Завдяки великій кількості учасників такого способу спілкування виникає своєрідний мережевий етикет, правилами якого є мережевий індивідуалізм і необхідність захисту мережі [5].

З точки зору сьогодення важко судити про це технологічне досягнення людства і намагатися оцінювати його недоліки і переваги в галузі комунікації. Адже свого часу винайдення алфавіту також здійснило велику революцію і в комунікативних процесах, і у психології людей. Важливим є те, що це абсолютно новий процес розвитку людських відносин. Він потребує вивчення і подальшого розгляду.

Список використаних джерел:

1. Бондар С.І Іншомовна освіта в сучасній парадигмі формування соціальної адаптованості та конкурентноспроможності майбутнього фахівця. Модернізація українського суспільства у світлі угоди про асоціацію з ЄС / С.І.Бондар - 36. Тез Міжнар. науково-практ. конфер. викладачів і аспірантів - К.: Акад. праці і соц. відносин Федер. проф. спілок України, 2015. – 144с., С.10-11
2. Максименко С.Д. Загальна психологія: Навч. Посібник./ С.Д. Максименко С.Д.– К.: Центр учбової літератури, 2008. – 270 с.
3. Різун В. Природа й структура комунікативного процесу / В. Різун / [Електронний ресурс]. – Режим доступу :<http://journlib.univ.kiev.ua/index.php?act=article&article=2>.
4. Тетерук С.П. “Рольова гра як засіб підвищення рівня саморегуляції студентів при вивченні іноземної мови” Проблеми Загальної та педагогічної психології/ С.П.Тетерук - Збірник наукових праць Інституту психології ім. Г.С.Костюка АПН України /За ред.. С.Д.Максименка. Т.Х., част. 5. -К., 2008. -662с.
5. Турецька Х.І. Особливості особистісної ідентичності користувачів Інтернету як чинник Інтернет-адикції / Х.І. Турецька // Збірник наукових праць Кам'янець-Подільського національного університету імені Івана Огієнка, Інституту психології імені Г.Костюка. – Кам'янець-Подільський. – 2010. – Вип. 10.– С. 750-762.

РОЗПІЗНАВАННЯ БАГАТОКАНАЛЬНИХ СИГНАЛІВ ЗА ДОПОМОГОЮ СПАЙКІНГОВИХ НЕЙРОННИХ МЕРЕЖ

Колесницький Олег, Куцман Владислав

Вінницький національний технічний університет

Анотація

У доповіді розглядається метод розпізнавання багатоканальних сигналів за допомогою спайкінгових нейронних мереж, структури і моделі нейронних елементів і мережі загалом, а також результати комп'ютерного моделювання процесу розпізнавання.

Abstract

The report examines the multichannel signals recognition method, based on spiking neural networks. report examines the structure and model of neural elements and the network as a whole, as well as the results of computer simulation of the recognition process

Головна мета функціонування інтелектуальних систем – вирішення когнітивних задач не гірше за людину [1].

Людина сприймає образи за допомогою органів чуття (очі, вуха, ніс і т.д.), які є багатоконтактними рецепторами. Ці багатоконтактні рецептори видають багатоканальну інформацію у вигляді сукупності сигналів (багатоканальні імпульсні сигнали). Центральна нервова система (ЦНС) людини має справу не з самим образом, а з результатом дії цього образу на рецептори. Для ЦНС образом є багатоканальні імпульсні сигнали, які генеруються рецепторами, а потім проходять складну обробку. Тому при побудові нейроморфних інтелектуальних систем нових поколінь велике значення має вирішення проблеми розпізнавання багатоканальних сигналів (в окремому випадку – імпульсних) [1].

Постановка задачі:

– Необхідно розпізнати n динамічних сигналів (сигнали мультисенсорів газів, антенних ґраток, параметри складних динамічних об'єктів і т.і.)

– Всі n сигналів надходять одночасно (паралельно) і обмежені на часовому відрізку

– Результат розпізнавання необхідно отримувати у реальному часі – відразу після закінчення сигналів.

Варіанти вирішення:

– Кореляційні методи – не підходять, оскільки необхідно багато паралельно працюючих кореляторів/

– Традиційні нейронні мережі – не підходять, оскільки часто для отримання результату необхідно декілька ітерацій і працюють із відліками вхідних сигналів або їх ознаками [2].

– Спайкінгові нейронні мережі [3] – підходять, оскільки 1) пристосовані до розпізнавання динамічних образів без їх попереднього перетворення у вектор ознак; 2) багатозадачні; 3) розпізнають із передбаченням. 4) мають просту процедуру навчання.

У доповіді розглядається метод розпізнавання багатовимірних сигналів за допомогою спайкінгових нейронних мереж, структури і моделі нейронних елементів [4] і мережі загалом [5], а також результати комп'ютерного моделювання.

Особливе значення має задача навчання спайкінгових нейронних мереж. При програмній або програмно-апаратній реалізації нейронних мереж застосовують будь-які алгоритми навчання з учителем, оскільки необхідно навчити тільки вихідні (зчитувальні) нейрони мережі: дельта-правило, лінійну регресію, r -дельта правило, алгоритм

зворотного поширення та ін. (процес навчання здійснюється шляхом виконання обчислень за визначеними формулами на цифровому процесорі).

При апаратній реалізації нейронних мереж особливе значення має так зване on-line (або on-chip) навчання, тобто навчання за допомогою спеціальних схмотехнічних засобів, які змінюють ваги синаптичних зв'язків нейронних елементів без застосування яких би то не було обчислювальних операцій на цифрових процесорах.

В якості схмотехнічних засобів для адаптації ваг зв'язків вихідних нейронів можуть використовуватись електронні та оптоелектронні компоненти з параметрами, що змінюються. Це, наприклад, варіапи, МДН-транзистори з плаваючим затвором, варістори, програмовані за допомогою імпульсів різної полярності резистори на основі оксидів вісмуту або аморфного полікристалічного кремнію, мемрістори, аналогові оптично керовані транспаранти з пам'яттю та режимами додавання та віднімання зображень.

Переваги нейрокомп'ютерних систем на основі спайкінгових нейронних мереж

- 1) динамічні сигнали подаються на розпізнавання одночасно без розділення у часі або у просторі, а також без попереднього запам'ятовування,
- 2) підвищення швидкодії – результат розпізнавання може бути оцінено ще до завершення періоду дії самих сигналів за інтенсивною імпульсацією на відповідному виході (розпізнавання з передбаченням),
- 3) спрощення процесу навчання – по-перше, за рахунок використання схмотехнічних засобів для навчання та відсутності складних обчислювальних процедур при навчанні нейронної мережі та пристроїв для їх здійснення, по-друге, навчаються не всі нейрони мережі, а лише вихідні нейрони,
- 4) підвищена завадостійкість за рахунок передачі інформації в імпульсній формі.
- 5) спрощення системи – за рахунок скорочення кількості нейронів завдяки застосуванню оптоелектронних нейронних елементів з однаковою полярністю сигналів для збуджувальних та гальмівних імпульсів,
- 6) покращення конструктивно-технологічних параметрів системи - за рахунок використання оптичних, а не електричних сигналів для організації величезної кількості зв'язків між нейронами мережі та реалізації системи на оптоелектронній елементній базі.

Список використаних джерел:

1. Колесницький О. К. Принципи побудови архітектури спайкових нейрокомп'ютерів / О. К. Колесницький // Вісник Вінницького політехнічного інституту. – Вінниця: УНІВЕРСУМ-Вінниця. – 2014. – №4 (115), С.70-78.
2. Савчук Т. О. Використання ієрархічних методів кластеризації для аналізу надзвичайних ситуацій на залізничному транспорті / Т. О. Савчук, С. І. Петришин // Вимірювальна та обчислювальна техніка в технологічних процесах. – 2009. – № 1 : – С. 193–198.
3. Kolesnytskyj O. K. Optoelectronic Implementation of Pulsed Neurons and Neural Networks Using Bispin-Devices / O. K. Kolesnytskyj, I. V. Bokotsey, S. S. Yaremchuk // Optical Memory & Neural Networks (Information Optics). – 2010. – Vol.19. – №2. – P.154–165. – ISSN 1060-992X.
4. O. K. Kolesnytskyj, S. A. Vasyletskyj, „BISPIN - based optoelectronic neuron element” in Selected Papers from the International Conference on Optoelectronic Information Technologies, Sergey V. Svechnikov, Volodymyr P. Kojemiako, Sergey Al. Kostyukevych, Editors, Proceedings of SPIE Vol. 4425, 417 - 424 (2001).
5. V. P. Kozemiako ; O. K. Kolesnytskyj ; T. S. Lischenko ; W. Wojcik and A. Sulemenov " Optoelectronic spiking neural network ", Proc. SPIE 8698, Optical Fibers and Their Applications 2012, 86980M (January 11, 2013); doi:10.1117/12.2019340; <http://dx.doi.org/10.1117/12.2019340>

ВЕБ-ДОДАТОК УПРАВЛІННЯ ТОВАРНИМИ ЗАПАСАМИ НА ОСНОВІ ТРИРІВНЕВОЇ АРХІТЕКТУРИ

Никуляк Артем, Месюра Володимир

Вінницький національний технічний університет

Анотація

Здійснено аналіз трирівневої архітектури програмного забезпечення у проектуванні веб-додатків. Описано структуру, функціональні можливості рівнів та переваги архітектури для проектування і розробки веб-додатку управління товарними запасами.

Abstract

Was performed the analysis of three-tier software architecture in the design of web-applications. The structure, functional capabilities of levels and advantages of architecture for designing and developing inventory management web application was described.

Вступ

При проектуванні програмного рішення основним кроком є вибір архітектури. Вибір архітектури системи здійснюється з врахуванням цілей системи, її вхідних і вихідних даних. Вдало підібрана архітектура може забезпечити зручність масштабування і підтримки спроектованого програмного забезпечення та зменшити час, необхідний для його розробки. Такі можливості для веб-додатку управління товарними запасами надає трирівнева архітектура.

Результати дослідження

Веб-додаток управління товарними запасами підприємства розробляється для підприємства продажу комп'ютерної техніки. Програмний модуль надасть зручні інструменти для здійснення управління товарами підприємства, відстежування гарантійних термінів товарів. Створення та відстежування заявок на гарантійне обслуговування, зміна їх статусів після виконання. Ці процеси можуть бути успішно впроваджені у веб додатку на основі трирівневої архітектури.

Трирівнева архітектура (англ. three-tier або Multitier architecture) – це тип архітектури програмного забезпечення, що складається з трьох "ярусів" або "шарів" логічного обчислення. Вони часто використовуються в програмах як специфічний тип клієнт-серверної системи. Трирівнева архітектура забезпечує багато переваг для середовища та процесу розробки шляхом розбиття на модулі користувацького інтерфейсу, бізнес-логіки та зберігання даних. Це дає більше можливостей для груп розробників, дозволяючи їм оновлювати певну частину програми незалежно від інших частин. Ця додаткова гнучкість може поліпшити загальний час виходу на ринок і скоротити час розробки, надаючи командам розробників можливість заміни або модернізації незалежних рівнів, не змінюючи інших частин системи.

Ця архітектурна систем часто використовується для вбудовування та інтеграції стороннього програмного забезпечення в існуючу програму. Ця інтеграційна гнучкість також робить систему зручною для вбудовування програмного забезпечення для аналітики, і з цієї причини часто використовуються постачальниками аналітичних засобів. Трирівневі архітектури часто використовуються у хмарних або локальних додатках, а також у програмних сервісах (SaaS) [1].

Веб-додаток управління товарними запасами на основі трирівневої архітектури складаються з наступних рівнів:

– Presentation Tier. Рівень презентації – це шар інтерфейсу в трирівневій системі, що визначає інтерфейс користувача. Цей користувацький інтерфейс є графічним, доступним через веб-браузер або веб-додаток і відображає вміст і інформацію для користувачів системи. Цей рівень часто побудований на веб-технологіях HTML5, JavaScript, CSS, і виконує доступ до інших шарів через виклики API.

– Application tier. Рівень застосування містить функціональну бізнес-логіку, яка виконує основні операції керування товарами у веб-додатку. Цей рівень розробляється за допомогою мови програмування C # .NET.

– Data tier. Рівень даних складається з системи збереження та доступу до даних і бази даних підприємства. Доступ до даних здійснюється на рівні додатків через виклики API.

Структуру веб-додатку з трирівневою архітектурою зображено на рисунку 1.

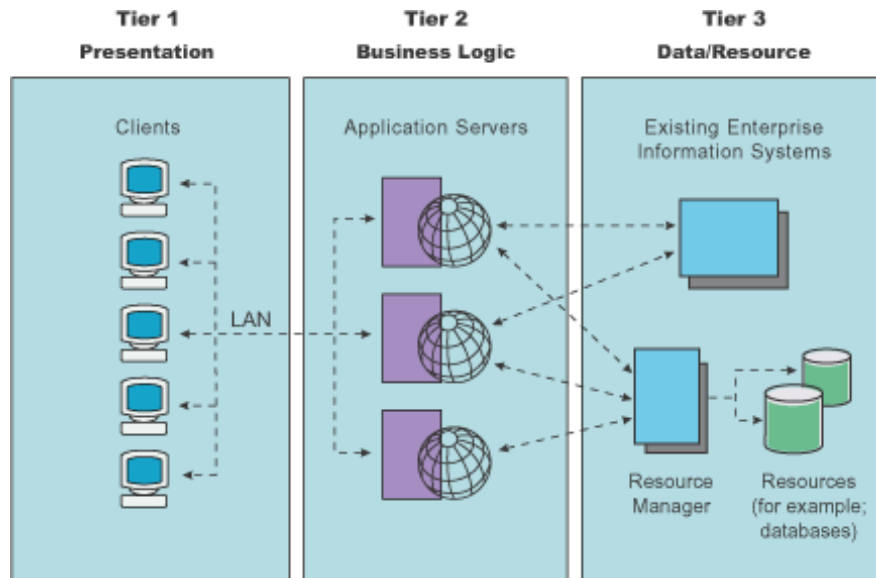


Рисунок 1 – Структура веб-додатку управління товарними запасами на основі трирівневої архітектури

Використання трирівневої архітектури дає багато переваг, включаючи швидкість розробки, масштабованість, продуктивність і доступність. Розбиття на модулі різних рівнів програми дає командам розробників можливість розробляти та підвищувати продуктивність з більшою швидкістю, ніж розробка унікальної кодової бази, оскільки певний шар може бути оновлений з мінімальним впливом на інші шари. Це також може допомогти покращити ефективність розвитку, дозволяючи командам зосередити увагу на їхній основній компетенції[2].

Список використаних джерел:

1. Paul Clements; Felix Bachmann; Len Bass. Documenting Software Architectures: Views and Beyond. – Second Edition. – Addison-Wesley Professional, 2010. – 79с. – ISBN 978-0-13-248861-7.
2. Len Bass, Paul Clements, Rick Kazman. Software Architecture in Practice, Third Edition. Addison Wesley, 2012. – 127с. – ISBN 978-0321815736

К РАЗРАБОТКЕ СИСТЕМ АВТОМАТИЗАЦИИ ПРОИЗВОДСТВА ДЛЯ ПРЕДПРИЯТИЙ ГИДРОПОНИКИ

Кокая Гига

Грузинский университет им.Святого Андрея Первозванного Патриаршества Грузии, Тбилиси, Грузия

Аннотация

Работа посвящена проблематике, связанной с разработкой систем автоматизации производства для предприятий, производящих сельскохозяйственную продукцию на базе гидропоники.

Автор дает обобщенный анализ рассматриваемого подхода, делится собственным опытом создания конкретной системы вышеуказанного профиля, а также приводит соображения о перспективном развитии подобных систем.

Abstract

This work is devoted to the problems associated with the development of production automation systems for enterprises that produce agricultural products based on hydroponics.

The author gives a generalized analysis of the approach in question, shares his own experience in creating a specific system of the above profile, and also gives reasons for the future development of such systems.

Введение

С внедрением новейших компьютерных технологий, одна из древнейших форм разведения сельскохозяйственной продукции, гидропоника (исторически наиболее ярко представленная “висячими садами Семирамиды”) получила мощный импульс для дальнейшего развития ([1-3]). В частности, стали появляться различные предприятия профиля гидропоники, с высоким уровнем автоматизации производственных процессов. Небезынтересно, что в настоящее время до 80 % всех овощей, зелени и фруктов в Израиле выращивается гидропонным способом.

Преимущества гидропоники

По сравнению с разведением растений на земельных участках, гидропоника имеет целый ряд преимуществ:

1. Вода расходуется существенно экономнее.
2. Благодаря возможности вертикального этажирования, требует намного меньше площади.
3. Процедура выращивания не требует использования химикатов, поэтому не сопровождается загрязнением окружающей среды, а полученный продукт является экологически чистым.
4. Производство и отдельные его составляющие обладают свойством переносимости (модульности).
5. Производственный процесс независим от времени года.
6. Имеется возможность получать несколько урожаев в год
7. Процесс в целом легче подвержен автоматизации, благодаря чему имеется возможность создавать и поддерживать оптимальные условия выращивания растений, что благотворно сказывается на продуктивности производства и качестве полученной продукции.
8. Масштабируемость производства.

В настоящий момент следует выделить два фактора, препятствующих распространению технологий, основанных на гидропонике:

1. Ощутимая дороговизна качественных светодиодных лампочек, обеспечивающих оптимальное освещение выращиваемых растений.
2. Отсутствие стандартизованных автоматизированных систем производства.

Основные функции автоматизированной системы

Перед автором стояла задача автоматизации системы производства, на базе вертикально этажированной гидропоники. В частности, следовало автоматизировать следующие производственные функции:

1. Обеспечение бесперебойной циркуляции воды в системе.
2. Контроль температуры.
3. Контроль освещения.
4. Контроль pH (водородный показатель) воды.
5. Контроль циркуляции и вентиляции воздуха.
6. Непрерывная подача воздуха в резервуар с водой (для обогащения кислородом).
7. Контроль влажности воздуха.
8. Контроль содержания питательных веществ.

Некоторые особенности реализации

Управляющая часть системы была создана на языке Python и работает на мини-компьютере Raspberry Pi. Компоненты системы, предназначенные для работы с датчиками и соленоидами под управлением Arduino ([4,5]), созданы на C++. Для удобства конечного пользователя создана система, доступная из глобальной сети и предназначенная для вывода текущей информации о состоянии производственного процесса в виде текстов и графиков.

Заключение

На данный момент система уже в течение более чем полугода обеспечивает автоматизацию полного цикла производства на одном из предприятий, расположенном в Грузии и специализирующемся на выращивании салата. В течение данного периода система подтвердила свою жизнеспособность. Ведется работа по увеличению надежности системы за счет более полной обработки ситуаций, связанных с возможными отказами со стороны отдельных аппаратных составляющих, а также в направлении дублирования наиболее важных функций.

Главной преградой на пути стандартизации системы в настоящий момент представляется отсутствие де-факто стандарта в сфере аппаратных составляющих. Нынешнее состояние разработки позволяет уверенно прогнозировать быструю стандартизацию подобных систем по мере решения вопроса стандартизации аппаратного обеспечения.

Список использованных источников:

1. Keith Roberto, How-To Hydroponics - ISBN 978-0967202617
2. John Mason, How to Grow 86 Different Plants in Hydroponics - ISBN: 978-0864173003
3. Hydroponic Food Production: A Definitive Guidebook for the Advanced Home Gardener and the Commercial Hydroponic Grower - ISBN-13: 978-1439878675
4. Улли Соммер, Программирование микроконтроллерных плат Arduino/Freduino - БХВ-Петербург - ISBN: 978-5-9775-0727-1
5. Торо Карвинен, Киммо Карвинен, Вилле Валтокари, Делаем сенсоры. Проекты сенсорных устройств на базе Arduino и Raspberry Pi, Вильямс, ISBN: 978-5-8459-1954-0, 2015

ВИКОРИСТАННЯ RESTFUL API ПРИ РОЗРОБЦІ МОДУЛЯ КЕРУВАННЯ ТОВАРНИМИ ЗАПАСАМИ.

Педоренко Владислав, Месюра Володимир

Вінницький національний технічний університет

Анотація

Проведено аналіз використання RESTful API при розробці модуля керування товарними запасами. Розглянуто базові принципи проектування, схему взаємодії різних частин модуля.

Abstract

Was performed the analysis of the use of the RESTful API in the development of the inventory management module. The basic principles of design, the scheme of interaction of different parts of the module are considered.

Вступ

При розробці модуля керування товарними запасами використовується трирівнева архітектура проектування, тобто будується екосистема, до якої входить: клієнтська частина, серверна частина, яка буде побудована за принципом Restful API та шар даних.

REST визначає ряд архітектурних принципів проектування Web-сервісів, орієнтованих на системні ресурси, включаючи способи обробки і передачі станів ресурсів по HTTP різноманітними клієнтськими додатками, написаними на різних мовах програмування. За останні кілька років REST стала переважаючою моделлю проектування Web-сервісів. Фактично REST зробила настільки великий вплив на Web, що практично витіснила дизайн інтерфейсу, заснований на SOAP і WSDL, через більш простий стиль проектування.

Результати дослідження

REST - це набір принципів і обмежень взаємодії клієнта і сервера в мережі інтернет, який використовує існуючі стандарти (HTTP протокол, стандарт побудови URL, формати даних JSON і XML) в ході взаємодії.

Схема взаємодії клієнтської частини модуля керування товарними запасами з RESTful API наведена на рисунку 1.

Розробляючи модуль керування товарними запасами, REST використовується в чистому вигляді, тобто слідує чотирьом базовим принципам проектування:

- Явне використання HTTP-методів.
- Незбереження стану.
- Надання URI, аналогічних структурі каталогів.
- Передача даних в XML, JavaScript Object Notation (JSON) або в обох форматах.

Однією з ключових характеристик RESTful API при розробці модуля є явне використання HTTP-методів згідно з протоколом, визначеним в RFC 2616. Цей основний принцип проектування REST встановлює однозначну відповідність між операціями create, read, update і delete (CRUD) і HTTP-методами. Згідно з цим, для роботи з ресурсами використовується:

- Для створення ресурсу на сервері використовується POST.
- Для вилучення ресурсу використовується GET.
- Для зміни стану ресурсу або його поновлення використовується PUT.
- Для видалення ресурсу використовується DELETE.

Слідуючи загальноприйнятим підходам, відповідно рекомендаціям REST при явному застосуванні HTTP-методів, використовуються іменники в URI замість дієслів. В RESTful API дієслова POST, GET, PUT і DELETE вже визначені протоколом.

Для реалізації узагальненого інтерфейсу і явного виклику операцій клієнтськими додатками API не визначає додаткові команди або віддалені процедури, наприклад / adduser або / updateuser. Цей загальний принцип застосовано також до тіла HTTP-запиту, який призначений для передачі стану ресурсу, а не імені викликаного віддаленого методу або віддаленої процедури.

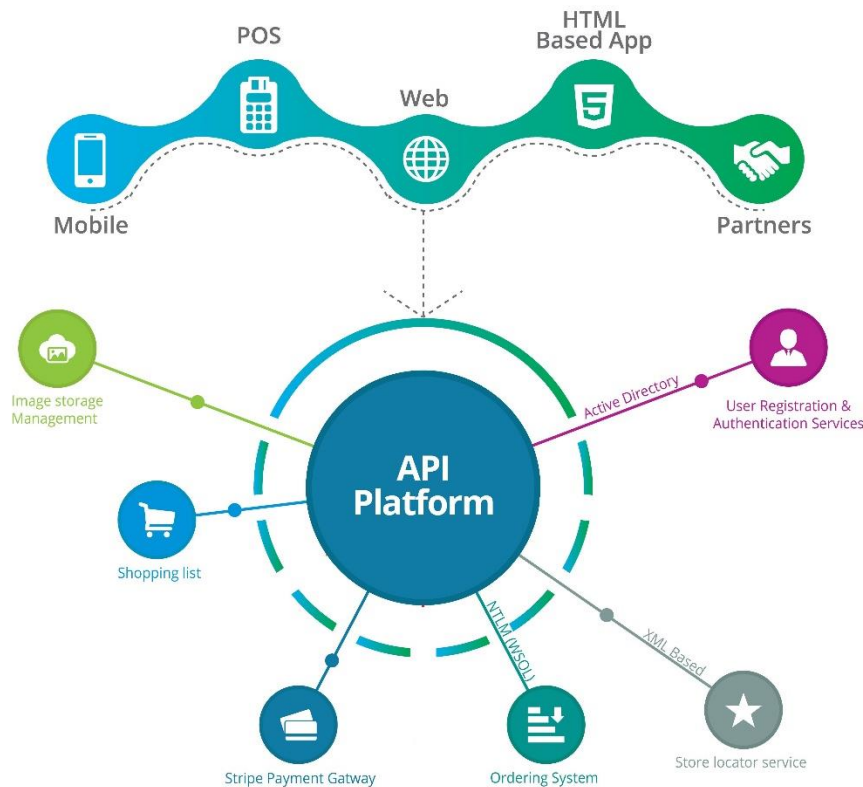


Рисунок 1 – Схема взаємодії клієнтської частини з RESTful API

Для задоволення постійно зростаючих вимог до продуктивності, REST API розробляється масштабованим. Для формування топології сервісів, що дозволять при необхідності перенаправляти запити з одного сервера на інший з метою зменшення загального часу реакції на виклик Web-сервісу, застосовано кластери серверів з можливістю розподілу навантаження і аварійного перемикавання на резерв, проксі-сервери і шлюзи. Використовуючи проміжні сервери для поліпшення масштабованості клієнти Web-сервісів REST відправляють повні самодостатні запити, що містять всі необхідні для їх виконання дані, щоб компоненти на проміжних серверах могли перенаправляти, маршрутизувати і розподіляти навантаження без локального збереження стану між запитами.

При обробці повного самодостатнього запиту сервер не витягує стан або контекст програми. Додаток (або клієнт) Web-сервісу REST включає в HTTP-заголовки і в тіло запиту всі параметри, контекст і дані, необхідні серверному компоненту для генерування відповіді.

Для забезпечення функціонування сервісів RESTful API, які не зберігають стан, його розділено на дві сфери відповідальності:

Сервер

– Генерує відповіді, які містять посилання на інші ресурси для навігації додатків по зв'язаних ресурсах. Такі відповіді містять вбудовані посилання. Аналогічним чином при запиті батьківського або контейнерного ресурсу RESTful-відповідь містить посилання на нащадків батьківського елемента або на підлеглі ресурси, щоб зберігали зв'язок з ними.

– Генерує відповіді, що містять інформацію про те, чи підлягають вони кешуванню з метою підвищення продуктивності за рахунок зменшення кількості запитів, що дублюються ресурсів і повної відмови від деяких запитів. Для цього сервер включає в відповідь HTTP-заголовки Cache-Control і Last-Modified (значення даних).

Клієнтська програма

– За заголовком Cache-Control відповіді визначає можливість кешування ресурсу (його локального копіювання). Також клієнтська програма читає заголовок Last-Modified відповіді і повертає значення дати в заголовку If-Modified-Since для відправки на сервер запиту про зміну ресурсу. Такий запит, т.зв. Conditional GET, використовує обидва заголовка. Якщо ресурс з зазначеного часу не змінився, відповіддю сервера є стандартний код 304 (Not Modified) і запитаний ресурс не відправляється. Код відповіді 304 HTTP означає, що клієнтський додаток може спокійно використовувати кешовану локальну копію подання ресурсу в якості самої останньої його версії, фактично опускаючи наступні запити GET до тих пір, поки ресурс не буде змінений.

– Відправляє повні запити, які можуть оброблятися незалежно від інших запитів. Це вимагає від клієнтського додатка використання в повному обсязі HTTP-заголовків, визначених інтерфейсом Web-сервісу, і відправки повних представлень ресурсів в тілі запиту. Клієнтська програма відправляє запити, які практично нічого не знають про попередні запити, про існування сеансу на сервері, про здатність сервера додавати контекст в запит і про стан додатки, що зберігається між запитами.

Така спільна робота клієнтського додатка і сервісу дуже важлива для відмови від збереження стану в Web-сервісах RESTful. Результатом відмови від збереження стану є зростання продуктивності за рахунок зменшення трафіку і мінімізації стану серверного додатка.

URI-адреси REST розроблені щоб бути інтуїтивно зрозумілими. Тому структура URI є простою, передбачуваною і зрозумілою. Одним із способів досягти такого рівня зручності використання – була побудова URI за аналогією зі структурою каталогів. Такого роду URI є ієрархічними, що походить із одного кореневого шляху, розгалуження якого відображають основні функції сервісу.

Подання системних ресурсів через RESTful API - це гнучкий спосіб забезпечення різних додатків даними в стандартному форматі. Це допомагає виконати вимоги до інтеграції, що мають вирішальне значення для створення систем, що дозволяють легко комбінувати дані, а також для побудови на основі набору базових RESTful-сервісів більших конструкцій.

Список використаних джерел:

1. Leonard Richardson, Sam Ruby, RESTful Web Services - O'Reilly Media, 2008. – 235 с.
2. Педоренко, В.Ю. Модуль керування товарними запасами, клієнтська частина [Текст]/В.Ю. Педоренко, В.І. Месюра // XLVII Науково-технічна конференція ф-ту інформ. технологій та комп. інженерії : Тез. доп. – Вінниця, 2018. – с. 2

УДК 316.77

ВИКОРИСТАННЯ ГЕОЛОКАЦІЇ В СОЦІАЛЬНИХ МЕРЕЖАХ

Ніколайчук Максим, Озеранський Володимир

Вінницький національний технічний університет

Анотація

В роботі приведено приклади використання геолокації в соціальних мережах. Описано головні переваги та недоліки геолокації. Доведено необхідність використання геолокації в соціальних мережах.

Abstract

Examples of using geolocation in social networks are given in this work. The main advantages and disadvantages of geolocation are described. The necessity of using geolocation in social networks is proved.

Вступ

Геолокація – це визначення реального місця розташування електронного пристрою. Цим поняттям може описуватися сам процес визначення місцезнаходження пристрою, а також його безпосереднє розташування на географічній карті.

Дані геолокації можна отримати через:

- IP-адресу пристрою.
- Технологію GPS.
- Технологію Wi-Fi.
- Мобільні мережі.
- Дані користування електронним пристроєм.

Додатки, які будуть виконувати геолокацію, повинні підтримувати стандарт геолокації W3C.

Деякі браузерери для визначення місця розташування користувача використовують IP-адреси. Однак такий спосіб може лише приблизно визначити положення користувача. Метод W3C є найпростішим і широко підтримуваним, і тому саме йому слід віддавати пріоритет перед іншими методами геолокації.

Геолокація в соціальних мережах

Вперше користувачі дізналися, що таке геолокація, завдяки технології визначення місця розташування пристрою за його IP-адресою. Але, на жаль, даний спосіб дає не дуже точні географічні дані, тому сьогодні 4його використовують вкрай рідко. Цей метод полягає в автоматичному визначенні IP-адреси і відповідно фізичної особи, на яку він зареєстрований. Але так як IP-адреса, як правило, надається інтернет-провайдером, то і місце розташування визначається не конкретного пристрою, а фірми, яка надає інтернет-послуги.

Перевагою даного способу геолокації є те, що він доступний в будь-якому місці, у будь-який час. Дані обробляються на стороні сервера.

Його недоліки:

- Низька точність визначення геолокації. Розташування обмежується населеним пунктом, в якому розташовується інтернет-провайдер.

- Висока вартість. Деякі веб-ресурси використовують ваш IP-адресу при розміщенні контекстної реклами. Ви зможете це виявити під час перебування за межами вашої країни, рекламні оголошення будуть відображати послуги місцевих компаній.

Технологія GPS в даний час найбільш популярна, а також саме цей спосіб дає уявлення про те, що таке геолокація. Технологія GPS заснована на отриманні найточніших даних з навігаційних супутників. Але для отримання результату запиту про

місцезнаходження потрібно деяку кількість часу, що є невеликим недоліком даної технології. Безперечною перевагою даного методу є висока точність результату. Недоліки:

- Низька швидкість обробки даних.
- Переривання зв'язку зі супутником в деяких приміщеннях/метро/ліфті.

Визначення геолокації за допомогою технології Wi-Fi доречно лише в міських умовах. Результати, отримані цим методом, також відрізняються високою точністю, як і технологія, заснована на використанні GPS. Але найчастіше ці два способи визначення геолокації діють в сполученні один з одним.

Переваги:

- Висока точність.
- Доступність в будь-яких приміщеннях.
- Висока швидкість і економічність.

Недоліки:

- Потрібно Wi-Fi адаптер.

Соціальні мережі з використанням технології геолокації мають назву «геосоціальні мережі».

Геосоціальна мережа - це вид соціальних мереж, в яких використовуються геокодування і гео-мітки, що розширюють можливості соціалізації. Користувачі залишають дані про своє місцезнаходження, що дозволяє об'єднувати і координувати дії користувачів на підставі того, які люди присутні в тих чи інших місцях, або які події відбуваються в цих місцях. Геолокація за допомогою комп'ютерів може використовувати або IP, або трилатерацію. У мобільних пристроях геолокація реалізується за допомогою GPS, текстової інформації, або LBS.

Висновки

Отже, результуючи даний огляд, можна зробити висновок що геолокація приносить позитивний вплив на спілкування між людьми.

Багато соціальних мереж використовують геолокацію, щоб відзначити місце розташування зроблених вами фотознімків. Це позбавляє від необхідності додаткового опису фотографії. А також дозволяє краще скооперувати дії певних груп людей та використовувати можливості соціальних мереж в повній мірі.

Принципи визначення місцеположення реального електронного пристрою не складні, хоча деякі труднощі виникають у правильному виборі технології для реалізації геолокації.

Список використаних джерел:

- 1.Що таке геолокація? [Електронний ресурс]. Режим доступу: <https://hi-news.pp.ua/tehnka-tehnologyi/1315-scho-take-geolokacya-yiyi-plyusi-mnusi.html> (Дата звернення - 28.04.18)
- 2.Геолокация [Електронний ресурс]. Режим доступу: [https://ru.wikipedia.org/wiki/Геолокация_\(информатика\)](https://ru.wikipedia.org/wiki/Геолокация_(информатика)) (Дата звернення - 28.04.18)
- 3.Геосоциальные сети [Електронний ресурс]. Режим доступу: https://ru.wikipedia.org/wiki/Геосоциальные_сети (Дата звернення - 28.04.18)
- 4.Геолокация: отображение положения пользователя или устройства на картах [Електронний ресурс]. Режим доступу: <https://developers.google.com/maps/documentation/javascript/geolocation?hl=ru> (Дата звернення - 29.04.18)
- 5.Ніколайчук М.Д. Технології створення соціальних мереж / М.Д. Ніколайчук, В.С. Озеранський // Тези XLV науково-технічної конференції професорсько-викладацького складу, співробітників та студентів університету, 21–23 березня, 2018. – Вінниця: ВНТУ, 2018

РОЗРОБКА САЙТУ ПСИХОЛОГІЧНОГО ТЕСТУВАННЯ «ВІКНО ДЖОХАРІ»

Ярова Анастасія, Сілагін Олексій

Вінницький національний технічний університет

Анотація

Метою роботи є розробка сайту психологічного тестування. У роботі розглянуто оцінювання на основі методу Джозефа Лафта та Харрінгтона Інгама а також використання нечіткої логіки для розробки сайту психологічного тестування «Вікно Джохарі»

Abstract

The aim is to develop a site of psychological tests. The paper describes the evaluation on the basis of Lafta Joseph and Harrington Ingham and use fuzzy logic to develop psychological testing site "Window Jokhar"

Вступ

Актуальною задачею є програмна реалізація психологічного тесту “Вікно Джохарі” з можливістю адміністрування, що суттєво скоротило б час на проведення і збереження результатів тестування, а також з додатковою функцією визначення психологічного типу людини.

Мета дослідження це розширення функціональних характеристик психологічного тесту «Вікно Джохарі».

Дослідження присвячене застосуванню до оцінювання результатів тестування за технікою “Вікно Джохарі” апарату нечіткої логіки .

Оцінювання на основі методу Джозефа Лафта та Харрінгтона Інгама

Техніка “Вікно Джохарі” створена у 1955 році двома американськими психологами — Джозефом Лафтом та Харрінгтоном Інгамом. Цю методику широко використовують психологи у своїй практиці.

Соціальний центр, що контактує з людьми різного віку й статі, використовує тест на основі цієї техніки для визначення, наскільки добре людина знає саму себе, а також, щоб людина зуміла зрозуміти, як оточуючі ставляться до неї. [1,2].

Цей тест був придуманий Джозефом Лафтом і Харрінгтоном Інгамом в 1950 році в процесі дослідження групової динаміки. Метод добре ілюструє і пояснює процеси, що відбуваються між окремим індивідом і групою, допомагає краще пізнати себе, налагодити спілкування з близькими або поліпшити розуміння в колективі [1].

Під час виконання вправи (рисунок 1) суб'єкту дається список із 58 прикметників, з якого йому треба вибрати ті, що найбільше характеризують його особистість. Кожен із знайомих суб'єкта вибирає ті прикметники з списку, що на їхню думку, описують цього суб'єкта. Вибрані характеристики заносяться в спеціальну таблицю.

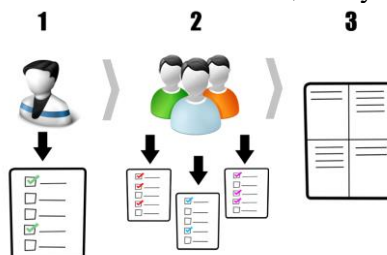


Рисунок 1 – Схема методу оцінювання

"Вікно Джохарі" являє собою символічне зображення особистості людини. Візуально – це квадрат (рисунок 2), розділений на чотири частини, кожна з яких – частина інформації про людину, передана під час спілкування [2].

Модель використовується для того, щоб зрозуміти:

- як особистість вибудовує контакт з іншими індивідуумами соціуму;
- якою особистість уявляє себе в суспільстві;
- як інші люди сприймають певного індивідуума під час спілкування.

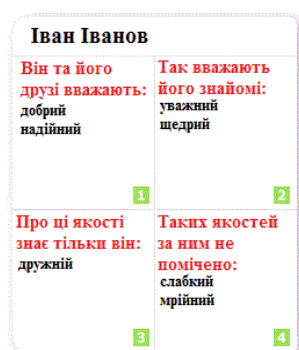


Рисунок 2 – Результат оцінювання

Оскільки для визначення результатів тесту його мають пройти користувач та декілька його друзів або знайомих (мінімальна кількість 3 людини), виникає проблема громістких обрахунків які займають багато часу.

