МАТЕРИАЛЫ

V - МЕЖДУНАРОДНОЙ НАУЧНО-ПРАКТИЧЕСКОЙ КОНФЕРЕНЦИИ «ИНФОРМАТИКА И ПРИКЛАДНАЯ МАТЕМАТИКА», ИНСТИТУТА ИНФОРМАЦИОННЫХ И ВЫЧИСЛИТЕЛЬНЫХ ТЕХНОЛОГИЙ

29 сентября - 01 октября 2020 года

Институт информационных и вычислительных технологий МОН РК

Казахский Национальный Университет имени аль-Фараби

Университет Туран

Люблинский технический университет, Польша

«Ғылым ордасы»

МАТЕРИАЛЫ

V международной научно-практической конференции "Информатика и прикладная математика", 29 сентября - 1 октября 2020, Алматы, Казахстан

Алматы 2020

УДК 378 (063)
ББК 74.58
И74

Главный редактор:
Калимолдаев М.Н. - генеральный директор ИИВТ, академик НАН РК, доктор физико-математических наук, профессор

Ответственные редакторы:
Мамырбаев О.Ж. - заместитель генерального директора ИИВТ, доктор PhD
Калижанова А.У. - заместитель генерального директора ИИВТ, кандидат физико-математических наук
Юничева Н.Р. - ученый секретарь ИИВТ МОН РК, кандидат технических наук, доцент

И 74 **Информатика и прикладная математика:** Мат. V Межд. науч. конф. (29 сентября -1 октября 2020 г.). Алматы, 2020. – с. 435

ISBN 978-601-332-384-8

В сборнике опубликованы доклады, представленные по 4 секциям от Республики Казахстан, Российской Федерации, США, Латвии, Польши, Республики Беларусь, Украины, Азербайджана, Узбекистана, Японии, Кореи, Ирана, Португалии, Испании, Великобритании, Греции, Кыргызской Республики и других.

Рассмотрены актуальные вопросы в области математики, информатики и управления: математического моделирования сложных систем и бизнес-процессов, исследования и разработки защищенных и интеллектуальных информационных и телекоммуникационных технологий, математической теории управления, технологий искусственного интеллекта.

Материалы сборника предназначены для научных работников, докторантов и магистрантов, а также студентов старших курсов.

УДК 378 (063)
ББК 74.58

ISBN 978-601-332-384-8

© Институт информационных и вычислительных технологий МОН РК, 2020

Программный комитет

Почетный председатель:

- Мутанов Г.М., академик НАН РК, Казахстан

***Председатель Международного Программного комитета*:**

- Калимолдаев М.Н., академик НАН РК, д.ф.-м.н., профессор, генеральный директор ИИВТ МОН РК, Казахстан

Сопредседатель:

- Алшанов Р.А., академик Международной инженерной академии, д.э.н., профессор, президент Ассоциации вузов РК, ректор университета «Туран», Казахстан

Заместители председателя:

- Wójcik Waldemar, doctor of technical sciences, professor, Poland

Члены международного программного комитета:

- Абламейко С.В., академик НАН Беларусь
- Адамов А., д.ф.-м.н., профессор, Азербайджан
- Айда-заде К.Р., д.ф.-м.н., член-кор. НАН, профессор, Азербайджан
- Амиргалиев Е.Н., д.т.н., профессор, Казахстан
- Арсланов М.З., д.ф.-м.н., профессор, Казахстан
- Ахмед-Заки Д.Ж., д.т.н., доцент, Казахстан
- Ашимов А.А., академик НАН РК, Казахстан
- Балгабаева Л.Ш., к.т.н, доцент, Казахстан
- Бияшев Р.Г., д.т.н., профессор, Казахстан
- Бобров Л.К., д.т.н., Россия
- Дженалиев М.Т., д.ф.-м.н., профессор, Казахстан
- Дрозденко А.А., PhD, Украина
- Евтушенко Ю.Г., академик РАН, Россия
- Ерзин А.И., д.ф.-м.н., профессор, Россия
- Имомназаров Х.Х., д.ф.-м.н., профессор, Россия
- Исмаилов Б.И., д.т.н., профессор, Кыргызстан
- Ищукова Е.А., к.т.н., Россия
- Конявский В.А., д.т.н., профессор, Россия
- Коплык И.В., PhD, Украина
- Кочетов Ю.А., д.ф.-м.н., профессор, Россия
- Куандыкова Д.Р., к.т.н., профессор, Казахстан
- Кубеков Б.С., к.т.н., доцент, Казахстан
- Кудайкулов А.К., д.ф.-м.н., профессор, Казахстан
- Мазаков Т.Ж., д.т.н., профессор, Казахстан
- Медянкина И.П., к.т.н., Россия
- Мусабаев Р.Р., к.т.н., Казахстан
- Набиев О.М., д.т.н., профессор, Узбекистан
- Нусупбекова Г.С., д.т.н., профессор, Казахстан
- Нысанбаева С.Е., д.т.н., доцент, Казахстан
- Пак И.Т., д.т.н., профессор, Казахстан
- Посыпкин М.А., д.ф.-м.н., Россия

- Родионов А.С., д.т.н., профессор, Россия
- Рысбайулы Б., д.ф.-м.н., профессор, Казахстан
- Сакабеков А.С., д.ф.-м.н., профессор, Казахстан
- Самигулина Г.А., д.т.н., доцент, Казахстан
- Суйменбаев Б.Т., д.т.н., Казахстан
- Соколова О.Д., к.т.н., Россия
- Ташев А.А., д.т.н., профессор, Казахстан
- Тузиков А.В., академик НАН, Беларусь
- Тукеев У., д.т.н., профессор, Казахстан
- Тультаев Б.Т., к.т.н., Казахстан
- Тарасов В.Б., д.ф.-м.н., профессор, Россия
- Тусупова С.А., д.т.н., профессор, Казахстан
- Ускенбаева Р.К., д.т.н., профессор, Казахстан
- Утепбергенов И.Т., д.т.н., профессор, Казахстан
- Федотов А.М., д.ф.-м.н., Россия
- Хайрова Н.Ф., д.т.н., Украина
- Харин С.Н., академик НАН РК, Казахстан
- Шаронова Н.В., д.т.н., Украина
- Шаршеналиев Ж.Ш., академик НАН КР, Кыргызстан
- Яворский В.В., д.т.н., Казахстан
- Erol Kurt, Professor, Doctor, Turkey
- Prof. Bagher Baba Ali, Iran
- Prof. Leonid Perlovsky, USA
- Prof. Frank Chong woo Park, South Korea
- Prof. Mohamed Othman, Malaysia
- Prof. Hamdani bin Saidi, Malaysia
- Prof. Hiroshi Inaba, Japan
- Prof. Keylan Alimhan, Japan
- Prof. Marat Ahmet, Turkey
- Prof. Masayasu Ito, Japan
- Prof. Nenad Mladenovich, Serbia
- Prof. Ravil Muhamediev, Latvia
- Prof. Tenreiro Machado, Portugal
- Prof. Thanos Stouraitis, Greece
- Prof. Kisala Piotr, Poland
- Prof.Kotyra Andrzej Antoni, Poland

Ученые секретари конференции:
- к.т.н. Юничева Н.Р.
- к.т.н. Капалова Н.А.
- PhD, Абдилдаева А.А.
- PhD, Шаяхметова А.С.
- PhD, Козбакова А.Х.

Организационный комитет

Председатель:
- PhD, ассоц. профессор, Мамырбаев О.Ж.

Сопредседатели:

- К.ф.-м.н., ассоц. профессор, Калижанова А.У.
- PhD, Ахметжанов М.А.

Члены организационного комитета:

- Айтмухамбетова Г.А.
- Ахметов Е.А.
- Амирханова Г.А.
- Анищенко Л.Н.
- Асқарова А.
- Аспантаев А.
- Абишева А.
- Ахмедиярова А.
- Бегимбаева Е.Е.
- Бегалиева К.
- Калиева Г.С.
- Касымова Д.Т.
- Кулемзин А.А.
- Мажитов Ш.С.
- Масимканова Ж.А.
- Маусымбекова С.Д.
- Науменко В.В.
- Нуржанов Ч.
- Зиятбекова Г.
- Джаксылыкова А.
- Дуйсенбаева А.
- Дюсенбаев Д.
- Елеусинов А.
- Нуркаманова М.А.
- Тасболатұлы Н.
- Тойбаева Ш.Ж.
- Турдалы М.
- Утегенова А.У.
- Усатова О.
- Шахмаев Р.А.
- Шокишалов Ж.

Место проведения

Республика Казахстан, г. Алматы, ул. Шевченко 28,
Ғылым ордасы, с 29 сентября по 1 октября 2020 г.

Тел.:

+7 727 272 37 11;

+7 727 272 73 27;

+7 727 272 39 13

СЕКЦИЯ 1

Қолданбалы математика, информатика және басқару теориясының қазіргі заманғы мәселелері. Бизнес процесстер мен күрделі жүйелерді оңтайландыру мен модельдеу. Есептеу математикасы, сандық талдау және программалау, математикалық логика. Статистика теориясы. Статистикалық әдістер

Современные проблемы прикладной математики, информатики и теории управления. Моделирование и оптимизация сложных систем и бизнес процессов. Вычислительная математика, численный анализ и программирование, математическая логика. Теория статистики. Статистические методы

Current issues of applied mathematics, computer science and control theory. Modeling and optimization of complex systems and business processes. Computational mathematics, numerical analysis and programming, mathematical logic. Theory of statistics. Statistical methods

ГИДРОТЕХНИКАЛЫҚ ҚҰРЫЛЫСТАРДАҒЫ СУ ДЕҢГЕЙІН КЛИМАТТЫҚ МӘЛІМЕТТЕР АРҚЫЛЫ БАҚЫЛАУДЫ АВТОМАТТАНДЫРУ ЖӘНЕ ОНЫҢ МАҢЫЗДЫЛЫҒЫ

[1,2]Мазаков Т.Ж., [1]Айпанов Ш.А, [3]Kisala P., [1,2]Зиятбекова Г.З., [1,2]Әлиасқар М.С.
e-mail: ziyatbekova@mail.ru
[1]ҚР БҒМ ҒК Ақпараттық және есептеуіш технологиялар институты, Қазақстан
[2]әл-Фараби атындағы Қазақ ұлттық университеті, Қазақстан
[3]Люблин техникалық университеті, Польша

Аннотация. *Бұл мақалада ел аумағындағы су қорларының қауіпсіздігін ескере отырып, ондағы су деңгейін бақылаудың маңыздылығы туралы айтылады. Атап айтқанда, гидротехникалық құрылыстардағы су деңгейін климаттық мәліметтер арқылы бақылаудың артықшылығы қарастырылған. Сонымен қатар климаттық мәліметтерді шынайы уақытта қабылдау және таратуды автоматтандыру қарастырылады. Бөгеттердегі апатқа әкелетін төтенше жағдайлардың түрлі себептері талданады.*

Түйін сөздер: *бөгет, гидротехникалық құрылыс, климаттық бақылау жүйесі, су қоймасы, серпінді толқын, болжау.*

Кіріспе. Еліміздің аумағында су қорлары көптеп саналады. Энергияның бірден бір құралы ретінде суды пайдалану энергетикасы саласын айтарлықтай дамытады. Соның нәтижесінде елімізде су элекр станциялары өз жұмысын жалғастыруда, олардың саны 30-дан асып жығылады. Әйтсе де, жолындағыны сыпыра шайып кететін дүлей күшті де судан көруге болады. Ол таспен қоса сеңболып қатқан мұзды да таситын алапат тақын жасайды. Өзен жағалауларын пайдалану мүмкіндігі жайлы мәселені шешу үшін, жекелей алғанда, бөгеттердің күйреуінен болатын су тасқындарының шығындарын айқындау керек [1].

Ауылшаруашылықпен айналысатын аудандарда егістік алқаптарды су басып қалуы салдарынан орасан зор шығын келеді. Мысалы, селдің жүруі дәнді-дақылдарға айтарлықтай нұқсан келтіріп, әр түрлі инженерлік және мелиорациялық жүйелерді құртады. Су басудан сақтану үшін әр алуан айла-шарғы ойластыру керек. Солардың бірі әрі бірегейі жағалауды бекініс тәрізді мықтап бекіту жұмыстарын атқарған абзал. Бүгінгі таңда көпшіліктің жөн көретін ең қарапайым жолы – қапшыққа салынған құмнан үйіп қолдан жасалатын шағын бөгеулер. Оны қалау үшін де дәлме-дәл өлшемдерін алдын ала білген дұрыс, өйткені су кемерінен асып кеткен кезде оларды шайып әкетеді де еш көмегі болмай қалады. Судың ары қарай жайылуын болдырмау үшін үйінді дамбаларды салу орындарын дәл анықтау қажет. Үйінді бөгет құрылысының құны оның ұзындығы мен биіктігіне тікелей байланысты, сондықтан олардың параметрлерін ыңғайлы етіп жасаған дұрыс. Жағалауды бекітуді жобалау мен оларды салу кезінде су басуы мүмкін жерлерді алдын ала білу үшін өзен суының ағынына модель жасауды қолданған жөн. Кейіннен, алынған нәтижелерді басты назарда ұстап, үйінді бөгеттердің қажет өлшемдерін есептеу оңай. Жоспарлы түрде мұқият ойластырыла жүргізілген есептеулер әрқашан оң нәтиже беретіні анық. Мұндайда өңірді сел жүруден сақтайтын жағалаудағы кішігірім бекіністердің атқарар қызметі ұшан теңіз. Ал жойқын әрі қатты толқынның жайылып кетуін модельдеудің оңтайлылы болуы мен дәлме-дәлдігін бағалау оңайға соқпайды. Әзірше қайсыбір нақты нәтиже болған

емес. Оған қоса, рас нәтижелерді алуға болатын ешбір дұрыс амал да табылмаған. Бар тәсілдердің қай-қайсысын қолданбасақ та, қатты толқындардың бұзып-жарып өтуінің кесірінен болатын су басу аймақтары жайында тексерілген, нақты мәлімет болмай тұр. Алынған нәтижелердің дәлдігін бағалау тіптен үлкен жұмыс [2, 3].

Қолданылған әдіс. Бақылау ақпараты болжаудың негізі болып табылады.

Нәтижелерге талдау. Су бөгетінің бұзылуының математикалық моделін зерттеу мәселесін зерделеуге К.А. Степановтың, М.Ю. Стриганованың, М.В. Хамутованың, В.А. Кушниковтың, М.П. Шагаевтың, Е.Н. Куликтің, Д.В. Стефанишиннің, A.J. Raudkivi, F. Aureli, P. Mignosa, M. Tomirotti, Podobnikar T., Li, M. және тағы басқа шетел ғалымдарының еңбектері арналған [4-6].

Сонымен бірге, осы бағыттағы зерттеулердің өзектілігі отандық ғалымдардың қомақты еңбектерімен расталады. Елімізде мұндай зерттеулерді Қ.И. Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университетінің ғалымдары жүргізіп жатқанын атап өтуге болады. Қазақстандық гидротехника ғылымының негізін қалаушы, академик Ш.Ч. Чокин тұңғыш рет Қазақстанда көпмақсатта қолданылатын бөгендердің есептеулері үшін ЭЕМ қолданды. Ол бөгеттердің жарылуының математикалық моделінің мәселелерімен айналысатын алғашқы отандық ғалымдардың бірі болып танылды. Гидротехникалық құрылыстар тіпті қалыпты жұмыс режимінде экологиялық және табиғатты пайдалану мәселелерінің тұтас кешенін құратын ауыр техникалық нысандар қатарына кіреді [7].

Қазіргі заманда адам өміріне төнетін қауіп артып келеді. Егер табиғи апаттар – жер сілкіністері, су тасқындары, орман өрттері замана бойы қауіп төндіріп келсе, соңғы уақытта оларға техногенді апаттар қосылды. Ең қауіптілері ірі экологиялық осал нысандарда болатын апаттар, оларға көптеген сушаруашылық құрылыстары (бөгеттер, бөгендер, дамбалар) жатады. Бөгеттер ерте заманнан бері тасқындардан сақтау, энергия көздерін алу, ауызсумен қамту, бір сөзбен айтқанда «су – тіршілік көзі» екенін мойындаймыз. 1950 жылдары алыс-жақын шетелдерде ел үкіметі халықтың тұрмыс-тіршілігі үшін, кейде тіпті жекелеген ірі мекемелердің өзі ұлттық экомиканың дамуына әрі кемелденуіне үлес қосатындықтан ірі су бөгеттерін салуды жөн санады. Ғалымдар бөгеттер құрылысы қоршаған ортаға зор ықпалын тигізетіндігі туралы қорытындыға келді, өйткені ағыс жылдамдығы мен топырақ эрозиясы өзара тікелей байланысты. Өзендердегі шөгінділер мен лайланған қалдықтардың теңізге шығуына бөгеттер де кедергі жасайды. Сондықтан өзендер қосылатын жерлерде эрозия турыратын осындай қалдықтар жиналады.

Төтенше жағдайлар зардаптарын жүйелі түрде талқылауда, оның моделін жасауда және алдын ала бағдарлауға бағытталған қолданбалы әдістерді зерделеп-дайындау жолында аянбай еңбектенген ғалымдар жетерлік. Мысалы Ахметов Б.С., Симагин И.М., Полуян Л.В., Василенко А.А., Арифуллин Е.З., Федянин В.И., Арефьева Е.В., Фурсов В.А., Сергеев В.В., Фурман Я.А., T. Kohonen, M. Turk, T. Ahonen, T. Cootes, I. Chingovska, P. Kisala және тағы басқа шетелдік ғалымдар айналысуда. Әйтсе де, оның тигізер залалдарын жан-жақты талдап, болжайтын белгілі тәсілдердің шарттары түбегейлі шешілмеген. Сол себепті, кететін шығындардың аз мөлшері мен құны төмен болатындай болжаудың тез әсері мен шынайылығының жоғары көрсеткіштерін қамтамасыз ететін математикалық модельдерді, сандық әдістерді, алгоритимдер мен бағдарламалық кешенді әзірлеп, зерттеу қажеттілігі туындайды [8].

Серпіліс толқыны болған кездегі жалпы жағдайды анықтау үшін оның қажетті есептеулерін жүргізу қажет, айталық: серпінді толқынының ең жоғарғы биіктіктегі көрсеткіші; толқын денесінің ең жоғары жылдамдығы; жойқын толқынының бастапқы және соңғы легінінің жылдамдықтары; серпінді толқынның (бастапқы шебінің, орта тұсының немесе жотасының, толқынының соңғы жағының) өзіндік нүктелерінің есептік тұстамаға жету уақыты. Халықты, нысандар мен аумақтарды тиімді қорғау үшін біздің еліміздегі гидроморфометриялық жағдайларда қолдануға болатын, серпіліс толқыны мен су басу аймақтарының параметрлерін есептеу әдістемесі мен бағдарламасы қажет. Сонымен қатар су астында қалған өлкені мұқият зерттей отырып, келешекте төтенше жағдайлардан қалай сақтануға болатыны туралы амалдарды ойластыра жасауды жедел қимылдау ережелеріне қосу.

Қазіргі сәтте бөгеттің қирауы сияқты төтенше оқиға әсерінен сел жүру, су деңгейінің күрт өсуі мен шайылуына толып жатқан мысал келтіруге болады. Бөгет құрылысы қирағанда және оларды зақымдайтын серпінді толқынмен қатар маңайдың су астында қалуы себепті сипатталатын төтенше жағдайларға қосымша әрекет етуші жағдайлар мыналар:

−өрт – электр кабельдері мен сымдарының үзіліп қалуы және қысқа тұйықталудың себептерінін;

−көшкіндер, опырылулар – топырақтың шайылуы әсерінен;

−жұқпалы аурулар – ауызсудың, азық-түліктің ластануы салдарынан.

Гидротехникалық құрылыстардың бүлінуінен және серпінді толқынның қалыптасуынан болатын апаттар көбінесе құрылыс іргетасының бұзылуынан және су ағызғыштардың жетіспеушілігінен болады. Түрлі жағдайлардың пайыздық мөлшері 1-кестеде келтірілген.

1- кесте. Серпінді толқынның пайда болуымен қатар келетін гидротехникалық құрылыстар апатының сан түрлі себептерінің жиілігі.

Бүлінудің орын алуы	**Қайталану жиілігі, %**
Іргетастың бүлінуі	40
Су ағызғыш бұрандалардың тапшылығы	23
Құрылымдық олқылықтар	12
Әр келкі шөгу (отыру)	10
Сулап үйілген бөгеттегі жоғары бастапқы қысым	5
Бүлікшілік әрекеттері	3
Беткейлердің сырғып түсуі	2
Материалдардың дұрыс болмауы	2
Жер дүмпулері	1
Ережеге сай қолданбау	2
БАРЛЫҒЫ:	100

Су қоймаларындағы су деңгейін өлшеу әдістерінің жеткіліктілігіне қарамастан, яғни ең қарапайымынан күрделісіне дейін, су деңгейін тіркеудің автоматтандырылған жүйесін беретін бақылауды ойлап табу қашан да келелі мәселелердің бірі болып есептеледі. Судың деңгейлік сызығы – оның бетінің салыстырмалы түрде басқа затқа қатысты алғандағы биіктігі. Су әрқашан тыныш

күйде болмайтынын ескерсек, оның биіктігін өлшеу де оңайға соқпасы анық. Кейбір өлшегіш құралдарды көпірдің астына орнатып, олар орналасқан жерден су бетіне дейінгі қашықтықты тіркеп тұруға арналғандары да бар. Бүкіл өлшеу жабдығының жұмысы электр энергиясымен атқарылады, мұндай мүмкіндік үнемі ескеріле бермейді. Айталық, өлшегіш құралды теңіз-көлдердің жағалауынан қашықтау жерге бекітсек, ондағы су мөлшерін анықтау өте қиынға соғады. Сондықтан өлшегіш аспаптарды еш көмексіз өздері жұмыс істейтіндей су деңгейі бойынша ақпарат алатын әрі таратанын құрылғы ретінде қабылдау керек. Бақылаудың негізгі атқаратын әркеті – ақпарат қабылдау. Оларға сенсордан келетін мәлімет өңдеу қорына дер кезінде жіберілгені дұрыс. Бақылау құралдары қайда орналастырылса да ақпарат өздіксіз берілуі керек. Қорыта келе айтарымыз, мәліметтерді төмен орбиталдық байланыспен берген оңтайлы. Жабдықтау орнын ток көзіне қосу әлі де болса шешілмей, сұрақ күйінде тұрғаны анық. Осы тығырықтан шығатын жалғыз ғана жол – қолжетімді, ең тиімді күн энергиясы [9].

Ақпараттық мониторинг жүйелері үшін шынайы уақыт жағдайында деректер жинауды қамтамасыз ету керек. Деректерді берудің бірегей торабы ғарыш көздерімен ақпарттарды беру болып табылады, оларға энергиямен қамтылған автоматтандырылған ішкі жүйені де қосуға болады. Негізгі ойды түйіндей отырып, теңіздегі, өзен-көлдер мен су торабындағы су деңгейін бақылауды автоматтандырылған және біртұтас беру жүйесінің көмегімен атқарған нәтижелі болады.

Іс жүзінде пайдалану үшін ақпаратты жинау және өңдеу процесін автоматтандыруға негізделген шынайы уақыт жағдайында су қоймаларының жағдайын бақылау жүйесі жасалады. Автоматтандырылған бақылау жүйелерінде температура мен қысымды, сондай-ақ түрді ағып кетулер мен деформацияларды анықтайтын сенсорлар қолданылады [10].

Қондырғыларды қосудың екі нұсқасы бар. Алдымен Arduino микропроцессоры бірден серверге жалғанады. Ол кезде электрмен үздіксіз жабдықтау жүйесін әрі оның басында адамның тұруын міндеттейді. Содан соң, Arduino ағымдағы мәліметті жерсерік көмегімен серверге беретін RaspberryPi микрокомпьютеріне қосылады. Бұл нұсқа су жүйесінде жұмыс істейтін қызметкерлердің үнемі болуын қажет етпейді. Мөлшерінің кішкентай және қуатының аздығына байланысты оны кішігірім күн энергиясы да қоректендіреді. Бөгеттің бұзылу қаупін бақылау үшін негізгі ақпарат көзі су деңгейінің сенсорынан алынған мәліметтер болып табылады. Қосымша ақпарат температура мен жауын-шашын сенсорларынан алынған мәліметтермен қамтамасыз етіледі.

Н.Т. Исимовтың диссертациялық жұмысындағы негізгі ақпарат – бұл температура мен жауын-шашын сенсорларынан алынған мәліметтер, яғни індетке шалдыққандар мен оларды тасымалдаушылардың санын болжау үшін қолданылады [11].

Қолдағы бар деректі алатын әрі беретін бөлігі қажетті үш түрлі ақпаратты сенсорлар түрінде орындайды және бөгеттің басына орналастырылады. Сенсорлар Arduino микропроцессорына қосылған, ол сенсорлардан алынған мәліметтерді алдын-ала өңдеуді қамтамасыз етеді және оларды әрі қарай өңдеуге жібереді. Климаттық мәліметтерді берудің автономды микропроцессорлық жүйесін құру үшін біз RaspberryPi 3 B + микрокомпьютерін қолдандық. Электр қуатын күн батареясы береді [12].

Жүйе қажетті сенсорлар мен бағдарламалық жасақтамалардың жиынтығын қамтиды. Өлшеу модульдері компьютерге USB адаптері арқылы қосылады. Бағдарламалық жасақтама өлшеу нәтижелерін кестелік және графиктік түрде ұсынады, сонымен қатар кез келген уақытта мәліметтер базасында жинақталған өлшемдер архивін қарауға және басып шығаруға мүмкіндік береді. Сенсорлардан деректерді жергілікті желідегі және Интернеттегі басқа компьютерлерден көруге болады.

Arduino – ATmega 328 микроконтроллеріне негізделген құрылғы. Мұнда микроконтроллермен ыңғайлы жұмыс істеу үшін қажет барлық заттар бар. Құрылғымен жұмыс істеуді бастау үшін айнымалы AC/DC тұрақты ток адаптерінен немесе батареядан қуат беріңіз немесе компьютерге USB кабелі арқылы қосыңыз. RaspberryPi – бұл банктік карта өлшеміндегі жалғыз тақталы компьютер, яғни компьютердің әр түрлі бөліктері бөлек тақталарда орналасқан. Raspberry Pi негізінен Linux және Windows операциялық жүйелерінде жұмыс істейді [13].

Су қоймасындағы су деңгейін өлшеу үшін біз US-015 ультрадыбыстық сенсорды қолдандық. Оның атқаратын қызметі ол белгілі бір жиілікте дыбыстық толқындарды жібере алады.

US-015 сенсорының техникалық сипаттамалары:

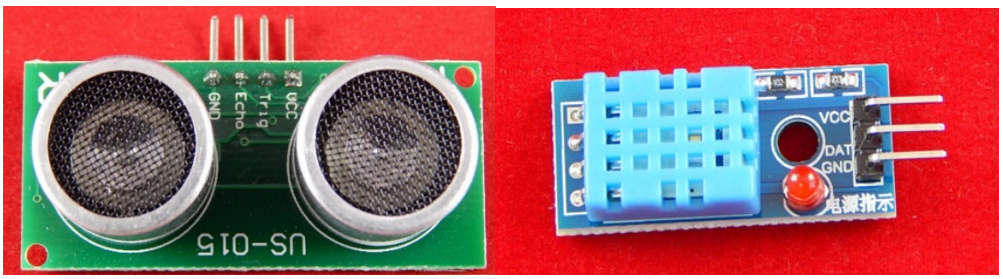
• Қоректендіру кернеуі: 5 В;
• Тұтыну тогы: 20 мА;
• Күту режиміндегі ток шығыны: 2,2 мА;
• Өлшем бұрышы: 15˚;
• Өлшенген қашықтық диапазоны: 2 - 700 см;
• Дәлдігі: 0,3 см + 1%.

Температураны және жауын-шашынның мөлшерін өлшеу үшін бір сандық шығысы бар DHT11 сенсоры қолданылды, сондықтан ондағы көрсетаіштерді 1-2 секундта бір реттен жиі өткізуге болмайды.

DHT11 сенсорының ерекшеліктері:

• электрмен жабдықтау және енгізу-шығару 3-5 В;
• 5% дәлдікпен 20-80% ылғалдылықты анықтау;
• 2% дәлдікпен 0-50 градус температураны анықтау;
• Таңдама жиілігі 1 Гц-тен аспайды (1 секундта бір реттен аспайды).

1-суретте қолданылған сенсорлар көрсетілген.



а) US-015 сенсоры ә) DHT11 сенсоры

1- сурет. Сенсорлардың түрі: а) су деңгейі және ә) температура мен ылғалдылық

Бөгетке төнетін қауіп жайында тыңғылықты әрі тез алынатын мәліметті өңдейтін бөлігінде су жүйесі мен бөгет сипаттамалары жайлы дерек бар, сондай-ақ ағымдағы мәліметті де жылдам қабылдайды. Өңдеу кезінде қондырғы су жүйесінің қауіпсіздігін, алаңдаушылығын немесе апаттық мөлшерін есептейді. Соңғы

жағдайда, яғни судың оқыс деңгейін анықтағанда, ол автоматты түрде мемлекеттік органдарға (төтенше жағдайлар, әкімдіктер және т.б.) бөгеттің бұзылу қаупі туралы хабарлайды.

Мақалада әзірленген математикалық модель негізінде бөгеттің қирауын анықтау құрылғысы, су сақтайтын қойманың өлшемдері (бөгеттің көлемі, биіктігі, ені) бөгеттен әркелкі шақырымда кездесетін жойқын толқынның қаншалықты биік көтерілгенін есептей алады, сөйтіп, қауіпті апаттың салдарын айқындауға көмектеседі [14-16].

Қорытынды

Қазіргі заманғы математикалық модельдеу технологиялары мен есептеу экспериментін қолданып, табиғи және техногенді сипаттағы төтенше жағдайлардан болатын зардаптар пайымдалды, дамбаның бұзылуының математикалық моделі зерттелді. Мақалада климаттық мәліметтерді берудің дербес шағынкомпьютерлік жүйесі жасалынды, белгілі бір уақытта қуатты толқындардың әсерлерін болжау мәселесінің жалпы сипаттамасы және тұжырымы келтірілген. Су бөгенінің хал-ахуалын басты назарда ұстап, анықтаудың математикалық моделі жасалды, оның көмегімен мүдделі ұйымдарды, айталық, әкімдіктер мен жергілікті төтенше жағдайлар бөлімшелеріне тез хабарлауға болады.

Жұмыс AP05131027 «Ақпаратты қорғаудың биометриялық әдістері мен құралдарын жасау» жлбасы бойынша 2018-2020 жылдарға арналған ғылыми зерттеулерге гранттық қаржыландыру есебінен жүргізілді.

Әдебиеттер

1. Қазақстан Республикасының 2003 жылғы 9 шілдедегі № 481-II Су кодексі (2019 жылғы 28 қазандағы өзгерістер мен толықтырулармен). 25-бап. Ерекше стратегиялық маңызы бар су шаруашылығы құрылыстары. https://online.zakon.kz/document/?doc_id=1042116#pos=33;-60 (15.05.2020).

2. Мазаков Т.Ж., Зиятбекова Г.З. Су тасқындарын бағалау мәселелерін шешу үшін геоақпараттық жүйелерді қолдану // «Информатика және қолданбалы математика» III халықар. ғыл. конф. матер. – Алматы, 2018. – 1 Б. – 278-284 б.

3. Симагин И.М., Полуян Л.В. Гидротехникалық құрылыстардағы апат кезіндегі су басу мүмкін болатын жерлерді модельдеу. SAFETY. – Екатеринбург, 2018. – 14-21 б.

4. Хамутова М.В., Кушников В.А. Су тасқынының салдарын болжаудың математикалық моделі. Астрахан мем. техн. ун-ті. хабаршысы. Басқару, есептеу техн. информ. сериясы, 2016. – № 3. – 109-114 б.

5. F. Yusuf, G. Lang, M. Garrett. Modernization of BC Hydro’s inundation modelling and mapping: a high resolution, flexible and reshonsive approach. Whisrler, BC, Canada, 2009. – 55 p.

6. Nikitin N. V., Nicoud F., Wasistho B., Squires K. D., Spalart P. R. An approach to wall modeling in large-eddy simulations. // Phys. Fluids 12, 2000. – P. 1629-1632.

7. Чокин Ш.Ч., Баишев Б.Б., Григорьев В.А. Су қоймасының көп мақсатты есебі. – Алма-Ата: Наука КазССР, 1983. – 208 б.

8. Арефьева Е.В. Су тасқыны төтенше жағдайдың ықтимал көзі ретінде // Азаматтық қауіпсіздік технологиясы. Ғылыми-техникалық журнал. – М.: ФГУ ВНИИ ГОЧС (ФЦ), 2007. – № 4(14). – 69-74 б.

9. Гугушвили И.В. Өзен алқабындағы серпінді толқынның қозғалысының параметрлерін есептеу әдістерін жетілдіру // Техн. ғыл. канд. ғылыми дәрежесін алуға арналған дисс. – М., 2011. – 147 б.

10. Әлиасқар М.С., Джомартова Ш.А., Зиятбекова Г.С., Исимов Н.Т., Амирханов Б.С., Мазақова Ә.Т. Дербес микропроцессорлық климаттық деректерді беру жүйесі // Қ.И. Сәтбаев атындағы ҚазҰТЗУ хабаршысы, 2019. –№ 1 (131). – 371-377 б.

11. Исимов Н.Т. Моделирование и разработка автоматизированной системы для мониторинга и управления социально-эпидемиологической ситуацией регионам Казахстана // Диссертация на соискание степени доктора философии (PhD) по специальности 6D070400 – Вычислительная техника и программное обеспечение. – Алматы: 2020. – 102 с.

12. Саймон Монк. Мейкерство. Arduino и Raspberry Pi. Управление движением, светом и звуком. – СПб.: БХВ-Петербург, 2017. – 336 с.

13. Mazakov T.Zh., Dzhomartova Sh.A., Kisala P., Ziyatbekova G.Z. New approaches for solving problems of the simulation of flood wales and breakthrough to justify protective measures // HERALD of the Kazakh – British Technical University. – Almaty, 2019. – Vol. 16. – № 4(51). – pp. 138-144.

14. T. Mazakov, Sh. Jomartova, G. Ziyatbekova, M. Aliaskar. Automated system for monitoring the threat of waterworks breakout // Journal of Theoretical and Applied Information Technology, 2020. – Vol. 98, – No 15. – pp. 3176-3189. ISSN: 1992-8645, E-ISSN: 1817-3195.

15. Мазаков Т.Ж., Зиятбекова Г.З., Әлиасқар М.С. Су тораптарының бұзылу қатерін бақылаудың автоматтандырылған жүйесі // ҚазТБУ хабаршысы, Нұр-Сұлтан, 2020. – № 1. – 8-19 б.

16. Мазаков Т.Ж., Джомартова Ш.А., Kisala P., Зиятбекова Г.З. Су ресурстарын бақылауды дамытуға арналған іс-шаралар мен туындайтын мәселелер // Қ.И. Сәтбаев атындағы ҚазҰТЗУ хабаршысы, 2020. – № 2(138). – 365-369 б.

ДИСТАНЦИОННЫЙ МЕТОД МОНИТОРИНГА ЖИЗНЕННЫХ ПОКАЗАТЕЛЕЙ ЧЕЛОВЕКА

[1,4]Амирханов Б.С., [1,2]Мазаков Т.Ж., [2]Мазакова А.Т., [1]Исимов Н.Т., [3]Жолмагамбетова Б.Р., [1]Әбдіразақ Б.К.
e-mail: amirkhanov.b@gmail.com
[1]Институт информационных и вычислительных технологий КН МОН РК, Казахстан
[2]Казахский национальный университет имени аль-Фараби, Казахстан,
[3]Евразийский национальный университет имени Л.Н. Гумилева, Казахстан
[4]Университет «Туран», Казахстан

Аннотация. *Данная работа описывает концепцию измерения частоты сердечных сокращений (пульса) человека, снятого на простую видео или веб-камеру, при помощи визуализации потока крови на лице. Представлены несколько возможных методов постобработки для улучшения извлечения фактического импульсного сигнала: независимый компонентный анализ, Эйлерово усиление видео,*

детрендинг. Приведены алгоритмы получения частоты сердечных сокращений по видеосигналу: спектр мощности, набор уравнений, обнаружение импульсной волны, алгоритм обнаружения и проверки нарастающих фронтов импульсного сигнала. Для создания приложения использованы следующие технологии: Python 3 и Open CV.

***Ключевые слова**: BioPython, биоинформатика, независимый компонентный анализ, Эйлерово усиление видео, детрендинг, спектр мощности, обнаружение импульсной волны, Open CV.*

Введение. С развитием информационных технологий телеметрии неинвазивное дистанционное измерение жизненно важных показателей человека стало важнейшим направлением биоинформатики. *Эйлерово усиление видео* - это метод, представленный на SIGGRAPH 2012, способный выявлять временные вариации в видео, которые невозможно увидеть невооруженным глазом. Используя этот метод, можно визуализировать поток крови, когда он заполняет лицо [1]. И оценить частоту сердечных сокращений бесконтактным способом с помощью камеры [1-3]. Основной областью данной исследовательской работы является обработка изображений и компьютерное зрение, медицинские приложения, разработка программного обеспечения, цифровая обработка сигналов, целью которого является перевод размерных данных из реального мира в виде изображений в числовую или символическую информацию.

На сегодняшний день были предприняты некоторые успешные усилия бесконтактного способа (с помощью веб-камеры) оценки жизненно важных показателей, таких как частота сердечных сокращений и частота дыхания [1-3]. Также разработаны другие подобные продукты, которые требуют специального оборудования и поэтому являются дорогостоящими, включают лазерный Доплер [1], микроволновый доплеровский радар [4] и тепловизионную систему [5]. Поскольку рассматриваемый метод Эйлерового видеоусиления это более экономный метод оценки жизненно важных показателей бесконтактным способом, чем вышеупомянутые продукты, эта исследовательская работа имеет потенциал для развития таких областей, как телемедицина, личное здравоохранение и устройства интернета вещей.

Методы исследования. Фотоплетизмография. Одним из методов неинвазивного снятия показателей является *фотоплетизмография* (ФПГ) – это концепция оптического измерения объемных изменений органа. Его наиболее широко используют в пульсоксиметрах. ФПГ основан на принципе, что кровь поглощает больше света, чем окружающие ткани, таким образом, изменения объема крови влияют на светоотражение [6]. Использование специальных источников света и инфракрасных длин волн, а также контактных зондов было нормой [4,5,7]. Однако в последнее время была изучена дистанционная бесконтактная PPG-визуализация [8,9]. Метод, используемый в статье [9], захватывает значения пикселей (красный, зеленый и синий каналы) лицевой области ранее записанного видео, где добровольцев просили минимизировать движения. Затем значения пикселей в пределах интересующей области (ROI) усреднялись для каждого кадра. Было обнаружено, что это пространственное усреднение значительно увеличивает отношение сигнал/шум. Далее оценка частоты сердечных сокращений вычислялась с помощью быстрого преобразования Фурье и спектра мощности. Авторы работы [6] демонстрируют, что зеленый канал имеет более сильный сердечный сигнал по

сравнению с красным и синим каналами. Это убедительное доказательство того, что сигнал обусловлен колебаниями объема крови, поскольку гемоглобин поглощает зеленый свет лучше, чем красный и синий.

Постобработка сигналов. После получения необработанных значений пикселей (красный, зеленый и синий каналы) для извлечения и улучшения отраженного сигнала плетизмографии может быть использована комбинация следующих методов. Однако каждый метод вносит сложность и дорогостоящие вычисления. В этом случае основным источником сигнала, представляющего интерес, является сердечный импульс, распространяющийся по всему телу, который изменяет длину пути падающего окружающего света из-за объемных изменений в лицевых кровеносных сосудах во время сердечного цикла, так что последующие изменения количества отраженного света указывают на время сердечно-сосудистых сокращений. Записывая видео лицевой области, датчики красного, зеленого и синего цветов (RGB) улавливают смесь отраженного плетизмографического сигнала вместе с другими источниками флуктуаций света из-за артефактов. Каждый датчик цвета записывает смесь сигналов исходного источника с немного различными весами. Эти наблюдаемые сигналы от датчиков красного, зеленого и синего цветов обозначаются соответственно x_1(t), x_2(t) и x_3(t), которые являются амплитудами регистрируемых сигналов в момент времени t. В традиционной модели независимого компонентного анализа число извлекаемых источников не может превышать число наблюдений, поэтому были приняты три базовых сигнала источника, представленных s_1(t), s_2(t) и s_3(t). Модель независимого компонентного анализа предполагает, что наблюдаемые сигналы являются линейными смесями источников, т.е. $x_i(t) = \sum_{j=1}^{3} a_{ij}\, s_j(t)$для каждого $i = \overline{1,3}$. Это можно компактно представить уравнением смешивания

$$x(t) = As(t) \tag{1}$$

где векторы столбцов $x(t) = [x_1(t), x_2(t), x_3(t)]^T, s(t) = [s_1(t), s_2(t), s_3(t)]^T$, квадратная 3×3-матрица A содержит коэффициенты смеси a_{ij}. Цель модели независимого компонентного анализа состоит в том, чтобы найти разделяющую или демикширующую матрицу W, которая является аппроксимацией обратной исходной смешивающей матрицы A, выход которой

$$\hat{s}(t) = Wx(t)$$

представляет собой оценку вектора x(t), содержащая базовые источники сигналов. Чтобы выявить независимые источники, W должен максимизировать негауссовость каждого источника. На практике итерационные методы используются для максимизации или минимизации заданной функции затрат, которая измеряет негауссовость [2, 3].

Эйлерово усиление видео. В отличие от модели независимого компонентного анализа, которая фокусируется на извлечении одного числа, Эйлерово видеоусиление использует локализованное пространственное объединение и временную фильтрацию для извлечения и визуального выявления сигнала, соответствующего сердечному импульсу. Это позволяет усилить и визуализировать сигнал сердечного ритма в каждом месте на лице. Это создает потенциал для

мониторинга и диагностического применения в медицине, например асимметрия лицевого кровотока может быть симптомом артериальных проблем.

Помимо усиления цвета, метод Эйлерова видеоусиления также способен выявить низкоамплитудное движение, которое может быть трудно или невозможно увидеть человеку. Предыдущие попытки раскрыть незаметные движения в видео были сделаны, например [10], который следует Лагранжевой перспективе, как в гидродинамике, где траектория частиц отслеживается сверхурочно. Полагаясь на точную оценку движения и дополнительные методы для получения качественного синтеза, такие как сегментация движения и рисование изображений, сложность алгоритма и вычисление являются дорогостоящими и трудными.

Напротив, метод Эйлерова видеоувеличения вдохновлен теорией Эйлера, где свойства вокселя жидкости, такие как давление и скорость, развиваются с течением времени. Подход этого метода к увеличению движения заключается в преувеличении движения путем усиления временных изменений цвета в фиксированных положениях, а не в явной оценке движения.

Этот методический подход, показанный на рисунке 1, сочетает в себе пространственную и временную обработку, чтобы подчеркнуть тонкие временные изменения в видео. Во-первых, видеоряд разлагается на различные пространственные частотные полосы. Поскольку они могут демонстрировать различные отношения сигнал-шум, они могут быть увеличены по-разному. В общем случае можно вычислить полную лапласианскую пирамиду [11]. Затем на каждой пространственной полосе выполняется временная обработка. Временная обработка одинакова для всех пространственных полос и для всех пикселей внутри каждой полосы. После этого извлеченный полосовой сигнал увеличивается на коэффициент α, который может быть задан пользователем, и может быть ослаблен автоматически. Наконец, увеличенный сигнал добавляется к исходному изображению, и пространственная пирамида сворачивается, чтобы получить конечный результат.

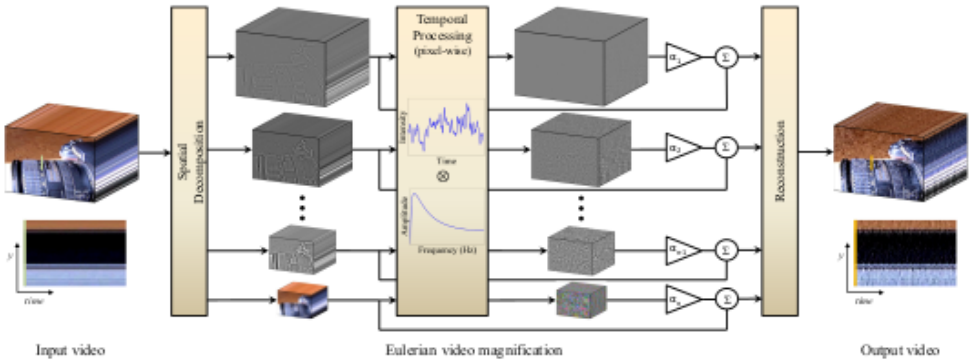


Рис. 1. Обзор метода Эйлерова видеоусиления (источник: [1])

Пространственная фильтрация. Как уже упоминалось ранее, работа [1] вычисляет полную лапласианскую пирамиду [11] в качестве общего случая пространственной фильтрации. Каждый слой пирамиды может быть увеличен по-разному, потому что он может демонстрировать различные отношения сигнал-шум

или содержать пространственные частоты, для которых линейная аппроксимация, используемая при увеличении движения, не выполняется [1].

Пространственная фильтрация также может быть использована для значительного увеличения отношения сигнал/шум, как ранее упоминалось в разделе и продемонстрировано в работах [1] и [6]. Тонкие сигналы, такие как частота сердечных сокращений человека на видеозаписи его лица, могут быть усилены таким образом. Для этого в работе [1] вычисляется слой гауссовой пирамиды, который может быть получен путем последовательного масштабирования изображения путем вычисления среднего Гаусса для каждого пикселя.

Однако для обнаружения интересующего сигнала применяемый пространственный фильтр должен быть достаточно большим. В работе [1] приводится уравнение для оценки размера пространственного фильтра, необходимого для обнаружения сигнала при определенном уровне мощности шума:

$$S(\lambda) = S(r) = \sigma'^2 = k\frac{\sigma^2}{r^2} \ (2),$$

где $S(\lambda)$ представляет собой сигнал на пространственных частотах, а так как длина волны λ отсечения пространственного фильтра пропорциональна его радиусу r, то сигнал может быть представлен в виде S(r). Мощность шума σ^2, может быть оценена с использованием методики [12]. Наконец, поскольку уровень мощности фильтруемого шума σ'^2 обратно пропорционален r^2, то можно решить уравнение для r, где k- константа, зависящая от формы фильтра нижних частот.

Временная фильтрация. Временная фильтрация используется для извлечения движений или сигналов, подлежащих усилению. Таким образом, выбор фильтра зависит от приложения. Для увеличения движения предпочтителен широкополосный фильтр, такой как фильтр баттерворта. Узкополосный фильтр дает более бесшумный результат для цветового усиления кровотока. Идеальный полосовой фильтр используется на [1] из-за его резких частот среза. Альтернативно, для реализации в реальном времени низкоуровневые IIR-фильтры могут быть полезны как для усиления цвета, так и для увеличения движения. Эти фильтры показаны на рисунке 2.

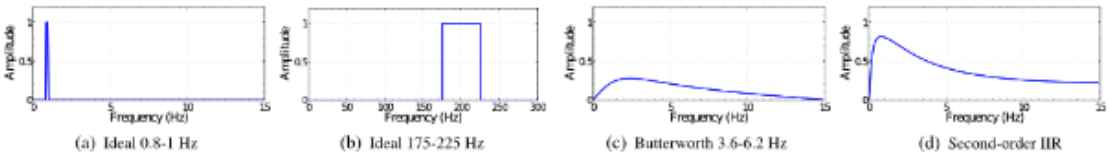


Рис. 2. Пример временных фильтров. (источник: [13])

Выделение цветовых вариаций для определения пульса человека. Извлечение сердечного импульса человека с помощью метода Эйлерова видеоусиления продемонстрировано в работе [1]. Было также представлено, что использование правильной конфигурации может помочь извлечь нужный сигнал. Существует четыре шага, которые необходимо предпринять при обработке видео с использованием этого метода:

1. выбор временного полосового фильтра;
2. выбор коэффициент усиления, α;

3. выбор пространственной частотной отсечки (заданной пространственной длиной волны λ_c), за пределами которой используется ослабленная версия α;

4. выбор формы затухания для α: либо α равно нулю для всех $\lambda<\lambda_c$, либо α линейно уменьшается до нуля.

Для изменения цвета человеческого импульса могут быть использованы два временных фильтра, сначала выбирающие частоты в пределах 0,4-4 Гц, соответствующие 24-240 ударам в минуту (уд/мин), затем узкая полоса 0,83-1 Гц (50-60 уд/мин) может быть использована, если извлечение частоты пульса было успешным.

Чтобы максимально подчеркнуть изменение цвета, применяется большой коэффициент усиления $\alpha\approx100$ и пространственная частотная отсечка $\lambda_c\approx1000$. С ослаблением α до нуля для пространственных длин волн ниже λ_c. Результат можно увидеть на рисунке 3.

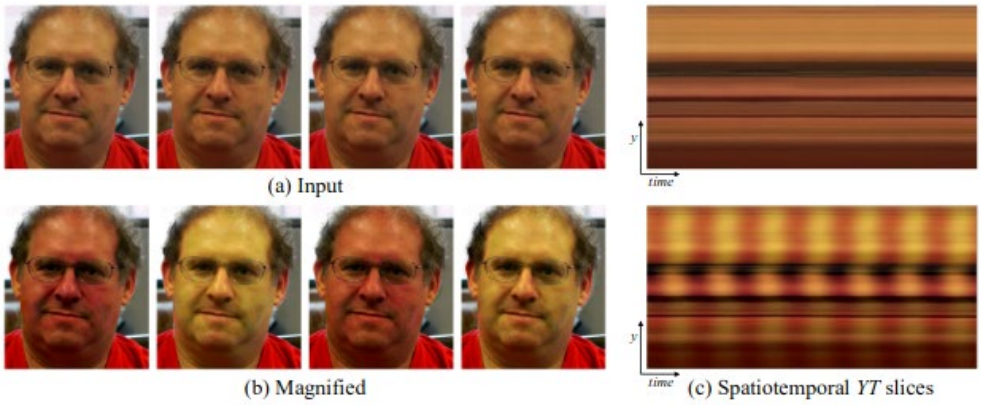


Рис. 3. Выделение изменений цвета лица с помощью метода Эйлерова видеоусиления (источник: [1])

Детрендинг – это метод удаления очень больших ультранизкочастотных трендов входного сигнала без каких-либо искажений величины, действующий как фильтр высоких частот.

Основным преимуществом метода является его простота. Метод заключается в разделении входного сигнала z на две составляющие: $z = z_{stat} + z_{trend}$, где z_{stat}-почти стационарная составляющая, а z_{trend}-низкочастотная апериодическая составляющая тренда. Оценка почти стационарной составляющей, $\hat{z}_{stat}$, может быть получена с помощью приведенного ниже уравнения. Подробный вывод уравнения можно найти в [14].

$$\hat{z}_{stat} = (I - (I + \lambda^2 D_2^T D_2)^{-1})z \tag{3}$$

где I-матрица тождества, D2-дискретная аппроксимация второго порядка, λ-параметр регуляризации. На рисунке 4 представлен пример того, чего может достичь этот метод. В примере, взятом из работы [14], используется реальный ряд RR, и показано влияние метода на временной и частотно-временной анализ вариабельности сердечного ритма, чтобы не потерять никакой полезной информации.

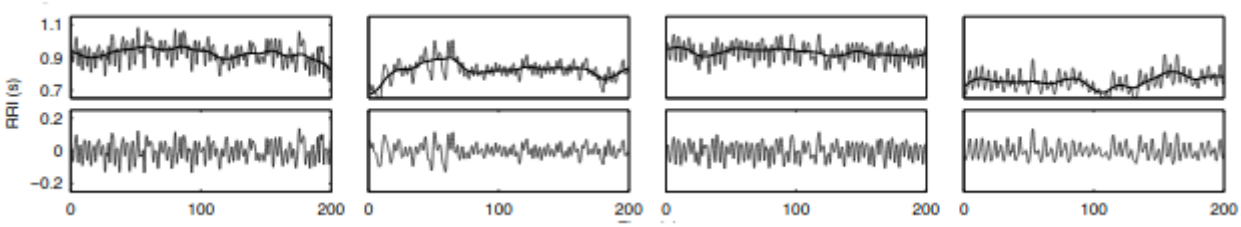


Рис. 4. Оригинальные серии RR и установлены тенденции (выше) и бестрендовый серии без искажения масштаба (источник: [14])

Оценка частоты сердечных сокращений. Чтобы преобразовать извлеченный плетизмографический сигнал в число ударов в минуту (чсс), необходимо выполнить дальнейшую обработку. Ниже выделены два метода, способных достичь этой цели.

Спектр мощности. Преобразование Фурье – это математическое преобразование, способное преобразовывать функцию времени f(t) в новую функцию, представляющую частотную область исходной функции. Чтобы вычислить спектр мощности, полученная функция от преобразования Фурье умножается на саму себя. Поскольку значения захватываются из видео, последовательности кадров, функция времени фактически дискретна, с частотой, равной частоте кадров видео в секунду (FPS).

Индекс *i*, соответствующий максимуму спектра мощности, можно затем преобразовать в значение частоты F, используя уравнение:

$$F = \frac{i*FPS}{2N} \tag{4}$$

где N-размер извлекаемого сигнала. Затем F можно умножить на 60, чтобы преобразовать его в удары в минуту, и получить оценку частоты сердечных сокращений по извлеченному сигналу.

Обнаружение импульсной волны. В работе [15] представлен автоматизированный алгоритм быстрого обнаружения импульсных волн. Алгоритм способен получать оценку частоты сердечных сокращений по сигналу ФПГ, как альтернативу описанному выше спектру мощности. Кроме того, он также вводит проверку для обнаружения формы волны путем проверки ее формы и времени. Ниже представлено упрощенное описание алгоритма. Более подробное описание можно найти в [15].

1. Идентификация возможных пиков и ступеней отдельных импульсов

(a) максимум (MAX)

Сигнал делится на последовательные интервалы времени по 200 мс, и для каждого сегмента определяется абсолютный максимум. Некоторые из этих максимумов отклоняются: если они опускаются ниже заранее определенного порога амплитуды; или если расстояние между двумя максимумами меньше или равно 200 мс, то меньший максимум отклоняется.

(b) минимум (MIN)

Абсолютный минимум определяется между каждыми двумя соседними максимумами. Минимум отклоняется, если он превышает заданный порог амплитуды. Когда минимум отклоняется, также отбрасывается максимум с меньшей амплитудой из двух максимумов, смежных с отклоненным минимумом.

2. Обследование и проверка нарастающих фронтов

(a) Проверка одного нарастающего фронта

Если нарастающий фронт отклоняется, отклоняются его максимум и минимум. Нарастающий фронт отклоняется, если его амплитуда (AMPL = MAX-MIN) ниже порогового значения амплитуды; или его продолжительность ниже порога, который зависит от частоты дискретизации; или его амплитуда не увеличивается плавно.

(b) Оценка сходства нарастающего фронта с предшествующим и последующим нарастающим фронтом, признается действительной.

Два нарастающих фронта считаются одинаковыми, если амплитуда нарастающего фронта с меньшей амплитудой превышает 50% амплитуды нарастающего фронта с большей амплитудой; и если максимум нарастающего фронта с меньшей амплитудой находится в пределах ± 60% от максимума нарастающего фронта с большей амплитудой; и если минимум нарастающего фронта с меньшей амплитудой находится в пределах ± 60% от минимума нарастающего фронта с большей амплитудой; и если длительность более короткого нарастающего фронта больше 33% длительности более длинного фронта. Допустимые нарастающие фронты затем классифицируются в соответствии с их характеристиками для следующего шага. Описание категоризации опущено для краткости и может быть найдено в [15].

(c) Проверка текущего нарастающего фронта

Нарастающие фронты, отнесенные к категории на предыдущем шаге, считаются допустимыми фронтами импульсной волны, если они удовлетворяют по крайней мере одному из правил принятия решения, представленных в [15] и подавленных для краткости.

Описанный здесь процесс проверки важен для отбрасывания сигналов, которые не представляют пульсовые волны. Обеспечение возможности расчета оценки частоты пульса только по действительным импульсным сигналам.

Выводы. В этой работе разработано приложение (рисунок 5) для мониторинга жизненно важных показателей на основе метода Эйлерова видеоусиления, которое включает в себя следующие функции:

- определение и оценка частоты сердечных сокращений на основе метода Эйлерова видеоусиления;
- отображение изменений в реальном времени, таких как увеличенный кровоток, полученный с помощью метода Эйлерова видеоусиления;
- решение проблемы с движением артефактов, вызванным движением человека и/или смартфона.

Следует отметить, что простая реализация метода Эйлерова видеоусиления невозможна по разным причинам. Во-первых, этот метод обеспечивает усиление движения наряду с увеличением цвета, что создаст несколько проблем с движением артефактов. Во-вторых, работа приложения в реальном времени создает проблемы производительности, которые были реализованы несколькими компромиссными решениями.

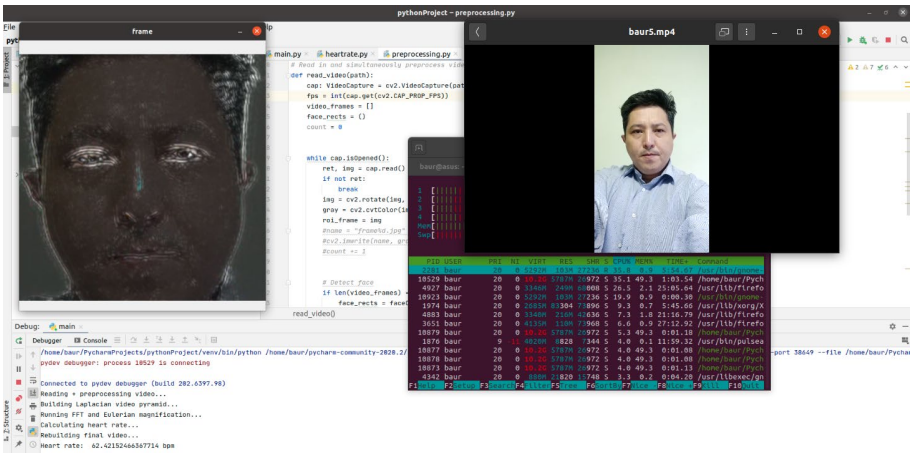


Рис.5. Результат работы приложения: вырезано лицо из видеопотока

Для реализации приложения был использован высокоуровневый язык программирования Python версии 3 и библиотека компьютерного зрения Open CV. Язык программирования Python 3 — это мощный инструмент для создания программ самого разнообразного назначения. С его помощью можно решать задачи различных типов. Open CV – это библиотека функций, в основном предназначенная для обработки изображений в реальном времени. Для их поддержки он также включает библиотеку статистического машинного обучения. Более того, это кроссплатформенная библиотека с открытым исходным кодом, которую можно бесплатно использовать и изменять по лицензии BSD.

Работа выполнена за счет средств грантового финансирования научных исследований на 2018-2020 годы по проекту AP05132044 «Разработка аппаратно-медицинского комплекса оценки психофизиологических параметров человека».

Литература

1. Hao-Yu Wu, Michael Rubinstein, Eugene Shih, John Guttag, Frédo Durand, andWilliam T. Freeman. Eulerian video magnification for revealing subtle changes inthe world.ACM Trans. Graph. (Proceedings SIGGRAPH 2012), 31(4), 2012.

2. M.Z. Poh, D.J. McDuff, and R.W. Picard. Non-contact, automated cardiac pulsemeasurements using video imaging and blind source separation. Optics Express,18(10):10762–10774, 2010.

3. M.Z. Poh, D.J. McDuff, and R.W. Picard. Advancements in noncontact, multi-parameter physiological measurements using a webcam. Biomedical Engineering, IEEE Transactions on, 58(1):7–11, 2011.

4. EF Greneker. Radar sensing of heartbeat and respiration at a distance with applications of the technology. InRadar 97 (Conf. Publ. No. 449), pages 150–154. IET,1997.

5. M. Garbey, N. Sun, A. Merla, and I. Pavlidis. Contact-free measurement of cardiacpulse based on the analysis of thermal imagery. Biomedical Engineering, IEEETransactions on, 54(8):1418–1426, 2007.

6. Wim Verkruysse, Lars O Svaasand, and J Stuart Nelson. Remote plethysmographicimaging using ambient light. Optics express, 16(26):21434–21445, 2008.

7. IDC. Android marks fourth anniversary since launch with 75.0in third quarter, according to idc.http://www.idc.com/getdoc.jsp?containerId=prUS23771812.

8. P Wieringa, F Mastik, and AFW Van der Steen. Contactless multiple wavelength photoplethysmographic imaging: a first step toward “spo2 camera” technology. An-nals of biomedical engineering, 33(8):1034–1041, 2005.

9. Sijung Hu, Jia Zheng, Vassilios Chouliaras, and Ron Summers. Feasibility of imaging photoplethysmography. InBioMedical Engineering and Informatics, 2008. BMEI 2008. International Conference on, volume 2, pages 72–75. IEEE, 2008.

10. C. Liu, A. Torralba, W.T. Freeman, F. Durand, and E.H. Adelson. Motion magnification. InACM Transactions on Graphics (TOG), volume 24, pages 519–526.ACM, 2005.

11. P. Burt and E. Adelson. The laplacian pyramid as a compact image code. Communications, IEEE Transactions on, 31(4):532–540, 1983.

12. C. Liu, W.T. Freeman, R. Szeliski, and S.B. Kang. Noise estimation from a singleimage. InComputer Vision and Pattern Recognition, 2006 IEEE Computer SocietyConference on, volume 1, pages 901–908. IEEE, 2006.

13. Daniel A Litvack, Tim F Oberlander, Laurel H Carney, and J Philip Saul. Timeand frequency domain methods for heart rate variability analysis: a methodological comparison. Psychophysiology, 32(5):492–504, 1995.

14. Mika P Tarvainen, Perttu O Ranta-aho, and Pasi A Karjalainen. An advanced detrending method with application to hrv analysis. Biomedical Engineering, IEEETransactions on, 49(2):172–175, 2002.

15. Bistra Nenova and Ivo Iliev. An automated algorithm for fast pulse wave detection. International Journal Bioantomation, 14(3):203–216, 2010.