Сайт психологічного тестування «Вікно Джохарі» потрібний для того щоб спростити процес проходження та визначення результатів тесту.

За допомогою сайту користувач може:

- дізнатися про свої сильні і слабкі сторони;
- зрозуміти, яким його бачать друзі;
- розібратися у власному характері;
- виявити свої приховані сторони;
- створити свій портрет.

Проектування модуля класифікації психологічного типу з використанням нечіткої логіки.

Після психологічного тестування користувач також отримує лінгвістичну характеристику своєї особистості. Для цього використовується нечітка логіка. Мабуть, найбільш вражаючою властивістю людського інтелекту є здатність приймати правильні рішення в умовах неповної і нечіткої інформації. Побудова моделей наближених роздумів людини і використання їх у комп'ютерних системах представляє сьогодні одну з найважливіших проблем науки.

Сьогодні елементи нечіткої логіки можна знайти в десятках промислових виробів - від систем керування електропоїздами і бойовими вертольотами до пилососів і пральних машин. Рекламні кампанії багатьох фірм (переважно японських) підносять успіхи у використанні нечіткої логіки як особливу конкурентну перевагу [3].

Формалізація вихідної інформації

Ідея, що лежить в основі формалізації причинно-наслідкових зв'язків між змінними «входи-вихід», полягає в описі цих зв'язків на природній мові із застосуванням теорії нечітких множин і лінгвістичних змінних. Мета цього розділу полягає у введенні основних формалізмів, необхідних для визначення нечітких баз знань, що є носієм експертної інформації.

Функції належності: представимо за допомогою таблиці психологічні типи та прикметники які їх характеризують.

Таблиця 1 - Психологічні типи

№	Тип	Прикметники
1	Інтроверт	спокійний, стриманий, замкнутий, тихий, зібраний, пасивний, незалежний, самодостатній;
2	Екстраверт	жвавий, балакучий, відкритий, взаємодіючий, ініціативний, цікавий, залежний від думки інших;
3	Раціональний	Обережний, обдуманий, чіткий, пунктуальний, серйозний, категоричний, організований;
4	Ірраціональний	Мобільний, мінливий, несподіваний, безтурботний, неоднозначний, спонтанний, замріяний;
5	Аналітичний	Розумний, прискіпливий, урівноважений, досвідчений, практичний, конкурентний, точний;
6	Гармонічний	Удосконалюється, винахідливий, оригінальний, надзвичайний, товариський, традиційний;
7	Емоційний	М'який, піддатливий, чуттєвий, емоційний, співчуваючий, запальний, захоплений;
8	Цілеспрямований	Рішучий, розсудливий, законослухняний, відповідальний, справедливий, об'єктивний, строгий.

При великому числі вхідних змінних процес побудови нечіткої бази знань стає складним і заплутаним. Це обумовлено тим, що в оперативній пам'яті людини одночасно може утримуватися не більше 7 ± 2 понять, ознак. У зв'язку з цим доцільно провести класифікацію вхідних змінних і по ній побудувати дерево виводу, що визначає систему вкладених один в одного нечітких баз знань меншої розмірності.

Висновки

Розроблено сайт психологічного тестування, розглянуто оцінювання на основі методу Джозефа Лафта та Харрінгтона Інґама а також використання нечіткої логіки для розробки сайту психологічного тестування «Вікно Джохарі».

Система подана у вигляді онлайн-порталу, завдяки чому можна здійснювати доступ до системи з будь-якого комп'ютера, що має доступ до інтернету.

На відміну від аналогічних систем, програмний продукт має адміністративну панель, де адміністратор може здійснювати корективи в існуючих тестах та створювати нові. База даних системи зберігає детальну інформацію про проходження опитування.

Список використаних джерел:

- 1.Noogenesis article on the Johari Window [Electronic resource] — Access mode: http://www.noogenesis.com/game_theory/johari .
- 2.Online Johari Window tool [Electronic resource] — Access mode: <http://www.wdcb.ru/mining/book/cap4.html#4.3.1> .
- 3.Сілагін О.В., Евтушенко В.В. Ідентифікація кольорових відтінків із застосуванням апарату нечіткої логіки // Збірник праць Десятої Міжнародної науково практичної конференції «Інтернет-Освіта-Наука» (ІОН-2016). – Вінниця: ВНТУ, 2016. – С. 50 – 51.
- 4.І. Арсенюк, О.Сілагін, С.Кукунін. Застосування апарату нечіткої логіки для оцінки якості графічних растрових зображень. // Збірник праць Дев'ятої Міжнародної науково практичної конференції «Інтернет-Освіта-Наука» (ІОН-2014). – Вінниця: ВНТУ, 2014. – С. 223 – 225.

ОСОБЛИВОСТІ РЕАЛІЗАЦІЇ ПРОГРАМНИХ ПРОДУКТІВ (ДОДАТКІВ) НА БАЗІ БЛОКЧЕЙН ТЕХНОЛОГІЇ

Марков Дмитро, Сілагін Олексій

Вінницький національний технічний університет

Анотація

У даній статті розглянуто технологію блокчейн і реалізацію програмних продуктів на цій технології. Визначимо, які саме додатки можуть бути створені, переваги і недоліки їх використання, схему їх роботи і правильного функціонування. Також потрібно приділити увагу і дослідити їхньому захисту, конфіденційності і проблемам безпеки.

Abstract

The article discusses the technology of blocks and implementation of software products on this technology. Determine which applications can be created, the advantages and disadvantages of their use, the scheme of their work and the proper functioning. It is also necessary to pay attention and to investigate their protection, confidentiality and security issues.

Вступ

Особливості реалізації програмних продуктів(додатків) на базі блокчейн технології. Основна «фішка» blockchain — можливість створювати на його базі не лише щось, пов'язане із криптовалютами, а будь-який сервіс, ця технологія лежатиме в його основі. На даний момент, для цього найкраще підходить блокчейн Ethereum. Платформа Ефіріум об'єднує потужності комп'ютерів, щоб її користувачі могли створювати на відповідній основі свої додатки. Ці програми, по суті, є сукупністю алгоритмів — смарт-контрактів. Блокчейн гарантує їх безпеку та незмінність, а валюта Ефір — слугує своєрідним паливом для їх запуску і роботи

Результати дослідження

Блокчейн — спеціальна структура для запису групи транзакцій. Транзакція при цьому здійснюється лише тоді, коли вважається підтвердженою. Це зручно і надійно, якщо йдеться про здійснення платежів чи передачу конфіденційних даних. Аби транзакція вважалася достовірною («підтвердженою»), її формат і підписи мають бути перевірені. Після цього групу транзакцій записують в спеціальну структуру (так званий блок). В цих блоках інформацію можна швидко перевірити. А ще в кожному наступному зберігається інформація про попередній. При операціях із криптовалютами, наприклад, у ланцюжку блоків міститься інформація про всі вчинені коли-небудь операції з біткойнами[8].

В блок входять заголовок та список транзакцій. Заголовок блоку включає в себе свій хеш, хеш попереднього блоку, хеши транзакцій та додаткову службову інформацію. Першою транзакцією в блоці завжди вказується отримання комісії, яка стане нагородою користувачеві за створений блок. Для проведення транзакцій в блоці використовують деревоподібне хешування, аналогічне формуванню хеш-суми файлу в протоколі BitTorrent (тому самому, який використовується в роботі торент-трекерів). Транзакції, крім нарахування комісії за створення блоку, містять всередині атрибута input посилання на транзакцію, за якою на цей рахунок були отримані біткойни (або інші дані чи цифрові валюти). Комісійні операції можуть містити в атрибуті будь-яку інформацію (для них це поле носить назву Coinbase parameter), оскільки у них немає батьківських транзакцій. Створений блок буде прийнятий іншими користувачами, якщо числове значення хешу заголовка дорівнює або нижче певного числа, величина якого періодично коригується[9].

Оскільки результат хешування (функції SHA-256) непередбачуваний, немає алгоритму отримання бажаного результату, окрім випадкового перебору. Якщо хеш не задовольняє умову, то довільно змінюється блок службової інформації в заголовку — і хеш перераховується. Після співпадиння варіантів вузол розсилає отриманий блок іншим підключеним вузлам, які перевіряють блок. Якщо помилок немає, то блок вважається доданим в ланцюжок і наступний блок повинен включити в себе його хеш. А тоді все починається спочатку[10].

Величина цільового числа, з яким порівнюється хеш, коригується через кожні 2016 блоків. Заплановано, що вся мережа буде витрачати на генерацію одного блоку приблизно 10 хвилин, на 2016 блоків — близько двох тижнів. Якщо 2016 блоків сформовані швидше, то мета трохи зменшується і досягти її стає важче, в іншому випадку мета збільшується. Зміна складності обчислень не впливає на надійність криптовалют (наприклад, Bitcoin) і потрібна лише для того, щоб система генерувала блоки майже з постійною швидкістю незалежно від потужності.

Найчастіше умисна зміна інформації в будь-якій з копій бази або навіть в досить великій кількості копій не буде визнана істинною, оскільки не відповідатиме правилам. Деякі зміни можуть бути прийняті, якщо будуть внесені в усі копії бази (наприклад, видалення кількох останніх блоків через помилку в їхньому формуванні). Як бачите, такий підхід робить blockchain дуже захищеним способом генерування та передачі даних чи коштів через будь-які канали інтернет-з'єднання.

Маніпулювання даними в блокчейні(Ethereum) забезпечується так званими розумними контрактами (smart contracts). Вони описують які дані зберігати на блокчейні й набір функцій для операцій над ними. Виконання функцій і отримання доступу до даних здійснюється через надається кожним контрактом інтерфейс. Цей інтерфейс генерується з вихідного коду окремо від компіляції і дозволяє виконувати бінарний код. Дані для учасників мережі відкриті, і читання їх нічого не варто, адже як уже було сказано, дані зберігаються у всіх учасників мережі. Зміна даних відбувається за допомогою транзакцій. Кожну транзакцію можна уявити структурою такого вигляду:

- Одержувач транзакції;
- Цифровий підпис відправника;
- Кількість валюти, що відправляється;
- Довільні дані (необов'язково);
- Ліміт газу на транзакцію;
- Ціна за одиницю газу.

Виконання транзакцій вимагає витрат внутрішньої валюти і очікування коли черговий створений майнером блок з вашої транзакцією включиться в загальну ланцюжок. Код контракту виконується на комп'ютері майнера, у віртуальній машині EVM, а в нагороду майнер отримує комісію[7].

Основні переваги смарт-контрактів:

- Автономність (для укладення та підтвердження угоди не потрібно шукати посередника в особі брокера, банку, нотаріуса тощо. д.);
- Надійність і безпека (багаторазово продубльований контракт зберігається в зашифрованому вигляді в блокчейні;
- Безпека системи гарантується математичними законами і робить практично неможливим хакерські атаки, а також підміну інформації заднім числом;
- Економія і швидкість - завдяки блокчейну усуваються багато посередників і автоматизуються процеси;
- Точність - завдяки автоматизації і мінімізації ручної роботи знижується ймовірність помилок, які часто з'являються при заповненні форм в процесі узгодження і при ручному проведенні різних операцій за контрактом[7].

Недоліки:

- Недостатньо розвинута інфраструктура та можливі критичні помилки в самому коді;

- Багато «пробілів» в нормативно-правовому регулюванні;
- Менш гнучкі, ніж звичайні контракти (оскільки ті дані, що потрапили в блокчейн вже неможливо далі змінити) [7].

Висновки

Отже, провівши дослідження можна бачити, що блокчейн технологія швидко розвивається і має дуже високий потенціал, також додатки на базі цієї технології (смарт-контракти) мають багато переваг і сфер застосувань, і після видалення недоліків стануть ще кращі і перспективніші у застосуванні.

Список використаних джерел:

1. Ashton K. That Internet of Things / K. Ashton // Thing. RFID Journal, 22 July 2009. [Electronic resource]. – Mode of access <http://www.rfidjournal.com/articles/view?4986>.
2. Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015. [Electronic resource]. – Mode of access <http://www.gartner.com/newsroom/id/3165317>.
3. Shancang Li. The internet of things: a survey / Li Shancang, Li Da Xu, and Shanshan Zhao // Information Systems Frontiers 2015, 17.2. – Pp. 243-259.
4. Whitmore Andrew. The Internet of Things – A survey of topics and trends / Whitmore Andrew, Anurag Agarwal, and Li Da Xu // Information Systems Frontiers 17.2, 2015. – Pp. 261-274.
5. Dorri, Ali. Kanhere, and Raja Jurda / Ali Dorri, S. Salil // Blockchain in internet of things: Challenges and Solutions" arXiv preprint arXiv:1608.05187, 2016.
6. Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. [Electronic resource]. – Mode of access <https://bitcoin.org/bitcoin.pdf>.
7. Christidis Konstantinos, Michael Devetsikiotis. Blockchains and Smart Contracts for the Internet of Things. [Electronic resource]. – Mode of access <http://ieeexplore.ieee.org/iel7/6287639/6514899/07467408.pdf?arnumber=7467408>.
8. Brody, Paul. Device democracy: Saving the future of the Internet of Things / Paul Brody, Pureswaran Veena // IBM, September, 2014.
9. Veena P. Empowering the Edge-Practical Insights on a Decentralized Internet of Things. Empowering the Edge-Practical Insights on a Decentralized Internet of Things / P. Veena, S. Panikkar, S. Nair, P. Brody // IBM Institute for Business Value, 17 Apr. 2015. [Electronic resource]. – Mode of access <http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?infotype=PM&subtype=XB&htmlfid=GBE03662USEN#loaded>.
10. Boohyung Lee. Blockchain-based secure firmware update for embedded devices in an Internet of Things environment / Lee Boohyung, Lee Jong-Hyouk. The Journal of Supercomputing, 2016. – Pp. 1-16.
11. Ferrer E.C. The blockchain: a new framework for robotic swarm systems. arXiv preprint arXiv:1608.00695, 2016.
12. Bahga Arshdeep. Blockchain Platform for Industrial Internet of Things / Bahga Arshdeep, Vijay K. Madiseti // Journal of Software Engineering and Applications. – 2016. – № 9. – Pp. 533-546.
13. Мельник А.О. Кіберфізичні системи: проблеми створення та напрями розвитку // Вісник Національного університету "Львівська політехніка". – Сер.: Комп'ютерні системи та мережі. – Львів : Вид-во НУ "Львівська політехніка". – 2014. – № 806. – С. 154-161.
14. Andreas M. Antonopoulos. Mastering Bitcoin: unlocking digital cryptocurrencies. "O'Reilly Media, Inc.", 2014. – 298 p.



ОДИНАДЦЯТА МІЖНАРОДНА КОНФЕРЕНЦІЯ
ІОН - 2018
ІНТЕРНЕТ-ОСВІТА-НАУКА-2018



**СЕКЦІЯ F. ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА
ІНТЕРНЕТ У НАВЧАЛЬНОМУ ПРОЦЕСІ ТА
НАУКОВИХ ДОСЛІДЖЕННЯХ**



THE ELEVENTH INTERNATIONAL
CONFERENCE
IES-2018
INTERNET-EDUCATION-SCIENCE - 2018



**SECTION F. INFORMATIONAL TECHNOLOGIES
AND INTERNET IN EDUCATION PROCESS AND
SCIENTIFIC RESEARCH ACTIVITIES**



ОДИНАДЦАТАЯ МЕЖДУНАРОДНАЯ
КОНФЕРЕНЦИЯ
ИОН-2018
ИНТЕРНЕТ– ОБРАЗОВАНИЕ – НАУКА 2018



**СЕКЦІЯ F. ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ
ТА ІНТЕРНЕТ В
ОБРАЗОВАТЕЛЬНОМУ ПРОЦЕСІ І НАУЧНИХ
ІССЛЕДОВАНИЯХ**



ЗАСТОСУВАННЯ МЕТОДУ ДИХОТОМІЇ ДЛЯ ПОБУДОВИ МАТЕМАТИЧНОЇ МОДЕЛІ АДАПТИВНОГО ТЕСТУВАННЯ

Пікуляк Микола

ДВНЗ «Прикарпатський національний університет імені Василя Стефаника»

Анотація

Розглянуто проблеми тестового контролю знань у сучасних навчальних системах; запропонована інформаційна технологія побудови моделі адаптивного тестування із застосуванням методу дихотомії; визначено переваги запропонованого методу під час організації та проведення адаптивного навчання.

Abstract

The problems of test control of knowledge in modern educational systems are considered; the information technology of constructing an adaptive testing model with the use of the dichotomy method is proposed; the advantages of the proposed method during the organization and implementation of adaptive training are determined.

Вступ

Проблема об'єктивного визначення рівня знань студентів є однією з найважливіших задач побудови навчальних траєкторій у сучасних адаптивних навчальних системах.

Особливу увагу при цьому приділяють розробці нових інформаційних технологій для комп'ютерного тестування знань студентів, в основі яких лежать різного роду математичні методи збору й обробки результатів тестування, а також сучасні технології обробки інформації.

У даний час існує безліч найрізноманітніших математичних моделей і підходів, що використовуються для дослідження процесу контролю знань. Вони спираються на різні розділи математики, зокрема теорію ймовірностей, математичну статистику, теорію графів, теорію нечітких множин і нечітку логіку, теорію прийняття рішень і дослідження операцій, комбінаторну топологію та теорію фракталів і багато іншого [1].

Тому актуальною є задача подальшого дослідження методик комп'ютерного адаптивного тестування та розробки інструментальних засобів, що дозволяють якісно реалізувати навчальний процес із використанням сучасних інформаційних технологій.

Побудова математичної моделі встановлення рівня знань студента

Метод дихотомії відомий в першу чергу як метод пошуку і широко використовується в математичному аналізі, криптографії, при одновимірних оптимізаціях, тощо.

У тестовому контролі він застосовується до тих випадків, коли число рівнів складності наборів тестових завдань задається формулою $2^p - 1$, де p – натуральне число.

Будемо вважати, що в навчальній системі використовується сукупність добре прокаліброваних тестів [2], які пронумеровані в порядку зростання їх ваги (складності). При цьому вага $(N + 1)$ -го тесту настільки більша від ваги N -го тесту, наскільки вага N -го тесту більша за вагу $(N - 1)$ -го тесту.

Тоді алгоритм застосування методу дихотомії буде складатись із наступних процедур:

1) У занумерованій множині тестів потужності $2^p - 1$ вибирають тест із номером $N = 2^{p-1}$ середнього рівня складності. Цей тест розбиває всю множину тестів на

дві різні групи: множину тестів меншої ваги (із номерами меншими за $N = 2^{p-1}$), яку назвемо лівою множиною тестів та групу тестів більшої ваги (із номерами більшими за $N = 2^{p-1}$), яку назвемо правою множиною тестів (рис. 1).

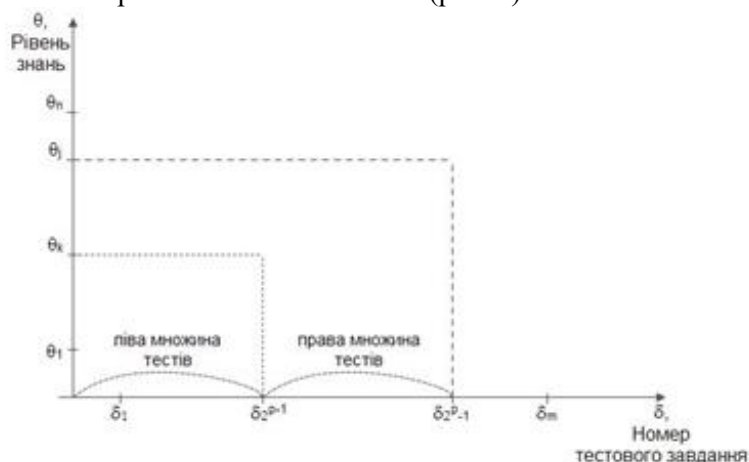


Рисунок 1 – Математична модель методу дихотомії

2) Проводиться тестування за тестом середньої ваги із номером 2^{p-1} . Якщо стовідсоткове успішне проходження тесту оцінюється параметром c , то розглядають три інтервали: $\left[0, \frac{c}{2} - \varepsilon(c)\right]$, $\left[\frac{c}{2} - \varepsilon(c), \frac{c}{2} + \varepsilon(c)\right]$, $\left[\frac{c}{2} + \varepsilon(c), c\right]$, де $\varepsilon(c)$ – деяке достатньо мале значення параметра (похибка), що залежить від c .

3) У випадку, коли оцінка s проходження тесту середньої ваги належить до першого інтервалу (лівого), переходять до розгляду лівої множини тестів меншої ваги, тобто до множини потужності $2^{p-1} - 1$. Якщо ж оцінка проходження тесту середньої ваги належить до третього інтервалу (правого), то розглядають праву множину тестів більшої ваги, яка має таку саму потужність що й ліва множина. Таким чином, в обох випадках переходять до тестування за тестом середнього рівня ваги, який у випадку лівої множини матиме номер $N - 2^{p-2}$, а у випадку правої множини – номер $N + 2^{p-2}$, тобто по суті переходять до п.1). Якщо ж оцінка s належить до другого (середнього інтервалу), то переходять до п.4.

4) Вважають, що рівень засвоєння знань θ відповідає тесту із знайденим номером (ваги) δ , відповідно до шкали логітів (рис. 1) і зупиняють роботу алгоритму.

Використання запропонованого методу дозволяє:

- мінімізувати кількість проведених тестувань для визначення поточної оцінки рівня вмінь та навичок студента;
- підвищити точність оцінки рівня знань сильних і слабких студентів завдяки використанню більшого банку запитань різного рівня складності;
- підвищити якість знань студентів за рахунок подачі на повторне чи поглиблене вивчення тих інформаційних одиниць, які найбільш повно відповідають прогалинам у знаннях студента з обраної тематики.

Список використаних джерел:

1. Загребельний С. Методи адаптивного тестування знань студентів / С. Загребельний, О. Загребельна, О. Костіков. – Педагогічні науки: теорія, історія, інноваційні технології, 2016. – № 3 (57). – С. 376-384.
2. Федорук П. І. Адаптивна система дистанційного навчання та контролю знань на базі інтелектуальних Інтернет-технологій: Монографія / П. І. Федорук. – Івано-Франківськ: Видавничо-дизайнерський відділ ЦІТ Прикарпатського національного університету імені Василя Стефаника. – 2008. – 326 с.

НАУКА В ІНФОРМАЦІЙНОМУ СУСПІЛЬСТВІ: ПРОФІЛІ НАУКОВЦІВ ТА АКАДЕМІЧНІ МЕРЕЖІ

Семигіна Тетяна

Академія праці, соціальних відносин і туризму

Анотація

Визначено характеристики ідентифікаторів науковців (Google Scholar, Scopus, ResearcherID, ORCID), які свідчать про публікаційну активність, та наукових мереж (Academia, Figshare, ResearchGate), які є платформами для оприлюднення наукових робіт. Обговорено мотивацію до ведення наукових профілів.

Abstract

Characteristics of academic profiles (Google Scholar, Scopus, ResearcherID, ORCID) that show publishing activity, and academic networks (Academia, Figshare, ResearchGate), which are platforms for the publication of scientific papers are defined. The motivation for conducting scientific profiles is discussed.

Вступ

У сучасному світі набули поширення академічні наукові мережі, відбувається рейтингування науковців та навчальних закладів за рівнем цитованості їхніх наукових праць. Це привертає увагу до можливостей наукових профілів та наукових мереж у розвитку потенціалу науково-педагогічних працівників.

Ця розвідка має на меті визначити ключові характеристики наукових ідентифікаторів (Google Scholar, Scopus, ResearcherID, ORCID) та наукових мереж (Academia, Figshare, ResearchGate), охарактеризувати мотивацію до ведення наукових профілів.

Основні результати

Існують різні наукові профілі та ідентифікатори науковців. Як вони формуються?

В певних базах даних вони формуються автоматично – при публікації навіть однієї статті (Author ID у Scopus).

Scopus AuthorID – це унікальний ідентифікатор автора в Scopus. Представлена наступна інформація: варіанти імені автора, місце роботи (афіліація), кількість публікацій, роки публікаційної активності, галузь досліджень, співавтори, загальна кількість цитувань автора, індекс Гірша автора тощо. На певний профіль можливо підписатися й відстежувати публікаційну активність науковця. Оскільки інформація генерується автоматично, то у певного науковця може виявитися два профілі в Scopus, особливо за умови різної транслітерації прізвища.

В інших базах наявні спеціальні інструменти для реєстрації профілю та коренування даних (ResearcherID у Web of Science, ідентифікатор ORCID, авторський профіль у Google Scholar,) тощо.

ResearcherID – система однозначної ідентифікації авторів, створена компанією Thomson Reuters для використання у наукометричній базі Web of Science. Ця система покликана вирішити проблему прив'язки автора до конкретної публікації.

ORCID – це 16-значний числовий код, погоджений із стандартом ISO (ISO 27729). Він відображається як адреса: <http://orcid.org/xxxx-xxxxxxxx-xxxx>. Цей ідентифікатор створює сам автор і стежить за наповненням профілю. Проте він може бути прив'язаний до Scopus. Подання ORCID ID вимагають чимало журналів при публікації рукопису або його можуть вимагати при заповненні заявок на наукові гранти.

Профіль Google Scholar є частиною пошукової системи Google. Ця пошукова платформа індексує повний текст наукових публікацій усіх форматів та дисциплін, дає змогу авторам стежити за цитованістю власних публікацій або цитованістю певного автора, стежити за певною тематикою, побачити свій коефіцієнт Гірша тощо. Профіль може бути закритим (доступним лише власнику) і відкритим (тоді він буде відображатись у пошуку за іменем людини). Якщо профіль є відкритим і прив'язаним до університетської адреси автора, то такий профіль береться до уваги під час визначення рейтингу університетів за індексом цитованості (Webometrics). У Google Scholar публікаційна активність автора представлена найбільш широко. Проте, оскільки профіль формується автоматично, у ньому може бути чимало помилок і далеко не всі автори витрачають час на «вичищення» свого профілю, підтримання його в актуальному стані.

Наукові профілі та ідентифікатори, започатковані видавництвами (Scopus, ResearcherID), дають змогу журналам побачити всі публікації авторів, зв'язатися з ними, зрозуміти рівень цитованості конкретного автора чи окремої статті. Видавництва надсилають інформацію щодо публікацій того чи іншого автора до бази ORCID.

Ці профілі корисні університетам, адже вони дозволяють відстежувати інформацію щодо науково-педагогічних працівників, формувати звіти щодо наукової діяльності. Для бібліотек спрощується процес каталогізації за авторами. У організацій, які надають гранти, з'явилась можливість побачити перелік публікацій певного автора та отримати ним гранти. Наукові співтовариства можуть побачити публікаційну активність своїх членів чи потенційних учасників конференцій.

Окрім наукових ідентифікаторів можливо ще ведення наукових профілів у наукових мережах (Academia, Flagshare, ResearchGate).

Academia (<http://www.academia.edu>) – наукова мережа, зареєструватись у якій може будь-хто. Вона дозволяє викладати будь-які опубліковані та неопубліковані праці, презентації, тексти лекцій абощо, стежити за певними авторами чи конкретними науковими темами (дослідницькими інтересами). Якщо автор викладає повнотекстовий файл, то він доступний для завантаження читачами. Важливою функцією цієї наукової мережі можна вважати обговорення чернетки рукопису із закритою групою або певними особами, змогу прямої комунікації з певним автором.

Figshare (<http://www.figshare.org>) – платформа для накопичення наукових, академічних текстів. На ній можуть зберігатись як чернетки та робочі матеріали (у закритому, доступному лише власнику форматі), так і опубліковані праці у відкритому доступі. Наявна можливість побачити, скільки читачів було у публікації.

ResearchGate (<http://www.researchgate.net>) – наукова мережа, зареєструватись у якій можна тільки з університетської або службової адреси. У ній автори інформують про свої публікації – з викладенням тексту чи без нього, проекти тощо. Система дозволяє стежити за певними авторами чи конкретними науковими темами (дослідницькими інтересами). Особливістю цієї мережі є можливість поставити публічне питання й отримати відповідь від колег. Система генерує власний коефіцієнт Гірша, рейтингує науковців, зокрема, за статистикою перегляду в межах навчального закладу.

Узагальнено характеристики наукових профілів представлено в табл.1.

Дослідження засвідчують, що тексти, викладені у наукових мережах, можуть мати вищий рівень цитованості [3], хоча деякі з науковців вважають сумнівним вплив он-лайн профілів на ступінь використання наукових документів [1; 6] та якість показників цитованості [4].

Ефективне використання науковцями нових онлайн-можливостей сприяє популяризації результатів досліджень і вищих навчальних закладів. Більше того використання науковцями Інтернет-інструментів зумовило розвиток нових галузей знань, зокрема вебометрії, яка вивчає інформаційні ресурси за допомогою бібліометричного та інфометричного підходів [2; 5].

Таблиця 1. Характеристики наукових профілів та академічних мереж

	Цитування	Додавання назви роботи	Додавання файлу /лінку	Пошук	Стеження за іншими	Питання, консультація
Scopus	+	+ (статті у цій базі)		+		
ResearchID			+ (лінк на ORCID)	+		
ORCID		+	+ (лінк на веб-ресурс)	+		
Google Scholar	+	+		+	+	
Academia		+	+ (файл)	+	+	+
Figshare			+ (файл, лінк)	+		
ORCID		+	+ (лінк)	+		
ResearchGate	+	+	+ (файл)	+	+	+

Ведення наукових профілів, підтримання їх в актуальному стані потребує часових ресурсів і певних навичок, а в деяких випадках (як-от у випадку ResearchGate.net) ще й базового знання англійської мови. Проте науково-педагогічні працівники можуть бути зацікавлені у веденні наукових профілів, бо це дає їм такі можливості, як: поширення власних досліджень і матеріалів, наприклад навчальних; відстеження використання досліджень; отримання актуальної інформації стосовно роботи колег; розбудова власної наукової репутації; налагодження зв'язків та співпраці; піднесення рейтингів закладів.

Таким чином, наукові профілі та академічні мережі є не лише практикою видавництва та вимогою певних організацій, а й сприяють розвиткові науковців, забезпечують їх актуальною інформацією про роботи колег, надають змогу отримати зворотний зв'язок та наукову консультацію.

Список використаних джерел:

1. Назаровець С. Вплив відкритого доступу на цитованість робіт молодих українських науковців // Вісник Книжкової палати. 2015. № 2. С. 24-28.
2. Bornmann L., Thor A., Marx W., Schier H. The application of bibliometrics to research evaluation in the humanities and social sciences // Journal of the Association for Information Science and Technology. 2016. URL: <https://doi.org/10.1002/asi.23627>
3. De Bellis N. Bibliometrics and Citation Analysis: From the Science Citation Index to Cybermetrics. Lanham: Scarecrow Press, 2009. 450 p.
4. Halevi G., Moed H., Bar-Ilan J. Suitability of Google Scholar as a source of scientific information and as a source of data for scientific evaluation – Review of the Literature // Journal of Informetrics. 2017. Vol. 11(3), P. 823-834.
5. Leydesdorff L., Wouters P., Bornmann L. Professional and citizen bibliometrics: complementarities and ambivalences in the development and use of indicators – a state-of-the-art report // Scientometrics. 2016. Vol. 109(3), P. 2129-2150.
6. Mas-Bleda A., Thelwall M., Kousha K., Aguillo I. F. Do highly cited researchers successfully use the social web? // Scientometrics. 2014. Vol. 101(1). P. 337–356.

АНАЛІЗ ВІТЧИЗНЯНОГО ДОСВІДУ ВИКОРИСТАННЯ ХМАРО ОРІЄНТОВАНИХ ТЕХНОЛОГІЙ У НАВЧАЛЬНОМУ СЕРЕДОВИЩІ ВИЩИХ НАВЧАЛЬНИХ ЗАКЛАДІВ

Гайдаш Богдан

Інститут інформаційних технологій НАПН України

Анотація

У статті розглядаються погляди сучасних вітчизняних науковців що до використання хмаро орієнтованих технологій у процесі навчання студентів вищих педагогічних навчальних закладів України. Оглянуто короткі характеристики та можливості окремих хмаро орієнтованих сервісів що широко використовуються у процесі навчання.

Abstract

The article considers the views of modern domestic scientists on the use of cloud-based technologies in the process of teaching students of higher educational institutions of Ukraine. The short characteristics and possibilities of individual cloud-based services that are widely used in the learning process are reviewed.

Вступ. Підготовка сучасного спеціаліста, який матиме необхідні знання, вміння та навички для роботи та самореалізації у сучасному інформаційному суспільстві вимагає якісної підготовки.

Вищий навчальний заклад повинен готувати таких фахівців, які в своїй подальшій трудовій діяльності могли б використовувати сучасні інформаційні технології та засоби для розв'язання повсякденних завдань що будуть виникати перед молодими спеціалістами не лише на перших етапах професійної діяльності, а і в подальшому розвитку і вдосконаленні своїх знань та навичок.

Поступовий перехід від звичайних засобів наочностей до використання ІКТ, комп'ютерних програм та хмаро орієнтованих сервісів має суттєві позитивні аспекти.

Виклад основного матеріалу. Питання та методику використання хмаро орієнтованих сервісів у ВНЗ розглядали такі вчені: В.Ю. Биков, О.М. Спірін, М.П. Шишкіна, Т.А. Вакалюк, С.Г. Литвинова, А.М. Стрюк.

Однак у сучасному науковому світі все більшого вирішення потребує проблема наявності спеціальних методик використання хмаро орієнтованих технологій у процесі навчання студентів математичних спеціальностей вищих навчальних закладів. Тому доцільно проаналізувати вітчизняний досвід використання хмаро орієнтованих технологій у навчальному середовищі вищих навчальних закладів.

Сучасний етап розвитку суспільства характеризується суттєвим розширенням масштабів наукових досліджень і різноманітних розробок, що проводяться зараз практично у всіх галузях суспільства та на всіх його рівнях. На цій основі змінюються вже існуючі та утворюються нові високоінтелектуальні та високопродуктивні засоби людської діяльності, альтернативні засоби добування та перетворення енергії, удосконалюються різні системи управління та керування соціально-економічними та матеріально-технічними процесами. Не винятком є і система освіти. Спираючись на вже існуючі здобутки в галузі освіти і науки, створюються все нові і нові засоби та системи організації діяльності що базуються на високотехнологічних платформах та їх використання у різних сферах людського існування, адже для того щоб підготувати компетентного спеціаліста, який зможе жити, навчатися, працювати, збагачувати свої знання, розширювати вміння та здобувати нові навички роботи у сучасному інформаційному світі, потрібні нові системи навчання та виховання підростаючого покоління.

Сьогодні в Україні та за її межами багато вчених працюють над зміною існуючих та написанням нових методик навчання та виховання учнів та студентів в умовах сучасного суспільства, та використанням у такому навчанні новітніх комп'ютерних технологій.

Так С.Г. Литвинова вважає що з розвитком сучасних технологій навчання вчителів все складніше стає підтримувати постійний інтерес учнів до процесу навчання. Адже нині основна увага приділяється результатам освітньої діяльності, які передбачають у собі формування в учнів особистісних якостей і загальної культури, розуміння важливості та цінності освіти і відповідальності за свій освітній розвиток. Тому при організації навчання у сучасній школі мають бути прийняті до уваги не лише сучасні тенденції розвитку новітніх технологій в освіті, а й відповідно вимоги сучасного інформаційного суспільства до якості освітніх послуг що надаються освітніми закладами [5].

За означенням О. Г. Глазунова, одним із найефективніших методів виконання даного завдання цілком можна вважати використання ІКТ та інших електронних засобів у процесі навчання та виховання учнів сучасних загальноосвітніх закладів освіти [3].

Використання ІКТ, хмаро орієнтованих сервісів та інших мультимедійних засобів наочності дозволяє не лише урізноманітнити навчальний процес, а й збільшити увагу та цікавість учнів до навчально-виховного процесу, критично та нестандартно мислити, підвищувати свій інтелектуальний рівень та розширювати власний світогляд. Хмаро орієнтовані сервіси дають можливість створити таке навчальне середовище, що забезпечує використання сучасних методів навчання, використання мультимедійних наочностей, презентацій та навчального відео для кращого засвоєння навчального матеріалу учнями з різних навчальних предметів, а зокрема з предметів математичного циклу під час пояснення тем що потребують глибокого абстрактного мислення.

Литвинова С.Г. вважає що поряд зі стрімким розвитком ІКТ та хмаро орієнтованих навчальних середовищ, розвиваються також можливості що до реалізації спільної роботи учня та учителя. Технології що використовуються у хмаро орієнтованих середовищах для активізації навчальної діяльності учнів у процесі навчання – перевернуте навчання[5].

«Перевернуте» навчання –це технологія навчання, у якій передбачається, що учні за допомогою різноманітних персональних гаджетів, мають доступ до «хмари», у середовищі якої вони можуть переглядати відеоуроки з окремої теми, вивчати додаткові матеріали тієї чи іншої тематики, а потім всі разом обговорювати отримані знання та навички, роль вчителя полягає у допомозі засвоєти вже набуті навички. Така організація навчання спонукає учнів навчатися в самих себе[5].

У сучасному світі люди для повноцінного життя та діяльності повинні «встигати» за науково-технічними та соціально-економічними змінами у суспільстві, що з кожним роком невпинно крокують вперед. Відповідно до цього з'являється гостра потреба постійного переосмислення та переглядання відомих знань та отримання нових знань про сучасні засоби, системи та технології. На думку В.Ю. Бикова саме такий шлях обрала Україна, який детальніше описаний у «Стратегії інноваційного розвитку України на 2010-2020 роки»[1].

Вакалюк Т.А. розглядаючи хмаро орієнтовані технології навчання вважає що найбільш поширеними є хмарні сервіси Microsoft Live@edu, за допомогою яких користувачі мають змогу вивчати на практиці поширені офісні додатки через звичайний браузер, також використовувати e-mail, календарі, проводити віртуальні конференції, віртуальну дошку та розробку і редагування веб-сайтів. Основними інструментами сервісу Google Apps Education Edition виступають: електронна пошта з можливістю голосового та відео чатів, календар та хмарне сховище що дає можливість зберігати власні файли із можливістю керування правами доступу до них[2].

Різні аспекти впровадження хмаро орієнтованих технологій в навчання розглядалися вченими. На їх думку використання таких технологій в навчальному процесі має великий ряд переваг, основними з яких є спільний доступ до файлів, навчання з будь-якого місця, жоступність, відкритість, створення власного навчального

середовища. Також суттєвою перевагою є те, що студент не прив'язаний до одного робочого місця чи одного персонального комп'ютера, адже всі виконані завдання зберігаються у хмарному сховищі, доступ до яких можна отримати із будь-якого гаджета що підключений до глобальної мережі Інтернет.

О.М. Спірін та М.П. Шишкіна досліджуючи сучасну тенденцію розвитку можливостей хмаро орієнтованих технологій акцентують увагу на різноманітності та складності системи електронного навчання [6]. Це в свою чергу відкриває нові можливості у процесі вибору, систем чи сервісів що будуть використовуватися у процесі навчання. Але в час такого різноманіття електронних систем навчання постає проблема вибору інформаційної платформи для коректного використання її у процесі навчання. Для того щоб зробити правильний вибір стосовно використання системи, її ефективність та доступність, на перший план постає проблема оцінки засобів інформаційної системи та її наповненість.

Також предметом багатьох вітчизняних досліджень є проблема оцінювання навчання з використанням сучасних інформаційних технологій. Ця проблема стосується всіх сфер навчально-наукової діяльності. Існують безперечно і проблеми, які виникають під час реалізації контролю знань з використанням комп'ютера. О.М. Спірін вважає що існує проблема у ризику раптової відмови обладнання, досить високої вартості локальних серверів, які здатні давати доступ до системи контролю одночасно великій кількості користувачів та проблема опанування даної системи викладачами і студентами [6].

Аналізуючи вітчизняний досвід використання хмаро орієнтованих технологій у навчальному процесі можна з впевненістю сказати, що хмаро орієнтовані технології широко використовуються в навчальному процесі як вищих так і загальноосвітніх навчальних закладах. Але існує ряд причин, які певною мірою перешкоджають їх використанню в процесі навчання, серед яких можна відзначити відсутність необхідної кількості персональних робочих комп'ютерів, наявність коректного програмного забезпечення. Це питання потребує більш ґрунтовного дослідження як вітчизняного сучасного досвіду використання хмаро орієнтованих технологій так і закордонного, виявлення кращих прикладів програмного забезпечення та систем електронного навчання.

Список використаних джерел:

1. Биков В. Ю. Інноваційний розвиток засобів і технологій систем відкритої освіти / В. Ю. Биков. // Сучасні інформаційні технології та інноваційні методики навчання в підготовці фахівців: методологія, теорія, досвід, проблеми. – 2012. – №29. – С. 37–49.

2. Вакалюк Т. А. Можливості використання хмарних технологій в освіті / Тетяна Анатоліївна Вакалюк. // Актуальні питання сучасної педагогіки. Матеріали міжнародної науково-практичної конференції (м. Острог, 1-2 листопада 2013 року).. – 2013. – №1. – С. 97–99.

3. Глазунов О.Г. Теоретико-методичні засади проектування та застосування системи електронного навчання майбутніх фахівців з інформаційних технологій в університетах аграрного профілю : дис. докт. пед. наук : 13.00.10 / . – Київ, 2015. – 545 с.

4. Литвинова С. Г. Поняття та основні характеристики хмаро орієнтованого навчального середовища середньої школи / Світлана Григоріївна Литвинова. // Інформаційні технології і засоби навчання: електронне наукове фахове видання.. – 2014. – С. 26–41.

5. Литвинова С. Г. Технології навчання учнів у хмаро орієнтованому навчальному середовищі загальноосвітнього навчального закладу / Світлана Григоріївна Литвинова. // Інформаційні технології і засоби навчання. – 2015. – №3. – С. 49–66.

6. Спірін О. М. Проблеми інформатизації освіти України у контексті розвитку досліджень оцінювання якості засобів ІКТ / О. М. Спірін, М. П. Шишкіна, Ю. Г. Запорожченко. // Інформаційні технології і засоби навчання. – 2012. – №1. – С. 29–38.

СПОСОБИ ВІДБОРУ ДАНИХ ДО JAVASCRIPT СЦЕНАРІЮ ПОБУДОВИ ДІАГРАМИ

Качурівська Ганна, Качурівський Володимир

Відокремлений підрозділ Національного університету біоресурсів і природокористування України
«Бережанський агротехнічний інститут»

Анотація

Розглянуто питання відбору числових даних із незалежних носіїв даних для автоматизації побудови діаграм засобами CANVAS API. Подано фрагмент Javascript коду відбору даних із зовнішнього файлу. Реалізовано метод відбору даних з рядка та стовпця таблиці даних, вкладеної в HTML-сторінку.

Abstract

Issues of numerical data selection from independent data carriers for automation diagrams construction by means of the CANVAS API are considered. The fragment of data selection code from an external file is given. The data selection method from a row and a column of a data table embedded in the HTML page is implemented.

Вступ

Усе частіше в аналітичних матеріалах сайтів використовують супровід числових даних їх візуальним поданням (інфографіка) за допомогою різного роду графічних об'єктів, призначених для швидкого та доступного сприйняття усієї інформації комплексно. Одним із засобів створення інформаційної графіки є побудова діаграм засобами CANVAS API.

Постановка практичної проблеми

У публікаціях Danny Goodman [3] та Володимира Дронова [5] розглянуто питання створення комп'ютерної графіки в HTML-документах за допомогою CANVAS. У працях Steve Fulton та Jeff Fulton [2] та Джоша Маріначі [4] детально висвітлено оператори для побудови геометричних фігур, які можна використовувати для комплексної побудови інфографіки. Основи роботи з елементом HTML5 <canvas> описано в публікаціях [1; 6]. На даний час практично відсутні публікації, в яких описані методи та способи адаптації полотна побудови графіки під розміри екрану, а також не розглянуті способи передачі до Javascript сценарію числових даних, на основі яких будується інформаційний графік.

Перелік вирішуваних завдань. Визначити фрагмент коду JavaScript сценарію з побудови діаграми для відбору числових даних із зовнішнього файлу, а також із рядка або стовпця таблиці, вкладеної в HTML-документ.

Виклад суті дослідження

Побудова діаграми засобами CANVAS API здійснюється на основі числових даних, сформованих у масиві, для прикладу data. Спосіб передачі числових даних безпосередньо при виклику JavaScript сценарію має певну незручність, а саме: при зміні числових даних необхідно проводити зміни в записаних параметрах виклику сценарію на нові числові дані в тексті Web-сторінки. Одним із способів вирішити дану проблему є реалізація відбору даних із зовнішнього файлу. Змінивши файл на новий, з актуальними даними, при активізації web-сторінки проводиться зчитування уже нових числових даних та здійснюється відповідна побудова діаграми.

Зосередимо свою увагу на формуванні числового масиву, використовуючи зовнішні джерела даних, який використовується для побудови діаграми.

Відбір числових даних із зовнішнього файлу.

Проаналізувавши різного типу файли збереження даних, зробили висновок, що найпростішим та зручним для формування числових даних є звичайний текстовий файл, створений в будь-якому текстовому редакторі з розширенням txt. Текстовий файл підпорядковується таким правилам запису: числові дані записуються у рядок, між даними ставиться розподільник «пробіл».

Наприклад, файл data.txt має такі числові дані: 20 30 50 40

Заголовок JavaScript сценарію побудови діаграми буде наступним:

function diagram_2(path), де path – формальна змінна, яка прийме значення визначеного шляху доступу до файлу даних при його виклику.

Виклик JavaScript сценарію буде таким: diagram_2('.../data.txt');

Фрагмент коду. Зчитування даних з файлу data.txt проведемо асинхронно за допомогою технології AJAX.

```
var oAJAX= new XMLHttpRequest();  
oAJAX.open("GET",path,false);  
oAJAX.send();
```

Результатом роботи операторів буде тестовий рядок. Для розподілу даних скористаємося функцією split() із вказаним розподільником «пробіл», згідно до формату файлу даних.

```
var arr=oAJAX.responseText.split(' ');
```

Результатом роботи функції буде масив arr із текстовими значеннями.

Для перетворення символьних рядків у числові дані використаємо функції Number та наступну конструкцію.

```
var data=[];var j=0;  
for(i=0;i<arr.length;i++)  
if ( !isNaN(Number(arr[i].innerHTML)))  
    {data[i]=Number(arr[i]);j++;}
```

Кількість переданих числових значень визначається як n=data.length;

Сформований числовий масив data використовується для побудови діаграми.

Відбір числових даних таблиці, вкладки у HTML-сторінку.

Ще одним способом відбору даних для побудови діаграми є використання значень з таблиці, яка розміщена у HTML-документі. Таблиця формується парними тегами <table> </table>, <tr> </tr> та <td> </td>. Для реалізації вибірки числових даних таблиця повинна бути простою (відсутні об'єднання комірок). Також врахуємо такий факт, що перший стовпець або рядок таблиці містять текстові підписи.

Відбір даних з рядка таблиці

Зазвичай джерелом даних для побудови діаграми є певний рядок таблиці. Рядок даних таблиці формується парними тегами <tr></tr> та <td></td>. Таблиця може містити декілька рядків. Для однозначного визначення рядка таблиці з якого необхідно взяти дані для побудови діаграми, доцільно задати ідентифікатор рядка. Наприклад (фрагмент HTML-документа конструювання таблиці):

```
<table>  
<tr id="data1"><td>20</td><td>30</td> <td>50</td><td>40</td>  
</tr> </table>, де data1 – ідентифікатор рядка даних.
```

Заголовок JavaScript сценарію буде наступним:

function diagram_3(id_tr), де id_tr – формальна змінна-ідентифікатор рядка таблиці.

Виклик JavaScript сценарію буде таким: diagram_3('data1');

Фрагмент коду. Вибір числових даних здійснюється такою конструкцією.

```
var data=[];
```

```
var row=document.getElementById(id_tr);
cell = row.getElementsByTagName('td');
var n=cell.length;var j=0;
for(i=0;i<n;i++)
    if ( !isNaN(Number(cell[i].innerHTML)))
        {data[j]=Number(cell[i].innerHTML);j++;}
```

Примітка: `isNaN()` – перевірка чи є вміст комірки числом.

Числовий масив `data` сформований і може використовуватися для побудови.

Відбір числових даних із вказаного стовпця таблиці

Враховуючи тегову структуру побудови таблиці, однозначної ідентифікації стовпця, з якого необхідно взяти дані для побудови діаграми, провести неможливо. Для програмування відбору даних слід скористалися такою гіпотезою:

Із колекції вибраних комірок (за тегом `<td>`) необхідно вибрати кожну k -ту (k – кількість стовпців таблиці) починаючи з n -ої за індексом колекції.

Опишемо гіпотезу, детальніше:

1. Створити колекцію комірок таблиці;
2. Визначити кількість рядків та відповідно кількість стовпців;
3. Запустити процедуру відбору необхідних комірок даних.

Заголовок JavaScript сценарію буде наступним:

```
function diagram_4(id_table,n_coll), де id_table -
ідентифікатор таблиці, яка містить необхідні дані, n_coll - номер колонки, з якої
вибирати числові дані.
```

Фрагмент коду. Вибір числових даних з стовпця здійснюється такою конструкцією.

```
var data_td=document.getElementById(id_table);
var cell=data_td.getElementsByTagName('td');
var n=cell.length;
var row = data_td.getElementsByTagName('tr');
var k=n/row.length;
var data=[];
var j=0;
for(i=n_coll-1;i<n;i+=k)
    if ( !isNaN(Number(cell[i].innerHTML)))
        {data[j]=Number(cell[i].innerHTML);j++;}
```

Числовий масив `data` сформовано.

Висновки. Використання автономних носіїв числових даних дозволяє автоматизувати побудову діаграм для певної множини вхідних даних. Подальшої розробки потребують питання відбору числових даних з файлів формату `csv`.

Список використаних джерел:

1. HTML5 Canvas. URL: <https://www.tutorialrepublic.com/html-tutorial/html5-canvas.php> (дата звернення: 15.01.2018).
2. Steve Fulton, Jeff Fulton. HTML5 Canvas. O'Reilly Media, 2011. 654 p.
3. Д. Гудман, JavaScript и DHTML. Сборник рецептов. Для профессионалов. Москва, 2015. 523 с.
4. Джош Мариначи. Основы рисования. URL: <https://webref.ru/dev/canvasdeepdive/chapter01> (дата звернення: 15.01.2018).
5. Дронов В. HTML 5, CSS 3 и Web 2.0. Разработка современных Web-сайтов. Москва, 2013. 416 с.
6. Элемент Canvas HTML5. URL: [https://msdn.microsoft.com/uk-ua/gg589510\(v=vs.85\)](https://msdn.microsoft.com/uk-ua/gg589510(v=vs.85)) (дата звернення: 21.01.2018).

OPEN SOURCE SOFTWARE TO SUPPORT THE EDUCATION PROCESSES IN SOFTWARE DEVELOPMENT IN POST-SOVIET COUNTRIES

Gakh Dmitri

Institute of Control Systems, Azerbaijan National Academy of Sciences

Abstract

This report considers the advantages, problems and the inevitability of involvement of students studying computer sciences in open source software development projects. The current situation, trends, as well as the case of post-Soviet countries on the example of Azerbaijan are considered.

Аннотация

Данный доклад включает рассмотрение преимуществ, проблем и необходимости вовлечения студентов, изучающих компьютерные науки в проекты разработки программного обеспечения с открытым исходным кодом. Рассматриваются существующая ситуация, тенденции, а также случай пост-советских стран на примере Азербайджана.

Introduction

Long-term sustainability can be considered as a major indicator of quality and health of software systems. Many organisations have requirements for long-term sustainable software systems and associated digital assets. Open Source Software (OSS) has been identified as a strategy for implementing long-term sustainable software systems [1]. For any OSS project, the sustainability of its communities is fundamental to its long-term success [2].

Taking into account that the OSS communities can consist of developers, users, and many other specialists, education of specialists in subjects of OSS support as well as its communities is essential. Teaching students how to participate in OSS projects provides them with meaningful and highly marketable hands-on experience, and potentially helps ensure OSS communities to have a sufficient number of qualified developers to meet their needs [3].

In many cases OSS in education process is considered just as a free tool to use [4][5][6]. Generally, it is a reasonable approach. But in case of teaching subjects relating to software development, OSS should be used not only as tools or libraries, but also as examples of how to implement real projects. Indispensability of OSS implementation in education processes, troubles and approaches of the implementation are in the consideration here on base of teaching experience within post-Soviet countries.

Situation with OSS and education

Experience of teaching programming and study situation in post-Soviet countries show that overwhelming majority of students do not understand well the value of OSS. The only feature of OSS they mentioned in discussions is just free acquisition and use. The root of such limited evaluation of OSS lays in remains of Soviet culture where no institute for intellectual property existed. This fact leads to a cursory consideration of software licenses including its components [5], resulted in absence of knowledge and methodology established by teachers as well as of software development companies.

While software development has been steadily growing in developed countries, the isolation of USSR resulted in the fall behind in software development and education in software related subjects. Although there are single cases of a breakthrough, we cannot speak of a satisfactory situation in these sectors on the whole. Many undeveloped countries (such as Zanzibar) have the similar issues [6].

Prerequisites for development of OSS in education

Software development is one of the cheapest start-ups because everything it requires is a computer, some working space, and power. OSS makes it cheaper because it reduces/eliminates cost for operating system, development tools, and utilities. The two main problems observed in the post-Soviet countries (as well as in Zanzibar) are academic staff resistance to change and little understanding of OSS by educational institutions [6].

This fact means that training the trainers/teachers and motivating them to implement OSS in education in higher extent is a starting condition to train specialists who can be a part of OSS community. In order to initiate and support this process the following facts should be taken into consideration:

- Current OSS growth;
- Motivation of Individuals and Organizations;
- Influence to Economy and Education.

Current OSS growth:

- Corporations and companies contribute to OSS projects;
- Organized programmers' teams are involved in the projects;
- Modern methodologies are used in project management;
- Closed Source Software is turning to Open Source Software (Microsoft, IBM, Oracle, etc.).

Motivation of Individuals:

- Personal enthusiasm, fun;
- Willingness to create something useful and significant for people;
- Improvement of skills, career (becoming a community leader, employment, ...).

Motivation of Organizations:

- Open Source software allows small enterprises to afford innovation;
- Independence on the price and licensing policies of large software companies;
- Good IT specialists are easy to be found in Open Source;
- Opening source code allows gaining the sound reputation among customers and competitors;
- Recognize the values of the Open Source movement;
- Companies want to place source code and skills at the disposal of the Open Source Community and hope that other companies will do the same;
- Companies think that software should not be a proprietary commodity;
- Useful to fix bugs and improve the software;
- Reliability and quality of the Open Source software;
- Allows studying the code written by other programmers and using it for developing new programs and products;
- Allows obtaining products unavailable on the proprietary software market.

Influence to Economy and Education:

- Participation in OSS of universities and companies;
- International participation;
- Participation of trainees add temporary unemployed individuals;
- Use of gained international experience of OSS project management:
 - Bringing more labor force;
 - Lower development cost;
 - Bringing proven business models and technical tools.

Involvement in OSS projects

To become a valuable member of OSS community an individual should be involved in corresponding OSS project in as much extent as possible. Education of students in the way they are practically involved in OSS project can be based on different level of the involvement. This approach is convenient for evaluation of individual's progress and different involvement for different specialties. SSTypesLT Project [7] as an example with seven levels of involvement in OSS was elaborated, including the following stages:

1. Downloading, installation and use of the software. Reporting feedback;
2. Development of documentation, translation;
3. Study of code and documentation;
4. Correction of code;
5. Development of new code;
6. Creating the original project;
7. Introduction and popularizing of the original project.

Results

Involvement of teachers and students in OSS projects is very important and creates ground for sustainable OSS communities as well as improves their skills. This involvement can be in different extent that makes implementation of OSS in education processes smooth and manageable.

Involvement in OSS projects as a part of countries' integration into the world economy is important for developing ones. The detailed analysis should be made to determine the impact of OSS in education [6]. Motivation of individuals and organizations should be considered as the main movers in OSS adoption process.

Acknowledgments

Some information regarding this research was provided by Software Systems Research Group, School of Informatics, University of Skövde.

References:

1. G. Blondelle, P. Arberet, A. Rossignol, B. Lundell, C. Labezin, R. Berrendonner, P. Gauffillet, R. Faudou, B. Langlois, L. Maisonobe, P. Moro, J. Rodriguez, J.M. Puerta Peña, E. Bonnafeous, R. Mueller. Polarsys towards long-term availability of engineering tools for embedded systems. [Text] / Proceedings of the Sixth European Conference on Embedded Real Time Software and Systems (ERTS 2012). - Toulouse, France, 1–2 February, 2012.
2. J. Gamalielsson, B. Lundell. Sustainability of Open Source software communities beyond a fork: How and why has the LibreOffice project evolved ? [Text] / Journal of Systems and Software. - Volume 89, March 2014. : pp. 128–145.
3. B. Morgan, C. Jensen. Lessons Learned from Teaching Open Source Software Development [Electronic resource] / HAL, Sep 2016. <https://hal.inria.fr/hal-01373081>
4. M. O. Arslan. Free and open source software as a public good: Implications for education [Text] / European Journal of Research on Education, 2014. - Special Issue : pp. 158-165. - DOI 10.15527/ejre.201426572
5. D. R. Lipşa, Robert S. Laramée. Open Source Software in Computer Science and IT Higher Education: A Case Study [Electronic resource] / <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.364.4348&rep=rep1&type=pdf> : accessed in March, 2018.
6. A. A. Shaame. The Adoption of Free and Open Source Software in Teaching and Learning: Case Study Zanzibar Education Institutions [Text] / International Journal of Managerial Studies and Research (IJMSR). - Volume 2, - Issue 5, June 2014. : pp. 53-59.
7. D. Gakh. SSTypesLT Project [Electronic resource] / <https://github.com/dgakh/SSTypes> : accessed in March, 2018.

METHODOLOGICAL APPROACH TO THE CONSTRUCTION OF CULTURAL HERITAGE ONTOLOGY

Baeva Desislava, Rashkova Victoria, Ivanov Ivan

Angel Kanchev University of Ruse

Аннотация

Использование онтологий для моделирования исторических знаний является ключевым аспектом интеграции информационных технологий для многих исторических институтов. Авторы статьи подытоживают вывод о том, что для создания онтологии с основами культурно-исторического знания методология METHONTOLOGY является наиболее подходящим методом. Также рассматриваются различные этапы этой методологии.

Abstract

The use of ontologies to model historical knowledge is a key aspect of the integration of the information technologies for many historical institutions. The authors of the article summarize the conclusion that for the creation of ontology with culturally-historical knowledge bases the methodology METHONTOLOGY is the most appropriate method. The different stages of the methodology are also considered.

Keywords: ontology, cultural-historical heritage, methodologies, information system, knowledge

Introduction

Nowadays, it is clear that the use of computer technologies to preserve and promote the cultural and historical heritage for future generations becomes a major goal for many cultural institutions.

Increasing globalization requires the perception of historical memory as a powerful and valuable resource for spiritual survival and sustainable development of our society. In the era of the creation of large multinational organizations such as the European Union, societies are faced with various problems the most disturbing among which are the mixing of cultures and domination of the strongest of them, which often leads to depersonalization / zoning out smaller ethnicities; an increasingly global introduction of English-language words into local languages; loss of national identity at the expense of the modern world trend - a citizen of the world; loss / neglect of ethnic identity at the expense of the national one. In this respect, the preservation of cultural heritage is a sign of a strategically built policy of unification of the nation. The following basic national targets are outlined - identification of cultural values, physical preservation of heritage, use of national wealth.[4][5]

The need to change the ways of integrating and expanding the possibilities of including folklore by practical implementation for the purposes of education in patriotism.

According to eCultValue, a project funded jointly by FP7 [2] of the European Commission, the current areas of development that focus on work with cultural and historical heritage based on ICT are:

- scientific, educational and entertainment applications related to archaeological monuments and objects; interactive games based on collections; Big Data solutions customized for the growing amount of data related to the presentation of cultural and historical heritage; 3D technologies and virtual reality; methodologies to assist in the search and presentation of content; standards for metadata, related data and semantic technologies; language technologies, automated translation and localization - to facilitate the exploitation and valorisation of digital assets of cultural exhibitions online in a global context; creating links to education - learning outside museums, electronic workbooks; interactive online knowledge tests; computer creativity (for example, digital storytelling) and interdisciplinary research.

It is of great importance that technological solutions are compatible with specific scientific profiles and needs. In many cases, decisions are made for other sectors that switch to adapted products for museums and historical research - this trend must be changed and the software product should be set up for the relevant scientific or applied purpose[3].

As a result of the intensive development of ICT, the opportunities for access to publications in the electronic environment have grown rapidly. Global access to information requires the idea of "no walls" libraries. It is now quite possible to navigate not only in the electronic resources of a library, but in all virtual libraries of computer networks. The global users with unlimited access rights, needs a more flexible and open search system. They should not be bound by the strict rules of cataloging and bibliographic standards.

Conceptual software approach to presenting semantic information

Semantic web technologies extend existing data services by enabling data warehouse deployments, creating glossaries of concepts, and setting up data processing rules.[1]

The use of ontologies to model knowledge from specific areas is a key aspect of integrating information from different sources to support collaborative work within virtual communities. Ontologies serve to improve the process of retrieving information and are important for making automated logical conclusions from the knowledge provided. Their popularity is increasing as they offer elegant IT opportunities such as interoperability, information sharing, repeat data usage, etc [7].

Ontologies have a potential for applications that provide a vocabulary for a subject area designed for users and programming systems. They allow the creation of intelligent interfaces. These systems, based on set rules, customize the dialogue with the user on the basis of simple conclusions from the available restrictions on certain properties.

The digitalization of Bulgaria's rich cultural and historical heritage has been the subject of many projects, resulting in the accumulation of a large amount of digital material, the access of which is hampered by the lack of good presentation and structure of the available data.

Sharing common understanding of the structure of information among people and software agents is one of the goals in developing ontologies.

It is widely recognized that building ontologies is an important step in the development of knowledge-based systems. However, there is no clear understanding of the processes of building them. Nowadays, building ontologies is considered rather art, than science. Research in the field is still formal and relies heavily on the expertise gained by the specialists rather than the generalized scientific model.

Procedures for building ontologies include actions that relate to knowledge acquisition, assessment, integration, documentation, and configuration management [6]. They are described in a number of ontology-based methodologies. In our opinion, the methodology describes in the most appropriate way the necessary activities[5]:

(1) Specification: identifying the purpose and scope of an ontology, determining the intended target group of users, scenarios for its use, the degree of formalities required, the scope of the ontology, including a set of terms which are characteristics of the objects.

(2) Acquisition of knowledge: represents the accumulation of knowledge from a given subject area. It runs largely parallel to stage (1).

(3) Conceptualization: Conceptualization reflects human interests and goals, a particular domain can be described and classified differently according to different purposes.

(4) Integration: obtain some homogeneity in ontologies, the definitions of other ontologies.

(5) Performance: it is formally presented in a language.

(6) Evolution: the construction of technical solutions for the assessment of the ontology.

(7) Documentation: documentation that provides detailed and comprehensive information for each phase and the product as a whole. The process also involves adding documents that come from other activities.

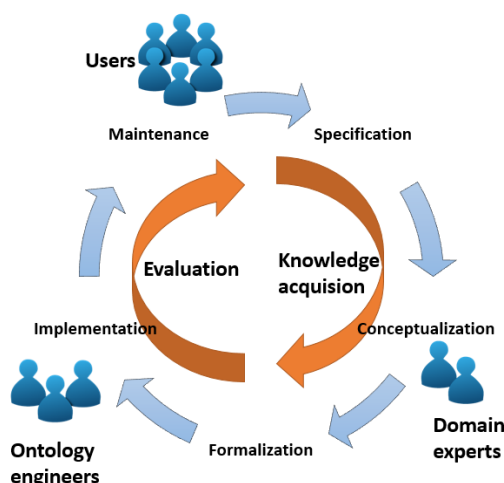


Figure 1. Phases and activities of Methontology and their relation to the actors [8]

Conclusion

The creation of an ontological model with a folklore knowledge base would contribute to preserving and promoting the cultural heritage of each nation.

Each created model is specific, depending on the area of information it represents. This requires different procedures to be used in order to describe it.

It is clear that building ontologies is still a matter of skill and not of the engineering process of their creation. If ontologies need to realize their potential, it is important to take into account the variety of experience available and an appropriate methodology with a clearly defined scope of application.

Acknowledgments

This research was supported by the Bulgarian Science Fund, with the grant for financial support for projects of junior researchers and postdocs, agreement M12.1/2018 „Develop and explore a modern approach to conceptual software presentation of the semantic information stored in the Bulgarian national embroidery“

References

1. Борисова Н., Семантичен уеб- модели и приложения, Югоападен университет „Неофит Рилски“, 2015.
2. Европейска Комисия Изследване на общността, 7РП Утрешните отговори започват от днес (7Рамкова програма) https://ec.europa.eu/research/fp7/pdf/fp7-factsheets_bg.pdf.
3. Златева Р., Религиозно-провиденциалните възгледи в живота на българина езичник (VII-ср. IX в.) Научни трудове на Русенския университет 48 (сер. 6.2), 242-247
4. Стоянов, Св. Бележки върху осигуреността на културното наследство, Известия на съюза на учените – Варна, 2013
5. Cristani, Matteo; CUEL, Roberta. A survey on ontology creation methodologies. International Journal on Semantic Web and Information Systems (IJSWIS), 2005, 1.2: 49-69.
6. Jones Dean, Bench-Capon Trevor, Visser Pepijn, Methodologies for ontology development, 1998, 2014 , <https://cgi.csc.liv.ac.uk/~tbc/publications/itknows.pdf>
7. Navigli R., Paola V., Automatic acquisition of a thesaurus of interoperability terms, Università di Roma “La Sapienza”, 2005.
8. Scherer, Franca, et al. "Similarity as a quality indicator in ontology engineering." Formal Ontology in Information Systems. 2008.

ОСОБЛИВОСТІ ПРОЕКТУВАННЯ ПЕРСОНАЛЬНОГО ОСВІТНЬОГО СЕРЕДОВИЩА В УМОВАХ КОННЕКТИВІСЬКОГО ПІДХОДУ

Ткачук Галина, Стеценко Надія, Стеценко Володимир

Уманський державний педагогічний університет імені Павла Тичини

Анотація

У статті здійснено аналіз теорії навчання в цифрову епоху – коннективізм, яка передбачає організацію навчального процесу у динамічному інформаційному середовищі. Визначено, що навчання на основі коннективізму передбачає формування персонального освітнього середовища, яке являє собою сукупність інформаційних ресурсів, які використовуються суб'єктами навчання з метою отримання знань, стимуляції навчальної активності, розвитку особистісних здібностей, пошуку та опрацювання інформації, комунікації та співпраці.

Abstract

The article analyzes the theory of learning in the digital age – connectivism, which involves organizing the learning process in a dynamic informational environment. It has been determined that training on the basis of connectivism involves the formation of a personal educational environment, which is a set of information resources used by the subjects of learning in order to acquire knowledge, stimulate learning activity, development of personal abilities, data processing and searching, communication and cooperation.

Вступ

Розвиток технологій електронного навчання та активне використання онлайн-засобів сприяло появі нової теорії навчання в цифрову епоху, яка отримала назву коннективізм. Основна ідея цієї теорії є комплексне навчання з базою знань, яка швидко змінюється, з великою кількістю ресурсів та сервісів, які дають змогу упорядкувати, структурувати, представити будь-які дані, а також побудова власних індивідуальних цілей навчання [1, с.147]. Навчальний процес здійснюється у невизначеному та динамічному інформаційному середовищі, яке побудоване на основі штучного інтелекту та створюється за рахунок суб'єктів навчання. Велика кількість інформаційних вузлів дає змогу виходити на більш високий рівень розуміння, отримання нових знань, вмінь, навичок, набуття цінностей тощо.

Окремі питання, що стосуються організації навчання на основі коннективіського підходу розглядалися у працях вітчизняних учених К.Л.Бугайчука, В.М.Кухаренка, М.С.Голованя, П.В.Саварина та зарубіжних Д.Сіменса (G.Siemens), С.Даунса (S.Downes), Д.Кларка (D.Clark) А.В.Калмикова, Є.Д.Патракіна, С.А.Щенникова. Аналіз науково-педагогічної літератури дає змогу зробити висновок, що проблема реалізації коннективіського підходу залишається доволі дискусійною і потребує подальших розвідок. Зокрема, потребує розгляду питання щодо проектування персонального освітнього середовища студента та інтеграції різних інформаційних ресурсів, які дають змогу організувати спільну роботу учасників навчального процесу, реалізувати нові форми взаємодії викладача та студентів, діяти спільно для отримання нових знань та навичок.

Персональне освітнє середовище є невід'ємною частиною освітнього простору суб'єктів навчання і дає змогу організовувати різні види діяльності і форми взаємодії з метою отримання нових знань. Розвиток інформаційних технологій, поява нових та перспективних онлайн-сервісів, заснованих на Веб 2.0., хмарні обчислення сприяли зміні підходів до проектування персонального освітнього середовища. Сучасне персональне освітнє середовище реалізується на базі мережевих технологій та програмних засобів,

використанні спеціалізованих баз даних, електронних освітніх ресурсів та освітніх ресурсів мережі Інтернет. Навчання в освітньому середовищі, що засноване на принципах коннективізму – це активний процес, який може підтримуватись ззовні в умовах об'єднання інформаційних ресурсів, які дають змогу розвиватись та формувати більш високий рівень розуміння та усвідомлення явищ, процесів, об'єктів, що вивчаються.

Створення персонального освітнього середовища можна здійснювати на базі існуючої системи управління навчанням – LMS (переважна більшість навчальних закладів України використовує систему Moodle), яка може бути встановлена на сервері закладу вищої освіти. Така система може інтегрувати в собі навчально-методичне забезпечення дисциплін, електронні навчальні ресурси, зовнішні онлайн-сервіси та ресурси, хмарні обчислення.

Необхідність інтеграції зовнішніх онлайн-сервісів та ресурсів можна пояснити тим, що програмні модулі систем управління навчанням не завжди в повній мірі відповідають основним засадам коннективістського підходу та дуже часто є громіздкими, з великою кількістю налаштувань, незручні у використанні. Впровадження зовнішніх онлайн-сервісів дасть змогу активізувати навчальний процес, реалізувати нові організаційні форми та методи навчання, підвищити продуктивність роботи студентів.

При цьому наявність системи управління навчанням на внутрішньому сервері навчального закладу є обов'язковою, оскільки вона забезпечує персоніфіковану систему доступу до навчання, конфіденційність даних користувача, фактичне оцінювання результатів навчальної діяльності та представляє собою середовище, що інтегрує в собі всі інші можливі засоби здійснення навчальної діяльності. Ресурси, що представлені в системі управління навчанням можна охарактеризувати як систематизоване зібрання інформації та засобів навчально-методичного характеру, необхідних для засвоєння навчальних дисциплін (програм), які доступні через локальну мережу або мережу Інтернет за допомогою веб-браузера та/або інших доступних користувачеві програмних засобів [3].

Персональне освітнє середовище можна визначити як сукупність інформаційних ресурсів (засобів, інструментів, технологій, методів, сервісів, спільнот), які використовуються суб'єктами навчання (студентами) з метою отримання знань, стимуляції навчальної активності, розвитку особистісних здібностей, пошуку та опрацювання інформації, комунікації та співпраці (рисунк 1.).



Рисунок 1 – Модель персонального освітнього середовища

За визначенням Д.Сіменса [5], персональне навчальне середовище не є структурним об'єктом, програмою чи системою управління навчанням. Це своєрідний

набір інструментів, які засновані на концепції відкритості, доступності, здатності до взаємодії учасників навчального процесу та можливістю управління своєю навчальною діяльністю.

Організація персонального освітнього середовища на засадах коннективізму зменшує бар'єри в навчанні і підвищує самостійність студентів, вони набувають навичок отримання знань в результаті спільної діяльності. Таким чином, проектування персонального освітнього середовища на засадах коннективізму повинно відповідати таким вимогами [1, с.78]:

- застосування різних підходів до набуття знань;
- можливість створення мережі зв'язків між різними джерелами навчання;
- діяльнісний підхід до навчання;
- формування здатності будувати мережі знань;
- формування здатності усвідомлення зв'язків між концепціями та ідеями;
- залучення технологій, які допомагають, сприяють у навчанні;

В умовах коннективізму також змінюється роль викладача, який буде освітнє середовище і є «центром кристалізації» навчального процесу [2, с.120]. Його основна функція полягає у тому, щоб організувати та координувати роботу студентів, а знання отримуються ними у процесі виконання різних видів діяльності в персональному освітньому середовищі. Оскільки використовуються різні засоби та технології навчальної діяльності, то викладач також повинен володіти відповідними навичками: 1) письмового та аудіального спілкування; 2) тайм-менеджменту у синхронному та асинхронному режимі спілкування; 3) гнучкої організації індивідуального навчання засобами ІКТ [4, с.64].

Реалізації ідей коннективізму дають змогу спроектувати синергетичну систему взаємодій викладача та студентів для досягнення спільної мети. При цьому система дає змогу працювати як в загальному (зовнішньому) середовищі, так і в персоналізованому. Процес навчання стає більш особистісно-орієнтованим на студента, тоді як викладач виконує роль координатора, помічника у навчанні. Важливу роль в організації навчального процесу відіграє організація персонального навчального середовища учасників навчального процесу, яке створюється з метою отримання нових знань, формування навичок, досягнення цілей навчання.

Список використаних джерел:

1. Головань М. С. Коннективізм – новий підхід до процесу навчання в умовах інформаційно-телекомунікаційних технологій / М. С. Головань // Актуальні проблеми розвитку електронної освіти у вищій школі: Матеріали II Міжнародної науково-практичної конференції 18-20 травня 2012 р. – Х.: ФОП Александрова К. М.; «ІНЖЕК», 2012. – С. 76-78.
2. Кухаренко В. М. Розвиток дистанційного навчання на сучасному етапі / В. М. Кухаренко // Науковий вісник Національної академії статистики, обліку та аудиту. – 2012. – № 2. – С. 117-121.
3. Положення про дистанційне навчання [Електронний ресурс] / Режим доступу: <http://zakon3.rada.gov.ua/laws/show/z0703-13>. – Назва з екрану.
4. Стрюк А.М. Теоретичні основи комбінованого навчання / А.М. Стрюк // Збірник наукових праць Кам'янець-Подільського національного університету. Серія педагогічна / [ред.-кол.: П.С. Атаманчук (голова, наук. ред.) та ін.]. – Кам'янець-Подільський: Кам'янець-Подільський національний університет імені Івана Огієнка, 2011. – Вип. 17: Інноваційні технології управління компетентнісно-світоглядним становленням учителя: фізика, технології, астрономія. – С. 63–66.
5. Siemens George PLEs – I Acronym, Therefore I Exist [Electronic resource] / G. Siemens. – Mode of access: <http://www.elearnspace.org/blog/2007/04/15/ples-i-acronym-therefore-i-exist/>. Last access: 24.03.2018. – Title from the screen.

ВІДТВОРЕННЯ ПРОМИСЛОВОЇ ЕАМ-СИСТЕМИ У НАВЧАЛЬНІЙ КОМП'ЮТЕРИЗОВАНІЙ ЛАБОРАТОРІЇ

Папінов Володимир

Вінницький національний технічний університет

Анотація

Розглянуто питання розробки комп'ютеризованого навчального засобу для практичного вивчення системи автоматизованого обліку та моніторингу промислового обладнання (ЕАМ). Навчальний засіб призначений для використання у лабораторному курсі дисципліни «Інтегровані системи управління», що читається студентам спеціальності "Автоматизація та комп'ютерно-інтегровані технології".

Abstract

The problems of development of the computerized educational tools for a practical studying of the automated system for enterprise asset management (EAM) are considered. The computerized educational means will be used in laboratory course of "Integrated control systems" for students of "Automation and computer-integrated technologies".

Вступ

В наш час під ЕАМ-системою (англ. Enterprise Asset Management, ЕАМ) розуміється комплексна автоматизована система обліку та моніторингу промислового обладнання, яка може також управляти його технічним обслуговуванням і ремонтом [1]. Таку систему у ВНТУ студенти спеціальності "Автоматизація та комп'ютерно-інтегровані технології" вивчають в рамках дисципліни "Інтегровані системи управління", в якій для набуття студентами відповідних професійно-орієнтованих знань та навичок на лабораторних заняттях досліджується реалістична імітація виробничої ЕАМ-системи, яка створена на основі сучасної комп'ютеризованої лабораторії [2].