МОДЕЛИРОВАНИЕ ТЕРМОСИФОННОЙ СИСТЕМЫ СОЛНЕЧНОГО КОЛЛЕКТОРА

Амиргалиев Е.Н, Кунелбаев М.М, Орманов Т.А.
e-mail: murat7508@yandex.kz
Институт информационных и вычислительных технологий КН МОН РК, Казахстан

Аннотация. *В данной статье рассматривается новая концепция дизайна плоского солнечного коллектора с использованием гибких трубок. Плоский солнечный коллектор предназначен для запуска холодной воды в системы солнечного теплоснабжения вместо использования дорогих антифризных жидкостей и для удаления вторичных средств. Разработка такого типа солнечных тепловых коллекторов позволит снизить стоимость установки традиционных солнечных тепловых систем без необходимости использования вторичных теплообменников. Определены основные параметры теплоемкости плоского солнечного коллектора. С помощью коммерческого программного пакета CFD (Computational Fluid Dynamics) ANSYS FLUENT 19.0 были разработаны фазовый дизайн, основанный на прогнозах тепловых характеристик коллектора и эквивалентный коэффициент теплопередачи пластин поглотителя.*

1.Введение

Для снабжения бытовой горячей водой широко используются плоские солнечные коллекторы, солнечное тепловое коллекторное устройство с низкотемпературными солнечными тепловыми системами [1] и обслуживания солнечных теплоцентралей [2], а также солнечные гибридные тепловые насосы [3]. Плоские солнечные коллектора с тепловыми характеристиками имеют первостепенное значение с точки зрения повышения энергоэффективности [4,5]. Как представлено в [5] солнечные тепловые коллекторные устройства состоят из прозрачной крышки, пластины поглотителя, соединенной с стояками трубами, задней теплоизоляции и металлической рамы, трубками на листе [6]. Существуют различные конфигурации листовой трубки на пластинах коллектора, например, паяные изогнутые стояки, используемые Gunjo et другие [7], и алюминиевые гофрированные вертикальные трубки, как у Alvarez et al. [8]. Del Col et al. в работе [9] показали экспериментальные результаты, с высокой производительностью по сравнению с обычными листовыми и трубными коллекторами. Chen и другие в работе [10] изготовили плоский солнечный коллектор с полимерными материалами из-за легкого свойства полимеров, и обнаружили, что эффективность полимерного коллектора была на 8–15% ниже, чем у традиционного металлического коллектора.

2.Экспериментальные испытания для определения тепловых характеристик FPSC

Тепловые испытания плоского солнечного коллектора были проведены помещении Института Информационных и Вычислительных Технологии МОН РК, в г.Алматы, Республика Казахстан.

На рисунке 1 изображена модель плоского солнечного коллектора Сущность и новизна состоит в том, что в отличие от известного принципа конструирования, коллектор содержит прозрачный стеклопакет 2 с двойным стеклом и с уменьшенным давлением, а так же периметрическую раму 1. Днище деревянной рамы 7 сделана из фанеры толщиной 8 мм. и к ним приклеена теплоизолирующая пленка 5 с фольгой. В зазоре образующиеся между стеклопакетом и днищем рамы проложена гибкая тонкостенная нержавеющая гофрированная трубка 4∅16 мм.в виде змеевика. Концы трубки прикреплены к входным и выходным торчащим трубам 6.

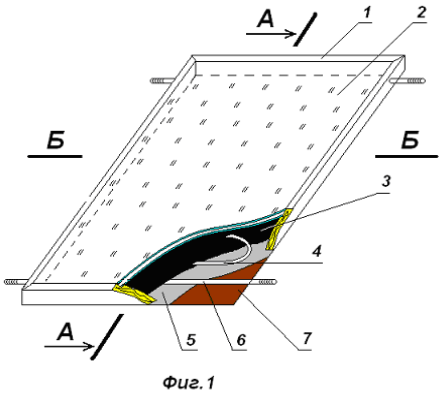


Рис. 1. Принципиальная схема плоского солнечного коллектора

Рис.2. Изображение плоского солнечного коллектора, протестированных в Институте Информационных и Вычислительных Технологии МОН РК

Таблица 1. Технические показатели плоского солнечного коллектора

Параметры	Значение
Материал поглощающей пластины	медь
Размеры пластины поглотителя	2 m×1 m
Толщина плиты	0.4 mm
Материал для остекления	Закаленное стекло
Размеры остекления	2 m×1 m
Толщина остекления	4 mm
Изоляция	Пеноплекс (пено поли уретан)
Угол наклона коллектора	45^0
Теплопроводность поглотителя	401 W/(m K)
Теплопроводность изоляции	0.04 W/(m K)
Коэффициент пропускания-поглощения	0.855
Видимая температура солнца	4350 K
Температура окружающей среды	303 K
Интенсивность излучения	1000 W/m^2

Температура на входе коллектора (обычно ± 1 ° C) в течение небольшого промежутка времени, равного 3–5 мин, была принята в качестве стационарного условия для получения эффективных точек тестирования. Широкий диапазон входной температуры коллектора был реализован посредством уменьшения объема воды в резервуарах, соединенных с коллекторами в контуре, для достижения различных пониженных температурных перепадов при скорости потока 1,7 л / мин, чтобы определить тепловую производительность коллектора, так же при скорости потока 2,3 л / мин были выполнены тепловые КПД коллектора, близкие к тепловому КПД с нулевыми потерями.

3. Результаты

Четыре температурных условия на входе, 10 ° C, 30 ° C, 50 ° C, 70 ° C, рассматривались для получения эквивалентных коэффициентов теплопередачи абсорбирующих пластин для прогнозирования тепловых характеристик коллектора.

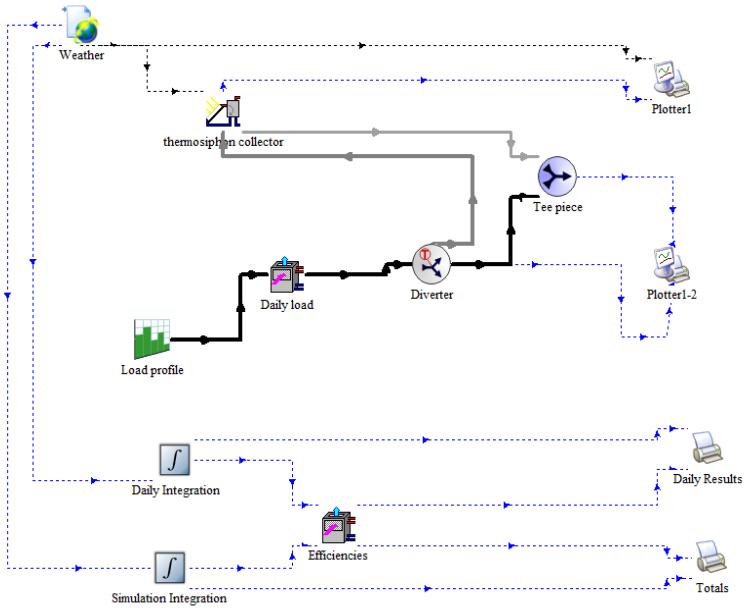


Рис.3. Схема TRNSYS моделируемой термосифонной системы солнечного коллектора

Чтобы проверить надежность нового типа TRNSYS TYPE 15-3, по сравнению со стандартным TYPE 45a, проводится сравнение результатов моделирования с соответствующими экспериментальными данными. В частности, были исследованы температура рабочей жидкости на входе / выходе из / в коллектор, массовый расход термосифона и полученная полезная тепловая мощность.

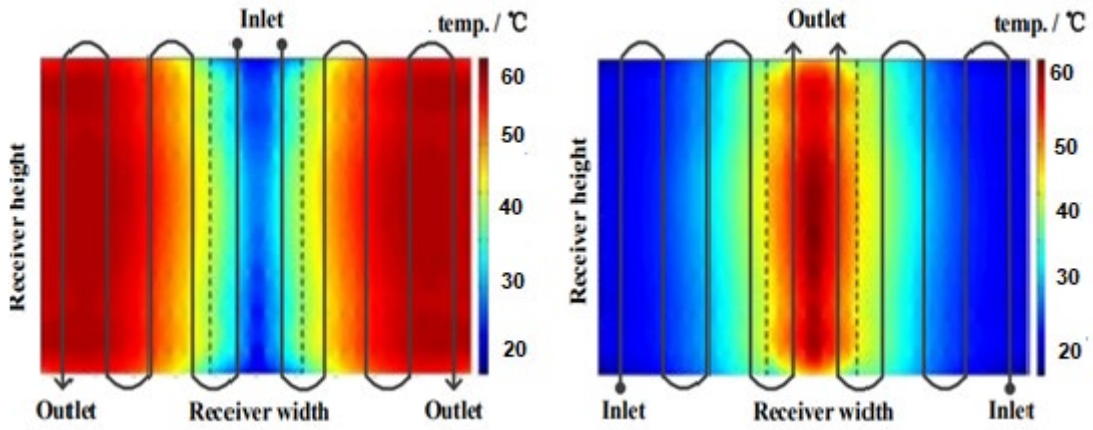


Рис.4. Температурные данные по ширине и длине приемника плоского солнечного коллектора

В приемнике обычно используется двухконтурная компоновка с несколькими соединенными трубными панелями в каждой петле. Влияние различных схем потока жидкости на распределение средней температуры поверхности внутренней компоновки может быть значительно ниже, чем у внешней компоновки, что может помочь уменьшить потери тепла и зону с высоким термическим напряжением.

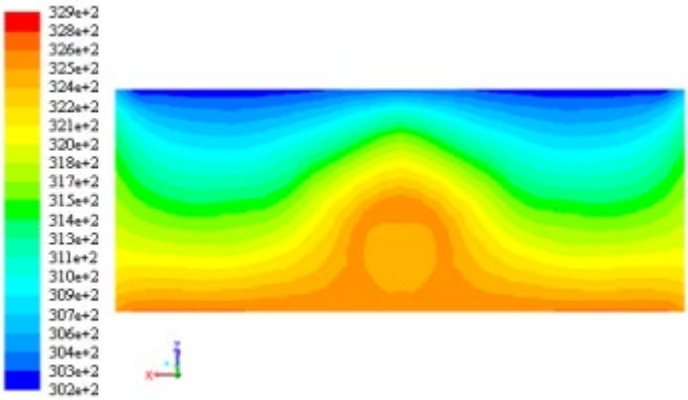


Рис.5. Контуры температуры воды в плоском солнечном коллекторе

На рис. 5 показана теплопередача от абсорбера к стояку с помощью механизмов кондукции и конвекции.

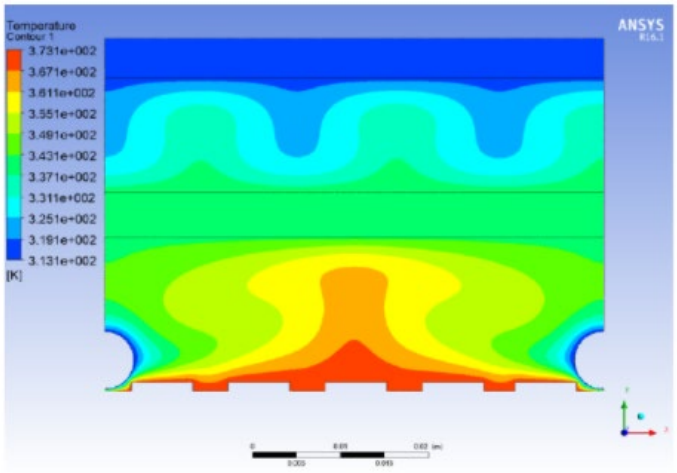


Рис.6. Температурный контур в расчетной области плоского солнечного коллектора

На рис. 6 показаны распределения температуры в расчетной области. Максимальная температура 373 К, показанная красным цветом, а минимальная температура 313 К, показанная синим цветом. В расчетной области температура изменяется между этими значениями. Самая низкая температура у верхнего стекла, близкая к температуре окружающей среды. С другой стороны, самая высокая температура близка к пластине поглотителя. Температура нижнего стекла крышки 341,5 К. Это можно отнести к категории низких.

Испытания плоского солнечного коллектора проводились в течение нескольких ясных дней с 1 января по 1 апреля 2020 года.

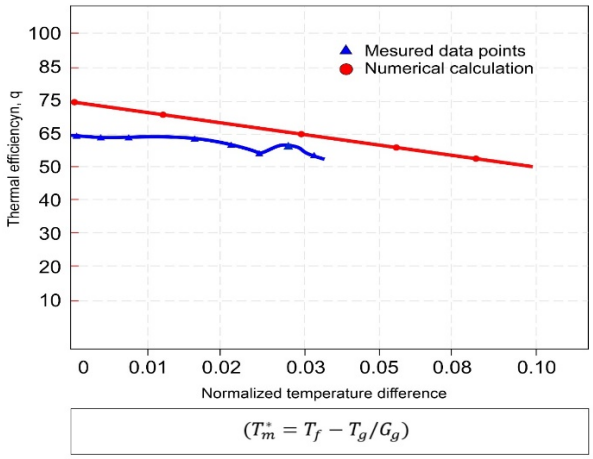


Рис.7. Численный расчет панели из змеевидной трубки

Как видно из рисунка 8 тепловые характеристики плоского солнечного коллектора с трубкой, работает немного лучше. Тепловые КПД коллектора змеевидных трубок на 4 % выше, чем у других типов антифризных коллекторов

4.Выводы

Представлена новая концепция плоского солнечного коллектора, в котором проведены численные расчеты наряду с экспериментальными испытаниями для анализа параметров эффективности коллектора. Численные расчеты показывают, что температура возле змеевидной трубки намного ниже между соседними параллельными частями трубки. Градиент температуры обусловлен эффективностью пластины поглотителя. В отличие от температурного контура типа змеевика с трубкой, обнаружено, что максимальная температура пластины-поглотителя коллектора при одинаковых условиях температуры на входе намного ниже, чем у первой. Тепловые КПД коллектора змеевидных трубок на 4 % выше, чем у других типов антифризных коллекторов. Как видно из графика при исследовании численным моделированием на 7-10 процентов тепловое КПД плоского солнечного коллектора будет выше чем при экспериментальных данных.

Литература

1. Sint NKC, Choudhury IA, Masjuki HH, Aoyama H. Theoretical analysis to determine the efficiency of a CuO-water nanofluid based-flat plate solar collector for domestic solar water heating system in Myanmar. Sol Energy 2017;155:608–19.

2. Tian Z, Perers B, Furbo S, Fan J. Annual measured and simulated thermal performance analysis of a hybrid solar district heating plant with flat plate collectors and parabolic trough collectors in series. Appl Energy 2017;205:417–27.

3.Li Q, Chen Q, Zhang X. Performance analysis of a rooftop wind solar hybrid heat pump system for buildings. Energy Build 2013;65:75–83.

4.Tian Z, Zhang S, Deng J, Fan J, et al. Large-scale solar district heating plants in Danish smart thermal grid: Developments and recent trends. Energy Convers Manag 2019;189:67–80.

5.Kalogirou SA. Solar thermal collectors and applications. Progress Energy Combust Sci 2004;30:231–95.

6.Cerón JF, Pérez-García J, Solano JP, García A, Herrero-Martín R. A coupled numerical model for tube-on-sheet flat-plate solar liquid collectors. Analysis and validation of the heat transfer mechanisms. Appl Energy 2015;140:275–87.

7.Gunjo DG, Mahanta P, Robi PS. Exergy and energy analysis of a novel type solar collector under steady state condition: experimental and CFD analysis. Renew Energy 2017;114:655–69.

8.Álvarez A, Tarrío-Saavedra J, Zaragoza S, López-Beceiro J, Artiaga R, Naya S, et al. Numerical and experimental study of a corrugated thermal collector. Case Stud Thermal Eng 2016;8:41–50.

9.Del Col D, Padovan A, Bortolato M, Dai Prè M, Zambolin E. Thermal performance of flat plate solar collectors with sheet-and-tube and roll-bond absorbers. Energy 2013;58:258–69.

10. Chen G, Doroshenko A, Koltun P, Shestopalov K. Comparative field experimental investigations of different flat plate solar collectors. Sol Energy 2015;115:577–88

РАЗРАБОТКА ПРОЦЕДУР ПРИНЯТИЯ РЕШЕНИЙ ПО ПРЕДУПРЕЖДЕНИЮ АВАРИЙНЫХ СИТУАЦИЙ С УЧЕТОМ ВЗАИМОСВЯЗИ ФАКТОРОВ РАЗВИТИЯ ПРОБЛЕМЫ

Есмагамбетова М.М., Сонькин М.А., Клюева Е.Г., Касымова Д.Т., Яворский В.В.
e-mail: yavorskiy-v-v@mail.ru
Институт информационных и вычислительных технологий КН МОН РК, Казахстан

Аннотация. *Статья посвящена вопросам снижения аварийности на производстве за счет выбора резервных технологических схем. Целью исследования было получение модели, отражающей взаимосвязь возникновения аварийных поражающих факторов на отдельных участках производства и влияние этого события на дальнейшую работу производства. Для определения вероятности возникновения поражающих факторов был применен метод экспертных оценок, для получения частоты отказов – дискретное распределение Пуассона. Предложены способы определения вероятностей отказов отдельных производственных звеньев при выходе из строя других. Рассмотрены понятия устойчивости и гибкости производственной систем. Исследованы возможности формирования алгоритма выбора совокупности программ предупреждения аварий всеми заинтересованными контрагентами Исследования проводятся в рамках проекта AP05133699 «Исследование и разработка инновационно-телекоммуникационных технологий с использованием современных кибер-технических средств для интеллектуальной транспортной системы города».*

В настоящее время при планировании производства особое внимание уделяется снижению аварийности его участков и повышения безопасности труда. Аварийные ситуации на отдельных участках производства могут происходить с

периодическими повторениями, в том числе одна и та же авария может произойти на разных участках и привести к различным последствиям [1].

Рассмотрим метод выбора резервной схемы, который основывается на анализе вероятностей возникновения аварий на производственных участках и состоящий из следующих шагов.

1. Расчет вероятностей отказов схем технологических процессов.

Зная условные вероятности $P_j^k(A_i)$ отказов отдельных производственных звеньев s_j в результате возникновения поражающего фактора x_k на звене s_j, можно рассчитать условные вероятности отказов $P_j^k(K)$ для схем технологических процессов. Их можно определить как единица минус произведение вероятностей безаварийной работы составляющих ее звеньев:

$$P_j^k(K) = 1 - \prod_{\substack{i=1 \\ k_j \neq 0}}^{S} (1 - P_j^k(A_i)) \tag{1}$$

где $K = (k_1, ..., k_S)$ - технологическая схема процесса, на которую возможен переход.

2. Выбор схемы процесса.

Среди схем процесса, на которые может быть осуществлен переход, выберем схему, удовлетворяющую правилу (2):

$$\min_{K:k_j=0} P_j^k(K) C(K^0, K) \tag{2}$$

Схема процесса, на которой достигается глобальный минимум, будет являться компромиссной с точки зрения максимизации надежности, с одной стороны, и минимизации затрат на перенастройку производства и потерь в эффективности — с другой.

Если не важны или пренебрежимо малы затраты на перенастройку технологических звеньев, а также если мало время, затрачиваемое на перенастройку, то в качестве критерия выбора схемы процесса можно взять следующий:

$$\min_{K:k_j=0} P_j^k(K)(C(K^0) - C(K)) \tag{3}$$

На основании условных вероятностей $P_j^k(K)$ отказов для схем технологических процессов можно рассчитать вероятность $P(K)$ отказа схемы технологического процесса:

$$P(K) = \sum_{j=1}^{S} \sum_{k=1}^{X} P(s_j, x_k) \cdot P_j^k(K) \tag{4}$$

Будем полагать, что из-за возникшей аварии применение операции s_i, которая входила в используемую в данных момент технологическую схему производственного процесса t^0 (или K^0 в других терминах) стало невозможным. Также предположим, что при помощи одного из описанных методов уже получено аварийное множество R_A и структурно-технологический резерв R_P для операции s_i, выполняемой на аварийном участке.

Проанализируем различные свойства сети. Если после вычеркивания из сети Петри N всех переходов, принадлежащих $R_A(s_i)$, в усеченной сети N_A остается достижимой конечная маркировка, то это означает, что рассматриваемая система обладает резервом при невозможности выполнения операции s_i. Набор последовательностей срабатывания переходов усеченной сети N_A, которые ведут к достижению конечной маркировки, назовем резервной технологической схемой производственной системы при невозможности выполнения операции s_i и будем обозначать ее как $L_P(s_i)$.

Структурно-технологическим резервом системы (комплекса операций), заданной сетью Петри N, назовем множество переходов $R_N = \{t_i^n\}$, такое, что при удалении любого из этих переходов из исходной сети N остается достижимой конечная маркировка сети N.

В случае, если выходит из строя любой единичный элемент множества R_N, технологический процесс продолжает функционировать, возможно, с меньшей эффективностью. При выходе из строя любого количества элементов, не принадлежащих R_N, система перестает функционировать. Если повреждено более одной операции из R_N, то нельзя сделать определенный вывод о работоспособности системы.

Множество $\overline{R}_N$ (дополнение к R_N) будем называть множеством уязвимости комплекса N. В него войдут те элементы, повреждение которых влечет за собой выход из строя всей системы.

Множество $\overline{R}_N$ может быть получено следующим образом: в него войдут те и только те переходы, которые принадлежат всем словам языка L.

На этом множестве вводятся различные характеристики: число операций в $\overline{R}_N$; число операций в $\overline{R}_N$, отнесенное к общему числу операций; суммарная эффективность операций из $\overline{R}_N$ при использовании любых технологических схем на этих операциях и т.д. Подобные численные характеристики назовем мощностью структурно-технологического резерва операции s_i.

Введем еще одну характеристику мощности структурно-технологического резерва операции s_i.

Множеством применимости структурно-технологического резерва операции s_i назовем множество переходов сети $\Gamma(s_i) = \{t_i^n\}$, таких, что найдется технологическая схема T_i^k рассматриваемой операции s_i и соответствующий этой схеме переход t_i^k, для которых верно $t_i^k \in R_P(s_j, T_j^n)$.

Другими словами, это - множество технологических схем операций, для замены которых могут использоваться технологические схемы операции s_i.

Как было показано выше, производственная система может реагировать на удаление одной из операций по-разному: от уменьшения эффективности производства до полного останова. Введем количественные характеристики этого реагирования.

Гибкостью производственной системы $G(s_i)$ относительно невозможности выполнения операции s_i назовем отношение числа возможных технологических цепочек $L_P(s_i)$, достижимых при повреждении s_i, к общему числу цепочек L, достижимых при нормальном функционировании системы [2]:

$$G(s_i) = \frac{|L_P(s_i)|}{|L|} \tag{5}$$

Как видно из определения, значением гибкости будет неотрицательное число, не превосходящее 1. Если гибкость $G(s_i)$=0, то при невозможности выполнения операции s_i вся система выходит из строя (жесткая система). Если гибкость $G(s_i)$ = 1, то операция s_i не используется ни в одной технологической цепочке и может быть без всякого ущерба удалена из производственной системы. Чем выше значение гибкости, тем меньше возникает потерь из-за невозможности выполнения операции s_i.

Для изучения гибкости системы в целом может быть использовано значение средней гибкости. Оно может быть получено по следующей формуле:

$$G_{cp} = \sum_{i=1}^{S} P(A_i) G(s_i) \tag{6}$$

где $P(A_i)$ - вероятность отказа звена.

По аналогии с утверждением о гибкости относительно невозможности выполнения одной операции можно утверждать, что чем выше значение средней гибкости системы, тем меньше потери из-за невозможности выполнения какой-либо операции.

Недостаток данного определения гибкости в том, что в нем не учитываются стоимостные характеристики потерь в результате ЧС. При расчете гибкости производственной системы указанным выше способом учитывается, сколько схем технологического процесса не смогут выполняться, но не учитывается их стоимость.

Для производственных звеньев могут быть рассчитаны потери, вызванные выходом из строя технологического звена s_i. Предположим, что с использованием одного из методов, описанных выше, была выбрана схема процесса K_i, на которую будет осуществляться переход.

Затратами производственной системы $\overline{C}(s_i)$ относительно невозможности выполнения операции s_i назовем стоимость перехода на выбранную схему технологического процесса:

$$\overline{C}(s_i) = C(K^0, K_i) \tag{7}$$

Чем выше эта величина, тем большие потери вызовет невозможность выполнения операции s_i.

Долей сохраняемой стоимости систем относительно невозможности выполнения операции s_i. назовем отношение стоимости замещающей схемы процесса K_i к стоимости исходной схемы процесса K^0:

$$\Phi(s_i) = \frac{C(K_i)}{C(K^0)} \tag{8}$$

Величина $\Phi(s_i)$ может быть отрицательной, в случае если после возникновения аварии система работает с убытками [3].

На основе вероятностей отказов звеньев и долей сохраняемой стоимости введем понятие гибкости производственной системы в целом.

Гибкостью производственной системы, заданной сетью Петри N, назовем величину:

$$G_N = \sum_{i=1}^{S} P(A_i)\Phi(s_i) \tag{9}$$

Эта величина характеризует способность производственной системы сохранять эффективную работу в случае возникновения аварийной ситуации на одном из ее участков. Чем она выше, тем большим структурно-технологическим резервом обладает производственная система и, как следствие, тем устойчивей она в целом.

Может возникнуть вопрос о сравнении способа реагирования различных производственных систем, реализующих одну и ту же функцию, на возникающие в них аварии. Поскольку эти системы могут состоять из разного количества операций s_i, то их сопоставление путем сравнения средних значений гибкости не будет показательным. Поясним это утверждение на следующем примере.

Пусть построены сети Петри N_1 и N_2 двух производственных систем, реализующих одну и ту же функцию. Число операций в первой равно $S_1 = 5$, во второй $S_2 = 20$. Пусть гибкость обеих систем равна $G_{N_1} = G_{N_2} = 0{,}9$. Это означает, что при невозможности выполнения одной операции из строя выходит 10% технологических цепочек в обеих системах. Но невозможность выполнения одной операции означает выход из строя 20% операций в первой системе и 5% операций - во второй. Следовательно, сравнивать системы с различным числом операций, основываясь только на значении средней гибкости, нельзя.

Для преодоления этого недостатка следует также учитывать долю вышедших из строя операций. При невозможности выполнения одной операции эта доля составит $1/|S|$ от общего числа операций, и при аварии на операции s_i она будет равна:

$$\frac{|L| - |L_i|}{|L|} \tag{10}$$

где $|L|$ - число всех технологических цепочек, а $|L_i|$ - число цепочек, выполнение которых становится невозможным при аварии на операции.

Рассчитаем среднюю долю выходящих из строя технологических цепочек при невозможности выполнения одной операции производственной системы:

$$\begin{aligned} &\frac{1}{|S|}\cdot\sum_{i=1}^{|S|}\frac{|L|-|L_i|}{|L|} = \frac{1}{|S|}\cdot\sum_{i=1}^{|S|}\left(1-\frac{|L_i|}{|L|}\right) = \frac{|S_i|}{|S|} - \frac{1}{|S|}\cdot\sum_{i=1}^{|S|}\frac{|L_i|}{|L|} = \\ &= 1 - \frac{1}{|S|}\cdot\sum_{i=1}^{|S|}G(s_i) = 1 - G_{cp} \end{aligned} \tag{11}$$

Введем понятие устойчивости производственной системы.

Устойчивостью *H* производственной системы относительно невозможности выполнения части ее операций назовем отношение доли выходящих из строя операций к доле технологических цепочек выполнение которых стало невозможным [4].

При выходе из строя одной операции значение устойчивости будет равно:

$$H = \frac{1}{|S|} : (1 - G_{cp}) = \frac{1}{|S| \cdot (1 - G_{cp})} \qquad (12)$$

Поскольку при вычислении устойчивости учитывается доля невыполняемых операций, то это позволяет сравнивать производственные системы различного масштаба.

В приведенном выше примере устойчивость для первой производственной системы будет равна:

$$H_1 = \frac{1}{|S_1| \cdot (1 - G_{cp}^1)} = \frac{1}{5 \cdot 0{,}1} = 2,$$

для второй:

$$H_2 = \frac{1}{|S_2| \cdot (1 - G_{cp}^2)} = \frac{1}{20 \cdot 0{,}1} = 0.5.$$

Сравнивая H_1 и H_2можно утверждать, что первая система сохраняет большую работоспособность при возникновении на ней аварий, поскольку $H_1 > H_2$.

Таким образом, можно сделать заключение о зависимости значения устойчивости производственной системы и способности ее сохранять технологические цепочки при возникновении аварий:

– если устойчивость (*H*) производственной системы меньше 1, то при возникновении даже мелких аварий и выходе из строя относительно небольшого числа операций резко снижается число технологических цепочек, сохраняющихся в работоспособном состоянии. Такие производственные системы крайне чувствительны к возникающим на них авариям;

– если устойчивость (*H*) производственной системы больше 1, то при возникновении относительно крупных аварий и выходе из строя части операций число допустимых технологических цепочек остается достаточно большим. Подобные производственные системы менее чувствительны к возникающим авариям.

Любое крупное производство состоит из отдельных участков, на каждом из которых существуют опасные факторы, которые при определенных обстоятельствах могут создать аварийную ситуацию. Возникновение аварии на одном из участков производства вызывает как минимум остановку других, которые непосредственно с ним связаны. Однако на реальном производстве авария на одном участке может вызвать изменение параметров других, что также может привести к аварии.

Обозначим факторы, которые вызывают аварии через x_k а их общую совокупность – *X*. Предположим, что на производственном участке s_i возникает поражающий фактор x_i, который может переместиться на другие производственные

участки. Это может вызвать возникновение таких же факторов уже на новых участках производства, что также может привести к аварии. Чрезвычайная ситуация может развиваться по нескольким сценариям для каждого поражающего фактора. Время моделирования распространения поражающего фактора по производственным звеньям ограничено. Будем считать невозможным функционирование тех звеньев, где по окончании моделирования будут расположены поражающие факторы.

Пользуясь методом экспертных оценок, можно задать вероятности возникновения поражающих факторов на участках производства. Для получения вероятности $P\ (s_i,\ x_k)$ можно также применять модели теории надежности, отражающие возможность функционирования производства на данном участке безотказно [2]. Среди таких моделей можно отметить те, которые характерны для систем с малой наработкой на отказ, которые могут выходить из строя чаще, и высоконадежных, новых систем, для которых аварии – редкий случай.

Для расчета вероятностей возникновения аварии можно также использовать методы дискретного распределения Пуассона и статистики, которые применяются для прогнозирования редких событий.

Вероятность отказа представляет собой функцию риска из-за возникновения чрезвычайной ситуации и вычисляется по формуле (13):

$$\begin{aligned} &H(t) = 1 - P(t) \\ &P(t) = \exp\left(-\int_0^1 \lambda(\zeta)d\zeta\right) \end{aligned} \tag{13}$$

где $P(t)$ - вероятность безотказной работы;

$\lambda(t)$ - интенсивность отказов, равная вероятности того, что после безотказной работы до момента времени *t* авария произойдет в ближайшем времени.

Следует отметить, что после начального опытного периода эксплуатации, функция $\lambda(t)$ является достаточно стабильной и может считаться постоянной, т.е. $\lambda(t) = const.$ Такие факторы, как износ оборудования, его моральное и физическое устаревание должны регламентироваться внутренними нормативными документами предприятия.

Примем для периода нормального функционирования $\lambda(t) = const.$ Тогда получим экспоненциальное распределение вероятности безотказной работы:

$$P(t) = e^{-\lambda r} \tag{14}$$

Обозначим среднюю наработку на отказ (математическое ожидание срока службы) как $\overline{\theta} = 1/\lambda.$

Тогда функцию риска можно записать так:

$$H(t) = 1 - e^{-t\overline{\theta}} \tag{15}$$

Частота отказов будет соответствовать дискретному распределению Пуассона:

$$Q(N,\lambda\tau)=\frac{(\lambda\tau)^N}{N!}\cdot e^{-\lambda\tau} \tag{16}$$

Согласно представленной формуле, аварии во временном интервале $(t,t+\tau)$ произойдут N раз с вероятностью $Q(N,\lambda\tau)$, а отсутствие аварийных ситуаций будет обладать вероятностью $Q(N,\lambda\tau)=e^{-\lambda\tau}$.

Также можно определить вероятность появление хотя бы одной аварии:

$$\overline{Q}(\tau)=1-Q(0,\lambda\tau)=1-e^{-\lambda\tau} \tag{17}$$

Применяя данный метод, можно определить вероятность возникновения поражающего фактора x_k на производственном участке s_i из-за произошедшей на нем аварии [5]. Аналогично можно получить вероятность возникновения поражающего фактора при использовании определенной технологической схемы T_i^j. Обозначим эту вероятность как $P(s_i,T_i^j,x_k)$.

Должно выполняться равенство:

$$P(s_i,x_k)=\sum_{j=1}^{n_i}P(s_i,T_i^j,x_k) \tag{18}$$

Располагая данными оценками, можно определить вероятностное пространство возникновения аварийных ситуаций $\langle\Omega,P\rangle$, где $\Omega=\{\omega_k\}$ - множество элементарных исходов, а P – их вероятность.

Множество элементарных исходов Ω, все элементы которого являются векторами, зададим следующим образом:

$$\Omega=\{\omega_k=(\theta_1,...,\theta_s),\text{где } \theta_i\in\{0,1\}\}, \tag{19}$$

где $\theta_i=1$, если в результате ЧС стало невозможным выполнение операции s_i. В обратном случае, если $\theta_i=0$, выполнение операции s_i допустимо.

Соответственно, исход $\omega_0=(0,...,0)$ означает функционирование производства без аварий.

Если возникает необходимость учета отдельных операций технологических схем, то пространство элементарных исходов можно определить:

$$\Omega=\{\omega_k=(\theta_1^1,...,\theta_1^{n_1},\theta_2^1,...,\theta_2^{n_2},...,\theta_s^1,...,\theta_s^{n_s}),\text{где } \theta_i\in\{0,1\}\}, \tag{20}$$

где n_i – число технологических схем на производственном звене s_i.

В случае если некоторый элемент этого вектора $\theta_i^j=1$, то это означает, что в результате произошедшей аварии на операции s_i применение технологической схемы T_i^j стало невозможным. Если $\theta_i^j=0$, то применение этой технологической схемы допустимо [3].

Будем предполагать, что множество элементарных исходов Ω задано первым способом, а все дальнейшие вывод могут быть обобщены и для второго случая.

Обозначим:

$$\omega_{(i)} = (0,...,0,\theta_i \approx 1,0,...,0) \tag{21}$$

т.е. $\omega_{(i)}$ - такой исход, при котором авария возникает только на звене s_i,

$$\omega_{(i_1,...,i_n)} = (\theta_i\ ,...,\theta_S) \tag{22}$$

где $\theta_{i_k} = 1$ для $k = \overline{1,n}$, а остальные $\theta_i = 0$, т.е. $\omega_{(i_1,...,i_n)}$ - такой исход, при котором авария возникает на звеньях $s_{i_1},...,s_{i_n}$ и только на них.

На множестве элементарных исходов Ω определим вероятность P. Для этого будем использовать следующие процедуры.

1. Построение модели.

Для построения модели будем применять методы, которые были описаны выше. Каждому производственному участкуs_i поставим в соответствие объект S_i. Построим следующие подсети: $N^{П}$– распространения поражающих факторов, N^{C} – моделирование исходного размещения и процесс перемещения между объектами сил и средств ликвидации поражающих факторов, $N^{ПС}$ – моделирование процесса ликвидации поражающих факторов с использованием имеющихся сил и средств [2].

2. Проведение моделирования.

Для каждого производственного объекта S_i, где может возникнуть поражающий фактор и для каждого поражающего фактора, который может возникнуть на производственном участке s_i, поместим маркер, который отвечает возникшему виду поражающего фактора, в позицию, которая соответствует очагу аварии – звену s_i.

Для того, чтобы получить несколько сценариев развития аварийных ситуаций, проведем несколько циклов моделирования. Необходимое количество повторений зависит от требуемой точности, а также от имеющихся в распоряжении времени и техники.

3. Анализ результатов моделирования.

Условная вероятность $P_i^k = (\omega_{(i_1,...,i_n)})$ поражения объектов $S_{i_1},...,S_{i_n}$ в результате возникновения поражающего фактора x_k на объекте S_i будет равна отношению числа сценариев, при которых на объекты $S_{i_1},...,S_{i_n}$ заносятся какие-либо поражающие факторы, к общему числу сценариев развития аварийной ситуации.

4. Определение вероятности.

Имея результаты расчетов условных вероятностей, можно определить вероятности для произвольного элементарного исхода $\omega_k = (\theta_1,...,\theta_S)$.

Пусть для этого исхода $\theta_{i_1} = 1,...,\theta_{i_n} = 1,$ а остальные $\theta_i = 0.$ Тогда определим вероятность данного исхода как:

$$P(\omega_k) = \sum_{j=1}^{S}\sum_{k=1}^{X} P(s_i, x_k) \cdot P_j^k(\omega_{(i_1,...,i_n)}) \tag{23}$$

Вероятность работы без аварий ω_0 определим как единица минус сумма вероятностей всех исходов, при которых происходят аварии [4]:

$$P(\omega_0) = 1 - \sum_{\substack{\omega_k \in \Omega \\ \omega_k \notin \omega_0}} P(\omega_k) \tag{24}$$

Если вероятность работы без аварии меньше нуля или вероятности исходов, при которых происходят аварии, стремятся к нулю, следует изменить продолжительность исследуемого периода: уменьшить в первом случае или увеличить во втором.

Следует отметить, что вероятность P была задана с предположением, что за период происходит не более одной аварии.

Выделим события, вероятности которых будут использованы далее.

Назовем событием A_i совокупность всех таких исходов $\{\omega_{(i)} = (\theta_1, ..., \theta_S)\} \subseteq \Omega$, в которых $\theta_i = 1$. Это событие будет отражать выход из строя производственного участка s_i как при возникновении в нем первичных поражающих факторов, так и при повреждении его вторичными поражающими факторами. Вероятность события A_i будет равна сумме вероятностей элементарных исходов, которые его составляют [6]:

$$P(A_i) = \sum_{\omega \in A_i} P(\omega) \tag{25}$$

Аналогично можно рассчитать условную вероятность $P_j^k(A_i)$ поражения объектов S_iв результате возникновения фактора x_k на объекте S_j:

$$P_j^k(A_i) = \sum_{\omega \in A_i} P_j^k(\omega) \tag{26}$$

Допустим, что множество элементарных исходов задано с точностью до технологических схем, применяемых на производственных звеньях (второй способ). В этом случае событием A_i^j назовем совокупность таких элементных исходов [2]:

$$\omega_k = (\theta_1^1, ..., \theta_1^{n_1}, \theta_2^1, ..., \theta_2^{n_2}, ..., \theta_s^1, ..., \theta_s^{n_s}) \subseteq \Omega, \text{ в которых } \theta_i^j = 1.$$

После нарушения работы производственного участка S_j, входящего в схему процесса K_0, и появления на этом участке поражающего фактора x_k потребуется переход на другую схему производства. В качестве замещающей схемы можно выбрать схему, переход на которую потребует меньших затрат:

$$\min_{K:k_j=0} C(K^0, K) \tag{27}$$

В (27) требование $k_j=0$ означает, что в дальнейшем невозможно использовать вышедшее из строя звено s_j.

Литература

1. Mozer D., Fofanov O., Yavorskiy V. Satellite radar interferometry as a reliable tool for monitoring displacements of rock masses // Proceedings of 2015 International Conference on Mechanical Engineering, Automation and Control Systems, MEACS 2015.
2. Архипова Н.И., Кульба В.В. Управление в чрезвычайных ситуациях. Учебное пособие. – М.: Российский государственный гуманитарный университет, 2008. – 470 с.
3. Матвеевский В.Р. Надежность технических систем. Учебное пособие – М.: Московский государственный институт электроники и математики, 2002. – 113 с.
4. Основы расчета надежности технических систем по надежности их элементов. [Электрон.ресурс]. – 2015. – URL: http://www.obzh.ru/nad/4-5.html. (Дата обращения: 13.08.2020).
5. Karagiannis, G.-M., Piatyszek, E., Flaus, J.-M., 2010. Industrial emergency planning modeling: a first step toward a robustness analysis tool. J. Hazard. Mater. 181. 1. 324–334.
6. Валиуллина В.А., Садофьев В.А. Разработка функциональных схем автоматизации технологических процессов. Учебное пособие. – Казань: Издательство КНИТУ, 2013. – 126 с.

RESEARCH OF NEW STRUCTURES OF THE TILT FIBER BRAGG GRATINGS AND THEIR PROPERTIES

[1,4]A. Kalizhanova, [1,3]S. Amirgalieva, [4,5]A. Kozbakova,
[6]G. Kashaganova, [1,3]Zh. Aitkulov,
e-mail: kalizhanova_aliya@mail.ru
[1]Institute of Information and Computational Technologies CS MES RK, Almaty
[2]Lublin Technical University, Poland
[3]International University of Information Technology, Almaty, Kazakhstan
[4]Almaty University of Power Engineering and Telecommunications, Almaty
[5]Almaty University of Technology, Almaty
[6]Astana IT-University, Nur-Sultan, Kazakhstan

Abstract. *In this paper new structures of tilted fiber Bragg gratings and their properties are considered. The article presents the results of experimental research of periodic structures with a linearly variable value of the period of chirped tilted fiber Bragg gratings (CTFBG) and twisted tilted fiber Bragg gratings (TTFBG). Among the many new types of periodic structures, that are currently being developed, the structures considered are promising. The proposed designs represent a new approach to reducing the sensitivity to polarization of tilted fiber Bragg gratings, which can be used to measure the refractive index, and open up wide possibilities for their practical application in creating fiber-optic systems in various industries and other fields of activity. The properties of the indicated periodic structures are experimentally researched, their parameters and functional capabilities are determined.*

Introduction

Chirped tilted fiber-optic Bragg gratings (CTFBG) periodic structures with variable period.

One of the groups of periodic structures with tilted modulation of refractive index are tilted structures with linear variable value of CTFBG period. Those structure types are used as edge filters in the filtration systems signals, for insrance, from sensors, on the basis of standard, simple and uniform Bragg gratings [1-5], as well, as the structures, used for restrainting the effect of combinational scattering in fiber lasers [6].

Apart from that, CTFBG structures recording on optic fibers with large mode area (LMA) allows limit their sensitivity to the temperature [7].

Mutual arrrangement of CTFBG transfer characteristics, used in the system and FBG reflection characteristics is shown in the Figure 3. Unbroken red line in the Figure demostrates the CTFBG characteristics form, while the dotted lines show the form and position of FBG characteristics. In the situation, when CTFBG transmission characteristics have symmetric downslopes, there might be operated the system both at the left (discending) and at the right (ascending) downslopes of CTFBG. System's operating area at the ascending CTFBG downslope is indicated in green color, and system's characteristics, changing the position at the descending downslope, denoted in bleu color.

As it can be seen, the FBG structure can work as a sensor, for instance, of voltage, at that, there is possible both compression and extension.

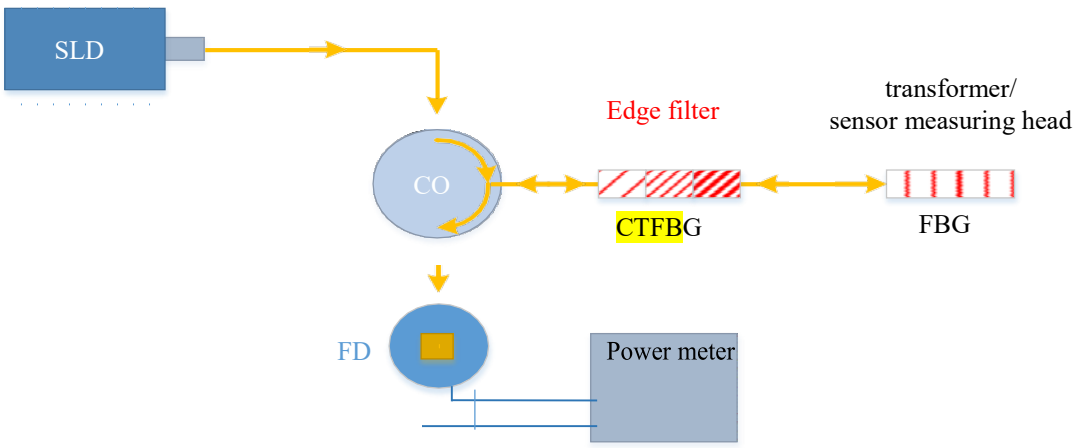


Fig. 1 CTFBG usage in edge filter system for FBG sensors

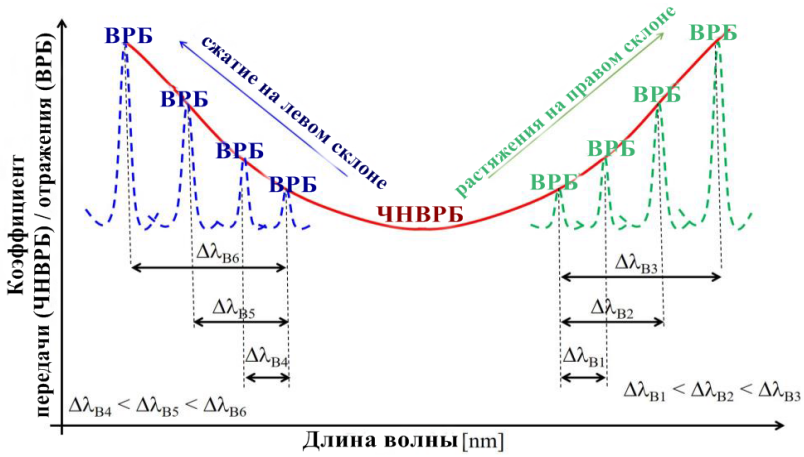


Fig. 2 Edge filter characteristics on the basis of tilted gratings with variable period (CTFBG) and sensors, using uniform and simple Bragg gratings (FBG)

At such selection of CTFBG and FBG spectral characteristics there is possible transformation of the wave shift value, prescribed FBG elements length onto the power value, being reflected by FBG and reaching, for instance, the photodetector.

The first of them consists in non-uniformity separate modes spectral dilatation, propagating in the CTFBG structure in the result of increasing the length of refraction index modulation period value. The second phenomenon is decreasing of minimums height, obtained from separate cladding modes, due to increase of the tilt, caused with increasingly stronger «leakage» of modes from the CTFBG structure. Thus, both phenomena thereof cause flattening of the total CTFBG transmission characteristics.

Possibilities of the CTFBG spectral characteristics tilt formation are important in terms of their potential usage as edge filters. All described structures with tilt modulation of refraction index have one common feature, which imposes some restrictions on detection systems. If we introduce polarizing light into optic fiber from TFBG, then spectral range, corresponding to cladding modes, will change dependent on the state of that light polarization. Therefore, influence of polarization inlet light at TFBG structures spectrum, including CTFBG, defines the necessity of state control, for example, of polarization. Accordingly, of the research, leading to decreasing or eliminating effect of inlet light polarization angle at optical parameters, for instance, form of transmission characteristics, tilted periodical structures.

Tilted twisted fiber-optical periodic structures of CTFBG

An example of TFBG new structure is Brag grating, made of twisted tilted fiber Bragg grating, first offered in [8]. As it has been shown, the inlet light polarization state influences at TFBG structures optical parameters. In the work it has been proved, that twisting of already tilted modulation of refraction index lowers the sensitivity of such structure to the angle of inlet light polarization. Optical fibers and recorded on them simple and uniform periodic fiber-optic structures are insensitive to the inleted light polarization changes, as they are cylindrically symmetric. Such symmetry is their important advantage, as upon measuring the signals, entering from such structures, for example, in the interrogator system there is no need in polarized light. Moreover, there is no necessity to control polarization along whole optic trajectory, for instance, using the fibers, supporting polarization [9, 10, 11]. Optic fiber might become sensitive to the inlet light polarization plane under certain conditions. As it has been already mentioned, the most frequent reason of polarization sensitivity is its cylindrical symmetry breaking. Hereby it should be noted, that TFBG structures are fabricated by means of change axle tilt of refraction index in respect to surface normal to optic fiber axle, which is the disturbance of such cylindrical symmetry [12-16].

Described method of minimizing the influence of polarization changes consists in fabricating the new TFBG structure, which will be insensitive to the light polarization change. Solution in that case is in creating the structure, which, apart from infraction index modulation tilt will be twisted along its length for definite angle ϕ, as it is shown in the Figure 3.

Figure 3 shows the method of specifying the angle of structure ϕ twisting. The same structure is also characterized with angle θ, defining refraction index modulation tilt in respect to surface normal to the fiber, on which is written TFBG.

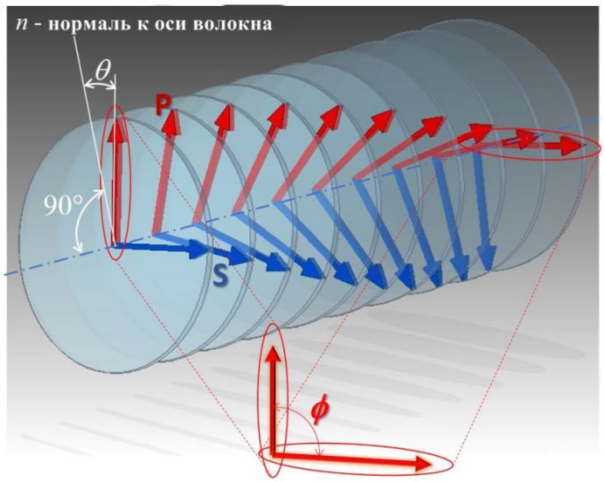


Fig. 3 Twisting the TFBG structure to the angle ϕ. Red arrows denote polarization type P, blue arrows correspond to polarization type S

In order to demonstrate the structure twisting effect on the dependence of its transmission spectrum from inlet light polarization, at the first stage there has been carried out testing, in which TFBG is twisted under known angle ϕ. For testing there has been fabricated the TFBG structure with tilted angle θ= 5°. Transmission characteristics of total structure without induced twisting have been shown in the Figure 4. Spectrum evolution due to changes of polarization for untwisted structure (ϕ=0°) is shown in the Figure 5.

Three spectral characteristics have been measured for three different values of the inlet light polarization angle in compliance with P-type polarization, polarization is turned for 45 °, which conforms to polarization S | P-type, and polarization turned for на 90 °, which corresponds to S-type polarization. Figure 6 shows the outcomes of analog spectral measurements, already made on construction, twisted under angle ϕ = 45°.

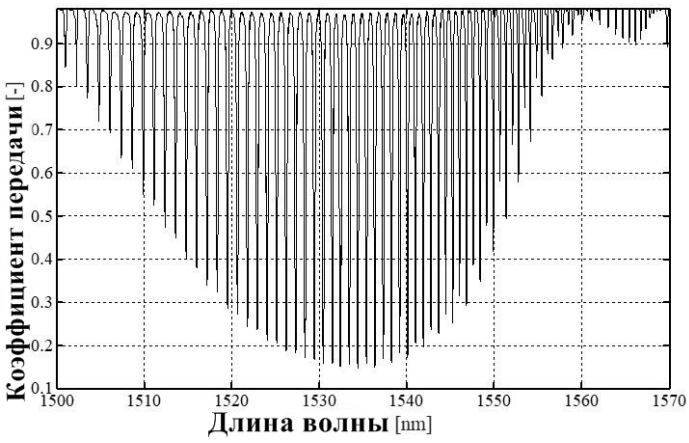


Fig. 4 Spectral characteristics of TFBG structures: θ=5°, ϕ=0°

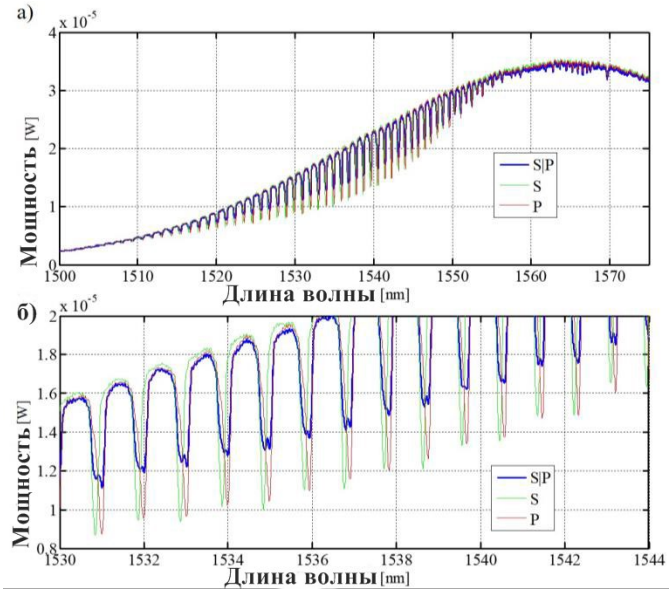


Fig.5 Outcomes of TFBG spectral measurements θ=5°, ϕ=0° has been twisted for three inlet light polarization states of inlet type for waves length:
а) 1500-1575 nm, б) 1530-1544 nm

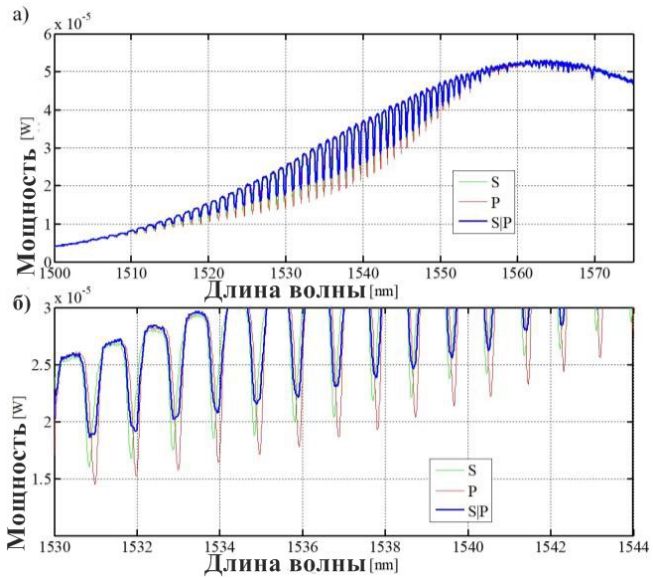


Fig. 6 Outcomes of TFBG spectral measurements θ=5°, twisted under angle ϕ=45° for three inlet light polarization states for waves lengths:
а) 1500-1575 nm, б) 1530-1544 nm

Measurements outcomes, presented in Figures 5-6, prove, that it is possible to control sensitivity to the inlet light polarization angle changes, choosing the twisted angle of the whole TFBG structure. Amplitude change of the peak, obtained from cladding modes, so much the less, than bigger the twisting angle ϕ of TFBG structure.

All received gratings had the tilt of refraction index modulation - θ =5°. Measurements outcomes for two spectral ranges, complete (a) and narrowed for selected cladding modes (б), are generalized in the figure 7.

The structure twisting direct effect is in decreasing the transmission index changes for separate cladding modes with the inlet light polarization changes.

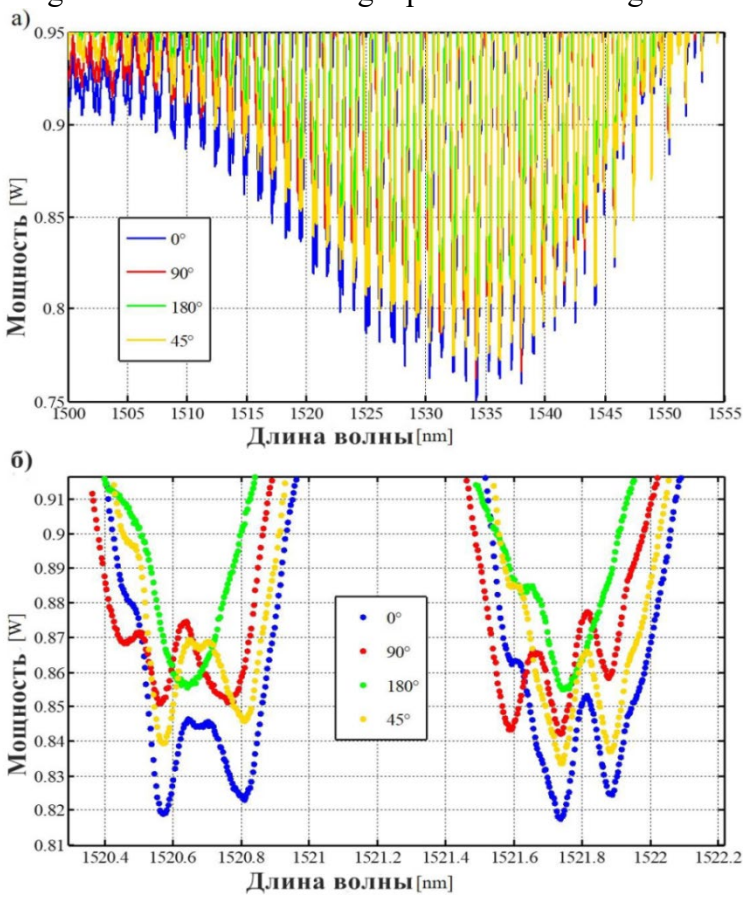


Fig. 7 Comparison of spectral characteristics of four CTFBG structures, differing according to angle ϕ: a) total spectral range, б) selected spectral range, conforming to two selected cladding modes

Figure 8 demonstrates changes of transmission modes P and S due to changes in the inleted light polarization state for TFBG structure, CTFBG structure is twisted along its total length for 45°, 90° and 180°. For comparison, all structures had similar length of L=10 mm. Graphs, presented in the Figure 8, show the changes of transmission index values of the selected cladding mode.

Graphs have been obtained by means of numerical computations through the structure breaking down into 50 elements. Each such element has been prescribed a corresponding transmission spectrum. To illustrate spectrum dependence on polarization rotation, the graphs in the Figure 8 present transmission indices for the minimum, obtained from the selected mode.

The most important stage of numerical computation is definition of transmission index of uniform grating T (α) for each polarization state, presented with an angle α of linear polarization light. Such transmission has been defined, using the measurements, executed for uniform twisted TFBG structure with 1 cm length and angle θ, equal to 5°. Twisted grating transmission was specified as the product of transmitting 50 uniform TFBG structures with 1/50 cm length. In that case transmission index of simple uniform TFBG structure will be defined with the equation:

$$T_{\phi}(\alpha) = \sqrt[50]{T(\alpha)} \tag{1}$$

Accordingly, the transmission index of the grating twisted for 90° angle will be defined with an equation:

$$T_{0-90}(\alpha) = T_{\phi}(\alpha)T_{\phi}\left(\alpha + \frac{1}{50}90^0\right) \cdot T_{\phi}\left(\alpha + \frac{2}{50}90^0\right) \cdot \ldots \cdot T_{\phi}\left(\alpha + \frac{49}{50}90^0\right), \tag{2}$$

quite the reverse, for the structure, twisted for 180° angle, its transmission coefficient has been defined with an equation:

$$T_{0-180}(\alpha) = T_{\phi}(\alpha)T_{\phi}\left(\alpha + \frac{1}{50}180^0\right) \cdot T_{\phi}\left(\alpha + \frac{2}{50}180^0\right) \cdot \ldots \cdot T_{\phi}\left(\alpha + \frac{49}{50}180^0\right). \tag{3}$$

At the extreme left of the grating position at the angle ϕ=180° separate simple gratings were twisted at angles 0°, 180°/50, 2·180°/50, 3·180°/50, 4·180°/50, ..., 49·180°/50. Figure 8 shows outcomes of numerical computations of transmission index, carried out for the minimum, received from the selected cladding mode.

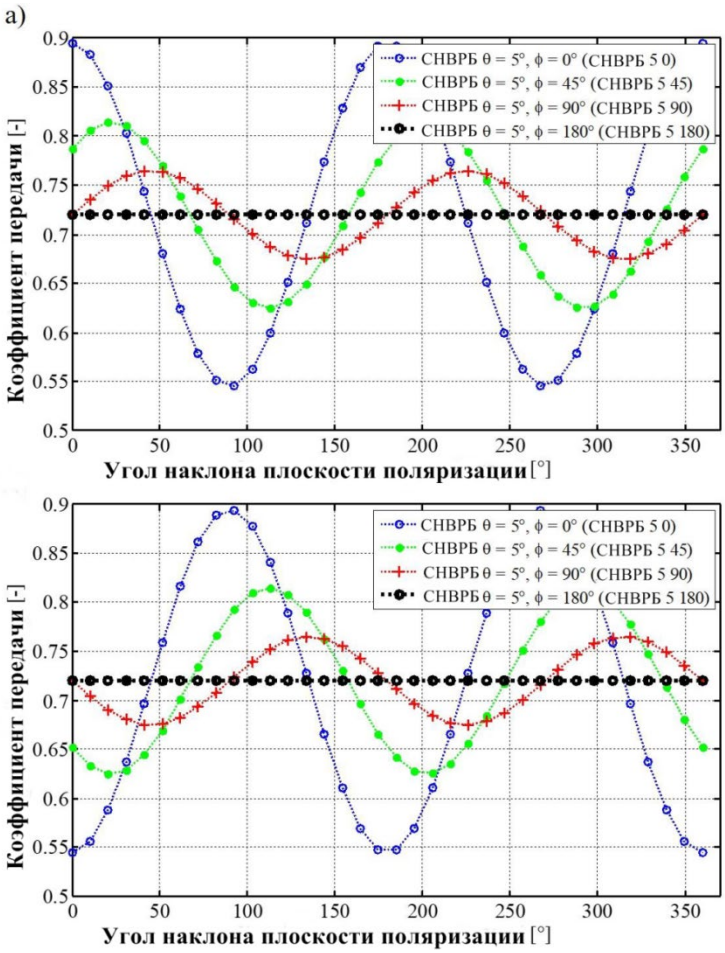


Fig. 8 Outcomes of numerical computations of CTFBG structure transmission index change for different angles ϕ: a) for P type mode, б) for S type mode.

In case of twisted structure the form of transmission modes changes is asymmetric. Therefore, both polarization rotation direction and such grating rotation direction cannot be defined on the basis of spectral characteristics. In case of structure for which $\phi = 45°$, when polarization plane rotation angle changes in the range from-22,5 to +22,5°°, such discrimination is acceptable. Such structure's twisting angle also can be identified. The grating, turned for 180 degrees along its length, does not show polarization sensitivity.

Conclusion

In the result of conducted experimental researches it has been shown, that the inlet light polarization state influences at TFBG structures optic parameters. In the work it has been proved, that twisting of already tilted modulation of refraction index lowers the sensitivity of such structure to rotation angle of the inlet light polarization. As well, it should be noted, that offered structures represent a new approach to decreasing the sensitivity to the tilted fiber Bragg gratings polarization, which might be applied to refraction index measuring. Obtained results are of interest upon fabricating the fiber-optic measuring systems in different industry fields, for instance, automobile industry (refractometers for working liquids), food industry, agriculture, cattle-breeding (refractometers for measuring concentration of, for instance, sugar, salt in water solutions), industrial technologies (refractometry, for example, of oil products, refractometer for measuring oil emulsions, cooling oils), as well, in the area of point by point measurements applying. As well, attention should be paid to practical aspects of the CTFBG structures usage, comparing them, for example, with two structures, fabricated under 180° angle in respect to each other. Technologically, it is better to conduct one process of periodic structure recording on a single-mode fiber.

Experimental researches have been carried out in the laboratories of Optoelectronic faculty of electric engineering and computer sciences of Lublin technical university in the frame of the project SF #AP05132778 «Research and development of interrogation system of signals with optic-fiber refractometer, using telecommunication networks» IICT CS MES RK.