Матеріали доповіді

Для досягнення поставлених навчально-методичних задач усі програмно-апаратні засоби комп'ютеризованої лабораторії факультету комп'ютерних систем та автоматики ВНТУ були згруповані так, щоб з них формувалась сучасна структура інтегрованої автоматизованої системи управління (ІАСУ) промисловим підприємством. В такій лабораторній імітації ІАСУ чітко виділяються рівні вертикальної інтеграції системи – рівень низової автоматики (DAS, CONTROL), рівень контролерів (DCS), рівень управління технологічними процесами (SCADA), рівень управління виробничими процесами (АСУВ, MES) та рівень управління підприємством (АСУП, MRP). В доповіді запропонований варіант використання програмно-апаратних засобів такої лабораторної ІАСУ для відтворення роботи промислової ЕАМ-системи.

На рисунку 1 показана загальна конфігурація ЕАМ-системи. Як видно з рисунку, усі рівні, крім нижчого, обмінюються інформацією через промислову мережу Ethernet, а загальні дані зберігаються у базі даних реального часу, що працює на сервері системи (DB SQL Server). Програмний модуль "ЕАМ", що розробляється за допомогою "T-Factory 6", отримує дані реального часу або з АРМ операторів, де встановлені SCADA"Trace Mode 6", або безпосередньо з ПЛК, які управляють технологічними об'єктами ТОН₁ – ТОН₄. В ході лабораторних чи практичних занять студенти, використовуючи усі ці програмно-апаратні засоби, розробляють та запускають до дії автоматизовану систему обліку та моніторингу реального промислового обладнання, а саме, промислових датчиків, виконавчих пристроїв та електроприводів, встановлених на ТОН₁ – ТОН₄, а також чотирьох промислових контролерів (ПЛК) та чотирьох АРМ операторів.

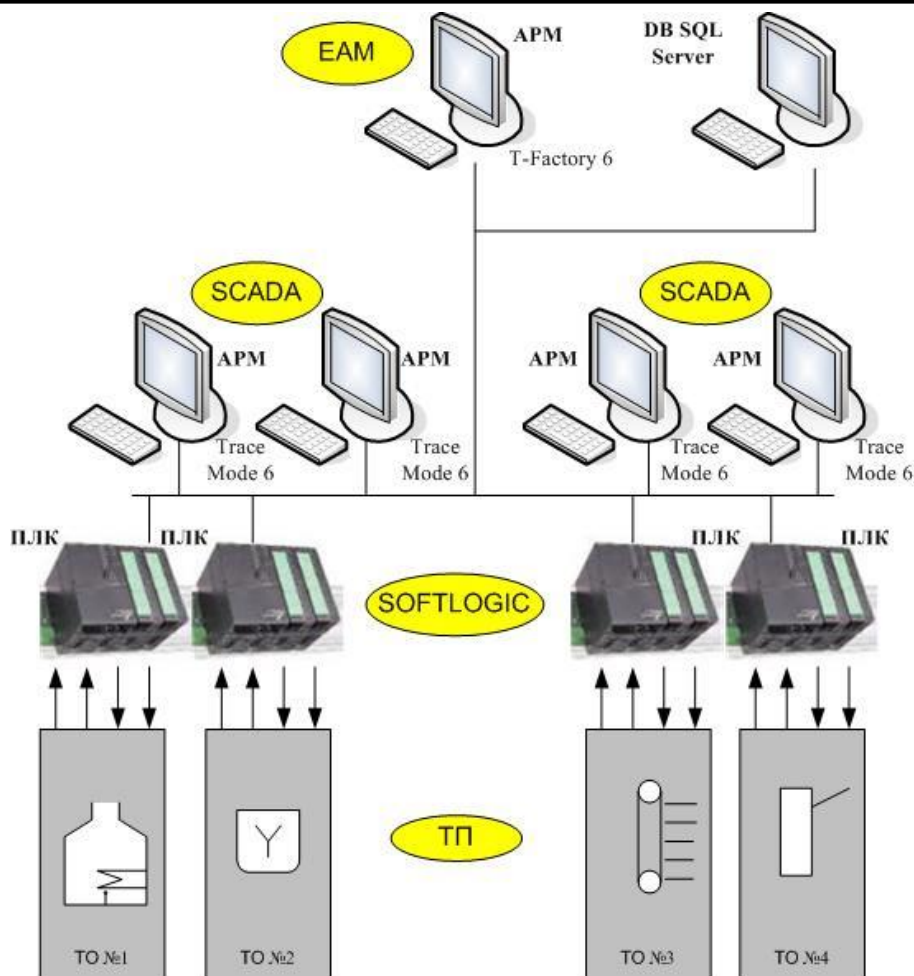


Рисунок 1 – Загальна конфігурація ЕАМ-системи

Запропонована конфігурація ЕАМ-системи дозволяє вивчати такі її функції: виконання паспортизації обладнання; активування регламентів профілактичного техобслуговування (ТО); зв'язування регламентів ТО з інформацією реального часу зі SCADA/HMI (АРМ операторів) і SOFTLOGIC-систем (ПЛК); автоматичне генерування замовлення на матеріали й наряди для ТО; здійснення сіткового планування робіт з ТО; здійснення контролю виконання робіт з ТО; автоматичне генерування звітів й обчислення показників, необхідних для прийняття рішень і т.д.

Список використаних джерел:

1. ЕАМ: системы управления активами повышают надежность и эффективность производства [Електронний ресурс]. – Режим доступу : <http://ua.automation.com/content/eam-cistemy-upravlenija-aktivami-povyshajut-nadezhnost-i-jeffektivnost-proizvodstva>.
2. Бісікало О.В., Биков М.М., Кривоғубченко С.Г., Кулик Я.А., Кучерук В.Ю., Папінов В.М. Багатофункціональний учбовий комп'ютеризований комплекс засобів промислової мікропроцесорної техніки / Збірник тез доповідей третьої міжнародної наукової конференції "Вимірювання, контроль та діагностика в технічних системах (ВКДТС-2015)" (м. Вінниця, 27-29 жовтня 2015 року). – Вінниця: ВНТУ, 2015. – С.152-153 [Електронний ресурс]. – Режим доступу: http://mpa.vntu.edu.ua/images/conference/conf2015/Abstacts_2015.pdf.

ВІДТВОРЕННЯ ПРОМИСЛОВОЇ ММ-СИСТЕМИ У НАВЧАЛЬНІЙ КОМП'ЮТЕРИЗОВАНІЙ ЛАБОРАТОРІЇ

Папінов Володимир

Вінницький національний технічний університет

Анотація

Розглянуто питання розробки комп'ютеризованого навчального засобу для практичного вивчення системи автоматизованої системи управління техобслуговуванням та ремонтом промислового обладнання (ММ). Навчальний засіб призначений для використання у лабораторному курсі дисципліни «Інтегровані системи управління», що читається студентам спеціальності "Автоматизація та комп'ютерно-інтегровані технології".

Abstract

The problems of development of the computerized educational tools for a practical studying of the automated system for maintenance management (MM) are considered. The computerized educational means will be used in laboratory course of "Integrated control systems" for students of "Automation and computer-integrated technologies".

Вступ

Під ММ-системою (від англ. Maintenance Management, MM) розуміється комплексна автоматизована система управління техобслуговуванням і ремонтом (ТОiP), яка відслідковує й управляє обслуговуванням обладнання й інструментів, забезпечуючи планування їх періодичного й попереджувального ремонтів, а також ремонту по стану [1]. Таку систему у ВНТУ студенти спеціальності "Автоматизація та комп'ютерно-інтегровані технології" вивчають в рамках дисципліни "Інтегровані системи управління", в якій для набуття студентами відповідних професійно-орієнтованих знань та навичок на лабораторних заняттях досліджується реалістична імітація виробничої ММ-системи, яка створена на основі сучасної комп'ютеризованої лабораторії [2].

Матеріали доповіді

Усі програмно-апаратні засоби комп'ютеризованої лабораторії згруповані так, щоб з них формувалась сучасна структура інтегрованої автоматизованої системи управління (IACU) промисловим підприємством. В IACU чітко виділяються рівні вертикальної інтеграції – рівень низової автоматики (DAS, CONTROL), рівень контролерів (DCS), рівень управління технологічними процесами (SCADA) та рівень управління виробничими процесами (АСУВ, MES). В доповіді запропонований варіант використання програмно-апаратних засобів IACU для відтворення роботи промислової ММ-системи (рисунок 1). Як видно з рисунку, усі рівні, крім нижчого, обмінюються інформацією через промислову мережу Ethernet, а загальні дані зберігаються у базі даних реального часу, що працює на сервері системи (DB SQL Server). Програмні функції "MM" та "RAS" (Resource Allocation and Status), що розробляються за допомогою "T-Factory 6", отримують дані реального часу або з АРМ операторів, де встановлені SCADA"Trace Mode 6", або безпосередньо з ПЛК, які управляють технологічними об'єктами ТОН№1 – ТОН№3 та настільними спеціалізованими стендами НСС №1, НСС №2. В ході лабораторних занять студенти можуть розробляти та запускати до дії ММ-систему управління ТОiP для ТОН№1 та ТОН№2, НСС №1 та НСС №2, ПЛК №1 – ПЛК №3, АРМ оператора №1 – АРМ оператора №3. Технологічний об'єкт №3 (ТОН№3), який є фізичною моделлю автоматизованого промислового складу, може бути застосований для віртуального зберігання запасних частин для ТОiP, а обліковувати ці запчастини повинна функція "RAS" лабораторної IACU.

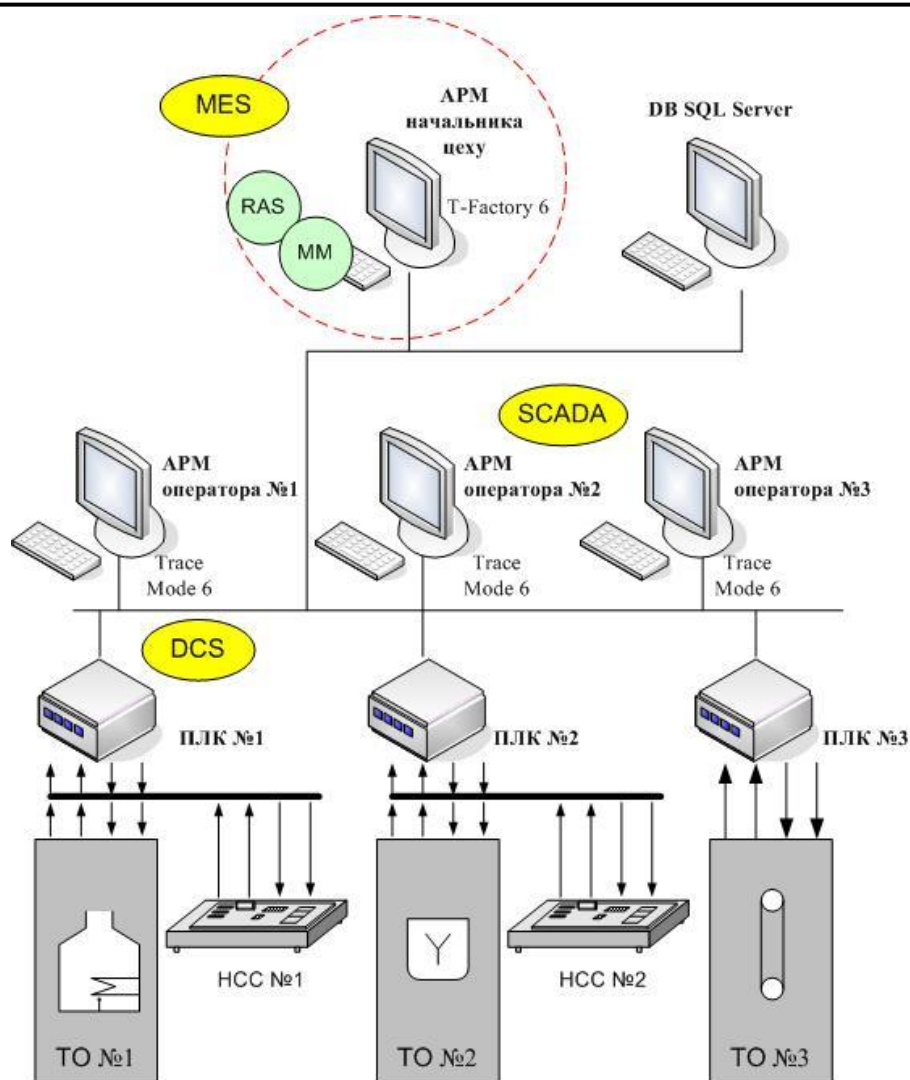


Рисунок 1 – Загальна конфігурація ММ-системи

Запропонована конфігурація ММ-системи дозволяє вивчати такі її функції: планування робіт для ТОіР; автоматичне генерування замовлення на матеріали й наряди на роботи, направлення нарядів їхнім виконавцям; контроль виконання робіт з ТОіР; контроль відповідності часу й вартості виконаних виробничих завдань з ТОіР плановим показникам і т.д.

Список використаних джерел:

1. Кац Б. Информационные системы управления процессами ТОиР и их использование на ранних этапах жизненного цикла предприятия [Електронний ресурс]. – Режим доступу : <http://www.i-mash.ru/materials/automation/10621-informacionnyye-sistemy-upravleniya-processami.html>.
2. Бісикало О.В., Биков М.М., Кривогубченко С.Г., Кулик Я.А., Кучерук В.Ю., Папінов В.М. Багатофункціональний учбовий комп'ютеризований комплекс засобів промислової мікропроцесорної техніки / Збірник тез доповідей третьої міжнародної наукової конференції "Вимірювання, контроль та діагностика в технічних системах (ВКДТС-2015)" (м. Вінниця, 27-29 жовтня 2015 року). – Вінниця: ВНТУ, 2015. – С.152-153 [Електронний ресурс]. – Режим доступу: http://mpa.vntu.edu.ua/images/conference/conf2015/Abstracts_2015.pdf.

PREREQUISITES FOR CREATION AND MAIN IDEAS OF THE SEMANTIC WEB

Федосенко Никита, Груздо Ирина

Харьковский Национальный Университет Радиоэлектроники

Abstract

In this article we will discover how the semantic analysis works, types of semantic search and why we need Semantic Web. Also we will discover the main ideas and building blocks of the Web 3.0 standard, such as Resource Description Framework and Web Ontology Language.

Анотація

У даній публікації ми розглянемо основні моменти роботи семантичного аналізу, види семантичного пошуку і навіщо ж нам потрібна Семантична Павутина. Також ми розглянемо основні ідеї та компоненти стандарту Web 3.0, такі як RDF (середовище опису ресурсів) і OWL (мова опису онтологій).

Introduction

With the increasing amount of textual information, automatic text processing systems are becoming increasingly relevant. The main goal of such systems is the semantic analysis of the text. Semantic analysis of the text evaluates the number of words or phrases that determine the meaning of the text, its semantic core and statistical indicators. The statistical indicators consist of variety of criteria, such as symbols, grammatical errors, unique and meaningful words.

Semantic search is one of the methods of information retrieval and is a process of searching documents by the semantic content. There are two main types of semantic search:

- Full-text search - search through the entire contents of the document using pre-built indexes.
- Searching by metadata is a search for certain document attributes that describe certain objects supported by the system. For example, the author, address, organization name, etc.

Using full-text search is a time-consuming and not optimized solution. The concept of using of metadata search is becoming popular nowadays. Although, this solution has some obstacles on its way. Most of today's Web content is suitable for human consumption. Typical uses of the Web today involve humans seeking and consuming information, searching and getting in touch with other humans. The software tools to support these activities are not particularly well developed; in fact, the main ones remain search engines. Moreover, the technology of these tools remains roughly the same, and Web content outgrows technological progress. In particular, information retrieval is not very well supported. The major obstacle is that, at present, the meaning of the Web content is not machine accessible [1], in the sense that computers cannot interpret words, sentences, and the relationships between them.

The concept of creating a network of websites' metadata was introduced by Tim Berners-Lee, one of the founders of the World Wide Web in 2001. His idea was promoted by the W3C consortium then. This idea was called Semantic Web or Web 3.0. Its main goal was to add some logic to the current Web, express the meaning of the data by a series of formal rules, which would make information accessible to machines. It would give machines the ability to query the data, independent of the form where this data was presented. By the way, the Semantic Web is just an extra layer over the current Web. The semantic web improves web technologies in order to generate, share and connect content through search and analysis based on the ability to understand the meaning of words, rather than on keywords or numbers.

Such solution introduces an extra layer on the top of XML, adding more meaning to encoded information. This layer is represented by Resource Description Framework (RDF), RDF Schema and Web Ontology Language (OWL).

RDF is a description language, which holds the semantics of data represented on the Web. Though, RDF is based on XML, it does not depend on XML syntax, that's a different layer of abstraction. RDF is based on three main concepts: resources, classes and properties. Resources are the describe things e.g. articles, books, authors. All of the resources have unique identifier called Uniform Resource Identifier (URI). Classes are the collections of objects with same properties. And properties describe the relation between classes or resources.

Web Ontology Language (OWL) is a knowledge representation language for authoring ontologies. Ontology itself is a formal naming and definition of the types, properties that really exist in a particular domain of discourse [2]. RDF and Web Ontology Language work together to provide the most precise description of web resources.

Combining this capability with natural language processing, in Web 3.0, computers can understand information like humans in order to provide faster and more relevant results. They become more intelligent to satisfy the needs of users. Also With Web 3.0, information is getting more connected thanks to semantic metadata. As a result, the user experience evolves to another level of connectivity that leverages all the available information.

From a mathematical point of view, the semantic web represents a graph with resources in vertices, and relations between resources in arcs. This global semantic network is a set of subsystems that reflects to some resource, idea or term.

In this publication, we cover the most fundamental concepts and abstracts of semantic analysis, semantic search and have a look on the Semantic Web concept. Also, we have discovered the main techniques of semantic search and building blocks of the Web 3.0 standard. We have learnt about Resource Description Framework language and Web Ontology Language presented by the Semantic Web network. On one hand, the Semantic Web will allow users to talk to machines like to real people, what can make searching of information a lot easier. But on the other hand, this solution requires all of the websites add metadata to be indexed in the Semantic Web. All in all, the Semantic Web seems to be a promising solution for process automation using artificial intelligence.

References:

1. Antoniou G, Van Harmelen F. A Semantic Web primer. Cambridge, MA: MIT Press, Apr 2004. (Preliminary version available at: <<http://www.ics.forth.gr/isl/swprimer/>>. [rev. 3 Jul 2004; cited 25 Apr 2005].).
2. Sowa JF. Knowledge representation: logical, philosophical, and computational foundations. Pontiac Grove, CA: Brooks Cole Publishing Co, 2000. Quoted in: Jacob EK. Ontologies and the Semantic Web. Bull Am Soc Inform Sci Technol. 2003 Apr/May; 29(4):19–22

ОНТОЛОГІЧНА СИСТЕМА КЕРУВАННЯ ОСОБИСТИМИ КАБІНЕТАМИ КОРИСТУВАЧІВ ОСВІТНЬОГО ПОРТАЛУ

Приходнюк Віталій

Інститут телекомунікацій і глобального інформаційного простору НАН України

Анотація

Описується програмна система керування користувачами освітнього порталу на основі онтологій. Основною особливістю системи є онтолого-керованість, тобто всі можливості, права доступу і ролі користувачів задаються з допомогою конфігурації, виконаної на основі онтологій.

Abstract

This paper describes a system, dedicated to managing users of educational portal, based on ontologies. The main feature of the system is that it is ontology-driven, which means that all features, access rights and roles of users are controlled by configuration, based on ontologies.

Сучасні портали є достатньо складними програмними системами, що дозволяють користувачам користуватись широким спектром функцій. Однак, такі системи достатньо важко розробляти, підтримувати і впроваджувати. З часом кількість взаємозв'язків між різними елементами зростає, що негативно впливає на її надійність. Обмежити вплив даного фактору можна створюючи модульні системи, в яких кожен елемент є відносно незалежним. Однак певні взаємозв'язки між модулями мусять існувати, при цьому зі зміною завдань, що стоять перед розробниками порталу, їх склад і структура може істотно змінюватись. Запропонована програмна система вирішує цю проблему з допомогою конфігурації, що створюється на основі онтологій [1, 2].

Інформаційну модель системи представлено сукупністю модулів Π_{R_i} , що інтегрується, які використовуються в процесі роботи порталу:

$$\Pi_R = \sum_{i=1}^n \Pi_{R_i} \quad (1)$$

Онтологічна конфігурація O_C використовується для реалізації відображення G_{Π_R} інтеграції функцій окремих програмних модулів порталу:

$$G_{\Pi_R} : \bigcup_{i=1}^n S_{R_i} \xrightarrow{O_C} F_R \quad (2)$$

Дане відображення перетворює об'єднання множини функцій S_{R_i} кожного з її програмних модулів Π_{R_i} в узагальнену (цільову) функцію F_R – надання інтерактивних веб-сервісів.

Онтологічна модель O_C реалізує в собі функціонально-компонентну модель програмної системи освітнього порталу, що має такий вигляд:

$$S_R = \langle M_D, M_S, M_C \rangle \quad (3)$$

Елементи, що входять в дану модель: M_D – модель, що задає поведінку системи; M_S – модель, що задає структуру системи; M_C – модель (схема) компонентів програмної системи.

Приклад онтологічної конфігурації зображено на Рисунок 1. Така конфігурація включає в себе користувачів, їх ролі, програмні сутності, що зберігають в собі інформацію, і програмні модулі, призначені для її обробки.

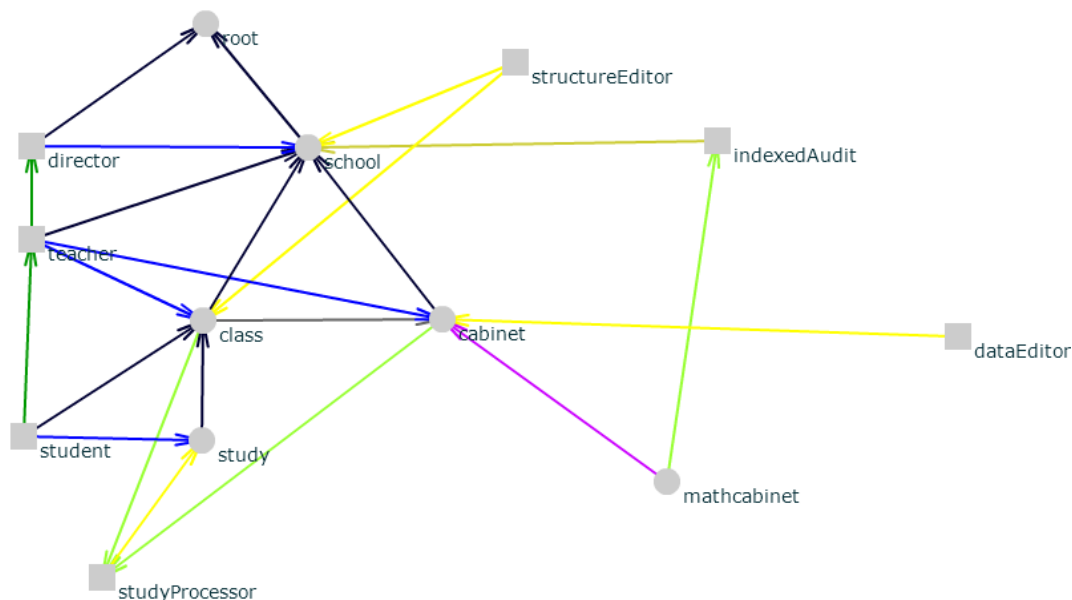


Рисунок 1 – Приклад онтологічної конфігурації порталу

Особливістю системи є те, що роль користувача присвоюється не самому користувачу, а інформаційній сутності (також реалізованій з допомогою онтології). Користувачі зв'язані з онтологіями відношенням «власник», і наслідують роль від них. Тобто якщо існує онтологія типу «клас», то власник даної онтології автоматично отримує роль «класний керівник».

Інформаційні сутності зв'язані також з програмними модулями. Такі зв'язки можуть бути двох типів: «перегляд» і «редагування». Зв'язок інформаційної сутності з програмним модулем означає, що власник інформаційної сутності (або той, кому власник відкрив доступ) може переглядати або редагувати відповідну інформації з допомогою відповідного модуля.

Використання онтологічних конфігурацій дозволяє значно спростити процес розробки порталу, а в подальшому – його модифікацію при зміні вимог до його функціональності, зокрема, при введенні в систему нових ролей користувачів, зміні структури навчального процесу та ін. Використання онтологій в якості власника ролі дозволяє збільшувати гнучкість системи, забезпечуючи простий механізм надання користувачу великої кількості різномірних ролей.

Список використаних джерел:

1. Величко В. Ю. ТОДОС – ІТ-платформа формування трансдисциплінарних інформаційних середовищ / В. Ю. Величко, М. А. Попова, В. В. Приходнюк, О. Є. Стрижак // Системи озброєння і військова техніка. – 2017. – Vol. 1(49). – С. 10–19.
2. Приходнюк В. В. Онтологічне представлення функціональності систем / В. В. Приходнюк, О. Є. Стрижак, О. Г. Лебідь // Екологічна безпека та природокористування. – 2016. – Vol. 3–4 (22). – С. 5–23.

ОСОБЕННОСТИ РАБОТЫ В ЯЗЫКАХ C# / C++ С УКАЗАТЕЛЯМИ И ССЫЛКАМИ В ОБЪЕКТНО- ОРИЕНТИРОВАННОМ ПРОГРАММИРОВАНИИ

Голубь Надежда

Национальный аэрокосмический университет имени Н.Е. Жуковского «ХАИ»

Аннотация

Данная статья на конкретном примере показывает разницу в использовании указателей и ссылок при реализации динамических данных – членов класса при обучении основам объектно-ориентированного программирования на двух популярных алгоритмических языках C# и C++, которые обеспечивают работу с управляемыми и неуправляемыми объектами.

Abstract

This article shows, on a concrete example, the difference in the use of pointers and references when implementing dynamic data-class members when learning the basics of object-oriented programming in the two popular algorithmic languages C# and C++ that provide work with managed and unmanaged objects.

Введение

В алгоритмическом языке C++ есть очень распространенное, эффективное и активно применяемое средство программирования – работа с динамическими переменными посредством использования указателей и ссылок. С помощью оператора new программист помещает такие объекты в «кучу» (heap) и должен сам заботиться о своевременном её освобождении с помощью оператора delete. Это порождает ряд проблем, особенно у начинающих программистов, а также и у более опытных - при использовании наследования и динамического полиморфизма.

Язык C# работает с динамическими объектами в так называемом защищенном (safe) режиме без явного использования указателей и ссылок, организуя с помощью одноименного оператора new размещение объектов в «управляемой куче» (managed heap) [1]. При этом автоматически, по специальным алгоритмам делается анализ и освобождение уже ненужных объектов из «управляемой кучи» - так называемая «сборка мусора».

Постановка задачи

Язык C# при необходимости тоже может работать с указателями и ссылками, но в так называемом незащищенном (unsafe) режиме, сводя к минимуму проблемы с распределением и освобождением памяти, но уже не в управляемой куче, а в стеке. Для этого используется ключевое слово stackalloc, которое является допустимым только для выделения памяти локальным переменным. После выхода из локального блока они автоматически прекращают своё существование, избавляя тем самым программиста от заботы по очистке оперативной памяти.

В качестве базового примера был взят простейший пример вычисления $y = a + b$ на языке C++, причем все переменные динамические и являются членами класса TCalc. Этот пример затем был переписан на язык C#. Это позволило увидеть особенности в реализации, а также в идеях управляемого (язык C#) и неуправляемого кода (unsafe C# и C++), а также некоторые «подводные камни».

Изложение основного материала

Описание основного фрагмента класса для вычисления арифметического выражения (язык C++):

```
class TCalc
{
private:
    // описание динамических данных - членов класса:
    // входные
    int* A;    double* B; // указатели
    // результат
    double* Y;
    void Calc() // функция вычисления y=a+b
    { *Y = *A + *B; } // разыменование указателей
public:
    // Конструктор
    TCalc(int av, float bv)
    // выделение памяти в «куче» и инициализация входных данных - членов класса
    {
        A = new int; *A=av;
        B = new float; *B=bv;
        Y = new double;
    }
    // Деструктор - уничтожение данных-членов класса
    // ОБЯЗАТЕЛЬНОЕ освобождение «неуправляемой кучи»
    ~TCalc()
    { delete A; delete B; delete Y; }
    // Вычисление и выдача результата
    int show ()
    { Calc();
      cout << "\nРезультат y = " << *Y << " по адресу: " << Y << endl;
      return (_getch());
    }
}; // TCalc
```

Фрагмент главной программы:

```
int main()
{ int a = 100; double b = 2.657;
  // Создание объекта
  TCalc Object (a, b);
  // Вычисления и вывод результата
  Object.show();
}
```

Теперь посмотрим, как работу с указателями для данных – членов класса можно реализовать на языке C#. При этом надо обязательно при создании проекта разрешить использование небезопасного кода, а также всюду, где появляются указатели или ссылки в коде, должно быть ключевое слово `unsafe`.

Описание класса для вычисления арифметического выражения (язык C#):

```
unsafe class TCalc
{
    // Исходные данные (поля класса) - УКАЗАТЕЛИ!
    private int* a ;
    private double* b ;
    public unsafe TCalc(int* x, double* y) // Конструктор
    {
```

```
// Но память полям – членам класса в конструкторе НЕ выделяется!!!
a = x; // присваивание АДРЕСОВ исходных данных
b = y;
// Разыменование адресов (поля a и b ПОЛУЧАЮТ значения - инициализация)
Console.WriteLine("\na = {0}, Address = {1:X}", *a, (int)a);
Console.WriteLine("b= {0}, Address = {1:X}", *b, (int)b);
}
private unsafe double Add() // функция вычисления y=a+b
{ return *a + *b; }
public unsafe void Show()
{
    // выделение памяти для ЛОКАЛЬНОЙ ПЕРЕМЕННОЙ (результат) в СТЕКЕ!!!
    double* ans = stackalloc double[1];
    *ans = Add();
    Console.WriteLine("a+b= {0}, Address = {1:X}", *ans, (int)ans);
}
} // TCalc
Фрагмент главной программы:
static unsafe void Main() // режим UNSAFE
{
    int a=100;
    double b=2.657;
    TCalc c = new TCalc(&a, &b); // передача АДРЕСОВ ЛОКАЛЬНЫХ переменных
    c.Show();
    .....
}
```

В С# можно инициализировать указатель, используя и УПРАВЛЯЕМЫЕ элементы: массив, строку, буфер фиксированного размера. Для этого используется оператор `fixed`, который не позволяет сборщику мусора переносить перемещаемую переменную. Оператор `fixed` задает указатель на управляемую переменную и "закрепляет" эту переменную на всё время выполнения оператора. Этот оператор допускается только в небезопасном (`unsafe`) контексте. Без оператора `fixed` указатели на перемещаемые управляемые переменные были бы бесполезны, так как при сборке мусора переменные переносились бы непредсказуемым образом [2].

Выводы

- Язык С# может явно обрабатывать ссылки и указатели только в небезопасном (`unsafe`) режиме.
- При использовании С++ программист сам должен следить за освобождением «неуправляемой» кучи.
- При обучении профессиональных программистов объектно-ориентированному программированию очень важно понимание студентами разницы в обработке динамических данных – членов класса, чтобы избежать трудно понимаемых проблем, связанных с «уборкой мусора» или его накоплением.

Список использованных источников:

1. С#. Руководство по С#. Базовые сведения о времени жизни объектов [Электронный ресурс]. - Режим доступа: [www. URL: https://professorweb.ru/my/csharp/charp_theory/level13/13_1.php](http://www.professorweb.ru/my/csharp/charp_theory/level13/13_1.php) - 2018.
2. Оператор `fixed` (Справочник по С#) [Электронный ресурс]. - Режим доступа: [www. URL: https://docs.microsoft.com/ru-ru/dotnet/csharp/language-reference/keywords/fixed-statement](http://www.microsoft.com/ru-ru/dotnet/csharp/language-reference/keywords/fixed-statement) - 20.07.2015.

УНІВЕРСИТЕТИ У ЦИФРОВУ ЕПОХУ

Буяшенко Вікторія, Семігіна Тетяна

Академія праці, соціальних відносин і туризму

Анотація

Охарактеризовано екзогенні (зовнішні) та ендогенні (внутрішні) чинники впливу інформаційно-комп'ютерних технологій на вищу освіту. Обговорено виклики цифрової педагогіки для сучасних університетів.

Abstract

External and internal determinants of informational and computer technologies impact on the higher education are reviewed. Challenges of the digital pedagogy for modern universities are discussed.

Вступ

Розвиток інформаційно-комп'ютерних технологій (ІКТ) і розвиток університетів, закладів вищої освіти тісно взаємопов'язані. В інформаційному суспільстві впровадження інформаційних технологій слугує ключовим орієнтиром розвитку різних сфер життєдіяльності спільноти, є одним із пріоритетних напрямів піднесення освіти.

У цій роботі розглянуто екзогенні та ендогенні чинники впливу ІКТ на сучасні університети.

Основні результати

В сучасному інформаційному суспільстві змінюються очікування та вимоги до вищої освіти та університетів (в українському нормативному дискурсі – заклади вищої освіти).

Як відзначає Е. Герасимова [3], змінюється характер відносин між наукою, освітою, технікою та виробництвом, а зв'язок між ними вже не може мати лінійного характеру. Авторка пропонує розглядати освіту як складний культурний процес і звертає увагу на необхідність змінити погляд на учня як на суб'єкт виховання та сприймати його як суб'єкта життєдіяльності загалом.

До екзогенних (зовнішніх) чинників впливу ІКТ на сучасні університети віднесемо наступні:

- нові очікування від університетів, зокрема, формування нових компетентностей, потрібних в інформаційному суспільстві, і навичок критичного мислення [4];
- стрімке зростання обсягу знань про суспільство, природу та людину, що можуть бути використані під час навчання
- динамічність знання, появу нових професій і навичок, що зумовлює потребу в отриманні знання впродовж життя [2];
- появу масових он-лайн курсів, які можуть викладатись як на базі певного університету, так і поза ним, але які, за своєю суттю, становлять альтернативу традиційній університетській освіті і кидають їй виклик своїм надкороткими лекціями та інтерактивним спілкуванням учасників [8];
- рейтингування університетів, зокрема, з огляду на їх присутність в Інтернеті та цитованість наукових праць (методологія Вебометрікс);
- посилення контролю за діяльністю закладів вищої освіти (бази даних вступників, бази даних випускників, котрі отримали дипломи; он-лайн інформація щодо ліцензування закладів освіти тощо);
- інтернаціоналізацію освітнього простору та міжнародну мобільність суб'єктів навчального процесу (конференції, фахові форуми, робоче та навчальне стажування, навчання, обмін досвідом).

З-поміж ендогенних (внутрішніх, таких, що стосуються педагогічних технологій) чинників впливу ІКТ на сучасні університети виокремимо наступні:

- зміну форматів заочної освіти, яка перетворюється на дистанційну, підкріплену новітніми технологіями – вебінари, он-лайн лекції;

- використання у педагогічному процесі платформ, що дають змогу оприлюднювати навчальні матеріали, здійснювати контроль знань студентів (як-от MOODLE, Blackboard тощо);

- швидке поширення знань і зростання випадків плагіату (копіпасту), що потребує застосування програм перевірки унікальності текстів; доступ до необмежених навчальних ресурсів створює для студентів спокусу переписувати вже готові реферати, контрольні роботи [5];

- формування у молоді так званого кліпового мислення і нерозвиненість навичок читання довгих текстів.

Науковці [1; 6; 7] ведуть мову про формування цифрової (електронної) педагогіки та трансформацію суб'єкт-суб'єктних відносин у вищій освіті, появу нових стандартів освіти, зміну аксіологічних та праксеологічних підходів до вищої освіти, відзначають, що інформаційні технології позитивно впливають на процес навчання і виховання насамперед тому, що змінюють схему передачі знань і методи навчання. У зв'язку з цим виникає нагальна потреба у прискоренні підготовки викладачів та фахівців у сфері ІКТ, в оснащенні закладів освіти сучасною комп'ютерною технікою, педагогічними програмними засобами, електронними підручниками тощо. Хоча, як звертає увагу А. Олійник [5], впровадження інформаційних технологій як засіб інноваційного розвитку освіти має не тільки позитивне, але й суперечливе значення, оскільки передбачає відмову від науко- та раціоцентризму. Наявне й технічне обмеження: далеко не всі університети спроможні адекватно зреагувати на новітні виклики, забезпечити студентів і викладачів засобами та ресурсами, потрібними для цифрової педагогіки.

Перелічені зміни вимагають від науково-педагогічних працівників не лише комп'ютерної грамотності та вміння використовувати сучасні платформи для поширення знань і власних наукових напрацювань, а й осмислення нових реалій вищої освіти.

Список використаних джерел:

1. Биков В.Ю. Лещенко, М.П. Цифрова гуманістична педагогіка: актуальні проблеми педагогічних досліджень у галузі використання ІКТ в освіті // Інформаційні технології і засоби навчання. 2016. № 3 (53). С. 1-17.
2. Буяшенко В.В. Сталий розвиток і сучасна парадигма освіти // Вісник Академії праці, соціальних відносин і туризму. 2017. №2. С.72-74.
3. Герасимова Е.М. Технологічна реальність масових комунікацій як ресурсна можливість розвитку освіти постмодерну // Вісник НАУ. Серія: Філософія. Культурологія. 2015. № 1 (21). С. 10-15.
4. Курбатов С. Феномен університету в контексті часових та просторових викликів. Суми: Університетська книга, 2014. 262 с.
5. Олійник А.І. Інформаційні технології як основа і засіб реалізації інноваційних процесів в сучасній освіті : автореф. дис. ... канд. філос. наук : 09.00.10. Київ, 2008. 20 с.
6. Позднеев Б.М. и др. Новые горизонты стандартизации в эпоху цифрового обучения и производства // Вестник МГТУ «СТАНКИН». 2015. № 4(35). С. 101-108.
7. Семеног О.М. Академічна лекція і академічний учитель в цифрову епоху: праксеологічний підхід // Фізико-математична освіта. 2017. Вип. 2(12). С. 140-146.
8. Semigina T. MOOCs: A few considerations for/from academia // «Психолого-педагогічні аспекти навчання дорослих в системі неперервної освіти» : м-ли III Міжнар. наук.-практ. інтернет-конф.(30 листопада 2017 р.). Біла Церква : БІНПО ДВНЗ УМО, 2017. С. 372-376.