References

[1]Guo T., Tam H.-Y., Albert J., Chirped and tilted fiber Bragg grating edge filter for in-fiber sensor interrogation. CLEO:2011 – Laser Applications to Photonic Applications 1-2 (2011). doi: 10.1364/CLEO_SI.2011.CThL3

[2]Guo T., Tam H.-Y., Albert J., Linearly chirped and weakly tilted fiber Bragg grating edge filters for in-fiber sensor interrogation. Proceedings of SPIE 7753, 21st International Conference on Optical Fiber Sensors, 77537V-1- 77537V-4 (2011). doi: 10.1117/12.884956

[3]Liu Y., Zhang L., Bennion I., Arbitrary spectral response fibre edge filters based on tilted chirped grating structures. Technical Digest. Summaries of papers presented at the Conference on Lasers and Electro- Optics. Postconference Edition. CLEO '99. Conference on Lasers and Electro-Optics (IEEE Cat. No.99CH37013), 297 (1999). doi: 10.1109/CLEO.1999.834214

[4]Liu Y., Zhang L., Bennion I., Fabricating fibre edge filters with arbitrary spectral response based on tilted chirped grating structures. Measurement Science and Technology 10(1), L1-L3 (1999). doi: 10.1088/0957-0233/10/1/001

[5]Osuch T., Jurek T., Jędrzejewski K., Spectral transmission characteristics of weakly tilted and tilted chirped fiber gratings: comparative studies, Proceedings of SPIE 8903, Photonics Applications in Astronomy, Communications, Industry, and High-Energy Physics Experiments, 89030W-1- 89030W-6 (2013). doi: 10.1117/12.2035446

[6]Wang M., Zhang Y., Wang Z., Sun J., Cao J., Leng J., Gu X., Xu X., Fabrication of chirped and tilted fiber Bragg gratings and suppression of stimulated Raman scattering in fiber amplifiers. Optics Express 25(2), 1529-1534 (2017). doi: 10.1364/OE.25.001529

[7]Wang M., Li Z., Liu L., Wang Z., Gu X., Xu X., Fabrication of chirped and tilted fiber Bragg gratings on large-mode-area doubled-cladding fibers by phase-mask technique. Applied Optics 57(16), 4376-4380 (2018). doi: 10.1364/AO.57.004376

[8]Kisała P., Mroczka J., Cięszczyk S., Skorupski K., Panas P., Twisted tilted fiber Bragg gratings: new structures and polarization properties. Optics Letters 43(18), 4445-4448 (2018). doi: 10.1364/OL.43.004445

[9]Dai R., Zhang L., Liu Y., Zhou Y., Twist characteristics of the helical long-period fiber gratings written in the polarization maintaining fiber. 2017 16th International Conference on Optical Communications and Networks (ICOCN), IEEE 1-3 (2017). doi: 10.1109/ICOCN.2017.8121284

[10] Jiang Ch., Liu Y., Zhao Y., Zhang L., Mou Ch., Wang T., Helical Longperiod Fiber Grating Written in Polarization-maintaining Fiber by CO2- laser. Conference on Lasers and Electro-Optics OSA Technical Digest 1-2 (2018). doi: 10.1364/CLEO_SI.2018.SM2K.2

[11] Liu Q., Chai Q., Tian Y., Zhao Y., Liu Y., Wang S., Zhang J., Yang J., Yuan L., Spectral characteristics of rotated fused polarization maintaining fiber Bragg gratings subjected to transverse loading. 2017 25th Optical Fiber Sensors Conference (OFS), Proceedings of SPIE 10323, 103233Q1-103233Q4 (2017). doi: 10.1117/12.2265310

[12] Wojcik, J., Czyzewska, L., Klimek, J., Chodkowska, E. and Warda, J., "Technology of silver structural elements for special waveguides production," Proc. SPIE 5028, 35-39 (2003).

[13] Wójcik, W., Kisała, P., “The method for the recovery of the apodization function of the fiber Bragg gratings on the basis of its spectra,” Przeglad Elektrotechniczny 86(10), 127-130 (2010).

[14] S. Cieszczyk, D. Harasim, and P. Kisała. A Novel Simple TFBG Spectrum Demodulation Method for RI Quantification. IEEE Photonics technology letters, vol. 29, no. 24, pp. 2264-2267, 2017.

[15] P. Kisała, Światłowodowe struktury periodyczne o pochylonej modulacji współczynnika załamania: właściwości i zastosowania. Monografie – Politechnika Lubelska, pp. 177- 214. Lublin 2019.

[16] P. Kisała,J. Mroczka,S. Cieszczyk, K. Skorupski, P. Panas. Twisted tilted fiber Bragg gratings: new structures and polarization properties. Vol. 43, No. 18 / 15 September 2018 / Optics Letters, pp. 4445-4448.

[17] Hill K. O., Meltz G., Fiber Bragg grating technology fundamentals and overview. Journal of Lightwave Technology 15(8), 1263-1276 (1997). doi: 10.1109/50.618320

[18] Shang R. B., Zhang W. G., Zhu W. B., Geng P. C., Ruan J., Gao S. C., Li X. N., Cao Q. X., Zeng X, Fabrication of twisted long period fiber gratings with high frequency CO2 laser pulses and its bend sensing. Journal of Optics 15, 1-6 (2013). doi: 10.1088/2040-8978/15/7/075402.

[19] Caucheteur Ch., Voisin V., Mégret P., Light Polarization-Assisted Sensing with Tilted Fiber Bragg ratings, The Open Optics Journal 7(1) (2013). doi: 10.2174/1874328501307010095

ПРИЛОЖЕНИЕ ДЛЯ МОНИТОРИНГА ДАННЫХ СЛОЖНЫХ СИСТЕМ, ПРЕДСТАВЛЕННЫХ МАТРИЦАМИ БОЛЬШОЙ РАЗМЕРНОСТИ

Калимолдаев М.Н., Клюева Е.Г., Яворский В.В., Есмагамбетова М.М.
e-mail: e.klyueva@kstu.kz
Институт информационных и вычислительных технологий КН МОН РК, Казахстан

Аннотация. *Статья посвящена вопросам разработки web-приложения для нахождения оптимальной формы разбиения элементов матриц между тремя абстрактными гетерогенными процессорами при выполнении операции их перемножения. Оптимальность форм определяется для двух классов алгоритмов: последовательной коммуникации с барьером и параллельной коммуникации с барьером. Для оценки коммуникационной трудоемкости алгоритмов используется модель Хокни. Исследования проводятся в рамках проекта AP05133699 «Исследование и разработка инновационно-телекоммуникационных технологий с использованием современных кибер-технических средств для интеллектуальной транспортной системы города».*

В настоящее время в связи с необходимостью мониторинга состояния сложных транспортных, урбанистических, информационных, телекоммуникационных, природно-экологических, техногенных и аналогичных систем предусматривающих описание в виде матриц корреспонденций, размещения и т.п. возникает необходимость применения высокопроизводительных вычислений (High Performance Computing), которые стремительно развиваются, чтобы охватить все новые архитектуры вычислительных систем и внедряемые алгоритмы.

Неоднородность вычислительных систем подразумевает под собой неоднородность вычислительной мощности или коммуникационного соединения и порождает новые подводные камни в создании и разработке алгоритмов. В настоящее время стоит задача адаптировать для использования в новых гетерогенных параллельных системах алгоритмы, разработанные для однородных параллельных систем. Однако возникают трудности с решением поставленной задачи, потому что алгоритмы, перенесенные из гомогенных систем, не всегда могут быть применимы к гетерогенным системам.

Матричные операции линейной алгебры находят широкое применение в научных областях и вычислениях и активно исследуются в области высокопроизводительных вычислений. Матричное умножение является одной из наиболее важных операций над матрицами. Оно широко используется в таких

областях, как теория сетей, решение линейных систем уравнений, преобразование систем координат, моделирование развития популяций и многих других.

Примером практического применения умножения матриц могут служить матрицы гипперсетей для транспортных систем городов. Если такие матрицы построены, то на их основе можно формировать безопасные схемы передвижения, составлять точное расписание движения общественного транспорта, определить загрузки элементов улично-дорожной сети, определить главные пассажирообразующие пункты, оценить количество перевозимых пассажиров по типам пассажиров, по видам транспорта, маршрутам и направлениям, а также оценить интенсивность пассажиропотоков между различными пунктами.

Разбиение данных является важным аспектом в решении задач линейной алгебры, который заключается в определении способа распределения элементов матрицы между доступными ресурсами. Разбиение данных позволяет оптимизировать такие показатели, как время выполнения задачи и энергоэффективность.

Целью разбиения данных является оптимальное распределение вычислительной нагрузки матриц среди доступных процессоров. Наиболее важным фактором, влияющим на долю назначаемых процессору элементов, является скорость, с которой данный процессор может выполнять такие основные операции, как сложение и умножение. При использовании разбиения данных все процессоры будут выполнять вычисления одновременно, и ни один процессор не будет простаивать.

Другим важным фактором в разбиении данных является его форма. Форма разбиения – это местоположение в матрице назначенной части каждого процессора. В случае умножения матриц, форма разбиения не оказывает влияние на стоимость вычислений, однако оказывает влияние на стоимость коммуникации. Процессору могут потребоваться данный, назначенные другому процессору, чтобы вычислить его назначенную часть.

Время коммуникации между процессорами играет большую роль и становится все более значимым, поскольку растет вычислительная эффективность высокопроизводительных систем. За последние годы был проведен ряд исследований в целях минимизации связи матричных вычислений в гетерогенных системах. Однако были исследовано только прямоугольные формы разбиений. В целях поиска оптимального решения проблемы разбиения данных, необходимо проводить исследование не только прямоугольных форм, но и иных вариаций.

Проблема оптимального матричного разбиения для задач линейной алгебры на p гетерогенных процессорах, как правило, сводится к геометрическому разбиению единичного квадрата на прямоугольники. В общем случае эта задача является NP-полной. Поэтому ограничения этой проблемы, учитывающие полиномиальные решения, должны быть изучены. На данный момент лучше всего было изучено ограничение, основанное на столбцах.

В большинстве случаем проблема оптимального распределения вычислений согласно одномерному расположению гетерогенных процессоров может быть сведена к математической проблеме разбиения множества или упорядоченного множества, даже если исходная задача связана с матрицами, она сводится к проблеме разбиения матрицы в одном измерении.

Для эффективного моделирования умножения матриц на трех абстрактных гетерогенных процессорах было сделано несколько допущений:

- в работе использованы квадратные исходные матрицы A, B и результирующая матрица C размером N × N элементов;
- элементы матрицы разделены между абстрактными процессорами P, R и S, пропорционально их вычислительным мощностям, которые определены отношением $P_r : R_r : S_r$, где P является самым мощным процессором и $S_r = 1$. $T = P_r + R_r + S_r$;
- процессоры объединены полносвязной топологией, с пропускными способностями сети передачи β_1 между процессорами P и S, β_2 между процессорами P и R, β_3 между процессорами S и R;
- в качестве форм-кандидатов рассмотрены формы Square Corner (SC), Rectangle Corner (RC), Square Rectangle (SR), Block Rectangle (BR), L-Rectangle (LR), Traditional 1D Rectangular (TR), выявленные Эшли ДеФлумер в работе [1] в результате применения техники перераспределения элементов матрицы между процессорами «Push» (рисунок 1).
- для оценки коммуникационной трудоемкости рассматриваемых алгоритмов использована модель Хокни.

Для определения оптимальности форм разбиения элементов матрицы в данном исследовании используются пять классов алгоритмов:

- последовательная коммуникация с барьером (Serial Communication with Barrier, SCB);
- параллельная коммуникация с барьером (Parallel Communication with Barrier, PCB);
- последовательная коммуникация с перекрытием (Serial Communication with Bulk Overlap, SCO);
- параллельная коммуникация с перекрытием (Parallel Communication with Bulk Overlap, PCO);
- параллельное перекрытие с чередованием (Parallel Interleaving Overlap, PIO) [1].

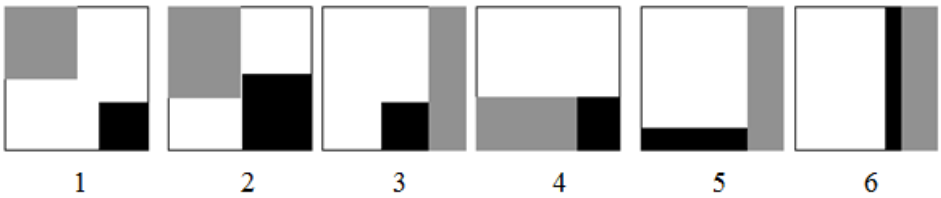


Рисунок 1 – Формы-кандидаты, определенные как потенциально оптимальные для трехпроцессорных систем:
1) Square Corner; 2) Rectangle Corner; 3) Square Rectangle;
4) Block Rectangle; 5) L-Rectangle; 6) Traditional 1D Rectangular

Первые два алгоритма SCB и PCB базируются на идее массовой коммуникации с барьером, при которой все данные отправляются процессорами до начала вычислений. Алгоритм их работы показаны на рисунке 2.

SCB Algorithm PCB Algorithm

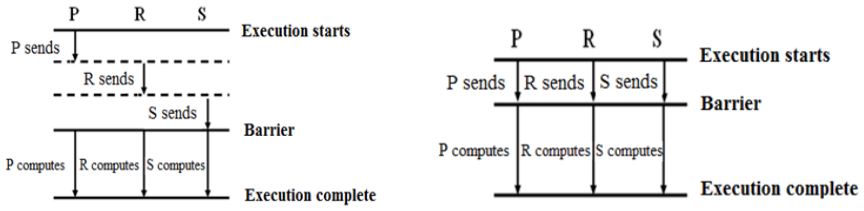


Рисунок 2 – Алгоритмы умножения матриц SCB и PCB

При выполнении алгоритма последовательной коммуникации с барьером все процессоры отправляют данные последовательно, друг за другом, и только после этого начинаются вычисления, которые выполняются параллельно.

Время выполнения рассчитывается по формуле (1):

$$T_{exe} = V\beta + \max(c_{p1}, c_{p2}, \dots, c_{p_p}) \quad (1)$$

где V– число коммуникаций;

c_{p_x}– время, необходимое для вычисления назначенной процессору X части матрицы.

В случае параллельной коммнуникации с барьером, все данные отправляются параллельно, и только когда они будут отправлены, вычисления начинают выполняться так же параллельно.

Время выполнения рассчитывается по формуле (2):

$$T_{exe} = \max\left(v_{p1}, v_{p2}, \dots, v_{p_p}\right)\beta + \max\left(c_{p1}, c_{p2}, \dots, c_{p_p}\right) \quad (2)$$

где V– число коммуникаций;

c_{p_x}– время, необходимое для вычисления назначенной процессору X части матрицы;

v_{p_x}– число элементов, которые должны быть отправлены процессором X.

Алгоритмы SCO, PCO и PIO предусматривают одновременное выполнение коммуникации и вычислений с целью минимизации затрачиваемого времени.

При использовании алгоритма SCO (рисунок 3) все процессоры отправляют данные последовательно, однако параллельно с установлением коммуникации процессор производит вычисления на основе уже имеющихся у него данных. Когда все данные будут отправлены, происходит вычисление оставшихся частей.

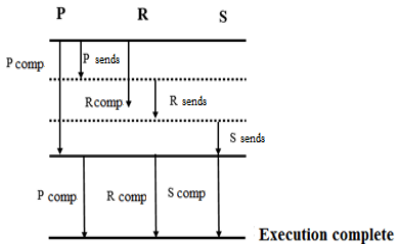


Рисунок 3 – Алгоритм умножения матриц SCO

Таким образом, время, затрачиваемое на выполнение операции, рассчитывается по формуле (3):

$$T_{exe} = \max\left(\max(V\beta, o_{p1}) + c_{p1},\ \max(V\beta, o_{p2}) + c_{p2}, \dots, \max\left(V\beta, o_{p_p}\right) + c_{p_p}\right) \quad (3)$$

где V– число коммуникаций;

o_{p_x}– время, необходимое процессору X для вычисления некоторых элементов, не предполагающих коммуникации с другими процессорами;

c_{p_x}– время, необходимое для вычисления назначенной процессору X оставшейся части матрицы.

Алгоритм PCO (рисунок 4) предполагает параллельное установление коммуникации между процессорами и одновременное с этим вычисление тех элементов матрицы C, для которых не существует необходимости в межпроцессорной связи. После этого выполняется вычисление оставшейся части матрицы.

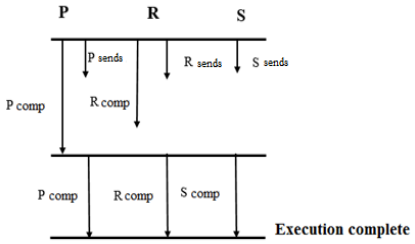


Рисунок 4 – Алгоритм умножения матриц PCO

Время выполнения определяется по формуле (4):

$$T_{exe} = \max\left(\max(T_{comm}, o_{p1}) + c_{p1},\ \max(T_{comm}, o_{p2}) + c_{p2}, \dots, \max\left(T_{comm}, o_{p_p}\right) + c_{p_p}\right) \quad (4)$$

где V– число коммуникаций;

T_{comm}– время, соответствующее формуле алгоритма параллельной коммуникации с барьером;

o_{p_x}– время, необходимое процессору X для вычисления некоторых элементов, не предполагающих коммуникации с другими процессорами;

c_{p_x}– время, необходимое для вычисления назначенной процессору X оставшейся части матрицы.

В случае алгоритма PIO на каждом шаге часть данных отправляется соответствующим процессором всем остальным процессорам, которым требуются эти элементы, и параллельно происходит вычисление матрицы с использованием данных, которые были отправлены.

Время выполнения определяется по формуле (5):

$$T_{exe} = Send\ k + (N - 1)\max\left(V_k\beta, \max\left(k_{p1},\ k_{p2}, \dots, k_{p_p}\right)\right) + Compute(k+1) \quad (5)$$

где V_k– число элементов, отправленных на шаге k;

k_x– время вычисления данных на шаге k для процессора X.

Для определения оптимальности форм для каждого из алгоритмов параллельного умножения матриц при разработке web-приложения были использованы математические модели, описанные в работах [2, 3].

Целью разработки web-приложения в рамках данного исследования является определение оптимальной формы разбиения элементов матриц при выполнении их перемножения, основываясь на исходных мощностях процессоров, латентности между ними и математических моделях определения оптимальной формы распределения ресурсов между тремя гетерогенными узлами с полносвязной топологией.

Функциональность разрабатываемого приложения включает в себя:

–расчет времени вычисления параллельного умножения матриц большой размерности на основе математических моделей для алгоритмов SCB, PCB, SCO, PCO, PIO в соответствии с введенными исходными параметрами вычислительной системы;

–отображение интерактивных графиков времени выполнения для каждого алгоритма по формам разбиения элементов матрицы SC, BR, SR, LR и RC.

Web-приложение представляет собой одностраничный сайт (рисунок 5). Для отображения графиков применяется функция Ajax, которая подгружает данные на веб-странице.

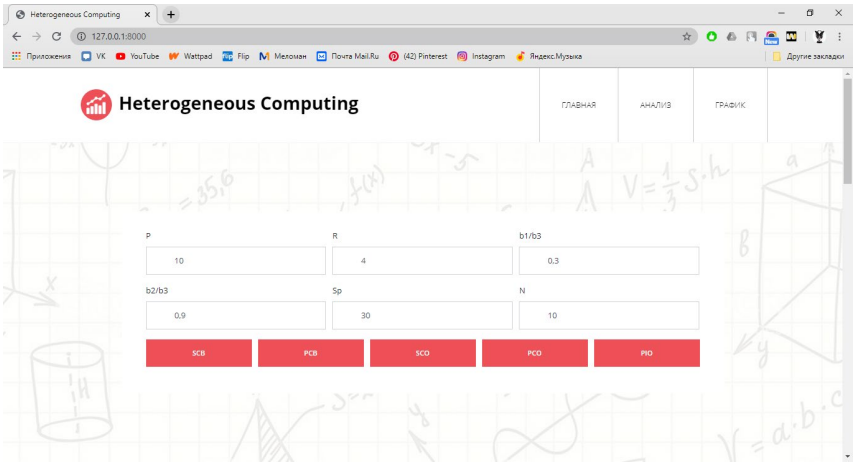


Рисунок 5 – Вид главной страницы web-приложения

Соответствующий алгоритмам SCB, PCB анализ для входных параметров P = 10, R = 4, β1/β3 =0,3, β2/β3 =0,9 показан на рисунке 6.

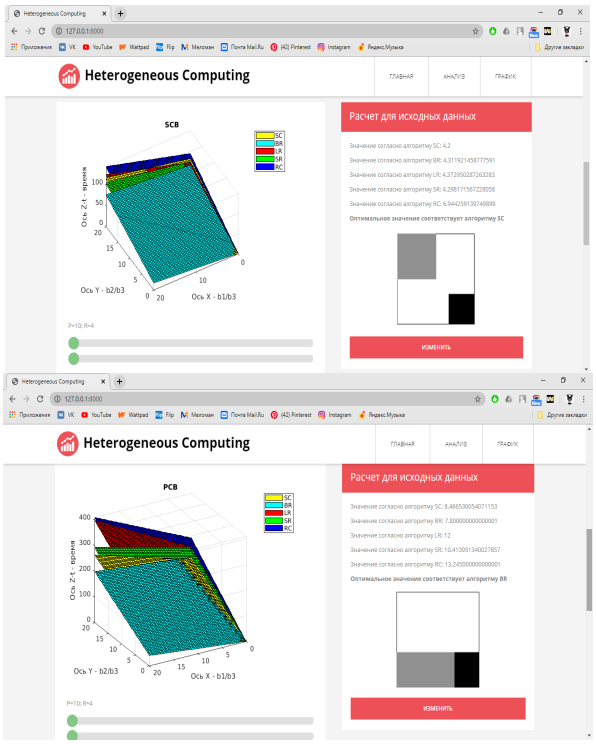


Рисунок 6 – Результаты работы web-приложения

На основании полученных результатов можно сделать заключение, что, как и в случае трехпроцессорных систем с одинаковой пропускной способностью сетей, соединяющих вычислительные элементы, формы разбиения данных Rectangle Corner и Traditional 1D Rectangular не могут быть оптимальными ни при одном наборе параметров.

В отличие от результатов, полученных в работе 1], форма L-Rectangle может быть оптимальной при мощностях процессоров P и R гораздо превышающих мощность процессора S и примерно равных друг другу в случае $\frac{\beta_1}{\beta_3} < 1$ для алгоритма SCB и $\frac{\beta_1}{\beta_3} = 0{,}1$ для алгоритма PCB. Однако в данных случаях нет смысла в использовании маломощного процессора S, и задача может быть решена на двух процессорах.

Форма Square Rectangle является оптимальной при малых значениях коэффициентов $\frac{\beta_1}{\beta_3}, \frac{\beta_2}{\beta_3}$ и мощностях процессоров P и R, значительно превышающих мощность процессора S. При таких исходных данных задача также может быть решена с использованием двух мощных процессоров.

В остальных случаях оптимальными в случае использования обоих алгоритмов в зависимости от значений коэффициентов $P_r, R_r, \frac{\beta_1}{\beta_3}, \frac{\beta_2}{\beta_3}$ являются формы Square Corner и Block Rectangle.

По итогам исследования было оформлено и получено свидетельство о внесении сведений в государственный реестр прав на объекты, охраняемые авторским правом «Web-приложение «Heterogeneous Computing»» № 9777 от 12.05.2020.

Литература

1. DeFlumere, A. // Optimal Partitioning for Parallel Matrix Computation on a Small Number of Abstract Heterogeneous Processors, – 2014. – P. 30-37.
2. Клюева Е.Г., Адамов А.А., Оспанова А.Е., Сницарь Л.Р., Кулбаева Л.Н. Исследование оптимальной формы разбиения данных для умножения матриц на трех гетерогенных процессорах с полносвязной топологией и различными пропускными способностями // Современные наукоемкие технологии. – 2019. – № 2 – С. 83-88.
3. Klyuyeva Y, Yavorskij, V.V., Adamov, A.A., Utepbergenov, I.T. Determination of the optimal shape of matrix elements partitioning on three abstract heterogeneous processors. Cogent Engineering Открытый доступ Volume 7, Issue 1, 1 January 2020, Номер статьи 1769948. https://doi.org/10.1080/23311916.2020.1769948.

УАҚЫТЫ КЕШІККЕН ЖОҒАРЫ РЕТТІ АНЫҚТАЛМАҒАН СЫЗЫҚТЫ ЕМЕС ЖҮЙЕЛЕР ҮШІН БЕЛГІЛЕНГЕН ӨТПЕЛІ ӨНІМДІЛІГІ БАР КЕҢ АУҚЫМДЫ ПРАКТИКАЛЫҚ ІЗГЕ ТҮСІРУ МӘСЕЛЕСІ

Ахметкалиевва А.С. [1], Мамырбаев О.Ж.[2], Алимхан К[1]
e-mail: almira_vko@mail.ru; morkenj@mail.ru; keylan@live.jp
[1]*Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Қазақстан*
[2]*Ақпараттық және есептеуіш технологиялар институты, Қазақстан*

Аннотация: *Бұл жұмыста біз уақыты кешіккен жоғары ретті анықталмаған сызықты емес жүйелер үшін белгіленген өтпелі өнімділігі бар кең ауқымды практикалық ізге түсіру мәселесін қарастырамыз. Осы ізге түсірудің екі тамаша ерекшелігі бар. Оның бірі ізге түсіру қателігі белгіленген шұңқыр шегінде дамитынына кепілдік береді. Екіншісі - жүйелердегі ауыр сызықты еместік пен елеулі белгісіздік, әсіресе белгісіз басқару бағыттарына жол беру.Бұл үшін белгіленген өтпелі сипаттаманы қамтамасыз ету үшін уақыт айнымалы күшейткіш енгізіледі. Сонымен қатар мұндай уақыт айнымалы күшейткіш жүйедегі және тірек сигналындағы елеулі белгісіздікті, сондай-ақ белгісіз басқару бағыттарын Нуссбауым жалпыланған функциясын біріктіру арқылы орнын толтырады. Содан кейін күй кері байланысы арқылы уақыт айнымалы контроллер құру нәтижесінде алынған тұйық жүйенің шешімдері кең ауқымды шектелген және ізге түсіру қателігі белгіленген шұңқыр шегінде дамиды.*

Кіріспе және есептің қойылымы

Соңғы онжылдықтар ішінде практикалық ізге түсіруге көп көңіл бөлінді, өйткені ол көптеген практикалық қолдануға сәйкес келеді және асимптотикалық ізге түсірумен салыстырғанда жүйелер мен тірек сигналдарына айтарлықтай жеңіл шектеулерді қажет етеді. Мысалы, [1-3] анықталмаған сызықты емес жүйелер үшін шығыс кері байланысы арқылы практикалық ізге түсіруді қарастырды, ал [4-9] жоғары ретті сызықты емес жүйелер үшін күй кері байланысы арқылы практикалық

ізге түсіру мәселесін зерттеді. Алайда, қолданыстағы жұмыстардың көпшілігінде өтпелі ізге түсіру өнімділігі есепке алынбады. Салыстырмалы түрде белгіленген өтпелі өнімділігі бар ізге түсіру практикалық қолдануға көбірек қызығушылық тудырады, бірақ басқарудың күрделі мақсатына байланысты үлкен қиындық туғызады. Осы уақытқа дейін жұмыстардың тек бірнешеуі осындай бағытқа арналған (мысалы, [10-13]), олардың бәрі әлі де ондағы жүйелер үшін белгісіздікті немесе сызықты еместікке кейбір елеулі шектеулерді қажет етеді. Бұл жұмыста біз келесі түрдегі уақыты кешіккен жоғары ретті анықталмаған сызықты емес жүйелер үшін белгіленген өтпелі өнімділігі бар кең ауқымды практикалық ізге түсіру мәселесін қарастырамыз:

$$\begin{cases} \dot{x}_i = g_i(t,x)x_{i+1}^{p_i} + f_i(t,x,x(t-d)), \ i=1,\dots,n-1 \\ \dot{x}_n = g_n(t,x)u^{p_n} + f_n(t,x,x(t-d)), \\ y = x_1 \end{cases} \tag{1}$$

Мұндағы $x=[x_1,\dots,x_n]^T \in R^n$ бастапқы мәні $x(t_0)=x_0$ болатын жүйенің күй векторы, $u \in R$ және $y \in R$ жүйенің сәйкесінше кірісі мен шығысы, $p_i \in R_{odd}^{\geq 1} = \{q \in R \mid q \geq 1$ және q бүтін сандардың қатынасы $\}$, $i=1,\dots,n$ жүйенің жоғары реттілігін білдіреді және $g_i : R_{\geq t_0} \times R^n \times R,\ i=1,\dots,n$ және $f_i : R_{\geq t_0} \times R^n \times R,\ i=1,\dots,n$ белгісіз үздіксіз функциялар, олар сәйкесінше жүйенің басқару коэффициенттері және сызықты еместігі деп аталады, және $g_i(\cdot)$ белгілері жүйенің басқару бағыттары деп аталады, ал $d \geq 0$ уақыт кешігу параметрі.

Біз (1) жүйесіне қатысты келесі болжамдар жасаймыз және жүйенің y шығысы арқылы y_r тірек сигналымен ізге түсіреміз:

1-болжам. $g_i(t,x)$, $i=1,\dots,n$ белгілері белгісіз. Сонымен қатар, θ_{g1},θ_{g2} - белгісіз оң тұрақтылары және $\underline{g}_i(x_{[i]}), \overline{g}_i(x_{[i]}), i=1,\dots,n$ - белгісіз тегіс оң функциялары бар болады, ол

$$\theta_{g1}\underline{g}_i(x_{[i]}) \leq |g_i(t,x)| \leq \theta_{g2}\overline{g}_i(x_{[i]}), i=1,\dots,n.$$

2-болжам. $\overline{f}_i(x_{[i]}), i=1,\dots,n$ белгілі тегіс теріс функциялары, $q_i \in [0,p_i), i=1,\dots,n$ белгілі тұрақтылары және θ_f белгісіз оң тұрақтысы бар болады, ол

$$|f_i(t,x,u)| \leq \theta_f\left(1+|x_{i+1}|^{q_i}\right)\overline{f}_i(x_{[i]}), i=1,\dots,n,$$ мұндағы $x_{n+1}=u$.

3-болжам. y_r тірек сигналы $W^{1,\infty}(R_{\geq t_0},R)$ тиісті болады. Сонымен қатар, M белгісіз оң тұрақтысы бар болады, ол

$$ess\sup_{t\geq t_0}\left(|y_r(t)|+|\dot{y}_r(t)|\right) \leq M.$$

Нақтырақ айтсақ, осы жұмыстың басқару мақсаты тұйық жүйенің барлық шешімдері $[t_0,+\infty)$ аралығында кең ауқымды шектелген және $e(t)=y(t)-y_r(t)$ ізге түсіру қателігі келесі шұңқырдың төңірегінде дамитындай [10-11] сияқты 1-3-

болжамдарға сәйкес (1) жүйе үшін күй кері байланысы арқылы уақыт айнымалы контроллер құру [7] сияқты адаптивті емес:

$$\mathsf{F}_{\psi,\lambda} := \left\{ (t,e) \in R_{\geq t_0} \times R \mid \psi_\lambda(t)|e| < 1 \right\},$$

мұндағы λ ізге түсірудің шекті дәлдігін білдіретін белгіленген оң тұрақты және

$$\psi_\lambda \in S := \left\{ \psi \in W^{1,\infty}\left(R_{\geq t_0}, R\right) \mid \psi(t_0) \right\} = 0,$$

$$\psi(t) > 0 \forall t > t_0, \liminf_{t \to +\infty} \psi(t) > \frac{2}{\lambda}.$$

Бұл жұмыс (1) жүйедегі және y_r тірек сигналындағы елеулі белгісіздерді эффективті өңдеу үшін уақыт айнымалы схема құруға және (1) жүйе үшін белгіленген өтпелі өнімділігі бар кең ауқымды практикалық ізге түсіруге арналған. [3], [10-11] негізінде белгіленген өтпелі өнімді ізге түсіру қателігін қамтамасыз ету үшін уақыт айнымалы күшейткіш енгізіледі. Сонымен қатар мұндай уақыт айнымалы күшейткіш жүйедегі және тірек сигналындағы елеулі белгісіздікті, сондай-ақ белгісіз басқару бағыттарын Нуссбауым жалпыланған функциясын біріктіру арқылы орнын толтырады. Осыған сүйене отырып, [8] ұсынылған координаталық түрлендірудің арқасында уақыт айнымалы күй кері байланыс контроллері құрылады, осылайша тұйық жүйелердің шешімдері кең ауқымды шектелген және ізге түсіру қателігі белгіленген өнімділік шұңқырында дамиды.

Ізге түсіруді басқару құрылымы

Бірнеше пайдалы теңсіздіктерді жинайтын келесі ұсынысты береміз.

1-ұсыныс. $\theta > 0$ белгісіз тұрақты және $\phi_i\left(x_{[i]}\right) \geq 0, i = 1,\ldots,n$ белгілі тегіс функциялары бар болады, ол

$$\begin{cases} \left|f_i(t,x,u)\right| \leq \frac{1}{4}\left|g_i(t,x)\left(x_{i+1}^{p_i} + x_{i+1}\right)\right| + \theta\phi_i\left(x_{[i]}\right), \ i = 1,\ldots,n-1, \\ \left|f_n(t,x,u)\right| \leq \frac{1}{4}\left|g_n(t,x)u^{p_n}\right| + \theta\phi_n\left(x_{[n]}\right). \end{cases} \tag{2}$$

Оның үстіне, мұнда кез келген $i = 1,\ldots,n-1$ үшін

$$\begin{cases} \left|\dot{x}_i\right| \leq \frac{5}{4}\theta_{g2}\overline{g}_i\left(x_{[i]}\right)\left|x_{i+1}^{p_i}\right| + \theta\phi_i\left(x_{[i]}\right), \\ \left|g_i(t,x)x_{i+1}\right| \leq \frac{1}{2}\left|g_i(t,x)\left(x_{i+1}^{p_i} + x_{i+1}\right)\right| + \xi^2\overline{g}_i^{\,2}\left(x_{[i]}\right) + \frac{\left(p_i - 1\right)^2\theta_{g2}^2}{4p_i^2}. \end{cases} \tag{3}$$

Дәлелдеуі. [7-8] де көрсетілген. .

Әрі қарай күй кері байланыс ізге түсіру контроллерін құру процедурасын орнату арқылы нақты басқару заңын таңдаймыз

$$u=\left(\xi_n N\left(k_n\right)\rho_n\left(x,k_{[n-1]},y_r\right)\Big/\underline{g}_n\left(x\right)\right)^{1/p_n}, \tag{4}$$

мұнда $k_n := k_n\left(t,\xi_n\right)=1\Big/\left(1-\left(\varphi_n\left(t\right)\xi_n\right)^2\right)$, $\varphi_n\in S_0$. Онда $t\ge t_0$ барлығына дерлік мынаған жетеміз

$$\dot{V}_n\le\left(p_{n-1}x_n^{p_{n-1}-1}+1\right)\left(\hat{g}_n\left(t,x\right)N\left(k_n\right)\Big/\underline{g}_n\left(x_{[n]}\right)+1\right)\xi_n^2\rho_n\left(x_{[n]},k_{[n-1]},y_r\right)+\theta_n.$$

1-теорема. (1) жүйе үшін 1-3-болжамдар мен (4) контроллер кез келген $x_0\in R^n$ бастапқы мәні үшін тұйық жүйенің барлық сигналдары (яғни жүйенің x күйі, u кірісі және k_i күшейткіші) $\left[t_0,+\infty\right)$ аралығында шектеулі болуын қамтамасыз етеді және сонымен қатар $\sup_{t\ge t_0}\varphi_\lambda\left(t\right)\left|y\left(t\right)-y_r\left(t\right)\right|<1$.

Дәлелдеуі. Кез келген $x_0\in R^n$ бастапқы мәні үшін $\left[t_0,t_e\right)$ аралығында анықталған тұйық жүйенің $x\left(t\right)$ шешімі бар болады, ол кез келген $i=1,\ldots,n$ үшін

$$\varphi_i\left(t\right)\left|\xi_i\left(t\right)\right|<1,\ \forall t\in\left[t_0,t_e\right), \tag{5}$$

мұндағы t_e жоғарыда көрсетілгендей $x\left(t\right)$ шешімінің максималды бар болу уақыты және төменде көрсетілгендей $t_e=+\infty$.

Алдымен $\left[t_0,t_e\right)$ аралығында $\xi_i\left(t\right)$ шектеулі болатынын көрсетеміз. Шын мәнінде, $t_e=+\infty$ немесе $t_e<+\infty$ болғанына қарамастан, кез келген $i=1,\ldots,n$ үшін $\varphi_i\left(t\right)>e_i,\ \forall t\in\left[T_i,t_e\right)$ кейбір $e_i>0$ және $T_i\in\left(t_0,t_e\right)$ үшін $\varphi_i\left(t\right)>0,\ \forall t>t_0$ және $\liminf_{t\to+\infty}\varphi_i\left(t\right)>0$. Онда кез келген $i=1,\ldots,n$ үшін (5)-мен бірге $\left|\xi_i\left(t\right)\right|<1\big/\varphi_i\left(t\right)<1/e,\ \forall t\in\left[T_i,t_e\right)$ болатынын береді. Осылайша $\xi_i\left(t\right)$ шектеулігі шығады.

Әрі қарай индукция бойынша $\left[t_0,t_e\right)$ аралығында $x_i\left(t\right)$ мен $k_i\left(t\right)$ шектеулі болатынын дәлелдейміз. $\xi_1\left(t\right)$ мен $y_r\left(t\right)$ шектеулілігінен $\left[t_0,t_e\right)$ аралығында $x_1\left(t\right)=\xi_1\left(t\right)+y_r\left(t\right)$ шектеулі болады. Бұдан (5) арқылы $\left[t_0,t_e\right)$ аралығында $k_1\left(t\right)$ шектеулі. Айталық әрбір $i=1,\ldots,l$ үшін $\left[t_0,t_e\right)$ аралығында $x_i\left(t\right)$ мен $k_i\left(t\right)$ кез келген $l=1,\ldots,n-1$ үшін шектеулі болсын. Онда $\xi_{l+1}\left(t\right)$ мен $y_r\left(t\right)$ шектеулілігі және $x_{l+1}^{p_l}+x_{l+1}=\xi_{l+1}+\alpha_l^{p_l}\left(x_{[l]},k_{[l]},y_r\right)$ ескере отырып, $\left[t_0,t_e\right)$ аралығында $x_{l+1}\left(t\right)$ шектеулі болады. Бұдан $x_i\left(t\right)$ мен $k_i\left(t\right)$ шектеулілігі шығады.

Сонымен қатар u анықтамасынан $\left[t_0,t_e\right)$ аралығында $u\left(x_{[n]}\left(t\right),k_{[n]}\left(t\right),y_r\left(t\right)\right)$ шектеулі болады. Және $k_i\left(t\right)$ шектеулілігінен $e>1$ бар болады, ол

$$\frac{1}{1-\left(\varphi_i\left(t\right)\xi_i\left(t\right)\right)^2}=k_i\left(t\right)\le e,\ \forall t\in\left[t_0,t_e\right),$$

яғни $\varphi_i\left(t\right)\left|\xi_i\left(t\right)\right|\le\sqrt{1-1/e},\quad\forall t\in\left[t_0,t_e\right)$.

Бұдан барлық $t\in\left[t_0,+\infty\right)$ үшін $t_e=+\infty$ орындалады,

$$\psi_\lambda(t)\left|y(t)-y_r(t)\right| = \varphi_1(t)\left|\xi_1(t)\right| \le \sqrt{1-1/e}\,.$$

Дәлелдеуі осымен аяқталады. □

Қорытынды

Бұл жұмыста белгісіз басқару бағыттары бар жоғары ретті анықталмаған сызықты емес жүйелер үшін күй кері байланысы арқылы шұңқыр басқару схемасы жасалынды. Бір жағынан, [7-8] де көрсетілген Нуссбаумның жалпыланған функцияларымен үйлесе Нуссбаум күшейткішіне негізделген адаптивті басқаруға қарағанда басқару коэффициенттері туралы неғұрлым өрескел ақпаратты талап ететін басқарудың белгісіз бағыттары үшін уақыт айнымалы өтемақы стратегиясы ұсынылады.

Жұмыс AP05131207 «Терең нейрондық желілерді пайдаланатын мультитілдік автоматты сөйлеуді тану технологиясын құру» жобасы негізінде дайындалды.

Әдебиеттер

1. Q. Gong and C. J. Qian. Global practical tracking of a class of nonlinear systems by output feedback./ Automatica, 43(1): 184–189, 2007.
2. X. H. Yan and Y. G. Liu. Global practical tracking by output-feedback for nonlinear systems with unknown growth rate./ Science China Information Sciences, 54(10): 2079–2090, 2011.
3. A. BenAbdallah and T. Khalifa and M. Mabrouk. Adaptive practical output tracking control for a class of uncertain nonlinear systems./ International Journal of Systems Science, 2013, DOI: 10.1080/00207721.2013.822606.
4. C. J. Qian and W. Lin. Practical output tracking of nonlinear systems with uncontrollable unstable linearization./ IEEE Transactionson Automatic Control, 47(1): 21–36, 2002.
5. W. Lin and R. Pongvuthithum. Adaptive output tracking of inherently nonlinear systems with nonlinear parameterization. /IEEE Transactionson Automatic Control, 48(10): 1737–1749, 2003.
6. X. H. Yan and Y. G. Liu. Global practical tracking for high-order uncertain nonlinear systems with unknown control directions. /SIAM Journalon Control and Optimization, 48(7): 4453–4473, 2010.
7. X. H. Yan and Y. G. Liu. The further resulton global practical tracking for high-order uncertain nonlinear systems./ Journal of Systems Science and Complexity, 25(2): 227–237, 2012.
8. Z. Y. Sun and Y. G. Liu. Adaptive practical output tracking control for high-order nonlinear uncertain systems. /Acta Automatica Sinica, 34(8): 984–989, 2008.
9. A. Ilchmann, E. P. Ryanand C. J. Sangwin. Tracking with prescribed transient behaviour, /ESAIM: Control, Optimisation and Calculus of Variations, 7: 471-493, 2002.
10. A. Ilchmann, E. P. Ryanand P. Townsend. Tracking control with prescribed transient behaviour for systems of known relative degree, /Systems & Control Letters, 55(5): 396–406, 2006.
11. C. P. Bechlioulis and G. A. Rovithakis. A low-complexity global approximation-free control scheme with prescribed performance for unknown pure feedback systems./ Automatica, 50(4): 1217–1226, 2014.

12. D. E. Miller and E. J. Davison. Anadaptive controller which provides an arbitrarily good transientand steadystate response, /IEEE Transactionson Automatic Control, 36(1): 68–81, 1991.
13. P. Hartman. Ordinary differential equations. /SIAM, Philadelphia, 2002

АЛГОРИТМ ФОРМИРОВАНИЯ ПРОГРАММ ПРЕДУПРЕЖДЕНИЯ ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЙ

Есмагамбетова М.М., Бобров А.К., Утепбергенов И.Т.,
Клюева Е.Г., Ахмедиярова А.Т
e-mail: e.klyueva@kstu.kz
Институт информационных и вычислительных технологий КН МОН РК, Казахстан

Аннотация. *Статья посвящена вопросам предупреждения аварийности производственных участков повышения устойчивости и гибкости производственной систем. В рамках работы формируется алгоритм выбора совокупности программ предупреждения аварий с заинтересованными предприятиями. Были разработаны варианты формирования совокупности программ для ситуаций, когда предприятия консорциума вкладывают равные по величине средства и когда сумма средств различна. Исследования проводятся в рамках проекта AP05133699 «Исследование и разработка инновационно-телекоммуникационных технологий с использованием современных кибер-технических средств для интеллектуальной транспортной системы города».*

Базой для выбора стратегических решений по предупреждению аварийных ситуаций в масштабе горно-геологического района являются разработка и реализация систем целевых комплексных программ, направленных на снижение возможных негативных последствий и потерь от них [1]. Типичная для сегодняшней ситуации ограниченность ресурсного обеспечения и финансовых средств для реализации программ безопасности, как правило, вызывает неоднозначные оценки в процессе их утверждения.

Это модели и методы группового выбора программ обеспечения безопасности и предупреждения чрезвычайных ситуаций в крупном горно-геологическом районе, который представляет собой консорциум предприятий, имеющих частично согласованные экономические интересы в рамках единого рыночного сообщества.

Таким образом необходимо определить алгоритмы формирования совокупности программ предупреждения аварийных ситуаций в горно-геологическом районе с учетом интересов всех находящихся в нем предприятий.

Пусть имеется множество программ $P = \{p_i, i = \overline{1,.I}\}$, направленных на обеспечение безопасности и предупреждение аварийных ситуаций по всему району. При этом считать, что общая программа представляет совокупность программ предприятий, интересы каждого из них различны. Проявляются интересы предприятий $\Pi = \{\pi_j, j = \overline{1,.J}\}$ через финансирование той или иной программы. Обозначим затраты на реализацию каждой из предлагаемых программ как $s_i, i = \overline{1,.I}$. В пределах определенного финансирования b_i предприятие вкладывает

определенную сумму средств c_{ij} на реализацию интересующей его i-й программы [2].

Допустим также, что есть определенное ограничение на реализацию всех программ, которое устанавливается консорциумом предприятий. Обозначим его как R.

Задача заключается в том, чтобы сформировать такую совокупность программ, которая бы максимально учитывала интересы всех сторон.

Для формализованной постановки задачи введем переменную:

$$x_i = \begin{cases} 1 \ - \ \textit{если } i-\textit{я программа входит в набор} \\ \quad \textit{для рассмотрения или обсуждения} \\ 0 \ - \ \textit{если нет.} \end{cases}$$

Опишем интересы предприятий. Пусть:

$$y_i = \begin{cases} 1 \ - \ \textit{если } s_i x_i - \sum_{j=1}^{J} c_{ij} x_i \le 0, \\ 0 \ - \ \textit{если } s_i x_i - \sum_{j=1}^{J} c_{ij} x_i > 0. \end{cases} \tag{1}$$

Другими словами y_i= 1 означает, что i-я программа обеспечена средствами и, наоборот, y_i= 0 средств для реализации i-й программы нет.

Очевидно, что суммарный дефицит по всем программам, отобранным для обсуждения, составит:

$$f(x_i) = \sum_{i=1}^{I} s_i x_i - \sum_{j=1}^{J} c_{ij} x_i \tag{2}$$

при условии, что $a_i = s_i x_i - \sum_{j=1}^{J} c_{ij} x_i > 0$.

Тогда функция дефицита средств:

$$f(x_i) = \sum_{i=1}^{I} a_i x_i \tag{3}$$

y_i - функция обеспеченности программ финансовыми средствами.

Критерии (1) и (3) согласованы и показывают интересы консорциума предприятий района в смысле максимизации обеспеченности средствами и минимизации дефицита финансирования программ [3]:

$$\max \sum_{i=1}^{I} y_i \ \text{ и } \ \min \sum_{i=1}^{I} a_i x_i$$

Определим матрицу, показывающую участие отдельных предприятий в финансировании программ:

$$A = \left\| a_{ij} \right\|, i = \overline{1, I}, j = \overline{1, J} \tag{4}$$

где:

$$a_{ij} = \begin{cases} 1 \ - \ \textit{если } j-\textit{е предприятие} \\ \quad \textit{финансирует } i-\textit{ю программу}; \\ 0 \ - \ \textit{если нет.} \end{cases} \tag{5}$$

Это означает, что:

$$a_{ij} = \begin{cases} 1 \ - \ \textit{если } c_{ij} > 0 \\ 0 \ - \ \textit{если } c_{ij} = 0. \end{cases}$$

Тогда функция:

$$\varphi_i(x) = \sum_{i=1}^{I} a_{ij} y_i \tag{6}$$

позволяет определить интересы предприятия путем выражения количество финансируемых им программ. Предприятие, вкладывая финансовые средства, стремится обеспечить $\max \sum_{i=1}^{I} a_{ij} y_i$.

Как видно из сравнения (1) и (6), целевые функции согласованы, т. е. интересы консорциума согласованы с интересами каждого предприятия. Дальнейшее усиление функции (6) состоит в обеспечении:

$$\max_j \sum_{j=1}^{J} \max \sum_{i=1}^{I} a_{ij} y_i \tag{7}$$

что выгодно и для каждого предприятия в отдельности, и для консорциума в целом. Тогда задача определения совокупности программ формулируется следующим образом:

$$\min \sum_{i=1}^{I} a_i x_i \tag{8}$$

при ограничении финансирования каждого предприятия:

$$\sum_{i=1}^{I} c_{ij} x_i \le b_j, j = \overline{1, J} \tag{9}$$

на централизованные средства для реализации всех программ, выделяемых для обсуждения (возможно, дотации от представителей власти):

$$\sum_{i=1}^{I} s_{ij} x_i \le R \tag{10}$$

При постановке задачи считалось, что все программы обладают одинаковым приоритетом, что характерно для крупных аварий. При этом могут также быть учтены и интересы контролирующих органов (со стороны руководства города, области), которые могут участвовать как представители *П₀*, наделенные одинаковыми правами с предприятиями *П₀*, $j = \overline{1, J}$.

Вместе с тем у представителей власти могут быть приоритетные программы, реализация которых необходима в масштабе всей страны или региона. Тогда консорциум предприятий, вкладывая свои финансовые средства B_0, может улучшить полученное решение путем предоставления средств приоритетным программ с последующим отбором их для утверждения на уровне города, области, страны [4].

Заметим, что консорциум предприятий горно-геологического района заинтересован в том, чтобы итоговая совокупность программ охватывала максимально возможное количество объектов, подтвержденных аварийным ситуациям. С другой стороны, также следует отметить заинтересованность в минимизации функции дефицита, так как в условиях их ограниченности сумма дотации предприятий должна быть минимальной для эффективного покрытия дефицита. Интересы отдельных предприятий выражаются в увеличении количества программ, в которые они вложили средства, и в их полном финансовом обеспечении.

Задачу, которая учитывает все интересы, можно сформулировать несколькими критериями:

$$\sum_{i=1}^{I} x_i \to \max, \tag{11}$$

$$\sum_{i=1}^{I} a_i x_i \to \min, \tag{12}$$

$$\sum_{i=1}^{I} y_i \to \max, \tag{13}$$

Анализ структуры и особенностей задачи позволяет предложить следующий алгоритм.

1. Ввод исходных данных: матрицы затрат, перечень программ и ограничения финансирования.

$$C = \left\| c_{ij} \right\|, i = \overline{1, I}; j = \overline{1, J}; S_i = \overline{1, i}; b_j, j = \overline{1, j}.$$

Переход к 2.

2. Разбиваем множество программ P на подмножества: $p^1 = \{p_i : a_i \le 0\}$ и $p^2 = \{p_i : a_i \le 0\}$. Переход к 3.

3. Если $p^1 = 0$, то переход к 7. В противном случае - к 4.

4. Для всех элементов $p_i \in p^1$ присваиваем $x_i = 1$. Вычисляем значение $\sum_{i=1}^{I} y_i$ по $\forall p_i \in p^1$ Переход к 5.

5. Проверяем ограничение. Если оно удовлетворено, переход к 5. В противном случае - к 6.

6. В множестве p^1 со значением $\min_i s_i$ последовательно исключаются программы из множества P^1 до тех пор, пока не будет выполнено условие $R - \sum_{p_i \in p^1} \min_i s_i \le 0.$. Переход к 8.

7. Располагаем элементы множества P^2 в порядке возрастания значений α_i. Присваиваем $x_i = 1$ первому элементу множества P^2. Проверяем ограничение. Если оно удовлетворено, присваиваем $x_i = 1$ очередному элементу.

В противном случае - переход к 8.

8. Вывод решения задачи $X = \{x_i : x_i = 1\}$.

Вывод значений функций $\sum_{i=1}^{I} y_i$ и $\sum_{i=1}^{I} a_i x_i$.

Контроль ограничения по финансам находится на контроле самих предприятий.

Рассмотрим решение задачи. В решение задачи в этом случае войдут те программы $P^1 = \{p_i : a_i \le 0\}$, которые финансируются. В пределах множества P^1 значения функций (11) и (13) совпадают.

Функция (12) имеет минимальное значение, равное нулю. Если при этом ограничение (10) удовлетворено, можно улучшить значение функции (11) за счет ухудшения значений функции (12). Значение функции (13) остается постоянным. Таким образом, решение задачи будет основано на компромиссе между значениями функций (11) и (12), а также ограничением вида (10).

Таким образом, для поиска оптимального решения задачи может использоваться приведенный выше алгоритм решения.

В указанных постановках считалось, что величины вкладываемых средств c_{ij} фиксированы, т.е. заранее известно, какую долю вкладывает каждое предприятие в интересующие его программы.

	π_1	π_2	π_3	π_4	π_5	π_6	σ_i	S_i
p_1	2	1	0	1	1	0	5	7
p_2	0	2	1	0	0	1	4	5
p_3	1	0	0	3	0	1	5	4
p_4	4	0	1	2	1	0	8	8
p_5	0	2	1	1	0	1	5	9
p_6	0	2	1	1	0	2	0	6
σ_i*	8	5	5	7	4	3	31	39
b_i	8	5	6	7	4	3	33	

Рисунок 1 - Матрица вкладов $C = \|c_{ij}\|$

	π_1	π_2	π_3	π_4	π_5	π_6	Δ_i
p_1	1	1	0	1	1	0	4
p_2	0	1	1	0	0	1	3
p_3	1	0	0	1	0	1	3
p_4	1	0	1	1	1	0	4
p_5	0	1	1	1	0	1	4
p_6	1	0	1	0	1	0	3
σ_i*	4	3	4	4	3	3	23

Рисунок 2 -Матрица вкладов $A = \|a_{ij}\|$

Рассмотрим постановку и решение задачи в условиях, когда размеры вкладываемых средств могут варьироваться с тем, чтобы прийти к консенсусу, т.е. к взаимоприемлемому решению, с которым согласны все предприятия (либо их значительное большинство).

Предположим, что при тех же исходных данных предприятия для улучшения финансирования программ могут менять величину вложенных средств в пределах выделенных средств по интересующим их программам (задается матрицей A).

Необходимо так распределить средства по программам и объединить последние в набор (комплект), чтобы обеспечить финансированием как можно больше программ, интересующих каждое предприятие [5].

Введем для этого случая следующие переменные:

$$x_i = \begin{cases} 1 \ - \ \textit{если } i - \textit{я программа входит в набор} \\ \quad \textit{для рассмотрения или обсуждения} \\ 0 \ - \ \textit{если нет.} \end{cases} \tag{14}$$

z_{ij} – сумма финансирования j-го предприятия, выделенная на реализацию i-й программы.

Тогда i-я программа будет обеспечена финансированием при выполнении следующего условия.

$$y_i = \begin{cases} 1 \ - \ \textit{если } s_i x_i - \sum_{j=1}^{J} z_{ij} x_i \le 0, \\ 0 \ - \ \textit{если } s_i x_i - \sum_{j=1}^{J} z_{ij} x_i > 0. \end{cases} \tag{15}$$

При этом каждое предприятие заинтересовано в увеличении своей выгоды, целевой функции вида $\sum_{i=1}^{I} a_{ij} y_i$. Каждое предприятие не возражает против суммарного выигрыша для всех остальных. Задача формулируется следующим образом:

$$\max_j \sum_{j=1}^{J} \max_i \sum_{i=1}^{I} a_{ij} y_i \tag{16}$$

при ограничениях консорциума на общие бюджетные средства предприятий:

$$\sum_{i=1}^{I} a_{ij} z_{ij} x_{ij} \le b_j, i = \overline{1, I} \tag{17}$$

Целевая функция нацелена на обеспечение максимальной выгоды каждого предприятия и всех вместе. При этом стратегия каждого предприятия по финансированию программ должна быть «дозированной», т. е. оно намерен финансировать все программы, в которых заинтересован, вкладывая имеющиеся средства по частям [6]. Следовательно, каждое предприятие стремится обеспечить

ресурсами интересующие его программы (без приоритетов) в равных долях согласно выражению:

$$z_{ij} = \left]\frac{b_j}{\sum a_{ij}}\right[\tag{18}$$

При этом должно быть удовлетворено следующее условие:

$$\sum_j z_{ij} > s_i \tag{19}$$

Если данное условие выполнено, то веса дуг принимают вычисленные значения. В противном случае значения весов дуг увеличиваются с минимальных на максимальные.

После установления значений z_{ij} программа p_1 включается в набор (т. е. x_1= 1), и для каждого предприятия пересчитываются значения:

$$\Delta_j^{*T} = \sum_{i=1}^{i} a_{ij} - 1;\ \ b_j^T = b_j - z_{ij},$$

где Δ_j^{*T} и b_j^T - текущие значения в процессе работы алгоритма.

Затем выбирается следующая программа и все вышеуказанные операции повторяются. Условием окончания работы алгоритма будет:

$$b_j=0 \text{ для } \forall j = \overline{1, J}.$$

Для решения задачи (16), (17) на основе проведенного анализа предлагается такой алгоритм.

1. Ввести исходные данные матрицы:

$$A = \left\| b_{ij} \right\|,\ \ i = \overline{1, I},\ \ \ j = \overline{1, J},\ \ b_j.$$

Переход к 2.

2. Упорядочить множество программ P в матрице A в порядке убывания значений Δ_i. Переход к 3.

3. Упорядочить множество предприятий П в матрице A в порядке убывания значений Δ_j^*. Переход к 4.

4. Выбрать *i-ю* программу из упорядоченного множества P. Вычислить значения z_{ij} по формуле (18) для *i-й* программы упорядоченного множества P.

5. Определить значения z_{ij} для рассматриваемой *i-й* программы. Рассчитать текущие значения Δ_j^{*T} и b_j^T. Проверить условие $b_j=0$, $j = \overline{1, J}$.

Если условие удовлетворено, переход к 6.

В противном случае - переход к 4.

6. Увеличить значения z_{ij} до выполнения условия (19) и назначить их для рассматриваемой программы.

Таким образом, в работе предложены алгоритмы определения совокупности программ по предупреждению аварийных ситуаций в горно-геологическом районе, на территории которых осуществляют свою деятельность несколько предприятий.

Предложены варианты для ситуации, когда вкладываемые предприятиями средства одинаковы, и когда различны.

Литература

7. Mozer D., Fofanov O., Yavorskiy V. Satellite radar interferometry as a reliable tool for monitoring displacements of rock masses // Proceedings of 2015 International Conference on Mechanical Engineering, Automation and Control Systems, MEACS 2015.

8. Архипова Н.И., Кульба В.В. Управление в чрезвычайных ситуациях. Учебное пособие. – М.: Российский государственный гуманитарный университет, 2008. – 470 с.

9. Предупреждение и ликвидация чрезвычайных ситуаций: электронное учебное пособие. [Электрон.ресурс]. – 2018. - URL:http://obzh.ru/pre.

10. Есмагамбетов Т.У., Шикульская О.М. Информационно-аналитическая поддержка деятельности ситуационного центра МЧС / Современные наукоемкие технологии. 2016. № 3-1. С. 18-23

11. Доррер Г.А. Методы и системы принятия решений: учебное пособие. – Красноярск: Сиб. федер. ун-т, 2016. – 210 с.

12. Антипов К.В. Система предупреждения аварийных ситуаций в металлургической промышленности. //Международный научно-исследовательский журнал. – 2012. - №5. – с.67-68.

АНАЛИЗ СУЩЕСТВУЮЩИХ МЕТОДОВ И МОДЕЛЕЙ ПРОГНОЗИРОВАНИЯ И ИХ СРАВНЕНИЕ

А.У. Калижанова, И.М. Кемельбекова
e-mail: inkara27@bk.ru
Алматинский университет энергетики и связи им. Г. Даукеева, Казахстан.

Аннотация. *Выполнен обзор основных методов прогнозирования: интуитивные и формализованные. Произведена классификация формализованных методов прогнозирования, а также описаны их различия. Рассмотрены регрессионные, авторегрессионные модели и модели экспоненциального сглаживания, а также нейросетевые и модели на базе цепей Маркова. На основании проделанной работы отмечены достоинства и недостатки каждой модели.*

Регрессионные модели Линейная регрессия – самая простая модель. В основе модели лежит процесс Y(t) на который оказывает влияние дискретный внешний фактор X(t), связь между ними линейна. Для линейного случая модель регрессии записывается в виде уравнения:

$$Y(t) = \alpha_0 + \alpha_1 X(t) + \xi_t \qquad (1)$$

где α_0, α_1 - коэффициенты модели;

ξ_t - случайная ошибка.

Метод группового учета аргументов (МГУА) – метод порождения и выбора регрессионных моделей оптимальной сложности. С усложнением модели точность прогнозирования увеличивается. Наиболее часто МГУА применяется при содержании в выборке нескольких элементов. Для данного случая модель записывается в виде уравнения:

$$Y(t) = w_0 = \sum_{i=1}^{m} w_i X_i(t) + \sum_{i=1}^{m}\sum_{j=1}^{m} w_{ij} X_i(t) X_{j(t)} + \sum_{i=1}^{m}\sum_{j=1}^{m}\sum_{k=1}^{m} w_{ijk} X_i(t) X_j(t) X_k + \ldots \quad (2)$$

где $x = \{x_i = 1, \ldots m\}$ - множество свободных переменных;

w - вектор параметров весовых коэффициентов.

Уравнение (2) называется опорной функцией. Для всех или выборочных аргументов строятся модели. Каждая модель обладает весовым коэффициентом, из которых, на следующем шаге выбираются лучшие. Если качество найденных моделей и полученных из нее прогнозных значений удовлетворяет, то процесс прекращается. Иначе, на предыдущем шаге выбранные $X_1(t) \ldots X_n(t)$ модели используются в качестве $Y(t)$ аргументов .

Авторегрессионные модели Значение процесса линейно зависит от некоторого количества предыдущих значений данного процесса $Y(t-1), \ldots Y(t-n)$, что является основой авторегрессионных моделей.

Авторегрессионная модель скользящего среднего (ARMA) — модель, использующаяся для анализа и прогнозирования стационарных временных рядов. Данная модель объединила в себе две тривиальные модели: авторегрессионную модель и модель скользящего среднего. Моделью ARMA описывается следующей формулой:

$$X(t) = C + \xi_t + \sum_{i=1}^{p} a_i X_{t-i} + \sum_{i=1}^{q} \beta_i \xi_{t-i} \quad (3)$$

где с – константа;

$\xi(t)$ - последовательность независимых и одинаково распределённых случайных величин, с нулевым средним (белый шум);

p и q — целые числа, задающие порядок модели;

$\alpha_1 \ldots \alpha_p$, $\beta_1 \ldots \beta_q$ - действительные числа, определяющие авторегрессионные коэффициенты и коэффициенты скользящего среднего, соответственно. Модели экспоненциального сглаживания Модели экспоненциального сглаживания являются одними из наиболее надежных и широко распространенными в прогнозировании, в силу простоты и наглядности. Основа данной модели – постоянный пересмотр прогнозных значений и их изменение, в связи с поступлением фактических. Каждому наблюдению присваивается экспоненциально убывающие веса, с уменьшением их актуальности. Таким образом, последние наблюдения обладают большим влиянием на прогнозируемое значение, по сравнению с предыдущими, причем веса наблюдений убывают по экспоненте. Модель экспоненциального сглаживания имеет следующий вид:

$$Y(t) = S(t) + \xi_t \quad (4)$$

$$S(t) = \alpha \cdot Y(t-1) + (1-\alpha) \cdot S(t-1) \quad (5)$$

где α - коэффициент сглаживания ($0 < \alpha < 1$).

Модель экспоненциального сглаживания включает модели, представленные в таблице 1.

Таблица 1 – Модели экспоненциального сглаживания

Модель Хольта(двойное экспоненциальное сглаживание)	Модель Хольта-Винтерса(тройное экспоненциальное сглаживание)
Используется при моделировании процессов, имеющих тренд.	Используется при моделировании процессов, имеющих тренд и сезонность.
$Y(t) = S(t) + \xi_t$ $S(t) = \alpha \cdot Y(t-1) + (1-\alpha)\cdot)(S(t-1) - \mathrm{B}(t-1))$, $B(t) = \gamma(S(t-1) - S(t-2)) + (1+\gamma)\mathrm{B}(t-1)$, Где B(t) - тренд; γ - параметр сглаживания тренда.	$Y(t) = R(t) + G(t)) \cdot S(t)$ R(t)- сглаженный уровень без учета сезонной составляющей;G(t)-сглаженный тренд; S(t)-сезонная составляющая.

Модели экспоненциального сглаживания в основном применяются для долгосрочного прогнозирования. Нейросетевые модели. На сегодняшний день в сравнении с другими моделями прогнозирования востребована модель на основе искусственной нейронной сети (ИНС). Нейронная сеть – система соединённых и взаимодействующих между собой нейронов. В задачах связанных с прогнозированием под нейронами понимаются простые процессы. На рисунке 1 изображена схема нейрона.

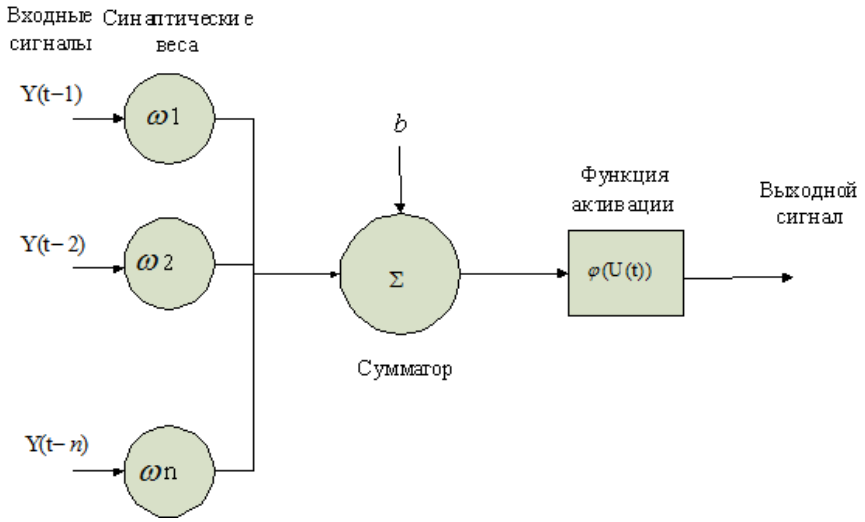


Рисунок 1 - Схема нейрона

Модель нейрона описывается следующей парой уравнений:

$$U(t) = \sum_{i=1}^{m} \omega_i \, \mathrm{Y(t-i)} + \mathrm{b} \tag{6}$$

$$\mathrm{Y(t)} = \varphi(\mathrm{U(t)}) \tag{7}$$

где: $\mathrm{Y(t-1)} \ldots \mathrm{Y(t-}n\mathrm{)}$ - входные сигналы;

$\omega_1 \ldots \omega_i$ - веса нейрона;

b – пороговое значение;

$\varphi(\mathrm{U(t)})$ - активационная функция.

Структурная схема нейронной сети изображена на рисунке 2.

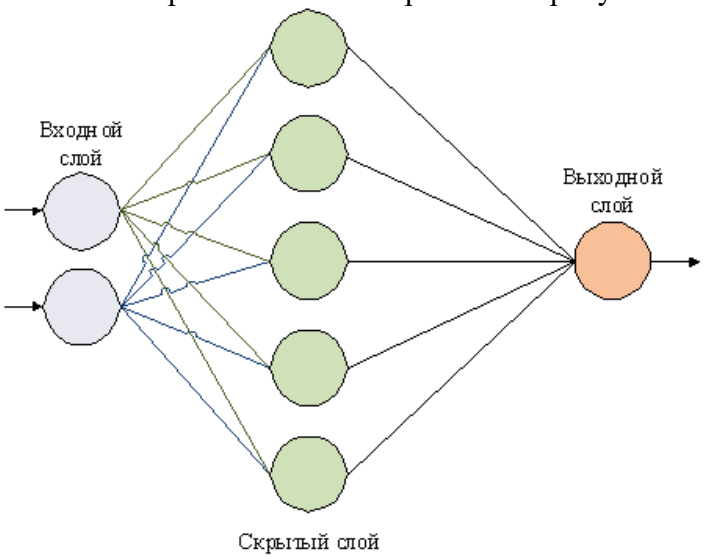


Рисунок 2 - Структурная схема нейронной сети

Нейросетевой метод прогнозирования, подходит как для решения линейных и сложных задач, так и для задач классификации. Обучение нейронной сети зависит от значений весовых коэффициентов. Нейросетевой подход, позволяет решать задачи разных масштабов.

Модели на базе цепей Маркова. В моделях прогнозирования на основе цепей Маркова на состояние процесса влияет лишь текущего состояния, и не имеет никакого влияние предыдущее состояние. Данные модели подходят для решения задач только к процессам с короткой памятью. На рисунке 3 изображена цепь Маркова с тремя состояниями.

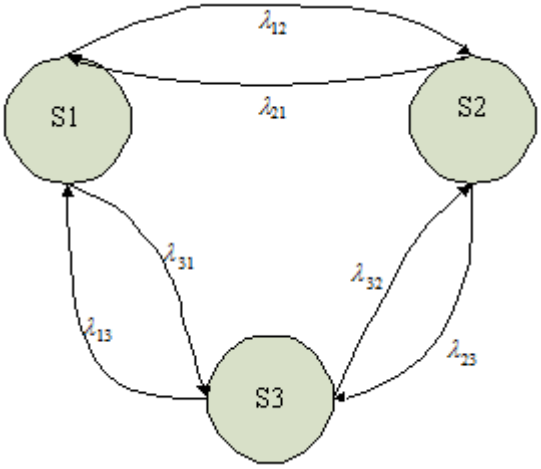


Рисунок 3 - Цепь Маркова; 3 состояния

Таким образом, структура цепи Маркова и вероятности перехода состояний определяют зависимость между будущим и его текущим значением процесса.

В таблице 2 приведено сравнение достоинств и недостатков методов прогнозирования.

Таблица 2 – Сравнение достоинств и недостатков методов прогнозирования

Модели прогнозирования	Достоинства	Недостатки
Регрессионные модели	Быстрота получения результата; Доступность промежуточных вычислений; Простота моделей; Разнородность решаемых задач.	Трудоемкость определения параметров; Возможность моделирования лишь линейных процессов; Сложность определения вида функциональной зависимости.
Авторегрессионные модели	Быстрота получения результата; Доступность промежуточных вычислений; Простота моделей; Разнородность решаемых задач.	Трудоемкость определения параметров;Возможность моделирования лишь линейных процессов.
Модели экспоненциального сглаживания	Простота моделей; Быстрота получения результата; Решение задач долгосрочного прогнозирования.	Отсутствие гибкости.
Нейросетевые модели	Возможность моделирования не линейных процессов; Адаптивность; Масштабируемость; Разнородность решаемых задач.	Сложность программной реализации; Отсутствие промежуточных вычислений; Высокие требования к непротиворечивости обучающей выборки.
Модели на базе цепей Маркова	Простота моделей;	Узкая применимость моделей.Невозможность решение задач прогнозирования с длинной памятью.

Литература

[1] Norizan M., Maizah Hura A., Zuhaimy I. Short Term Load Forecasting Using Double Seasonal ARIMA Model // Regional Conference on Statistical Sciences, Malaysia, Kelantan, 2010. P. 57 – 73.

[2] Collantes-Duarte J., Rivas-Echeverriat F. Time Series Forecasting using ARIMA, Neural Networks and Neo Fuzzy Neurons // WSEAS International Conference on Neural Networks and Applications, Switzerland, 2002 [электронный ресурс]. 6 p. URL: www.wseas.us/e-library/conferences/switzerland2002/papers/464.pdf (дата обращения 28.08.2011).

[3] Day-Ahead Electricity Price Forecasting Using the Wavelet Transform and ARIMA Models / A.J. Conejo [at al.] // IEEE transaction on power systems. 2005, Vol. 20, No. 2. P. 1035 – 1042.

[4] Тихонов Э.Е. Прогнозирование в условиях рынка. Невинномысск, 2006. 221 с.

[5] Леоненков А. Нечеткое моделирование в среде MATLAB и fuzzyTECH. СПб: БХВ-Петербург, 2005. 736 с.

[6] Armstrong J.S. Forecasting for Marketing // Quantitative Methods in Marketing. London: International Thompson Business Press, 1999. P. 92 – 119.

[7] Семенов В.В. Математическое моделирование динамики транспортных потоков мегаполиса. М.: ИПМ им. М.В.Келдыша РАН, 2004. 44 с.

[8] Self-organization in leaky threshold systems: The influence of near-mean field dynamics and its implications for earthquakes, neurobiology, and forecasting / J.B. Rundle [at al.] // Colloquium of the National Academy of Sciences, Irvine, USA, 2002. P. 2514 – 2521.

[9] Draper N., Smith H. Applied regression analysis. New York: Wiley, In press, 1981. 693 p.

[10] Maximum likelihood // The free encyclopedia «Wikipedia» [электронный ресурс]. URL: http://en.wikipedia.org/wiki/Maximum_likelihood (дата обращения 28.08.2011).

[11] Ивахненко А.Г. Обзор задач, решаемых по алгоритмам Метода Группового Учета Аргументов (МГУА) // Group Method of Data Handling [электронный ресурс]. URL: http://www.gmdh.net/articles/rus/obzorzad.pdf (дата обращения 28.08.2011).

МОДЕЛИРОВАНИЕ В СКАЛЯРНОЙ ФУНКЦИИ С ПОМОЩЬЮ ТРЕХМЕРНОГО СИМПЛЕКС ЭЛЕМЕНТА

[1]Казыхан Р., [2]Ташев А.
e-mail: [1]rysgulkazykhan@gmail.com, [2]azattash@mail.ru
[1]Институт информационных и вычислительных технологий КН МОН РК, Казахстан
[2]Институт информационных и вычислительных технологий КН МОН РК, Казахстан

Аннотация. *Основная идея метода конечных элементов состоит в том, что любую непрерывную величину, такую, как температура, давление и перемещение, можно аппроксимировать дискретной моделью, которая строится на множество кусочек- непрерывных функций, определенных на конечном числе подобластей.*

Метод конечных элементов является численным методом решения дифференциальных уравнений, встречающихся в физике и технике. Возникновение этого метода связано с решением задач космических исследований. Впервые он был опубликован в работе Тернера, Клужа, Мартина и Топпа. Эта работа способствовала появлению других работ; был опубликован ряд статьей с примерениями метода конечных элементов к задачам стройтельной механики сплошных сред.

В общем случае непрерывная величина заранее неизвестна и нужно определить значение этой величины в некоторых внутренних точках области. Дискретную модель, однако, очень легко построить, если сначала предположить, что числовые значение этой величины в каждой внутренней точке области известны. После этого можно перейти к общему случаю. Итак, при построении дискретной модели непрерывной величины поступают следующим образом:

1. В рассматриваемой области фиксируется конечное число точек. Эти точки называются узловыми точками или просто узлами.

2. Значение непрерывной величины в каждой узловой точке считается переменной, которая должна быть определена.

3. Область определения непрерыной величины разбивается на конечное число подоблостей, называемых элементами. Эти элементы имееют общие узловые точки и в совокупности аппроксимируют форму областей.

4. Непрерывная величина аппроксимируется на каждом элементе полиномом, который определяется с помощью узловых значений этой величины. Для каждого элемента определяется свой полином, но полиномы подбираются таким образом, что бы сохранялась непрерывность величины вдоль границ элемента.

Метод конечных элементов основан на идее аппроксимации непрерывной функции дискретной моделью, которая строится на множестве кусочно-непрерывных функци, определенных на конечном числе подобластей, называемых элементами. В качестве функции элемента чаще всего применяктся полином. Порядок полинома зависит от числа используемых в каждом узле элемента данных о непрерывной функции.

Одномерный симплекс- элемент представляет собой прямолинейный отрезок длины L с двумя узлами, по одному на каждом конце отрезка.

$$T = \varphi_1 T_1 + \varphi_2 T_2 \tag{1}$$

$$\varphi_1 = \frac{x_2 - x}{L} \qquad \varphi_2 = \frac{x - x_1}{L} \tag{2}$$

Двумерный симплекс- элемент это треугольник с прямолинейными сторонами и тремя узлами, по одному каждой вершине Необходима логическая нумерация узлов элемента.

$$T = \varphi_1 T_1 + \varphi_2 T_2 + \varphi_3 T_3$$

$$\varphi_1 = \frac{1}{2A}(a_1 + b_1 x + c_1 y)$$

$$\begin{cases} a_1 = x_2 y_3 - x_3 y_2 \\ b_1 = y_2 - y_3 \\ c_1 = x_3 - x_2 \end{cases}$$

$$\varphi_2 = \frac{1}{2A}(a_2 + b_2 x + c_2 y)$$

$$\begin{cases} a_2 = x_3 y_1 - y_3 y_1 \\ b_2 = y_3 - y_1 \\ c_2 = x_1 - x_3 \end{cases}$$

$$\varphi_3 = \frac{1}{2A}(a_3 + b_3 x + c_3 y)$$

$$\begin{cases} a_3 = x_1 y_2 - x_2 y_1 \\ b_3 = y_1 - y_2 \\ c_3 = x_2 - x_1 \end{cases}$$

$$2A = \begin{vmatrix} 1 & x_1 & y_1 \\ 1 & x_2 & y_2 \\ 1 & x_3 & y_3 \end{vmatrix}$$

Мы рассмотрим трехмерный симплекс-элемент

$$T = \varphi_1 T_1 + \varphi_2 T_2 + \varphi_3 T_3 + \varphi_4 T_4$$

Рассмотрим трехмерную функцию T(x, y, z), значение которой задано в угловых точках параллелепипеда (1,2,…8) (1-T, 2-T,…8-T) (Рис. 1)

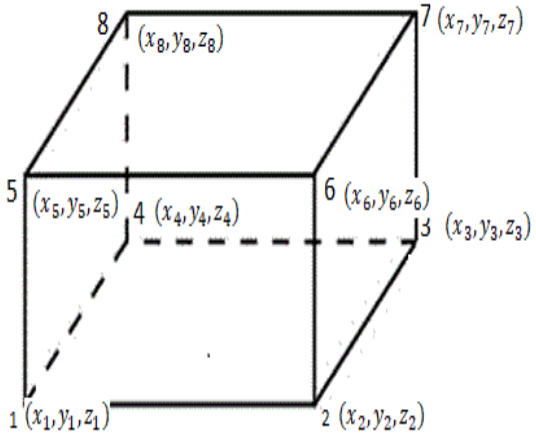


Рис. 1 параллепипед

Если длина параллелепипеда по оси $x \to 2a$, по оси $y \to 2b$, а по оси $z \to 2c$ тогда координаты угловых точек относительно центра параллелепипеда будет равна

1- (-a; в; -c)= (x_1, y_1, z_1)
2- (a; в; -c)= (x_2, y_2, z_2)
3- (a; -в; -c)= (x_3, y_3, z_3)
4- (-a; -в; -c)= (x_4, y_4, z_4)
5- (-a; в; c)= (x_5, y_5, z_5)
6- (a; в; c)= (x_6, y_6, z_6)
7- (a; -в; c)= (x_7, y_7, z_7)
8-(-a; -в; c) = (x_8, y_8, z_8)

Значение функции T(x, y, z) произвольной точке (x, y, z) внутри параллелепипеда аппроксимируем так:

$$\mathrm{T}(x, y, z) = \lambda_1 + \lambda_2 x_1 + \lambda_3 y_1 + \lambda_4 z_1 + \lambda_5 x_1 y_1 + \lambda_6 x_1 z_1 + \lambda_7 y_1 z_1 + \lambda_8 x_1 y_1 z_1 \qquad (3)$$

Для определения констант Λ_i(i=1; 8) составим следующую систему управлений:

$$\begin{gathered} T_1 = \mathrm{T}(x_1, y_1, z_1);\ T_2 = \mathrm{T}(x_2, y_2, z_2);\ T_3 = \mathrm{T}(x_3, y_3, z_3); \\ T_4 = \mathrm{T}(x_4, y_4, z_4);\ T_5 = \mathrm{T}(x_5, y_5, z_5);\ T_6 = \mathrm{T}(x_6, y_6, z_6); \\ T_7 = \mathrm{T}(x_7, y_7, z_7);\ T_8 = \mathrm{T}(x_8, y_8, z_8); \end{gathered} \qquad (4)$$

Подставляя значения аргументов получим систему уравнении:

$$\lambda_1 + \lambda_2 x_1 + \lambda_3 y_1 + \lambda_4 z_1 + \lambda_5 x_1 y_1 + \lambda_6 x_1 z_1 + \lambda_7 y_1 z_1 + \lambda_8 x_1 y_1 z_1 = \mathrm{T}_1;$$
$$\lambda_1 + \lambda_2 x_2 + \lambda_3 y_2 + \lambda_4 z_2 + \lambda_5 x_2 y_2 + \lambda_6 x_2 z_2 + \lambda_7 y_2 z_2 + \lambda_8 x_2 y_2 z_2 = \mathrm{T}_2;$$
$$\lambda_1 + \lambda_2 x_3 + \lambda_3 y_3 + \lambda_4 z_3 + \lambda_5 x_3 y_3 + \lambda_6 x_3 z_3 + \lambda_7 y_3 z_3 + \lambda_8 x_3 y_3 z_3 = \mathrm{T}_3;$$

$$\lambda_1 + \lambda_2 x_4 + \lambda_3 y_4 + \lambda_4 z_4 + \lambda_5 x_4 y_4 + \lambda_6 x_4 z_4 + \lambda_7 y_4 z_4 + \lambda_8 x_4 y_4 z_4 = \mathrm{T}_4; \quad (5)$$
$$\lambda_1 + \lambda_2 x_5 + \lambda_3 y_5 + \lambda_4 z_5 + \lambda_5 x_5 y_5 + \lambda_6 x_5 z_5 + \lambda_7 y_5 z_5 + \lambda_8 x_5 y_5 z_5 = \mathrm{T}_5;$$
$$\lambda_1 + \lambda_2 x_6 + \lambda_3 y_6 + \lambda_4 z_6 + \lambda_5 x_6 y_6 + \lambda_6 x_6 z_6 + \lambda_7 y_6 z_6 + \lambda_8 x_6 y_6 z_6 = \mathrm{T}_6;$$
$$\lambda_1 + \lambda_2 x_7 + \lambda_3 y_7 + \lambda_4 z_7 + \lambda_5 x_7 y_7 + \lambda_6 x_7 z_7 + \lambda_7 y_7 z_7 + \lambda_8 x_7 y_7 z_7 = \mathrm{T}_7;$$
$$\lambda_1 + \lambda_2 x_8 + \lambda_3 y_8 + \lambda_4 z_8 + \lambda_5 x_8 y_8 + \lambda_6 x_8 z_8 + \lambda_7 y_8 z_8 + \lambda_8 x_8 y_8 z_8 = \mathrm{T}_8;$$

Решая эту систему линейных уравнений получим значения коэффицентов $\lambda_1, \lambda_2 \dots \lambda_8$

$$\wedge_1 = \frac{\mathrm{T}_8 + \mathrm{T}_7 + \mathrm{T}_6 + \mathrm{T}_5 + \mathrm{T}_4 + \mathrm{T}_3 + \mathrm{T}_2 + \mathrm{T}_1}{8}$$
$$\wedge_2 = \frac{-\mathrm{T}_8 + \mathrm{T}_7 + \mathrm{T}_6 - \mathrm{T}_5 - \mathrm{T}_4 + \mathrm{T}_3 + \mathrm{T}_2 - \mathrm{T}_1}{8\mathrm{a}}$$
$$\wedge_3 = \frac{-T_8 - T_7 + T_6 + T_5 - T_4 - T_3 + T_2 + T_1}{8b}$$
$$\wedge_4 = \frac{\mathrm{T}_8 + \mathrm{T}_7 + \mathrm{T}_6 + \mathrm{T}_5 - \mathrm{T}_4 - \mathrm{T}_3 - \mathrm{T}_2 - \mathrm{T}_1}{8\mathrm{c}}$$
$$\wedge_5 = \frac{\mathrm{T}_8 + \mathrm{T}_7 + \mathrm{T}_6 + \mathrm{T}_5 + \mathrm{T}_4 + \mathrm{T}_3 + \mathrm{T}_2 + \mathrm{T}_1}{8\mathrm{ab}}$$
$$\wedge_6 = \frac{\mathrm{T}_8 - \mathrm{T}_7 + \mathrm{T}_6 - \mathrm{T}_5 + \mathrm{T}_4 - \mathrm{T}_3 + \mathrm{T}_2 - \mathrm{T}_1}{8\mathrm{ac}}$$
$$\wedge_7 = \frac{-\mathrm{T}_8 - \mathrm{T}_7 + \mathrm{T}_6 + \mathrm{T}_5 + \mathrm{T}_4 + \mathrm{T}_3 - \mathrm{T}_2 - \mathrm{T}_1}{8\mathrm{bc}}$$
$$\wedge_8 = \frac{\mathrm{T}_8 - \mathrm{T}_7 + \mathrm{T}_6 - \mathrm{T}_5 - \mathrm{T}_4 + \mathrm{T}_3 - \mathrm{T}_2 + \mathrm{T}_1}{8\mathrm{abc}}$$

(7) подставляя эти значение в уравнение (2) получим:

$$\mathrm{T}(\mathrm{x}, \mathrm{y}, \mathrm{z}) = \varphi_1(\mathrm{x},\mathrm{y},\mathrm{z}) * T_1 + \varphi_2(\mathrm{x},\mathrm{y},\mathrm{z}) * T_2 + \varphi_3(\mathrm{x},\mathrm{y},\mathrm{z}) * T_3 + \varphi_4 T_4 + \varphi_5(\mathrm{x},\mathrm{y},\mathrm{z}) * T_5 + \varphi_6(\mathrm{x},\mathrm{y},\mathrm{z}) * T_6 + \varphi_7(\mathrm{x},\mathrm{y},\mathrm{z}) * T_7 + \varphi_8(\mathrm{x},\mathrm{y},\mathrm{z}) * T_8; \quad (6)$$

$-a \le x \le a$; $-b \le x \le b$; $-c \le x \le c$;

Здесь φ_i(i= 1, 8) определяются следующим образом:

$$\varphi_1(\mathrm{x}, \mathrm{y}, \mathrm{z}) = \left(\frac{1}{8} - \frac{x}{8a} + \frac{y}{8b} - \frac{z}{8c} - \frac{xy}{8ab} + \frac{xz}{8ac} - \frac{yz}{8bc} + \frac{xyz}{8abc}\right);$$
$$\varphi_2(\mathrm{x}, \mathrm{y}, \mathrm{z}) = \left(\frac{1}{8} + \frac{x}{8a} + \frac{y}{8b} - \frac{z}{8c} + \frac{xy}{8ab} - \frac{xz}{8ac} - \frac{yz}{8bc} - \frac{xyz}{8abc}\right);$$
$$\varphi_3(\mathrm{x}, \mathrm{y}, \mathrm{z}) = \left(\frac{1}{8} + \frac{x}{8a} - \frac{y}{8b} - \frac{z}{8c} - \frac{xy}{8ab} - \frac{xz}{8ac} + \frac{yz}{8bc} + \frac{xyz}{8abc}\right);$$
$$\varphi_4(\mathrm{x}, \mathrm{y}, \mathrm{z}) = \left(\frac{1}{8} - \frac{x}{8a} - \frac{y}{8b} - \frac{z}{8c} + \frac{xy}{8ab} + \frac{xz}{8ac} + \frac{yz}{8bc} - \frac{xyz}{8abc}\right); \quad (7)$$
$$\varphi_5(\mathrm{x}, \mathrm{y}, \mathrm{z}) = \left(\frac{1}{8} - \frac{x}{8a} + \frac{y}{8b} + \frac{z}{8c} - \frac{xy}{8ab} - \frac{xz}{8ac} + \frac{yz}{8bc} - \frac{xyz}{8abc}\right);$$
$$\varphi_6(\mathrm{x}, \mathrm{y}, \mathrm{z}) = \left(\frac{1}{8} + \frac{x}{8a} + \frac{y}{8b} + \frac{z}{8c} + \frac{xy}{8ab} + \frac{xz}{8ac} + \frac{yz}{8bc} + \frac{xyz}{8abc}\right);$$
$$\varphi_7(\mathrm{x}, \mathrm{y}, \mathrm{z}) = \left(\frac{1}{8} + \frac{x}{8a} - \frac{y}{8b} + \frac{z}{8c} - \frac{xy}{8ab} + \frac{xz}{8ac} - \frac{yz}{8bc} - \frac{xyz}{8abc}\right);$$
$$\varphi_8(\mathrm{x}, \mathrm{y}, \mathrm{z}) = \left(\frac{1}{8} - \frac{x}{8a} - \frac{y}{8b} + \frac{z}{8c} + \frac{xy}{8ab} - \frac{xz}{8ac} - \frac{yz}{8bc} + \frac{xyz}{8abc}\right);$$

Здесь -a ≤ x ≤a; -b ≤y ≤b; -c ≤ z≤ c.

Значение функций φ_i(x, y, z) (i=1,8) в угловых точках параллелепипеда определяем так:

$\varphi_1(x_1,\ y_1,\ z_1)=1$; $\varphi_1(x_1,\ y_1,\ z_1)=\varphi_1(x_2,\ y_2,\ z_2)=\varphi_1(x_3,\ y_3,\ z_3)=\varphi_1(x_4,\ y_4,\ z_4)=\varphi_1(x_5, y_5, z_5)=\varphi_1(x_6, y_6, z_6)=\varphi_1(x_7, y_7, z_7)=\varphi_1(x_8, y_8, z_8)=0$

$\varphi_2(x_2,\ y_2,\ z_2)=1$; $\varphi_2(x_1,\ y_1,\ z_1)=\varphi_2(x_2,\ y_2,\ z_2)=\varphi_2(x_3,\ y_3,\ z_3)=\varphi_2(x_4,\ y_4,\ z_4)=\varphi_2(x_5, y_5, z_5)=\varphi_2(x_6, y_6, z_6)=\varphi_2(x_7, y_7, z_7)=\varphi_2(x_8, y_8, z_8)=0$

$\varphi_3(x_3,\ y_3,\ z_3)=1$; $\varphi_3(x_1,\ y_1,\ z_1)=\varphi_3(x_2,\ y_2,\ z_2)=\varphi_3(x_3,\ y_3,\ z_3)=\varphi_3(x_4,\ y_4,\ z_4)=\varphi_3(x_5, y_5, z_5)=\varphi_3(x_6, y_6, z_6)=\varphi_3(x_7, y_7, z_7)=\varphi_3(x_8, y_8, z_8)=0$

$\varphi_4(x_4,\ y_4,\ z_4)=1$; $\varphi_4(x_1,\ y_1,\ z_1)=\varphi_4(x_2,\ y_2,\ z_2)=\varphi_4(x_3,\ y_3,\ z_3)=\varphi_4(x_4,\ y_4,\ z_4)=\varphi_4(x_5, y_5, z_5)=\varphi_4(x_6, y_6, z_6)=\varphi_4(x_7, y_7, z_7)=\varphi_4(x_8, y_8,\ z_8)=0$

$\varphi_5(x_5,\ y_5,\ z_5)=1$; $\varphi_5(x_1,\ y_1,\ z_1)=\varphi_5(x_2,\ y_2,\ z_2)=\varphi_5(x_3,\ y_3,\ z_3)=\varphi_5(x_4,\ y_4,\ z_4)=\varphi_5(x_5, y_5, z_5)=\varphi_5(x_6, y_6, z_6)=\varphi_5(x_7, y_7, z_7)=\varphi_5(x_8, y_8, z_8)=0$

$\varphi_6(x_6,\ y_6,\ z_6)=1$; $\varphi_6(x_1,\ y_1,\ z_1)=\varphi_6(x_2,\ y_2,\ z_2)=\varphi_6(x_3,\ y_3,\ z_3)=\varphi_6(x_4,\ y_4,\ z_4)=\varphi_6(x_5, y_5, z_5)=\varphi_6(x_6, y_6, z_6)=\varphi_6(x_7, y_7, z_7)=\varphi_6(x_8, y_8, z_8)=0$

$\varphi_7(x_7,\ y_7,\ z_7)=1$; $\varphi_7(x_1,\ y_1,\ z_1)=\varphi_7(x_2,\ y_2,\ z_2)=\varphi_7(x_3,\ y_3,\ z_3)=\varphi_7(x_4,\ y_4,\ z_4)=\varphi_7(x_5, y_5, z_5)=\varphi_7(x_6, y_6, z_6)=\varphi_7(x_7, y_7, z_7)=\varphi_7(x_8, y_8, z_8)=0$

$\varphi_8(x_8,\ y_8,\ z_8)=1$; $\varphi_8(x_1,\ y_1,\ z_1)=\varphi_8(x_2,\ y_2,\ z_2)=\varphi_8(x_3,\ y_3,\ z_3)=\varphi_8(x_4,\ y_4,\ z_4)=\varphi_8(x_5, y_5, z_5)=\varphi_8(x_6, y_6, z_6)=\varphi_8(x_7, y_7, z_7)=\varphi_8(x_8, y_8, z_8)=0$

Результаты данной работы могут быть использованы для определения закона распределения температуры в трехмерных стержнях виде параллелепипеда.

Литература

1. Ларри Дж. Сегерлинд. Прикладной конечно-элементный анализ. - Джон Уилли и Сыновья, Inc. Нью-Йорк / Лондон / Сидней / Торонто, 1976.- 392 с.

2. Carslaw H.S., Jaeger J.C. Теплопроводность в твердых телах. Издательство Оксфордского университета, Лондон, 1986 - 526 с.

3. Тимошенко С., Гудиер Дж. Н. Теория упругости. МакГроу-Хилл. Книга. Компания. Inc., 1987. - 567 с.

4. Зенкевич О.С. Метод в инженерных науках. Butterworth-Heinemann. - Оксфорд-Окленд-Бостон-Йоханнесбург-Мельбурн-Нью-Дели, 2000. - 690 с.

POINCARE CHAOS IN IMPULSIVE SYSTEMS

[1]Akhmet M., [2,3]Tleubergenova M., [2,3]Nugayeva Z.
E-mail: marat@metu.edu.tr, madina_1970@mail.ru, zahira2009.85@mail.ru
[1]Department of Mathematics, Middle East Technical University, 06800, Ankara, Turkey
[2]Department of Mathematics, Aktobe Regional University, 030000, Aktobe, Kazakhstan
[3]Institute of Information and Computational Technologies CS MES RK, Kazakhstan

Abstract. *The impulsive differential equations with unpredictable perturbations are under investigation. The definition of the discontinuous unpredictable function with the discrete unpredictable set of discontinuity moments is introduced. The existence and*

uniqueness of asymptotically stable discontinuous unpredictable solutions for quasi-linear systems are proved.

1. Introduction and preliminaries

The theory of differential equations with impulses has been developed having in focus oscillations of various types. The fundamentals for discontinuous periodic, quasi-periodic and almost periodic solutions one can find in books [1–3]. Apparently, the most convenient start point for building the theory analogously to that of differential equations, were theorems on existence and stability of periodic solutions, and their applications [4–6]. More sophisticated are discontinuous quasi-periodic solutions [7], and most interesting almost periodic functions. Initially, the functions were introduced in the book [8] as solutions of impulsive systems. The modern state of the theory and the history on the subject one can found in the book [2]. Basics of stability analysis were laid in papers [3]. Nowadays, numerous papers are known [9–14], which investigate discontinuous periodic and almost periodic oscillations in different types of differential equations and neural networks. The line of discontinuous oscillations had been broken at the recurrent motions [2]. Next, chaotic dynamics of impulsive equations have been considered for irregular oscillations. Similarly to that in continuous dynamics, the oscillations are investigated not as isolated motions, but as members of chaotic attractors [15–18]. This makes the impression that chaotic oscillations are strange for dynamical systems [19]. The perception has been changed, since of the unpredictable point [20, 21], which is a sort of the Poisson stable point. The closure of the orbit is the quasi-minimal set. It was proved that the sensitivity presents in the set. Now, the term of Poincar´e chaos is naturally placed in the line with Li-Yorke and Devaney chaos. For instance, A. Miller [22], R. Thakur and R. Das [23] use the unpredictable point in the chaos theory.

Unpredictable points considered in the dynamics of shifts of bounded functions on the real line produce new classes of oscillations, unpredictable functions and unpredictable sequences [20, 21]. They have been followed by results on unpredictability of solutions of differential equations [24–26]. In the present paper, we consider discontinuous functions to be unpredictable. For this reason, the methods introduced and developed for discontinuous dynamical systems [1] became very useful. The existence and uniqueness of asymptotically stable unpredictable solutions for quasi-linear impulsive systems are in the focus of this study. We have specified the set of discontinuity moments and provided definitions not only for discontinuous unpredictable functions, but also specified the systems.

Throughout the paper, R, N and Z will stand for the set of of real, natural and integer numbers, respectively. We use the norm $\|u\| = \max_{1\le x\le p}|u_i|$, where $|\cdot|$ - is the absolute value, $u = (u_1,\dots,u_p)\in R^p$ and $p-$a fixed natural number. Correspondingly, for a square matrix $A = (a_{ij})$, $i,j = 1,\dots,p$, the norm $\|A\| = \max_{1\le x\le p}\sum_{j=1}^{p}|a_{ij}|$, is utilized.

Denote by B the set of all $p-$dimensional functions defined on the real lines such that they are continuous except countable sets of points unbounded on both sides, left-continuous, and admit one-sided limits at the points. The sets of discontinuity points do not have finite accumulation points. Two functions φ and ψ from the set are said to be $\varepsilon-$equivalent on a bounded interval $J\subset R$ if the points of discontinuity of the functions

in J can be numerated θ_i^{φ} and θ_i^{ψ}, $i=1,\dots,p,$ respectively, such that $\left|\theta_i^{\varphi}-\theta_i^{\psi}\right|<\varepsilon$ for all $i=1,\dots,p,$ and $\|\varphi(t)-\psi(t)\|<\varepsilon$ for each $t\in J,$ except those between θ_i^{φ} and θ_i^{ψ} for each i. We also say that the functions are $\varepsilon-$neighborhoods of each other, if φ and ψ are $\varepsilon-$equivalent on J. The topology defined with the aid of such neighborhoods is called the *B-topology*.

A $p-$dimensional vector-function $g(t,x)$ with domain $R\times S, S\in R^p$, is said to be from the set $B(S)$ if $g(t,x)\in B$ for each fixed $x\in S$ with points of discontinuity common for all x in S. Two functions $g(t,x)$ with $h(t,x)$ from $B(S)$ are said to be $\varepsilon-$equivalent on a bounded interval $J\subset R$ if for each fixed $x\in S$ they are $\varepsilon-$equivalent as functions from B.

In what follows we denote $[\alpha\hat{,}\beta]$, $\alpha,\beta\in R$, the interval $[\alpha,\beta]$, if $\alpha<\beta$ and the interval $[\beta,\alpha]$, if $\beta<\alpha$.

Let us fix the set of of real numbers θ_i, $i\in Z$, such that $\underline{\theta}\le\theta_{i+1}-\theta_i\le\overline{\theta}$ for some positive numbers $\underline{\theta},\overline{\theta}$, and all integers i. It is clear that the set is not bounded from both sides, and $|\theta_i|\to\infty$ as $|i|\to\infty$.

Definition 1. *A function $\varphi(t)\in B$ with the set of discontinuity points $\theta_i, i\in Z$ is called discontinuous unpredictable function (d.u.f.), if there exist positive numbers ε_0,σ and sequences t_n,s_n of real numbers and sequences l_n,m_n of integers all of which diverges to infinity such that*

(a) $|\theta_{i+l_n}-t_n-\theta_i|\to\infty$ as $n\to\infty$ for each i in bounded intervals of integers and $\left|\theta_{m_n+l_n}-t_n-\theta_{m_n}\right|\ge\varepsilon_0$ for each $n\in N$;

(b) for every positive number ε there exists a positive number δ such that $\|\varphi(t_1)-\varphi(t_2)\|<\varepsilon$ whenever the points t_1 and t_2 belong to the interval of continuity and $\|t_1-t_2\|<\delta$;

(c) $\varphi(t+t_n)\to\varphi(t)$ as $n\to\infty$ in B-topology on *each bounded interval;*

(d) for each natural number n there exists an interval $[s_n-\sigma,s_n+\sigma]\subseteq[\theta_{m_n}\hat{,}(\theta_{m_n+l_n}-t_n)]$ which does not contain any point of discontinuity of $\varphi(t)$ and $\varphi(t+t_n)$, and $\|\varphi(t+t_n)-\varphi(t)\|\ge\varepsilon_0$ for each $t\in[s_n-\sigma,s_n+\sigma]$.

Definition 2. *A function $f(t,x)\in B(S)$, $f=(f_1,\dots,f_p)$ with the set of discontinuity points $\theta_i, i\in Z$ is called unpredictable function in t, if there exist positive numbers ε_0,σ and sequences t_n,s_n of real numbers and sequences l_n,m_n of integers all of which diverges to infinity such that*

(a) $|\theta_{i+l_n}-t_n-\theta_i|\to\infty$ as $n\to\infty$ for each i in bounded intervals of integers and $\left|\theta_{m_n+l_n}-t_n-\theta_{m_n}\right|\ge\varepsilon_0$ for each $n\in N$;

(b) for every positive number ε there exists a positive number δ such that $\|f(t_1,x)-f(t_2,x)\|<\varepsilon$ whenever the points t_1 and t_2 belong to the interval of continuity and $\|t_1-t_2\|<\delta$;

(c) $\sup_s \|f(t+t_n,x)-f(t,x)\| \to 0$ *as* $n\to\infty$ on *each bounded interval of the time axis;*

(d) for each natural number n *there exists an interval* $[s_n-\sigma, s_n+\sigma] \subseteq [\theta_{m_n} \hat{,} (\theta_{m_n+l_n}-t_n)]$ *which does not contain any point of discontinuity of* $f(t,x)$ *and* $f(t+t_n,x)$, *and* $\inf_s \|f(t+t_n,x)-f(t,x)\| \ge \varepsilon_0$ *for each* $t\in[s_n-\sigma, s_n+\sigma]$.

Definition 3. *Suppose that* $f(t,x)$ *is an unpredictable function in* t *with the set of discontinuity points* $\theta_i, i\in Z$, $G_i(x), i\in Z$, *is a sequence of* $p-$*dimensional vectors bounded on* S. *The couple* $(f(t,x), G_i(x))$ *is a called unpredictable, if there exist positive numbers* ε_0, σ *and sequences* t_n, s_n *of real numbers and sequences* l_n, m_n *of integers all of which diverges to infinity such that*

(a) $|\theta_{i+l_n}-t_n-\theta_i| \to \infty$ *as* $n\to\infty$ *for each* i *in bounded intervals of integers and* $|\theta_{m_n+l_n}-t_n-\theta_{m_n}| \ge \varepsilon_0$ *for each* $n\in N$;

(b) for every positive number ε *there exists a positive number* δ *such that* $\|f(t_1,x)-f(t_2,x)\| < \varepsilon$ *whenever the points* t_1 *and* t_2 *belong to the interval of continuity and* $\|t_1-t_2\| < \delta$;

(c) $\sup_s \|f(t+t_n,x)-f(t,x)\| \to 0$ *as* $n\to\infty$ on *each bounded interval of the time axis;*

(d) for each natural number n *there exists an interval* $[s_n-\sigma, s_n+\sigma] \subseteq [\theta_{m_n} \hat{,} (\theta_{m_n+l_n}-t_n)]$ *which does not contain any point of discontinuity of* $f(t,x)$ *and* $f(t+t_n,x)$, *and* $\inf_s \|f(t+t_n,x)-f(t,x)\| \ge \varepsilon_0$ *for each* $t\in[s_n-\sigma, s_n+\sigma]$;

(e) $\sup_s \|G_{i+l_n}(x)-G_i(x)\| \to 0$ *as* $n\to\infty$ *on each bounded interval of integers and* $\inf_s \|G_{m_n+l_n}(x)-G_{m_n}(x)\| \ge \varepsilon_0$ *for all number* n.

On account of the goal of the present study, we define the discontinuity moments of the impulsive systems that will be shaped as

$$\theta_i = iT+\tau_i,\ i\in Z, \tag{1}$$

where $\tau_i, i\in Z$, is an unpredictable sequence of real numbers [25], and $T\ge 4$, is a number such that $\sup_{i\in Z}|\tau_i| < \frac{T}{h}$ for some $h\ge 3$.

2. Quasi-linear systems with non-unpredictable impulses

The main object of the present paper is the impulsive system of quasi-linear differential equations,

$$\begin{aligned} x' &= Ax+f(t,x),\ t\ne\theta_i, \\ \Delta x\big|_{t=\theta_i} &= Bx, \end{aligned} \tag{2}$$

where $t\in R, x\in S$, the constant matrices $A\in R^{p\times p}$ and $B\in R^{p\times p}$, of discontinuity moments is defined by equation (1), $f(t,x): R\times S\to R^p$ is an unpredictable function in

the sense of Definition 2, and $S = \{x \in R^p, \| x \| < H\}$, where H is a positive number. We suppose that $\det(I + B) \neq 0$, where I is the $p \times p$ identity matrix.

Let us consider the following system associated with (2),

$$\begin{aligned} &x' = Ax, t \neq \theta_i, \\ &\Delta x \big|_{t=\theta_i} = Bx. \end{aligned} \tag{3}$$

Since matrices A and B are commutative, it follows that the transition matrix of system (3) can be written as [3].

$$X(t,u) = e^{A(t-u)}(I + B)^{i([u,t))}, \tag{4}$$

where $i([u,t))$ is number of points $\theta_i, i \in Z$, which belong to the interval $[u,t)$. Let us denote by λ_j, $j = 1,\ldots,n$, the eigenvalues of the matrix $A + \frac{1}{T} Ln(I + B)$.

The following conditions will be needed throughout the paper:

(C1) $\max_j \operatorname{Re} \lambda_j = \lambda < 0$, where $\operatorname{Re} \lambda_j$ is real part of λ_j for each $j = 1,\ldots,p$;

(C2) there exists a positive number L_f such that $\|f(t,x) - f(t,y)\| \leq L_f \|x - y\|$ for all $t \in R$, $x, y \in S$;

(C3) there exists a positive number M_f such that $\|f(t,x)\| \leq M_f$ for all $(t,x) \in R \times S$;

The condition (C1) and (4) imply that [1, 4] there exist numbers $K \geq 1$ and $0 < \alpha < -\lambda$, such that

$$\|X(t,u)\| \leq Ke^{-\alpha(t-u)}. \tag{5}$$

(C4) $\frac{KM_f}{H} < \alpha$;

(C5) $KL_f < \alpha$.

Theorem 1. *Suppose that conditions (C1)-(C5) are valid. Then system (2) possesses a unique asymptotically stable discontinuous unpredictable solution.*

3. Quasi-linear systems with unpredictable impulses

Consider the following linear impulsive system,

$$\begin{aligned} &x' = Ax + f(t,x), t \neq \theta_i, \\ &\Delta x \big|_{t=\theta_i} = Bx + G_i(x), \end{aligned} \tag{6}$$

where $t \in R, x \in S,$ the constant matrices $A \in R^{p \times p}$ and $B \in R^{p \times p}$, of discontinuity moments is defined by equation (1), $(f(t,x), G_i(x))$ is an unpredictable couple in the sense of Definition 3. Additionally, $\det(I + B) \neq 0$, where I is the $p \times p$ identity matrix.

It is worth noting that (6) is a linear impulsive system with unpredictable impulses, and it is not a particular case of system (2).

The following conditions will be needed throughout the section:

(C6) there exists a positive number L_G such that $\|G_i(x_1) - G_i(x_2)\| \leq L_G \|x_1 - x_2\|$ for all $x_1, x_2 \in S,\ i \in Z$;

(C7) there exists a positive number M_G such that $\sup_{x \in S} \|G(x)\| \leq M_G$;

(C8) $\dfrac{KM_f}{\alpha} + \dfrac{KM_G}{1-e^{-\alpha\underline{\theta}}} < H$;

(C9) $\dfrac{KL_f}{\alpha} + \dfrac{KL_G}{1-e^{-\alpha\underline{\theta}}} < 1$;

(C10) $KL_f + \dfrac{1}{\underline{\theta}}\ln\left(1 + KL_G\right) < \alpha$.

Theorem 2. *Suppose that conditions (C1)-(C3), (C6)-(C10), are valid. If the couple* $\left(f(t,x), G_i(x)\right)$ *is unpredictable in the sense of Definition 3, then system (6) possesses a unique asymptotically stable discontinuous unpredictable solution.*

References

1. Akhmet M. Principles of discontinuous dynamical systems / M. Akhmet.– New York: Springer-Verlag, 2010. – P. 176.
2. Akhmet M. Almost periodicity, chaos, and asymptotic equivalence / M. Akhmet. – Switzerland: Springer International Publishing, 2020. – P. 360.
3. Samoilenko, A.M., Perestyuk, N.A. Theory of impulsive differential equations / A.M. Samoilenko, N.A. Perestyuk, – Singapore: World Scientific, 1995. – P. 472.
4. Erbe L.H., Liu X. Existence of periodic solutions of impulsive differential systems / Appl.Math. and Stoch. Anal. 1991. – Vol. 4, N.2 –P. 137-146.
5. Liz E., Nietto, J.J. Periodic Solutions of Discontinuous Impulsive Differential Systems / J. Math. Anal.Appl. 1991. – Vol.161, N. 2, P. 388-394.
6. Niu Y., Li X. Periodic Solutions of Sublinear Impulsive Differential Equations / Commun. Nonlinear. Sci. Numer. Simulat. 2018. – Vol. 13. – P. 439-452.
7. Akhmet M.U. Quasiperiodic solutions of systems with impulses, in Asymptotic Methods in Problems of Mathematical Physics / Akad. Nauk Ukrain. SSR, Inst. Mat., Kiev. 1989. – P. 8-12.
8. Halanay A., Wexler D. Qualitative theory of impulse systems (russian) / A. Halanay, D. Wexler. – Moscow: Mir, 1971.
9. Akhmet M.U., Fen M.O., Kirane, M. Almost periodic solutions of retarded SICNNs with functional response on piecewise constant argument / Neural Comput. Appl. 2015. – Vol. 27. –P. 2483-2495.
10. Feˇckan M. Existence of almost periodic solutions for jumping discontinuous systems / Acta Math. Hungar. 2000. – Vol.86, N. 4. –P. 291-303.
11. Frigon M., O'Regan D. First order impulsive initial and periodic problems with variable moments / J. Math. Anal. Appl. 1999. – Vol. 233, N.2. – P. 730-739.
12. Hakl R. Almost periodic evolution systems with impulse action at state-dependent moments / J. Math. Anal. Appl. 2017. – Vol. 446, N.1. –P. 1030-1045.
13. He M.X., Chen F.D., Li Z. Almost periodic solution of an impulsive differential equation model of plankton allelopathy / Nonlinear Anal. RWA. 2010. – Vol. 11, N.4. – P. 2296-2301.
14. Liu J., Zhang Ch. Existence and stability of almost periodic solutions for impulsive differential equations / CUBO. Math. J. 2013. – Vol. 15. –P. 77-96.
15. Jiang G., Lu Q., Qians L. Chaos and its control in an impulsive differential system / Chaos Solit. Fract. 2007. – Vol 34, N.4. – P. 1135-1147.

16. Akhmet M.U. Li-Yorke chaos in the system with impacts / J. Math. Anal. Appl. 2009. – Vol. 351, N.2. – P. 804–810.

17. Li C., Liao X., Zhang R. Impulsive synchronization of nonlinear coupled chaotic systems / Phys. Lett. A. 2004. – Vol. 328, No.1. – P. 47-50.

18. Li P., Li Z., Halang W.A., Chen G. Li-Yorke chaos in a spatiotemporal chaotic system / Chaos Solit. Fract. 2007. – Vol. 33, N. 2. – P.335-341.

19. Birkhoff G.D., Dynamical Systems / G.D. Birkhoff. – New York: American Mathematical Soc. 1927. – P. 305.

20. Akhmet M., Fen M.O. Unpredictable points and chaos / Commun. Nonlinear Sci. Nummer. Simulat. 2016. – Vol. 40. – P. 1-5.

21. Akhmet M., Fen M.O., Alejaily E.M. Dynamics with Chaos and Fractals / M. Akhmet, M.O. Fen, E.M.Alejaily. – Berlin: Springer-Verlag, 2020. – P. 226.

22. Miller A. Unpredictable points and stronger versions of Ruelle–Takens and Auslander–Yorke chaos / Topology Appl. 2019. – Vol. 253. –P. 7-16.

23. Thakur R., Das R. Strongly Ruelle-Takens, strongly Auslander-Yorke and Poincar´echaos on semiflows / Commun Nonlinear Sci Numer. Simulat. 2019. – Vol.81. 05018.

24. Akhmet M., Fen M.O. Non-autonomous equations with unpredictable solutions / Commun. Nonlinear Sci. Numer. Simulat. 2018. – Vol. 59. –P. 657-670.

25. Akhmet M., Fen M.O., Tleubergenova M., Zhamanshin A. Unpredictable solutions of linear differential and discrete equations / Turk. J. Math. 2019. – Vol 43. – P. 2377-2389.

26. Akhmet M., Tleubergenova M., Zhamanshin A. Quasilinear differential equations with strongly unpredictable solutions / Carp. J. Math. Issue 3/2021.

РАЗРАБОТКА СИСТЕМЫ ПИТАНИЯ, АЛГОРИТМА УПРАВЛЕНИЯ И АРХИТЕКТУРЫ ВЕРБАЛЬНОГО РОБОТА

Амиргалиев Е.Н, Сундетов Т.Р, Кунелбаев М.М.
Институт информационных и вычислительных технологий КН МОН РК, Казахстан
e-mail: sundetovtalgat@gmail.com

Аннотация. *В данной статье рассмотрена разработка системы питания, алгоритма управления и архитектуры вербального робота. Робот основан на общедоступном 3D печатном принтере. В этом исследовании была разработана архитектура общей программной системы вербального робота, а так же усовершенствована система питания и алгоритм управления целой системы. С помощью оборудования Jetson Tx1 и сенсорным экраном для взаимодействия с InMoov был сделан интерфейс для управления всей системы. Датчик Kinect играет главную роль в прогрессе изучения данной темы. По сравнению с существующими гуманоидными роботами в вербальном роботе развита автоматизированная платформа, низкая стоимость и полностью функциональна.*

1. Введение

Гуманоидные роботы имеют подобный человеку дизайн и в состоянии подражать человеческим движениям [1]. Среди гуманоидных роботов с двойными манипуляторами и ловкими руками имеет большое значение обслуживания. Они могут предоставить компаньона, операцию, манипуляцию, погрузочно-разгрузочные работы и много других услуг людям. Исследование гуманоидных роботов всегда - самая активная область в интеллектуальной робототехнике и многих крупных учреждениях научного исследования. Много гуманоидных роботов было построено за прошлые несколько лет, таких как ASIMO [2,3,4], HPR[5], WABIANRV[6].

2. Дизайн аппаратных средств автоматизированного вербального робота на платформе “Inmoov”

На рисунке 1а,б показана схема разработанного 3D печатного недорогого вербального робота. Высота робота составляет приблизительно 170 см, который похож на нормальную высоту взрослого человека. Данный робот состоит из двух частей: 3D печатная передняя часть вербального робота, 3D печатная задняя часть вербального робота и мобильная основа. Мобильную основу изготовляют из железа и стимулируют три двигателя по 750 Вт. Для вербального робота в натуральную величину с сильной подвижностью это очень экономически эффективно.

Как показано в таблице 1, вербальный робот имеет 50 степеней свободы, 27 двигателей, 25 сервоприводов с различными нагрузками и 3 двигателями центра, специально предназначенные для электрического управления системы 24 В, 16Ah литиевый батарейный блок установлен в мобильной основе, и обеспечивает все электрическую роботу робота.

Таблица 1- Степени своды вербального робота

Часть	Степени свободы	Моторы
Правая и левая рука	30	10
Запястье	2	2
Локоть	2	2
Плечо	6	6
Голова	3	3
талия	1	2
Передвижная база	6	3

Преимуществ колесного робота более быстрое, более стабильное, легкое управляемое, более эффективное и может предоставить больше полезного груза в внедрении, больше степени свободы позволяет эффективно двигается диагонально, направо, налево и вперед, назад.

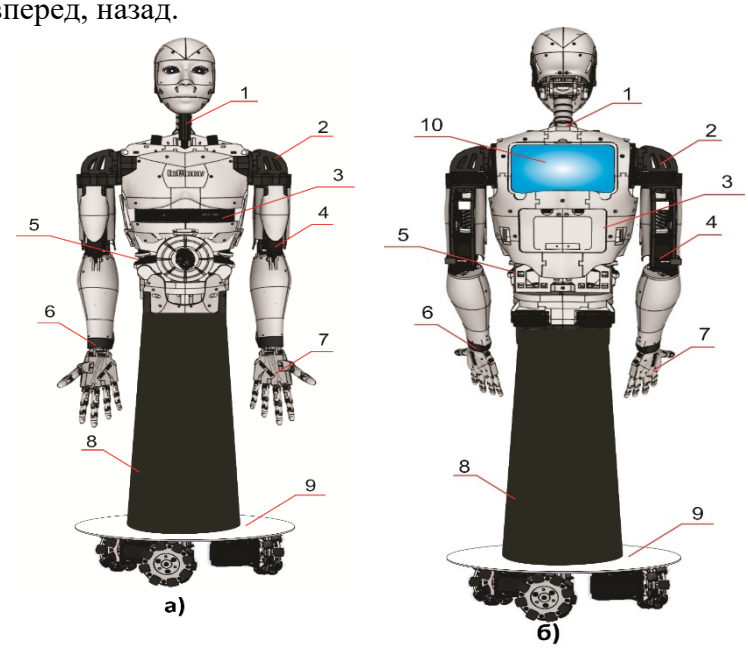


Рис.1.а) 3D печатная передняя часть вербального робота; б) 3D печатная задняя часть вербального робота

Вербальный робот состоит из 1-головная часть, 2- плечо, 3- устройство для распознавания лица, 4- локоть, 5- туловище, 6- кисть, 7- руки, 8- платформа для управления всей системы, 9- всенаправленная мобильная платформа, 10- сенсорный экран.

Мобильная платформа содержит три универсальных колеса, каждое колесо расположено по 120 градусов между собой, чтобы сделать робот статическим и с тремя отличительными колесами двигателя, чтобы заставить робот перемещаться.

2.1 3D печатная передняя часть вербального робота

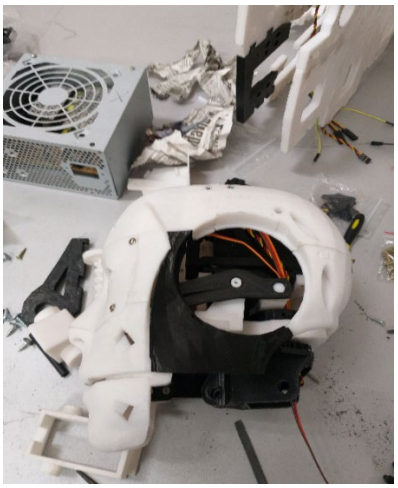
Передняя часть тела робота - абсолютно 3D печатное использование (PLA) пластик, который является своего рода биоразлагаемой пластмассой и не имеет никакого острого запаха. У 3D принтера, который мы использовали, есть рабочая зона 200*200*300 мм, удовлетворяющая требования робота “InMoov”. Левая и правая модульная рука имеет пять пальцев и сустав запястья. У пальцев есть 15 степеней свободы (DOF), и их ведут пять сервоприводов-MG996R через провод. Каждый палец пронизывает два провода, один провод управляют числом, чтобы возвратиться к прямому, и другой провод управляют числом, чтобы согнуться. Поскольку есть 15 DOFs левых и правых ловких ручных модулей, они находятся под приводимой в действие механической системой. Когда левая или правая рука захватит объект, палец будет конвертировать объект автоматически. Для сустава запястья другого сервопривода MG996R необходим, чтобы управлять назад и вперед вращение.

а)

б)

Рис.2. а) Правая рука вербального робота; б) Левая рука вербального робота

а)



б)

С)

Рис.3. а) Левая сторона головы вербального робота; б) Правая сторона головы вербального; с) Передняя часть головы вербального робота

Как видно из рисунка 3, голова вербального состоит из четырех моторов, который позволяет двигать глаз направо и налево, а также верх и вниз. Рот и голова поворачивается направо и налево с общими 7 степенями свободы. Левое плечо у модуля коленчатого соединения есть 4 DOFs, и это ведет к высокотехнологичному сервоприводу HS-805BB. Модуль плеча и коленчатого соединения симметричен с левым плечом и с модулем коленчатого соединения. Главный модуль и модуль талии рассматриваются как один модуль в нашем “Inmoov” роботе, потому что они связаны с тем же пультом управления. У главного модуля есть 3 DOFs, в то время как модуль талии может управлять роботом “Inmoov”, чтобы наклонить приблизительно 20 градусов.

2.2 Бортовое оборудование

Как показано на рисунке 4 бортовое оборудование установлено в автоматизированной системе. Помимо вложенного Мега Ардуино, используется шесть модулей “Inmoov” вербального робота, чтобы изучить человеческие проблемы взаимодействия робота.

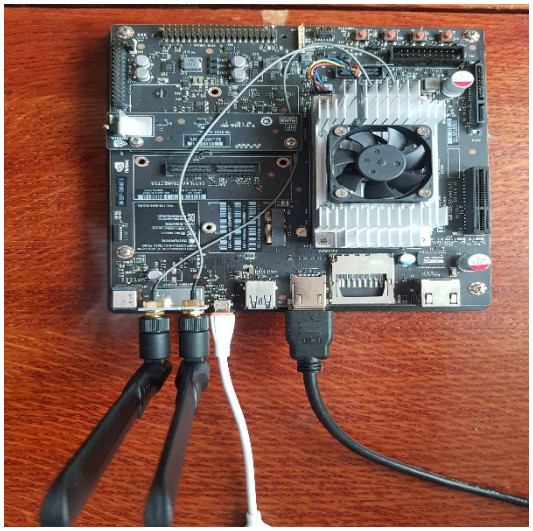


Рис.4. Бортовое оборудование

Чтобы увеличить способность к обработке, Jetson tx-1 центральный процессор с 32G памяти, 128G твердотельным диском установлен в конце робота. PC, управляющий Linux и Robot Operating System (ROS), может общаться с Мега Ардуино через последовательный интерфейс.

Рис. 5. Датчик Microsoft Kinect

Датчик Microsoft Kinect включен в живот робота, чтобы ощутить условия эксплуатации и взаимодействовать с людьми. Kinect, соединяются с Jetson tx-1. Существующими библиотеками ROS, такими как запуск openni пользуются, чтобы получить информацию о датчике. 7-дюймовый сенсорный экран установлен в зади, чтобы обеспечить дополнительную обратную связь и способность к взаимодействию.

2.3 Электрическое соединение вербального робота

На борту оборудования приведены в действие на 24 В, 16Ah литиевый батарейный блок. Управление батареей и единицы выключателя установлены на мобильной основе. У оборудования есть различная номинальная мощность и требования. Сервоприводы и Ардуино - приведенных в действие 6 В, но они должны быть изолированы друг от друга. Kinect требует 12-вольтового источника питания. Jetson tx-1 нужен 19-вольтовый источник питания. Кроме того, чтобы обеспечить безопасность и стабильность Jetson tx-1 и сенсорного экрана, 24-вольтовый DC к инвертору установлен на 220 В. Блок-схема системы управления питанием показано на рисунке 6.

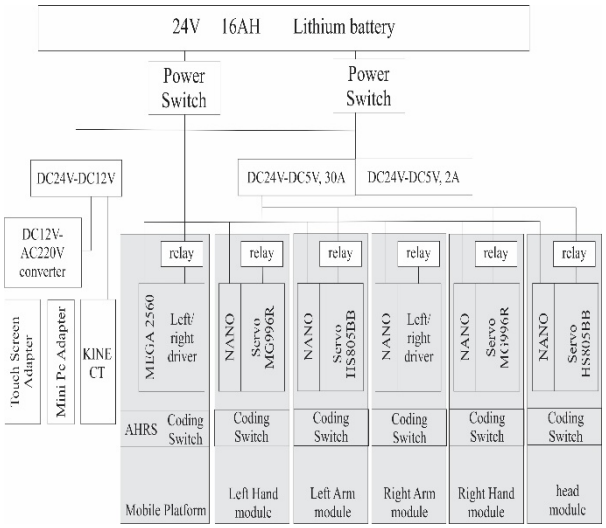


Рис. 6. Блок-схема системы управления питанием

3. Структура программного обеспечения вербального робота

Чтобы согласовываться с аппаратными средствами, данное программное обеспечение разработано в модульности. Модульным приводом легко управлять и поддерживать. У шести модулей есть шесть пультов управления, и все эти шесть модулей связаны и используется в RS485 для связи с основным Ардуино Мега 2560.

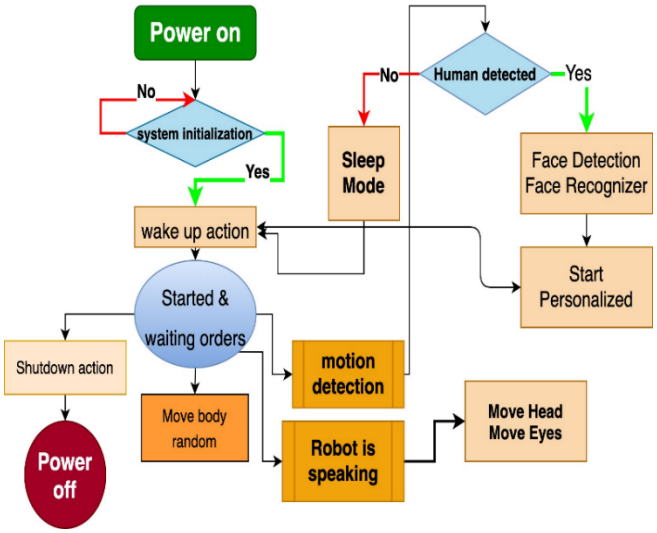


Рис. 7. Алгоритм управления вербального робота

Как мы видим из рисунка 8, при включении робота, система начинает инициализироваться. После вся система подключается к модулям робота с 28 степенями свободы начинает двигается хаотичным образом и параллельно в платформе для управления всей системы будет голосовое сопровождение, а также параллельно будет считывать данные датчика движение. Если есть движение, тогда устройство для распознавания лица распознает движущийся облик человека. Далее начинается персонализация человека и будет вести диалог с человеком и создается база данных каждому человеку с которым общался робот. После завершения диалога данные отправляются в двигательную систему. Если датчик не распознает движение, тогда робот переходит в режим сна. После режима сна в определенное время система вся отключается.