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ОБРАЗОВАТЕЛЬНОМ ПРОЦЕССЕ ФОРМИРОВАНИЯ САМОСОЗНАНИЯ ГИПЕРАКТИВНЫХ ДЕТЕЙ

Сухомлин Светлана, Шевяков Алексей

Международная академия информационных технологий, Днепровский филиал

Аннотация

Изучение самосознания у детей с гиперактивностью позволяет решить дискуссионные вопросы их самооценки и проявлений защитных психологических механизмов. Разработанные на основе полученных эмпирических данных психокоррекционные мероприятия позволяют значительно снизить степень социальной дезадаптации данной категории лиц.

Abstract

The study of self-awareness in children with hyperactivity allows solving debatable questions of their self-assessment and manifestations of protective psychological mechanisms. Developed on the basis of the obtained empirical data, psycho-corrective measures can significantly reduce the degree of social disadaptation of this category of persons.

Введение

Личностное развитие детей и подростков с расстройствами поведения имеет особенности, затрудняющие их социальную адаптацию.

Трансформация гипердинамических расстройств поведения в психопатоподобные поведенческие проявления, обусловлена сочетанием биологических и социальных факторов. Среди биологических факторов, оказывающих влияние на возникновение девиаций в формировании самосознания детей с гиперактивностью, основным выступает дисфункция лобных долей, в частности проявления так называемой «лобной симптоматики» – недостаточной способности произвольно регулировать свои психические процессы и поведение, что проявляется в расторможенности, импульсивности, эмоциональной лабильности, недостаточной концентрации внимания. Негативная реакция социума на поведение и последующая стигматизация, нарушение детско-родительских и внутрисемейных отношений играют неблагоприятную роль в процессе становления самосознания. Комплекс этих факторов обуславливает проявления девиантного формирования самосознания.

Неблагоприятные условия для развития личности очень часто приводят к различным формам девиантного поведения. Гипердинамические расстройства проявлялись в детстве в 44,1% подростков, совершивших тяжелые уголовные действия[1].

В связи с этим, возникает актуальный вопрос о возможности психокоррекционного воздействия на факторы, лежащие в основе искажений в формировании самосознания у детей с гиперактивностью. Также, учитывая, что лица с поведенческими расстройствами особенно чувствительны к социальным воздействиям, важной задачей становится изучение влияния микросоциального окружения на формирование самосознания и возможностей гармонизации межличностных отношений.

С целью предотвращения возникновения девиаций в процессе личностного развития детей и подростков с гиперактивностью, необходимо уделять особое внимание обучению навыкам оценки своих психических состояний, своих возможностей, предвидению последствий своих действий. Однако, соответствующие

психокоррекционные мероприятия и информационные технологии еще недостаточно разработаны.

Необходимость разработки системы психологической коррекции для раннего пубертатного возраста, обусловлена тем, что хотя основные симптомы синдрома гиперактивности - двигательная расторможенность и проявления когнитивной недостаточности по данным Н.Ю.Максимовой [2] у 55-62% лиц этой возрастной категории в значительной степени редуцируются, психологические проблемы, в частности, аффективные взрывы, происходящие вследствие противоречивой самооценки и недостаточной способности прогнозировать последствия своих действий, имеют тенденцию к увеличению. Это проявляет себя в утяжелении аффективных нарушений, агрессивном поведении и трудностях общения.

Потребность в самоутверждении, становление которой происходит в этот период, при отсутствии соответствующих психокоррекционных вмешательств, также становится причиной развития психопатоподобных форм поведения [3].

Объект исследования: самосознание детей с расстройствами поведения.

Предмет исследования: самосознание детей с синдромом гиперактивности.

Цель исследования: выявить особенности самосознания детей с синдромом гиперактивности и разработать систему психологической коррекции их поведения.

В ходе исследования, была выдвинута гипотеза о том, что у детей с синдромом гиперактивности недостаточность осознания своего опыта, оценки возможностей и прогнозирования последствий своих действий приводят к снижению регулирующей функции самосознания. Развитие самосознания у детей с гиперактивностью может быть обеспечено в ходе психокоррекционных мероприятий, которые решают комплексную задачу развития навыков анализа, планирования и гармонизации межличностных отношений в микросоциальной среде.

Задачи исследования:

1. Обосновать теоретико-методологические основы изучения самосознания у детей с расстройствами поведения.

2. Разработать структурно-динамическую модель самосознания детей и подростков с гиперактивностью.

3. В ходе эмпирического исследования выявить особенности функционирования самосознания детей и подростков с гиперактивностью и выяснить уровень развития рефлексии и способности прогнозировать последствия своих действий.

4. Разработать систему коррекционных мероприятий, направленных на повышение уровня саморегулирующей функции самосознания у детей и подростков с гиперактивностью.

Теоретико-методологической основой исследований является положение общей психологии и психологии личности, касающиеся: онтогенеза, структуры, условий и закономерностей формирования самосознания (Г.С. Костюк, Р. Бернс); принципов компенсации дефекта и осложнения аномального развития вторичными отклонениями в психическом развитии (Л.С. Выготский, В.В. Ковалев, М.М. Семаго); проблем нарушения самосознания при девиантном развитии (Б.С. Братусь, Н.Л. Белопольская, Б.Я. Зейгарник, Н.Ю. Максимова, Е.И. Соколова); особенностей детей с гиперактивностью (Р. Баркли, Е. Меш, Б. Хоза); роли самосознания и рефлексивных процессов в личностном развитии (Л. И. Божович, И.И. Чеснокова, А. Цукерман, А.С. Зак); антиципации как феномена, пронизывающем все уровни психического отражения действительности (П.К. Анохин, И.Г. Батраченко, В.Д. Менделевич); развитие ресурсных возможностей ребенка и подходов к гармонизации семейных отношений (Р. Грин, Р. Брукс, А.С.Кочарян, Н.В.Барина, А.В.Кукуруза).

Для решения поставленных задач и проверки гипотезы были использованы следующие **методы**:

теоретические методы: анализ и обобщение научных данных по проблеме исследования, теоретическое моделирование;

эмпирические методы: изучение медицинской документации, методика Т.В. Дембо-С.Я. Рубинштейн (модификация П.В. Яньшина), методика исследования уровня притязаний Ф. Хоппе (модификация С. Соловьева), «Шкала самоуважения М. Розенберга», «Метаморфозы» в модификации Н.Я. Семаго, М.М. Семаго, «Рисунок несуществующего животного» в модификации Венгера Л.А., модифицированная методика «Изучение системы детских самохарактеристик» В.Г. Щур, методики: экспериментальное задание «Алгоритм действий», «Оценки уровня рефлексии и антиципации», которые включали ряд предложенных ситуаций для обсуждения, анкетирование родителей и методика «Фиксация поведенческих проявлений» для родителей.

Полученные результаты были обработаны статистическими методами с помощью программы SPSS 17.0.

Выводы

1. В ходе теоретического анализа проблемы становления самосознания у детей с гиперактивностью, определено, что самосознание можно рассматривать как динамическую систему, которая состоит из «Я-концепции» и соматического, аффективного, когнитивного и поведенческого компонентов. Их взаимосвязь осуществляется с помощью рефлексии и антиципации, за счет которых происходит осознание своего опыта индивидом и включение его в «Я-концепцию».

2. Девиации в формировании самосознания ребенка гиперактивностью, обусловлены комплексом социальных и биологических факторов. Биологическим базисом девиаций самосознания детей с синдромом дефицита внимания с гиперактивностью, является дисфункция лобных долей, следствием которой является недостаточность произвольной регуляции высших психических функций и когнитивные нарушения, в результате чего формируется недостаточность уровня рефлексии и антиципации. Среди социальных факторов можно выделить нарушение микросоциальных отношений, негативную социальную реакцию на поведение ребенка, негативную оценку его личности со стороны социума, что способствует возникновению внутриличностного конфликта у данной категории детей и появлению неконструктивных защитных механизмов.

3. Установлена значимая корреляция между низким уровнем рефлексии и антиципации с неустойчивостью представлений о себе, конфликтностью самооценки, неадекватностью притязаний, негативным самопредъявлением, наличием аффективных вспышек при неудачах.

Список использованных источников:

1.Максимова Наталія Юріївна. Сімейне консультування: навч. посіб. / Н.Ю.Максимова. – К.:ДП: «Вид. дім «Персонал»,2011. – 304 с. ISBN 978-617-02-0068-6.

2.Максимова Наталія Юріївна. Патопсихологія підліткового віку / Н.Ю.Максимова, К. Л. Мілютіна, В.М. Піскун – Київ: Главник, 2008. – 192 с. ISBN 978-966-8774-46-9.

3.Романчук Олег Иванович. Синдром дефицита внимания и гиперактивности у детей: практ. рук.: пер. с укр. / О. И. Романчук. – М.: Генезис, 2010. – 333 с. ISBN 978-5-98563-204-0.

НАВЧАЛЬНО-ПІЗНАВАЛЬНА ДІЯЛЬНІСТЬ УЧНІВ В УМОВАХ ВИКОРИСТАННЯ ІНТЕРНЕТ ОРІЄНТОВАНИХ ОСВІТНІХ ТЕХНОЛОГІЙ

Пінчук Ольга, Соколюк Олександра

Інститут інформаційних технологій і засобів навчання НАПН України

Анотація

Зміни в освіті обумовлюються деякими суперечностями: на рівні глобального інформаційного простору; на рівні національної освітньої системи; на рівні навчального закладу. На основі комп'ютерно-технологічної платформи сучасної освіти, що набуває ознак відкритої, відбувається трансформація традиційного навчального середовища в середовище комп'ютерно опосередкованої комунікації, у якому й здійснюється навчально-пізнавальна діяльність учнів.

Annotation

Changes in education are conditioned by some contradictions: at the level of the global information space; at the level of the national educational system; at the level of the educational institution. Based on the computer-technology platform of modern education, which acquires characteristics of open, there is a transformation of traditional learning environment into the environment of computer-mediate communication, in which the educational and cognitive activity of students is carried out.

Вступ

Динаміка розвитку факторів зовнішнього і внутрішнього середовища впливає безпосередньо на розвиток інноваційного потенціалу закладів освіти і його реалізацію у навчальному процесі. Це вимагає істотної трансформації системи освіти, заснованої на:

- психолого-педагогічних та дидактичних принципах цифрової освіти;
- нових підходах до відбору змісту освіти;
- принципах гнучкості та адаптивності педагогічних систем;
- принципах рівних можливостей для всіх суб'єктів освітнього процесу;
- нових формах, методах, технологіях та засобах навчання й учіння, що реалізовані у сучасних навчальних середовищах.

Нові риси сучасної освіти, Інтернет орієнтованої, відображають світові тенденції розвитку освітніх систем, передбачаючи комплексне застосування ІКТ під час реалізації навчальної, наукової та управлінської функцій, здійснення взаємозв'язків із оточуючим середовищем, з метою реалізації принципів відкритої освіти.

З Інтернет орієнтованою освітою, на нашу думку, передусім пов'язується розвиток таких її змістово-технологічних складових:

- комп'ютерно орієнтованого навчального середовища;
- локальних і загальнодоступних електронних освітніх ресурсів,
- ІКТ-підтримки функціонування глобального, в у тому числі відкритого, інформаційно-освітнього простору, відкритих ІКТ-орієнтованих педагогічних систем, зокрема електронних соціальних спільнот.

На основі комп'ютерно-технологічної платформи сучасної освіти, що набуває ознак відкритої, відбувається трансформація традиційного навчального середовища в середовище комп'ютерно опосередкованої комунікації. Цьому середовищу притаманні використання розподілених освітніх ресурсів і інфраструктур підтримки освітніх співтовариств різних типів. Значна частина дидактично обґрунтованої і спеціально організованої навчально-пізнавальної діяльності учнів здійснюється в мережі Інтернет і, має специфічні особливості, трансформуючись у сучасну форму навчання в силу ряду чинників.

Пізнавальну діяльність розглядаємо як елемент цілісного процесу навчання, що представляє собою цілеспрямовану, систематично організовану, керовану ззовні або самостійну взаємодію учня з навколишньою дійсністю, результатом якої є оволодіння ним на рівні відтворення або творчості системою наукових знань і способів діяльності. В

процесі навчання пізнання набуває чіткого оформлення в особливій, властивій тільки людині навчально-пізнавальній діяльності, або учінні.

До основних видів навчально-пізнавальної діяльності учнів в Інтернет орієнтованому середовищі відносимо: пошукову діяльність, практичне освоєння нових технологій, створення нового контенту, інтернет-комунікацію в пізнавальних цілях, навчання з використанням інтернет-ресурсів. Форми навчально-пізнавальної діяльності в інформаційно-освітньому середовищі визначаються організацією та/або самоорганізацією інформаційно-комунікаційної взаємодії та інформаційно-пізнавальної діяльності учнів. Формування та сталий розвиток когнітивних (пізнавальних) здібностей у людини протягом усього життя – неодмінний елемент будь-якого освітнього процесу.

Формування ключових компетентностей для навчання впродовж життя [1], зокрема математичної компетентності та компетентності у науках, технологіях та інженерії (Mathematical competence and competence in science, technology and engineering) й цифрової компетентності (Digital competence) [2] можливе на базі сучасних освітніх технологій з використанням засобів інформаційно-комунікаційних технологій, електронних освітніх ресурсів, електронних соціальних мереж, що дозволяють зменшити навчальне навантаження і водночас інтенсифікувати навчальний процес, надаючи навчально-пізнавальній діяльності творчого, дослідницького спрямування. При цьому значно зростають можливості для індивідуалізації і диференціації навчання, формуються навички самоосвіти, метапредметні й предметні уміння, здатності застосовувати отримані знання на практиці тощо.

Результативність навчально-пізнавальної діяльності учнів зокрема визначається новою парадигмою освіти інформаційного суспільства. Зазнає змін весь інструментарій, що дозволяє проводити оцінку і контроль навчально-пізнавальної діяльності. ІКТ і засоби ІКМ формують нові рішення, що можуть впливати на базові процеси в освітній системі: формування та розвиток компетентностей, фіксацію досягнень, оцінку якості навчання, створення позитивної мотивації та стимулювання самостійності у навчально-пізнавальній діяльності.

Інструментами передавання вербальних знань (або самостійне вивчення), невербальних знань за рахунок комунікації з носієм, невербальних знань за рахунок тренування навиків є онлайн мультимедійні бібліотеки, багатокористувацькі онлайн-курси, е-підручники, освітні канали YouTube, предметні блоги, віртуальні наставники, тренажери, віртуальні тренажери, роботи-наставники.

Самостійне здобуття учнями досвіду (випробовування, виконання дослідження або експерименту, творчий індивідуальний або груповий проект) може бути реалізоване в ігрових середовищах, квестах, з використанням доповненої реальності, робо-змаганнях, віртуальних лабораторіях, дискусійних наукових спільнотах, у соціальних мережах та ін.

Інструментами фіксації й оцінювання навчальних досягнень учнів може бути особистий профіль компетенцій, особисте віртуальне портфоліо, створення і стрес-тест віртуального світу або цифрової моделі.

З метою заохочення та мотивування учнів до навчально-пізнавальної діяльності в інтернет орієнтованому середовищі застосовуються змагальні ігрові моделі (гейміфікація), системи управління репутаційним капіталом, превентивне управління результатом (системи прогнозування досягнень), ігрові адаптивні моделі, системи моніторингу стану (що відстежують емоційний стан учнів).

Список використаних джерел:

1. Proposal for a Council recommendation on Key Competences for Lifelong Learning // European Commission. – Brussels, 17.01.2018. – Available at: <https://ec.europa.eu/education/sites/education/files/recommendation-key-competences-lifelong-learning.pdf>. – (accessed 11 February 2018).

2. Annex to the Proposal for a Council Recommendation on Key Competences for Lifelong Learning // European Commission. – Brussels, 17.01.2018. – Available at: <https://ec.europa.eu/education/sites/education/files/annex-recommendation-key-competences-lifelong-learning.pdf>. – (accessed 11 February 2018).

3. Формування інформаційно-освітнього середовища навчання старшокласників на основі технологій електронних соціальних мереж / [В. Ю.Биков, О. П. Пінчук, С. Г. Литвинова та ін. ; наук. ред. О.П. Пінчук] ; Ін-т інформ. технологій і засобів навчання НАПН України. – К. : Педагогічна думка, 2018. – 188 с.

РЕАГИРОВАНИЕ СИСТЕМЫ ОБРАЗОВАНИЯ НА ПОТРЕБНОСТИ РЫНКА ТРУДА (РЕАЛЬНОСТЬ И ПЕРСПЕКТИВЫ)

Хатуна Путькарадзе

Грузинский университет имени Святого Андрея Первозванного Патриаршества Грузии

Аннотация

В работе рассматривается корреляция системы образования и рынка труда. Сферы производства и обслуживания всё больше опираются на цифровые технологии.

В статье предпринята попытка изучить эти вопросы, выявить проблемы и представить рекомендации по их решению.

Abstract

The paper discusses the correlation of the education system and the labor market. Spheres of Industry and Services depend on digital technologies.

The paper tries to explore this and other questions to demonstrate problems and provide recommendations for their solutions.

В результате распада Советского Союза больше всего из секторов образования пострадали профессиональные училища. С 1992 года в Грузии вместе с фабриками и заводами исчезли профучилища.

С 2007 года в рамках Программы по интегрированию национального учебного плана с учебным курсом профессионального образования в более чем 40 общеобразовательных школах в виде пилотных проектов было осуществлено ремесленное образование, ориентированное на рынок труда.

С 2007 года в целях гармонизации системы образования с рынком труда началось создание законодательной базы: был принят Закон о профессиональном образовании; было утверждено Положение Национального профессионального совета по профессиональному образованию (Постановление правительства Грузии №203, 04/11/2009); утверждено Положение о проведении профессионального тестирования; была утверждена Стратегия реформирования профессионального образования (2013 - 2020). На сегодняшний день в Грузии функционирует 67 профессиональных образовательных учреждений. Среди них: 17 авторизованных государственных колледжей, 6 колледжей, учреждённых с долевым участием государства, и 44 авторизованных частных колледжа.

Следует отметить усилия Грузии по развитию цифровых компетенций. С 2004 года Министерством образования и науки Грузии была осуществлена четырёхлетняя программа компьютеризации школ. В настоящее время в Грузии на каждого 20-го учащегося приходится один компьютер. Информационно-коммуникационные технологии позволили установить связи между тысячами школ и гражданами Грузии, благодаря чему они сыграли положительную роль в процессе интеграции страны.

В январе 2016 года недалеко от Тбилиси, в Окрокана, было построено высокотехнологическое пространство – технопарк. Это один из главных проектов ЮЛПП (юридическое лицо публичного права) «Агентство инноваций и технологий», находящегося в ведении Министерства экономики и устойчивого развития Грузии. Одной из главных целей данного проекта является поддержка и развитие инновационного производства.

С 2015-2016 годов Еврокомиссия предприняла кампанию по «повышению осведомлённости в коммуникации»¹. Целью кампании являлось:

1. Диагностирование владения информационными и коммуникативными умениями и навыками;
2. Определение потребностей в их развитии.

¹ <http://www.digitaleurope.org/Our-Work/Projects/Past-projects/eSkills-for-Jobs>

До настоящего времени европейские страны, несмотря на высокий уровень безработицы, испытывают жёсткий дефицит специалистов по информационно-коммуникационным технологиям. Что может быть причиной этому, если не то, что среди европейского населения уровень владения и использования информационно-коммуникационных технологий низок. Причиной этому следует признать также то, что ничто так быстро не устаревает и выходит из употребления, как современная цифровая техника и оборудование. В результате кампании цифровые компетенции населения стран Евросоюза выросли, а количество безработных уменьшилось.

Каковы Статистические данные, отражающие уровень цифровых компетенций в Грузии. У большинства учащейся молодёжи и студентов Грузии цифровые компетенции развиты в недостаточной степени. Интернет ресурсами эффективно пользуется лишь ограниченная часть граждан.

Согласно информации, полученной Институтом развития свободы информации (IDFI) в результате запроса публичной информации у Национальной комиссии коммуникаций Грузии, количество потребителей проводного и беспроводного Интернета в разных регионах и городах значительно различается; в частности, в Тбилиси - 251788 (71%) потребителя, а в 9 других городах вместе взятых - 101864 (29%) потребителя².

В целом, в Грузии количество абонентов проводного Интернета - 392 436, количество же потребителей беспроводного Интернета (Wifi) - 17 872 человек. Получается, что у 17,4% жителей Тбилиси совершенно нет компьютерной техники, а в регионах это число гораздо выше и составляет 27,9%.

Согласно данным Кавказского центра исследовательских ресурсов (CRRC, Кавказский барометр) за 2012 год, основными тенденциями, проблемами и факторами, обуславливающими небольшое количество потребителей Интернета в Грузии, являются: отсутствие в необходимости Интернета для граждан (26,8%), высокая цена компьютерной техники (24,3%), слабая заинтересованность (18,6%) и отсутствие умений, необходимых для использования Интернета (11,7%)³.

В результате анализа графика использования потребителями интернета электронных ресурсов выявляется, что: чаще всего потребители пользуются социальными сетями, занимаются поиском информации и отправляют/получают электронные письма⁴. Следует предположить, что наибольший дефицит цифровых компетенций испытывает безработная часть населения. От безработных никто не требует наличия цифровых компетенций, да и сами они лишены всякой мотивации приобрести соответствующие компетенции. Поэтому безработному не нужны цифровые технологии, соответственно, он и не владеет ими, а в результате, он не представляет никакого интереса для работодателя. Жертвами вот такого порочного круга становятся тысячи трудоспособных граждан в Грузии.

Согласно рейтингу глобальной конкурентоспособности Международного экономического форума за 2017-2018 год, в качестве главного фактора, препятствующего развитию бизнеса в Грузии, названа некавалифицированность рабочей силы. Согласно рейтингу⁵, Грузия по показателям эффективности рынка труда среди 137 стран находится на 67-ой позиции⁶. В результате исследования выявлено, что на рынке труда в Грузии существует высокий спрос на квалифицированные рабочие кадры, однако среди местных человеческих ресурсов наблюдается дефицит квалификации, соответствующей спросу.

Согласно исследованию, наиболее проблемными факторами осуществления бизнеса являются: недостаточное образование трудовых кадров – 17.3%, отсутствие финансовых

² <https://eparticipationge.files.wordpress.com/2013/06/3.png>

³ <https://eparticipationge.files.wordpress.com/2013/06/9.png>

⁴ <https://eparticipationge.files.wordpress.com/2013/06/13.png>; Общее исследование «Развитие электронной коммуникации в Грузии - доступ в Интернет» См.: <https://idfi.ge/public/migrated/uploadedFiles/files/%e1%83%9c%e1%83%a2%e1%83%94%e1%83%9b%e1%83%9d%e1%83%9b%e1%83%ae%e1%83%9b%e1%83%90%e1%83%a0%e1%83%94%e1%83%91%e1%83%94%e1%83%9a%e1%83%97%e1%83%90%e1%83%99%e1%83%95%e1%83%9a%e1%83%94%e1%83%95%e1%83%90.pdf>

⁵ <http://reports.weforum.org/global-competitiveness-index-2017-2018/countryeconomy-profiles/#economy=GEO>

⁶ В рейтинге 2014-2015 гг. Грузия была на 41-м месте.

возможностей – 12.0%, инфляция – 11.0%, низкая трудовая этика местных трудовых кадров – 9.7%, низкий уровень инновации – 9.7%, неэффективная государственная бюрократия – 9.2%, неадекватное снабжение инфраструктуры – 7.3%, политическая нестабильность – 6.5%, нестабильность правительства / переворот – 6.2%, налоги – 3.8%, налоговые регуляции – 1.8%, валютные правила – 1.8%, коррупция – 1.7%, низкое общественное здравоохранение – 1.3%, ограниченные трудовые нормы – 0.7%, воровство и криминал – 0.0.

Анализ вакансий, опубликованных в Грузии в прошлом году, даёт возможность составить список самых востребованных профессий. Среди них: финансист и кредитный эксперт – 20.1%, менеджер по продажам – 18.5%, технический персонал – 13.2%, врач/медицинский персонал – 9.7%, дистрибьютор – 8%, IT менеджер – 7.4%, менеджер различных сфер – 7.2%, учитель, тренер, консультант – 6.4%, туроператор – 3.5%, маркетолог – 3.1%, юрист – 1.9%, инженер – 1%.

Перечень бизнес-секторов, заинтересованных в востребованных профессиях выглядит следующим образом: банковско-финансовый сектор – 26%, розничная торговля – 18%, медицинский сектор/фармация – 15%, гостиница/ресторан/туризм – 17%, коммуникации/транспорт – 9%, строительство – 5%, образовательные учреждения – 7%, медиа – 1%, пищевая промышленность и производство напитков – 2%.

Картирование востребованных профессий по бизнес-секторам выглядит следующим образом: Тбилиси – 77%, Имерети – 5%, Аджария – 4%, Кахети – 3%, Шида Картли – 2.5%, Самегрело – 3%, Квемо Картли – 2.5%, Самцхе-Джавахети – 2%, Гурия – 1%.

Самыми высокооплачиваемыми являются должности банковско-финансового и государственного управления, самой низкооплачиваемой же – профессиональная деятельность в секторе образования.

Избранные проблемы и рекомендации :

Выявленные проблемы	Рекомендации
Система образования Грузии не удовлетворяет потребностям рынка труда.	Причина дисбаланса, существующего между спросом (рынок труда) и предложением (образование): отсутствие информационной карты рынка труда. Необходимо создание информационной карты рынка труда.
В исследованиях по трудовой и социальной защите встречается термин –отчаявшаяся рабочая сила (discouraged worker); это люди, которые не смогли найти работу и потеряли надежду. У безработных которым за 45 нет никакой надежды найти работу.	На самом деле среди них много таких, которые в случае повышения квалификации и переподготовки, при овладении цифровыми компетенциями могли бы стать востребованными на рынке труда. Ведь у большинства безработных данной категории имеется высшее образование.

Таким образом, если данные спроса (рынок труда) и предложения (система образования) будут открытыми, прозрачными, гибкими, многокомпонентными и удобными для использования, потребитель даже с применением элементарных цифровых компетенций сможет сделать необходимый для него анализ. Наличие сбалансированной информации облегчит ему процесс выбора желаемой профессии, планирования карьеры, а также ориентации в последипломном образовании. Для системы образования станет возможным своевременное и правильное реагирование на потребности рынка труда.

Список использованных источников:

1. Турашвили Теона, Развитие электронной коммуникации в Грузии - Доступ в Интернет, т., 2013⁷
2. Altinok Nadir, Human Capital Quality and Economic Growth, 2007, <https://halshs.archives-ouvertes.fr/halshs-00132531v2>
3. Barro Robert J., Education and Economic Growth, Harvard University, London, 2003.

ІННОВАЦІЙНА МОДЕЛЬ «ШКОЛА НОВІТНІХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ»

Лосіцький Володимир

Пальмірська ЗОШ І-ІІІ ступенів Золотоніської районної ради Черкаської області

Анотація

Презентовано досвід закладу загальної середньої освіти щодо створення та впровадження моделі «Школа новітніх інформаційних технологій». Умови інноваційного розвитку: система неперервної освіти в межах суспільно-педагогічного комплексу, ресурсне забезпечення освітнього процесу, залучення хмарних технологій.

Abstract

The experience of the institution of general secondary education on the creation and implementation of the model "School of Advanced Information Technologies" was presented. Conditions of innovative development: a system of continuous education within the socio-pedagogical complex, resource provision of the educational process, attraction of cloud technologies.

Вступ

Інноваційна діяльність школи сьогодні пов'язана із Концепцією Нової української школи, в якій визначено завдання формування інноваційно-цифрової компетентності кожного учня, що передбачає впевнене і водночас критичне застосування інформаційно-комунікаційних технологій для створення, пошуку, оброблення, обміну інформацією [1]. Для розвитку та забезпечення ефективної діяльності закладу освіти необхідно також забезпечити формування цифрової та медіаграмотності учнів і вчителів, сприяти оволодінню ними основами алгоритмізації і програмування, роботі з базами даних, розвивати навички безпечної поведінки в Інтернет, критичного оцінювання веб-ресурсів, а також сформувати розуміння етики роботи з інформацією на основі дотримання авторського права та інтелектуальної власності.

Пальмірська загальноосвітня школа І-ІІІ ступенів стала учасником обласної цільової програми «Інноваційні школи Черкащини». Вона працює в рамках всеукраїнських експериментів з проблем: «Хмарні сервіси в освіті» (2014-2017 рр.), «Технологія навчання початкової школи «Розумники» (2017-2022 рр.) й набула статусу експериментального навчального закладу регіонального рівня за темою «Реалізація моделей перспективного розвитку інноваційних шкіл Черкаської області» (2017-2020 рр.). Школа отримала в 2017 році почесне міжнародне звання «Microsoft Showcase School» – «Зразкова школа Microsoft». Особливістю «Зразкових шкіл Microsoft» є повна й глибока реалізація у навчальному плані закладу принципів цифрової освіти, персоналізоване навчання, акцент на точних науках, активне використання комп'ютерно орієнтованих технологій, проектування сучасного інформаційно-освітнього середовища і STEM-освіта.

Саме сучасні технології управлінської та навчально-пізнавальної діяльності забезпечують змістове наповнення розробленої й упровадженої педагогічним колективом Пальмірської загальноосвітньої школи інноваційної моделі «Школа новітніх інформаційних технологій» (рис. 1). Модель орієнтована на забезпечення педагогічно виваженого використання можливостей інформаційно-освітнього середовища задля розвитку всіх суб'єктів навчально-виховного процесу.

Використання хмарних технологій у процесі управління закладом загальної середньої освіти створює можливості мати доступ до комп'ютерних ресурсів сервера та використання програмного забезпечення як онлайн-сервісу.

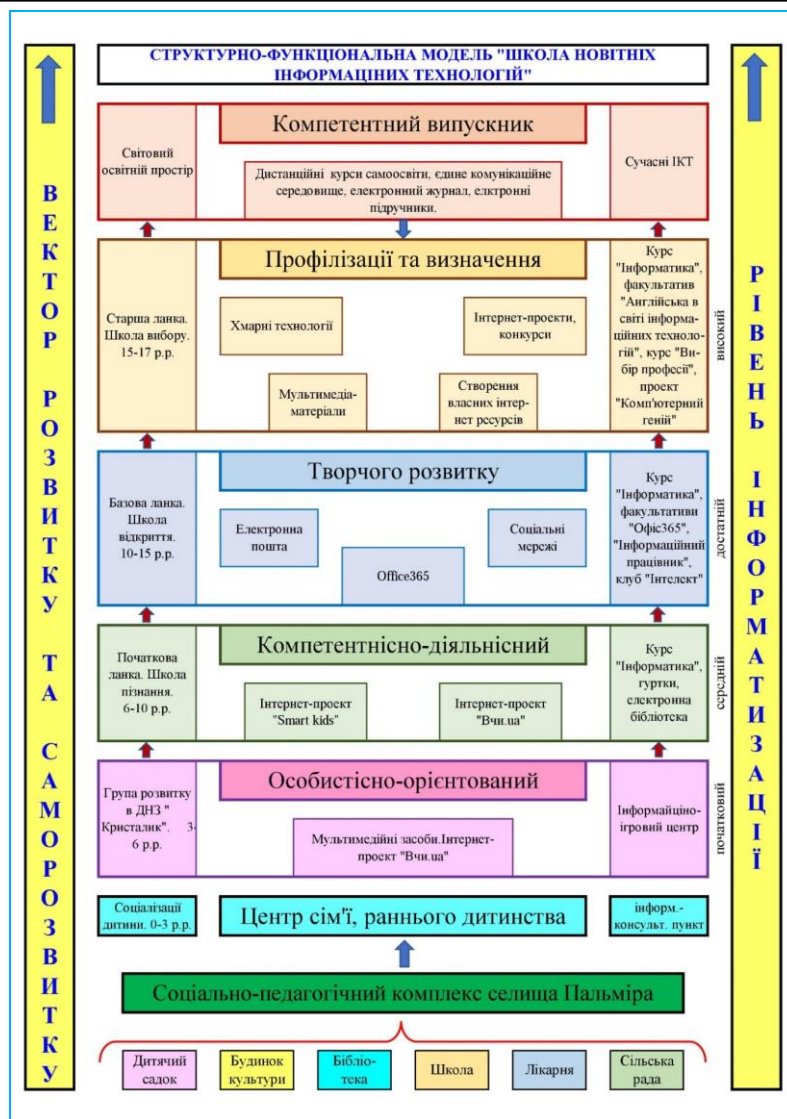


Рисунок 1 – Структурно-функціональна модель розвитку школи

Нами реалізовано такі напрями використання сервісів хмарних обчислень: 1) організація файлового сховища та налагодження електронного документообігу (OneDrive, Google-диск); 2) планування і оперативний контроль (календар-органайзер Office 365, Google-календар, Forms, Planner, Delve); 3) співробітництво (Google Календар, Google Диск, Google Форма, Блог, OneNote, Teams).

Перспективним для розвитку сучасного навчального середовища нашого закладу вважаємо відкриття в цьому році академії Cisco Palmira School та отримання двома вчителями школи статусу інструкторів міжнародної мережної академії Cisco. Це надало можливість учням отримувати додаткову освіту на сертифікованих навчальних курсах. Також плануємо активно розвивати навчальну робототехніку та програмування.

Список використаних джерел:

1. Концепція Нової української школи [Електрон. ресурс]. – Режим доступу: <http://mov.gov.ua/activity/education/zagalna-serednya/ua-sch-2016/>
2. Цифровий контент школи новітніх інформаційних технологій : Методичний посібник / В. М. Лосіцький та ін. – Черкаси: Видавництво КНЗ ЧОПОП, 2018. – 272 с.

ОСОБЛИВОСТІ ВІРТУАЛЬНОГО НАВЧАЛЬНОГО СЕРЕДОВИЩА НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ “ЛЬВІВСЬКА ПОЛІТЕХНІКА”

Думанський Нестор

Національний університет “Львівська політехніка”, кафедра соціальних комунікацій та інформаційної діяльності

Анотація

Ці тези описують основні особливості функціонування системи дистанційного навчання Національного університету “Львівська політехніка”. Особливості її використання викладачами при підготовці матеріалів для студентів дистанційної та заочної форми навчання.

Abstract

These theses describe the main features of the functions of the distance learning system at the Lviv Polytechnic National University. Features of its use by teachers in the preparation of materials for students of distance learning.

У Національному університеті “Львівська політехніка” функціонує система дистанційного навчання “Віртуальне навчальне середовище”, яка використовується як для підготовки студентів заочної форми навчання, так і для самостійної роботи студентів стаціонару. Інформація про систему дистанційного навчання та навчально-консультаційний центр інституту дистанційного навчання (ІДН) Львівської політехніки (нормативні документи, навчальні плани напрямків і спеціальностей) знаходиться у вільному доступі в деканаті та на веб-сайті ІДН за адресою <http://lp.edu.ua/idn>.

Організація дистанційного навчання, налагодження зв'язків між університетом, викладачами і студентами має спільні риси з традиційним навчанням. Взаємодія викладачів і студентів відбувається за допомогою віртуального навчального середовища (ВНС) – програмної системи, створеної для підтримки процесу дистанційного навчання з наголосом саме на навчання, на відміну від керованого навчального середовища, для якого властивий акцент на управлінні процесом навчання.

Це мережевий сервіс для щоденного користування, що містить усі необхідні елементи теоретичних і практичних знань, контролю і самооцінки навчальної діяльності, форми організації адаптації, мотивації і творчої спрямованості [1].

Розміщена на веб-сайті навчальна дисципліна (електронний курс) є структурованим набором електронних навчально-методичних матеріалів, підготовлених автором модуля (лектором), а також навчальних засобів та засобів контролю, що функціонують з використанням стандартних компонентів і сервісів Moodle.

Основу ВНС складають навчально-наукові інститути. У кожному інституті відображені напрями, за якими готують спеціалістів. У межах кожного напрямку реалізовано навчальні плани у вигляді переліку дисциплін, розбитих по курсах.

У кожній дисципліні розміщені такі матеріали: анотація дисципліни, її мета та завдання, робоча програма, система та критерії оцінювання знань студентів, список рекомендованої літератури, перелік індивідуальних завдань, перелік лабораторних, практичних робіт, семінарів, конспекти лекцій, методичні розробки автора, посилання на електронні підручники, які є в бібліотеці університету або в мережі Інтернет та посилання на Інтернет-ресурси з конкретної дисципліни (спеціалізовані сайти, журнали, форуми тощо).

У межах дисципліни матеріал розбито на змістові модулі, кількість яких відповідає кількості тем, визначених у навчальній програмі. Кожен змістовий модуль має наступну структуру: теоретичний матеріал (конспект лекцій з кожної теми), контрольні завдання та

запитання, індивідуальні завдання з методичними вказівками та прикладами виконання, лабораторний практикум (методичні вказівки або інструкції), автоматизовані тести для оцінювання вивченого матеріалу змістового модуля та для самоконтролю знань студентів. Особливістю ВНС є те, що його можна застосувати для проведення фактично всіх видів занять: лекцій, практичних, лабораторних, консультацій тощо.

Проведення лекцій за допомогою ВНС може мати безліч реалізацій залежно від специфіки дисципліни, стилю викладання. Перший варіант реалізації наповнення електронної дисципліни передбачає, що викладач підготував у електронному вигляді слайди, які він коментуватиме, і тексти коментарів в окремому файлі. У тексті у відповідних місцях вказують номери слайдів, які відповідають фрагменту коментаря.

Підготовлені матеріали викладач розміщує на сайті ВНС, тому слайди та тексти лекції доступні для студентів в онлайн-режимі та можуть бути завантажені на локальний комп'ютер. За іншого підходу викладач розміщує у ВНС анотацію лекції та графічні матеріали (рисунок, таблиці, графіки, відео- та аудіоматеріали тощо), які використовує при читанні лекції. За такої умови доцільно розмістити посібник чи конспект лекцій у форматі pdf чи djvu.

Ще одним варіантом наповнення електронної дисципліни є розміщення всіх матеріалів лекції у html-форматі, що дає змогу студентам вивчати теоретичний матеріал, користуючись лише засобами браузера без застосування додаткового програмного забезпечення. Під час проведення лабораторних, практичних робіт та семінарських занять ВНС дає змогу використовувати на занятті такі засоби:

- відеодемонстрації для практичних та лабораторних робіт;
- інтерактивні інструкції та методичні вказівки до лабораторних робіт;
- відео- та аудіоматеріали для практичних та семінарських занять.

Для проведення консультацій в офлайн-режимі у ВНС передбачено форуми. У кожній дисципліні є стандартний форум «Новини». Крім того, викладач може організувати форум з конкретного розділу чи питання. На ньому викладачі визначають тематику обговорення, відповідають на запитання студентів, надають інформацію про останні версії і зміни навчальних матеріалів.