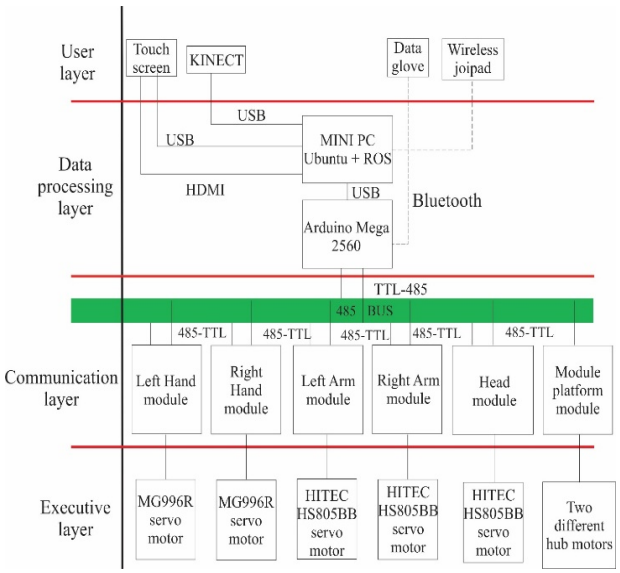


Рис. 8. Программная архитектура вербального робота "INMOOV"

Рисунок 8 показывает предложенную структуру программной архитектуры вербального робота. Программное обеспечение разделен на четыре слоя, пользовательский слой, слой обработки данных, коммуникационный слой и исполнительный слой. Пользовательский слой включает функцию, непосредственно взаимодействующую с оператором робота, сенсорным экраном, датчиком Kinect.

4. Выводы

В данной статье было предложено полностью функциональный недорогой 3D печатный вербальный робот с помощью“InMoov”. Робот основан на общедоступном 3D печатном вербальном роботе “InMoov”. Разработан диспетчер в механических деталях и электрическая система питания, который делает все части взаимозаменяемыми. Jetson-tx1 исследует новый тип программной технологии робота. У вербального робота есть подобное человеку структура, а так же есть множество интерактивных образцов. Человек может общаться с сенсорным экраном и датчиком Kinect. Датчик Kinect играет главную роль в прогрессе изучения. У робота есть два мобильных манипулятора с DOFs.

Литература

1. N. Rodriguez, G. Carbone, and M. Ceccarelli, “Antropomorphic design and operation of a new low-cost humanoid robot,” in Biomedical Robotics and Biomechatronics, 2006. BioRob 2006. The First IEEE/RAS-EMBS International Conference on, Feb 2006, pp. 933– 938.

2. K. Hirai, M. Hirose, Y. Haikawa, and T. Takenaka, “The development of honda humanoid robot,” in Robotics and Automation, 1998. Proceedings. 1998 IEEE International Conference on, vol. 2, May 1998, pp. 1321–1326 vol.2.

3. Y. Sakagami, R. Watanabe, C. Aoyama, S. Matsunaga, N. Higaki, and K. Fujimura, “The intelligent asimo: system overview and integration,” in Intelligent Robots and Systems, 2002. IEEE/RSJ International Conference on, vol. 3, 2002, pp. 2478–2483 vol.3.

4. S. Okita, V. Ng-Thow-Hing, and R. Sarvadevabhatla, “Learning together: Asimo developing an interactive learning partnership with children,” in Robot and Human Interactive Communication, 2009. ROMAN 2009. The 18th IEEE International Symposium on, Sept 2009, pp. 1125–1130.

5. K. Kaneko, F. Kanehiro, S. Kajita, K. Yokoyama, K. Akachi, T. Kawasaki, S. Ota, and T. Isozumi, “Design of prototype humanoid robotics platform for hrp,” in Intelligent Robots and Systems, 2002. IEEE/RSJ International Conference on, vol. 3, 2002, pp. 2431–2436 vol.3.

6. G. Carbone, H. ok Lim, A. Takanishi, and M. Ceccarelli, “Numerical and experimental estimation of stiffness performances for the humanoid robot wabian-rv,” in Advanced Intelligent Mechatronics, 2003. AIM 2003. Proceedings. 2003 IEEE/ASME International Conference on, vol. 2, July 2003, pp. 962–967 vol.2.

НАЧАЛЬНОЕ ПРИБЛИЖЕНИЕ ПРИ ПОИСКЕ ОПТИМАЛЬНОГО РЕШЕНИЯ В ТЕМАТИЧЕСКОМ МОДЕЛИРОВАНИИ КАК ЗАДАЧЕ МАТРИЧНОГО РАЗЛОЖЕНИЯ

Мусабаев Р.Р., Козбагаров О.Б.
rmusab@gmail.com, o.kozbagarov@iict.kz
Институт информационных и вычислительных технологий КН МОН РК, Казахстан

***Аннотация*:**
В данной статье описан подход по выбору начального приближения при поиске оптимального решения методом простых итераций в тематическом моделировании как задаче матричного разложения исходной матрицы частот употребления слов в текстовых документах на две матрицы. Первая матрица разложения определяет уровень отношения множества слов к каждой тематике; вторая – множества тематик к каждому документу. Выбор начального приближения согласно данному подходу, то есть начальной инициализации ненаблюдаемых значений двух вышеуказанных матриц, обеспечивает более быструю сходимость (за меньшее число итераций) к максимуму функции правдоподобия между исходной матрицей наблюдаемых частот и произведению двух ненаблюдаемых матриц. Нахождение начального приближения основывается на использование отдельной тематической модели, которая построена только на основе употреблении слов в текстовой коллекции без каких-то либо дополнительных допущений, в частности без использования вероятностного аппарата. То есть построение начального приближения основывается только на том, как слова взаимосвязаны друг с другом в коллекции документов, то есть на природе самих данных. В статье данный подход рассматривается в отношении новостных публикаций на русском языке и на их основе проведена оценка сходимости к максимуму функции правдоподобия. Дополнительно, в статье продемонстрировано, что подход практически реализуем в отношении “больших данных”.

Ключевые слова: *обработка текстов естественных языков, тематическое*

моделирование, “нечеткая” кластеризация, “большие данные”, текстовый корпус, разложение матриц

1. Введение

Тематическое моделирование – активно применяемое на практике и широко используемое направление статистического анализа текстов. Тематические модели используются для информационного поиска, классификации, категоризации, аннотации документов и пр. Тематическая модель выявляет к каким темам относится документ и какие слова (термины) образуют каждую тему путем построения двух матриц: одна матрица определят уровень отношения тематик к каждому документу; вторая матрица определяет отношения слов к каждой тематике, где под тематикой понимается дискретное вероятностное распределение слов (терминов) заданное на множестве всех слов (словаре).

Одной из первых тематических моделей была модель латентного семантического анализа (Latent semantic analysis, LSA, Deerwester 1990), основанная на сингулярном разложении матриц [1]. В 1999 году Томасом Хофманном была предложена модель вероятностного семантического анализа (Probablistic latent semantic analysis, PLSA), которая раскладывает исходную матрицу частот на произведение двух ненаблюдаемых матриц [2]. Неизвестные матрицы подбираются так, что они максимизируют функцию правдоподобия между наблюдаемой матрицей и произведением ненаблюдаемых матриц, что эквивалентно минимизации разницы между наблюдаемой матрицей и произведением двух матриц по норме - средневзвешенная дивергенция Кульбака-Лейблера [4]. Данное разложение не единственно и может иметь бесконечное число решений, поэтому полученные решения не устойчивые в том смысле, что два различных полученных решения могут определять совершенно непохожие друг на друга тематики. В 2003 году Дэвидом Блеем была предложена модель латентного размещения Дирихле (Latent накладывается дополнительное вероятностное предположение о том, что распределения слов в каждой тематике и тематик в каждом документе имеет распределение Дирихле. Данное предположение не имеет лингвистического обоснования, но удобно тем, что при малых значениях параметров распределения Дирихле, распределение слов в тематике будет обладать свойством, что относительно большие вероятности присваиваются лишь значительно малому подмножеству слов (в то же время другим присваиваются близкие к нулю, но ненулевые значения, что является недостатком). На сегодняшний день LDA является одной из частой используемой, самой популярной на практике моделью; много различных модификации данной модели были разработаны. В 2014 году Константин Воронцов предложил новый подход к построению тематических моделей, названный аддитивной регуляризацией тематических моделей (ARTM) [4]. Согласно данному подходу выбор регуляризатора, доопределяющего неизвестные значения элементов двух матриц, задает определенную тематическую модель. Было показано, что при выборе конкретного регуляризатора получается тематическая модель, которая идентична LDA; в случае же отсутствия регуляризаторов получается тематическая модель PLSA. Достоинство подхода в том, что не требуется задействовать трудоемкий вероятностный аппарат в виде байесовского вывода для разработки тематической модели. Достаточно заложить в выборе регуляризатора

продиктованные практическими целями ограничения на решения. Также достоинством подхода является то, что любые комбинации различных требуемых ограничений на значения неизвестных матриц выражаются просто через аддитивное добавление регуляризаторов друг к другу. Выбор регуляризатора может обеспечить большую интерпретируемость получаемых тематик, также позволяет получать тематики характеризующиеся разреженностью и сглаженностью [4]. Тематическая модель, полученная на основе подхода ARTM с заданными регуляризаторами, обеспечивающими сглаженность фоновых тематик и разреженность специфичных тематик, является state-of-the-art и превосходит LDA [5].

В подходе ARTM на практике значения ненаблюдаемых элементов двух матриц находятся численным методом - методом простых итераций. Данный метод позволяет получить численное решение системы уравнений, где система уравнений – это условия Каруша-Куна-Таккера для задачи математического программирования (максимизации функции правдоподобия с заданными ограничениями). Данная система уравнений является необходимым условием для локального экстремума. Метод простых итераций требует задания начального приближения (начальной инициализации) для выполнения итеративного процесса и получения решения; при разном выборе начального приближения могут получаться различные решения. Обычно на практике в качестве начального приближения берутся матрицы, элементы которой выбраны случайном образом (тематики присваиваются словам в документе по равномерному распределению), что не может иметь никакого лингвистического обоснования в случае тематического моделирования. В данной статье предлагается подход по выбору начального приближения, которое строится на основе природы данных, а именно на основе того как слова употребляются в коллекции текстовых документов. Взаимное употребление слов друг с другом позволяет выявить скрытые тематики, заложенные в текстовой коллекции и тем самым построить отдельную тематическую модель. Данная тематическая модель не использует в основе никаких вероятностных допущений о том, как происходит генерация текста, что является ее достоинством. Так согласно утверждению А. Н. Колмогорова, создателя современной теории вероятности, который в книге "Теория информации и теория алгоритмов (1987)" писал «Представляется важной задача освобождения всюду, где это возможно, от излишних вероятностных допущений». Результат работы данной тематической модели, в частности, может служить в качестве начальной инициализации двух матриц (определяющих связанность тематик с словами и с документами), структура которых не случайна, а продиктована текстовой коллекцией и имеет естественное обоснование. Данное приближение можно использовать в подходе ARTM для более быстрой сходимости методом простых итераций.

2. Получение неизвестных матриц на основе ARTM

В ARTM функция правдоподобия при заданных регуляризаторах имеет следующий вид [4]:

$$L(D,\Phi,\Theta,R) = \sum_{d\epsilon D} \sum_{w\epsilon d} n_{dw}\, ln \sum_{t\epsilon T} \varphi_{wt}\theta_{td} + R(\Phi,\Theta) \;\rightarrow \max_{\Phi,\Theta} \qquad (1)$$

Матрицы Φ,Θ определяют отношение слов к тематикам и тематик к документам соответственно; n_{dw}частота слова w в документе d.На элементы данных матриц накладываются следующие ограничения:

$$\varphi_{wt} \geq 0, \sum_{w \epsilon W} \varphi_{wt}, \theta_{td} \geq 0, \sum_{t \epsilon T} \theta_{td}$$

Система уравнений (условия Каруша-Куна-Таккера), которая задает необходимые условия для локального экстремума для вышеуказанной задачи математического программирования следующая:

$$p_{tdw} = \frac{\varphi_{wt}\,\theta_{td}}{\sum_{t \epsilon T} \varphi_{wt}\,\theta_{td}}$$

$$\varphi_{wt} = norm\left(n_{wt} + \varphi_{wt}\frac{\partial R}{\partial \varphi_{wt}}\right)_{+}; \quad n_{wt} = \sum_{d \epsilon D} n_{dw} p_{tdw}; \tag{2}$$

$$\theta_{td} = norm\left(n_{td} + \theta_{td}\frac{\partial R}{\partial \theta_{td}}\right)_{+}; \quad n_{td} = \sum_{w \epsilon d} n_{dw} p_{tdw};$$

где n_{dw} – частота слова w в документе d.

На практике решение данной системы происходит с помощью численного метода - методом простых итерации [5]. Для работы данному методу необходимо задать начальное приближение решению. Система уравнений может иметь бесконечное число решений, поэтому выбор различных начальных приближений может приводить к совершенно различным решениям – локальным экстремумам. Обычно приближение выбирается случайным образом, что в случае тематической модели не имеет лингвистического обоснования. Далее будет показан подход для получения начального приближения, который основывается на тематической модели, построенной на употреблении слов в коллекции и на алгоритме кластеризации. Данное начальное приближение естественным образом отражает тематики, скрытые в документах коллекции и служит обоснованной отправной точкой.

3. Тематическая модель на основе употребления слов

Далее будет описана разработанная тематическая модель. Построение модели состоит из нескольких этапов.

Первый этап: составление словаря

Первоначальная задача стоит в определении всех слов, из которых составлены тексты корпуса. Для этого формируется словарь слов. В словарь обычно не включаются высокочастотные слова, служащим только функциональным целям, так называемые stopwords. Также можно исключить из рассмотрения очень редкие слова. Дополнительно можно произвести уменьшение размерности словаря, рассмотрев только определенные части речи, например, имена существительные (включая именные сущности), используемые в рассматриваемых текстах. Выбор размера словаря зависит от располагаемых вычислительных ресурсов. В итоге выбранное множество слов будет представлять из себя сформированный словарь слов (целевых единиц анализа).

Второй этап: группировка слов словаря согласно их тематической связанности

В основе разработанной модели лежит следующее допущение: контекст определяет тематическую/смысловую близость слов. То есть чем ближе по составу контекстное окружение сравниваемых слов, тем больше их тематическая/семантическая близость. И действительно, очевидно, что слова-

синонимы должны иметь одинаковый состав контекстного окружения. И наоборот, чем меньше смысловая связанность слов, тем сильнее различается их контекст. Под контекстным окружением понимается «мешок слов» составляющий фрагмент текста с анализируемым словом. Тонкая оценка близости контекстов даёт оценку семантической (смысловой) близости, а относительно грубая – тематической близости. Таким образом, под тематикой можно понимать относительно грубую оценку связанности анализируемых контекстов.

На втором этапе происходит группировка всех слов словаря согласно их тематической связанности. Здесь под тематикой понимается, как указано выше, совокупность сочетаний слов, которые либо используются часто в одном и том же контексте, либо используются постоянно в одних и тех же текстах с повторяющейся частотой совместного употребления.

Для группировки слов по тематике первоначально формируется матрица взаимной встречаемости слов в текстах корпуса, размерностью равной числу текстов на длину словаря. Элементы данной матрицы равны частоте встречаемости соответствующих слов в текстах, при этом считается, что два слова встречаются, если они использованы в одном и том же тексте в независимости от места расположения в нем по отношению друг к другу, то есть текст рассматривается как «мешок слов». Для получения векторного представления слов словаря транспонированную матрицу умножим на матрицу.

$$V = X^T \cdot X \qquad (3)$$

В результате получим квадратную симметричную матрицу с размерностью равной длине словаря на длину словаря, где каждая строка или столбец есть векторное представление отдельного слова словаря. Данное векторное представление слова характеризует контекстную связанность данного слова с другими словами словаря в отношении встречаемости в текстах корпуса. Векторные представления слов, имеющих одинаковый уровень связанности с другими словами и тем самым, с большой вероятностью относящихся к одной тематике, будут схожими и значение косинусной близости у них будет выше по сравнению с другими. Таким образом, рассчитав матрицу косинусных расстояний векторов слов (строки матрицы) словаря по формуле,

$$D = 1 - cos(V_1, V_2) = 1 - \frac{V_1 \cdot V_2}{||V_1|| \cdot ||V_2||} \qquad (4)$$

применим к ней алгоритм последующей кластеризации. Так как одно слово потенциально может относиться к нескольким различным тематикам, то необходимо применять алгоритм “нечеткой” кластеризации, где в результате каждое слово может попасть не только в один кластер, как в случае применения алгоритма “четкой” кластеризации. В результате применения алгоритма получим кластера из тематически/семантически связанных слов, при этом слова в зависимости от значений, в которых они употребляются, могут попасть в несколько кластеров (групп слов), а не исключительно только в один кластер.

Алгоритм “нечеткой” кластеризации

В качестве алгоритма “нечеткой” кластеризации выбран алгоритм, у которого минимальное число параметров, который строит кластера, основываясь на

расстояниях между элементами, который не требует задания итогового числа кластеров в виде параметра, так как заранее их число неизвестно, который также предполагает возможность реализации процесса работы алгоритма на основе параллельных вычислений и обеспечивает относительно быструю работу алгоритма по отношению к работе с большими данными.

Применяемый алгоритм “нечеткой” кластеризации для каждого элемента (слова) определяет элементы, находящиеся в заданной окрестности с радиусом *d*. Далее формирует множество, состоящее из элементов окрестности (включая центр окрестности) такое, что попарные расстояния между всеми элементами множества не превышают *d*. Формирование множества происходит следующим образом: берется центр окрестности и самый ближайший к нему элемент из окрестности; они формируют начальное состояние множества. Далее находится элемент из окрестности ближайший к сформированному множеству; если расстояние найденного элемента до каждого элемента из построенного множества меньше *d,* то оно добавляется в множество, в противном случае удаляется из окрестности. Процесс формирования множества продолжается, пока окрестность не станет пустой.

Данный алгоритм, согласно своему механизму работы, позволяет любому элементу, то есть слову, относиться к разным построенным множествам, то есть кластерам одновременно. Относительно высокое значение *d* приводит к более длительной работе алгоритма, так как из-за увеличения радиуса окрестности увеличивается число возможных элементов для формирования кластера.

Третий этап: агрегирование полученных кластеров для получения тематических категорий

Так как число полученных на втором этапе кластеров может быть очень высоким (максимально равным числу слов в словаре) и многие множества могут быть похожими, то для того, чтобы обеспечить уникальность получаемых тематик требуется произвести объединение кластеров слов, которые близки друг к другу. То есть объединим кластера слов, большая доля слов которых семантически/тематически друг с другом близкие. Объединение кластеров слов происходит через попарное определение уровня связанности кластеров по формуле:

$$Similarity(A,B) = \frac{\sum_{a\epsilon A}\sum_{b\epsilon B} w_a w_b \, d(a,b)}{\sum_{a\epsilon A}\sum_{b\epsilon B} w_a w_b} \qquad (5)$$

где *d(a,b)* – косинусное расстояние между векторами слов *a* и *b, w* – веса слов в кластере (обратно пропорционален расстоянию от слова до всех слов кластера; чем меньше суммарное расстояние (более центральным является слово для кластера), тем выше вес слова). Все кластера, у которых попарные отношения превосходят заданный пороговый уровень, объединяются в один. Причем происходит объединение кластеров не только напрямую связанных, но и косвенно. Например, если кластер имеет уровень связанности с другим кластером выше порогового уровня, который в свою очередь имеет уровень связанности с третьим кластером тоже выше порогового уровня, причем уровень связанности первого и третьего ниже порогового уровня, то несмотря на это, все три кластера будут объединены в один. Таким образом, для объединения кластеров требуется найти все попарные значения

по формуле 5 между всеми кластерами и определить прямую и косвенную связанность кластеров.

Процесс изменения значений порогового уровня позволяет получить механизм для регулировки итогового числа кластеров по результатам процесса объединения.

В дальнейшем полученные агрегированные кластера слов будем называть **тематическими категориями.**

Четвертый этап: определение матрицы слова на тематики

Определенные на третьем этапе тематические категории являются образованными тематиками. Для каждого слова из словаря найдем сумму близости (близость двух слов есть 1 – расстояние между векторами данных слов) данного слова к каждому слову, составляющих каждую отдельную тематическую категорию. Вычисленная сумма пропорциональна уровню связанности данного слова по отношению к данной тематической категории. Чем выше значение суммы, тем выше близость данного слова к данной тематике. Составим матрицу с размерностью равной размеру словаря на число тематических категорий, где элементом матрицы будет рассчитанная близость конкретного слова к конкретной тематической категории. Далее пронормируем каждый столбец так чтобы сумма всех элементов столбца равна единице, то есть столбец это дискретное распределение слов для тематики. Таким образом, каждая строка данной матрицы показывает уровень отношения слова к каждой отдельной тематике.

Пятый этап: определение матрицы документы на тематики

Для каждого документа, представленного как мешок слов, найдем уровень его семантической связи с каждой тематической категорией по формуле (5). На основе рассчитанных значений для каждого документа и каждой тематической категории построим матрицу с размерностью равной числу документов на число тематических категорий. Элементом матрицы будет уровень связанности отдельного документа с отдельной тематикой. Далее пронормируем каждую строку, чтобы сумма элементов строки была равно единице, то есть строка матрицы есть дискретное распределение тематик для каждого отдельного документа.

Полученные на четвертом и пятом этапах матрицы являются результатом работы любой тематической модели, готовые для дальнейшей работы, анализа, нахождения тематически близких документов, визуализации и пр. В частности, можно использовать полученные матрицы как начальную инициализацию решения в подходе ARTM.

5. Экспериментальные условия

Описание корпуса

Для проведения эксперимента по апробированию подхода был рассмотрен корпус новостных публикаций. Новости представлены на русском языке. Число новостей составляет 186 183.

Предобработка и первый этап разработанного подхода: формирование словаря

Для уменьшения размерности словаря рассмотрели только имена существительные (включая именные сущности), используемые в рассматриваемых текстах. Слова публикаций корпуса были получены токенизацией текстов (библиотека *nltk* в *python*), была удалена пунктуация, далее слова были

лемматизированы и был осуществлен их морфологический анализ (библиотека *pymorphy2* в *python*). В итоге получили все имена существительные (включая именные сущности). Из полученного множества слов были удалены высокочастотные слова (перечень русских высокочастотных слов был взят с библиотеки *nltk*) и слова, которые встречаются реже, чем в 10 публикациях и более, чем в 25% документах. Все полученное множество слов образовало словарь. В итоге словарь состоял из 17 842 слов имен существительных.

Второй этап: группировка слов словаря согласно их тематической/смысловой связанности

Первоначально была рассчитана матрица X, размерностью равной числу новостных публикаций 186 183 на размер словаря 17 842, где элементом матрицы является частота встречаемости слова в соответствующей публикации. Далее рассчитывались векторные представления каждого слова по формуле (3). В результате получилась квадратная и симметричная матрица V с размерностью равной 17 842 x 17 842. Каждая строка данной матрицы есть векторное представление слова. Затем рассчитывалась матрица расстояний между векторными представлениями слов с размерностью 17 842 x 17 842 по формуле (4) и к ней применялся алгоритм “нечеткой” кластеризации. Алгоритм “нечеткой” кластеризации при различных значениях параметра d (радиуса окрестности) рассчитывает различное число кластеров; чем выше d, тем выше число кластеров и больше времени требуется на работу алгоритма. Максимальное возможное число кластеров равно мощности словаря, в данном случае 17 842.

Третий этап: агрегирование полученных кластеров для получения тематических категорий

Агрегирование кластеров в тематические категорий осуществляется заданием значения порогового уровня, определяющим требуемый уровень минимальной взаимной общности кластеров, для их последующего объединения. Изменение значение данного параметра приводит к получению большего или меньшего итогового числа тематических категорий, где более низкие значения данного параметра обеспечивают меньшее итоговое число тематических категорий. Также дополнительным параметром для регулировки итогового числа тематических категорий служит наложение ограничения на необходимое минимальное число слов, которые составляют категорию. То есть те категории, которые не содержат достаточное число слов, далее не рассматриваются. Разные значения параметров влияют на итоговое число получаемых категорий, и оно разнится от десятка до нескольких тысяч.

Аггрегирование тематических категорий обеспечивает декоррелированость результирующих тематик, так как категорий, которые содержат слова тематически/семантически близкие друг другу, объединятся в одну категорию и две разные категории не будут связаны друг с другом. Дополнительно, если итоговое число слов, составляющих категорию, ограничивать сверху, то итоговые тематические категории будут обладать свойством разреженности.

Примеры полученных тематических категорий при d равным 0.37 (первая персентиль матрицы расстояний) и пороговым уровнем равным 0.7 приведены ниже. Первую категорию составляют слова, относящиеся к внешней политике США;

вторая к искусству, а именно опере и балету; третья к дорожным происшествиям, четвертая к погоде.

Содержание тематической категории
США, депеша, рекс, вашингтон, джон, госдеп, госдепартамент, обама, эрнест, союзник, хилари, пентагон, керри, конгресс, америка, госсекретарь, конгрессмен, барак
Онегин, филармония, цыганка, прима-балерина, опера, театр, альфий, скал, джузеппе, мухитдин, джульетта, ария, амарант, тоска, флейта, див, солист, контраст, станиславский, певцов, соната, григор, пианист, балет, балетмейстер, декорация, латиф, балерина, концертмейстер, гала, ромео, сопрано, модерн, галеев, жизель, оркестр, тенор, подмостки, фортепиано, луиджи, па-де-де, хор, хореограф, хореография, дирижёр, сценограф, сценография, хормейстер, бетховен, биза, виолончель, штраус, рубен, баритон, сюита, гастроль, меццо-сопрано, серенада, рудольф, сочинение, фриджерио, пуччини, репертуар, людвиг, худрук, пласидо, эсмеральда, пластика, ильдар, щелкунчик, произведение, спектакль, пьеса, сац, труппа, аттил, либретто, кармена, кихот, постановка, моцарт, постановщик, джакомо, композитор, адан, мими, генуя, верди, танцовщик, мудряк, миниатюра, минимализм, маэстро, богема, фигаро, богоматерь, музыковед, верона, тарлан, алтынай, гергиев, партитура
Джип, бок, лихач, кювет, кювета, пассажирка, поворот, повреждение, движение, разворот, багажник, погоня, полоса, салон, тормоз, приор, тяжесть, опор, уаз, обочина, бордюр, опрокидывание, ваза, нива, камаз, травма, бензобак, газель, опьянение, регулировщик, авария, маневрирование, фольксваген, педаль, пешеход, разметка, гаишник, помеха, прицеп, мерседес, ниссан, очевидец, жигули, угон, угонщик, бампер, манёвр, шофер, дтп, трасса, колесо, стекло, грузовик, виновник, бетономешалка, виновница, виновный, легковушка, авто, автоавария, капот, освидетельствование, наезд, автовладелец, ушиб, ограждение, автокатастрофа, ремень, автолюбитель, автомашина, автомобилист, автомобиль, днище, указатель, кузов, оставление, проезжий, столб, подушка, столкновение, тротуар, микроавтобус, руль, фара, перекрёсток, автотрасса, эвакуатор, фура, происшествие, пьяный, отбойник, неосторожность, дознаватель, ауди, сидение, дознание, внедорожник, спецмашина, промилле, зажигание, водитель, обгон, машина, тойота, светофор, минивэн, маз, инерция, маячок, пересечение, вождение, перестроение, иномарка
Метеослужба, похолодание, штиль, воздух, метеостанция, термометр, градус, отрог, гидрометцентр, погода, заморозок, столбик, фронт, север, тропосфера, жара, жарка, жаркое, мороз, ложбина, таймыр, нуль, дождь, позёмка, антициклон, декада, цельсий, юг, зима, гроза, прояснение, температура, вынос, холод, понижение, холодное, циклон, синоптик, заток, осадка, метеоролог
Младенец, плацента, акушер, акушерка, беременность, кормление, матерь, материнство, выкидыш, вскармливание, эмболия, роддом, патология, выписка, гинеколог, утроба, малыш, ребёнок, роды, роженица, сечение
Кабул, талиб, талибан, хамид, афганец, афганистан
Город, магистраль, линия, ветка
Яромир, авангард, зарип, салават, зиновьев, буллит, хоккеист, бросок, пережогин, даниса, атлант, овертайм, шайба
Сватовство, жених, замужество, калым

Офицер, взвод, батальон, рота, командир
Даун, синдром

Таблица 1: примеры образованных тематических категорий.

Четвертый этап: формирование матрицы распределения слов для каждой тематики

Для каждой полученной на третьем этапе тематической категории (выбрали категории, состоящие из не более 200 слов и не менее 10; в итоге число категорий равнялось 198) рассчитали сумму расстояний от каждого слова словаря до всех слов, составляющих каждую категорию по формуле (5). В результате получили матрицу с размерностью равной размер словаря на число тематик (17 842 x 198). Далее пронормировали каждый столбец полученной матрицы, чтобы сумма элементов каждого столбца равнялась 1.

Пятый этап: формирование матрицы распределения тематик для каждого документа

Для каждой полученной на третьем этапе тематической категории (выбрали категории состоящие из не более 200 слов и не менее 20, в итоге число категорий равнялось 198) рассчитали уровень ее связанности с каждым документом коллекции по формуле (5). В результате получили матрицу с размерностью равной числу документов на число тематик (186 183 на 198). Далее пронормировали каждую строку, чтобы сумма элементов каждой строки была равна единице.

Формирование начального приближения для метода простых итераций

Построенные матрицы на четвертом и пятом этапах используем как начальную инициализацию матриц Φ, Θ в методе простых итераций. После зададим число итерации (было выбрано 100 итераций) и на каждой итерации рассчитаем новые значения матриц Φ, Θ итеративного процесса (2). На каждой итерации вычислим значения функции максимального правдоподобия (1) (пропорционально перплексии). В таблице 2 приведены результаты, полученные при числе документов равному 1 000, 10 000.

	При начальной инициализации	к 10 итерации	к 90 итерации	к 100 итерации
Значения фукнции правдоподобия (**1 000** документов)	- 683 477	-402 464	- 354 801	- 354 678
Значения фукнции правдоподобия (**10 000** документов)	-7 072 607	-4 556 116	-4 164 093	-4 161 998

Таблица 2: значения функции максимального правдоподобия на k-итерации при начальной инициализации матриц Φ, Θ по разработанному подходу.

В таблице 3 приведены результаты при задании начального приближения

случайным образом.

	При начальной инициализации	к 10 итерации	к 90 итерации	к 100 итерации
Значения фукнции правдоподобия (**1 000** документов)	- 700 729	- 408 833	- 357 177	- 357 075
Значения фукнции правдоподобия (**10 000** документов)	-7 259 330	-4 986 240	-4 249 025	-4 244 172

Таблица 3: значения функции максимального правдоподобия на k-итерации при начальной инициализации случайным образом.

Сравнение полученных результатов при двух подходах к начальной инициализации матриц Φ, Θ показывает, что выбор начального приближения по разработанному подходу дает более высокое значение функции максимального правдоподобия вначале итеративного процесса и что меньшее число итерации требуется для итеративного процесса для преодоления заданного численного порога функции правдоподобия.

6. Заключение

В статье был представлен подход по выбору начальной инициализации в методе простых итерации для нахождения точки локального экстремума функции правдоподобия при работе с state-of-the-art подходом построения тематических моделей ARTM. Формирование начального приближения происходит на основе отдельной тематической модели, построенной на наблюдаемом употреблении слов друг с другом в текстовой коллекции и алгоритме нечеткой кластеризации, то есть на выявлении скрытых тематик в коллекции. Результаты показывают, что выбор приближения по описанному подходу обеспечивает более высокое значение функции правдоподобия на начальном этапе итеративного процесса и обеспечивает за меньшее числе итераций достижение численного порога функции правдоподобия, чем это происходит при случайной инициализации.

Отдельный интерес представляет, как именно начальная инициализация влияет непосредственно на качество получаемых итоговых тематик, ведь функция правдоподобия (пропорционально перплексии) не отражает этого. Поэтому в дальнейшем планируется провести работу по получения экспертной оценки качества получаемых тематик или по разработки метрики, которая позволит оценивать это автоматически.

Дополнительно планируется исследовать работу представленной тематической модели, рассмотреть вопрос о возможности ее совершенствования, в частности использовании модели ELMO и BERT для построения векторного представления слов; проанализировать свойства тематической модели; изучить какие значения параметров могут обеспечить более высокое значение функции максимального правдоподобия. Также планируется сравнить результаты, получаемые на различных корпусах и для разных языков.

Литература:

1. Deerwester S., Dumais S., Harshman R. Indexing by Latent Sematic Analysis. / - Journal of the American Society for Information Science, 1990. - p. 391-407.
2. Hoffman T. Probabilistic Latent Semantic Indexing. / - Proceedings of the 22nd annual international ACM SIGIR conference on Research and development in information retrieval, 1999. – p. 50–57.
3. Blei D., Ng A., Jordan M. Latent Dirichlet allocation. / - The Journal of Machine Learning Research, 2003.
4. Воронцов К.В. Аддитивная регуляризация тематических моделей коллекции текстовых документов. - Доклады РАН, 2014. - Т. 455., №3. стр. 268–271.
5. Воронцов К.В. Библиотека по тематическому моделированию. - http://bigartm.org

СИНТЕЗ СИСТЕМЫ УПРАВЛЕНИЯ НЕФТЕГАЗОВОЙ ОТРАСЛИ НА ОСНОВЕ ИСКУССТВЕННЫХ ИММУННЫХ СИСТЕМ И АЛГОРИТМА НЕГАТИВНОЙ СЕЛЕКЦИИ

Ширяева О.И.
e-mail: oshiryayeva@gmail.com
Казахский Национальный технический университет им.К.Сатпаева, Институт информационных и вычислительных технологий КН МОН РК, Казахстан

Аннотация. *Синтезирована система управления технологическими процессами нефтегазовой отрасли на основе алгоритмов искусственных иммунных систем, AIS. Представлены результаты применения алгоритма искусственных иммунных систем AIS с формированием начальных значений регуляторов на основе генетического алгоритма, GA, для решения задач оптимального управления. Получены результаты реализации алгоритма для решения проблемы поиска глобального минимума которой используется алгоритм негативной селекции, NSA.*

Ключевые слова. *Искусственные иммунные системы (AIS), алгоритм негативной селекции (NSA), нефтегазовая отрасль, синтез регуляторов.*

Эффективность использования методологии алгоритмов искусственных иммунных систем, AIS, для нахождения минимумов оптимизационных задач и синтеза типовых регуляторов, обуславливает перспективность развития данной методологии для управления процессами нефтегазовой отрасли. С целью решения задачи синтеза оптимальной сложной системы управления процессами дистилляционной колонны процесса очистки природного газа от различных примесей, в данной статье, используются алгоритмы AIS: алгоритм клональной селекции, CLONALG, в совокупности с алгоритмом негативной селекции, NSA[1,2].

Данная работа является продолжением использования алгоритмов GA, CLONALG [3,4] для синтеза систем управления, которые на данном этапе рассматриваются в совокупности с алгоритмом негативной селекции, NSA (рисунок

1), что позволяет решить проблему поиска глобального минимума, исключив локальные минимумы [5].

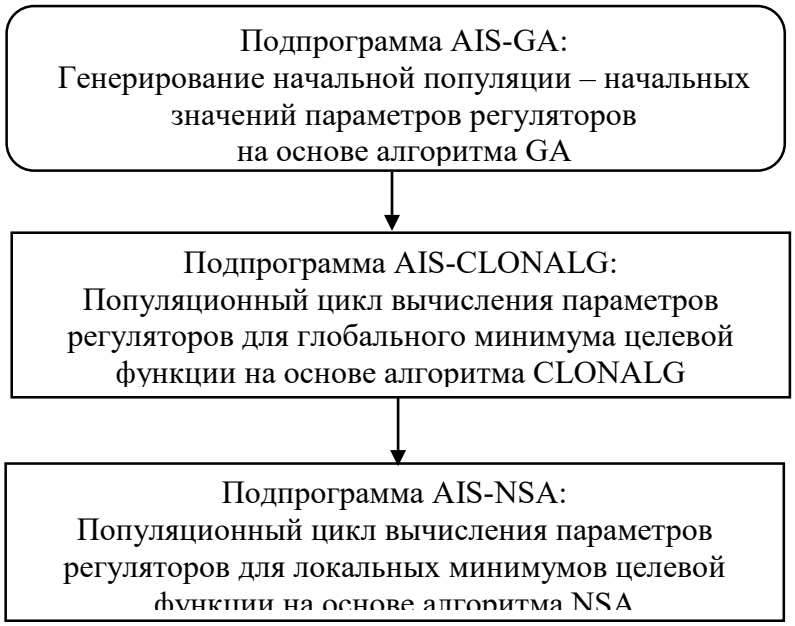


Рис. 1. Подпрограммы алгоритма AIS

В ходе реализации подпрограммы AIS-NSA, для нахождения минимального значения критерия качества системы, выполнены шаги, представленные на рисунке 2. На основе исключения найденных локальных минимумов, задача поиска глобального минимума на основе модифицированного алгоритма решается эффективнее.

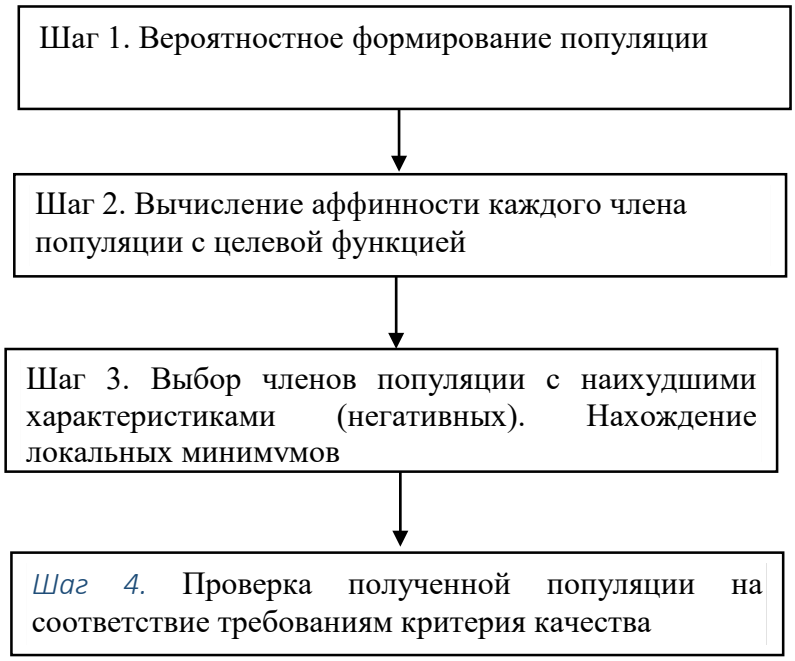


Рис. 2. Алгоритм подпрограммы AIS-NSA

Ab_{t+1}

Реализация алгоритма для решения задачи синтеза оптимальной системы управления технологическими процессами нефтегазовой отрасли проводится для объекта нефтегазовой отрасли – дистилляционной колонны процесса очистки природного газа от различных примесей [6]. Пусть $G_{11}(s), G_{12}(s), G_{21}(s), G_{22}(s)$ – передаточные функции дистилляционной колонны, связывающие входы и выходы двумерной системы:

$$\begin{vmatrix} y_1(s) \\ y_2(s) \end{vmatrix} = \begin{vmatrix} G_{11}(s) & G_{12}(s) \\ G_{21}(s) & G_{22}(s) \end{vmatrix} \cdot \begin{vmatrix} u_1(s) \\ u_2(s) \end{vmatrix}, \tag{1}$$

где $G_{11} = \dfrac{0.0042}{1.9588s+1}$, $G_{22} = \dfrac{0.0072}{1.9588s+1}$ – передаточные функции двух изолированных подсистем;

$G_{12} = \dfrac{-0.0062}{1.9588s+1}$, $G_{22} = \dfrac{-0.0052}{1.9588s+1}$ – передаточные функции взаимосвязей между подсистемами.

Постановка задачи. Построить сложную систему управления стабилизации процессов дистилляционной колонны (1), с целью достижения желаемых значений выходных сигналов на основе алгоритмов AIS (рисунок 1).

Синтез системы управления очистки газа в дистилляционной колонне определяется нахождением управляющих воздействий, для которых выбран PI закон регулирования:

$$\begin{aligned} u_1(s) &= P_1 \cdot e_1(s) + I_1 \cdot \frac{1}{s} \cdot e_1(s), \\ u_2(s) &= P_2 \cdot e_2(s) + I_2 \cdot \frac{1}{s} \cdot e_2(s), \end{aligned} \tag{2}$$

где $e_i(t), i = \overline{1,2}$ – ошибки рассогласования между желаемыми и выходными сигналами, y_1, y_2.

В качестве критериев качества для настройки регуляторов выбран интегральный квадратичный критерий, обеспечивающий решение задачи стабилизации:

$$ISE_i = \int_{t=0}^{\infty} e_i^2(t)dt, \quad i = \overline{1,2} \to \min . \tag{3}$$

Критерии качества (3) соответствуют локальным регуляторам (2), которые стоят в отдельных контурах.

Постановка задачи для подсистем. Синтезировать типовые регуляторы (2) для изолированных подсистем дистилляционной колонны (1) на основе алгоритма AIS-GA и NSA, минимизирующих критерии качества (3).

В качестве исходных данных задаются критерии качества задачи и параметры алгоритма AIS (таблица 1).

Таблица 1. Параметры алгоритма AIS

Параметры	Значения
размер популяции	N
популяция антител	Ab
число генераций	gen
вероятность мутации	pm
популяция, которая подвергается случайным перестановкам	d
множитель, контролирующий количество клонов	beta
лучшие индивидуальности	ind
временная популяция	T
конечная позиция каждого клона	pcs
начальное значение	pma
норма управления	pmr
итерации для восстановления	itpm
целевая функция (критерий качества)	@shiryayeva

В ходе реализации алгоритма (рисунок 1), были получены начальные популяции подпрограммы AIS-GA, то есть начальные значения PI-регуляторов:

$$\begin{aligned} P_1 &= 42.0698; \quad I_1 = 76.8209; \\ P_2 &= 37.4554; \quad I_2 = 73.2435. \end{aligned} \tag{4}$$

Для критериев (3) на основе программного обеспечения реализации алгоритмов AIS (GA, CLONALG и NSA) в среде MATLAB получены PI-регуляторы двух контуров:

$$\begin{aligned} P_1 &= 100.8357; \quad I_1 = 76.0759, \\ P_2 &= 199.7488; \quad I_2 = 99.8929. \end{aligned} \tag{5}$$

На основе полученных результатов программного обеспечения в виде параметров типовых регуляторов, в среде MATLAB Simulink сформирована схема моделирования системы управления дисцилляционной колонной по двум изолированным контурам. При этом собраны схемы моделирования с тремя типами PI-регуляторов:

– регулятор, настроенный на основе алгоритма AIS (GA, CLONALG и NSA) (5);

– регулятор, настроенный на основе алгоритма AIS (CLONALG) [6]:

$$\begin{aligned} P_1 &= 19.54; \quad I_1 = 48.12; \\ P_2 &= 22.73; \quad I_2 = 23.86. \end{aligned} \tag{6}$$

– регулятор, настроенный на основе алгоритма GA (4).

В соответсвии с построенными схемами, получены результаты моделирования первого контура сложной системы управления дисцилляционной колонны в виде переходного процесса (рисунок 3).

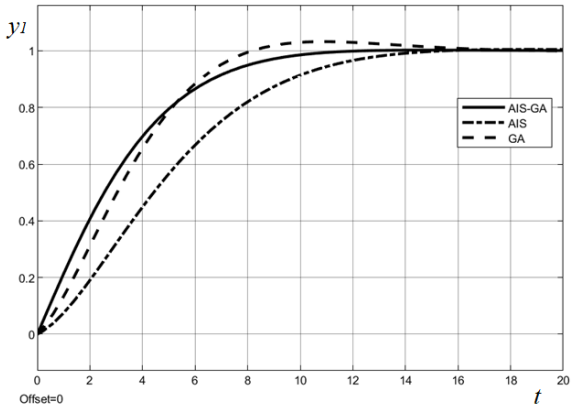


Рис. 3. Результаты моделирования первого контура системы управления

По переходным процессам можно сделать вывод о том, что с примненением AIS (GA, CLONALG и NSA) регулятора оценки качества переходного процесса замкнутой системы управления первым контуром имеют лучшие показатели, чем при AIS-регуляторе и при GA-регуляторе:

– перерегуливание равно нулю;

– время регулирования наименьшее (*Tset*=10);

– время нарастания наименьшее;

– установившаяся ошибка равна нулю.

Также получены результаты моделирования второго контура сложной системы управления дисцилляционной колонны (рисунок 4).

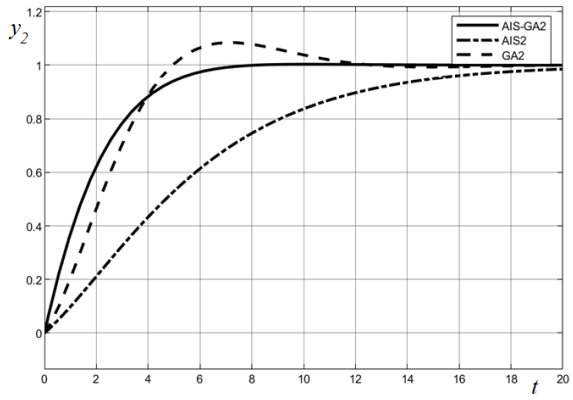


Рис. 4. Результаты моделирования второго контура системы управления

Здесь оценки качества переходного процесса при регуляторе, настроенном алгоритмом AIS (GA, CLONALG и NSA) также дают лучшие показатели:

– перерегуливание равно нулю;

– время регулирования наименьшее (*Tset*=8);

– время нарастания наименьшее;

– установившаяся ошибка равна нулю.

По полученным результатам можно сделать вывод об эффективности использования алгоритма AIS (GA, CLONALG и NSA) для синтеза типовых PI-регуляторов систем управления с целью достижения наилучшего быстродействия и точности процессов системы.

Заключение. В соответствии с поставленной задачей в среде MATLAB разработано программное обеспечение реализации алгоритма искусственных иммунных систем AIS (GA, CLONALG и NSA) для решения задачи синтеза оптимальной системы управления технологическими процессами нефтегазовой отрасли. Для обнаружения локальных минимумов задачи разработано программное обеспечение алгоритма негативной селекции. В ходе реализации программного обеспечения сделан вывод, что данный механизм позволяет распознать и проигнорировать нежелательные экстремумы при поиске оптимальных значений критерия качества.

Работа выполнена по гранту КН МОН РК по теме: "Разработка когнитивной Smart-технологии для интеллектуальных систем управления сложными объектами на основе подходов искусственного интеллекта" № AP05130018 (2018-2020 гг.).

Литература

1. Ayara, M., Timmis, J., Lemos, R., Castro, L. Negative Selection: How to Generate Detectors / M. Ayara, J. Timmis, R. Lemos, L. Castro // UK: In: Proceedings of the 1st International Conference on Artificial Immune Systems (ICARIS), 2002. – Vol.1. – P. 89-98.

2. Marciniak, J., Wawryn, K., Widulinski, P. An Artificial Immune Negative Selection Algorithm to Control Water Temperature in the Outlet of the Chamber / J. Marciniak, K. Wawryn, P. Widulinski // Poland: International conference on signals and electronic systems (ICSES), 2018. – P. 236-241.

3. Ширяева, О. И., Самигулин, Т. И. Базовые концепции развития искусственной иммунной системы на класс сложных систем / О. И. Ширяева, Т. И. Самигулина // Вестник КазНИТУ, 2019. – № 5. – С. 501-504.

4. Shiryayeva, O., Samigulin, T. CLONALG application to the PID-controller synthesis of MIMO-systems in oil and gas industry / O. Shiryayeva, T. Samigulin // Lublin: Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Środowiska, 2019. – № 3. – P. 50-53.

5. Ширяева, О. И., Самигулин, Т. И. Разработка программного обеспечения реализации технологии негативной селекции построения интеллектуальной системы управления для нефтегазовой отрасли / О. И. Ширяева, Т. И. Самигулин // «Сатпаевские чтения -2020»: в сборнике представлены материалы конференции Сатпаевские чтения. – Алматы: КазНИТУ имени Сатпаева, 2020. – С. 245-248.

6. Самигулин, Т.И., Ширяева, О. И. Разработка Smart-системы управления сложным технологическим процессом нефтегазовой отрасли с применением биоинспирированных алгоритмов / О. И. Ширяева, Т. И. Самигулин // Вестник КБТУ, 2019. – Т. 16. – Вып. 4. – С. 164-171.

РАЗРАБОТКА БАЗЫ ЗНАНИЙ ДЛЯ МУЛЬТИАГЕНТНОЙ СИСТЕМЫ НА ОСНОВЕ КООПЕРАТИВНОГО АЛГОРИТМА РОЯ ЧАСТИЦ С ВЕСОМ ИНЕРЦИИ

Самигулина Г.А., Масимканова Ж.А.
galinasamigulina@mail.ru, masimkanovazh@gmail.com
Институт информационных и вычислительных технологий КН МОН РК, Казахстан Казахский национальный университет им. аль-Фараби, Алматы, Казахстан

Аннотация. *Работа посвящена разработке базы знаний для мультиагентной интеллектуальной системы управления и прогнозирования сложными объектами на основе модифицированного алгоритма роя частиц с весом инерции (Cooperative Particle Swarm Optimization with Inertia Weight, CPSOIW) и онтологического подхода. Одной из проблем, возникающих при разработке мультиагентных систем, является представление и интеграция знаний на основе онтологий. Разработана база знаний для мультиагентной системы реализованной на платформе JADE на основе модифицированного CPSOIW алгоритма. Онтологическая модель построена в редакторе онтологий Protégé. Представлены таксономия классов и визуализация онтологической модели на основе CPSOIW алгоритма.*

Ключевые слова: *интеллектуальная система управления, мультиагентная платформа JADE, выделение информативных дескрипторов, кооперативный алгоритм роя частиц с весом инерции, база знаний, онтологический подход.*

В настоящее время актуально применение современных методов искусственного интеллекта для управления сложными объектами на базе реальных производственных данных. При разработке интеллектуальных систем прогнозирования и управления сложными объектами и анализе больших массивов данных в реальном времени актуальным является время вычислений алгоритма. В последнее время среди интеллектуальных подходов наблюдается большой интерес к применению алгоритмов роевого интеллекта (РИ) для решения оптимизационных задач. Активно развиваются алгоритмы муравьиных (Ant Colony Optimization, ACO) [1], пчелиных колоний (Artificial Bee Colony, ABC) [2], алгоритм серых волков (Grey Wolf Optimizer, GWO) [3], алгоритм роя частиц (Particle Swarm Optimization, PSO) [4] и другие.

Широкое распространение получил PSO алгоритм, который успешно применяется при предварительной обработки данных и выделении информативных дескрипторов для дальнейшего прогнозирования и управления сложным объектом. В классическом PSO алгоритме используется постоянный вес инерции, что приводит к проблеме преждевременной сходимости. В алгоритме роя частиц с весом инерции (IWPSO) для решения этой проблемы используется вес инерции [5], который изменяется от итерации к итерации для сохранения разнообразия решений и предотвращения попадания в локальные оптимумы. Для сокращения времени вычислений используется кооперативный алгоритм роя частиц (CPSO) [6], который за счет параллельной обработки детально и быстро исследует пространство поиска.

Для управления сложными объектами широко используются мультиагентные системы, которые способны работать в распределённой среде в режиме реального времени. Мультиагентная система (МАС) представляет собой совокупность автономно действующих агентов, взаимодействующих посредством сообщений, обладающих определёнными интеллектуальными способностями и возможностями индивидуальных и совместных действий [7]. На данный момент существует множество агентных платформ для построения МАС. Наиболее известными являются: JADE (Java Agent Development Framework), Jack Intelligent Agents, Eclipse AMP, MadKIT (Multi-Agent Development Kit), AgentBuilder, Cougaar (Cognitive Agent Architecture), MASON (Multi-Agent Simulator Of Neighborhoods), CogniTAO, Adaptive Modeler и др.

В качестве агентной платформы для реализации МАС широко применяется платформа JADE, реализованная на языке программирования Java с использованием возможностей Java RMI и Java CORBA IDL, что обеспечивает кроссплатформенность разрабатываемой системы [8]. Современные тенденции показывают, что существует множество гибридных систем на основе МАС и PSO алгоритма. Например, в работе [9] описывается распределённый PSO алгоритм на платформе JADE. Мультиагентная структура PSO алгоритма состоит из нескольких вычислительных блоков. Каждый блок является интеллектуальным агентом, основанным на стандартном PSO алгоритме. За счёт распределённой структуры работы системы повышается эффективность и скорость вычислений PSO алгоритма. В исследовании [10] предлагается МАС на основе PSO алгоритма для определения оптимального потока мощности. В работе [11] разрабатывается адаптивная МАС, которая позволяет планировать, оптимизировать и контролировать сложные и многоуровневые процессы производства.

При построении МАС необходимо создание агентов, описание их поведения (behaviors) и определение взаимодействий. Для достижения высокой производительности вычислений агентами используется параллельная обработка информации с использованием потоков (threads). Каждый агент нацелен на выполнение конкретной задачи. Коммуникация между агентами выполняется ACL-сообщениями.

Интеллектуальные агенты описываются онтологиями и UML моделями, которые используются для создания базы знаний при построении МАС. Структура базы знаний состоит из знаний предметной области и методов решения поставленной задачи [12]. База знаний предметной области (Domain ontology) содержит знания, необходимые для функционирования системы в целом. В настоящее время увеличивается использование онтологических моделей при создании МАС. Разработка МАС на этой основе позволяет систематизировать структуру данных, учитывать особенности функционирования и взаимосвязи агентов, снижает временные и вычислительные ресурсы [13]. Существует множество онтологических редакторов для построения OWL (Ontology Web Language) моделей. Редактор онтологий Protégé в открытом доступе успешно используется для проектирования онтологических моделей [14].

При разработке базы знаний для МАС на основе кооперативного алгоритма роя частиц с весом инерции также используюся онтологические модели. В работе [15] предлагается модифицированный семантический PSO алгоритм (Semantic Modified PSO, SMPSO) для облачных вычислений. В отличие от классического PSO алгоритма, предложенный алгоритм включает в себя семантические сети для обновления параметров при кооперации. Моделирование на основе PSO алгоритма

с семантической структурой показывает лучшие результаты по сравнению с другими алгоритмами. В статье [16] описывается гибридная модель на основе квантового PSO алгоритма (Quantum PSO, QPSO) и онтологического подхода для семантической сегмантации изображений. Квантовый PSO алгоритм используется при сегментации исходного изображения с наличием шума. Предложенный метод показывает хорошие результаты за счет семантической реализации и использования базы знаний. Точность классификации предложенного алгоритма составляет 86,2%.

Постановка задачи формулируется следующим образом: необходимо разработать базу знаний для мультиагентной интеллектуальной системы управления и прогнозирования сложными объектами на основе модифицированного алгоритма роя частиц с весом инерции (Cooperative Particle Swarm Optimization with Inertia Weight, CPSOIW) и онтологического подхода.

Для более эффективного и детального исследования многомерного пространства и выделения информативных дескрипторов разработан модифицированный алгоритм роя частиц с весом инерции (Cooperative Particle Swarm Optimization with Inertia Weight, CPSOIW). Данный алгоритм объединяет достоинства алгоритма роя частиц с весом инерции (IWPSO) [17], который позволяет избежать ранней сходимости и предотвращает попадание в локальные оптимумы за счет изменения веса инерции и кооперативного алгоритма роя частиц (CPSO), который более детально и эффективно исследует пространство поиска в режиме реального времени за счёт параллельных вычислений подчинённых роев. Агенты подчинённых роев ориентированы на интенсивный локальный поиск. Параллельное действие агентов подчинённого роя позволяет увеличить скорость вычисления алгоритма. Агенты основного роя сосредоточены на глобальном поиске и на сохранении разнообразия решений.

Модифицированный CPSOIW алгоритм:

Шаг 1. Ввод переменных и случайная генерация начальных положений (x_i) и скорости (v_i) агентов основного M и двух подчинённых S роев.

Шаг 2. Вычисление выбранной фитнес-функции для подчинённых S роев $f(x_i^s(t+1))$ и сохранение лучшего значения фитнес-функции $f(p_g^s)$, где $p_g^s -$ лучшее значение агентов подчинённого S роя, $t -$ итерация.

Шаг 3. Сравнение текущего значения фитнес-функции $f(x_i^s(t+1))$ и лучшего значения фитнес-функции $f(p_g^s)$ подчинённых роев.

Шаг 4. Сравнение лучшего значения фитнес-функции подчинённых S роев $f(p_g^s)$ и глобального лучшего значения $f(p_g^M)$ основного роя, вычисленного на основе лучших значений подчинённых S роев, где $p_g^M -$ лучшее значение агентов основного M роя.

Шаг 5. Обновление скорости v_i^M и положения x_i^M частиц основного M роя.

Шаг 6. Вычисление веса инерции w для всего роя.

Шаг 7. Выполнение 3-9 шагов до окончания количества итераций.

Шаг 8. Построение оптимального набора дескрипторов на основе лучших значений частиц основного M роя для дальнейшего использования при решении задачи прогнозирования и управления сложным объектом.

На рисунке 1 представлена блок-схема модифицированного CPSOIW алгоритма, где $w_{max} -$ максимальное значение веса инерции, $w_{min} -$ минимальное

значение веса инерции, t_{max} – максимальное количество итераций, c_1 и c_2 – коэффициенты ускорения.

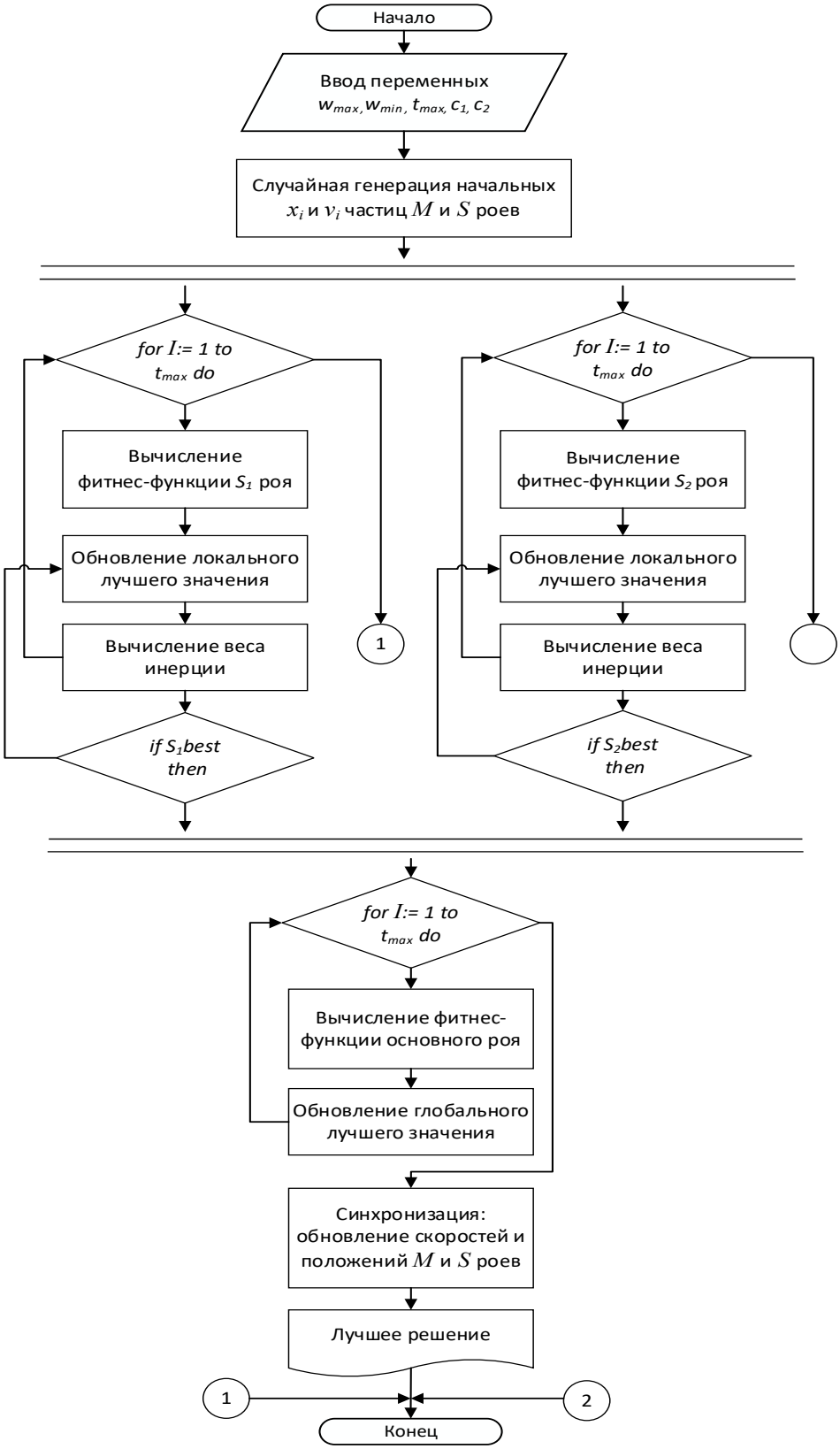


Рис. 1. Блок-схема модифицированного CPSOIW алгоритма

При разработке базы знаний для МАС на основе мультиагентной платформы JADE с использованием кооперативного алгоритма роя частиц с весом инерции разработана онтологическая модель [18] в редакторе онтологий Protégé. На рисунке 2 представлена таксономия классов МАС на основе модифицированного CPSOIW алгоритма.