Однією з головних особливостей ВНС є її модульність. Вся функціональність ВНС ґрунтується на модулях розширення. Модулі поділяють на такі типи: активності (до яких належать ресурси курсу, тести, глосарій, форуми тощо), блоки, фільтри, компоненти, а також модулі інтеграції сторонніх програм (гаджетів). Стандартний дистрибутив містить безліч модулів, які забезпечують базову функціональність ВНС. Однак розширення функціональності є актуальним завданням, оскільки дає змогу додати у ВНС нові можливості та підвищити ефективність роботи з наявними. Модуль потокового відео забезпечує можливість демонструвати відеоматеріали в лекційних курсах. Модуль аудіо-, відеоконференція Covcell дає змогу здійснювати односторонню трансляцію живих лекцій, двостороннє спілкування викладача зі студентом (наприклад, для усної відповіді) та багатосторонню відеоконференцію (наприклад, семінар). Отже, розширення функціональності за допомогою додавання нових модулів та гаджетів дозволяє суттєво удосконалити навчальний процес у ВНС та створити нові можливості в дистанційному навчанні.

Інтеграційні можливості ВНС є доволі широкими. Лектор може створити резервну копію своєї дисципліни у вигляді файлу. Використовуючи цей файл, можна розгорнути відповідну дисципліну на будь-якому іншому сервері з системою дистанційного навчання, об'єднати дисципліну з іншою і т. д.

Список використаних джерел:

1.Віртуальне навчальне середовище [Електронний ресурс] : офіційний сайт Національного університету «Львівська політехніка». – Режим доступу : <http://lp.edu.ua/virtualne-navchalne-seredovyshe>. – Назва з екрана.

ПІДВИЩЕННЯ РЕЙТИНГУ ВИЩОГО НАВЧАЛЬНОГО ЗАКЛАДУ У МІЖНАРОДНІЙ СИСТЕМІ ОЦІНКИ ДІЯЛЬНОСТІ УНІВЕРСИТЕТІВ WEBOMETRICS

Карагодіна Марина, Головка Ярослав

Академія праці, соціальних відносин і туризму

Анотація

Прагнення відповідати вимогам щодо якості в умовах глобалізації та займати якомога вище місце в міжнародних рейтингах вимагає від вищих навчальних закладів систематичного аналізу сучасних рейтингових систем та вчасного і гнучкого реагування на зміни їхньої методології. У матеріалі представлено досвід реалізації та оцінка ефективності практичних шляхів підвищення рейтингу Академії праці, соціальних відносин і туризму у міжнародному рейтингу оцінки діяльності університетів Webometrics.

Abstract

The desire to meet the quality requirements in a globalized environment and occupy the highest possible place in international rankings requires higher education institutions to systematically analyze current rating systems and timely and flexible response to changes in their methodology. The article presents the experience of implementing and assessing the effectiveness of practical ways to increase the rating of the Academy of Labour, Social Relations and Tourism in Webometrics Ranking of World Universities.

Вступ

У сучасному світі, в якому товари, послуги, інформація та технології вільно перетинають національні кордони, існує потреба у створенні універсальних показників та методів оцінки якості, в тому числі у сфері вищої освіти. Однією з авторитетніших систем рейтингування вищих навчальних закладів (ВНЗ) на сьогодні є ВебOMETричний рейтинг університетів світу (Webometrics Ranking of World's Universities), автори якого запропонували методологію оцінки світових вишів на основі їхньої присутності у мережі Інтернет та ступеню відкритості й цінності публікацій результатів наукової діяльності їхніх співробітників. Отже, задля реалізації стратегій підвищення власного рейтингу ВНЗ стикаються з викликами у двох площинах: інформаційно-технологічній та науковій. При цьому для вишу важливим є не тільки аналіз сьогоденних вимог до його діяльності, а й постійний моніторинг систем оцінки, які кожного року змінюються та вдосконалюються.

Про увагу українських науковців і практиків до міжнародних рейтингових систем оцінки ВНЗ свідчать як дослідницькі роботи останніх років [2, 5, 7, 8], так і поява власних аналітичних ресурсів щодо рейтингів на Інтернет-платформах національних вишів [6].

Метою даного дослідження було визначення та реалізація практичних шляхів підвищення рейтингу нашого вищого навчального закладу – Академії праці, соціальних відносин і туризму (АПСВТ), Україна, м. Київ – у системі Webometrics, а також подальша оцінка ефективності вжитих заходів. Відповідно до поставленої мети у період 2015-2018 рр. реалізовані такі завдання: 1) досліджено технології Webometrics щодо обчислення рейтингів університетів світу; 2) проаналізовано методології Webometrics у динаміці за інтервалом кожні півроку; 3) визначено та втілено стратегії підвищення основних показників рейтингу для АПСВТ; 4) скориговано або змінено обрані стратегії відповідно до виявлених змін у системі оцінки Webometrics; 5) оцінено ефективність обраних стратегій шляхом аналізу динаміки рейтингу АПСВТ у Webometrics. Реалізація завдань здійснювалась об'єднаними зусиллями маркетингового, наукового та технічного відділів Академії.

Основні результати

Вебометричний рейтинг університетів світу (Webometrics ranking of world's universities) – це один з рейтингів ВНЗ, за яким аналізується ступінь представлення діяльності вишів в Інтернет-просторі. Рейтинг з 2004 року за власною методологією складає Лабораторія кіберметрики (Cybermetrics Lab) Національної дослідницької ради Іспанії (Spanish National Research Council, CSIC). Результати оцінки оприлюднюються двічі на рік (у липні та лютому за даними збору даних у червні та січні відповідно) [3]. Рейтинг починався з аналізу діяльності 6 000 університетів; на сьогодні аналізу піддають понад 20 000 вищих навчальних закладів з усього світу.

У рейтингу Webometrics станом на 1.02.2018 року використовуються наступні параметри розрахунків [1]:

1. Присутність (Presence) – кількість присутніх на сайті університету сторінок усіх форматів, проіндексованих пошуковою системою Google, включаючи всі піддомени та всі типи файлів, наприклад, такі, як документи в форматі PDF. Питома вага даного параметра для розрахунку остаточного рейтингового результату зменшилась у порівнянні з 2017 роком з 10% до 5%.

2. Видимість (Visibility or Impact) – комбінація кількості зовнішніх гіперпосилань на домен університету (external inlinks) та кількості доменів, з яких ці посилання надходять (referring domains) за даними ресурсу Ahrefs Majestic. Питома вага даного параметра складає 50%.

3. Відкритість (Transparency or Openness) – кількість цитат авторів університету відповідно до Google Scholar Citations. Для обрахунку беруть 10 провідних особистих наукових профілів кожного університету. Перший профіль зі списку не враховується для підвищення репрезентативності, а дані інших топ-10 (максимум 9 профілів) складаються, і установи ранжуються за спаданням показника. Питома вага даного параметра складає 10%.

4. Висока якість (Excellence) – кількість наукових статей, що опубліковані авторами університету в журналах, проіндексованих бібліометричною базою Scopus, та входять до складу 10% статей, найбільш цитованих у 26 наукових галузях за версією Scimago Group. Під час обчислень враховуються дані за п'ять попередніх років. Питома вага даного параметра для розрахунку остаточного результату університету збільшилась у порівнянні з 2017 роком з 30% до 35%.

З моменту запровадження рейтингу Webometrics методологія його обчислення постійно змінювалася та вдосконалювалася. Так, у 2016 році найбільшої трансформації зазнав принцип розрахунку щодо параметру "Openness". Якщо раніше він відповідав за підрахунок на сайті університетів PDF-файлів документів, знайдених пошуковою машиною Google Scholar, то відтепер став вестися підрахунок цитувань наукових робіт співробітників університету за допомогою пошукової системи Google Scholar Citations. До такої ситуації більшість університетів світу були не готові. Виявилось, що з близько 22 000 університетів світу, ранжованих за допомогою Webometrics, особисті профілі вчених Institutional Google Scholar Citation мали лише 4 120 університетів.

У січні 2018 року укладачі рейтингу ввели нове обмеження щодо "Openness": "Присутність неіндифікованих групових профілів (журналів, відділів, груп) у першій десятці результатів закладу карається виключенням всього навчального закладу з оцінки OPENNESS (кількість цитат дорівнює нулю)" [4]. В результаті нововведення, зокрема, 197 з 327 українських вишів отримали у січні-2018 останнє місце за даним показником, що суттєво змінило всю картину рейтингу в Україні.

АПСВТ потрапила до рейтингу Webometrics після електронного звернення до компанії-укладача рейтингу на початку 2015 року і посіла у липні 2015 року 16 078 загальну рейтингову позицію серед університетів світу (за окремими показниками: Presence Rank – 9 614, Impact Rank – 17 642, Openness Rank – 12 316, Excellence Rank – 5 490) та 185 місце – в Україні.

Аналіз вимог укладачів рейтингу дозволив нам розробити та поступово втілювати стратегію підвищення позицій АПСВТ у Webometrics. Найбільш вагомого результату було досягнуто у липні 2017 року. Загальний рейтинг АПСВТ у порівнянні з 2015 роком виріс майже на 6 000 позицій (10 126 місце) та на 55 позицій – в Україні (130 місце). У січні 2018 року показники суттєво погіршились (15 186 місце у світі та 196 місце в Україні) внаслідок різкого погіршення параметру Openness.

Для поліпшення показнику Presence нами було ініційовано проведення професійного аналізу сайту Академії на предмет індексації пошуковими системами, виправлення некоректних налаштувань та здійснення базової внутрішньої оптимізації сайту. Застосовані заходи призвели до підвищення даного показника на 600 пунктів (9 096 місце у світі у січні 2018 року).

Для поліпшення показнику Impact було розширено присутність Академії у соціальних мережах, забезпечено систематичне поповнення сайту актуальною інформацією, яка становить інтерес для поширення на зовнішніх ресурсах, введено у постійну практику обмін матеріалами і посиланнями з сайтами партнерів. У результаті за 2,5 роки АПСВТ за даним показником піднялась більше ніж на 3 000 позицій (14 412 місце у світі у січні 2018 року).

Оскільки методологія обчислення показнику Openness суттєво змінювалась двічі за період, що розглядається, порівняння кількісних даних 2015 та 2018 року є некоректним. У липні 2016 року, коли для даного параметру почали враховувати цитування наукових робіт співробітників університетів у Google Scholar Citations, АПСВТ посіла 4 121 місце у світі – це було останнє місце серед всіх учасників рейтингу (його мали всі навчальні заклади, у яких даний показник дорівнював нулю). За півроку після централізованого створення наукових профілів викладачів АПСВТ у системі Google Scholar Citations рейтинг Openness Академії виріс майже на 500 пунктів (3 643 місце у світі у січні 2017 року). У січні 2018 року АПСВТ знов отримала нульовий результат за даним параметром (9 593 – останнє місце) через нові зміни у методології, що спричинило суттєве погіршення її загального рейтингу.

За параметром Excellence АПСВТ постійно посідає останнє місце, оскільки до 2018 року не мала наукових статей за авторством її співробітників, які відповідають вимогам рейтингу.

Специфіка ринку освітніх послуг у глобальному світі передбачає, що вищий навчальний заклад може ефективно презентувати себе у національному та світовому Інтернет-просторі лише за умов систематичного аналізу сучасних рейтингових систем та вчасного і гнучкого реагування на зміни їхніх технологій та вимог.

Список використаних джерел

1. 2018. Ranking Web of Universities. January New Edition. URL: <http://www.webometrics.info/en/node/200>
2. Dreshpak V., Starushenko G. Міжнародні рейтинги університетів як інструмент оцінювання державної політики у сфері вищої освіти // Аспекти публічного управління. – 2017. – № 7. – С. 27-35. URL: <https://doi.org/https://doi.org/10.15421/15201720>
3. Ranking Web of Universities. URL: <http://www.webometrics.info>
4. Transparent Ranking: Top Universities by Google Scholar Citations. Fifth Edition (December 2017 version 5.1) URL: <http://www.webometrics.info/en/node/169>
5. Дубинский А. Г. Пути повышения позиции вуза в рейтинге webometrics: фактор открытости // Системи обробки інформації – 2012. – № 9. – С. 286-290.
6. Рейтинги сайтів КПІ ім. Ігоря Сікорського. URL: <http://webometr.kpi.ua>
7. Тютюнник А. В. Основні критерії та показники вебметричного рейтингу університетів світу / А. В. Тютюнник, Б. І. Грицеляк // Інформаційні технології і засоби навчання. – 2013. – Т. 38, вип. 6. – С. 234-244.
8. Чекаловська Г. З. Ранжирування у вищій освіті як механізм оцінювання якості освітніх послуг / Г. З. Чекаловська // Економічний простір. – 2013. – № 73. – С. 298-310.

CHALLENGES OF CRITICAL INFORMATION MANAGEMENT TECHNOLOGY

Tinatin Mshvidobadze

Gori State University(Georgia)

Abstract

In this paper, we will review and analyze the challenges, and offer some directions for some of the subjects of research, so as to help marshal the creative energies of the corresponding segments of the research community for faster solutions to the challenges.

An important class of new and existing applications requires cooperating entities to share and exchange information seamlessly in real-time, while meeting stringent requirements for quality of service (QoS) and heterogeneity. This paper describes how the recently adopted OMG DDS standard, and the Open Splice DDS implementation of this standard, support the data distribution and management challenges posed by next-generation distributed systems, and systems of systems.

Introduction

Information management technology is technology for managing information, having evolved from file management, information retrieval and database management technologies to encompass customer relationship management, supply chain management, enterprise resource planning, data and application integration, multimedia processing, data mining, and Web personalization and recommendation, among others. Two of the most worthy and pressing areas of research and development in information management today are the taming of information explosion and options overload, and support for ubiquitous computing environments.

Recent trends in net-centric systems motivate the development of mission-critical information management capabilities that ensure the right information is delivered to the right place at the right time to satisfy quality of service (QoS) requirements in heterogeneous environments.

To support these mission-critical information management capabilities in net-centric systems, the Object Management Group (OMG) has adopted the Data Distribution Service (DDS) specification [1], which is a standard for QoS-enabled data-centric publish/subscribe (pub/sub) communication that enables net-centric mission and business-critical information management systems to share information in real time by utilizing QoS-driven publish/subscribe patterns.

This paper describes why Open Splice DDS is an important distributed software technology for mission critical net-centric systems because it supports (1) relational and object oriented modeling of the information shared by, and distributed within, the system (2) location independence, via anonymous publish/subscribe protocols that enable communication between collocated or remote publishers and subscribers, (3) scalability, by supporting large numbers of topics, data readers, and data writers and platform portability and (4) interoperability, via standard interfaces and transport protocols.

Mission-Critical Information Management in Next-Generation Net-Centric Pub/Sub Systems

DDS applications send and receive data within a domain. Domains can be divided into partitions that allow the separation and protection of different data flows. Although DDS entities can belong to different domains, only participants within the same domain can communicate, which helps isolate and optimize communication within communities that share common interests. This approach isolates domain participants across layers, which enables effective use of resources and helps enforce security and confidentiality policies. DDS provides a strongly typed global data space within each domain in which applications produce and

consume dynamically changing portions of a shared information model. DDS's information model capabilities are similar to those of relational databases, except that DDS's global data space is completely distributed, QoS-aware, and allows anonymous and asynchronous sharing of a common information model. By allowing data to flow where and when needed, DDS's global data space enables the sharing of mission-critical information and situational awareness needed to implement net-centric mission-critical information management systems[2].

Publishers and subscribers. In net-centric mission-critical information management systems, publishers and subscribers correspond to a range of do-main participants, such as embedded devices, air traffic control radars, visualization consoles, and online stock feeds, as well as planning and simulation services in operations centers. DDS applications use data writers to publish data values to the global data space of a do-main and data readers to receive data.

Configuring QoS policies allows publishers and subscribers to (1) define the local behavior of their interface with DDS, such as the number of historical data samples they require and the maximum update-rate at which they want to receive data, and (2) how DDS should provide global data availability with respect to reliability, urgency, importance, and durability of the distributed data. Since topics themselves can be annotated with QoS policies that drive the global data-availability, publishers and subscribers can use these pre-defined QoS policies as consistent defaults allowing them to concentrate purely on the local-behavior driving policies.

Subscriptions and matching. A subscription is an operation that associates a subscriber to its matching publishers, as shown in the center of Figure 1.

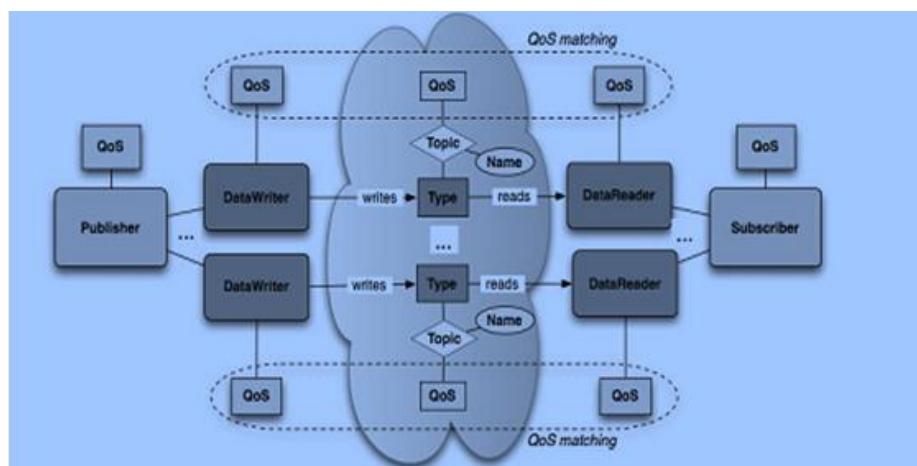


Figure 1 – DDS Publisher/Writer Sub-subscriber/Reader and Subscription/QoS Matching.

In addition to the topic-based subscriptions described above, DDS also supports content-based subscription, in which a subset of the standard Structured Query Language (SQL) is used to specify subscription filters. In DDS a matching subscription must match the following two types of topic's properties: (1) its features such as its type, name, key, and content, and (2) its QoS policies.

The matching process for QoS uses a requested/offered (RxO) model, where the requested QoS must be less than or equal to the offered QoS. For example, subscribers requesting reliable data delivery cannot communicate with publishers that only distribute data using best effort delivery[3].

Open Splice DDS use cases. Open Splice DDS was one of the most influential technologies contributing to the definition of the DDS standard, due in large part to its heritage of success during the past two decades in a range of mission-critical distributed systems. In particular, OpenSplice DDS has been deployed in several different application domains, such as defense, aero-space, transportation, etc. For example, the TACTI-COS combat management system [4] developed by THALES Naval Netherlands builds atop Open Splice DDS [5], which

allows TACTICOS to achieve very high scalability, from small ships to aircraft carrier grade, as well as high performance, availability, and determinism even under temporary overload conditions. TACTICOS is currently in use in over 15 Navies worldwide serving more than 26 ships-classes ranging from small patrol boats up to large frigates.

From a standardization perspective, DDS continues to evolve to meet new operational and technical challenges of net-centric mission-critical information management systems. The OMG is currently pursuing the following three types of extensions for DDS:

- The first involves adding new platform-specific models that fully leverage programming language ;
- The second extension deals with extensible topics that enable incremental system updates by ensuring that changes in the data model do not break interoperability;
- The third set of extensions focus on network data representation and the syntax used to define topics. For example, upcoming versions of the DDS standard will likely allow the definition of topics using XML, as well as the use of XML or JSON as the network data representation. DDS security has not yet been standardized.

Conclusion

In this paper, we reviewed and analyzed the two major challenges facing the information management technology today, namely, the information and options overload problems, and support for ubiquitous environments. As the pace of advances in research to meet these challenges is lagging behind the pace of the problems becoming ever more intractable and the spread of ubiquitous environments, I am hopeful that researchers working on various relevant subjects will find practical solutions faster.

OpenSplice DDS is standards-based QoS-enabled data-centric pub/sub middleware that provides a feature rich data-centric real-time platform to support the needs of current and planned net-centric mission-critical information management systems. Its powerful set of QoS policies—together with its scalable architecture—makes it an effective and mature choice for solving the data distribution and information management problems net-centric systems.

We should work toward a universal linked information system, in which generality and portability are more important than fancy graphics techniques and complex extra facilities.

References:

1. OMG, “Data Distribution Service for Real-Time Systems Specification,” www.omg.org/docs/formal/04-12-02.pdf
2. Ming Xiong, Jeff Parsons, James Edmondson, Hieu Nguyen, and Douglas C. Schmidt, “Evaluating Technologies for Mission-critical Information Management in Net-Centric Systems,” Proceedings of the Defense Transformation and Net-Centric Systems conference, April 9-13, 2007, Orlando, Florida.
3. Bertrand Meyer, Object Oriented Software Construction – 2nd Edition, Prentice Hall, 2001.
4. THALES, “TACTICOS Combat Management System, Exploiting the Full DDS Potential,” www.omg.org/docs/dds/06-12-06.pdf.
5. Open Splice DDS, www.prismtech.com/opensplice-dds.

КОНЦЕПЦІЯ СТВОРЕННЯ ЕЛЕКТРОННОГО УНІВЕРСИТЕТУ ДЛЯ ЗАКЛАДУ ВИЩОЇ ОСВІТИ

Коваленко Олена, Паламарчук Євген

Вінницький національний технічний університет

Анотація

Концепція створення електронного університету для вищого навчального закладу містить теоретико-практичні засади побудови ІТ-стратегії університету, визначення основних цілей, шляхів їх досягнення та отриманих вимірювальних результатів. ІТ-стратегія повинна бути узгодженою з загальною конкурентоздатною стратегією розвитку закладу вищої освіти. Кожна цільова проекція відповідає визначеним кількісним та якісним показникам та національним і міжнародним рейтинговим показникам розвитку закладів вищої освіти. Концепція містить також варіанти формування групи підтримки апаратного, програмного та контентно-методичного забезпечення розвитку електронного університету; реалізації методик змішаного навчання; залучення абітурієнтів; покращення процесів взаємодії університету та компаній-роботодавців.

Ключові слова: електронний університет, заклад вищої освіти, ІТ-стратегія, змішане навчання, рейтинг університету, ІТ-компанія.

Abstract

The concept of creating an e-university for a higher education institution contains theoretical and practical principles for building an IT strategy of the university, defining the main goals, ways to achieve them and they obtained measurement results. The IT strategy should be consistent with the overall competitive strategy of the institution of higher education. Each target projection meets the determined quantitative and qualitative indicators and national and international rating indicators for the development of higher education institutions. The concept also includes options for forming a support group for hardware, software and content-methodological support for the development of the e-university; implementation of mixed learning methods; attraction of entrants; improving the processes of interaction between the university and employer companies.

Keywords: e-university, higher education institution, IT strategy, mixed learning, university rating, IT-company.

Вступ

Ідеї та практики створення електронного університету виникли одразу з появою систем автоматизованого управління і стали активно розвиватись разом з технологіями Інтернет/Інтранет. Довгий час концепція електронного університету сприймалась як запровадження інформаційної систем управління навчанням, дистанційної освіти або/і електронного документообігу. Сьогодні вже зрозуміло, що електронний університет закладу вищої освіти є комплексною системою автоматизації адміністративних, освітніх, науково-методичних та науково-дослідних процесів функціонування вищого навчального закладу.

Постановка проблеми

Авторський досвід впровадження систем управління навчанням та підтримки методичної, науково-дослідної роботи у вищих навчальних закладах та аналіз низки науково-практичних праць щодо розвитку електронних університетів [1-3] дозволяє зробити висновок щодо необхідності уточнення основних понять та сутності електронного університету на даному етапі розвитку інформаційного суспільства та умов запровадження концепції електронного університету в Україні.

Мета дослідження створення концепції електронного університету для вищого навчального закладу.

Виклад основного матеріалу

Різноманітні підходи до побудови концепції електронного університету були обумовлені рівнем розвитку інформаційних технологій, готовності персоналу та одержувачів електронних послуг до їх активного використання. Сучасне інформаційне суспільство в поєднанні з концепцією навчання через все життя потребує комплексного підходу до розуміння та запровадження електронного університету.

Головна мета діяльності та розвитку закладу вищої освіти – надання якісних освітніх послуг. Вони можуть бути надані в електронному вигляді або мати електронну підтримку. Досвід запровадження різних форм дистанційного навчання в світі та в Україні свідчить про те, що найбільш ефективною формою – є змішане навчання [1;2], яке як раз і передбачає таку електронну підтримку.

Часто під електронним університетом розуміють наявність динамічного сайту та електронного документообігу. Не варто вважати це за помилку. Це є одною з складових електронного університету. Злиття традиційних та електронних послуг, традиційних та електронних освітніх, науково-дослідних, науково-методичних та адміністративних процесів в єдину комплексну систему управління є основою концепції електронного університету вищого навчального закладу.

На рис. 1. представлено концептуальну схему складових електронного університету.



Рисунок 1 – Концептуальна схема електронного університету «Навчання через все життя»

Вона враховує адміністративні, соціально-економічні та технічні аспекти розвитку університету та його інформаційного електронного середовища. Головними акторами такого середовища є студент та викладач. Розвиток такого середовища відповідає стратегічному розвитку закладу вищої освіти, його загальної та інформаційно-технологічної стратегій. Одною з головних цільових проєкцій є підвищення іміджу університету, його рейтингу в різноманітних інфометричних системах, зокрема таких як Webometrics. Відповідальність за головну цільову функцію такої стратегії бере на себе керівництво університету та безпосередньо ректор. Такий підхід дозволить стратегічно об'єднати зусилля технічних працівників щодо підтримки освітньої платформи та

апаратного забезпечення, фахівців з методичного контенту, програмного забезпечення, студентів та викладачів закладу вищої освіти.

Саме тому, структура робочих груп персоналу, що створює та підтримує електронний університет складається з таких цільових груп:

1. Проектна група «Електронний університет»;

2. Адміністративно-технічний персонал центрів інформаційних технологій університету; інститутів організаційного та методичного забезпечення навчання; довузівської підготовки, магістратури, аспірантури та докторантури, інтеграції навчання з виробництвом, деканатів факультетів університету; науково-технічної бібліотеки;

3. Активні викладачі та студенти.

Групи активних викладачів та студентів є учасниками робочої проектною групи створення та розвитку електронного університету, розробниками та тестувальниками його модульних складових.

Система персональних кабінетів викладача, методиста, студента дозволяє сформувати цільове електронне інформаційне середовище [4;5], застосувати інструменти змішаного навчання та здійснювати моніторинг освітнього процесу, науково-методичної та науково-дослідної діяльності викладачів та студентів.

Висновки

Концепція електронного університету повинна містити основні цільові проєкції ІТ-стратегії; вибір інформаційної освітньої платформи; концепцію інтеграції існуючих електронних ресурсів; орієнтовний перелік акторів системи електронного університету та їх інформаційно-технологічних процесів; контентно-методичні концепції змішаного навчання та моніторингу результатів освітнього процесу, науково-методичної та науково-дослідної діяльності викладачів та студентів. Концепція «Навчання через все життя» включає в себе електронну взаємодію з довузівськими закладами освіти та компаніями - роботодавцями.

Список використаних джерел:

1. How-do-you-create-a-digital-university (2017). Available at: <https://www.theguardian.com/higher-education-network/2017/jun/29/how-do-you-create-a-digital-university><http://www.smartinsights.com/marketplace-analysis/customer-analysis/web-design-personas/> (accessed 20 April 2018).

2. Кухаренко В.М. Сучасний електронний університет та змішане навчання. Сучасні інформаційні технології в дистанційній освіті. Матеріали V Всеукраїнського науково-практичного семінару (м. Івано-Франківськ, 25-26 травня 2017 року).– Івано-Франківськ : ПП «ФотоПринтСтудія», 2017.

3. Wendy W.PorterCharles R.GrahamKristian A.SpringKyle R.Welch Blended learning in higher education: Institutional adoption and implementationComputers & EducationVolume 75, June 2014, Pages 185-195

4. Свідоцтво про реєстрацію авторського права на твір № 72970 UA. Комп'ютерна програма «Система інтеграції електронних ресурсів вищого навчального закладу «Інтегровані електронні ресурси ВНТУ JetIQ («ІЕР ВНТУ JetIQ»)» [Текст] / В. В. Грабко, О. Н. Романюк, О. В. Бісікало, М. П. Боцула, Є. А. Паламарчук, О. О. Коваленко (Україна) ; Міністерство економічного розвитку і торгівлі України. - Дата реєстрації 20.07.2017 р. [Електронний ресурс] . - <http://ir.lib.vntu.edu.ua/handle/123456789/19302>

5. Свідоцтво про реєстрацію авторського права на твір № 72971 UA. Комп'ютерна програма «Електронний деканат JetIQ» («ЕД JetIQ») [Текст] / В. В. Грабко, О. В. Бісікало, Т. О. Савчук, Є. А. Паламарчук, О. О. Коваленко (Україна), Міністерство економічного розвитку і торгівлі України. - Дата реєстрації 20.07.2017 р. <http://ir.lib.vntu.edu.ua/handle/123456789/19991>

СУЧАСНІ СПОСОБИ ОЦІНКИ ПСИХОФІЗІОЛОГІЧНОЇ ЕФЕКТИВНОСТІ РЕАБІЛІТАЦІЇ ВЛАСТИВОСТЕЙ ЦЕНТРАЛЬНОЇ НЕРВОВОЇ СИСТЕМИ

Охромій Галина

ДВНЗ, «Український державний хіміко-технологічний університет»

Анотація

У статті описується пропонуваній нами винахід, який відноситься до медицини і призначається для використання під час експрес-оцінки за психомоторними показниками функціонального стану ССС у хворих з порушеннями серцевого ритму і ішемічною хворобою серця, що перенесли гострий інфаркт міокарду (ГІМ), при проведенні реабілітаційних програм і регламентації трудової діяльності.

Abstract

This article describes the proposed invention, which refers to the medicine and appointed for use at the time of rapid assessment on psychomotor indicators of functional status HVS in patient with violations of heart rate and and coronary heart disease, which had acute myocardial infarction (AMI) during rehabilitation programs and regulation of labor activity.

Актуальність дослідження

Порушення кровообігу при різних захворюваннях серцево-судинної системи (ССС) відбивається на функціях центральної нервової системи (ЦНС), знижуючи динаміку процесів нервової діяльності. Тому в діагностиці таких захворювань є закономірною поява і застосування різних тестів, орієнтованих на визначення моторно-координаційної продуктивності при виконанні робочих програм різної складності. Існує необхідність у розробці тестів і пристроїв, інформаційні показники яких дозволяли б робити об'єктивні оцінні висновки на різних стадіях лікувального процесу з застосуванням чітких кількісних критеріїв і градацій фізичного стану хворих із серцево-судинною патологією (ССП) [1].

Пропонуваній нами винахід відноситься до медицини і призначається для використання під час експрес-оцінки за психомоторними показниками функціонального стану ССС у хворих з порушеннями серцевого ритму і ішемічною хворобою серця, що перенесли гострий інфаркт міокарду (ГІМ), при проведенні реабілітаційних програм і регламентації трудової діяльності [2,3].

Метою пропонуваного нами винаходу є створення технічних засобів оцінки функціонального стану ССС і виявлення прихованої коронарної недостатності на різних етапах лікувального процесу хворих на СПП.

Розроблений нами пристрій автоматизує процес проведення Теплінг-тесту і обробку його результатів. Одиничні імпульси, формовані випробуванням у максимальному темпі, підлягають спеціальній обробці в рівних по тривалості послідовних інтервалах часу. Шляхом зіставлення інформації в суміжних інтервалах аналізують відносну динаміку частот імпульсів. За величиною відносних показників темпу судять про характер реабілітаційного процесу.

Пристрій працює в такий спосіб (Рис.1). Механічний вплив на чуттєвий елемент *тактильного датчика 1* перетворюється в електричний сигнал, нормований за тривалістю імпульсу *формувателем 2*. Повний цикл виміру визначається часом одного інтервалу, формованого *генератором 3* і загальною кількістю інтервалів, обчислених за допомогою *дешифратора 4*. В основу методики покладено наступну залежність:

$$k = \frac{(S_1 - S_2) + (S_1 - S_3) + \dots + (S_1 - S_n)}{S_1 + S_2 + \dots + S_n} \cdot 10$$

де:

k – результуючий коефіцієнт, що характеризує зумовлений параметр;

S_m – кількість імпульсів, зафіксована в m -ом інтервалі часу ($m = 1...n$);

n – кількість інтервалів часу, що фіксуються.

Визначення алгебраїчних різниць, зафіксованих у першому тимчасовому інтервалі S_1 і всіх наступних $(n-1)$ інтервалах здійснюється у *обчислювачах різниць* 12–16.

Визначення сумарної кількості імпульсів за всі n інтервалів часу здійснюється в *суматорі* 11. *Суматор* 17 робить операцію підсумовування алгебраїчних різниць і передачу отриманого результату в *АЛП* 18, що реалізує функцію розподілу попередньо визначених перемінних. *Масштабуючий перетворювач* 19 приводить отриманий результат до значень, що знаходяться в межах від 1 до 10. *Блоки* 20, 21 служать для здійснення візуалізації отриманих у ході дослідження результатів.

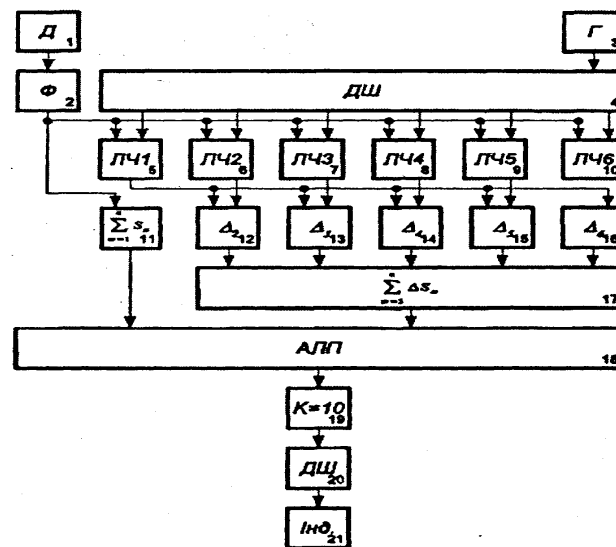


Рисунок 1 – Схема пристрою для оцінки психофізіологічної ефективності реабілітації властивостей ЦНС

Всі блоки системи за винятком 1 і 2 виконані: а) для переносного (індивідуального) використання з застосуванням програмно-апаратних засобів мікропроцесорної техніки;

б) для стаціонарного використання з застосуванням програмно-апаратних засобів персональних комп'ютерів. Прикладне програмне забезпечення стаціонарного варіанту системи дозволяє здійснювати статистичний аналіз і відображення динаміки процесу відновлення функцій центральної нервової системи конкретного пацієнта під час спостереження. За результатами статистичної обробки алгебраїчних інтервальних різниць у поточному експерименті визначаються показники, що характеризують лабільність і силу ЦНС конкретного пацієнта. Висновок про лабільність сенсомоторного аналізатора робиться по загальній сумі крапок. Статистичні оцінки лабільності в залежності від кількості крапок переводяться в бали за методикою Теппінг тесту.

Стаціонарний зразок пристрою виготовлений АТ "Комета" м. Дніпро і проходив клінічні іспити в Українському державному НДІ медико-соціальних проблем інвалідності м. Дніпро, Патент України, № 60783А Бюл. №10, 2003, затверджено заступником голови державного департаменту інтелектуальної власності від 16.04.2003 р., заявник, автор ідеї - Охромій Г.В. Для обробки результатів Теппінг-тестирования розроблена спеціальна програма "lability", призначена для роботи на звичайному персональному комп'ютері

(ПК). Програма обробляє дані приладу для виміру лабільності (патент № 60783А), що підключається до ПК через послідовний порт. Програма розроблена для роботи в операційних системах Windows 2000, Windows XP.

За підсумками проведеного дослідження, отримані наступні результати:

Існує зворотній кореляційний зв'язок середньої сили між показником лабільності НС і віком. Найбільша лабільність спостерігається в осіб, що займаються розумовою працею. Зі збільшенням ступеня ГХ знижуються показники лабільності і сили НС. Зі збільшенням ступеня ХСН лабільність знижується і спостерігається зворотній зв'язок сили НС із ступенем ХСН. Зі збільшенням класу ваги стенокардії напруги знижуються показники лабільності і сили нервової системи. На лабільність НС впливають клас ваги захворювання і режим фізичної активності – зі збільшенням класу ваги лабільність НС знижується, з розширенням режиму фізичної активності лабільність зростає. При призначенні належного режиму фізичної активності з урахуванням тяжкості перебігу захворювання спостерігається збільшення як лабільності, так і сили НС. Раннє призначення режиму фізичної активності сприяє більш швидкому відновленню лабільності НС. Показники лабільності і сили НС можуть використовуватися для оцінки ефективності індивідуальної програми реабілітації. Підібрані ППР за розширенням рухового режиму з урахуванням показань і протипоказань були ефективні, про що свідчить відновлення лабільності НС. У результаті дослідження взаємозв'язку гемодинаміки після кардіохірургічного втручання і психофізіологічного статусу виявлено, що з поліпшенням гемодинаміки показник лабільності НС не тільки відновлюється, але і перевищує вихідний рівень ($p < 0,05$). Зниження лабільності нервової системи на 2-3й день після кардіохірургічного втручання зв'язано з залишковим впливом наркозу, анальгезії і післяопераційної гіпокінезії. Підвищення лабільності НС у прооперованих пацієнтів пов'язане з поліпшенням гемодинаміки внаслідок хірургічного втручання. У хворих, що перенесли кардіохірургічне дослідження з метою постановки діагнозу, підвищення лабільності НС зумовлене адекватністю і ефективністю призначеного лікування. Зниження показника сили НС у ранньому післяопераційному періоді можна пояснити змушеним обмеженням фізичної активності, тобто гіподинамією.

Теплінг-тест може використовуватися для визначення психофізіологічного статусу хворих, що перенесли кардіохірургічне втручання, як частина комплексної оцінки їхнього стану для контролю ефективності лікування і реабілітації. Виявлено достовірний вплив ($p < 0,034$) ускладнень і супутніх захворювань (ХСН, стенокардія напруги, ГХ) на зниження показника лабільності НС, тобто на зниження реабілітаційного потенціалу, а також достовірний вплив ($p < 0,021$) на лабільність НС класу ваги захворювання і режиму фізичної активності (зі збільшенням класу ваги лабільність НС знижувалася, а з розширенням режиму фізичної активності лабільність зростала).

Висновки: встановлено взаємозв'язок показників психофізіологічного статусу з показниками тяжкості перебігу патології (вид інфаркту, функціональний клас і клінічна стадія СН, клас ваги стабільної стенокардії, групи ускладнень). Перераховані показники покладені в основу розроблених критеріїв контролю ефективності реабілітації осіб, що перенесли ГІМ, за лабільністю НС.

Список використаних джерел:

1. Охромий Г.В. Психофизиологические критерии эффективности реабилитации лиц, перенесших острый инфаркт миокарда / Г.В. Охромий // Журнал АМН України. – Київ, 2006. – №2. – Том.12. – С.392-402.
2. Оценка толерантности к физическим нагрузкам по психофизиологическому статусу / Охромий Г.В. – Свідectво про реєстрацію авторського права на твір № 21433 від 25.07.2007р.
3. Психофизиологические критерии эффективности реабилитации лиц, перенесших острый инфаркт миокарда / Охромий Г.В. – Свідectво про реєстрацію авторського права на твір № 21432 від 25.07.2007 р.

ВИКОРИСТАННЯ ПРОГРАМНОЇ СИСТЕМИ ANTLR ДЛЯ СТВОРЕННЯ МОВИ РЕЛЯЦІЙНОЇ АЛГЕБРИ

Фісун Микола, Кандиба Ігор

Чорноморський національний університету імені Петра Могили

Анотація

Розглянуто спосіб побудови компілятора мови реляційної алгебри як предметно-орієнтованої мови для використання в навчальному процесі при опануванні курсу з організації баз даних. Пропонується використати засоби генератора парсерів ANTRL, крос-платформової мови Python з подальшою передачею отриманого коду в SQL на виконання СКБД: SQLite або MySQL.

Abstract

This article is devoted to research the method of constructing a compiler for relational algebra as a domain-specific language. This language can be used in the database organization course. It is proposed to use the generators parsers ANTRL and cross platform programming language Python for generating SQL code for DBMS: SQLite and MySQL.

Вступ

Предметно-орієнтовані мови (ПОМ) відомі вже дуже давно. На зорі становлення мов програмування загального призначення вони розроблялися для програмування вузького кола завдань, щоб користувач комп'ютера, який добре володіє моделями предметної області і не дуже підготовлений як програміст, міг запрограмувати свої завдання. Однак цим мовам не судилося стати помітною частиною в ІТ-індустрії. Це пояснюється створенням спеціалізованих бібліотек в середовищі мов програмування загального призначення, можливостями графічного інтерфейсу і підвищенням програмістської підготовленості фахівців в предметних областях. Тому зараз серед багатьох і багатьох предметно-орієнтованих мов залишилися такі, що охоплюють широке коло специфічних задач. Як приклад можна навести такі мови моделювання, як GPSS, DYNAMO та ін. Але в останні роки спостерігається підвищення інтересу до предметно-орієнтованих мов [1], де вони англійською називаються Domain-Specific Languages (DSL). Вони стають популярними з двох основних причин. Перше – це підвищення продуктивності праці розробників, оскільки програмний код на ПОМ може бути в кілька разів коротше програмного коду на мові програмування загального призначення. Друге – поліпшення зв'язку з фахівцями в предметній області. Правильно вибрана мова може зробити складний блок коду істотно простіше і для програмування, і для розуміння, що підвищує продуктивність працюючих з ним. Вона спрощує спілкування розробника програмного забезпечення (ПЗ) з фахівцями в предметній області. Текст програми на ПОМ виступає одночасно і як виконуване ПЗ, і як опис проблеми, яке вузькі фахівці в цій галузі знань можуть прочитати, щоб зрозуміти, як їх уявлення виглядає в програмному представленні.

Мета дослідження

В даному дослідженні в якості такої ПОМ обрано мову реляційної алгебри (REAL), яка, разом з реляційним численням, є математичним базисом мови SQL. Звичайно, вона ні в якому разі не замислюється як конкурент SQL. REAL буде використовуватися в навчальному процесі в курсі з основ баз даних для глибшого розуміння реляційної моделі даних. Вихідним мовою відповідного компілятора буде мова SQL, програма на якій буде виконуватися в програмному середовищі обраної СКБД.

Результати дослідження

Оператори мови REAL діляться на два класи: створення і ведення реляційних таблиць, які схожі з відповідними операторами мови SQL, і оператори маніпулювання таблицями, тобто оператори самої реляційної алгебри. Останні включають такі ключові слова як INTERSECT, UNION, MINUS, INNER/LEFT/RIGHT JOIN, DIVIDE BY, WHERE та ін., що запропоновані в [2]. В мові передбачено пріоритетність операцій і використання дужок, тобто є можливість записувати вирази, що робить процес компіляції не простим. Наведемо приклад одного з можливих виразів маніпулювання з таблицями реляційної БД.

((TA,BLE1 minus TA,BLE2) where TA,BLE1.ATR1 = “good” and TABLE2.ATR4 > 120) union TA,BLE3) [ATR1, ATR2, ATR3, ATR4];

Послідовність виконання операторів наступна. Спочатку виконується операція віднімання (*minus*), над отриманим відношенням виконується операція вибірки (*where*), потім виконується операція об'єднання (*union*) цього відношення з відношенням/таблицею TA,BLE3 і останньою операцією є операція проєкції (*[...]*) отриманого після операції *union* відношення по атрибутах <ATR1, ATR2, ATR3, ATR4>. При цьому під час семантичного аналізу компілятор, зокрема, має перевіряти на сумісність відношень перед виконанням операцій *minus* і *union*.

Розглядалися кілька підходів для реалізації мови REAL. В результаті обрано генератор парсерів ANTLR (ANother Tool for Language Recognition) [3]. Він підтримує можливість роботи з багатьма сучасними мовами програмування: Python, C++, Java та ін.. Результат роботи даного інструменту є класи аналізаторів на мові обраній користувачем.

Побудова мови з використання інструменту ANTLR вимагає написання спеціалізованого файлу з набором граматичних правил, які будуть перетворені у лексичний та синтаксичний аналізатори. Перетворення створених правил у програмний код здійснюється застосунком на мові Java, що входить до складу пакету ANTLR: `java org.antlr.v4.Tool-Dlanguage=Python2 REALM_Union.g4` [4]. ANTLR підтримує можливість відображення синтаксичного дерева з використанням графічного інтерфейсу, як показано нижче на рисунку.

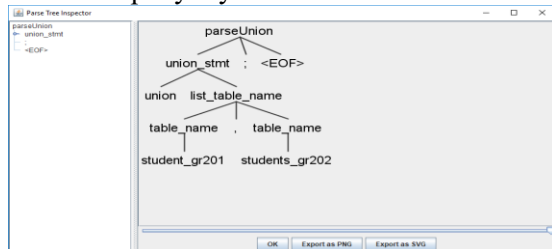


Рисунок – Синтаксичне дерево запиту Union

Виклик даного інструменту здійснюється також за допомогою `java`: `java org.antlr.v4.gui.TestRig REAL_Union parseUnion -gui input.txt`, де `input.txt` – файл, що містить запит на мові REAL, у даному випадку синтаксис запиту Union з переліком таблиць через кому.

Список використаних джерел:

1. Фаулер Мартин. Предметно-ориентированные языки программирования: Пер. с англ. М. : ООО “И.Д. Вильямс”, 2011. – 576 с.
2. Дейт К. Дж. Введение в системы баз данных. - Киев*Москва: Диалектика, 1998. - 787 с.
3. Теренс Парр. The Definitive ANTLR 4 Reference. - Pragmatic Bookshelf, 2011. – 322 с.
4. Документація інструментів ANTLR[Електронний ресурс]. – Режим доступу : URL : <https://github.com/antlr/antlr4/blob/master/doc/python-target.md> – Загол. з екрану/

ВИКОРИСТАННЯ ОНЛАЙН-КУРСІВ У НАВЧАННІ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

Дітковська Леся

Академія праці, соціальних відносин і туризму

Анотація

Це дослідження розкриває характеристики масових відкритих онлайн-курсів, визначає переваги використання онлайн-курсів у процесі навчання здобувачів вищої освіти, окреслює проблеми впровадження онлайн-курсів у навчальний процес вищих навчальних закладів.

Abstract

This research reviews the characteristics of massive open online courses, discusses the advantages of using online courses in the process of studying applicants for higher education, outlines problems of introducing online courses into the educational process of higher education institutions.

Вступ. Інтеграція України в міжнародний освітній простір ставить перед вищими навчальними закладами завдання підготовки висококваліфікованих фахівців, забезпечення доступу до якісної освіти, надання можливостей для навчання впродовж життя. Стрімкий розвиток інформаційно-комунікаційних технологій, піднесення мережевих технологій мотивує перехід до інноваційних форм навчання. Так, популярною потужною освітньою технологією стали масові відкриті онлайн-курси.

Метою цього дослідження є визначення переваг застосування та проблем впровадження онлайн-курсів у процес навчання здобувачів вищої освіти. Воно ґрунтується на аналізі літератури та власному досвіді слухача онлайн-курсів.

Результати. Закон України «Про освіту» забезпечує право кожного на освіту впродовж життя шляхом формальної, неформальної та інформальної освіти [1]. Сучасні студенти все частіше користуються можливостями навчання з використанням відкритих освітніх ресурсів та онлайн-курсів.

Перші масові відкриті онлайн-курси (MOOCs – massive open online courses), які зібрали величезну аудиторію, запустили у Стенфордському університеті у 2011 р. А вже у 2013 р. було створено перший український громадський проект масових відкритих онлайн-курсів Prometheus. Попит на масові безкоштовні онлайн-курси в Україні зростає. Слухачі онлайн-курсів можуть займатися у зручний час у зручному місці; опрацьовувати матеріали у комфортному темпі та при необхідності відтворювати їх повторно, що надає процесу навчання властивостей неперервності, гнучкості та мобільності. Маючи бажання, комп'ютер (планшет, смартфон) і доступ до глобальної мережі людина може не просто отримати інформацію з певної теми, а оволодіти відповідними знаннями і навичками. Так, «запровадження масових відкритих онлайн-курсів від провідних викладачів країни та світу дозволить допомогти українцям стати освіченими; підвищити кваліфікацію; опанувати суміжну галузь; отримати професійну онлайн-освіту з найпопулярніших спеціальностей; зробити найкращу освіту доступною кожному українському студенту» [2, С. 16].

Наразі, Європейська Комісія підтримала проект Virtual Mobility Pass щодо визнання навчання з використанням відкритих освітніх ресурсів та масових онлайн-курсів. В інноваційному «Паспорті навчання» «оцінки можуть бути задокументовані таким чином, що він може вважатися кваліфікацією вищої освіти» [3], що, на нашу думку, дозволить не втратити перспективних студентів, які можуть віддати перевагу західній освіті.

Поєднання традиційного, самостійного та онлайн навчання називають змішаним навчанням (blended learning). При змішаному навчанні, за висновками Sloan Consortium,

на опрацювання навчального матеріалу онлайн припадає від 30 % до 79 % часу, визначеного на засвоєння курсу [4].

Однією з моделей змішаного навчання є навчання з використанням онлайн-курсів (the blended MOOC). Навчальний онлайн-курс складається з коротких відеолекцій для ознайомлення з темою, практичних завдань, проміжних тестів, а також форуму для консультацій із викладачем та обговорення питань курсу з іншими слухачами. Аудиторні заняття присвячені розгляду найважливіших питань, виконанню лабораторних робіт та підсумковому оцінюванню знань студентів. Отже, є можливість прослухати лекції кращих викладачів, отримати найновішу інформацію, ознайомитись з актуальними технологіями.

Персональний профіль слухача онлайн-курсів налаштований таким чином, що можна відслідковувати досягнення і труднощі кожного. Викладач може одержувати відомості про успішність при виконанні конкретного завдання кожним студентом, загальну статистику перегляду відеоматеріалів, активність слухачів на форумі курсу [5]. Таким чином, враховуються індивідуальні особливості студента.

Пілотний проект 2017 р. зі змішаного навчання у чотирьох вищих навчальних закладах (ВНЗ) України показав, що поєднання онлайн-курсів із аудиторними заняттями підвищує ефективність навчання на 35 % [6]. А це, у свою чергу, відкриває перед студентами перспективу стати більш конкурентоспроможними і затребуваними. Крім того, результати змішаного навчання будуть занесені у диплом державного зразка.

Власний досвід залучення до онлайн-курсів свідчить, що при розробці навчального курсу актуальними є означення стратегій запобігання академічного плагіату; методи донесення інформації до слухачів курсу; наповнення тестів; рекомендації щодо підготовки до іспитів і планування часом.

До проблем впровадження онлайн-курсів слід віднести: залежність від технічних засобів; ступінь сформованості академічної доброчесності студентів, рівень їх ІКТ-компетентності та вмотивованість до самостійного опанування матеріалу.

Висновки. Процес інтеграції масових онлайн-курсів у навчальний процес ВНЗ спрямований на забезпечення конкурентоспроможності української освіти у міжнародному освітньому просторі. Така форма освіти дозволить навчати людей із обмеженими можливостями, збільшити кількість студентів заочної форми навчання, залучити іноземних студентів.

Подальшими завданнями вбачаємо розробку методики підготовки викладачів до використання масових онлайн-курсів в освітньому процесі.

Список використаних джерел:

1. Про освіту: Закон від 05.09.2017 № 2145-VIII // База даних «Законодавство України» / ВР України. URL: <http://zakon0.rada.gov.ua/laws/show/2145-19> (дата звернення: 27.02.2018).

2. Дітковська Л. А. Масові відкриті онлайн-курси Prometheus: реалії та перспективи // Мережеве суспільство: ринок праці, суспільні відносини, роль профспілок: Збірник матеріалів круглого столу (м. Київ, 22 березня 2018 р.) [Редкол.: Т. Семигіна, О. Корчинська, В. Співак]. К.: АПСВТ, 2018. С.16-17.

3. У Європі розроблений єдиний атестат онлайн-освіти. URL: http://osvita.ua/abroad/higher_school/distance-learning/44715/ (дата звернення 20.04.2018).

4. Allen I. E., Seaman J., Garrett R. Blending In: The Extent and Promise of Blended Education in the United States. 2007. 35 p. URL: <https://www.onlinelearningsurvey.com/reports/blending-in.pdf> (дата звернення: 19.04.2018).

5. Mintz S. The Future of MOOCs. 2014. URL: <https://www.insidehighered.com/blogs/higher-ed-beta/future-moocs> (дата звернення: 15.04.2018).

6. Змішана освіта: подружити «онлайн» і «офлайн». URL: <http://pedpresa.ua/178684-zmishana-osvita-podruzhyty-onlajn-i-oflajn.html> (дата звернення: 10.03.2018).

К РАЗРАБОТКЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ АВТОМАТИЗАЦИИ ОБУЧЕНИЯ ДИФФЕРЕНЦИРОВАНИЮ ФУНКЦИЙ

Заркуа Теодор

Европейский университет, проспект Давида Гурамишвили 76, Тбилиси, Грузия

Аннотация

Автор, опираясь на результаты, полученные им в направлении разработки инструментальных средств для автоматизации обработки функциональных выражений на уровне алгоритмических языков, предлагает подход для реализации сценария обучающей программы, покрывающей полный цикл обучения приемам аналитического дифференцирования функций.

Abstract

The author, relying on the results obtained by him in the direction of developing tools for automating the processing of functional expressions at the level of algorithmic languages, suggests an approach for implementing a script of a training program covering a full cycle of learning techniques for analytical differentiation of functions.

Введение

Благодаря программному обеспечению, предназначенному для автоматизации обработки функциональных выражений на уровне алгоритмического языка ([6]), стала возможна постановка задачи компьютерной реализации полнофункционального цикла автоматизации обучения дифференцированию функций.

Требования к обучающей программе

Для эффективной автоматизации процесса обучения по той или иной тематике, как правило, необходимо:

- уметь генерировать вопросы обучаемому в условиях управления сложностью вопроса;
- уметь определять правильность ответа, не ограничивая обучаемого жесткими требованиями формата этого ответа.

Применительно к тематике дифференцирования функций вышеизложенное означает, с одной стороны, умение генерировать разнообразные функциональные выражения для иллюстрации того или иного правила дифференцирования, а также для формирования задания обучаемому. А с другой стороны, умение установить тождественность ответа обучаемого с правильным ответом не ограничивая его необходимостью придать ответу вид, считающийся каноническим.

Серьезным подспорьем для решения обоих вопросов является возможность использования программного обеспечения, эквивалентного по своим возможностям описанному в [6]. Ведь совершенно очевидно, что для генерирования выражения удобнее использовать одну из бесскобочных (т.н. польских) форм записей. Причем каждая из этих форм удобна и для управления сложностью выражения, так как последнее определяется длиной выражения, набором операций (включая элементарные функции), входящих в него и максимальной глубиной стека при его преобразовании к инфиксной форме, что соответствует глубине вложенности скобок. Благодаря результатам, изложенным в [1-5], для наших целей вполне можно ограничиться использованием только префиксной бесскобочной формы функциональных выражений.

Что касается идентификации ответа, то эта проблема сродни той, которая решалась в [6] для упрощения выражения. Упрощение осуществлялось как раз на уровне

префиксной записи на основании определенных правил, которым была дана форма набора шаблонов. И так как для идентификации тождественности выражений только упрощения недостаточно (упрощение не позволяет учитывать, например, эффект от коммутативности той или иной операции или идентичность, достигаемую разными операциями) здесь имеет смысл задаться дополнительными правилами, которые позволят программно реализовать получение некоторого, единственного для всех тождественных выражений, вида данного выражения, которое можно назвать каноническим. В частности, для коммутативных операций необходимо будет определить дополнительное правило, в соответствии с которым однозначно определится последовательность операндов в канонической форме. Например, в соответствии с некоторым упорядочением. Совершенно ясно, что реализация данного подхода позволит исчерпывающе решить задачу идентификации правильного ответа.

Заключение

Вышеизложенный подход позволяет реализовать гибкий сценарий обучения, позволяющий оперативно реагировать на выполнение контрольных заданий обучаемым не только определением следующего шага обучения, но и регулированием степени сложности иллюстрационных примеров и контрольных ответов.

Очевидно, предлагаемый подход можно обобщить на любую обучающую программу, при условии наличия возможности регулирования сложности генерируемых примеров, а также наличия механизма автоматизации идентификации правильного ответа.

В дальнейшем представляется интересным разработка понятия удаленности от правильного ответа. Разумеется, подобная информация позволит еще более точно представить текущий уровень обучаемого и может быть использована для повышения эффективности процесса обучения.

Постольку поскольку, в основу предлагаемого подхода лежат понятия и алгоритмы, не привязанные к конкретному алгоритмическому языку, то соответствующие реализации легко переносимы с одного языка программирования на другой.

Список использованных источников:

1. Заркуа Т. К свойству перевернутой польской записи. Internet-Edication-Sciense-2008. New Informational and Computer Tecnologies in Education and Sciense. H. Intelligence Information Systems. 2008 year, p.543-544
2. Заркуа Т. Некоторые способы обработки функциональных выражений. Winter Programming School. Материалы зимней школы по программированию, Харьков, ХНУРЭ, 2009, p. 205-211
3. Zarkua T. An Approach to Functional Expressions Processing Automation. Billetin №2 of Saint Andrew the First-Called Georgian University of the Patriarchy of Georgia, Tbilisi, 2009, p. 50-61
4. Т.Заркуа.Автоматизация обработки функциональных выражений на уровне алгоритмических языков. Internet-Edication-Sciense-2010. New Informational and Computer Tecnologies in Education and Sciense.p.201-206.
5. Т.Заркуа.К вопросу об использовании понятия сопряженного по отношению к бесскобочным выражениям. Internet-Edication-Sciense-2012. New Informational and Computer Tecnologies in Education and Sciense.p.156-157.
6. Заркуа Теодор. Программное обеспечение на C++ для автоматизации обработки функциональных выражений. Internet-Edication-Sciense-2016. New Informational and Computer Tecnologies in Education and Sciense.p.159-163.

ЗАСТОСУВАННЯ СУЧАСНИХ ТЕХНОЛОГІЙ ТА ІННОВАЦІЙНИХ МЕТОДІВ НАВЧАННЯ У ВИЩИХ НАВЧАЛЬНИХ ЗАКЛАДАХ

Іванова Світлана

Державна інспекція навчальних закладів України

Аннотація

У статті розглядаються інноваційні методи навчання, які використовуються у системі сучасного освітнього процесу, визначені особливості засобів, форм і методів інноваційного навчання, розкривається специфіка їх використання в освітньому процесі.

Ключові слова: вища школа України, інновації, методи навчання, освітні технології, освітній процес, інформаційно-комунікаційні засоби навчання, онлайн-освіта, інформаційні технології.

Виникнення та розвиток інформаційного суспільства (ІС) припускає широке застосування інформаційно-комунікаційних технологій (ІКТ) в освіті, що визначається багатьма чинниками. Впровадження ІКТ у сучасну освіту суттєво прискорює передавання знань і накопиченого технологічного та соціального досвіду людства не тільки від покоління до покоління, а й від однієї людини до іншої. Сучасні ІКТ, підвищуючи якість навчання й освіти, дають змогу людині успішніше й швидше адаптуватися до навколишнього середовища, до соціальних змін. Це дає кожній людині можливість одержувати необхідні знання як сьогодні, так і в постіндустріальному суспільстві. Активне й ефективне впровадження цих технологій в освіту є важливим чинником створення нової системи освіти, що відповідає вимогам ІС і процесу модернізації традиційної системи освіти.

Важливість і необхідність впровадження ІКТ у навчання обґрунтовується міжнародними експертами і вченими. ІКТ торкаються всіх сфер діяльності людини, але, мабуть, найбільш сильний позитивний вплив вони мають на освіту, оскільки відкривають можливості впровадження абсолютно нових методів викладання і навчання. Інформатизація освіти - це перспективний шлях до розвитку суспільства. Навчання з використанням інформаційно-комунікаційних технологій має багато переваг, та звичайно, ми не повинні відмовлятися від традиційних ефективних методів навчання. Варто говорити про поєднання традиційних методів та новітніх технологій.

Нові інформаційні освітні технології на основі комп'ютерних засобів дають можливість значно підвищити ефективність. Інновації у навчальній діяльності пов'язані з активним процесом створення, поширення нових методів і засобів для вирішення дидактичних завдань підготовки фахівців у гармонійному поєднанні класичних традиційних методик та результатів творчого пошуку, застосування нестандартних, прогресивних технологій, оригінальних дидактичних ідей і форм забезпечення освітнього процесу [1].

Освітні інновації полягають в сучасному моделюванні, організації нестандартних лекційно-практичних, семінарських занять; індивідуалізації засобів навчання; розробці нової системи контролю оцінки знань; застосуванні комп'ютерних, мультимедійних технологій; навчально-методичної продукції нового покоління. Серед сучасних технологій навчання, можна виділити: особистісно-орієнтовані, інтеграційні, колективної дії, інформаційні, дистанційні, творчо-креативні, модульно-розвивальні тощо[2].

В освітній практиці диверсифікація навчальних технологій дозволяє активно і результативно їх поєднувати через модернізацію традиційного навчання та переорієнтацію його на ефективне, цілеспрямоване. За такого підходу акцентується на особистісному розвитку майбутніх фахівців, здатності оволодівати новим досвідом творчого і критичного мислення, рольового та імітаційного моделювання пошуку вирішення навчальних завдань та ін. [3]. Згідно із науковими положеннями

загальноприйняті методи викладання можна класифікувати за такими ознаками: види навчальних робіт студентів (усні, письмові; аудиторні, самостійні, позааудиторні); загальні (колективні, групові, індивідуальні та ін.); джерело одержання знань і формування навичок і вмінь (лекція, аналіз документа, робота із законодавчою базою, використання наочних засобів, інтернет-ресурсів тощо); ступінь самостійності та характер участі студентів у освітньому процесі (активні, інтерактивні, пасивні); рівень усталеності та новизни (традиційні, класичні, нестандартні, новаторські), авторство (оригінальні, авторські, загальні, дидактичні) та ін. У сучасній методиці викладання найбільш прийнятною виявилася класифікація, побудована на дієвому підході до навчання. Згідно з нею існують методи: а) які забезпечують опанування навчального предмета (словесні, візуальні, практичні, репродуктивні, проблемно-пошукові, індуктивні, дедуктивні); б) які стимулюють та мотивують навчально-наукову діяльність (навчальні дискусії, проблемні ситуації, професійно-орієнтовані ділові ігри, творчі завдання, пошук і дослідження, експерименти, конкурси, вікторини тощо); в) методи контролю і самоконтролю у навчальній діяльності (опитування, залік, іспит, контрольна робота, тестові завдання, питання для самоконтролю, у т. ч. через комп'ютерні освітні системи). Розглянемо окремі методики викладання з позиції їх новизни, ефективності, дієвості, доцільності використання у сучасних умовах інформатизації вищої школи. На сьогоднішньому ринку освітніх послуг такими є інноваційні активні та інтерактивні методики навчання. Оскільки суттєво зростає творча компонента освіти, активізується роль усіх учасників навчального процесу, зміцнюється творчо-пошукова самостійність студентів, особливої актуальності набули концепції проблемного та інтерактивного навчання, пов'язаного з використанням комп'ютерних систем. Під час такого освітнього процесу студент може комунікувати з викладачем он-лайн, вирішувати творчі, проблемні завдання, моделювати ситуації, включаючи аналітичне і критичне мислення, знання, пошукові здібності. Зокрема, сучасна методика викладання правничих наук має певний арсенал різноманітних способів, прийомів і засобів навчання, як загальнодидактичних (застосовуються у викладанні будь-яких навчальних предметів), так і галузеводидактичних (віддзеркалюють специфіку конкретної навчальної дисципліни або низки споріднених дисциплін) [4]. Серед «інноваційні методики викладання», інтерактивних методів, форм і прийомів, що найчастіше використовуються в навчальній роботі ВНЗ, слід зазначити такі, як аудіовізуальний метод навчання; брейнстормінг («мозковий штурм»); діалог Сократа (сократів діалог); «дерево рішень»; ділова (рольова) гра (студенти перебувають у ролі законодавця, експерта, юрисконсульта, нотаріуса, клієнта, судді, прокурора, адвоката, слідчого); майстер-класи; метод аналізу і діагностики ситуації; метод інтерв'ю (інтерв'ювання); метод проектів; моделювання; публічний виступ; тренінги індивідуальні та групові та ін.

Із впровадженням дистанційного навчання багато вузів уже сьогодні застосовують технологію онлайн-семінару під назвою «вебінар», який демонструє порівняльні таблиці, презентації, відеоролики тощо. За допомогою інтернет-технологій вебінар зберіг головну ознаку семінару – інтерактивність, яка забезпечує моделювання функцій доповідача, слухача, що працюватимуть інтерактивно, комунікуючи разом за сценарієм проведення такого семінару [5]. Ученими-практиками також розроблена й експериментально перевірена модель організації самостійної роботи студентів-юристів заочної форми навчання, яка передбачає три етапи: орієнтовний (підготовчий), діяльнісний (виконавчий), контрольно-корекційний (заклучний). Модель спрямована передусім на забезпечення підвищення рівня індивідуально-психологічної готовності студентів до самостійного навчання, оволодіння майбутніми юристами відповідними кваліфікаціями, набуття вмінь і навичок правової роботи, розвиток професійно значущих якостей особистості. Крім того, розкриваючи активні методи навчання здобувачів вищої освіти, необхідно також приділити увагу питанням соціально-психологічного тренінгу, в якому основним принципом виступає активна позиція кожного його учасника. Сутність і класифікація тренінгу, основні види вправ і процедур, етапи тренінгової роботи тощо зводяться до «зворотного зв'язку», який полягає у висловленні кожним учасником

власної думки з окремих питань навчального заняття. Включення в освітній процес активних форм навчання, у тому числі психологічних тренінгів, суттєво впливає на розвиток професійних та особистісних якостей майбутнього спеціаліста. Сучасні системи інтерактивного навчання юридичним дисциплінам доцільно розглядати як комплекси певним чином впорядкованих технологій (у т. ч. і технологій дистанційного навчання), що мають відповідну специфіку та логіку. Наприклад, інтерактивна система з викладання права може включати такі блоки, як: компетентнісний підхід до вивчення і викладання права (метод сократівського діалогу); «технологія продуктивної діяльності інтелекту», курс підвищення креативної компетентності; навчальні суди; робота у «юридичних клініках» тощо. У той же час при налагодженні зв'язку викладач – студент за допомогою онлайн-комунікації в інформаційному освітньо-науковому середовищі університетів необхідні суттєві консолідовані дії кафедр, інформаційних центрів, лабораторій, бібліотек для його наповнення якісними проблемно-орієнтованими ресурсами, як наслідок, забезпечення здобуття знань. Так, на фокус-опитуванні студентів-правознавців «чи допомагають електронні ресурси у вивченні фахових дисциплін» – 93% респондентів відповіли, що електронні навчальні комплекси, електронні підручники, інші навчально-методичні матеріали і віртуалізовані засоби є важливими в дистанційній освіті. Сучасний зміст освіти має орієнтуватися на використання інформаційних технологій, поширення інтерактивного, електронного навчання з доступом до цифрових ресурсів та інтелект-навчання для майбутнього [6].

Дуже актуальним зараз постає питання розширення самостійної роботи студентів. Навчальні платформи, наприклад Moodle можуть ефективно задовольнити потреби студента, а викладач отримує можливість запропонувати свої напрацювання та організувати контроль навчання. Інформаційно-комунікаційні технології змінили схему передачі знань та методи навчання, створили нові засоби впливу і значно підвищують ефективність знань.

У сучасному освітньому процесі проблема інноваційних методів навчання залишається однією із актуальних у світовій педагогічній і науково-дослідній діяльності, яка в умовах трансформаційних змін у вищій школі потребує постійного ретельного вивчення та науково-практичного обґрунтування питання: кращого досвіду інноваційної освітньої діяльності; характеристики змісту інтерактивних форм навчання, специфіки їх використання у вищих навчальних закладах.

Список використаних джерел:

1. Інноваційні педагогічні технології: теорія та практика використання у вищій школі : монографія / І. І. Доброскок, В. П. Коцур, С. О. Нікітчина [та ін.] ; Переяслав-Хмельниць. держ. пед. ун-т ім. Г. Сковороди, Ін-т пед. освіти і освіти дорослих АПН України. – Переяслав-Хмельниць. : Вид-во С. В. Карпук, 2008.
2. Лисенко М. В. Інноваційна парадигма вищої освіти України за умов переходу до інформаційного суспільства : автореф. дис.канд. філос. наук : 09.00.10 / Лисенко Микола Владиславович ; М-во освіти і науки, молоді та спорту України, Нац. техн. ун-т України «Київ. політехн. ін-т». – К., 2013.
3. Інновації у вищій освіті: проблеми, досвід, перспективи : монографія / П. Ю. Саух [та ін.] ; ред. П. Ю. Саух. – Житомир : Вид-во ЖДУ ім. І. Франка, 2011.
- 4.8. Абдалова О. И. Использование технологий электронного обучения в учебном процессе / О. И. Абдалова, О. Ю. Исакова // Дистанц. и виртуал. обучение. – 2014. – №12.
5. Галиця І. Інтелектуально-конкурентні ігри як креативний механізм активізації педагогічного, наукового та інноваційного процесів / І. Галиця, О. Галиця // Вища шк. – 2011. – №1.
6. Фатхутдінова О. В. Впровадження нових технологій в процесі підготовки спеціалістів правознавства / О. В. Фатхутдінова // Гуманіт. вісн. Запоріж. держ. інж. акад. – 2012. – Вип. 48.

ЄДИНЕ МЕРЕЖЕЦЕНТРИЧНЕ ІНФОРМАЦІЙНО-ОСВІТНЄ СЕРЕДОВИЩЕ ЗАГАЛЬНООСВІТНІХ НАВЧАЛЬНИХ ЗАКЛАДІВ

Пасіхов Юрій

Лабораторія ІКТ фізико-математичної гімназії Вінницької міської ради,

Анотація

Розглянуто проблему створення єдиного мережецентричного інформаційно-освітнього середовища регіону за запропоновано модель його створення на базі досліджень та розробок ЛІКТ ФМГ17.

Abstract

The problem of creation of a unified network-centered educational and educational environment of the region is considered, for the proposed model of its creation on the basis of research and development LIKT PMG17.

Вступ

Сьогодні технологічна основа конструктивної розбудови інформаційного суспільства знаходиться у площині взаємозв'язків між процесами, які визначають рівні розвитку освіти і науки. Парадигмою сучасного інформаційного суспільства є мережецентрична взаємодія між усіма його інституціями та системними складовими. Це призводить до того, що сучасні вчителі втрачають позиції бути єдиним джерелом знань у процесі еволюції освіти в інформаційному суспільстві. А вплив категорії трикутника знань на рівень змісту сучасного навчально-пізнавального процесу визначає його існування та подальше забезпечення доступу учнів до коректних, за змістом інформаційних джерел. Всесвітня мережа стала саме тим середовищем, де розгортається когнітивно-комунікативний сценарій розвитку освіти. Центральною їх ланкою є технології інженерії знань, які ґрунтуються на використанні IT-BigData, Semantic-WEB та Data Mining, що надає можливість забезпечити усі процеси управління знаннями в освітньому середовищі. Тому успішність даного напрямку багато в чому визначаються інтелектуальним рівнем і загальною ефективністю взаємозв'язків між мережевими інформаційно-освітніми системами.

1. Постановка проблеми

Використання знаннево-орієнтованих ІТ у навчально-виховному процесі дозволяє підвищити ефективність навчання, а також сприяє розвитку пізнавального інтересу учнів до здійснення навчально-дослідницької діяльності, формує позитивну мотивацію до вивчення. Створення середовища ефективної взаємодії усіх учасників навчально-виховного процесу (від учнів, вчителів, батьків, експертів-методистів до управлінців) можливе за умови використання електронних підручників, репозиторіїв цифрових освітніх ресурсів, віртуальних лабораторій, мультимедійних засобів навчання, рейтингових систем оцінювання навчальних досягнень учнів тощо. Крім того, вказані засоби сприятимуть розвитку критичного мислення та рефлексії учнівської молоді, оскільки вони залучаються до моделювання об'єкта вивчення та можуть спостерігати й оцінювати результати своїх дій.

За допомогою сучасних знаннево-орієнтованих ІТ відбувається формування єдиного мережецентричного інформаційно-освітнього середовища, що сприятиме систематизації набутих знань, формуванню інформатичної культури учня-дослідника. На його платформі для кожного учня та вчителя створюються відповідні електронні

площадки. Адже суспільно-політична, соціально-економічна ситуація в Україні вимагає створення та поширення єдиної ідеологічної концепції взаєморозуміння. Одним із шляхів реалізації цієї концепції є запровадження мережевих механізмів взаємодії усіх складових навчально-виховного процесу, формування культури мислення, розвиток творчих та дослідницьких здібностей учнівської молоді – майбутнього нашої нації.

З урахуванням науково-практичної значущості проблеми була сформульована тема нашої дослідно-експериментальної роботи: «Науково-методичні засади формування єдиного мережецентричного інформаційно-освітнього середовища навчальних закладів регіону».

2. Об'єкт дослідження – процес формування єдиного мережецентричного середовища в загальноосвітніх навчальних закладах.

3. Предмет дослідження – науково-методичні засади формування єдиного мережецентричного середовища в загальноосвітніх навчальних закладах.

4. Мета дослідження – науково обґрунтувати та експериментально перевірити ефективність науково-методичних засад формування єдиного мережецентричного середовища загальноосвітніх навчальних закладів, що безумовно, забезпечить інтегроване використання науково-освітніх ресурсів на засадах єдиного інформаційного простору в педагогічній системі освіти України.

5. Гіпотеза дослідно-експериментальної роботи полягає у припущенні формування єдиного мережецентричного середовища загальноосвітніх навчальних закладів, ефективність якого залежатиме від:

1) *концептуалізації* науково-методичних засад формування єдиного мережецентричного середовища загальноосвітніх навчальних закладів, орієнтованих на забезпечення ефективної взаємодії суб'єктів освітньої діяльності;

2) *технологізації* процесу формування єдиного мережецентричного середовища загальноосвітніх навчальних закладів, що передбачає розроблення та впровадження відповідної знаннєво-орієнтованої мережецентричної ІТ для розвитку інформатичної культури учнів у процесі навчально-дослідницької діяльності;

3) *розвитку та самореалізації* суб'єктів освітньої діяльності в умовах єдиного мережецентричного середовища, що передбачає створення електронних освітніх ресурсів та відповідних електронних площадок взаємодії між ними.

6. Завдання дослідно-експериментальної роботи.

1. Здійснити аналіз моделей єдиного освітнього простору систем освіти, дослідити їх характеристики та ефективність застосування в умовах глобалізації світового освітнього простору.

2. Вивчити стан розробленості проблеми формування єдиного мережецентричного середовища загальноосвітніх навчальних закладів для забезпечення ефективної взаємодії усіх суб'єктів освітньої діяльності.

3. З'ясувати зміст, структуру понять «мережецентричне середовище», «ефективна навчальна взаємодія», «інформатична культура», «репозиторій електронних освітніх ресурсів».

4. Уточнити та науково обґрунтувати критерії, показники, рівні розвитку інформатичної культури усіх школярів засобами навчально-дослідницької діяльності та підібрати відповідний діагностичний інструментарій.

5. Науково обґрунтувати та експериментально перевірити ефективність концепції формування єдиного мережецентричного середовища загальноосвітніх навчальних закладів.

6. Розробити та експериментально перевірити ефективність знаннєво-орієнтованої ІТ забезпечення ефективної навчальної взаємодії усіх суб'єктів освітньої діяльності.

7. Розробити мережеві засоби програмно-інформаційного та навчально-методичного забезпечення формування та розвитку єдиного мережецентричного середовища загальноосвітніх навчальних закладів.

7. Висновки

Існує нагальна необхідність створення мережецентричного освітнього середовища регіону, створення свого роду освітнього «кампусу». Заклад вищої освіти (в даному випадку ВНТУ) повинен мати в цьому процесі провідні позиції.

Список використаних джерел

1.Пасіхов Ю.Я. “З досвіду створення гімназійного вузла Інтернет та використання його можливостей в навчальному процесі” // Матеріали першої міжнародної науково-методичної конференції “ІнтернетОсвіта-Наука-98” УНІВЕРСУМ-Вінниця, 1998, ст 44-54;

2.Пасіхов Ю.Я. Впровадження дистанційної підтримки традиційних форм освіти в середній школі // ІНТЕРНЕТ-ОСВІТА-НАУКА-2006, П'ята міжнародна конференція ІОН-2006, 10-14 жовтня, 2006. Збірник матеріалів конференції. Том 1. – Вінниця: УНІВЕРСУМ-Вінниця, 2006. – С. 438-447

3.А.Е. Стрижак Применение локально-адаптивной мириадной фильтрации для комплексной модели одномерного сигнала / Н. О. Тулякова, Р. Ю. Лопаткин, А. Н. Трофимчук, А. Е. Стрижак // Радіоелектронні і комп'ютерні системи, – 2017. – № 3 (83) – с. 14–25.