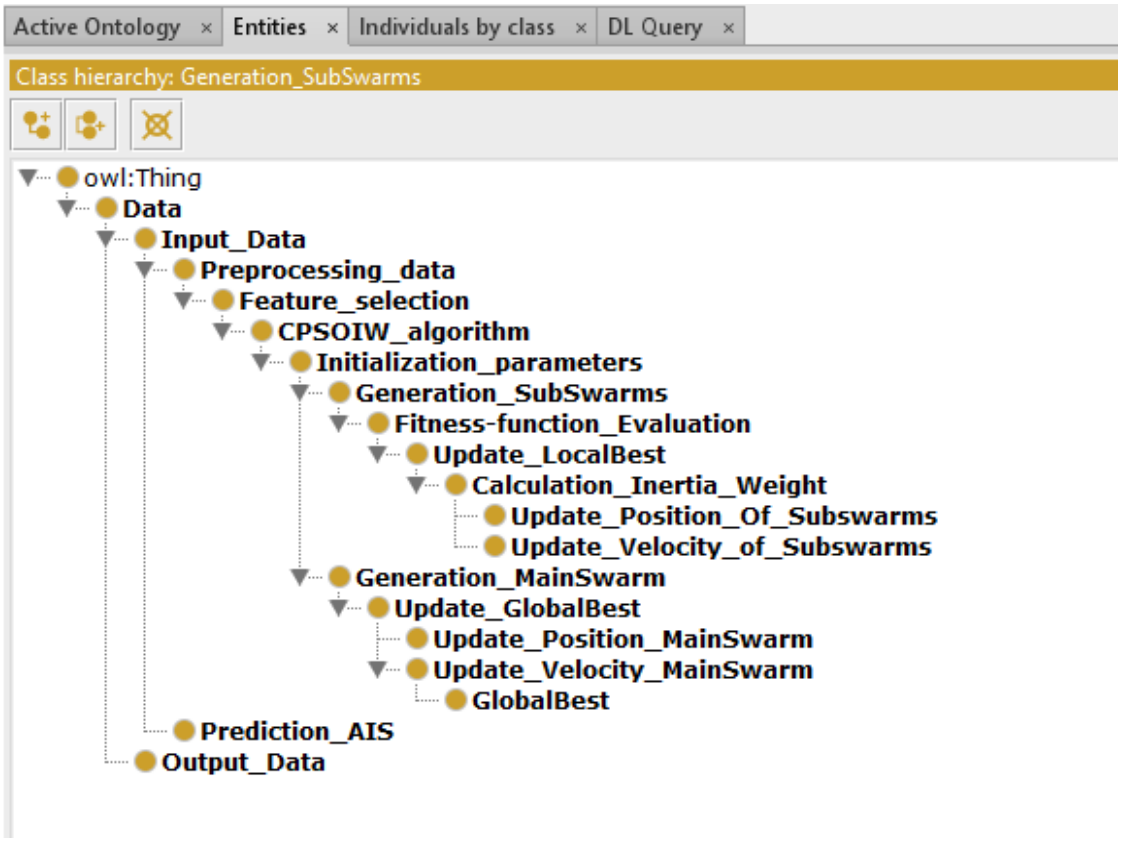


Рис. 2. Таксономия классов МАС на основе CPSOIW алгоритма

На рисунке 3 представлена визуализация онтологической модели на основе CPSOIW алгоритма с помощью инструмента OntoGraf в редакторе онтологий Protégé.

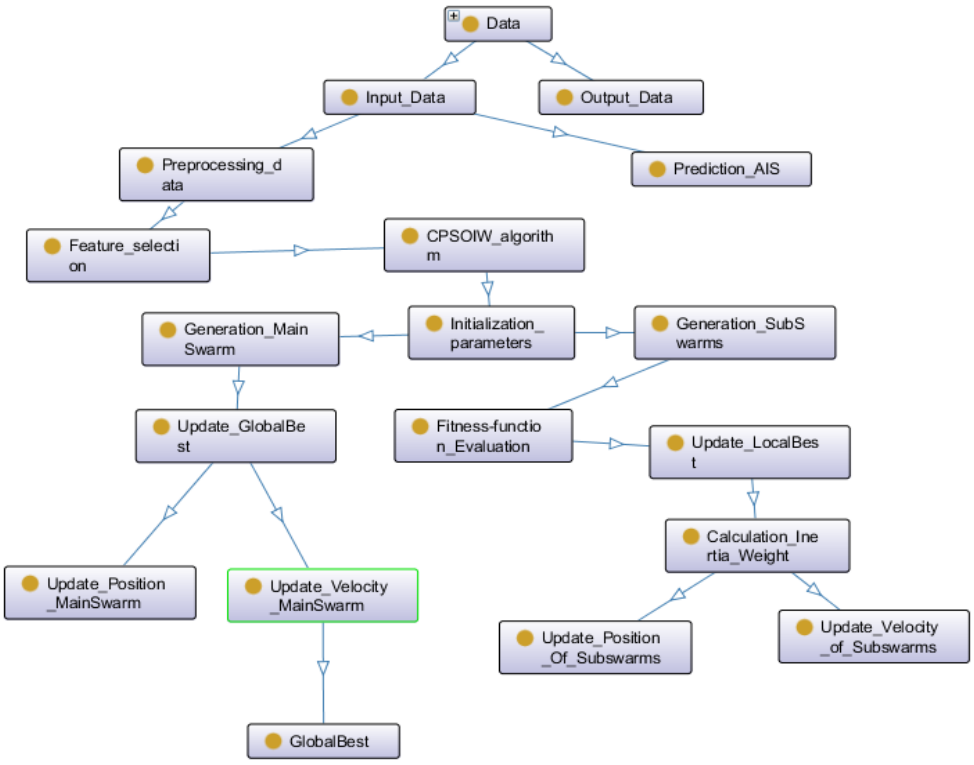


Рис. 3. Визуализация онтологической модели на основе CPSOIW алгоритма

Таким образом, разработка базы знаний для мультиагентной интеллектуальной системы прогнозирования и управления сложными объектами на основе модифицированного CPSOIW алгоритма и онтологического подхода позволяет более детально описывать функции агентов и их взаимосвязи, а также систематизировать входные и выходные параметры, что существенно увеличивает производительность системы.

Исследования проводятся по гранту №AP05130018 КН МОН РК (2018-2020 гг.) по теме: Разработка когнитивной Smart-технологии для интеллектуальных систем управления сложными объектами на основе подходов искусственного интеллекта.

Литература

1. Yaralidarani M., Shahverdi H. An improved Ant Colony Optimization (ACO) technique for estimation of flow functions from core-flood experiments // Journal of Natural Gas Science and Engineering. – 2016. – Vol. 33. – P. 624-633.

2. Chen X., Tianfield H., Li K. Self-adaptive differential artificial bee colony algorithm for global optimization problems // Swarm and Evolutionary Computation. – 2019. – Vol. 45. – P. 70-91.

3. Kohli M., Arora S. Chaostic grey wolf optimization algorithm for constrained optimization problems // Journal of Computational Design and Engineering. – 2018. – Vol. 5, Issue 4. – P. 458-472.

4. Huang S., Tian N., Wang Y., Ji Z. Particle swarm optimization using multi-information characteristics of all personal-best information // Springer Plus. – 2016. – Vol. 5 (1632). – https://doi.org/10.1186/s40064-016-3244-8.

5. Maca P., Pech P. The Inertia Weight Updating Strategies in Particle Swarm Optimization based on the Beta Distribution // J. Mathematical Problems in Engineering. – 2015. – http://dx.doi.org/10.1155/2015/790465.

6. Xia X., Gui L., Zhan Z. A multi-swarm particle swarm optimization algorithm based on dynamical topology and purposeful detecting // J. Applied Soft Computing. – 2018. – Vol. 67. – C.126-140.

7. Гаранина Н.О., Сидорова Е.А. Мультиагентный подход к извлечению информации из текстов и пополнению онтологии // Знания-Онтологии-Теории (ЗОНТ-2015). – http://elib.ict.nsc.ru/jspui/bitstream/ICT/1395/1/ЗОНТ10.pdf.

8. Bellifemine F.L., Caire G., Greenwood D. Developing Multi-Agent Systems with JADE. – John Wiley & Sons, 2007. – 300 p.

9. Sheng S. A Particle Swarm Optimization (PSO) Algorithm Based on Multi-agent System // 2008 International Conference on Intelligent Computation Technology and Automation (ICICTA). – DOI: 10.1109/ICICTA.2008.367.

10. Ravi Kumar K., Anand S., Sydulu M. Comparison of Multi Agent Based PSO Approach for Optimal Power Flows with Security Constraints // Applied Mechanics and Materials. – 2011. – P. 5206-5210.

11. Pavel V., Ondřej H., Martin K., Vladimír M. Agent-Based Production Scheduling for Aircraft Manufacturing Ramp-up // Industrial Applications of Holonic and Multi-Agent Systems. – Switzerland: Springer International Publishing, 2015. – P. 145-156.

12. Андреев В.В., Батищев С.В., Ивкушкин К.В., Искварина Т.В., Скобелев П.О. Инструментальные средства для разработки мультиагентных систем промышленного масштаба. http://www.ssc.smr.ru/media/ipuss_conf/06/5_01.pdf.

13. Самигулина Г.А., Масимканова Ж.А. Построение оптимальной иммунносетевой модели на основе модифицированного алгоритма роя частиц // Вестник КазНУ им. Аль-Фараби. – Алматы, 2018. – № 2(98). – С. 20-28.

14. Amini B., Ibrahim R., Othman M.S., Nematbakhsh M.A. A reference ontology for profiling scholar's background knowledge in recommender systems // Expert Systems with Applications. – 2015. – Vol. 42, Issue 2. – P. 913-928.

15. Zhang C., Yang Y., Du Z., Ma C. Particle swarm optimization algorithm based on ontology model to support cloud computing applications // Journal of Ambient Intelligence and Humanized Computing. – 2016. – Vol. 7, Issue 5. – P. 633-638.

16. Elsayed E.K., Aly M. Hybrid between Ontology and Quantum Particle Swarm Optimization for Segmenting Noisy Plant Disease Image // International Journal of Intelligent Engineering and Systems. – 2019. – Vol.12, No.5. – DOI: 10.22266/ijies2019.1031.30.

17. Amoshahy M.J., Shamsi M., Sedaaghi M.H. A Novel Flexible Inertia Weight Particle Swarm Optimization // J. PloS. – 2016. – Vol. 11(8). – DOI:10.1371/journal.pone.0161558.

18. Samigulina G.A., Massimkanova Zh.A. Multi-agent System for Forecasting Based on Modified Algorithms of Swarm Intelligence and Immune Network Modeling // Proceedings of the 12th International Conference Agents and Multi-agent Systems: Technologies and Applications (KES-AMSTA-18). – Australia: Springer, 2018. – P. 199-208.

СЕКЦИЯ 2

Ақпараттық-телекоммуникациялық технологиялар. Деректерді жіберу желілері мен жүйелері. Интернет технологиялар. Бұлттық технологиялар. Параллельді есептеу. Үлестірімділік есептеулер. Суперкомпьютерлік және кластерлік жүйелер. Үлкен көлемді деректерді (Big-data) өңдеу. Геоақпараттық жүйелер және технологиялар. Инновациялық оқыту технологиялары

Информационно-телекоммуникационные технологии. Системы и сети передачи данных. Интернет-технологии. Облачные технологии. Параллельные вычисления. Распределённые вычисления. Суперкомпьютерные и кластерные системы. Обработка больших объёмов данных (Big-data). Геоинформационные системы и технологии. Инновационные образовательные технологии

Information and telecommunication technologies. Systems and networks of data transmission. Internet technologies. Cloud technologies. Parallel computing. Distributed computing. Supercomputer and cluster systems. Processing large volumes of data (Big-data). Geoinformation systems and technologies. Innovative educational technologies

ВЕРИФИКАЦИЯ ОДНОЙ МОДЕЛИ ПЛОСКОЙ КРИСТАЛЛИЧЕСКОЙ РЕШЕТКИ

Г. А. Амирханова[1], А.Ю. Горчаков[2]
e-mail: gulshat.aa@gmail.com
[1]Институт информационных и вычислительных технологий Комитета Науки Министерства образования и науки Республики Казахстан,
[2]Вычислительный центр имени. А.А. Дородницына Федерального исследовательского центра "Информатика и управление" Российской академии наук

В работе проводится анализ результатов решения задачи поиска минимума энергии совокупности атомов фрагмента плоской кристаллической решетки. Рассматривается задачи минимизации в двух постановках. При решении задачи в первой постановке производится первичный отбор локальных минимумов. После этого решается задача во второй постановке. В качестве результата мы берем решение с минимальной энергией и с помощью методов кластеризации определяем основные трансляционные вектора и постоянную кристаллической решетки. Моделирование производилось для графена с использованием потенциала Терсоффа с двумя различными наборами параметров – оригинальным и оптимизированным. Эксперименты показали достаточную точность моделирования для оригинального набора параметров и неприменимость оптимизированного набора.

***Ключевые слова**: плоская кристаллическая решетка, глобальная оптимизация, локальный минимум энергии, кластеризация, потенциал Терсоффа.*

Введение

Задача верификации при моделировании кристаллической структуры является неотъемлемым этапом процесса моделирования, а также доказательством адекватности модели и работоспособности программы и вычислений.

Обычно верификация модели происходит следующим образом:

Этап 1. Проверка исходного кода программы с целью выявления ошибок синтаксиса/логических ошибок. Она позволяет предотвратить неверные расчеты и неявные ошибки, которые возникают при ошибочной постановке знака (сложение, вычитание) или мелкие ошибки преобразования типов данных, на которые некоторые компиляторы могут явно не указывать, и, тем самым, вводить исследователя в заблуждение по поводу правильности расчетов. Для более надежного функционирования программы в будущем следует разработать специальные тесты, покрывающие большинство возможных проблем и случаев.

Этап 2. Проверка формул и вычислений. Осуществляется по схеме: подать на вход исходные данные и сравнить результат с контрольными образцами, которые были вычислены заранее для этих исходных данных. При возникновении несоответствия в формулах делаются изменения, и процесс проверки повторяется. Данная проверка длится до тех пор, пока расхождение между полученными результатами и контрольными образцами не будет ниже определенного заранее значения.

После прохождения всех этапов возможно использовать новые данные, для которых еще не вычислен результат, но известны ограничения по нему.

После верификации модели считается, что данная модель может использоваться для дальнейших исследований и опытов.

1. Постановка задачи

Рассматриваемая в данной работе плоская модель многослойного кусочно-однородного материала предложена в [1, 2]. Материал представляется в виде периодической кусочно-однородной многослойной структуры, в рамках которой могут отличаться типы атомов в различных слоях. Модель накладывает ряд ограничений на структуру слоев:

1. каждый слой состоит из одинаковых атомов, в разных слоях могут находиться различные атомы;
2. расстояния между соседними атомами в одном слое одинаковы, но в разных слоях они могут отличаться;
3. в рассматриваемой системе выделяется группа из параллельных слоев, которая периодически повторяется в направлении оси y;
4. число атомов в каждом слое и общее число слоев считается потенциально неограниченным.

На Рис. 1 представлен пример модели, в которой повторяется группа из трех слоев. Каждый слой состоит из атомов своего вида.

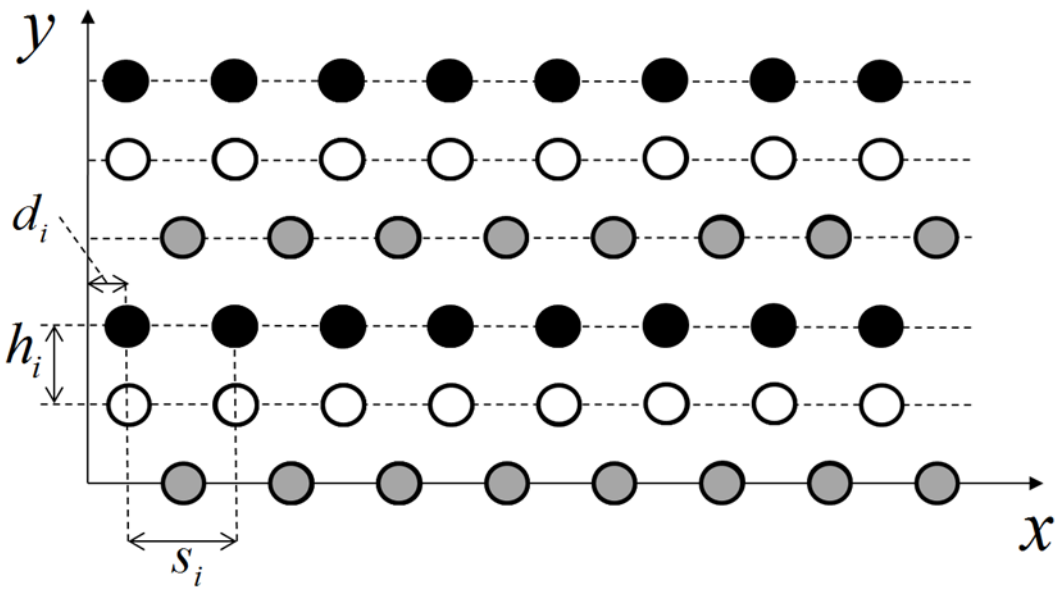


Рис. 1 Двумерная модель материала

В рамках данной модели положение атомов определяется следующими параметрами:

$h_i, i = 1, \ldots, K$– расстояние между слоем с номером i и предыдущим слоем;

$d_i, i = 1, \ldots, K$– смещение первого атома в слое i с положительной абсциссой относительно нулевой отметки;

$s_i, i = 1, \ldots, K$– расстояние между атомами в слое i.

Совокупность значений перечисленных параметров будем называть *конфигурацией*. Ниже рассматривается ситуация, когда материал находится в ненагруженном состоянии. Требуется определить конфигурацию, соответствующую минимальной энергии взаимодействия атомов, входящих в моделируемый фрагмент материала.

Рассматривается две постановки (далее – постановка I и постановка II). В обоих случаях минимизируется энергия $E(x)$ совокупности атомов, расположенных на Kсоседних слоях. Параметрами оптимизационной задачи являются переменные $x = (h_1, d_1, s_1, \ldots, h_K, d_K, s_K)$, составляющие вектор размерности $n = 3K$. Таким образом, решаемая задача оптимизации относится к числу так называемых задач с параллелепипедными ограничениями и математически формулируется следующим образом:

$$E(x) \to min, l_i \leq x_i \leq u_i, i = 1, \ldots, n.$$

В постановке I в моделируемую совокупность входят атомы, абсцисса которых лежит в заданном интервале $[0, L]$. При этом, в зависимости от значений параметров, задающих конфигурацию, число и состав атомов, входящих в моделируемую совокупность могут меняться. В постановке II считается, что атомы, входящие в эту совокупность, не меняются.

Энергия решетки рассчитывается с помощью потенциалов взаимодействия. Вычисляется энергия конечной совокупности соседних атомов («фрагмента»). Энергия фрагмента равна сумме энергий взаимодействия входящих в него атомов с остальными атомами решетки. В данной работе использовался потенциал Терсоффа с двумя различными наборами параметров, оригинальный [3] и оптимизированный [4].

2. Поиск минимума энергии атомов фрагмента кристаллической решетки и определение ее параметров

Для поиска минимума энергии атомов кристаллической решетки применялся метод мультистарта в сочетании с методом координатного спуска, описанный в работе [5]. Схема метода достаточно проста – случайным образом выбирается начальная точка и из нее запускается метод поиска локального минимума. В итоге мы получаем определенное количество локальных минимумов и как результат возвращается решение с минимальным значением энергии. Учитывая тот факт, что метод мультистарта является недетерминированным методом поиска глобального минимума и не гарантирует его нахождение за конечное количество шагов, мы вынуждены брать количество начальных приближений с достаточным запасом.

В начале решается оптимизационная задача в постановке I, затем выбираются наилучшие решения и запускается решение задачи в постановке II.

Определение постоянной кристаллической решетки и углов между основными трансляционными векторами производится следующим образом:

а) задаем некоторый радиус $r = 1{,}846A^o$, атомы, расположенные на расстоянии меньшем чем *r,* будут считаться соседями;

б) для каждого атома определяем его соседей, с помощью функции RadiusNeighborsTransformer [6]; и вычитаем его координаты из координат соседних атомов;

в) с помощью MeanShift [6,7] разбиваем все атомы на кластеры, по типу окружения атомов; пример кластеризации приведен на рис.2.

г) вычисляем расстояния между атомами одного типа и определяем угол между основными трансляционными векторами; при этом так же используем MeanShift.

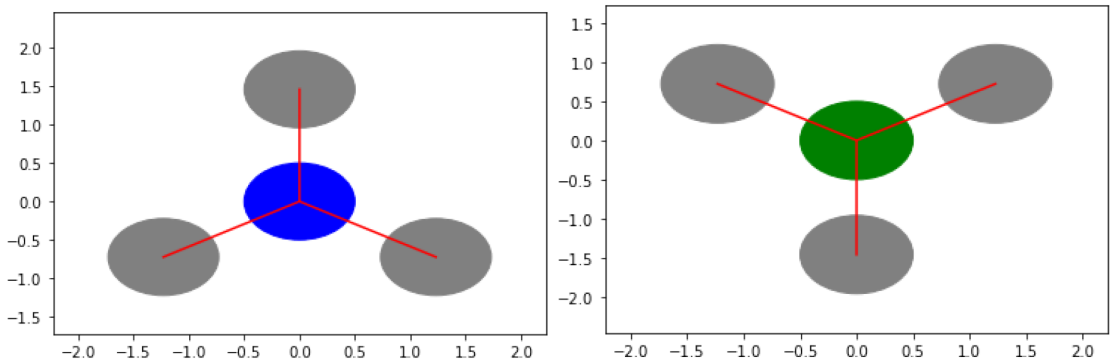


Рис.2 Атомы с различным типом окружения.

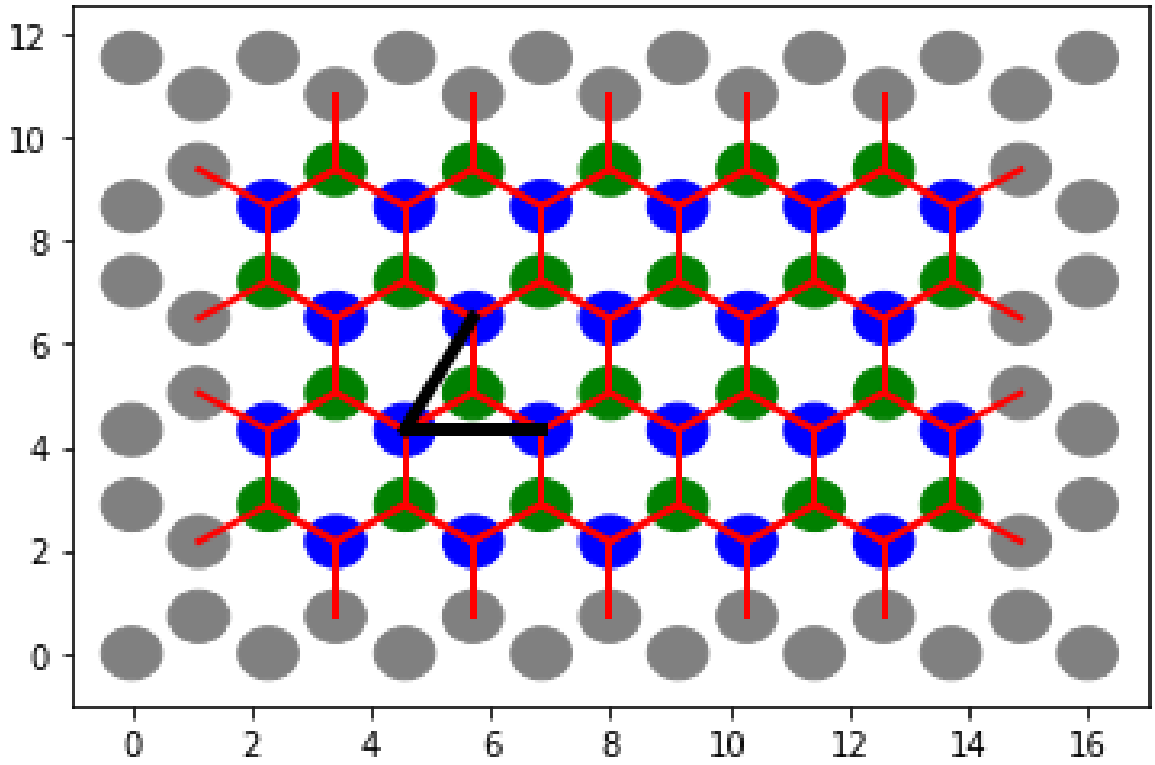


Рис. 3 Результат кластеризации атомов по типу их окружения и основные трансляционные вектора. Синие и зеленые круги атомы с различным типом окружения. Черные стрелки – основные трансляционные вектора.

3. Результаты численных экспериментов

Расчеты выполнялись с использованием инфраструктуры ЦКП «Информатика» ФИЦ ИУ РАН [8]. Метод мультистарта был распараллелен с помощью директив OpenMP на 160 потоков. Для каждого потенциала было

получено 32000 локальных минимумов задачи в постановке I. Далее для 20% наилучших значений была решена задача в постановке II.

Для оригинального набора параметров потенциала Терсоффа было найдено решение с энергией -443.73 (-419.42 для постановки I). Трансляционные вектора указаны в таб. 1.

	Постановка I		Постановка II	
№	Длина вектора	Угол с осью X	Длина вектора	Угол с осью X
1	2.29	0	2.53	0
2	2.45	62.18	2.53	60
3	2.45	117.82	2.53	120
4	2.29	180	2.53	180
5	2.45	-117.82	2.53	-120
6	2.45	-62.18	2.53	-60

Таблица 1. Трансляционные вектора для оригинального потенциала Терсоффа

Как видно из таблицы использование задачи в постановке I приводит к некоторому искажению решетки, связанному с существенным влиянием границ фрагмента. При переходе к постановке II эти искажения пропадают. Углы между основными трансляционными векторами совпадают с контрольными образцами, постоянная решетки (контрольное значение 2.46) определяется с погрешностью менее 3%.

Для оптимизированного набора параметров потенциала Терсоффа было найдено решение с энергией -1067.49 (-999.59 для постановки I). Трансляционные вектора указаны в таб. 2.)

	Постановка I		Постановка II	
№	Длина вектора	Угол с осью X	Длина вектора	Угол с осью X
1	1.23	0	1.29	0
2	11.52	90	13.84	90
3	1.23	180	1.29	180
4	11.52	-90	13.84	-90

Таблица 2. Трансляционные вектора для оптимизированного потенциала Терсоффа

Как видно из таб. 2 полученные значения далеки от значений контрольного образца. Отношение длин трансляционных векторов равно примерно 1/10. Это связано с тем, что по оси y материал не образует периодической структуры (точнее период равен сумме h_i).

4. Заключение

Анализ результатов проведенных экспериментов показал, что использование рассматриваемой модели плоской кристаллической решетки в сочетании с оригинальным набором параметров потенциала Терсоффа позволяет определить тип

и постоянную кристаллической решетки с достаточной точностью. При этом видно, что решения задачи в постановке I близки к контрольным образцам, но погрешности вносимые постановкой приводят к неравноценности осей *X* и *Y*, чего не наблюдается на практике. Только последовательное использование постановок I и II позволяет получить корректный результат.

Использование оптимизированных параметров потенциала Терсоффа приводит появлению множества «разреженных» конфигураций (либо по оси *Y*, либо по оси *X*). Для наилучшего найденного решения получается прямоугольная решетка вместо гексагональной. Поэтому, в нашем случае, использование оптимизированного набора параметров не рекомендуется.

Список литературы

1. Лурье С.А., Посыпкин М.А., Соляев Ю.О. Метод идентификации масштабных параметров градиентной теории упругости на основе численных экспериментов для плоских композитных структур // Internat. J. of Open Informat. Technol. 2015. Т. 3. № 6. С. 1-6.
2. Ю.Г. Евтушенко, С.А.Лурье, М.А.Посыпкин, Ю.О.Соляев. Применение методов оптимизации для поиска равновесных состояний двумерных кристаллов // Ж. вычисл. матем. и матем. физ. 2016. Т. 56. № 12. С. 50-59.
3. Tersoff J. Empirical interatomic potential for carbon, with applications to amorphous carbon Physical Review Letters. 1988. V. 61. 25.
4. Lindsay, L., & Broido, D. A. (2010). Optimized Tersoff and Brenner empirical potential parameters for lattice dynamics and phonon thermal transport in carbon nanotubes and graphene. Physical Review B, 81(20), 205441.
5. Горчаков А. Ю., Посыпкин М. А. Эффективность методов локального поиска в задаче минимизации энергии плоского кристалла //Современные информационные технологии и ИТ-образование. – 2017. – Т. 13. – №. 2.
6. Scikit-learn: Machine Learning in Python, Pedregosa et al., JMLR 12, pp. 2825-2830, 2011.
7. Comaniciu D., Meer P. Mean shift: A robust approach toward feature space analysis //IEEE Transactions on pattern analysis and machine intelligence. – 2002. – Т. 24. – №. 5. – С. 603-619.
8. Положение о ЦКП «Информатика» // [Электронный ресурс] – Режим доступа http://www.frccsc.ru/ckp (дата обращения 07.09.2020)

INVESTIGATION OF THE THERMOMECHANICAL STATE OF A ROD OF VARIABLE CROSS-SECTION UNDER THE INFLUENCE OF DISSIMILAR HEAT SOURCES.

[1]Anarbay Kudaykulov1, [1]Azat Tashev,[1,2] Mukaddas Arshidinova., Begaliyeva Kalamkas
E-mail: [1]kudaykulov2006@mail.ru, [2]azattash@mail.ru, [3]mukaddas_arshidi@mail.ru, kalamkas_b@mail.ru
1 Institute of Information and Computing Technologies CS MES RK, Almaty, Kazahstan
2 Al-Farabi Kazakh National University, Almaty, Kazahstan

Abstract. *In work on the basis of energy conservation laws with use square the spline of functions in the local system of coordinates is in number investigated thermo - the intense deformed condition of a horizontal core of variable section and limited length. At the same time on the areas of transverse sections of two ends of a core heat fluxes of identical intensity are brought. Through lateral areas middle (1/3) parts of a core there is a heat exchange to a surrounding medium. Other parts of a lateral area are heat-insulated. Distribution laws of temperatures, all being deformations and tension, movements, and also sizes of thermal lengthening and the arising squeezing axial force are defined. Particular regularities are revealed.*

Keywords: *Lengthening, axial force, section, temperature, movement, deformation, tension.*

Introduction

The bearing elements of the modern producer power stations, jet and hydrogen engines, nuclear and thermal power plants, and also technological lines of processing industry are rod stock of variable section. Most of them work at simultaneous influence of diverse types of sources of heat. In this regard reliable work of the above-stated installations and inventories will be depends on thermodurability of the used rod elements of variable section and limited length. Therefore a research thermo - an intense strained state of rod of variable section and limited length taking into account simultaneous existence of diverse types of sources of heat, local thermal insulations and physicomechanical properties of materials of rod stock are a relevant task. At the same time the received decisions have to be reliable at the level of fundamental laws of conservation of energy [1-3].

2. Formulation of the problem an methods

The horizontal rod of variable section and limited length of L [cm] is considered. The horizontal axis ox coincides with a rod axle. The transverse section of the considered rod is a circle

Rod section radius on coordinate changes linearly under the $r(x) = ax + b$ where and a and b constant. At this b – the radius of a transverse section of the left-hand end.

The cross-sectional area of the rod varies according to the formula $F(x) = \pi r^2 = \pi(a^2x^2 + 2abx + b^2)$, $(0 \le x \le L)$

Physicomechanical and thermal properties of material of a rod it is characterized by a material elastic modulus $E[\frac{kG}{cm^2}]$, thermal expansion coefficients $\alpha[\frac{1}{{}^0K}]$, and heat conductivity $K_{xx}[\frac{W}{cm^0K}]$. On the area of transverse sections of two ends of the studied core it is brought heat fluxes with identical intensity $q[\frac{W}{cm^2}]$.

Lateral areas the first $(0 \le x \le l)$, $l = \frac{L}{3}[cm]$, and third $(2l \le x \le 3l = L)$ (1/3) parts of a rod are heat-insulated.

Through a lateral area of average (1/3) parts $(l \le x \le 2l)$ happen heat exchange to a surrounding medium. At the same time heat exchange coefficient, and environment temperature of $h[\frac{W}{cm^2K}]$. Here it should be noted that. The settlement scheme of a task is provided in the figure-1.

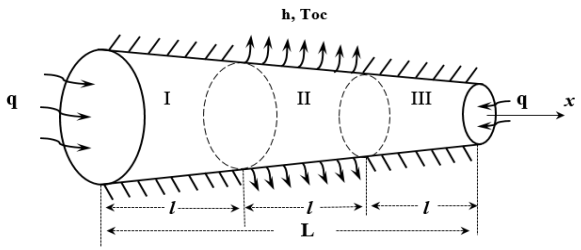


Figure 1: The settlement scheme of the considered task.

It is required: to construct approximating square a function spline in a local frame; to formulate a task at the level of the law of conservation of energy in the form of a functional of the total thermal energy for definition the field of temperatures; to define the integrated type of a functional of the total thermal energy; to construct the allowing system of the simple algebraic equations taking into account natural boundary conditions for definition the field of temperatures;In case one end of the studied rod rigid is jammed, and another is free it is necessary to determine the size of its lengthening taking into account simultaneous existence of local thermal insulations, heat exchange, heat fluxes, thermal properties of material of a core and its geometry; it is necessary to calculate values of the arising squeezing axial force taking into account geometry and physicomechanical and thermal properties of material of a core and also existence of diverse types of sources of heat and local thermal insulations in case of jamming of two ends of the considered core; to define the field of temperature, thermoelastic, temperature and elastic components of deformations and tension; to write a functional potential to energy of elastic deformation taking into account existence the field of temperature for definition the field of movement on the basis of the law of conservation of energy; to define the integrated type of a functional of a potential energy resilient deformations taking into account existence the field of temperature; o construct the allowing system of the simple algebraic equations taking into account natural boundary conditions; to build the field of movement taking into account a zashchemlennost of two ends of the studied rod of variable section and limited length.

3. Construction spline of functions and of a functional of energy

Let's consider one discrete site of a core length of l[cm]. The field of temperature longwise of a core, we approximate the complete polynom of the second order

$$T(x) = c_1x^2 + c_2x + c_3 = \varphi_i(x)\cdot T_i + \varphi_j(x)\cdot T_j + \varphi_k(x)\cdot T_k, \quad 0 \le x \le l \tag{1}$$

where $T_i = T(x=0)$;

$$T_j = T(x = \frac{l}{2}); \quad T_k = T(x = l);$$

$$\varphi_i(x) = \frac{2x^2 - 3lx + l^2}{l^2};$$

$$\varphi_j(x) = \frac{4lx - 4x^2}{l^2}; \tag{2}$$

$$\varphi_k(x) = \frac{2x^2 - lx}{l^2};$$

These functions we will call square a spline functions in a local frame $(0 \le x \le l)$.Within rod length $(0 \le x \le l)$ the gradient of temperature is defined from (1-2)

$$\frac{\partial T}{\partial x} = \frac{\partial \varphi_i}{\partial x} T_i + \frac{\partial \varphi_j}{\partial x} T_j + \frac{\partial \varphi_k}{\partial x} T_k = \frac{4x-3l}{l^2} T_i + \frac{4l-8x}{l^2} T_j + \frac{4x-l}{l^2} T_k, \quad 0 \le x \le l \tag{3}$$

Пользуясь законом сохранения энергии, для рассматриваемой задачи напишем функционал полной тепловой энергии [2]

Using the law of conservation of energy, for the considered task we will write a functional of the total thermal energy [2]

$$J = \int_{F(x=0)} qTds + \int_{V_1} \frac{K_{xx}}{2}\left(\frac{\partial T}{\partial x}\right)^2 dv + \int_{S(l \le x \le 2l)} \frac{h}{2}(T - T_{oc})^2 ds + \int_{V_2} \frac{K_{xx}}{2}\left(\frac{\partial T}{\partial x}\right)^2 dv + \int_{V_3} \frac{K_{xx}}{2}\left(\frac{\partial T}{\partial x}\right)^2 dv + \int_{F(x=L)} qTds \tag{4}$$

where $F(x=0)$ and $F(x=L)$ - cross-sectional area of the two ends of the investigated rod; Wherein $F(x=0) >> F(x=L)$ V1, V2 and V3 - volumes of three sections of the rod; For the 1st section $(0 \le x \le l)$ considered rod $T_i = T(x=0) = T_1$; $T_j = T(x=\frac{l}{2}) = T_2$; $T_k = T(x=l) = T_3$; For the 2nd section $(l \le x \le 2l)$ respectively $T_i = T(x=l) = T_3$; $T_j = T(x=\frac{3l}{2}) = T_4$; $T_k = T(x=2l) = T_5$; Finally, for the third section $(2l \le x \le 3l = L)$ will get $T_i = T(x=2l) = T_5$; $T_j = T(x=\frac{5l}{2}) = T_6$; $T_k = T(x=3l=L) = T_7$.

At this designated after an integration (4) has an appearance:

$$\begin{aligned}
J = {} & \pi \cdot b_1^2 \cdot q \cdot T_1 + \frac{\pi \cdot K_{xx}}{2}\Bigg[\left(\frac{a^2 l}{5} + ab_1 + \frac{7b_1^2}{3l}\right)\cdot T_1^2 + \left(\frac{32a^2 l}{15} + \frac{16ab_1}{3} + \frac{16b_1^2}{3l}\right)\cdot T_2^2 + \\
& + \left(\frac{26a^2 l}{15} + \frac{a(11b_1+3b_2)}{3} + \frac{7(b_1^2+b_2^2)}{3l}\right)\cdot T_3^2 - \left(\frac{4a^2 l}{5} + \frac{8ab_1}{3} + \frac{16b_1^2}{3l}\right)\cdot T_1 \cdot T_2 + \left(\frac{2a^2 l}{5} + \frac{2ab_1}{3} + \frac{2b_1^2}{3l}\right)\cdot T_1 \cdot T_3 - \\
& - \left(\frac{52a^2 l}{15} + 8ab_1 + \frac{16b_1^2}{3l}\right)\cdot T_2 \cdot T_3 + \left(\frac{32a^2 l}{15} + \frac{16ab_2}{3} + \frac{16b_2^2}{3l}\right)\cdot T_4^2 + \left(\frac{26a^2 l}{15} + \frac{a(11b_2+3b_3)}{3} + \frac{7(b_2^2+b_3^2)}{3l}\right)\cdot T_5^2 - \\
& - \left(\frac{4a^2 l}{5} + \frac{8ab_2}{3} + \frac{16b_2^2}{3l}\right)\cdot T_3 \cdot T_4 + \left(\frac{2a^2 l}{5} + \frac{2ab_2}{3} + \frac{2b_2^2}{3l}\right)\cdot T_3 \cdot T_5 - \left(\frac{52a^2 l}{15} + 8ab_2 + \frac{16b_2^2}{3l}\right)\cdot T_4 \cdot T_5 + \\
& + \left(\frac{32a^2 l}{15} + \frac{16ab_3}{3} + \frac{16b_3^2}{3l}\right)\cdot T_6^2 + \left(\frac{23a^2 l}{15} + \frac{11ab_3}{3} + \frac{7b_3^2}{3l}\right)\cdot T_7^2 - \left(\frac{4a^2 l}{5} + \frac{8ab_3}{3} + \frac{16b_3^2}{3l}\right)\cdot T_5 \cdot T_6 + \\
& + \left(\frac{2a^2 l}{5} + \frac{2ab_3}{3} + \frac{2b_3^2}{3l}\right)\cdot T_5 \cdot T_7 - \left(\frac{52a^2 l}{15} + 8ab_3 + \frac{16b_3^2}{3l}\right)\cdot T_6 \cdot T_7\Bigg] + h \cdot \pi \cdot \Bigg[\left(\frac{al^2}{60} + \frac{2b_2 l}{15}\right)\cdot T_3^2 + \\
& + \left(\frac{4al^2}{15} + \frac{8b_2 l}{15}\right)\cdot T_4^2 + \left(\frac{7al^2}{60} + \frac{2b_2 l}{15}\right)\cdot T_5^2 + \frac{2b_2 l}{15}\cdot T_3 \cdot T_4 - \left(\frac{al^2}{30} + \frac{b_2 l}{15}\right)\cdot T_3 \cdot T_5 + \left(\frac{2al^2}{15} + \frac{2b_2 l}{15}\right)\cdot T_4 \cdot T_5 + \\
& + \left(\frac{al^2}{2} + b_2 l\right)\cdot T_0^2 - \frac{b_2 l}{3}\cdot T_3 \cdot T_0 - \left(\frac{2al^2}{3} + \frac{4b_2 l}{3}\right)\cdot T_4 \cdot T_0 - \left(\frac{al^2}{3} + \frac{b_2 l}{3}\right)\cdot T_5 \cdot T_0 + \pi(3al+b)^2 \cdot q \cdot T_7;
\end{aligned}$$

Minimizing the last functional on nodal value of temperatures T1,T2,…,T7, we will receive the allowing system of the simple algebraic equations, natural boundary conditions are considered.

$$1)\ \frac{\partial J}{\partial T_1} = 0; \Rightarrow \pi \cdot b_1^2 \cdot q + \frac{\pi K_{xx}}{2}$$

$$\left[2 \cdot \left(\frac{a^2 l}{5} + a b_1 + \frac{7 b_1^2}{3l} \right) \cdot T_1 - \left(\frac{4a^2 l}{5} + \frac{8 a b_1}{3} + \frac{16 b_1^2}{3l} \right) \cdot T_2 + \left(\frac{2a^2 l}{5} + \frac{2 a b_1}{3} + \frac{2 b_1^2}{3l} \right) \cdot T_3 \right] = 0;$$

$$2)\ \frac{\partial J}{\partial T_2} = 0; \Rightarrow \frac{\pi K_{xx}}{2}$$

$$\left[2 \cdot \left(\frac{32 a^2 l}{15} + \frac{16 a b_1}{3} + \frac{16 b_1^2}{3l} \right) \cdot T_2 - \left(\frac{4a^2 l}{5} + \frac{8 a b_1}{3} + \frac{16 b_1^2}{3l} \right) \cdot T_1 - \left(\frac{52 a^2 l}{15} + 8 a b_1 + \frac{16 b_1^2}{3l} \right) \cdot T_3 \right] = 0;$$

$$3)\ \frac{\partial J}{\partial T_3} = 0; \Rightarrow \frac{\pi K_{xx}}{2}$$

$$\left[\left(\frac{2a^2 l}{5} + \frac{2 a b_1}{3} + \frac{2 b_1^2}{3l} \right) \cdot T_1 - \left(\frac{52 a^2 l}{15} + 8 a b_1 + \frac{16 b_1^2}{3l} \right) \cdot T_2 + 2 \cdot \left(\frac{26 a^2 l}{15} + \frac{a(11 b_1 + 3 b_2)}{3} + \frac{7(b_1^2 + b_2^2)}{3l} \right) \cdot T_3 - \left(\frac{4a^2 l}{5} + \frac{8 a b_2}{3} + \frac{16 b_2^2}{3l} \right) \cdot T_4 + \left(\frac{2a^2 l}{5} + \frac{2 a b_2}{3} + \frac{2 b_2^2}{3l} \right) \cdot T_5 \right] +$$

$$h\pi \left[2 \cdot \left(\frac{a l^2}{60} + \frac{2 b_2 l}{15} \right) \cdot T_3 + \frac{2 b_2 l}{15} \cdot T_4 - \left(\frac{a l^2}{30} + \frac{b_2 l}{15} \right) \cdot T_5 - \frac{b_2 l}{3} \cdot T_0 \right]_5 = 0;$$

$$4)\ \frac{\partial J}{\partial T_4}=0;\Rightarrow h\pi\left[\begin{array}{l}2\cdot\left(\frac{4al^2}{15}+\frac{8b_2l}{15}\right)\cdot T_4+\\ \frac{2b_2l}{15}\cdot T_3+\left(\frac{2al^2}{15}+\frac{2b_2l}{15}\right)\cdot T_5-\\ -\left(\frac{2al^2}{3}+\frac{4b_2l}{3}\right)\cdot T_0\end{array}\right]+\frac{\pi K_{xx}}{2}$$

$$\left[\begin{array}{l}2\cdot\left(\frac{32a^2l}{15}+\frac{16ab_2}{3}+\frac{16b_2^2}{3l}\right)\cdot T_4-\\ \left(\frac{4a^2l}{5}+\frac{8ab_2}{3}+\frac{16b_2^2}{3l}\right)\cdot\\ \cdot T_3-\left(\frac{52a^2l}{15}+8ab_2+\frac{16b_2^2}{3l}\right)\cdot T_5\end{array}\right]=0;$$

$$5)\ \frac{\partial J}{\partial T_5}=0;\Rightarrow h\pi\left[\begin{array}{l}2\cdot\left(\frac{7al^2}{60}+\frac{2b_2l}{15}\right)\cdot T_5-\\ \left(\frac{al^2}{30}+\frac{b_2l}{15}\right)\cdot T_3+\left(\frac{2al^2}{15}+\frac{2b_2l}{15}\right)\cdot T_4-\\ -\left(\frac{al^2}{3}+\frac{b_2l}{3}\right)\cdot T_0\end{array}\right]+\frac{\pi K_{xx}}{2}$$

$$\left[\begin{array}{l}\left(\frac{2a^2l}{5}+\frac{2ab_2}{3}+\frac{2b_2^2}{3l}\right)\cdot T_3-\left(\frac{52a^2l}{15}+8ab_2+\frac{16b_2^2}{3l}\right)\cdot T_4+\\ +2\cdot\left(\frac{26a^2l}{15}+\frac{a(11b_2+3b_3)}{3}+\frac{7(b_2^2+b_3^2)}{3l}\right)\cdot T_5-\\ \left(\frac{4a^2l}{5}+\frac{8ab_3}{3}+\frac{16b_3^2}{3l}\right)\cdot T_6+\\ +\left(\frac{2a^2l}{5}+\frac{2ab_3}{3}+\frac{2b_3^2}{3l}\right)\cdot T_7\end{array}\right]=0;$$

$$6)\ \frac{\partial J}{\partial T_6}=0;\Rightarrow\frac{\pi K_{xx}}{2}\left[\begin{array}{l}2\cdot\left(\frac{32a^2l}{15}+\frac{16ab_3}{3}+\frac{16b_3^2}{3l}\right)\cdot T_6-\\ \left(\frac{4a^2l}{5}+\frac{8ab_3}{3}+\frac{16b_3^2}{3l}\right)\cdot T_5+\\ -\left(\frac{52a^2l}{15}+8ab_3+\frac{16b_3^2}{3l}\right)\cdot T_7\end{array}\right]=0;$$

$$7)\frac{\partial J}{\partial T_7}=0;\Rightarrow\frac{\pi K_{xx}}{2}$$
$$\left[2\cdot\left(\frac{23a^2l}{15}+\frac{11ab_3}{3}+\frac{7b_3^2}{3l}\right)\cdot T_7+\right.$$
$$\left(\frac{2a^2l}{5}+\frac{2ab_3}{3}+\frac{2b_3^2}{3l}\right)\cdot T_5-$$
$$\left.-\left(\frac{52a^2l}{15}+8ab_3+\frac{16b_3^2}{3l}\right)\cdot T_6\right]+\pi(3al+b)^2\cdot q=0.$$

Solving this system we define nodal values of temperatures T1,T2,…,T7. On them the distribution law of temperature longwise of each site of the studied rod is under construction. For the first site $(0\le x\le l)$ of a rod it has the following appearance:

$$T^{(I)}(x)=\varphi_i(x)\cdot T_1+\varphi_j(x)\cdot T_2+\varphi_k(x)\cdot T_3 \tag{7}$$

Similar to the field of temperatures longwise of the 2nd and 3rd sites of a rod has an appearance:

$$T^{(II)}(x)=\varphi_i(x)\cdot T_3+\varphi_j(x)\cdot T_4+\varphi_k(x)\cdot T_5$$
$$T^{(III)}(x)=\varphi_i(x)\cdot T_5+\varphi_j(x)\cdot T_6+\varphi_k(x)\cdot T_7 \tag{8}$$

If one end of a rod it is rigidly jammed, and another is free, then because of existence of diverse types of sources of heat it is extended. The size of lengthening is defined on the basis of fundamental laws of an applied thermal physics [1]:

$$\Delta l_T=\int_0^L\alpha\cdot T(x)dx. \tag{9}$$

In case of jamming of two ends of a rod, the rod can't is extended, and owing to existence of diverse types of sources of heat there is axial R[kG] squeezing efforts. The size of this effort is defined from a consistency relation of deformation [4].

$$R=-\frac{E\cdot F_{av}\cdot\Delta l_T}{L}. \tag{10}$$

where $F_{av}=\frac{\int_0^L F(x)dx}{L}$ – average area of a transverse section.

In case of jamming of two ends of a rod there is also a field of distribution of the being deformations and tension. The distribution law of a thermoelastic component of tension is defined according to a Hooke law [4].

$$\sigma(x)=\frac{R}{F(x)},\qquad 0\le x\le l \tag{11}$$

In compliance of a Hooke law [4] it is also possible to construct the distribution law of a thermoelastic component of deformations Ɛ (x) [dimensionless]:

$$\varepsilon(x) = \frac{\sigma(x)}{E}, \quad 0 \le x \le l \tag{12}$$

In compliance the law of a thermal physics [2] the field of distribution of a temperature component of deformations is under construction:

$$\varepsilon T(x) = -\alpha\, T(x), \quad 0 \le x \le l \tag{13}$$

Then according to the generalized Hooke law [4] the distribution law of a temperature component of tension is defined

$$\sigma_T(x) = E \cdot \varepsilon_T(x), \quad 0 \le x \le l \tag{14}$$

At last in compliance of the theory of a thermoelasticity [4] it is possible to construct distribution laws of elastic components of deformations and tension

$$\varepsilon_x(x) = \varepsilon(x) - \varepsilon_T(x),$$
$$\sigma_x(x) = E \cdot \varepsilon_x(x) = \sigma(x) - \sigma_T(x), \quad 0 \le x \le l \tag{15}$$

For definition the field of movement we will write a functional potential to energy of elastic deformation in the presence the field of temperatures for one discrete element [4]:

$$\Pi = \int_V \frac{\sigma_x(x)}{2} \varepsilon_x(x) dv -$$
$$\int_V \alpha E \cdot T(x) \cdot \varepsilon_x(x) dv =$$
$$\frac{E}{2} \int_v \varepsilon_x^2 dv - \alpha E \int_V T(x) \cdot \varepsilon_x(x) dv =$$
$$= \frac{E\pi}{2} \int_0^l F(x) \left(\frac{\partial U}{\partial x} \right)^2 dx -$$
$$\alpha E \pi \int_0^l F(x) \cdot T(x) \frac{\partial U}{\partial x} dx =$$
$$\frac{E\pi}{2} \int_0^l \left(a^2 x^2 + 2abx + b^2 \right) \cdot$$
$$\cdot \left[\frac{4x - 3l}{l^2} U_i + \frac{4l - 8x}{l^2} U_j + \frac{4x - l}{l^2} U_k \right]^2 dx$$
$$- \alpha E \pi \int_0^l \left(a^2 x^2 + 2abx + b^2 \right) \cdot$$

$$\cdot\left[\frac{2x^2-3lx+l^2}{l^2}\cdot U_i\,\frac{4lx-4x^2}{l^2}\cdot U_j+\frac{2x^2-lx}{l^2}\cdot U_k\right]\cdot$$

$$\left[\frac{4x-3l}{l^2}U_i+\frac{4l-8x}{l^2}U_j+\frac{4x-l}{l^2}U_k\right]^2 dx \qquad (16)$$

where $U(x)=\varphi_i(x)\cdot U_i+\varphi_j(x)\cdot U_j+\varphi_k(x)\cdot U_k,\ 0\le x\le l$.

After an integration it has an appearance:

$$
\begin{aligned}
&+\frac{7(b_1^2+b_2^2)}{3l}\Bigg)\cdot U_3^2\Bigg]+\\
&\Bigg[-\left(\frac{4a^2l}{5}+\frac{8ab_2}{3}+\frac{16b_2^2}{3l}\right)\cdot U_3U_4+\left(\frac{2a^2l}{5}+\frac{2ab_2}{3}+\frac{2b_2^2}{3l}\right)\cdot U_3U_5+\\
&+\left(\frac{32a^2l}{15}+\frac{16ab_2}{3}+\frac{16b_2^2}{3l}\right)\cdot U_4^2-\left(\frac{52a^2l}{15}+8ab_2+\frac{16b_2^2}{3l}\right)\cdot U_4U_5+\\
&\Bigg(\frac{26a^2l}{15}+\frac{a(11b_2+3b_3)}{3}+\\
&+\frac{7(b_2^2+b_3^2)}{3l}\Bigg)\cdot U_5^2\Bigg]+\Bigg[-\left(\frac{4a^2l}{5}+\frac{8ab_3}{3}+\frac{16b_3^2}{3l}\right)\cdot U_5U_6+\\
&\left(\frac{2a^2l}{5}+\frac{2ab_3}{3}+\frac{2b_3^2}{3l}\right)\cdot U_5U_7+\\
&+\left(\frac{32a^2l}{15}+\frac{16ab_3}{3}+\frac{16b_3^2}{3l}\right)\cdot U_6^2-\left(\frac{52a^2l}{15}+8ab_3+\frac{16b_3^2}{3l}\right)\cdot U_6U_7+\\
&\left(\frac{23a^2l}{15}+\frac{11ab_3}{3}+\frac{7b_3^2}{3l}\right)\cdot U_7^2\Bigg]
\end{aligned}
$$

$$
\Pi=\frac{E\pi}{2}\Bigg\{\Bigg[\left(\frac{a^2l}{5}+ab_1+\frac{7b_1^2}{3l}\right)\cdot U_1^2-\left(\frac{4a^2l}{5}+\frac{8ab_1}{3}+\frac{16b_1^2}{3l}\right)\cdot U_1U_2+\left(\frac{2a^2l}{5}+\frac{2ab_1}{3}+\frac{2b_1^2}{3l}\right)\cdot U_1U_3+
$$

$$
\begin{aligned}
&+\left(\frac{32a^2l}{15}+\frac{16ab_1}{3}+\frac{16b_1^2}{3l}\right)\cdot U_2^2-\\
&\left(\frac{52a^2l}{15}+8ab_1+\frac{16b_1^2}{3l}\right)\cdot U_2U_3+\\
&\left(\frac{26a^2l}{15}+\frac{a(11b_1+3b_2)}{3}+\right.\\
&\left.+\frac{b_1^2-2b_2^2}{2}\right)T_3U_3\Bigg]+\\
&\Bigg[\left(\frac{a^2l^2}{15}+\frac{4ab_2l}{15}+\frac{2b_2^2}{3}\right)\cdot T_3U_4-\left(\frac{a^2l^2}{20}+\frac{2ab_2l}{15}+\frac{b_2^2}{6}\right)\cdot T_3U_5\\
&-\left(\frac{a^2l^2}{15}+\frac{2ab_2l}{5}+\right.\\
&\left.+\frac{2b_2^2}{3}\right)\cdot T_4U_3-\\
&\left(\frac{4a^2l^2}{15}+\frac{8ab_2l}{15}\right)\cdot T_4U_4+\\
&\left(\frac{a^2l^2}{3}+\frac{4ab_2l}{15}+\frac{2b_2^2}{3}\right)\cdot T_4U_5+\\
&\left(\frac{a^2l^2}{12}+\frac{ab_2l}{5}+\frac{b_2^2}{6}\right)\cdot T_5U_3-
\end{aligned}
$$

$$
\begin{aligned}
&-\alpha E\pi\Bigg[-\left(\frac{a^2l^2}{60}+\frac{2ab_1l}{15}+\frac{b_1^2}{2}\right)\cdot T_1U_1+\\
&\left(\frac{a^2l^2}{15}+\frac{4ab_1l}{15}+\frac{2b_1^2}{3}\right)\cdot T_1U_2-\\
&\left(\frac{a^2l^2}{20}+\frac{2ab_1l}{15}+\frac{b_1^2}{6}\right)\cdot T_1U_3-\\
&-\left(\frac{a^2l^2}{15}+\frac{2ab_1l}{5}+\frac{2b_1^2}{3}\right)\cdot T_2U_1-\\
&\left(\frac{4a^2l^2}{15}+\frac{8ab_1l}{15}\right)\cdot T_2U_2+\left(\frac{a^2l^2}{3}+\frac{14ab_1l}{15}+\frac{2b_1^2}{3}\right)\cdot T_2U_3\\
&+\left(\frac{a^2l^2}{12}+\frac{ab_1l}{5}+\frac{b_1^2}{2}\right)\cdot T_3U_1-\\
&\left(\frac{7a^2l^2}{15}+\frac{16ab_1l}{15}+\frac{2b_1^2}{3}\right)\cdot T_3U_2+\\
&\left(\frac{22a^2l^2}{60}+\frac{11al(b_1-b_2)}{15}+\right.
\end{aligned}
$$

$$-\left(\frac{7a^2l^2}{15}+\frac{16ab_2l}{15}+\frac{2b_2^2}{3}\right)\cdot T_5U_4+$$
$$\left(\frac{22a^2l^2}{60}+\frac{al(13b_2-2b_3)}{15}+\frac{b_2^2-b_3^2}{2}\right)\cdot T_5U_5\Bigg]+$$
$$\Bigg[\Bigg(\frac{a^2l^2}{15}+\frac{4ab_3l}{15}+$$
$$+\frac{2b_3^2}{2}\Bigg)\cdot T_5U_6-\left(\frac{a^2l^2}{20}+\frac{2ab_3l}{15}+\frac{b_3^2}{6}\right)\cdot T_5U_7$$
$$-\left(\frac{a^2l^2}{15}+\frac{2ab_3l}{5}+\frac{2b_3^2}{3}\right)\cdot T_6U_5-$$
$$\left(\frac{4a^2l^2}{15}+\frac{8ab_3l}{15}\right)\cdot T_6U_6+$$
$$+\left(\frac{a^2l^2}{3}+\frac{14ab_3l}{15}+\frac{2b_3^2}{3}\right)\cdot T_6U_7+$$
$$\left(\frac{a^2l^2}{12}+\frac{ab_3l}{5}+\frac{b_3^2}{6}\right)\cdot T_7U_5-$$
$$\left(\frac{7a^2l^2}{15}+\frac{16ab_3l}{15}+\frac{2b_3^2}{3}\right)\cdot T_7U_6+$$
$$+\left(\frac{23a^2l^2}{60}+\frac{13ab_3l}{15}+\frac{b_3^2}{2}\right)\cdot T_7U_7\Bigg]\Bigg\} \qquad (17)$$

For determination of value of movement of sections we minimize a functional of a potential energy on nodal points:

$$1)\frac{\partial\Pi}{\partial U_1}=0;\Rightarrow\frac{E\pi}{2}\Bigg[2\cdot\left(\frac{a^2l}{5}+ab_1+\frac{7b_1^2}{3l}\right)\cdot U_1$$
$$-\left(\frac{4a^2l}{5}+\frac{8ab_1}{3}+\frac{16b_1^2}{3l}\right)\cdot U_2+$$
$$\left(\frac{2a^2l}{5}+\frac{2ab_1}{3}+\frac{2b_1^2}{3l}\right)\cdot$$
$$\cdot U_3\Bigg]-\alpha E\pi\Bigg[-\left(\frac{a^2l^2}{60}+\frac{2ab_1l}{15}+\frac{b_1^2}{2}\right)\cdot T_1$$
$$-\left(\frac{a^2l^2}{15}+\frac{2ab_1l}{5}+\frac{2b_1^2}{3}\right)\cdot T_2+$$
$$\left(\frac{a^2l^2}{12}+\frac{ab_1l}{5}+\frac{b_1^2}{6}\right)\cdot T_3\Bigg]=0;$$

$$2)\frac{\partial \Pi}{\partial U_2}=0;\Rightarrow \frac{E\pi}{2}\left[\begin{array}{l}-\left(\frac{4a^2l}{5}+\frac{8ab_1}{3}+\frac{16b_1^2}{3l}\right)\cdot U_1\\ +2\left(\frac{32a^2l}{15}+\frac{16ab_1}{3}+\frac{16b_1^2}{3l}\right)\cdot U_2-\end{array}\right.$$

$$\left(\frac{52a^2l}{5}+8ab_1+\right.$$

$$\left.+\frac{16b_1^2}{3l}\right)\cdot U_3\Bigg]-\alpha E\pi\left[\left(\frac{a^2l^2}{15}+\frac{4ab_1l}{15}+\frac{2b_1^2}{3}\right)\cdot T_1-\right.$$

$$\left.\left(\frac{4a^2l^2}{15}+\frac{8ab_1l}{15}\right)\cdot T_2-\left(\frac{7a^2l^2}{15}+\frac{16ab_1l}{15}+\frac{2b_1^2}{3}\right)\cdot T_3\right]=0;$$

$$3)\frac{\partial \Pi}{\partial U_3}=0;\Rightarrow \frac{E\pi}{2}\left[\begin{array}{l}\left(\frac{2a^2l}{5}+\frac{2ab_1}{3}+\frac{2b_1^2}{3l}\right)\cdot U_1\\ -\left(\frac{52a^2l}{15}+8ab_1+\frac{16b_1^2}{3l}\right)\cdot U_2+\end{array}\right.$$

$$2\left(\frac{26a^2l}{15}+\frac{a(11b_1+3b_2)}{3}+\right.$$

$$\left.+\frac{7(b_1^2+b_2^2)}{3l}\right)\cdot U_3\Bigg]-\alpha E\pi\left[-\left(\frac{a^2l^2}{20}+\frac{2ab_1l}{15}+\frac{b_1^2}{6}\right)\cdot T_1\right.$$

$$+\left(\frac{a^2l^2}{3}+\frac{14ab_1l}{15}+\frac{2b_1^2}{3}\right)\cdot T_2+\left(\frac{22a^2l^2}{60}+\right.$$

$$\left.\left.\begin{array}{l}+\frac{al(13b_1-2b_2)}{15}+\frac{b_1^2-b_2^2}{2}\Big)\cdot T_3-\\ \left(\frac{a^2l^2}{15}+\frac{2ab_2l}{5}+\frac{2b_2^2}{3}\right)\cdot T_4+\left(\frac{a^2l^2}{12}+\frac{ab_2l}{5}+\frac{b_2^2}{6}\right)\cdot T_5\end{array}\right]=0;$$

$$4)\frac{\partial \Pi}{\partial U_4}=0;\Rightarrow \frac{E\pi}{2}\left[\begin{array}{l}-\left(\frac{4a^2l}{5}+\frac{8ab_2}{3}+\frac{16b_2^2}{3l}\right)\cdot U_3\\ +2\left(\frac{32a^2l}{15}+\frac{16ab_2}{3}+\frac{16b_2^2}{3l}\right)\cdot U_4-\end{array}\right.$$

$$2\left(\frac{52a^2l}{15}+8ab_2+\right.$$

$$\left.+\frac{16b_2^2)}{3l}\right)\cdot U_5\Bigg]-\alpha E\pi\left[\left(\frac{a^2l^2}{15}+\frac{4ab_2l}{15}+\frac{2b_2^2}{3}\right)\cdot T_3\right.$$

$$\left.-\left(\frac{4a^2l^2}{15}+\frac{8ab_2l}{15}\right)\cdot T_4-\left(\frac{7a^2l^2}{15}+\frac{16ab_2l}{15}+\frac{2b_2^2}{3}\right)\cdot T_5\right]=0;$$

$$5)\frac{\partial \Pi}{\partial U_3}=0;\Rightarrow \frac{E\pi}{2}\left[\begin{array}{l}\left(\frac{2a^2l}{5}+\frac{2ab_2}{3}+\frac{2b_2^2}{3l}\right)\cdot U_3\\ -\left(\frac{52a^2l}{15}+8ab_2+\frac{16b_2^2}{3l}\right)\cdot U_4+\end{array}\right.$$

$$2\left(\frac{26a^2l}{15}+\frac{a(11b_2+3b_3)}{3}+\right.$$

$$+\frac{7(b_2^2+b_3^2)}{3l}\Bigg)\cdot U_5-\left(\frac{4a^2l}{5}+\frac{8ab_3}{3}+\frac{16b_3^2}{3l}\right)\cdot U_6$$

$$+\left(\frac{2a^2l}{5}+\frac{2ab_3}{3}+\frac{2b_3^2}{3l}\right)\cdot U_7\Bigg]$$

$$-\alpha E\pi\Bigg[-\left(\frac{a^2l^2}{20}+\frac{2ab_2l}{15}+\frac{b_2^2}{6}\right)\cdot T_3+$$

$$+\left(\frac{a^2l^2}{3}+\frac{14ab_2l}{15}+\frac{2b_2^2}{3}\right)\cdot T_4+$$

$$\left(\frac{22a^2l^2}{60}+\frac{al(13b_2-2b_3)}{15}+\frac{b_2^2-b_3^2}{2}\right)\cdot T_5$$

$$-\left(\frac{a^2l^2}{15}+\frac{2ab_3l}{5}+\frac{2b_3^2}{3}\right)\cdot T_6+\left(\frac{a^2l^2}{12}+\right.$$

$$\left.+\frac{ab_3l}{5}+\frac{b_3^2}{6}\right)\cdot T_7\Bigg]=0;$$

$$6)\frac{\partial\Pi}{\partial U_6}=0;\Rightarrow\frac{E\pi}{2}\Bigg[-\left(\frac{4a^2l}{5}+\frac{8ab_3}{3}+\frac{16b_3^2}{3l}\right)\cdot U_5$$

$$+2\left(\frac{32a^2l}{15}+\frac{16ab_3}{3}+\frac{16b_3^2}{3l}\right)\cdot U_6-$$

$$\left(\frac{52a^2l}{15}+8ab_3+\right.$$

$$\left.+\frac{16b_3^2)}{3l}\right)\cdot U_7\Bigg]-\alpha E\pi\Bigg[\left(\frac{a^2l^2}{15}+\frac{4ab_3l}{15}+\frac{2b_3^2}{3}\right)\cdot T_5$$

$$-\left(\frac{4a^2l^2}{15}+\frac{8ab_3l}{15}\right)\cdot T_6-\left(\frac{7a^2l^2}{15}+\frac{16ab_3l}{15}+\frac{2b_3^2}{3}\right)\cdot T_7\Bigg]=0;$$

$$7)\frac{\partial\Pi}{\partial U_7}=0;\Rightarrow\frac{E\pi}{2}\Bigg[\left(\frac{2a^2l}{5}+\frac{2ab_3}{3}+\frac{2b_3^2}{3l}\right)\cdot U_5-$$

$$\left(\frac{52a^2l}{15}+8ab_3+\frac{16b_3^2}{3l}\right)\cdot U_6+$$

$$2\left(\frac{23a^2l}{15}+\frac{11ab_3}{3}+\frac{7b_3^2}{3l}\right)\cdot U_7\Bigg]-$$

$$-\alpha E\pi\Bigg[-\left(\frac{a^2l^2}{20}+\frac{2ab_3l}{15}+\frac{b_3^2}{6}\right)\cdot T_5+$$

$$\left(\frac{a^2l^2}{3}+\frac{14ab_3l}{15}+\frac{2b_3^2}{3}\right)\cdot T_6+$$

$$\left(\frac{23a^2l^2}{60}+\frac{13ab_3l}{15}+\frac{b_3^2}{2}\right)\cdot T_7\Bigg]=0;$$

Solving this system we define values U1, U1,…,U7. Then the field of relocation longwise of each site of the studied rod are defined as follows:

$$\left.\begin{aligned} U^{(I)}(x) &= \varphi_i(x)\cdot U_1 + \varphi_j(x)\cdot U_2 + \varphi_k(x)\cdot U_3 \\ U^{(II)}(x) &= \varphi_i(x)\cdot U_3 + \varphi_j(x)\cdot U_4 + \varphi_k(x)\cdot U_5 \\ U^{(III)}(x) &= \varphi_i(x)\cdot U_5 + \varphi_j(x)\cdot U_6 + \varphi_k(x)\cdot U_7 \end{aligned}\right\}, \qquad 0 \le x \le l \qquad (19)$$

4. NUMERICAL RESULTS

For approbation of the developed methods and algorithms we will solve the formulated problem at the following input datas

L=30cm; $a = -\frac{1}{10}$; $b = 12cm$; $\alpha = 0{,}0000125\frac{1}{^0K}$; $E = 2\cdot 10^6\,\frac{кG}{cm^2}$;

$K_{xx} = 100\frac{watt}{cm\cdot{}^0K}$; $h = 10\frac{watt}{cm^2\cdot{}^0K}$;

$T_{oc} = 40^0K$; $q = -500\frac{watt}{cm^2}$;

The received decisions are provided on figures 2-5.

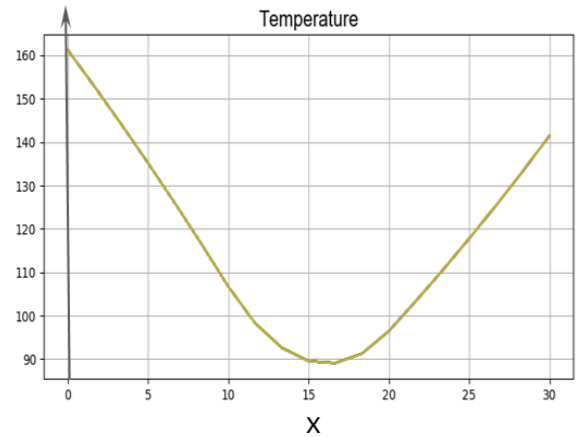


Figure 2: Dependences of temperature T the length of the rod

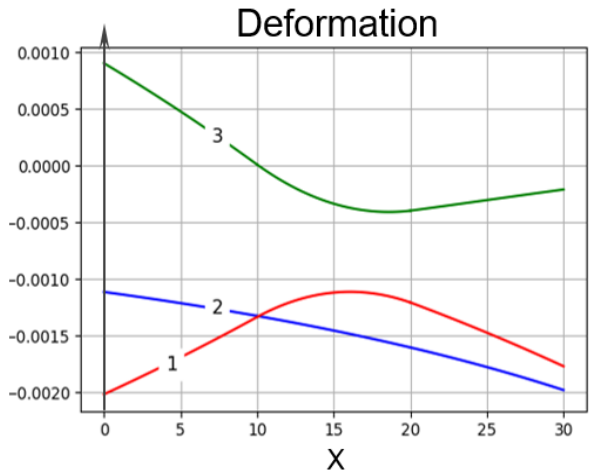


Figure 3: Dependences of deformation the length of the rod $1-\varepsilon(x);\ 3-\varepsilon_x(x);\ 2-\varepsilon_T(x)$

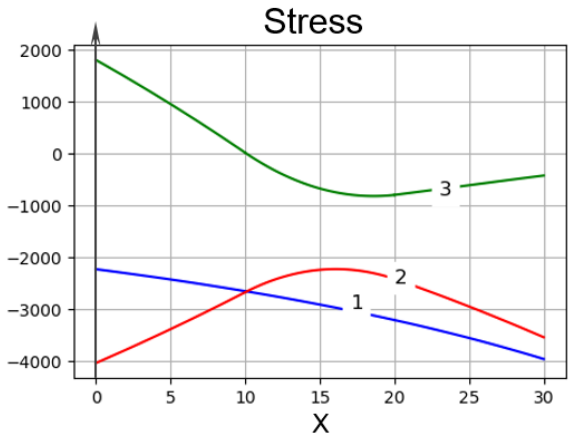


Figure 4: Dependences tensionthe length of the rod

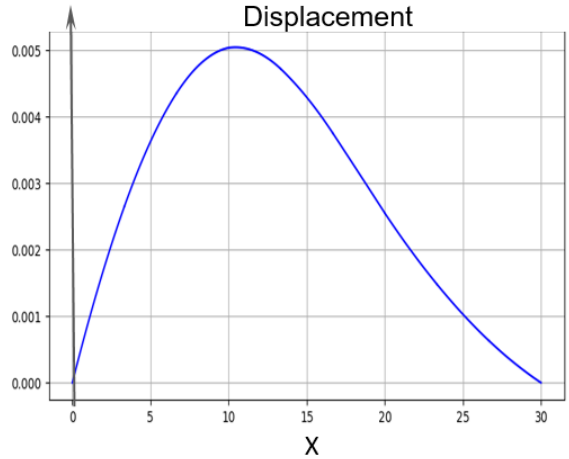


Figure 5: Dependences movementthe length of the rod $1-\sigma(x);\ 3-\sigma_x(x);\ \ 2-\sigma_T(x)$

For this example the sectional area of the left-hand end of a core is equal F(x=0)=144πcm2 and right end F(x=L)=81πcm2 it turns out (x=0)=1,77* (F(x=L)); From the figure-2 it is visible that value of temperature on the left-hand end of T(x=0)=161.230K, at that time on the right end of T(x=L)=141.4530K. It it is caused by the fact that the sectional area of the right end on 1.777 times is less than left-hand. The value of temperature is equal $T(x=\frac{5l}{3})=89.08^o K,$ in a point $x=\frac{5l}{3}$ it the least in all length of a rod.

It it is caused by the fact that through a lateral area of the site (l≤x≤2l) of a core there is a heat exchange to a surrounding medium, and variability of section. From the drawing it is visible that thermoelastic and temperature components of deformation on all length of a rod have the squeezing character while resilient making deformations Ɛx(x) on the site (0≤x≤l) of a rod has stretching, and in other sites the squeezing character. It is caused, the fact that the sectional area of the left-hand end of a rod is maximal, and there brought a heat flux with intensity $q=-500\frac{watt}{cm^2}.$

The similar phenomena are observed also in the nature. The distribution law of movement is provided in the figure-5. Where it is visible from the figure that all sections of a rod except jammed move at the left in the rights. At the same time maximal movements

corresponds to section with coordinate $x = \frac{4l}{3}$. This process is caused with a big sectional area of the left-hand end of a rod and existence of a heat flux constant intensity $q = -500 \frac{watt}{cm^2}$.

Also this phenomenon is promoted by existence of heat exchange through side the surface of the site (l≤x≤2l). After calculation the field of temperatures is defined the size of lengthening of a rod for a case of jamming of one end of a rod:

$$\Delta l_T = \int_0^L \alpha \cdot T(x)dx = 0{,}0432cm.$$

In case of jamming of two ends of a rod there is a squeezing axial force which size equally:

$$R = -\frac{E \cdot F_{av} \cdot \Delta l_T}{L} = -1006573{,}377[kG].$$

5. Conclusion

The method and computing algorithm is developed on a sonova of fundamental laws of conservation of energy, and also the program on Python allow to solve a class of tasks of definition established thermo - an intense strained state of a rod of variable section at influence of diverse types of local sources of heat taking into account existence of thermal insulations, physicomechanical and thermal characteristics of material of a rod, and also at its difficult geometrical sizes.

The received numerical results differ in a high precision and convergence. Besides the offered approach differs in the universality at the solution of relevant engineering tasks stationary thermoelasticities for rod stock of variable section.

Acknowledgments

This work was supported by the Committee of Science by the Ministry of Education of the Republic of Kazakhstan in the framework of the grant project AP05131093

References

1. G. Grimvall.Thermophysical Properties of Materials 1st Edition. – North Holland 1999. – 424 p.
2. Теплотехника / Под редакцией М.Г.Шатрова. М.: Академия, 2011. 288 с.
3. Gaspar Jr., Moreira M.L., Desampaio P.A.B. Temperature Distribution Fuel Rods: A study on the Effect of Eccentricity in the Position of U02 Pellets., 0-th International Conference «Nuclear Energy for New Europe», 2011.
4. Timoshenko S., Goodyear J. N. Theory of Elasticity. – McGRAW-Hill. Book. Company. Inc., 1987. – 567 p.

ОНЛАЙНОВЫЕ МОДЕЛИ НА ОСНОВЕ ВНИМАНИЯ ДЛЯ ИНТЕГРАЛЬНЫХ (END-TO-END) СИСТЕМ РАСПОЗНАВАНИЯ РЕЧИ

Мамырбаев О.Ж.[1], Оралбекова Д.О.[2]
e-mail: morkenj@mail.ru, dinaoral@mail.ru
[1]*Институт информационных и вычислительных технологий КН МОН РК, Казахстан*
[2]*Satbayev University, Казахстан*

Аннотация. *Автоматическое распознавание речи является стремительно развивающей областью в машинном обучении. Наиболее популярными системами распознавания речи на сегодня являются системы на основе интегрального (end-to-end) подхода, а особенно те модели, которые напрямую выводят последовательность слов с учетом входного звука в режиме реального времени, что представляют собой онлайновые модели end-to-end. В данной статье рассмотрен подробный обзор популярных онлайн-моделей на основе внимания для интегральных систем, такие как RNN-T, нейронный преобразователь (Neural Transducer; NT), монотонное внимание по фрагментам (Monotonic Chunkwise Attention; MoChA) и приведено краткое сравнение этих моделей.*

1 Введение

Традиционная система автоматического распознавания речи (АРР) представляет собой набор отдельных элементов, которыми являются акустическая модель (АМ), языковая модель (ЯМ) и декодер. АМ принимает акустические характеристики в качестве входных данных и прогнозирует распределение по подсловным единицам, обычно зависящим от содержания фонема. Декодер, который традиционно представляет собой составленный вручную лексикон, отображает последовательность единиц подслова, созданных акустической моделью, в слова. Наконец, ЯМ присваивает вероятности различным словесным гипотезам [1]. В традиционных системах ASR эти компоненты обучаются независимо на разных наборах данных с рядом предположений о независимости, которые сделаны для обеспечения управляемости.

За последние несколько лет отмечается повышенное внимание к разработке интегральных систем распознавания речи, которые объединяют все компоненты АРР в единую систему [2]. Модели на основе коннекционной временной классификации [3] (CTC), модели, на основе механизма внимания [4, 5], рекуррентный нейронный преобразователь [6, 7] (Recurrent Neural Transducer, RNN-T) и модели, на основе условных случайных полей (CRF) [8] являются наглядными примерами интегральных систем. CTC позволяет обучать акустическую модель без необходимости выравнивания на уровне кадра между акустикой и транкрибацией [3]. RNN-T дополняет модель на основе CTC рекурентным компонентом ЯМ. Эта компонента обучается совместно на имеющихся акустических данных. Как и в случае с CTC, этот метод не требует согласованных обучающих данных. В моделях кодер-декодера на основе механизма внимания, кодер является АМ – преобразует входную речь в высокоуровневое представление, механизм внимания – это и есть модель выравнивания, и определяет закодированные кадры, которые имеют

отношение к созданию текущего вывода, декодер аналогичен ЯМ – работает авторегрессивно, предсказывая каждый выходной токен в зависимости от предыдущих предсказаний [26]. Общая характеристика всех этих моделей является то, что они состоят из одной нейронной сети, которая при заданных входных акустических данных напрямую выводят распределение вероятностей по графемам или гипотезам слов. Действительно, как было продемонстрированы в недавних исследовательских работах [9, 10, 11], такие модели могут превосходить характеристики обычных систем ASR.

Основное преимущество интегральных моделей является не только высокая производительность с точки зрения скорости и точности распознавания речи, а также использование их локально на портативных устройствах. В последнее время проявился огромный интерес к обучению интегральных моделей для ASR, которые напрямую выводят последовательность слов с учетом входного звука. Распознавание потоковой речи позволяет передавать поток звука в преобразование речи в текст и получать результаты распознавания речи потока в реальном времени по мере обработки звука. Для реализации такой системы применяются онлайн-модели на основе внимания для интегральных систем, наиболее популярными являются RNN-T, нейронный преобразователь (Neural Transducer; NT) и монотонное внимание по фрагментам (Monotonic Chunkwise Attention; MoChA).

В данной статье мы осуществили подробный обзор онлайн моделей интегральных систем. Представили краткое сравнение этих моделей, подчеркнув при этом общие черты и различия между ними. В заключении даем свои выводы.

2 Рекуррентный нейронный преобразователь (RNN-T)

RNN-T был впервые предложен в работе [6, 7] как расширение подхода коннекционной временной классификации (CTC) [3] для задач маркировки последовательностей, в которых выравнивание между входной последовательностью x и выходными целями y неизвестно. Это достигается в формулировке CTC путем введения специальной метки, называемой пустой меткой, которая моделирует вероятность вывода метки, соответствующей данному входному кадру. Однако основным ограничением CTC является его предположение, что выходные данные модели в данном кадре не зависят от предыдущих выходных меток: $y_t \perp\!\!\!\perp y_j \mid x$ для $t<j$.

Модель RNN-T состоит из кодера [12], сети прогнозирования и совместной сети; как описано в [13], модель RNN-T можно сравнить с другими архитектурами кодера-декодера, такими как «listen, attend, and spell» [14], если мы рассматриваем комбинацию сети прогнозирования и объединенной сети как декодер. Кодер представляет собой RNN, который преобразует входной акустический кадр в представление более высокого уровня, и является аналогом AM на основе CTC в стандартном распознавателе речи [15]. Таким образом, как и в CTC, выходной сигнал сети кодера, обусловлен последовательностью предыдущих акустических кадров. RNN-T устраняет предположение об условной независимости в CTC, вводя сеть прогнозирования, RNN, которая явно обусловлена историей предыдущих непустых целей, предсказанных моделью. В частности, сеть прогнозирования принимает в качестве входных данных последнюю непустую метку для создания в качестве выходных данных. Наконец, объединенная сеть представляет собой сеть с прямой связью, которая объединяет выходные данные сети прогнозирования и

кодировщика для создания логитов, за которыми следует слой softmax для получения распределения по следующему выходному символу (рис. 1).

Во время каждого шага вывода в модель RNN-T подается следующий акустический кадр x_t и ранее предсказанная метка y_{u-1}, из которой модель производит следующие вероятности выходных меток $P(y|t, u)$. Если прогнозируемая метка y_u не является пустой, тогда сеть прогнозирования обновляется этой меткой в качестве входных данных для генерации следующих вероятностей выходной метки $P(y|t, u+1)$. И наоборот, если прогнозируется пустая метка, то следующий акустический кадр, x_{t+1}, используется для обновления кодировщика, при этом сохраняются те же выходные данные сети прогнозирования, что приводит к $P(y|t + 1, u)$. Таким образом, RNN-T может передавать результаты распознавания в поток, поочередно обновляя кодировщик и сеть прогнозирования в зависимости от того, является ли прогнозируемая метка пустой или непустой. Вывод прекращается, когда в последнем кадре T выводится пробел.

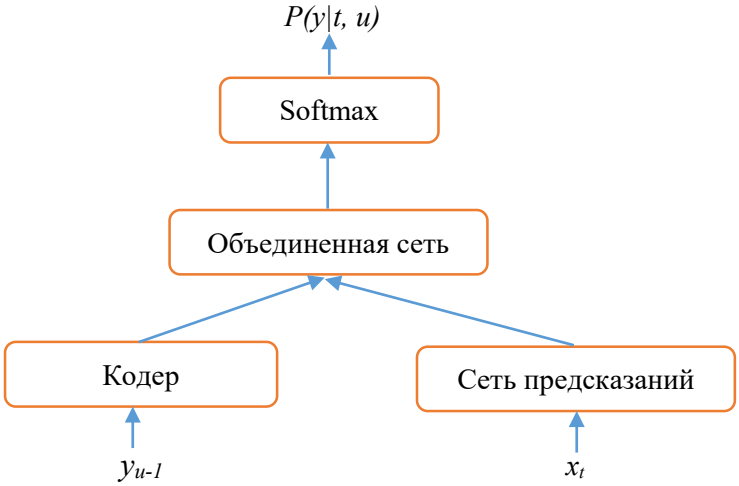


Рис. 1 Структура RNN-T

Во время логического вывода наиболее вероятная последовательность меток вычисляется с использованием поиска луча, как описано в [13], с незначительным изменением, которое, как было обнаружено, делает алгоритм менее ресурсоемким без ухудшения производительности: мы пропускаем суммирование по префиксам в *pref (y)*, если несколько гипотез не идентичны.

Kanishka Rao и др. обнаружили, что предварительное обучение кодера RNN-T с помощью CTC приводит к относительному улучшению WER на 5%, а использование более глубокого 8-уровневого кодера вместо 5-уровневого кодера дополнительно улучшает относительное значение WER на 10%.

В [16] модель RNN-T показала лучший результат – снижение WER до 15,0%, чем гибридная модель. В работе [17] было обнаружено, что модель RNN-T и RNN-T, дополненный вниманием, сопоставимы по своим характеристикам с сильной современной базовой линией на наборе для тестирования диктовки, даже при оценке без использования внешней языковой модели.

Необходимо обратить внимание, что в отличие от других архитектур потокового кодера-декодера, как NT [18], сеть прогнозирования не зависит от выходных данных кодера. Это позволяет предварительно обучить декодер в качестве языковой модели RNN на текстовых данных.

3 Нейронный преобразователь (Neural Transducer)

Neural Transducer (NT) может формировать часть выходных сигналов по мере поступления блоков входных данных, таким образом удовлетворяя условию «онлайн».

Речевой преобразователь обычно состоит из кодера, который преобразует акустические входы в представления высокого уровня, и декодера, который выдает лингвистические выходные данные, это символы или слова из закодированных представлений. Проблема заключается в том, что входные и выходные последовательности имеют переменную (также разную) длину, и обычно выравнивания между ними недоступны. Соневральные преобразователи должны изучить как классификацию от акустических характеристик до лингвистических предсказаний, так и согласование между ними. Модели датчиков различаются по составу классификатора и выравнивателя [19].

Более формально, учитывая входную последовательность $x = (x_1, .., x_T)$ длины T, и выходную последовательность $y = (y_1, ..., y_U)$ длины U, причем каждый y_u является V-мерным одноразовым вектором , преобразователи моделируют условное распределение $p(y \mid x)$. Кодер отображает вход x в высокоуровневое представление $h = (h_1, ..., h_{T'})$, которое может быть короче, чем входное ($T' \leq T$) с понижающей дискретизацией по шкале времени. Кодер может быть построен с использованием нейронных сетей с прямой связью (DNN), рекуррентных нейронных сетей (RNN) или сверточных нейронных сетей (CNN). Декодер определяет выравнивание и отображение от h до y [20].

В работе [21] в задаче распознавания фонем TIMIT нейронный преобразователь с трехуровневым однонаправленным кодировщиком LSTM и трехуровневым однонаправленным преобразователем LSTM достиг точности 20,8% коэффициента ошибок фонем (PER), что близко к современному уровню техники для однонаправленных моделей. А также было выявлено, что при наличии хороших согласований модель может достичь PER 19,8%.

4. Монотонное внимание по фрагментам (Monotonic Chunkwise Attention; MoChA)

Для разработки модели MoChA, необходимо для начала хорошо изучить структуру модели от последовательности к последовательности (seq2seq) и наиболее распространенную форму мягкого внимания, используемую с ней (описаны в работах [23, 17]).

Модель MoChA вычисляет контекст, используя два типа внимания: жесткое монотонное внимание и мягкое внимание по частям.

MoChA позволяет модели выполнять мягкое внимание над небольшими фрагментами памяти, предшествующими тому, где механизм жесткого монотонного внимания решил присутствовать. Он также имеет процедуру обучения, которая позволяет напрямую применять его к существующим моделям от последовательности к последовательности (seq2seq) и обучать с помощью стандартного обратного распространения ошибки. В [22] было показано, что MoChA эффективно сокращает разрыв между монотонным и мягким вниманием при распознавании речи в Интернете и обеспечивает относительное улучшение на 20% по сравнению с монотонным вниманием при резюмировании документов. Эти

преимущества влекут за собой лишь небольшое увеличение количества параметров и вычислительных затрат.

В [24] для потокового распознавания речи был использован подход на основе MoCha, в результате был получен WER в 9,95%. Экспериментально было показано [25], что MoChA обеспечивает высочайшую производительность при решении задачи распознавания речи в Интернете и существенно превосходит жесткую монотонную модель, основанную на внимании.

5 Заключение

В данной работе было рассмотрено текущее состояние основных онлайн–моделей на основе End2End-подхода распознавания потоковой речи. Следует отметить, что, к сожалению, данные подходы сегодня требуют большое количество данных, и это является основной проблемой этих моделей. Однако онлайн–модели интегральных систем хороши при наборе для тестирования диктовки без использования внешних ЯМ, но уступают при наборах голосового поиска от стандартных систем. В таком случае, в будущем такие модели дают возможность высококачественно распознавать слитную речь в режиме реального времени используя меньше вычислительных мощностей, при этом имея высокую производительность, чем другие модели АРР.

Литература

1. Казачкин А. Е. Методы распознавания речи, современные речевые технологии // Молодой ученый. — 2019. — №39. — С. 6-8. — URL https://moluch.ru/archive/277/62675/ (дата обращения: 01.08.2020)].

2. Мамырбаев О., Шаяхметова А., Кыдырбекова А., Турдалыулы М., Интегральный подход распознавания речи для агглютинативных языков, АУЭС Вестник, № 1(48) 2020

3. Graves A., Fernandez S., Gomez F., and Schmidhuber J. Connectionist Temporal Classification: Labelling Unsegmented Sequence Data with Recurrent Neural Networks. In ICML, Pittsburgh, USA, 2006.

4. Chorowski J. K., Bahdanau D., Serdyuk D., Cho, K., and Bengio Y. Attention-Based Models for Speech Recognition. In Advances in Neural Information Processing Systems, 2015, pages 577–585, Montréal, Canada.

5. W. Chan, N. Jaitly, Q. Le and O. Vinyals, "Listen, attend and spell: A neural network for large vocabulary conversational speech recognition," 2016 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Shanghai, 2016, pp. 4960-4964.

6. Graves, Alex & Mohamed, Abdel-rahman & Hinton, Geoffrey. Speech Recognition with Deep Recurrent Neural Networks. ICASSP, IEEE International Conference on Acoustics, Speech and Signal Processing - Proceedings. 2013.

7. Graves, A. Sequence transduction with recurrent neural networks, 2012, arXiv:1211.3711 .

8. E. Fosler-Lussier, Y. He, P. Jyothi, and R. Prabhavalkar, “Conditional random fields in speech, audio, and language processing,” Proceedings of the IEEE, vol. 101, no. 5, pp. 1054–1075, 2013.

9. Graves, A.; Jaitly, N. Towards end-to-end speech recognition with recurrent neural networks. In Proceedings of the International Conference on Machine Learning, Beijing, China, 21 June–26 June 2014; pp. 1764–1772.

10. Hori, T.; Watanabe, S.; Zhang, Y.; Chan, W. Advances in Joint CTC-Attention Based End-to-End Speech Recognition with a Deep CNN Encoder and RNN-LM. arXiv 2017, arXiv:1706.02737, 949–953.

11. Kim, S.; Hori, T.; Watanabe, S. Joint CTC-attention based end-to-end speech recognition using multi-task learning. In Proceedings of the 2017 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), New Orleans, LA, USA, 5–9 March 2017; pp. 4835–4839.

12. Y. He et al., "Streaming End-to-end Speech Recognition for Mobile Devices," ICASSP 2019 - 2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Brighton, United Kingdom, 2019, pp. 6381-6385.

13. R. Prabhavalkar, K. Rao, T. N. Sainath, B. Li, L. Johnson, and N. Jaitly, “A comparison of sequence-tosequence models for speech recognition,” in Interspeech, 2017.

14. W. Chan, N. Jaitly, Q. V. Le, and O. Vinyals, “Listen, attend and spell,” CoRR, vol. abs/1508.01211, 2015

15. Holmes, L.; LaHurd, A.; Wasson, E.; McClarin, L.; Dabney, K. Racial and Ethnic Heterogeneity in the Association Between Total Cholesterol and Pediatric Obesity. Int. J. Environ. Res. Public Health 2016, 13, 19 (article number: 19. https://www.mdpi.com/1660-4601/13/1/19).

16. J. Li, R. Zhao, H. Hu and Y. Gong, "Improving RNN Transducer Modeling for End-to-End Speech Recognition," 2019 IEEE Automatic Speech Recognition and Understanding Workshop (ASRU), SG, Singapore, 2019, pp. 114-121.

17. Prabhavalkar, Rohit & Rao, Kanishka & Sainath, Tara & Li, Bo & Johnson, Leif & Jaitly, Navdeep. A Comparison of Sequence-to-Sequence Models for Speech Recognition. 939-943. 10.21437/Interspeech. 2017-233.

18. N. Jaitly, Q. V. Le, O. Vinyals, I. Sutskever, D. Sussillo, and S. Bengio, “An online sequence-to-sequence model using partial conditioning,” in NIPS, 2016.

19. Sainath, Tara & Chiu, Chung-Cheng & Prabhavalkar, Rohit & Kannan, Anjuli & Wu, Yonghui & Nguyen, Patrick & Chen, ZhiJeng. Improving the Performance of Online Neural Transducer Models. pp. 5864-5868, 2018

20. Jaitly, Navdeep & Le, Quoc & Vinyals, Oriol & Sutskeyver, Ilya & Bengio, Samy. An Online Sequence-to-Sequence Model Using Partial Conditioning, 2015.

21. E. Battenberg et al., "Exploring neural transducers for end-to-end speech recognition," 2017 IEEE Automatic Speech Recognition and Understanding Workshop (ASRU), Okinawa, 2017, pp. 206-213.

22. Chung-Cheng Chiu and Colin Raffel, “Monotonic chunkwise attention,” in Proceedings of ICLR, 2018.

23. Chiu, Chung-Cheng & Sainath, Tara & Wu, Yonghui & Prabhavalkar, Rohit & Nguyen, Patrick & Chen, Zhifeng & Kannan, Anjuli & Weiss, Ron & Rao, Kanishka & Gonina, Ekaterina & Jaitly, Navdeep & Li, Bo & Chorowski, Jan & Bacchiani, Michiel. State-of-the-Art Speech Recognition with Sequence-to-Sequence Models. 4774-4778. 10.1109/ICASSP.2018.8462105., 2018.

24. Kim, Chanwoo & Kim, Sungsoo & Kim, Kwangyoun & Kumar, Mehul & Kim, Jiyeon & Lee, Kyungmin & Han, Changwoo & Garg, Abhinav & Kim, Eunhyang & Shin, Minkyoo & Singh, Shatrughan & Heck, Larry & Gowda, Dhananjaya. End-to-End Training of a Large Vocabulary End-to-End Speech Recognition System. 10.1109/ASRU46091.2019.9003976, 2019.

25. Hou, J., Guo, W., Song, Y. et al. Segment boundary detection directed attention for online end-to-end speech recognition. J AUDIO SPEECH MUSIC PROC. 2020.

26. Wang, D.; Wang, X.; Lv, S. An Overview of End-to-End Automatic Speech Recognition. Symmetry 2019, 11, 1018.

USE OF SPHTS AS A MEANS OF PROTECTION IN AIRCRAFT.

Demesinova S.[1], Alipbayev K.[2]
Sayle23@mail.ru, k.alipbayev@aues.kz
Doctoral student of Al-Farabi Kazakh National University, Kazakhstan[1]
AUPET named after. Gumarbek Daukeev, Kazakhstan[2]

Annotation. *One of the most promising directions in the field of obtaining new composite materials with a high level of complementary performance characteristics is the creation of intermetallic compounds of the Ti-Al system and the improvement of their production technology. Titanium aluminides are lighter, do not require expensive and scarce elements for alloying, which means they are cheaper, have high corrosion resistance and resistance to high-temperature oxidation. However, the mechanisms of structure formation during high-temperature synthesis in this system are insufficiently studied. In particular, the synthesis modes for the formation of a single-phase product of a particular stoichiometry are unknown. Thus, the creation of an experimental complex for the production of composite materials and the possibility of using SPHT-synthesis products in detonation-gas sputtering to obtain protective coatings is an urgent task.*

Report text. The current level of technological and industrial development of mechanical engineering, characterized by a qualitative increase in the intensity of operating modes of machines and equipment, implies an acceleration of the rate of expansion of production of composite materials and products, in which ensuring optimal effective properties is achieved by the presence of phases in the structure with complementary complexes of physical, mechanical and other parameters.

The combination of unique properties of titanium, such as high hardness, low density, and high operating temperature, has become the main application for its intensity in the manufacture of aircraft elements, hot path parts for stationary power plants and turbo heaters, and equipment parts for industry, including non-ferrous steel refining.

A process that has significant technological potential for obtaining composite materials with special properties is self-propagating high-temperature synthesis (SPHTS), discovered by academician A.G. Merzhanov and his scientific school. [1]. Having a number of common features with the technological processes of traditional powder metallurgy, SPHT-synthesis is characterized by such a unique feature as the existence of a high-temperature solid-liquid medium during the interaction, which allows various types of additional external influences, through which it is possible to regulate the structure and properties of the target products (materials). The combination of possible directional effects on the reaction medium and their combinations determines a variety of options for implementing the process of combustions operation and the corresponding set of technological processes. Composite materials synthesized using SPHTS technologies have

a wide range of applications in mechanical engineering, aircraft construction, shipbuilding, etc., primarily as protective coatings. These materials are characterized primarily by high heat resistance, heat resistance, hardness, and resistance to aggressive media. Production of protective coatings is carried out by methods of gas-thermal spraying, which include methods of detonation-gas, electric-arc and plasma spraying [2], which differ in the speeds and temperatures of the processes. The use of composite powders of various phase compositions and sizes as sprayed materials makes it possible to vary the physical and chemical properties of coatings.

The simplest classification of SHS processes is associated with a comparison of the calculated adiabatic combustion temperatures T_{ad} with the melting temperatures of the components, or with the value of the smallest eutectic temperature in the state diagram T_l .In accordance with this, three options are possible:

а) $T_{ad} < T_l$. The combustion process takes place in the solid phase. In this case, the condition for gasless combustion is: $p(T_г) << p_0$, where p - the vapor pressure of the most volatile component at the combustion temperature, p_0 - ambient pressure .

б) $T_{ad} > T_l$. The adiabatic combustion temperature is higher than the melting point of the components, while the solubility in the liquid phase is unlimited. In this case, melting ends in the preheating zone and chemical interaction occurs in the liquid phase. Here combustion is described in terms of the well-studied kinetic functions of homogeneous kinetics [5,6]

в) The combustion temperature is higher than the melting point of one of the components. In this case, the combustion process is heterogeneous and belongs to the most complex and widespread type of interaction. Naturally, such a division is conditional, since the synthesis mechanism largely depends on the physical environment of the process.

Typically, type (a) systems capable of interacting in the solid phase consist of refractory elements.

The interaction process occurs on the contact surface of dissimilar particles, which leads to the diffusion nature of heat release. There is no longitudinal diffusion transfer of synthesis products, which excludes their penetration into the pre-flame zone. This leads to the emergence of a maximum enthalpy in the combustion zone, which affects the stability of the stationary regime of the combustion wave.

Titanium and titanium alloys are widely used in many industries.

The combination of unique properties of titanium, such as high hardness, low density, and high operating temperature, has become the main application for its intensity in the manufacture of aircraft elements, hot section parts for stationary power plants and turbo heaters, equipment parts for industry, including non-ferrous oil refining steels.

Over time, as it is known, the strength of parts operating under stress at elevated temperatures decreases. The higher the operating temperature, the faster the detail strength decreases, and, consequently, the safety margin. The improvement in their performance without much increase in price and drastic change in production technology is unusually sharp. Currently, new methods of metallization of titanium and its alloy are being developed, among which aluminization is given special attention due to the fact that coatings based on titanium aluminides are multifunctional in themselves. Aluminum phases on the surface increase its corrosion resistance, heat resistance and heat resistance, and thus do not affect the mechanical properties of the matrix.

In the process of performing research works, the analysis of literature data on patent research on the problem of studying the diffusional interaction and equilibrium in the study of the Ti-Al system is carried out. Based on this, it can be concluded that the data obtained in the dissertation work, using the latest laboratory equipment, on the formation of aluminide layers in the Ti-Al system, are unique in their kind and correspond to the current level of scientific research.

The problem of increasing the service life of parts and assemblies of mechanisms is especially urgent. In this regard, the use of intermetallic compounds as protective and hardening coatings in many cases may be the only way to solve the problem among intermetallic compounds, titanium aluminides occupy a special place.

Titanium aluminides (TiAl, Ti_3Al_4, Al_3Ti) and alloys based on them belong to a new class of light heat-resistant materials, which are designed to operate at a temperature of 700-1100% higher than the temperatures at which modern test simereplas work (Tp $<600^0$C). Low density, high specific strength, rigidity, fracture toughness and high resistance to oxidation and combustion make them promising materials not only in aerospace engineering, but also in all energy-intensive industries. It is predicted that in the very near future titanium aluminides will replace heat-resistant alloys based on float metals. Currently, the use of titanium aluminides as protective coatings on the surface of titanium and aluminum alloys is being considered.

Literature

1. Merzhanov A.G., Borovinskaya I.P. Self-propagating high-temperature synthesis of inorganic compounds. // Rep. A.H. SSSR. 1972. т.201. №2. С. 366 - 369.
2. Powder metallurgy and sprayed coatings. Editing. Mitina B.S. M.: Metallurgy. 1987.791p.
3. Merzhanov A.G. The theory of gasless combustion. Chernogolovka, 1973, - 25p. (Preprint ОИХФ АН SSSR).
4. Semenov N.N. Chain reactions L.; Gostekhizdat 1934, 555p

ВСПОМОГАТЕЛЬНЫЕ ТЕХНОЛОГИИ ДЛЯ УЧАЩИХСЯ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ

Ибраимкулов А.Е.[1,3], Еримбетова А.С.[1,2], Кубеков Б.С.[1]
aibek_ibraimkulov@mail.ru, aigerian@mail.ru, b.kubekov@mail.ru
[1]*Институт информационных и вычислительных технологий КН МОН РК*
[2]*Казахская академия транспорта и коммуникации им. М. Тынышпаева*
[3]*Казахский национальный университет им. аль-Фараби*

Аннотация. *В данной статье рассматривается одна из самых актуальных проблем мира - проблема социальной интеграции и адаптации людей с ограниченными возможностями здоровья. Описаны современные адаптивные технологии для учащихся с разными видами ограничений. А также рассматриваются потенциал вспомогательных технологий для улучшения образования учащихся с особыми потребностями.*

Ключевые слова: *адаптивные технологии, инклюзия, социальная интеграция, информационные технологии, учащихся с ограниченными возможностями.*

В современных условиях стремительно меняющегося мира в связи с развитием информационных технологий совершенствуются и пересматриваются устоявшиеся организационные формы, позволяющие интегрировать людей с ограниченными возможностями в общество. Инклюзия - это процесс реального включения инвалидов в активную общественную жизнь, он одинаково необходим всем членам общества, во всех сферах общественных отношений которого мы наблюдаем различные формы социального неравенства.

В современном мире очень остро стоит проблема интеграции людей с ограниченными возможностями в общество и адаптации к нему. Согласно отчету Всемирной инвалидности, около 15% населения мира имеет некоторую форму инвалидности [1].

Вспомогательные технологии относятся к устройствам и службам, которые используются для расширения, поддержания или улучшения способностей учащегося с ограниченными возможностями. Одним из инструментов, помогающих учащимся с ограниченными возможностями даже в условиях нехватки учителей специального образования, являются вспомогательные технологии. Сегодня инструменты вспомогательных технологий могут помочь учащимся с определенными ограниченными возможностями учиться более эффективно.

Хотя фраза «вспомогательные технологии» может заставить нас думать о компьютерах и компьютеризированных устройствах, вспомогательные технологии также могут быть очень низкотехнологичными. Вспомогательные технологии, которые помогают учащимся с ограниченными возможностями обучения, включают компьютерные программы и приложения для планшетов, которые обеспечивают преобразование текста в речь (например, Kurzweil 3000), и наоборот преобразование речи в текст (Dragon Naturally Speaking), возможности предсказания слов (WordQ), и графические органайзеры (Inspiration).

По сравнению с другими технологиями, вспомогательные технологии могут иметь значительный эффект, помогая учащимся с ограниченными возможностями прогрессировать в достижении целей, изложенных в их индивидуальных планах обучения.

Поскольку вспомогательные технологии полезны для учащихся с широким спектром нарушений - от неспособности к обучению до серьезных физических нарушений - существует много разных типов. Вспомогательные технологии используются, чтобы помочь учащимся делать такие задачи как:

Способность слушать: некоторые учащиеся имеют нарушения слуха или не могут обрабатывать информацию. Некоторые типы вспомогательных технологий, используемых для учащихся с нарушениями слуха, включают субтитры, слуховые аппараты и персональные FM-устройства, в которых учитель носит передатчик, а ученик - приемник.

Коммуникация: для невербальных учеников или учащихся, которым трудно говорить, есть способы помочь им в общении со своими учителями и сверстниками. Коммуникационные платы, программное обеспечение для улучшения коммуникации и голосовой текстовый редактор - все это различные инструменты, которые можно использовать.

Наглядные пособия: у некоторых учащихся может быть нарушение зрения, и им может потребоваться использовать книги с крупным шрифтом,

высококонтрастные материалы, программы чтения с экрана и устройства увеличения экрана.

Работа за компьютером: для студентов с ограниченными возможностями компьютер также является отличным инструментом. Различное программное обеспечение дает учащимся возможность писать, писать по буквам и читать.

Выполнение задач - переключатели возможностей - это типы вспомогательных технологий, которые позволяют учащимся с физическими недостатками выполнять определенные задачи. Такая задача может включать в себя возможность пользоваться ножницами с батарейным питанием одним нажатием кнопки. Эти специальные переключатели или кнопки также могут использоваться для управления компьютером, игры с адаптированными игрушками или активации адаптированного устройства.

Вспомогательные инструменты преобразования текста в речь

В качестве вспомогательной технологии программное обеспечение преобразования текста в речь предназначено для помощи детям, которым трудно читать стандартные печатные издания. Общие нарушения восприятия печати могут включать слепоту, дислексию или любой тип нарушения зрения, неспособность к обучению или другое физическое состояние, которое препятствует способности читать. Тем не менее, другие учащиеся могут извлечь пользу из технологии, например, дети с аутизмом, синдромом дефицита внимания и гиперактивности (СДВГ) или с умственной отсталостью [2].

Технология работает путем сканирования и последующего чтения слов учащемуся синтезированным голосом с использованием большого количества речевых звуков, составляющих слова в любом заданном контексте.

Kurzweil 3000

Kurzweil 3000 - лидер в области программного обеспечения текста в речь для людей, которые борются с грамотностью. В дополнение к ряду функций текста в речь, полнофункциональная программа объединяет способности, которые могут помочь учащимся в других областях, потенциально привлекательные для тех, кто может иметь инвалидность, не связанную с печатью, или тех, кто обычно не рассматривает программу текста в речь. Некоторые функций:

• Говорящая проверка орфографии
• Графический словарь с картинками на более чем 40 000 слов
• Увеличение текста
• Инструменты для сдачи тестов, написания эссе, заметок, справочников и т.д.

Графические организаторы могут быть эффективными, помогая студентам систематизировать свои мысли в процессе письма. В качестве вспомогательной технологии графические органайзеры могут быть хорошим выбором для студентов с дисграфией или нарушениями письменной речи, особенно концептуальных аспектов письма.

Draft: Builder

Draft: Builder - это инструмент для письма, который объединяет функции создания набросков, заметок и черновиков, чтобы разбить процесс написания на три этапа. Используя графический органайзер, программа помогает студенту визуализировать проект и вставить информацию в нужное место без необходимости концептуализировать весь процесс. Затем он автоматизирует процесс создания статьи, где студент может перетащить то, что написано в каждой заметке, в черновик.

Другие функции включают говорящую проверку орфографии, которая использует технологию текста в речь, инструмент библиографии, словарь и возможность для учителей добавлять заблокированный текст в программу для дальнейшего руководства.

Системы Sip-and-Puff

Системы Sip-and-Puff используются учащимися, имеющими проблемы с мобильностью, такие как паралич и нарушение мелкой моторики. Эти системы позволяют ребенку управлять компьютером, мобильным устройством или каким-либо другим технологическим приложением, перемещая устройство ртом. Подобно джойстику, ребенок может перемещать контроллер в любом направлении и нажимать на различные инструменты навигации с помощью глотка или затяжки. Экранная клавиатура позволяет ребенку печатать одними и теми же движениями.

Системы Sip-and-Puff - это тип устройства переключения, которое относится к технологии, используемой для замены компьютерной клавиатуры или мыши. Другие устройства переключения включают кнопки или другие объекты, к которым ученик может прикоснуться, толкнуть, потянуть, пнуть или выполнить какое-либо другое простое действие, которое затем может управлять устройством.

Jouse3

Jouse3 - это система, позволяющая детям управлять устройством с помощью любой части рта, щеки, подбородка или языка. Благодаря точности и быстроте реакции домашние пользователи могут использовать его для рисования или компьютерных игр.

Программное обеспечение для корректуры

Программное обеспечение для корректуры - это отрасль вспомогательных технологий, которая выходит за рамки типичных функций корректуры, имеющихся в системе обработки текстов, таких как исправление слов, которые часто ошибочно пишут студенты с дислексией. Ряд других функций, предлагаемых в этой категории, может помочь студентам поработать над своим набором навыков языка, чтобы стать более эффективным и точным писателем.

Программное обеспечение для корректуры в первую очередь ориентировано на людей с дислексией, оно может быть полезно людям с любым типом нарушения обучения, затрудняющим письмо и чтение [3].

Программа экранного доступа - JAWS

Программа чтения с экрана JAWS - это программа, которая позволяет слепому или слабовидящему пользователю читать текст, отображаемый на экране компьютера с помощью синтезатора речи или дисплея Брайля. JAWS, Job Access With Speech, - это самая популярная в мире программа чтения с экрана, разработанная для пользователей компьютеров, у которых потеря зрения не позволяет им видеть содержимое экрана или перемещаться с помощью мыши. JAWS обеспечивает вывод речи и шрифта Брайля для наиболее популярных компьютерных приложений на ПК.

ZoomText Magnifier / Reader - это полностью интегрированная программа увеличения и чтения, предназначенная для пользователей с ослабленным зрением. Экранная лупа / Reader увеличивает и улучшает все на экране вашего компьютера, повторяет ваш набор текста и основные действия программы и автоматически читает документы, веб-страницы, электронную почту.

Устройство BrailleNote

Новозеландская компания Humanware представила интересное устройство для слепых и слабовидящих людей. Устройство BrailleNote - это карманный компьютер для людей, лишенных зрения. Он использует систему чтения и письма для слепых и дает возможность пользователям набирать тексты, работать в Интернете, слушать музыку, читать книги, а также подключаться к ПК и синхронизировать данные.

Ginger

Ginger предлагает несколько функций, которые могут помочь студентам с дислексией и другими нарушениями обучения письму. Он также предназначен для говорящих на других языках, кроме английского. Некоторые из функций включают:

• средство проверки грамматики, которое анализирует контекст, чтобы определить любые ошибки или орфографические ошибки. Например, Ginger может определить, следует ли использовать в предложении «там», «их» или «они», что является распространенной ошибкой в письменной форме.

• инструменты предсказания слов и перефразирования предложений, которые могут быть полезны учащимся, которые учатся правильно строить предложения.

• функциональность текст в речь, чтобы учащиеся могли слышать, что они написали.

• персональный тренер, который проводит практические занятия на основе прошлых ошибок, допущенных учеником.

Math Tools

Различные технологии и инструменты могут помочь учащимся, у которых проблемы с математикой, чаще всего возникающие при нарушении обучаемости, называемом дискалькулия. Дискалькулия затрудняет понимание чисел и характеризуется общим отсутствием понимания в области математики.

Вспомогательные технологии в математике предназначены не только для людей с дискалькулией. Он также может помочь учащимся со слепотой, нарушениями мелкой моторики или другим типом инвалидности, затрудняющим выполнение работы, связанной с математикой.

MathTalk

MathTalk - это математическая программа для распознавания речи, которая может помочь учащимся с различными формами инвалидности. На уровне математики учащиеся могут решать математические задачи, говоря в микрофон своего компьютера. Программа работает с программами Dragon NaturallySpeaking для преобразования голоса в текст, что делает ее идеальной для учащихся с нарушениями мелкой моторики. Студенты с нарушениями зрения или слепоты могут использовать встроенный переводчик Брайля.

Разнообразные вспомогательные слуховые системы или вспомогательные слуховые технологии могут помочь глухим или слабослышащим ученикам, а также тем, у кого есть другие проблемы со слухом и обучением. По данным Национальной ассоциации глухих, вспомогательные слуховые системы могут использоваться для увеличения охвата и повышения эффективности слуховых аппаратов и кохлеарных имплантатов или детьми, которым эти инструменты не нужны, но все же нуждаются в помощи со слухом. Вспомогательные системы прослушивания используют микрофон, технологию передачи и устройство для улавливания и передачи звука в ухо. Конкретная технология передачи, используемая в системе, обычно отличает один тип вспомогательной системы прослушивания от другого.

Многочисленные приложения были разработаны для смартфонов, которые позволяют глухим и слабослышащим, получить максимальную отдачу от своих

устройства. Эти приложения работают, предоставляя субтитры к фильмам, содействуют в разговоре между теми, кто может услышать и теми, кто не может.

Приложения Video Relay Service, или VRS, позволяют глухому человеку общаться по телефону без необходимости набора текста. Вместо этого, вызовы могут быть сделаны или приняты с использованием видео возможностей смартфона и языка жестов. Если необходимо, некоторые программы могут подключить пользователя к переводчику, который знает язык жестов и может взаимодействовать с ними. Sprint VRS, Purple VRS и IWRelay VRS это три бесплатных приложения, которые могут быть использованы для этой службы. Каждое из этих приложений обеспечивает возможность использования переводчика и использует контакты прямо с телефона или ссылки на них из интернета.

Благодаря быстрому развитию вспомогательных технологий, ученики, родители и учителя имеют в своем распоряжении, казалось бы, безграничное количество инструментов.

По мере того как эти инструменты начинают появляться дома и в классе, родители и учителя могут использовать их для академического и личностного роста учащихся. Но одной технологии недостаточно - для успешного использования этих инструментов критически важно разработать план их использования и проводить регулярные проверки, чтобы убедиться, что учащийся получает максимальную выгоду и не слишком полагается на эти инструменты.

Литература

1. Всемирный доклад об инвалидности. Всемирная Организация Здравоохранения, 2015 [Электронный ресурс] - URL: http://www.who.int/disabilities/world_report/2011/summary_ru.pdf, 16 января 2017

2. Как технологии помогают людям с ограниченными возможностями [Электронный ресурс] - URL: http://neinvalid.ru/kak-tehnologii-pomogayut-lyudyam-s-ogranichennyimivozmozhnostyami/, 16 января 2017

3. Технологии помогают людям с ограниченными возможностями [Электронный ресурс] - URL: http://nnd.name/2014/11/tehnologii-pomogayut-lyudyam-s-ogranichennyimivozmozhnostyami/, 16 января 2017

СПУТНИКОВЫЙ МОНИТОРИНГ ГИДРОТЕХНИЧЕСКИХ ОБЪЕКТОВ КИТАЙСКОЙ ЧАСТИ БАССЕЙНА РЕКИ ИЛИ В СЕЗОНЕ 2020 ГОДА

Терехов А.Г.
e-mail: aterekhov1@yandex.ru
Институт информационных и вычислительных технологий КН МОН РК, Казахстан

Аннотация. *Рассмотрены результаты спутникового мониторинга бассейна трансграничной реки Или (КНР-Казахстан). Недостаток гидрологической информации с территории КНР, может восполняться с помощью спутникового мониторинга. Сезон 2020 года характеризовался существенными отрицательными аномалиями водного эквивалента снежного покрова в зонах формирования стока реки (хребты Тянь-Шаня). Календарные даты начала сезонного пополнения доминирующих водохранилищ в китайском секторе бассейна были смещены на более поздние сроки, что указывает на дефицит воды в основных притоках реки Или. Спутниковые оценки расхода воды в реке Иле на границе КНР-Казахстан показали острую маловодность июня-августа.*

Трансграничный бассейн реки Или, с площадью около 140 тыс. км^2, верховья которого относятся к КНР (Синьцзян-Уйгурский автономный район), а нижняя часть к Казахстану расположен в аридной зоне Центральной Азии. Река собирает воду в хребтах Северного, Восточного и Внутреннего Тянь-Шаня. Водные ресурсы этой реки, по большей части, формируют одно из крупнейших озер мира – озеро Балхаш (18 тыс. кв. км). Ресурсы реки активно используются в народном хозяйстве, особенно на территории КНР, где проживает большая часть населения ее бассейна [1]. Резко континентальный климат Центральной Азии продуцирует значительные вариации в водности сезона [2,3]. Годовой объем стока реки Иле на границе с Казахстаном может варьироваться, в пределах от 9 (1992) до 14 (1958) км^3.

В условиях значительной антропогенной нагрузки в верхней, китайской, части бассейна информация о режиме водности года, определяемый погодными условиями, очень важна для эффективного водопользования в нижнем, Казахстанском секторе [4-6]. Оперативная гидрологическая информация с китайского сектора бассейна для казахстанских экспертов ограничивается данными пограничного гидропоста (Сандаохэцзы), чего недостаточно для прогноза водности сезона [7]. Это обстоятельство определяет актуальность, для казахстанских профильных организаций, спутниковых оценок водности сезона в верхней части бассейна реки Или [8].

Региональная система мониторинга, разработанная для территории СУАР КНР [9], предназначена для анализа состояния ряда водных объектов, расположенных в трансграничных бассейнах. В бассейне р.Или наиболее значимыми являются доминирующие водохранилища, расположенные на ее основных притоках: на реке Текес – Капшагайское вдхр.; и на реке Каш – Жарынтайское вдхр. Также представляет интерес снежный покров бассейна реки, который формируется в

холодный период и является важнейшим источником воды речного стока в теплое время [10-12].

В данной работе рассматривается текущее состояние и перспективы водности сезона реки Или на территории КНР. Главная цель спутникового мониторинга, как можно раньше зарегистрировать признаки маловодности. Маловодность сопряжена с наибольшими экономическими потерями в нижней части бассейна на территории Казахстана. Информация о водности сезона необходима для эффективного администрирование работой Капчагайского гидроузла (Казахстан), расположенного в районе крупнейшего мегаполиса Республики - города Алматы. Водохранилище работает в энергетическом режиме, вырабатывая электроэнергию для мегаполиса Алматы. Также водохранилище должно поддерживать высокий уровень воды в нижней части русла реки Или в определенное время, чтобы обеспечить ирригацию рисовых массивов в районе пос. Баканас.

Первая половина сезона 2020 года оказалась маловодной. В связи с этим представляло интерес проанализировать каким образом система регионального спутникового мониторинга СУАР может характеризовать гидрологические параметры бассейна р.Или. Какие прогнозы по водности реки Или могут быть сделаны для второй половине сезона и насколько они оправдаются.

Первый параметр, характеризующий потенциальную водность сезона – снежный покров бассейна р.Иле. Продукт Snow Water Equivalent Anomaly от программы Famine Early Warning System NET (SWEA FEWS NET), доступен на свободной основе на сайте программы (https://earlywarning.usgs.gov/fews/). По данным на 30 апреля в хребтах Тянь-Шаня, которые служат источником стока р. Иле регистрировались запасы снега существенно ниже нормы, рис.1.

Вторым параметром, связанным с водностью сезона, является календарные даты заполнения крупнейших водохранилищ в китайском секторе бассейна р.Или. Маловодный режим сдвигает на более поздние сроки календарные сроки заполнения основных водохранилищ, в частности Капшагайского на реке Текес и Жарынтайского на реке Каш. Сельскохозяйственное водопользование начала лета требует большого количества воды и в условиях маловодья ресурсов на сезонное пополнение резервуаров не остается. В конце лета (август) потребность воды в сельском хозяйстве значимо уменьшается и появляется возможность заполнения водохранилищ крупных гидроузлов. Однако такой режим продуцирует острое антропогенное маловодье р.Иле в нижней части бассейна, относящейся к Казахстану. Многолетний спутниковый мониторинг запасов воды в этих резервуарах, базирующийся на оценках размеров водных зеркал, показал, что в первой половине сезона 2020 года заполнение водохранилищ шло очень медленно, с графиком близким к 2014 году, когда наблюдалось исключительное маловодье, рис.2,3.

Третьим параметром, являются спутниковые оценки расхода воды в реке Или в районе границы КНР-Казахстан. Гидрологическая информация не попадает в программу международного обмена Всемирной метеорологической организации и поэтому данные о расходе воды в реках не имеют свободного распространения. Спутниковые снимки с разрешением 20-30 м (Landsat 7,8 и Sentinel-2A) свободного доступа достаточно часто покрывают территорию в районе границы КНР-Казахстан, раз в неделю и чаще. Для крупных рек, протекающих по слабонаклоненным равнинам в аридном климате с неразвитой древесной растительностью,

спутниковые снимки с разрешением 20-30 м позволяют оценивать расход воды. Сезон 2020 года по расходу воды в р.Иле начинался как обычный, но начиная со второй половины мая расход воды начал резко падать. В период июня – начала июля регистрировалось исключительное маловодье. Расход воды в реке оценивался, как более чем в 4 раза меньше климатической нормы, рис.2.

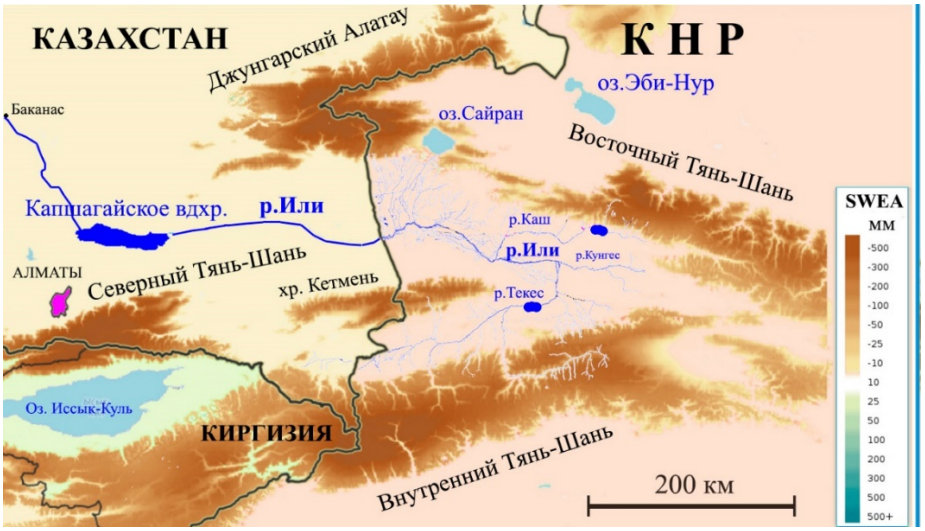


Рис. 1. Аномалии водного эквивалента снежного покрова (Snow Water Equivalent Anomaly [SWEA]) в районе трансграничного бассейна р.Иле. Построено по данным SWEA FEWS NET на 30 апреля 2020 года.

Рис. 2. Примеры различного расхода воды в р.Иле в различные по водности годы в районе границы Казахстан – КНР. Снимки спутника Sentinel-2A.

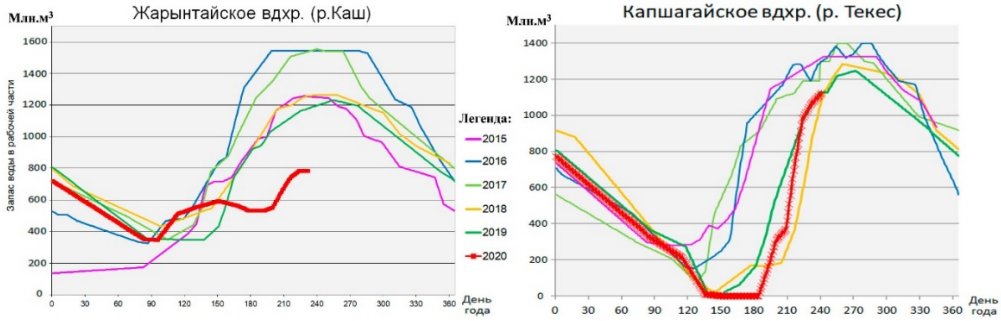


Рис. 3. Динамика запасов воды в рабочих частях основных водохранилищ (Капшагайское, Жарынтайское) в китайской части бассейна р.Иле в период 2015-2020 гг. Спутниковые оценки.

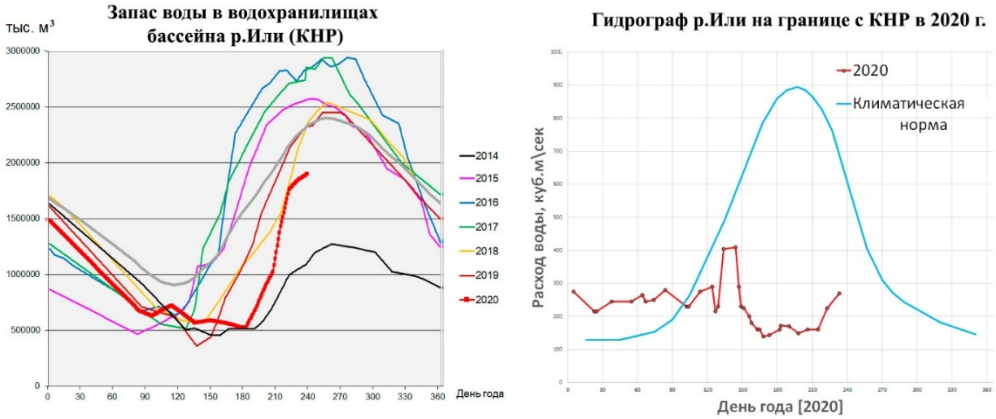


Рис. 4. Динамика суммарных запасов воды в рабочих частях основных водохранилищ (Капшагайское+Жарынтайское) в китайской части бассейна р.Иле в период 2014-2020 гг. А также спутниковые оценки расходов воды в р.Иле на границе с КНР.

Таким образом, система регионального спутникового мониторинга СУАР КНР регистрирует по всем основным параметрам маловодность сезона для реки Или в 2020 году.

Работа выполнена при поддержке грантового финансирования Министерства образования и науки Республики Казахстан, проект AP05134241.

Литература

1. Терехов А.Г., Абаев Н.Н., Лагутин Е.И. Диагностика водообеспеченности сельскохозяйственных культур СУАР КНР в течение 2003-2019 гг. по данным eMODIS NDVI C6// Ж. Современные проблемы дистанционного зондирования Земли из космоса. 2020.- Т.17.- № 1.- С. 128-138. DOI: 10.21046/2070-7401-2020-17-1-128-138.

2. Терехов А.Г., Витковская И.С., Абаев Н.Н., Долгих С.А. Многолетние тренды в состоянии растительности хребтов Тянь-Шаня и Джунгарского Алатау по данным eMODIS NDVI C6 (2002-2019 гг.) // Ж. Современные проблемы дистанционного зондирования Земли из космоса. 2019.- Т.16.- № 6.- С. 133-142. doi: 10.21046/2070-7401-2019-16-6-133-142.