ТЕХНОЛОГІЯ ТЕСТУВАННЯ ЗНАНЬ

Савчук Тамара¹, Філіпов Владислав¹, Іванова Світлана²

¹Вінницький національний технічний університет

²Державна інспекція навчальних закладів України

Анотація

Запропоновано технологію тестування знань, що базується на використанні нечіткої логіки, дає можливість адекватно оцінити знання фахівця з дисципліни, оперуючи даними, що були отримані в ході тестування, а також передбачає етап самотестування для оцінювання своїх знань з означеної тематики й отримання рекомендацій з їх удосконалення.

Ключові слова: нечітка логіка, тестування знань, база знань, база даних, автоматизований програмний засіб, знання

Abstract

The use of fuzzy logic to solve the intellectual problem of testing knowledge is proposed. The advantages of using this method over others, such as: the use of artificial neural networks and the method of group input of arguments, are given. It has been found that software tools capable of implementing such an approach are not limited to a set of typical tasks and can evaluate deployed answers to questions.

Key words: fuzzy logic, knowledge testing, knowledge base, database, automated software, knowledge

Для підвищення якості оцінювання знань фахівців, що здобувають освіту у закладах вищої освіти, важливим аспектом є об'єктивність самого процесу. Для цього доцільно використовувати автоматизовані програмні засоби, що здатні розв'язувати інтелектуальні задачі.

Так як задача тестування знань є задачею віднесення результатів тестування до певного класу оцінок, її можна трактувати як класичну інтелектуальну задачу класифікації [1], розв'язок якої може бути отриманим за відомими методами класифікації [2]. При цьому, результати тестування може представляти нечіткий, слабо структурований набір даних.

Найбільшого поширення на сьогодні набули два методи розв'язання подібних задач:

– Використання штучних нейронних мереж [3].

– Метод групового врахування аргументів – заснований на рекурсивному селективному відборі моделей, на основі яких будуються складніші моделі [4].

Штучні нейронні мережі потребують багато часу на навчання, і зі збільшенням кількості параметрів, що класифікуються, час значно зростає, що ускладнює їх використання при тестуванні знань, коли важливо в обмежений проміжок часу оцінити знання з урахуванням потужної кількості параметрів та характеристик. При цьому, штучна нейронна мережа не може враховувати особливості та оригінальність застосування засвоєних теоретичних знань до вирішення практичних задач. До того ж, даний метод не здатний оперувати не чітко заданими даними, або даними, що слабо структуровані.

В методі групового врахування аргументів після досягнення певного рівня складності моделі, середньоквадратичне відхилення починає зростати, тому похибка оцінювання знань при тестуванні з великою кількістю параметрів та характеристик може не відповідати об'єктивній.

Крім того, для роботи програмних засобів, що реалізують означені методи, необхідна потужні ресурси процесору та оперативної пам'яті, що є неприйнятним для використання на мобільних платформах, які є обмеженими в них та залежними від часу роботи від акумулятора [5].

Отже, актуальною є задача розробки підходу до вирішення інтелектуальної задачі тестування знань з використанням нечіткої логіки, що дасть можливість приймати рішення при оцінювання знань в умовах обмеженої визначеності.

До переваг використання нечіткої логіки, для задачі тестування знань, слід віднести такі [6]:

4. можливість оперувати вхідними даними, заданими нечітко: наприклад, відповідями на запитання, що потребують розгорнутої відповіді;

5. можливість нечіткої формалізації критеріїв оцінювання знань;

Слід відзначити важливість забезпечення самотестування знань аби кожен тестуємий зміг оцінити складність та глибину тестування з означеної тематики, а також отримати рекомендації з удосконалення своїх знань відповідно до необхідного ступеню деталізації їх вивчення. Серед існуючих варіантів автоматизованих рішень щодо тестування знань означений функціонал відсутній. З використанням такого підходу стає можливим оцінювання студентів за розгорнутими відповідями на складні запитання.

Алгоритм тестування знань можна подати діаграмою активності, що включатиме такі основні кроки:

1. Здійснюється активація додатка та усіх необхідних йому сервісів.
2. Якщо користувач зареєстрований, то відбувається вхід в систему з урахуванням рівня доступу. Якщо користувач не зареєстрований, то відбувається його реєстрація.
3. Визначення режиму тестування.
4. Якщо це режим безпосереднього тестування, користувач отримує завдання для тестування знань з подальшим оцінюванням результатів. Результати тестування фіксуються.
5. Якщо це режим самотестування, користувач отримує завдання з подальшим оцінюванням результатів та отриманням рекомендацій по удосконаленню знань. Результати тестування не фіксуються.
6. Також користувач може звернутися до бази знань з усіма навчальними матеріалами.

Діаграма активності при тестуванні знань наведена на рисунку 1.

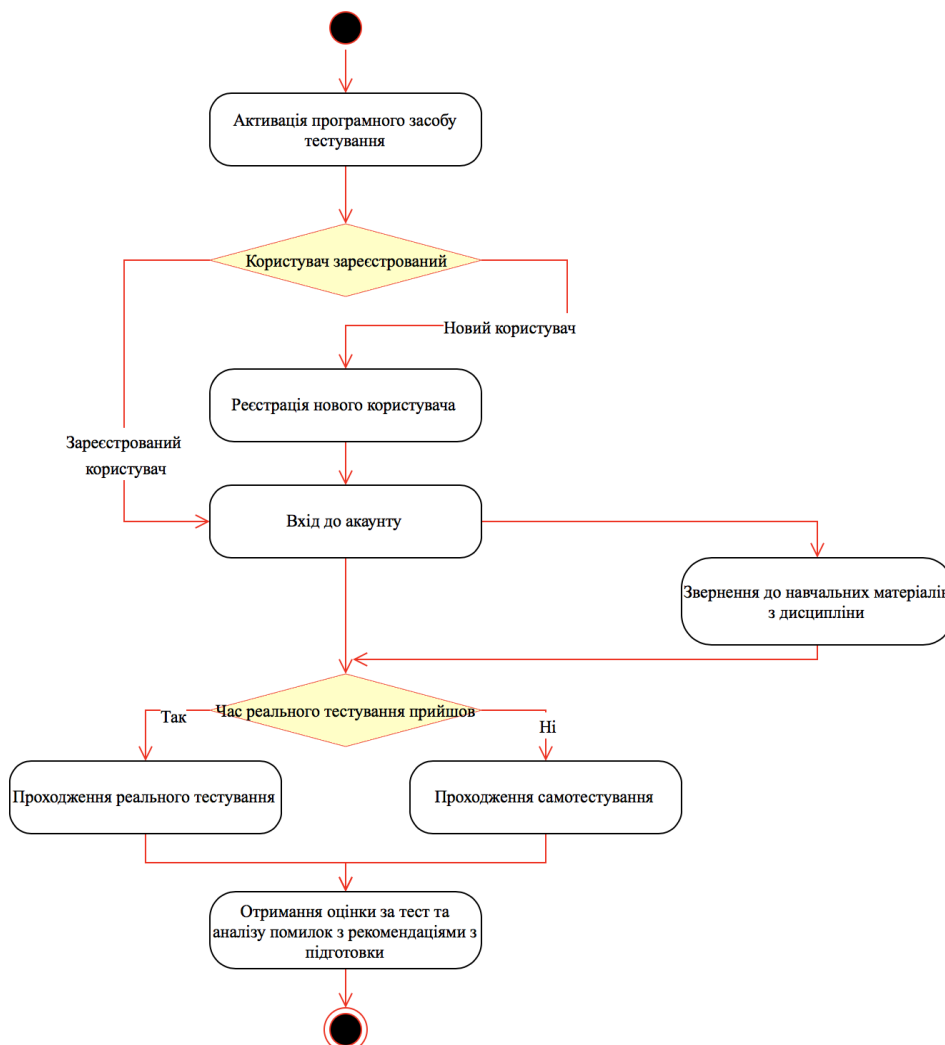


Рисунок 1 – Діаграма активності користувача модуля тестування знань

Таким чином, запропонована технологія тестування знань, що базується на використанні нечіткої логіки, дає можливість адекватно оцінити знання фахівця з дисципліни, коректно оперуючи даними, що були отримані в ході тестування та могли бути задані неточно, а також передбачає етап самотестування для оцінювання своїх знань з означеної тематики й отримання рекомендацій з їх удосконалення. Отримані дані обробляються індивідуально для кожного тестуємого, що вирішує проблему врахування індивідуальних особливостей застосування фахівцями засвоєних теоретичних знань.

Список використаних джерел:

1. Huajin Tang, Kay Chen Tan, Zhang Yi. Neural Networks: Computational Models and Applications [Text] / H. Tang, K. C. Tan, Z. Yi – Springer Science & Business Media, 2007. – 300 p.
2. Crina Grosan, Ajith Abraham. Intelligent Systems: A Modern Approach [Text] / C. Grosan, A. Abraham. – Berlin : Springer-Verlag Berlin Heidelberg, 2011. – 450 p.
3. Sumi Helal, Wendong Li, Raja Bose. Mobile Platforms and Development Environments (Synthesis Lectures on Mobile and Pervasive Computing) [Text] / S. Helal, W. Li, R. Bose. – Morgan & Claypool Publishers, 2012. – 120 p.
4. Timothy J. Ross. Fuzzy Logic with Engineering Applications [Text] / T. J. Ross. – New Mexico : Wiley, 2010. – 606 p.

	 ОДИНАДЦЯТА МІЖНАРОДНА КОНФЕРЕНЦІЯ ІОН - 2018 ІНТЕРНЕТ-ОСВІТА-НАУКА-2018	
	СЕКЦІЯ G. ГЕОІНФОРМАЦІЙНІ СИСТЕМИ	
	 THE ELEVENTH INTERNATIONAL CONFERENCE IES-2018 INTERNET-EDUCATION-SCIENCE - 2018	
	SECTION G. GEOINFORMATION SYSTEMS	
	 ОДИННАДЦАТАЯ МЕЖДУНАРОДНАЯ КОНФЕРЕНЦИЯ ИОН-2018 ИНТЕРНЕТ– ОБРАЗОВАНИЕ – НАУКА 2018	
	СЕКЦІЯ G. ГЕОІНФОРМАЦІОННІ СИСТЕМИ	
VNTU VINNYTSIA NATIONAL TECHNICAL UNIVERSITY 2018		

ПРИНЦИПИ ТА МЕТОДОЛОГІЯ АКТИВНОЇ ПРОТИДІЇ БПЛА ЗА АЛГОРИТМОМ АКАД

Троцишин Іван

Одеська національна академія зв'язку ім. О.С.Попова

Анотація

В сучасному світі БПЛА (дрони) набувають всеохоплюючого застосування для освоєння повітряного простору, та окрім позитивних рис, містять і значну загрозу мирному існуванню людства, створивши особливий акаунт. якому немає ефективної протидії. Технологія АКАД в значній мірі допомагає принципово вирішити вказані проблеми, створивши ефективну систему «фізичного знищення» БПЛА які виходять за межі надання послуг невійськового застосування.

Abstract

In the modern world, UAVs (drones) acquire an all-inclusive application for the development of airspace, and in addition to positive features, they also present a significant threat to the peaceful existence of humanity by creating a special account. which has no effective counteraction. The AKAD technology greatly helps to resolve these problems in principle by creating an effective system of "physical destruction" of UAVs that go beyond the scope of providing non-military services.

Вступ

Питання використання БПЛА, які стрімко розвиваються, і захоплюють весь повітряний простір, від декількох метрів, до одиниць і десятків кілометрів. Але найбільш небезпечними з точки зору використання, не лише як засобів ефективної повітряної розвідки, але також як ударних засобів для нанесення прицільних точкових знищень об'єктів наземної інфраструктури. На відміну від ППО і ПРО, які зорєєнтовані на «габаритні цілі», БПЛА, особливо малого класу (до 60-90см), випадають із зони виявлення, ну і відповідно стають «невидимими» але досить небезпечними повітряними засобами, як розвідки, так і нанесення вражаючих дій. Тому питання активної протидії БПЛА все більш гостро встає на порядку денному, але не дивлячись на існуючий парк засобів, ефективної протидії не запропоновано.

Основна частина

На рис 1. приведено в сучасні види БПЛА, які масово використовують як, в мирних, так і військових цілях, але також нові конструкції постійно з'являються.



Рисунок 1- Типові види сучасних БПЛА

У відкритому доступі не міститься жодної інформації про АНТИ-ДРОНИ типу «камікадзе», хоча це питання дискутується, але практичних наслідків не має.

Існуючі системи ППО і РЕБ лише частково можуть вирішити проблему блокування БПЛА (лише в активному режимі), але це потребує значних витрат (сотні тисяч мільйонів дол), і в принципі неможливо боротися із «малогабаритними» БПЛА, особливо які йдуть за програмою пасивного керування.

Всі активні системи протидії використовують радіовипромінювання (підсвічують себе перед нападником), в той же час АНТИ-ДРОН «камікадзе» використовує комбіновану систему самонаведення, і містить «місцеву РЕБ», чого не міститься в жодній системі протидії.

Реалізація комплексу можлива у вигляді автономних БПЛА «камікадзе», так і у вигляді модулів до існуючих моделей БПЛА (шляхом приєднання модуля АКАД та його прицільної адаптації), що в разі збільшує можливості використання (особливо в масових моделях).

Основним принциповим підходом є використання квантової теорії вимірювального перетворення, яка ПРИНЦИПОВО забезпечує ОДНОЧАСНЕ покращення в 10-100 разів і точності і швидкості вимірювальних операцій, в режимах відстеження, самонаведення, а також радіопеленгації і селективного радіоблокування систем керування та радіообміну БПЛА-цілі.

Основним вузлом є блок відслідкування та автонаведення, який може бути вмонтованим у БПЛА-АКАД, або ж, окремий приєднуваний модуль, до існуючих моделей БПЛА, які серійно випускаються, шляхом перепідключення каналів «верх-низ» і «ліво-право»

Технологія АКАД (аерокобра-антидрон), передбачає виявлення, відслідковування та нейтралізацію БПЛА в зоні територій які потребують захисту від повітряних об'єктів.

Принцип дії відповідає поведінці реальних об'єктів (кобри) на етапах вистеження і полювання на жертву, включаючи далеке виявлення (оптичне, радіопеленгація, інфрачервоне самонаведення), захоплення цілі, запуск за напрямком відстеження цілі, (дальня зона), перехід в зону теплового наведення (ближня зона), із одночасним блокування каналів зв'язку, які були індикатором радіопеленгу.

Алгоритм та сукупність комплексної дії різних систем самонаведення і радіоподавлення забезпечує (як після плювка ядом у реальної кобри), стабілізацію руху БПЛА, та створення ідеальних умов для виконання функції КАМІКАДЗЕ, (укус знедвиженої жертви коброю) стосовно цілі БПЛА - порушника повітряного простору.

Вказана технологія є подвійного застосування (військового (нейтралізація розвідувально-диверсійних польотів над закритими об'єктами), та цивільного (захистити об'єкти територій приватної власності від відео фото знімання).

Реалізація комплексу можлива у вигляді автономних БПЛА «камікадзе», так і у вигляді модулів до існуючих моделей БПЛА (шляхом приєднання модуля АКАД та його прицільної адаптації), що в разі збільшує можливості використання (особливо в масових моделях).

Основним принциповим підходом є використання квантової теорії вимірювального перетворення, яка ПРИНЦИПОВО забезпечує ОДНОЧАСНЕ покращення в 10-100 разів і точності і швидкості вимірювальних операцій, в режимах відстеження, самонаведення, а також радіопеленгації і селективного радіоблокування систем керування та радіообміну БПЛА-цілі.

Всі існуючі системи ПВО і ПРО не здатні виконувати весь комплекс протидії БПЛА, у всьому світі (наприклад «Петріоти і Томагавки» не збили жодного малагабаритного БПЛА), а існуючі спроби різних підходів, не мають достатнього ефекту саме із за використання «класичних вимірювальних та перетворювальних технологій для радіосигналів», в широкому їх розумінню.

В той же час, переваги у 10-100 разів, за «постійним для класики параметром ТОЧНІСТЬхШВИДКОДІЯ», новітніх підходів, які надає Квантова теорія вимірювальних

перетворень (КТВП), і чіткого дотримання технології АКАД, забезпечує простий у користуванні (оператора можливо навчити за кілька хвилин), і простотою запуску КАМІКАДЗЕ, який має автономне самонаведення, і стійкий до РЕБ та інших систем захисту, і працює на принципах реалізованих у відомій «Кольчусі».

Основним вузлом є блок відслідкування та автонаведення, який може бути вмонтованим у БПЛА-АКАД, або ж, окремий приєднуваний модуль, до існуючих моделей БПЛА, які серійно випускаються, шляхом перепідключення каналів «верх-низ» і «ліво-право», що дозволяє оптимізувати цінову політику, і вартість знешкодження БПЛА антидромом - КАМІКАДЗЕ. Розроблено (КТВП), яка забезпечує ОДНОЧАСНЕ покращення в 10-100 разів і точності і швидкості вимірювальних операцій, в режимах відстеження, самонаведення, а також радіопеленгації і селективного радіоблокування систем керування та радіообміну БПЛА-цілі.

Останні події із використання безпілотних апаратів для знищення військових баз на Харківщині, Запоріжській області та зоні АТО в Донецькій області, підтвердили проблему, яку США, Франція, Ізраїль, Арабські Емірати, заявили як однією із основних світових загроз безпеці, враховуючи безсилість існуючих систем ППО і ПРО стосовно БПЛА, та дронів, парк яких розвивається неконтрольовано, і їх використання для терористичних цілей стає все більш небезпечним. Для України це також одна із найбільших загроз, особливо у стані гібридної війни.

Єдиним безальтернативним і ефективним напрямом вирішення вказаної проблеми може слугувати запропонований нами напрямок розроблений під назвою «Принципи та методологія активної протидії БПЛА за алгоритмом АКАД».

Основна ідея: враховуючи підтверджену на практиці про неможливість ефективної протидії стосовно БПЛА, які несли термітні та фосфорні елементи враження, систем ППО (включаючи радіолокаційні), зенітних систем, і стрілецької зброї, а також враховуючи, що дані дії мали дистанційне керування, ефективним буде саме запропонований підхід, використання принципу «камікадзе», із використання одноразових БПЛА (аналогічного класу), із системами пасивного та активного самонаведення.

Захист об'єктів територій приватної власності від відео та фото знімання, є типовим «громадським» застосування системи АКАД.

Вартість типового БПЛА _АНТИДРОН не буде перевищувати 400-500 дол.

Приставка для встановлення на наявні БПЛА не буде перевищувати 100 дол.

Нейтралізація розвідувально-диверсійних польотів над закритими об'єктами є найбільш широким застосування розробленої системи БПЛА-АКАД.

Умови поставки спецтехніки на об'єкти під Держохороною, аналогічні приватним, але в будь якому разі менша 600-700 дол. за комплект.

Висновки

Простий у користуванні БПЛА _АНТИДРОН (оператора можливо навчити за кілька хвилин), і простотою запуску КАМІКАДЗЕ, який має автономне самонаведення, і стійкий до РЕБ та інших систем захисту, робить систему АКАД безальтернативною.

У приватних застосуваннях, вартість «брухту який впаде на приватну територію» в рази перевищуватиме витрати на АНТИДРОН, що робить проект економічно привабливим, а для військових систем він не має АЛЬТЕРНАТИВИ.

Розроблено блок відслідкування та автонаведення, який може бути вмонтованим у БПЛА-АКАД, або ж, окремий приєднуваний модуль, до існуючих моделей БПЛА, які серійно випускаються, шляхом перепідключення каналів «верх-низ» і «ліво-право».

Для завершення проекту потрібно встановити (виготовити) систему БПЛА – АНТИДРОН, та провести його польові (натурні) випробування.

ЗАХИСТ ДАНИХ В ЗАДАЧАХ НАВІГАЦІЇ В PHYSICAL WEB

Семеренко Василь, Кошолоп Микола

Вінницький національний технічний університет

Анотація

Розглянуто навігацію в закритих приміщеннях в рамках технології Physical Web. Показана можливість виправлення помилок в повідомленнях від маячків iBeacon та AltBeacon за допомогою завадостійкого кодування. Пропонується використання в межах стандартизованих форматів повідомлень двох полів CRC для реалізації ітеративного декодування циклічних кодів з примітивними породжувальними поліномами.

Abstract

The indoor navigation using beacons with Physical Web technology is considered. The capability to correct errors in messages from iBeacon and AltBeacon with the help of error correcting coding is shown. It is proposed to use two CRC fields within the standardized message formats to implement iterative decoding of cyclic codes with primitive generator polynomials.

Вступ

Ми знаходимось на початку якісно нового використання Інтернету – Інтернету Речей (Internet of Things, IoT). IoT дозволить підключити до традиційної мережі WWW широку сукупність електронних пристроїв, зв'язуючи між собою цифровий та фізичний світ [1].

В наш час багато об'єктів повсякденного життя ще не можуть безпосередньо встановити зв'язок із всесвітньою Мережею по традиційним інтерфейсам. Для підключення таких пристроїв були створені спеціальні ідентифікаційні мітки. Вперше ідея таких міток була реалізована ще на початку 2000-х років у вигляді радіоміток RFID та QR-кодів. Однак із-за складності реалізації та проблем із забезпечення захисту даних ці мітки не набули масового поширення.

Принципово інші підходи були закладені в рамках технології Physical Web [2], яка поєднала так звані “маячки” (англ. beacons) та посередницькі веб-сервіси. Хоча ідея цієї технології вперше була запропонована Google, сьогодні від цим загальним терміном розуміють проекти різних фірм: Apple, Radius Network та ін.

Навігація в Physical Web

У світі існують три найбільш популярні стандарти маячків:

- iBeacon (від Apple);
- AltBeacon (від Radius Network);
- Eddystone (від Google).

Сучасні маячки – це мініатюрні передавачі, які регулярно передають Bluetooth-сигнали з низьким енергоспоживанням. Ці сигнали можуть бути прийняті мобільними телефонами (смартфонами) на деякій відстані (до 50 метрів на відкритій місцевості та дещо меншій відстані у закритих приміщеннях). Далі запити передаються на хмарні сервіси для подальшого аналізу та видачі необхідного результату. А самим маячкам не потрібен доступ до Інтернету, що значно спрощує їх структуру і вартість.

Така технологія обробки інформації дозволяє ефективно розв'язати зовсім нові задачі, зокрема задачу навігації [3]. На відміну від GPS, маячки в основному використовуються для Indoor-навігації, тобто для навігації в закритих приміщеннях великого обсягу: торгових залах, складах, лікарнях тощо. Завдяки своїй простоті можна використати велику кількість маячків і розташувати їх в різноманітних місцях [4] (рис. 1).



Рисунок 1 – приклади маячків від різних виробників

GPS-навігація та Indoor-навігація взаємно доповнюють одна одну і можуть використовуватись спільно. Варто відзначити, що математичні основи просторової навігації однакові в різних фізичних системах: є сукупність базових точок з відомими координатами і необхідно визначити координату однієї додаткової точки. В обох системах можна використовувати метод тріангуляції (вимірювати кути прикутників) та метод трилатерації (вимірювати сторони трикутників).

Обчислення відстані в Indoor-навігації виконується за декілька етапів [5]. Спочатку смартфон отримує індикатор потужності прийнятого сигналу (*Received Signal Strength Indicator* – *RSSI*) і порівнює його з еталоном (рівнем сигналу, який був виміряний на відстані 1 метра від передавача). На другому етапі вибираються три маячки з кращими середніми значеннями *RSSI*, які будуть виконувати роль трьох базових точок. Далі методом трилатерації по трьом базовим точкам будуються трикутники в тривимірному просторі для обчислення координат спостерігача.

Для уточнення результатів необхідна подальша математична обробка даних, наприклад, за допомогою фільтра Калмана.

Організація захисту даних в Physical Web

Важливою складовою при роботі з інформацією в Інтернеті є її захист. Під цим розуміють два типи захисту: а) забезпечення секретності даних, що передаються; б) захист даних від спотворення внаслідок впливу навколишнього середовища.

Перший тип захисту – криптозахист на основі еліптичних кривих – використовується в маячках *Eddystone*, оскільки маячки в цьому форматі передають важливий контент (посилання на сайти та ін.).

Маячки *iBeacon* та *AltBeacon* використовуються лише для задач навігації, тому немає потреби в шифруванні їх повідомлень. Основною проблемою в цих задачах є забезпечення безпомилкової передачі ідентифікаційних даних маячка та значення *RSSI*. А на коректність передачі даних впливають багато факторів: структура антени маячків, рівень шумів, наявність різноманітних перешкод на шляху сигналів [3]. Вирішити цю проблему можна за допомогою завадостійкого кодування [6].

Розглянемо детальніше формати повідомлень від маячків *iBeacon* та *AltBeacon*, які містять поля ідентифікації маячка, поле *RSSI* та поле CRC (рис. 2). Перед кожною передачею повідомлення маячок-передавач формує для всіх інформаційних полів контрольну суму CRC. Після прийому повідомлення приймач (смартфон) знову обчислює контрольну суму і порівнює її із переданим значенням CRC.

поля ідентифікації	RSSI	CRC

Рисунок 2 – узагальнений формат маячків *iBeacon* та *AltBeacon*

При такому способі контролю передавання даних можна встановити факт наявності помилки і при додатковій обробці виправити лише один помилковий біт. Повторити передачу тих же даних неможливо, тому, що дані постійно змінюються. Збільшити

кількість виправлених помилок можуть більш потужні завадостійкі коди (наприклад, коди Ріда-Соломона), однак вони потребують складних обчислень та збільшення полів в форматах повідомлень.

І все ж ця проблема ефективно вирішується з тим же CRC-контролем і в межах стандартизованих форматів повідомлень. Для цього достатньо використати ітеративне декодування об'єднаних циклічних кодів [7]. Такими об'єднаними циклічними кодами можуть бути дві інтерпретації CRC-контролю [8]:

- Cyclic Redundancy Code, тобто CRC як циклічний надлишковий код,
- Cyclic Redundancy Check, тобто CRC як контрольна сума.

Оскільки в форматах маячків *iBeacon* та *AltBeacon* для поля CRC виділили лише три байти, тому в цьому полі повинні поміститись контрольне слово першого циклічного коду і контрольна сума другого циклічного коду. Розділимо поле CRC порівну і виберемо 12-розрядні породжувальні поліноми $g_1(x)$ та $g_2(x)$ для зазначених циклічних (n, k) -кодів. Нагадаємо, що ці поліноми степені $n - k = 12$ повинні бути примітивними та різними, наприклад:

$$g_1(x) = 1 + x + x^2 + x^5 + x^6 + x^9 + x^{12},$$

$$g_2(x) = 1 + x^4 + x^5 + x^{10} + x^{12}.$$

Як було доведено в [7] такі поліноми дозволяють при ітеративному декодуванні з ймовірністю $p_m = 1 - 2^{-12}$ виправити до 12 помилкових розрядів в повідомленнях від маячків.

Висновки

Для забезпечення точності задач навігації в технології Physical Web ключову роль має безпомилковість передачі повідомлень від маячків. Розробники стандартів *iBeacon* та *AltBeacon* передбачили лише дуже простий метод завадостійкого контролю. Запропонований метод дозволяє при незначному збільшенні тривалості декодування збільшити коректувальну здатність завадостійкого коду в 12 разів.

Список використаних джерел (References):

1. F. Hussain, "Internet of Things. Building Blocks and Business Models". – Springer, 2017. – 73 p.
2. M. Usama bin Aftab, "Building Bluetooth Low Energy Systems," Packt Publishing, Birmingham, UK, April 2017.
3. М. С. Васильева, А.В. Меженин Имитационная модель сигналов Beacon в среде Unity3D. – Научный альманах. – 2016. – N 12-2(26). – с.30-33.
4. <https://www.amazon.com/iBeacon-Bluetooth-Energy-Proximity-Device/dp/B00JEGXITG>.
5. P. Dickinson, G. Cielniak, O. Szymanczyk and M. Mannion, "Indoor Positioning of Shoppers Using a Network of Bluetooth Low Energy," Indoor Positioning and Indoor Navigation (IPIN), 2016 International Conference on, Alcalá de Henares, Spain, Oct. 4-7.
6. Семеренко В. П. Теорія циклічних кодів на основі автоматних моделей : монографія / В. П. Семеренко. – Вінниця : ВНТУ, 2015. – 444 с.
7. Semerenko, V.P. Iterative hard-decision decoding of combined cyclic codes, Eastern-European Journal of Enterprise Technologies. 2018. Vol. 1, issue 9 (91). P. 61–72.
8. Семеренко, В. П. Теория и практика CRC кодов: новые результаты на основе автоматных моделей / В. П. Семеренко // Східно-Європейський журнал передових технологій. – 2015. – Т. 4, № 9 (76). – С. 38–48.

ONTOLOGY-BASED SOFTWARE SYSTEM ABOUT THE SYMBOLIC IN NATIONAL REASONS IN THE DIFFERENT GEOGRAPHICAL REGIONS OF EUROPE AND ASIA

Baeva Desislava, Rashkova Victoria

Angel Kanchev University of Ruse

Аннотация

Древние артефакты хранят информацию о доисторических корнях народов. Качественное изучение скрытого в них символизма требует создания информационной системы для национальных мотивов в разных географических регионах Европы и Азии. Онтология является наиболее подходящей структурой для описания формально представленных знаний, основанных на некоторой концептуализации. Это было бы ценным ресурсом для будущих масштабных математических и алгоритмических исследований, связанных с автоматическим распознаванием фольклорных образов.

Abstract

The ancient artifacts store information about the prehistoric roots of the peoples. The qualitative study of symbolism hidden in them requires the creation of an information system for national motifs in the different geographic regions of Europe and Asia. Ontology is the most appropriate structure for describing a formally presented knowledge based on some conceptualization. It would be a valuable resource for future large-scale mathematical and algorithmic research related to the automatic recognition of folklore images.

Keywords: ontology, cultural-historical heritage, methodologies, information system, knowledge

Introduction

The ancient artifacts store information about the pre-historic foundations of the peoples, give information about our ancestors' knowledge of the world, and where we come from and where our place is in the world. The rich folklore information lies in the ancient symbols in the envelope. Over time, the width has undergone many changes passed from generation to generation, but some of the main symbols have been preserved to this day.

The common symbols in Bulgarian, Russian, Ukrainian, Indian, Chinese and others, which are of interest to a number of folk artists, but the lack of a quality and systematized database makes it harder for their research to limit their perimeter.[2]



Fig. 1 The Goddess on Two-Head Horse - Embroidery from Bulgaria, Russia.

The development of an **information system** (IS) with a focus on preserving, processing and popularizing the national embroidery knowledge base with the messages it carries would be of interest to both ethnologists and historians as well as to professionals and amateurs in various scientific fields - computer specialists, designers, embroiders, artists from different fields of application, etc., and correct approaches and methods for systematizing the accumulated knowledge base for national embroidery are almost absent.

Knowledge management technologies

Since, according to the scientific field of artificial intelligence ontology, the most appropriate structure for the description is formally presented knowledge based on some conceptualization of a number of objects and concepts, knowledge about them and relationships between them, describing the knowledge base describing the subject area for the national embroidery was chosen ontological structure.

Conceptualisation is one of the most critical activities in ontological design. It is based on the RDF standard, which is the basic infrastructure of the semantic web and related data. RDF is presented with the data model. Data and data models are stored in a single environment in which SPARQL creates rules for processing and retrieving information. Semantic Web technologies set data semantics and provide reasoning on the data scheme and the data itself. Ontology engineering technologies allow upgrading to existing data management systems and provide unified, unified and unified access to data in them without changing or duplicating them.[1]

The information retrieval process aims to derive certain information from certain criteria set in the ontological knowledge [3].

The proposed approach provides an opportunity to build a semantic library of national embroidery knowledge; creating a method for their semantic, unambiguous description, as well as an opportunity for ontological search for factual information through a systematic description and structuring of semantic knowledge. This approach has been realized thanks to an in-depth thorough study of the sources of cultural and historical heritage and, in particular, of the embroidery of the peoples. It provides the opportunity for future large-scale mathematical and algorithmic research related to automatic recognition of folklore images and generating L-grammars describing the various elements of symbolism and ornamentation of the embroidery.

Conclusion

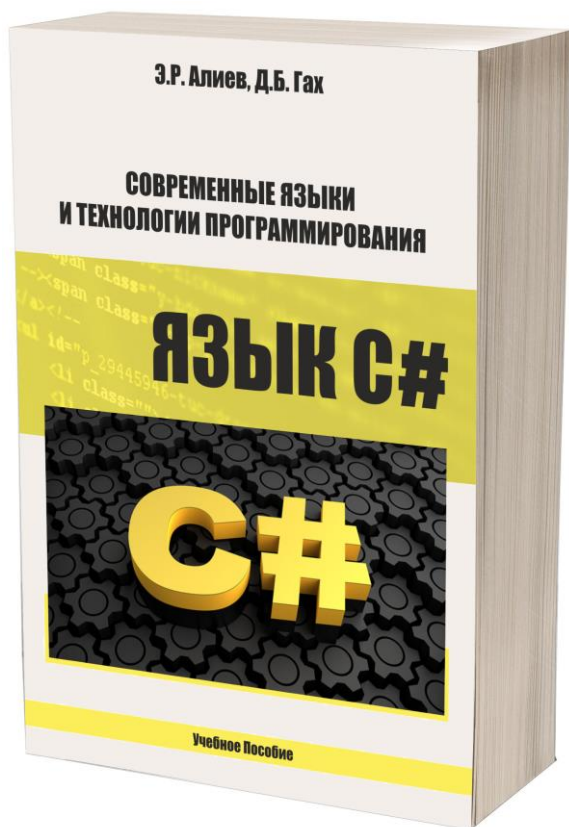
The creation of an information system containing a huge base of embroidery and describing its semantic meaning, with the ability to search by certain criteria, is a necessity as all authors who write a number of works on the meaning of embroidery are not engaged in creating a comprehensive and thorough work on the subject area. Usually, they analyze a particular embroidery item or describe and analyze only embroidery from a particular area.

Acknowledgments

This research was supported by the Bulgarian Science Fund, with the grant for financial support for projects of junior researchers and postdocs, agreement M12.1/2018 „Develop and explore a modern approach to conceptual software presentation of the semantic information stored in the Bulgarian national embroidery“

References

- [1] Борисова Н., Семантичен уеб-модел и приложения, Югозападен университет „Неофит Рилски“, 2015.
- [2] Стоянов, Св. Бележки върху осигуреността на културното наследство, Известия на съюза на учените – Варна, 2013
- [3] Cristani, Matteo; CUEL, Roberta. A survey on ontology creation methodologies. International Journal on Semantic Web and Information Systems (IJSWIS), 2005, 1.2: 49-69.
- [4] Jones Dean, Bench-Capon Trevor, Visser Pepijn, Methodologies for ontology development, 1998, 2014 , <https://cgi.csc.liv.ac.uk/~tbc/publications/itknows.pdf>
- [5] Navigli R., Paola V., Automatic acquisition of a thesaurus of interoperability terms, Università di Roma “La Sapienza”, 2005.



Э.Р. Алиев, Д.Б. Гах **Современные языки и** **технологии программирования.** **Язык C#**

Изложены и систематизированы основные технологии создания программного обеспечения, включая вопросы выполнения программ аппаратным обеспечением, архитектур информационных систем, сетевого взаимодействия, безопасности, а так же жизненного цикла ПО. Представлены вопросы для закрепления материала, а так же лабораторные работы для самостоятельного выполнения.

Пособие предназначено для студентов специальности «Вычислительные машины, комплексы, системы и сети», направления «Информатика и вычислительная техника», кроме того может быть использовано для студентов всех специальностей университета, изучающих курсы «Информатика» и «Программирование».

В этой книге:

- 309 страниц, 20 глав, 58 иллюстраций, большое количество примеров кода;
- 200 вопросов для закрепления материала с верными ответами в конце книги;
- 15 лабораторных работ;
- Рассмотрение тем блокчейна, жизненного цикла ПО, принципов разработки ПО NASA, философии программирования для ОС UNIX;
- Описание основ .NET Framework, аппаратного обеспечения ЦПУ и ОЗУ, ООП, UML, многопоточного программирования, информационной безопасности, шаблонов проектирования, сетевых протоколов стека TCP/IP, форматов данных и баз данных.

Уникальное содержание:

- Рассмотрение программирования на языке C# в контексте его практического применения в различных технологиях и сферах человеческой жизни;
- Широкий охват тем с кратким изложением ключевых концепций, методов и навыков;
- Сравнение концепций и конструкций языка C# с аналогичными концепциями и конструкциями, присущими языкам C++ и Java;
- Включение информации, базирующейся на официальных материалах авторизованных профессиональных курсов компании Microsoft.

Опыт авторов, лежащий в основе книги:

- Реализация крупных международных проектов в области ИТ, включая создание веб-портала www.GoMap.Az;
- Многолетний опыт преподавания, проведения семинаров и презентаций;
- Написание и публикация десятков научных и прочих технических статей.

Наукове видання

**ІНТЕРНЕТ-ОСВІТА-НАУКА-2018
(ІОН-2018)**

Збірник праць одинадцятої міжнародної науково-практичної конференції,
м. Вінниця, 22-25 травня 2018 року
(українською, англійською та російською мовами)

Підписано до друку 14.05.2018 р.
Формат 29,7×42¹/₂ Папір офсетний.
Гарнітура Times New Roman.
Ум. друк. арк. 39,50. Наклад 122 прим.
Зам № 2018-089.

Вінницький національний технічний університет,
ІРВЦ ВНТУ,
21021, м. Вінниця, Хмельницьке шосе, 95, ВНТУ,
ГНК, к. 114.
Тел. (0432) 65-18-06
Свідоцтво суб'єкта видавничої справи
серія ДК № 3516 від 01.07.2009 р.

Віддруковано у Вінницькому національному технічному університеті,
в інформаційному редакційно-видавничому центрі,
21021, м. Вінниця, Хмельницьке шосе, 95, ВНТУ, ГНК, к. 114.
Тел. (0432) 65-18-06
Свідоцтво суб'єкта видавничої справи
серія ДК № 3516 від 01.07.2009 р.