3. Терехов А.Г., Абаев Н.Н., Витковская И.С., Пак А.А., Егембердиева З.М. О связи между состоянием горной растительности Тянь-Шаня и индексами Северо-Атлантической Осцилляции в весенне-летний период следующего года// Ж. Современные проблемы дистанционного зондирования Земли из космоса. 2020.- Т.17.- № 2.- С.275-281. DOI: 10.21046/2070-7401-2020-17-2-275-281.

4. Терехов А.Г. Потенциал спутниковых данных в задаче оценки водности сезона в китайской части бассейна реки Иле// Гидрометеорология и экология. 2019.- № 4 (95).- с.184-189.

5. Terekhov A.G., Vitkovskaya I.S., Abayev N.N. The effect of changing

stratification in the atmosphere in central zone of Eurasia according to vegetation data of Tien Shan mountains during 2002-2019 //E3S Web of Conference. 2020.- Vol. 149.- No 03004. DOI: 10.1051/e3sconf/202014903004.

6. Терехов А.Г., Абаев Н.Н., Витковская И.С., Пак А.А., Егембердиева З.М. О связи между состоянием горной растительности Тянь-Шаня и индексами Северо-Атлантической Осцилляции в весенне-летний период следующего года// Ж. Современные проблемы дистанционного зондирования Земли из космоса. 2020.- Т.17.- № 2.- С. 275-281. DOI: 10.21046/2070-7401-2020-17-2-275-281.

7. Соглашение между Правительством Республики Казахстан и Правительством Китайской Народной Республики о сотрудничестве в сфере использования и охраны трансграничных рек// Постановление Правительства Республики Казахстан от 10 сентября 2002 г. N 989. - http://adilet.zan.kz/rus/docs/P020000989.

8. Терехов А.Г., Пак А.А. Спутниковый прогноз влияния пополнения Капшагайского водохранилища (КНР) на водность трансграничной реки Иле в 2019 году// Ж. Современные проблемы дистанционного зондирования Земли из космоса. 2019.- Т.16.- № 4.- С. 298-302. DOI: 10.21046/2070-7401-2019-16-4-298-302.

9. Terekhov A.G., Abayev N.N., Bolatov K., Egemberdieva Z. Opportunities of short-term weather forecasts data in the environmental monitoring of the Kazakhstan //E3S Web of Conference. 2020.- Vol. 149.- No 03003. DOI: 10.1051/e3sconf/202014903003.

10. Терехов А.Г., Ивкина Н.И., Юничева Н.Р., Витковская И.С., Елтай А.Г. Изменения снежного покрова сухих степей и полупустынь Казахстана на примере бассейна р. Эмба по спутниковым данным периода 2001-2019 гг. // Ж. Современные проблемы дистанционного зондирования Земли из космоса. 2020.- Т.17.- № 2.- С. 101-113. DOI: 10.21046/2070-7401-2020-17-2-101-113.

11. Терехов А.Г., Ивкина Н.И., Абаев Н.Н., Елтай А.Г., Егембердиева З.М. Валидация суточного продукта Snow Depth FEWS NET для бассейна реки Урал по данным метеорологических наблюдений// Ж. Современные проблемы дистанционного зондирования Земли из космоса. 2020.- Т.17.- № 3.- С.31-40. DOI: 10.21046/2070-7401-2020-17-3-31-40.

12. Терехов А.Г., Ивкина Н.И., Абаев Н.Н., Галаева А.В., Елтай А.Г. Реакция годового стока р. Урал на высоту снежного покрова в его бассейне в период 2001-2019 гг.// Ж. Современные проблемы дистанционного зондирования Земли из космоса. 2020.- Т.17.-№ 4.- С.207-217. DOI: 10.21046/2070-7401-2020-17-4-207-217.

ЭКСПЕРИМЕНТАЛЬНО-МОДЕЛЬНЫЕ ИССЛЕДОВАНИЯ ПЕРИОДИЧЕСКИХ СТРУКТУР ДЛЯ СИСТЕМЫ ИНТЕРРОГАЦИИ

[1,2]Вуйцик В.,[1,2]Кисала П., [1,3]Калижанова А.У., [3, 4]Козбакова А.Х.,
[1,5]Айткулов Ж.С., [1,6]Оразбеков Ж., [1]Искакова М., [1]Арсланова С.
[1]Институт информационных и вычислительных технологий КН МОН РК, Алматы, Казахстан
[2]Люблинский технический университет, Люблин, Польша
[3]Алматинский университет энергетики и связи, Алматы, Казахстан
[4]Алматинский технологический университет, Алматы, Казахстан

[5]Казахский национальный университет имени аль-Фараби, Казахстан
[6]Казахский национальный педагогический университет имени Абая
Алматы, Казахстан
e-mail: kalizhanova_aliya@mail.ru

Аннотация. *В статье рассматриваются типы периодических структур на основе наклонных волоконных решетках Брэгга (НВРБ). Приведены результаты экспериментально-модельных исследований и их возможных применений для системы интеррогации.*

Ключевые слова: *Ex-TFG, система опроса, датчик, сигнал, наклонная волоконная решетка Брэгга.*

Введение. Чрезмерно наклонные периодические структуры (Ex-TFG). Структуры наклонных волоконных решеток Брэгга (НВРБ) характеризуются сильной зависимостью коэффициента связи мод ядра и оболочечных мод от поляризации света. Степень сцепления также существенно зависит от угла наклона таких структур и их периода. Существуют три основные группы наклонных структур, которые отличаются механизмами связи света с оболочечными модами. Первая группа содержит структуры с углами наклона, достигающими значения до нескольких градусов. Вторая группа включает в себя структуры с углом наклона 45º. В третью группу входят решетки с очень большим углом наклона, называемые чрезмерно наклонными решетками и обозначаемыми как Ex-TFG (excessively tilted fiber grating-чрезмерно наклонная волоконная решетка).

Известно, что стандартные структуры НВРБ имеют ряд резонансов, полученных из обратно распространяющихся оболочечных мод. Они видны как гребень минимумов на спектральных характеристиках передачи НВРБ. Это свойство используется в датчиках для измерения влажности [1], уровня жидкости [2,3], вибрации [4,5], акселерометров [6], датчиков электромагнитного поля с использованием плазмонного эффекта [7], датчиков коррозии [8] и даже для измерения молекул с низким молекулярным весом [9] и многих других.

Датчики НВРБ с углом наклона 45º характеризуются высоким коэффициентом ослабления поляризованного света. В результате их можно использовать в качестве линейных поляризаторов [10,11], полностью волоконно-оптических. Этот тип решетки НВРБ также характеризуется высоким потенциалом применения в конструкции волоконных лазеров [12].

Первая работа с датчиками с наклонными брэгговскими решетками с чрезвычайно большими углами наклона касалась возможности их использования для измерения показателя преломления с пониженной перекрестной чувствительностью к температуре [13] и в системах измерения угла кручения [14]. Известно, что оболочечные моды, с которыми связана мода входного ядра, разделены на две моды в зависимости от полярностей LP_{mn}^{P} и LP_{mn}^{S}.

Из-за большой симметрии стандартного одномодового волокна его двулучепреломление незначительно. Несимметричное воздействие на такое волокно ультрафиолетового (УФ) света, например, при записи периодических структур, может привести к двойному лучепреломлению. Тем не менее, это небольшая асимметрия, и двулучепреломление такой структуры можно

игнорировать. В случае структур НВРБ, хранящихся в волоконно-оптическом сердечнике, они вызывают сильное нарушение круговой симметрии, что вызывает значительное двулучепреломление в сердцевине волокна. Из вышеизложенного, структуры НВРБ могут связывать мода ввода с ортогональными оболочечными модами LP_{mn}^{P} и LP_{mn}^{S}.

$$\lambda = \left[n_{\text{ядро}}(\lambda) - n^{P}{}_{m,\text{оболочка}}(\lambda)\right](\Lambda_{Ex-TFG}/cos\theta), \quad (1)$$

$$\lambda = \left[n_{\text{ядро}}(\lambda) - n^{S}{}_{m,\text{оболочка}}(\lambda)\right](\Lambda_{Ex-TFG}/cos\theta). \quad (2)$$

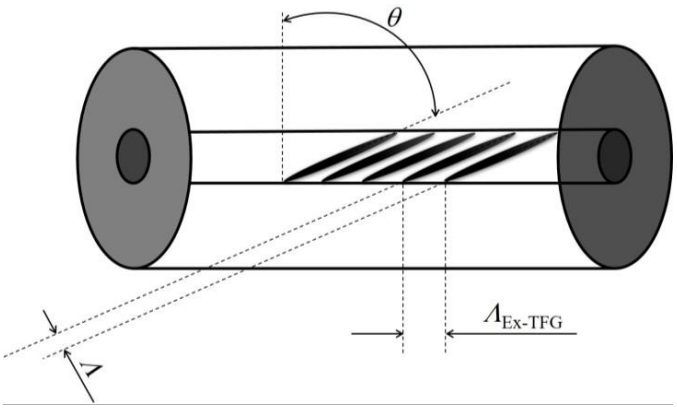


Рис.1. Схематическое представление структуры Ex-TFG с указанием характерных величин

В уравнениях (1) и (2) λ - длина волны резонанса, $n_{\text{ядро}}$- эффективный показатель преломления в сердцевине волокна со структурой Ex-TFG, записанной для данной длины волны λ, $n^{P}{}_{m,\text{оболочка}}$ и $n^{S}{}_{m,\text{оболочка}}$- эффективные показатели преломления m-порядка для моды P и S, θ - угол наклона конструкции, а Λ_{Ex-TFG} - период между наклонными плоскостями структуры $Ex-TFG$ и в соответствии с рисунком 1 Λ_{Ex-TFG}=$\Lambda\, cos\theta$, который после включения в уравнения (1) и (2), позволяет сохранить их в более простой форме:

$$\lambda = \left[n_{\text{ядро}}(\lambda) - n^{P}{}_{m,\text{оболочка}}(\lambda)\right]\Lambda, \quad (3)$$
$$\lambda = \left[n_{\text{ядро}}(\lambda) - n^{S}{}_{m,\text{оболочка}}(\lambda)\right]\Lambda, \quad (4)$$

Приведенные выше уравнения показывают, что длина волны, для которой имеет место наиболее сильная связь моды ядра и оболочек, в случае структур Ex-TFG зависит от показателя преломления ядра и оболочки, и периода решетки Λ. Модальный спектральный отклик LP^{P} и LP^{S} Ex-TFG структуры можно определить с помощью следующего уравнения [15]:

$$\Delta\lambda = \lambda^{LP^{P}} - \lambda^{LP^{S}} = \frac{\Delta n_{\text{оболочка}}{}^{S-P}\Lambda}{\Lambda\left(\frac{dn_{\text{оболочка}}{}^{P}}{d\lambda} - \frac{dn_{\text{ядро}}}{dz}\right)+1}, \quad (5)$$

что, можно написать как:

$$\Delta\lambda = \gamma^P \Delta n_{\text{оболочка}}{}^{S-P} \Lambda, \tag{6}$$

где γ^P - коэффициент, соответствующий данной моде LP^P [15], $\Delta n_{\text{оболочка}}{}^{S-P}$- разница показателей преломления между модами LP^P и LP^S. Также обратите внимание, что фактический угол наклона структуры отличается от угла фазовой маски относительно оси волокна. Это связано с цилиндрической природой волокна, которая приводит к тому, что угол наклона световых полос от УФ-лазера будет различным во внутренней и внешней частях волокна [16]. Это влияет на период изогнутой структуры, который также является функцией угла фазовой маски относительно волоконно-оптической оси $\theta_{\text{маска}}$, которые мы можем записать в виде $\Lambda_{Ex-TFG} = f\left(\theta_{\text{маска}}, n_{|\lambda_{UV}}\right)$. Фактический период, с которым структура будет сохранена, также зависит от фазы фазовой маски. Уравнение для вышеуказанных отношений принимает следующий вид:

$$\Lambda_{Ex-TFG} = \left[\frac{\Lambda_{\text{маска}}}{\cos(\theta_{\text{маска}})}\right] \cos\left[\frac{\pi}{2} - arc\ tan\left[\frac{1}{n_{|\lambda_{UV}} \tan((\theta_{\text{маска}}))}\right]\right], \tag{7}$$

$n_{|\lambda_{UV}}$ является показателем преломления оптического волокна для длины волны УФ-лазера, $\Lambda_{\text{маска}}$- это период фазовой маски. На рисунке 2 показана схема системы, в которой были изготовлены структуры НВРБ, включая также Ex-TFG.

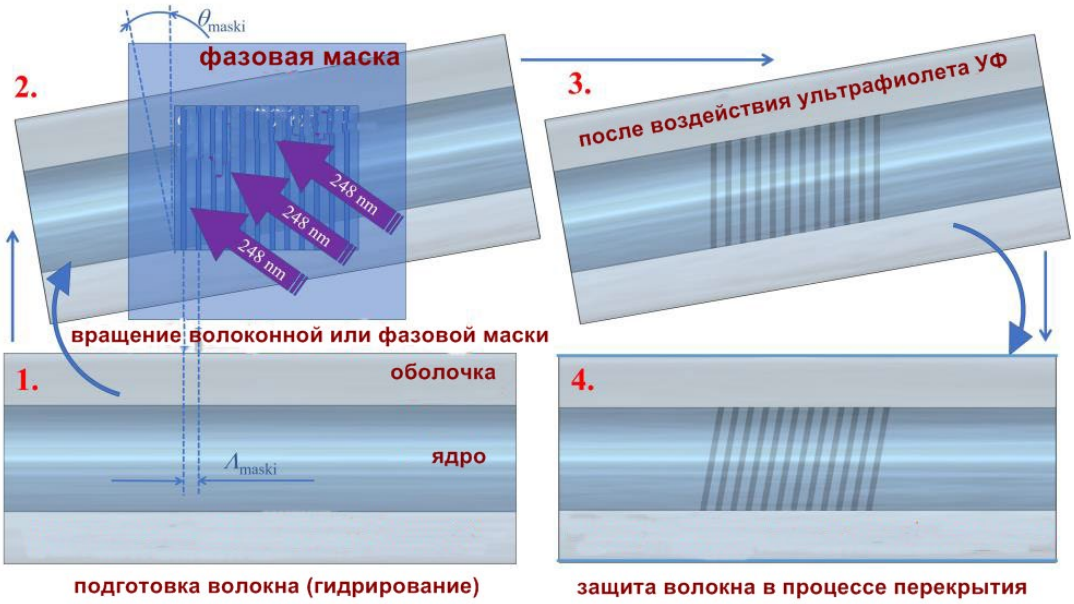


Рис.2. Система, в которой были созданы структуры Ex-TFG с углом поворота фазовой маски и периода маски

На рисунке 3 показано влияние поворота фазовой маски на период создаваемых структур. Были сопоставлены результаты измерений периода, определенные на основе спектральных измерений. Реальный период полученных структур определялся по длине волны Брэгга. Как видно, увеличение угла поворота фазовой маски относительно нормали к оси оптического волокна вызывает

относительное уменьшение периода НВРБ. Как упоминалось ранее, это связано с геометрией волокна.

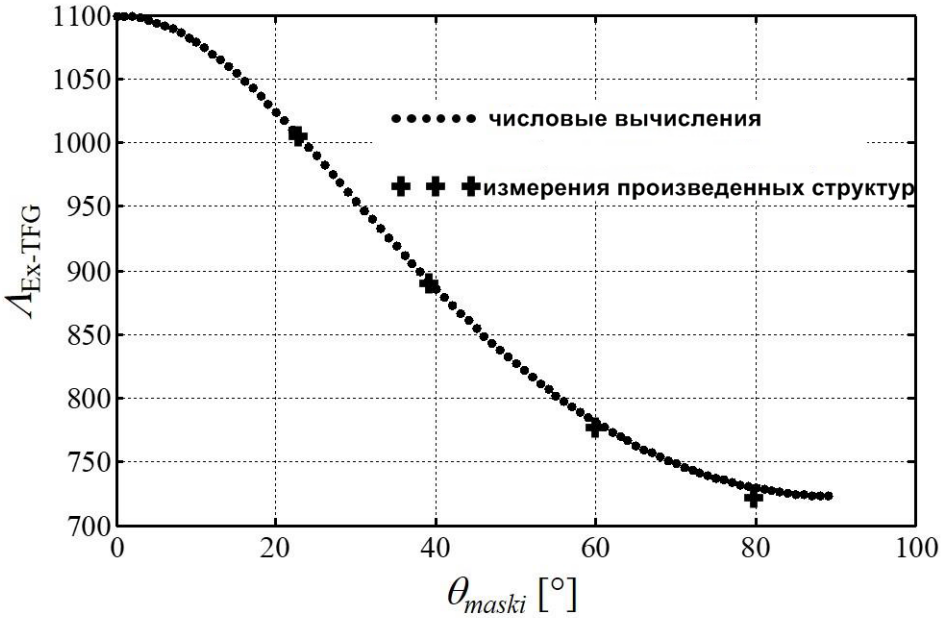


Рис.3. Влияние угла наклона фазовой маски относительно нормали к оси оптического волокна на период создаваемой структуры Ex-TFG

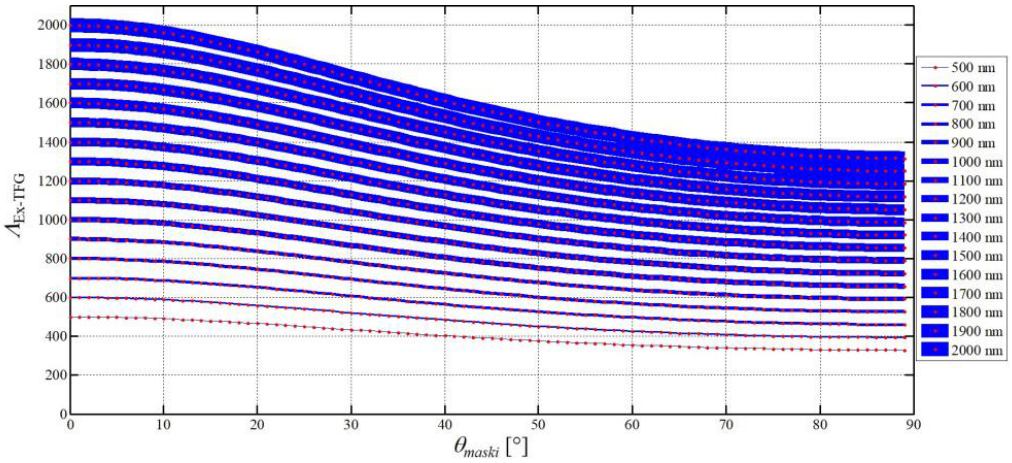


Рис.4. Кривые, показывающие зависимость периода Ex-TFG от угла наклона фазовой маски для различных значений периода маски (500-2000 nm)

При анализе результатов, показанных на рисунке 4, следует отметить, что период полученной структуры НВРБ также зависит от периода используемой фазовой маски. Это довольно очевидный вывод, вытекающий из свойств технологии записи структур НВРБ методом фазовой маски. Тем не менее, представленные результаты также указывают на другое важное свойство. Таким образом, чем больше период фазовой маски, тем больше чувствительность периода создаваемой НВРБ к углу наклона маски. Для больших значений периода маски больше диапазон изменений периода НВРБ в результате изменения угла наклона маски.

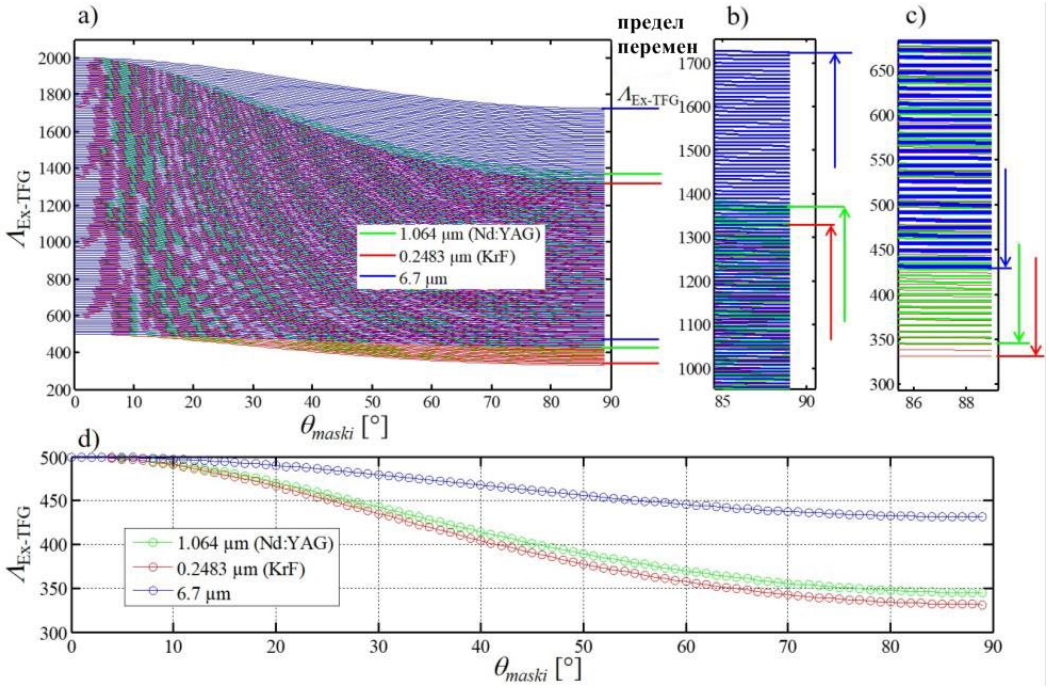


Рис.5. Теоретические значения кривых, показывающие зависимость периода НВРБ от угла наклона фазовой маски для различных значений периода маски, рассчитанных для трех длин волн лазера: 248 nm (UV, KrF), 1,064 μм (Nd: YAG), 6,7 μм (CO)

На рисунке 5 представлены совершенно гипотетические случаи, представляющие как бы изменился период создаваемой структуры НВРБ, если бы вместо эксимерного лазера с длиной волны 248 nm использовать лазерные системы, излучающие свет с другими длинами волн, например 1,064 μm и 10,6 μm. Хотя известны работы, в которых брэгговские структуры создаются с использованием неодимовых лазеров Nd: YAG, запись происходит для гармоники, близкой к УФ-излучению, например, 266 nm, с длительностью импульса 8 nm и энергией, равной 72 μJ (мкДж) [17].

Результаты, представленные на рисунке 5, иллюстрируют и показывают, как будет меняться период создаваемой структуры с изменением длины волны записывающего лазера НВРБ. Объяснение этого явления возможно, если мы повторно рассмотрим уравнение (7). Изменение длины волны падающего света вызывает изменение угла, под которым свет, падающий на фазовую маску, преломляется.

Это связано с различиями в значениях показателя преломления для разных длин волн. Для эксимерного лазера с длиной волны 248 nm показатель преломления составляет около 1,51. Для лазера с длиной волны 1,064 μm показатель преломления для кварцевого стекла составляет около 1,45, в то время как для длины волны 6,7 показатель преломления достигает 1,16. Отметим также, что для угла наклона фазовой маски, равной 0°, все характеристики начинаются и заканчиваются в одной и той же точке, то есть для одинаковых значений периода НВРБ, независимо от длины волны лазера.

Структуры Ex-TFG позволяют получить существенные различия в амплитуде пика по спектральным характеристикам, полученным из поляризованного света, в соответствии с поляризацией типа P и S. Кроме того, в случае неполяризованного света оба минимума по спектральным характеристикам Ex-TFG характеризуются одинаковым значением коэффициента пропускания (рис. 6).

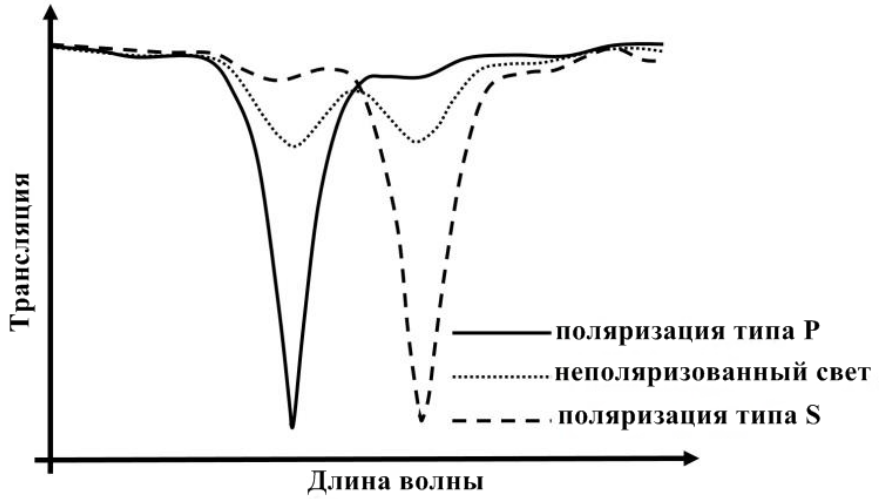


Рис.6. Показательные характеристики передачи Ex-TFG для неполяризованного света, а также для ортогонально поляризованного света

Эти уникальные поляризационные свойства структур Ex-НВРБ (Ex-TFBG) создают новые возможности их использования, например, в качестве рефрактометров [18], датчиков поворота [14], поперечной нагрузки [19] или уровня жидкости [20]. Последние работы касаются также возможности их применения в медицине, например, в качестве датчиков биомаркеров [21-22]. Метрологические свойства при измерениях поляризации света с использованием Ex-НВРБ также могут быть улучшены с использованием покрытия волокон, например, слоем графена [23]. Такие структуры могут найти потенциальные применения в волоконно-оптических модуляторах, волоконных лазерах и биохимических датчиках. Далее в работе представлены не -Ex-TFG структуры с модуляцией показателя преломления, наклоненной относительно оси оптического волокна.

Наклонные решетки Муара (НМВРБ)

Интересные свойства могут быть получены с помощью структур, являющихся суперпозицией нескольких брэгговских решеток, записанных в одном и том же месте в волоконно-оптической сердцевине. Такие структуры называются волоконные решетки Муара. Чаще всего отдельные решетки отличаются, например, периодами [24].

В отличие от всех наклонных решеток, представленных в этой работе, НМВРБ (англ.: tilted Moiré fiber Bragg gratings-наклонные брэгговские решетки из муарового волокна) являются единственными структурами, которые не были изготовлены для целей данного исследования, основное внимание было уделено представлению их структуры и основных параметров, которые отличают их от других наклонных структур. Пример структуры Муара, состоящей из решетки ВРБ и НВРБ, и способ ее изготовления показан на рисунке 7.

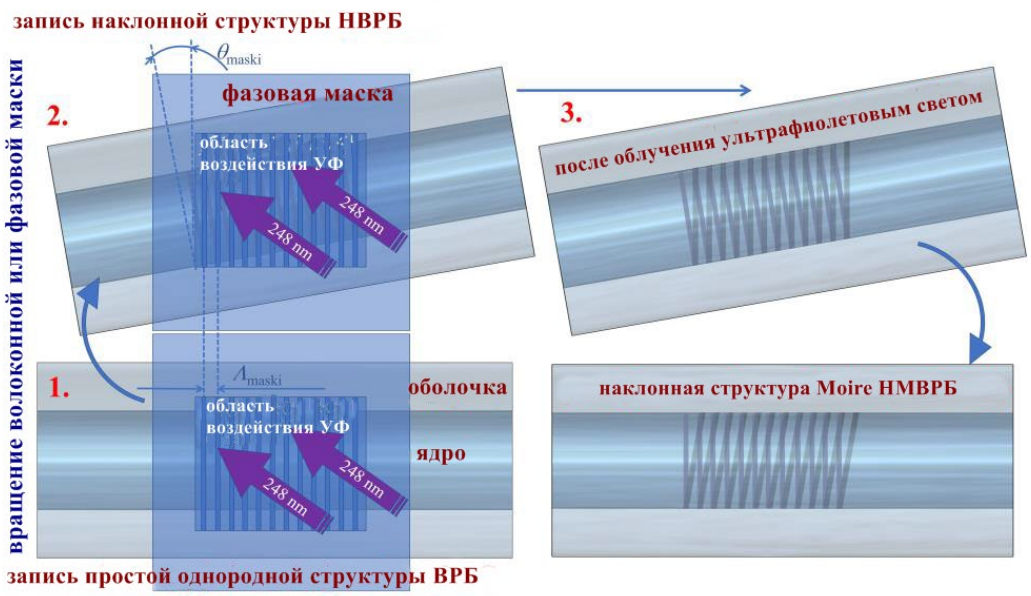
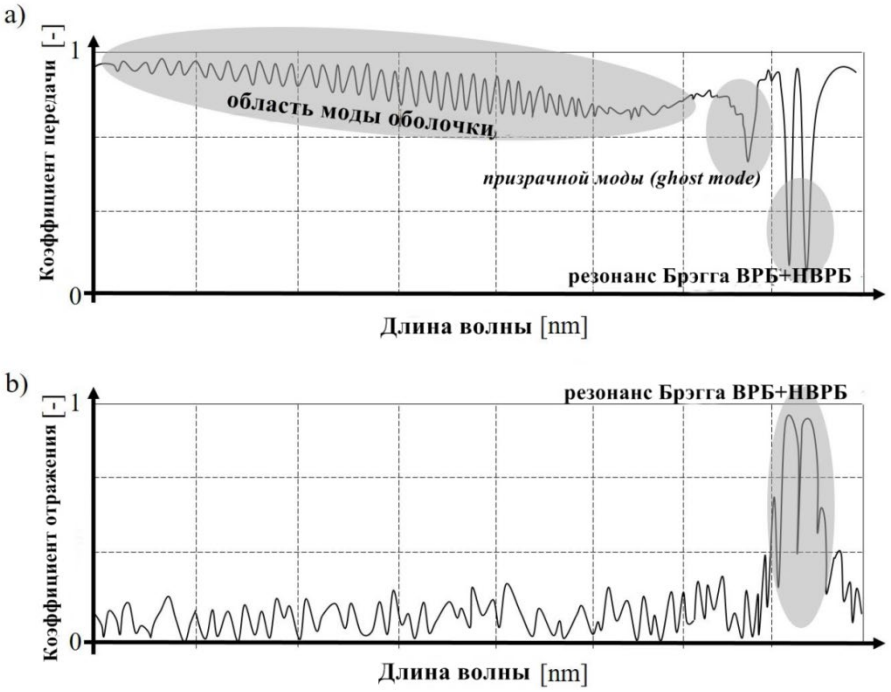


Рис. 7. Один из возможных способов записи структур НМВРБ

Спектральные характеристики структур НМВРБ содержат как минимум, полученный от простой структуры ВРБ, так и число минимумов, полученных из оболочечных мод НВРБ, распространение которых зависит от окружающей среды, такие структуры могут быть использованы для измерения двух физических величин одновременно. В этом случае датчик состоит из одной измерительной головки, содержащей структуры ВРБ и НВРБ, и может быть использованы, например, для измерения температуры и показателя преломления химических или биомедицинских растворов.

Структуры Муара также являются альтернативой явлению электромагнитно-индуцированной прозрачности EIT (англ. electromagnetically induced transparency-электромагнитно-индуцированная прозрачность) [25]. Однако решетки этого типа чаще всего используются в качестве датчиков для одновременного измерения двух физических величин [26]. На рисунке 8 показаны спектральные характеристики таких структур.



а) характеристики передачи, б) отражательная характеристика
Рис .8. Спектральные характеристики структур НМВРБ

Характерно, например, наличие двух минимумов на характеристике передачи, которым соответствуют два максимума на характеристике отражения. Они связаны с отражением Брэгга в решетке ВРБ и основным резонансом (также Брэгговским), возникающим в структуре НВРБ. Также возможно выбрать периоды структур ВРБ и НВРБ так, чтобы их длины волн Брэгга были равны. Это значительно улучшит брэгговское отражение в структуре НВРБ по сравнению с системой, в которой на волокне будет записываться только структура НВРБ.

Такое усиление отражения Брэгга, например, желательны при использовании датчика для одновременного измерения температуры и второй, другой физической величины.

Положение основного пика (Брэгга) затем рассматривается как эталонное и может использоваться для получения информации о температуре, при которой выполняется измерение. Запись НМВРБ в соответствии с процедурой, показанной на рисунке 7, приводит к возникновению двух периодических структур одинакового периода, причем один из них наклонен относительно оси волокна под определенным углом.

Это приводит к так называемому резонансному эффекту Муара [27]. Модуляция показателя преломления в такой структуре описывается следующим образом уравнением:

$$\Delta n(z) = \Delta n_0[2 + 2\sin(2\pi z/\Lambda_1)\cos(2\pi z/\Lambda_2)], \quad (8)$$

где Δn_0 является разностью составляющих констант показателя преломления, т.е. разница между значением n_0, соответствующим волокну без НМВРБ и значением n_0, соответствующим волокну с записанной структурой НМВРБ. В уравнении (8) периоды Λ_1 и Λ_2 описывают следующие уравнения:

$$\Lambda_1 = 2\frac{\Lambda_{FBG}\cdot\Lambda_{TFBG}}{\Lambda_{FBG}+\Lambda_{TFBG}} \quad (9)$$

и

$$\Lambda_1 = 2\frac{\Lambda_{FBG}\cdot\Lambda_{TFBG}}{\Lambda_{FBG}-\Lambda_{TFBG}}. \quad (10)$$

Таким образом, для структур НМВРБ существуют две компоненты модуляции показателя преломления, связанные с существованием простой и наклонной периодической структуры. Эти компоненты описываются следующими уравнениями:

$$\Delta n_{FBG}(z) = 1 + sin\left(z\frac{2\pi}{\Lambda_{FBG}}\right) \quad (11)$$

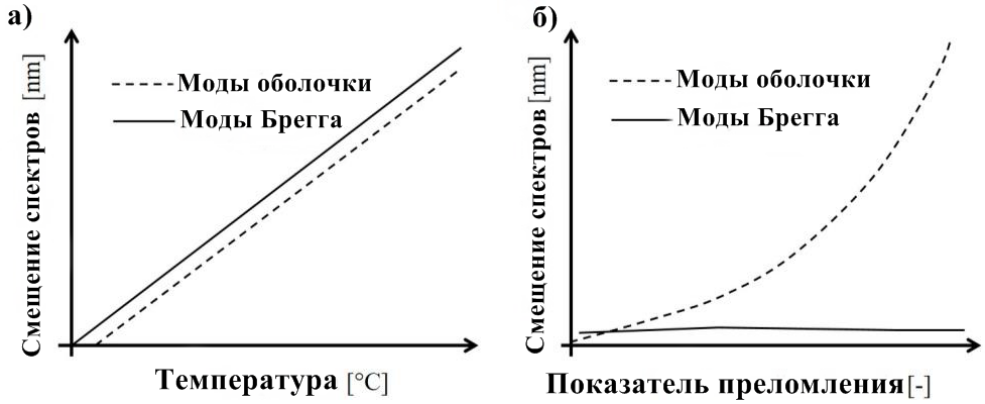
и

$$\Delta n_{TFBG}(z) = 1 + sin\left(z\frac{2\pi}{\Lambda_{TFBG}}\right) \quad (12)$$

при этом взаимосвязь между периодами структур ВРБ и НВРБ выглядит следующим образом:

$$\Lambda_{TFBG} = \frac{\Lambda_{FBG}}{cos\theta}. \quad (13)$$

Знание вышеуказанных зависимостей (8)–(13) позволяет точно контролировать записи структур НМВРБ. На рисунке 9 показана форма характеристик обработки датчика температуры и показателя преломления с использованием НМВРБ в качестве преобразователя этих двух величин.



а) температура, б) показатель преломления

Рис 9. Иллюстративные характеристики обработки НМВРБ:

Заключение

Встречающиеся различия спектрального сдвига под влиянием коэффициента преломления света, соответствующих главному резонансу Брэгга и резонансы, исходящие из оболочечных мод, позволяют проводить параллельно измерение температуры и показателя преломления. Изменения длины волны оболочечных мод и основных мод в случае изменения показателя преломления дают возможность различать эти две величины.

Представлены структуры с очень большими углами наклона плоскостей, так называемые чрезмерно наклонные волоконные решетки, также решетки, перезаписанные на одном волокне, так называемые решетки Муара, смешанные структуры, например НВРБ с переменным периодом. Предложены возможные пути развития рассмотренных периодических структур, определены их преимущества и применения.

Экспериментальные исследования проводились в лабораториях Оптоэлектроники факультета электротехники и компьютерных наук Люблинского технического университета в рамках проекта ГФ №AP05132778 «Исследование и разработка системы интеррогации сигналов с оптоволоконным рефрактометром с использованием телекоммуникационных сетей» ИИВТ КН МОН РК.

Литература

1. Miao Y., Liu B., Zhang H., Li Y., Zhou H., Sun H., Zhang W., Zhao Q., Relative Humidity Sensor Based on Tilted Fiber Bragg Grating With Polyvinyl Alcohol Coating. IEEE Photonics Technology Letters 21(7), 441-443 (2009). doi: 10.1109/LPT.2009.2013185

2. Gu B., Qi W., Zhou Y., Wu Zhifang, Shum P. P., Luan F., Reflective liquid level sensor based on modes conversion in thin-core fiber incorporating tilted fiber Bragg grating, Optics Express 22(10), 11834- 11839 (2014). doi: 10.1364/OE.22.011834

3. Jiang Q., Hu D., Yang M., Simultaneous measurement of liquid level and surrounding refractive index using tilted fiber Bragg grating, Sensors and Actuators A: Physical 170(1-2), 62-65 (2011). doi: 10.1016/j.sna.2011.06.001

4. An J. L., Liu T., Ji Y. G., Fiber optic vibration sensor based on the tilted fiber bragg grating. Advances in Materials Science and Engineering 2013, 346-349 (2013). doi: 10.1155/2013/545013

5. Huang Y., Guo T., Lu Ch., Tam H.-Y., VCSEL-Based Tilted Fiber Grating Vibration Sensing System. IEEE Photonics Technology Letters 22(16), 1235-1237 (2010). doi: 10.1109/LPT.2010.2052797

6. Guo T., Shao L., Tam H.-Y., Peter K. A., Albert Jacques, Tilted fiber grating accelerometer incorporating an abrupt biconical taper for cladding to core recoupling, Optics Express 17(23), 20651-20660 (2008). doi: 10.1364/OE.17.020651

7. Allsop T., Neal R., Rehman S., Webb D. J., Mapps D., Bennion I., Characterization of infrared surface plasmon resonances generated from a fiber-optical sensor utilizing tilted Bragg gratings. Journal of the Optical Society of America B 25(4), 481-490 (2008). doi: 10.1364/JOSAB.25.000481

8. Islam M. R., Bagherifaez M., Ali M. M., Chai H. K., Lim K., Ahmad H., Tilted Fiber Bragg Grating Sensors for Reinforcement Corrosion Measurement in Marine Concrete Structure, in IEEE Transactions on Instrumentation and Measurement 64(12), 3510-3516 (2015). doi: 10.1109/TIM.2015.2459511

9. Lépinay S., Ianoul A., Albert J., Molecular imprinted polymer-coated optical fiber sensor for the identification of low molecular weight molecules. Talanta 128, 401-407 (2014). doi: 10.1016/j.talanta.2014.04.037

10. Yan Z., Zhou K., Zhang L., In-fiber linear polarizer based on UVinscribed 45° tilted grating in polarization maintaining fiber. Optics Letters 37(18), 3819-3821 (2012). doi: 10.1364/OL.37.003819

11. Zhou K., Simpson G., Chen X., Zhang L., Bennion I., High extinction ratio in-fiber polarizers based on 45° tilted fiber Bragg gratings. Optics Letters 30(11), 1285-1287 (2005). doi: 10.1364/OL.30.001285

12. Zou Ch., Wang T., Yan Z., Huang Q., AlAraimi M., Rozhin A., Mou Ch., Wavelength-tunable passively mode-locked Erbiumdoped fiber laser based on carbon nanotube and a 45° tilted fiber grating. Optics Communications 406, 151-157 (2018). doi: 10.1016/j.optcom.2017.06.006

13. Zhou K., Zhang L., Chen X., Bennion I., Optic sensors of high refractive-index responsivity and low thermal cross sensitivity that use fiber Bragg gratings of >80° tilted structures. Optics Letters 31(9), 1193- 1195 (2006). doi: 10.1364/OL.31.001193

14. Chen X., Zhou K., Zhang L., Bennion I., In-Fiber Twist Sensor Based on a Fiber Bragg Grating With 81º Tilted Structure. IEEE Photonics Technology Letters 18(24), 2596-2598. doi: 10.1109/LPT.2006.887371

15. MacDougall T. W., Pilevar S., Haggans Ch. W., Jackson M. A., Generalized Expression for the Growth of Long Period Gratings. IEEE Photonics Technology Letters 10(10), 1449- 1451 (1998). doi: 10.1109/68.720290

16. Mihailov S. J., Walker R. B., Lu P., Ding H., Dai X., Smelser C., Chen L., UV-induced polarisation-dependent loss (PDL) in tilted fibre Bragg gratings: application of a PDL equalizer. IEE Proceedings - Oploelectronics 148(5/6), 211-216 (2002). doi 10.1049/ip-opt:20020669

17. Pereira L., Min R., Hu X., Caucheteur Ch., Bang O., Ortega B., Marques C., Antunes P., Pinto J. L., Polymer optical fiber Bragg grating inscription with a single Nd:YAG laser pulse. Optics Express 26(14), 18096-18104 (2018). doi: 10.1364/OE.26.018096

18. Yan Z., Mou Ch., Sun Z., Zhou K., Wang H., Wang Y., Zhao W., Zhang L., Hybrid tilted fiber grating based refractive index and liquid level sensing system. Optics Communications 351, 144-148 (2015). doi: 10.1016/j.optcom.2015.04.038

19. Suo R., Chen X., Zhou K., Zhang L., Bennion I., In-fibre directional transverse loading sensor based on excessively tilted fibre Bragg gratings. Measurement Science and Technology 20, 1-6 (2009). doi: 10.1088/0957-0233/20/3/034015

20. Morand A., Phan-Huy K., Desieres Y., Benech P., Analytical Study of the Microdisk's Resonant Modes Coupling With a Waveguide Based on the Perturbation Theory. Journal of Lightwave Technology 22(3), 827- 832 (2004). doi: 10.1109/JLT.2004.824528

21. Luo B., Wu S., Zhang Z., Zou W., Shi S., Zhao M., Zhong N., Liu Y., Xue Z., Wang L., Chai W., Hu Ch., Zhang L., Biomedical Optics Express 8(1), 57-67 (2017). doi: 10.1364/BOE.8.000057

22. Luo B., Wu S., Zou W., Zhang Z., Zhao M., Shi S., Liu Y., Xi X., Zeng Z., Liang W., Yan Z., Zhang L., Label-free immuneassay for porcine circovirus type 2 based on excessively tilted fiber grating modified with staphylococcal protein A. Biosensors and Bioelectronics 86, 1054-1060 (2016). doi: 10.1016/j.bios.2016.07.100

23. Jiang B., Yin G., Zhou K., Wang Ch., Gan X., Zhao J., Zhang L., Graphene-induced unique polarization tuning properties of excessively tilted fiber grating. Optics Letters 41(23), 5450-5453 (2016). doi: 10.1364/OL.41.005450

24. Min R., Marques C., Bangc O., Ortega B., Moiré phase-shifted fiber Bragg gratings in polymer optical fibers. Optical Fiber Technology 41, 78-81 (2018). doi: 10.1016/j.yofte.2018.01.003

25. Khurgin J. B., Light slowing down in Moiré fiber gratings and its implications for nonlinear optics. Physical Review A 62, 013821-1- 013821-4 (2000). doi: 10.1103/PhysRevA.62.013821

26. Wong A. C. L., Giovinazzo M., Tam H.-Y., Lu Ch., Peng G.-D., Single Tilted Moiré Fiber Bragg Grating for Simultaneous Measurement of Refractive Index and Temperature. Asia Communications and Photonics Conference and Exhibition 210-211 (2010). doi: 10.1109/ACP.2010.5682761

27. Reid D. C. J., Ragdale C. M., Bennion I., Buus J., Stewart W. J., Phaseshifted Moire grating fibre resonators. Electronics Letters 26(1), 10-12 (1990). doi: 10.1049/el:19900007

РАЗРАБОТКА ТЕХНОЛОГИИ ИНТЕЛЛЕКТУАЛЬНЫХ НАУЧНО-ОБРАЗОВАТЕЛЬНЫХ ИНТЕРНЕТ-РЕСУРСОВ

Ж.Б. Садирмекова[1], М.А. Самбетбаева[1,2]

Евразийский национальный университет им. Л.Н.Гумилева. г. Нур-Султан, Казахстан,

Институт информационных и вычислительных технологий КН МОН РК, г. Алматы, Казахстан

Аннотация. *Целью данной работы является разработка методов, технологии и инструментальных средств создания и сопровождения интеллектуальных научно-образовательных интернет-ресурсов (ИНОИР) на основе сервис-ориентированного подхода и технологий SemanticWeb. Главное назначение ИНОИР – обеспечивать содержательный доступ к научным и образовательным информационным ресурсам заданной области знаний и интегрированных с ними сервисам обработки информации.*

j
m
a
i
r
u
m
a
d
i
n
a
l
g
i
m
u
i
l
ru

Введение

Современные наука и образование испытывают в наши дни потребность в концентрации и обобщении накопленной информации по различным отраслям знаний и эффективном ее использовании, но удовлетворение этой потребности затрудняется тем, что в силу своей многоплановости и многоаспектности научные и образовательные информационные ресурсы рассредоточены на удаленных страницах множества сайтов и в распределенных электронных библиотеках и архивах. Для решения этой проблемы необходимо решить задачу сведения таких

ресурсов, относящихся к заданной области знаний, в единое информационное пространство.

Поддержка логической целостности интегрируемых ресурсов будет обеспечиваться на основе онтологии, дающей целостное и непротиворечивое представление об области знаний, к которой относятся интегрируемые ресурсы.

Сведение научно-образовательных ресурсов по заданной тематике в единое информационное пространство и поддержка их логической целостности создаст предпосылки для решения задачи обеспечения содержательного доступа к ним и механизмам их интеллектуальной обработки широкому кругу пользователей. Для обеспечения такого доступа будет разработана концепция и архитектура интеллектуальной информационной системы, управляемой онтологией.

Однако до сих пор не разработана концепция интеллектуального интернет-ресурса, ориентированного на поддержку работы с научно-образовательными ресурсами, в основе которого лежат знания (онтологии и тезаурусы), и тем более нет технологии управления знаниями, поддерживающей полный цикл создания и эксплуатации такого ресурса.

Вопросы онтологического моделирования рассматривались в работах Т. Грубера (Gruber T) [1], Н. Гуарино (Guarino N.) [2] и Гавриловой Т.А. [3], Загорулько Ю.А. [4], Калиниченко Л.А. [5], Когаловского М.Р. [6], Серебрякова В.А. [7], Тузовского В.Ф. [8], Хорошевского В.Ф. [9], Ямпольского В.З. и др. В то же время нет убедительных примеров совместного использования онтологий и научно-образовательных программных сервисов для целей, обозначенных авторами статьи.

Из аналогичных зарубежных разработок можно выделить выполнявшийся при финансовой поддержке Европейского Союза проект ЭЙЛЕР (EULER – European Libraries and Electronic Resources in Mathematical Sciences, www.emis.de/projects/EULER/About.html) задачей которого является обеспечение интегрированного доступа к библиотечным каталогам и математической информации в Интернете. Применяемый в этом проекте подход к интеграции разнородных ресурсов базируется на протоколе Z39.50 и общем методе описания ресурсов в формате DublinCore, что обеспечивает возможность их совместного использования.

Существуют также различные интернет-ресурсы, предназначенные для поддержки гуманитарных исследований. Самым известным из них является англоязычный каталог LINGUIST List (http://linguistlist.org/), созданный для обмена знаниями между лингвистами и содержащий информацию о публикациях, персоналиях, научных учреждениях, грантах, конкурсах, проектах, научных фондах, конференциях и семинарах лингвистической тематики. Из других разработок стоит также отметить созданный в Германском Исследовательском Центре Искусственного Интеллекта информационный портал «LanguageTechnologyWorld» (http://www.lt-world.org/), тематические разделы которого, кроме сведений о научных мероприятиях, проектах, организациях и персонах, содержат более подробную информацию о лингвистических технологиях, продуктах и информационных системах в области обработки естественного языка.

Следует заметить, что описанные выше проекты и ресурсы, по существу, представляют собой структурированные и аннотированные каталоги ссылок на Интернет-ресурсы, составные элементы которых практически не связаны между собой, что затрудняет поиск нужной информации и делает невозможной навигацию

по ним. Основным отличием нашего подхода является использование описания моделируемой области знаний и средств интеллектуальной обработки релевантных ей информационных ресурсов в виде системы онтологий, что позволяет систематизировано представлять знания и данные по тематике ИНОИР в виде сети знаний и данных (семантической сети) и обеспечивать пользователю удобную навигацию по ним и содержательный доступ как к аккумулированным в них знаниям и данным, так и средствам их обработки.

Другим близким подходом является разрабатываемая консорциумом W3C концепция SemanticWeb (http://www.w3.org/2001/sw/), которая предполагает наличие у любого размещенного в сети документа связанного с ним набора метаданных (семантической аннотации). Для описания метаданных используются принятые W3C стандарты – Resource Definition Framework (RDF) и Web Ontology Language (OWL), что позволяет не только описывать структурные свойства документов, но и представлять их смысл в терминах онтологий предметных областей (заданных на языке OWL). Наличие такого рода метаданных у документов облегчает их интеграцию и делает возможным их использование различными программными приложениями и сообществами. С использованием идеологии и средств этого подхода разработано и продолжает разрабатываться множество приложений, но не создана пока единая методология создания Интернет-ресурсов, ориентированных на поддержку научных исследований. Следует отметить, что наш подход естественным образом интегрирует наиболее важные компоненты технологии SemanticWeb, в частности, использование онтологии для представления семантики информационных ресурсов и поддержки их интеллектуального анализа. В то же время рассмотренный подход не предлагает целостной концепции интеллектуальных научных интернет-ресурсов и методологии их коллективного построения. Кроме того, этот подход не предоставляет методов интеллектуальной обработки интегрируемых ресурсов, а тем более содержательного доступа к ним.

Основываясь на идеях, изложенных в, под онтологией мы будем понимать точное подробное описание (модель) некоторой части мира применительно к конкретной области интересов. Формально онтология ИНОИР может быть описана семеркой вида:

$$O=\langle C, A, R_C, T, D, R_A, F\rangle$$

где C – множество классов, описывающих понятия некоторой предметной или проблемной области; A – множество атрибутов, описывающих свойства понятий и отношений; $R_C=\{r_c \mid r_c \subseteq C \times C\}$– множество отношений, заданных на классах (понятиях); T – множество стандартных типов значений атрибутов (string, integer, real, date); D – множество доменов (множеств значений стандартного типа string); $R_A = R_{AT} \subseteq R_{AD}$, где

$R_{AT} \subseteq A \times T$ – отношение, связывающее атрибуты и типы данных, из которых они могут принимать свои значения, $R_{AD} \subseteq A \times D$ – отношение, определяющее для каждого атрибута его дискретное множество значений (домен); F – множество ограничений на значения атрибутов понятий и отношений.

Для того чтобы онтология удовлетворяла целям интернет-ресурса, она должна быть хорошо структурирована и адекватно отражать его проблемную и предметную область. В качестве базовых онтологий были выбраны две онтологии. Первая из них характеризует проблемную область интернет-ресурса (рис.1). Она не зависит от предметной области интернет-ресурса и является онтологией верхнего уровня,

которая включает классы понятий, относящиеся к организации образовательной деятельности, такие как *Персона, Организация, Научная деятельность, Научная мероприятия, Публикация*, *Географическое место*, *Сборник материалов конференции* используемые для описания ее участников, организации учебной работы, мероприятий (семинаров, конференций), совместных проектов, различного типа информационных ресурсов.

В процессе эксплуатации интернет-ресурса могут появляться новые знания о его предметной области, обнаруживаться пробелы и неточности в знаниях, уже представленных в онтологии. Все это, безусловно, требует изменения онтологии. Однако при редактировании онтологии необходимо следить за тем, чтобы не нарушилась логическая целостность системы и не произошла потеря информации.

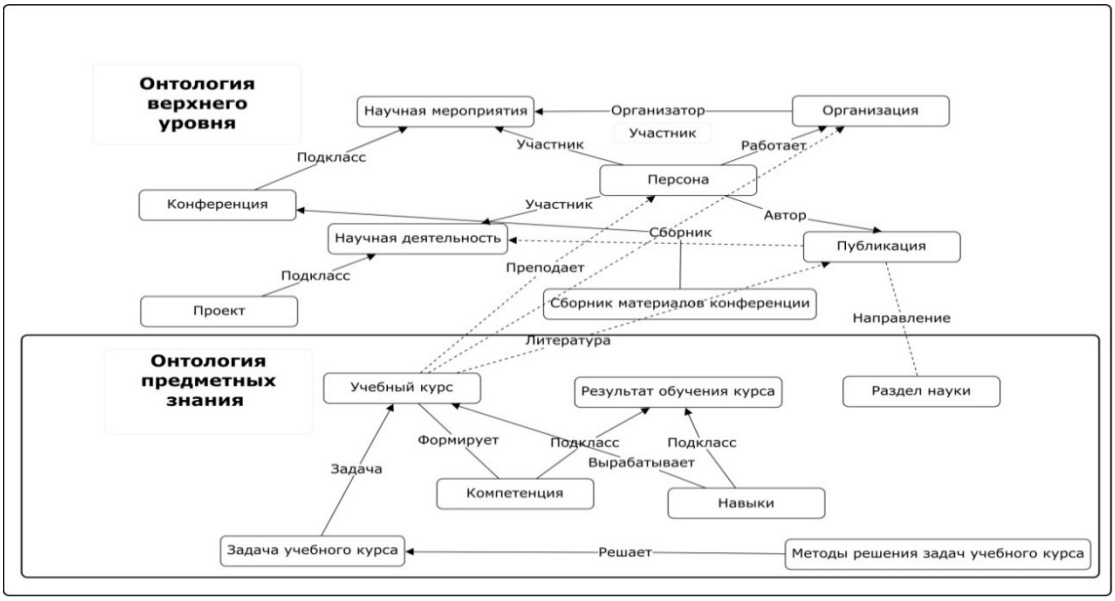


Рис. 1. Базовые онтологии ИНОИР

Редактор онтологий был построен на основе приведенного выше языка описания онтологий. Он строился с учетом возможности применения для распределенной разработки онтологий и реализован как веб-приложение, доступное зарегистрированным пользователям через Интернет. С целью обеспечения распределенной разработки онтологий в редакторе поддерживается механизм делегирования прав экспертам разных уровней.

С помощью редактора онтологий можно создавать, модифицировать и удалять любые элементы онтологии: классы понятий, отношения, домены.

При создании класса указываются его уникальное имя и набор атрибутов, служащих для задания различных свойств понятий, а фактически описывающих структуру объектов данного класса. Для класса может быть выбран родитель из ранее созданных классов, при этом от родительского класса наследуются не только все атрибуты, но и отношения, а сам родитель связывается с новым классом отношением «класс-подкласс». Для каждого атрибута класса задается имя, область допустимых значений (тип или домен), количество возможных значений (одно или множество), а также указывается обязательность заполнения.

Домен характеризуется названием и множеством элементарных значений. Для каждого значения домена можно также указать язык (на данный момент – русский, казахский или английский), на котором оно было введено.

Отношения могут связывать только уже созданные классы онтологии. Они являются направленными и бинарными и могут иметь собственные атрибуты, уточняющие связь между аргументами отношения. Для более удобного представления информации пользователю портала предоставляется возможность настройки визуализации знаний и данных. При этом для каждого класса в редакторе онтологий задается шаблон визуализации объектов этого класса и шаблон визуализации ссылок на них. По умолчанию, порядок, в котором отображаются атрибуты классов и связанные с ними отношения, в том числе и атрибуты отношений, определяется порядком их задания в онтологии. По желанию пользователя этот порядок может быть изменен.

Настройка интернет-ресурса на предметную область и управление его контентом осуществляется с помощью специализированных редакторов (редактора онтологии и редактора данных), реализованных как web-приложения и доступных зарегистрированным пользователям-экспертам через Internet. Язык описания онтологий и редактор онтологий выбирались и проектировались таким образом, чтобы они были понятны экспертам и ими было просто и удобно пользоваться. В частности, из-за этих требований мы отказались от использования таких популярных средств, как язык представления онтологий OWL и редактор Protégé. В качестве прообраза языка описания онтологий был взят язык представления знаний системы Semp-TAO.

Для конечного пользователя данные на интернет-ресурса представлены в виде множества связанных информационных объектов. Вся информация о конкретном объекте и его связях отображается в виде HTML-страницы (Рис.2), формат и наполнение которой зависят от класса данного объекта и заданного для него шаблона визуализации. При этом объекты, связанные с данным объектом, представляются на его странице в виде гиперссылок, по которым можно перейти к их детальному описанию. Список объектов отображается в виде страницы, содержащей набор ссылок на эти объекты. Для больших списков формируется составная страница, включающая список страниц с элементами навигации по этому списку. Навигация по данным интернет-ресурса представляет собой процесс перехода от одних информационных объектов к другим по заданным между ними связям. Например, при просмотре информации о конкретном проекте мы можем видеть значения его атрибутов и его связи с другими объектами. Используя представленные связи в качестве элементов навигации, можно перейти к просмотру подробной информации как по прямым связям (об описываемом объекте исследования, об используемых в проекте методах исследования и научных результатах), так и по обратным (об участниках проекта, об информационном ресурсе, описывающем данный проект). При переходе по конкретной связи любого информационного объекта мы можем получить достаточно большой список объектов (например, список всех участников крупного проекта или конференции). В связи с этим был введен механизм фильтрации списков информационных объектов. Фильтрация есть способ выборки подмножества ИО из списка путем наложения на него ограничений, т.е. задания фильтра. Фильтр является набором условий, которые определяют допустимые значения атрибутов ИО и требования к существованию связей с другими информационными объектами. Этот метод

позволяет, например, отфильтровать множество участников проекта как по возрасту или научной степени (условия на атрибут), так и по используемым ими методам исследования (условия на связанный объект).

Заключение

Согласно предварительной концепции интеллектуальный научно-образовательный интернет-ресурс будет представлять собой информационную систему, доступную через Интернет, которая обеспечивает на основе онтологии систематизацию и интеграцию научных знаний, данных и информационных ресурсов в единое информационное пространство, содержательный эффективный доступ к ним, а также поддерживающая их использование при решении различных научных и образовательных задач. ИНОИР снабжен эргономичным пользовательским web-интерфейсом и специальными редакторами, предназначенными для управления знаниями, интегрируемыми в него.

Литература

1. Арский Ю.М., Гиляревский Р.С., Туров И.С., Черный А.И. Инфосфера: Информационные структуры, системы и процессы в науке и обществе. – М.: ВИНИТИ, 1996. – 489 с.

2. Zh.B. Sadirmekova, O.L.Zhizhimov, D.A. Tussupov, M.A. Sambetbayeva//Requirements for information system to support scientific and educational activities// CEUR Workshop Proceedings(DICR-2019), //Novosibirsk, Russia,. 2019. 44-47pp.

3. Antoniou G., Harmelen F. Web Ontology Language: OWL // Handbook on Ontologies. Berlin: SpringerVerlag, 2004. P. 67-92.

4. Садирмекова Ж.Б., Тусупов Д.А.Институциональные репозитории открытого доступа.// Международной научно-практической интернет-конференции «Тенденции и перспективы развития Науки и образования в условиях глобализации».Переяслав-Хмельницкий. – 2019. 483-486 с.

5. Fedotov A.M., Tusupov J.A., Sambetbayeva M.A., Fedotova O.A., Sagnayeva S.K., Bapanov A.A., Tazhibaeva S.Z. Classification model and morphological analysis in multilingual scientific and educational information systems // Journal of Theoretical and Applied Information Technology. - 2016. - Vol.86, issue 1, - P.96-111.

6. Fedotov A.M., Tusupov J.A., Sambetbayeva M.A., Sagnayeva S.K., Bapanov A.A., Nurgulzhanova A.N., Yerimbetova A.S. Using the thesaurus to develop it inquiry systems // Journal of Theoretical and Applied Information Technology. - 2016. - Vol.86, issue 1, - P.44-61.

7. SadirmekovaZh.B., Tussupov J.A., Sambetbayeva M.A.// Development of distributed integrated information support systems for scientific activity// Второй Международный научный конференция «Ситуация, язык, речь. Модели и приложения» («Situation, Language, Speech. Models & Applications» — SLS 2019//Рим-Италия. 2019. С. 24-25.

8. Жижимов О.Л., Федотов А.М., Барахнин В.Б., Федотова О.А. Модель информационной системы для поддержки научно-педагогической деятельности // Вестник Новосибирского государственного университета. Серия: Информационные технологии. - 2014. - Т.12,№ 1. - С.89-101.

9. Загорулько Ю.А., Загорулько Г.Б., Боровикова О.И. Технология создания

тематических интеллектуальных научных интернет-ресурсов, базирующаяся на онтологии // Программная инженерия. 2016. Т. 7. № 2. С. 51-60.

ОБЕСПЕЧЕНИЕ ЭКОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ ПРИ ЭКСПЛУАТАЦИИ РАЙОНОВ ЗАПУСКА И ПАДЕНИЙ ПЕРСПЕКТИВНЫХ РАКЕТ-НОСИТЕЛЕЙ СВЕРХЛЕГКОГО КЛАССА

Ермолдина[1] Г.Т., Трушляков[2] В.И., Утегенова[1] А.У.,
Алипбаев[1,3] К.А., Суйменбаева[1] Ж.Б., Бапышев[1] А.М.,
Аден[1] А.Е., Гусейнов[1] С.Р.
[1]Институт информационный и вычислительных технологий, Казахстан
[2]Омский государственный технический университет, Россия,
[3]Алматинский университет энергетики и связи, Казахстан

Аннотация.
В статье проведен обзор состояния вопроса развития ракет-носителей (РН), предназначенных для запуска малых космических аппаратов (КА), а именно РН сверхлѐгкого класса (РН СЛК). Авторами предложена концепция информационного обеспечения эксплуатации РН СЛК с учетом требований экологической безопасности на основе модернизации ракеты и эффективной организации экологического мониторинга.

Наличие собственного космодрома определяет целый ряд политических, экономических и научно-технических причин, среди которых соображения военно-политического характера, ракетно-космические амбиции, масштабность собственной космической программы, потребность в собственных носителях, финансово-экономические возможности, общий научно-технический потенциал; и задает вектор дальнейшего его развития и наращивания предоставляемых услуг.

Анализ перспективных технологий и тенденций развития ракетостроения показывает повышение интереса бизнеса и военных к созданию ракет-носителей (РН) сверхлегкого класса (СЛК). Ожидаемое увеличение запусков фемто-, пико-, нано-, микро-, мини- и малых космических аппаратов (КА) для решения народнохозяйственных, научных и оборонных задач также свидетельствует об активном развитии рынка пусковых услуг [1-4]. По оценкам специалистов, объём рынка малых КА в 2018–2026 гг. может составить порядка $30,1 млрд.

Ситуацию в сфере активизации изучения космоса и развития средств выведения характеризуют также многие заголовки СМИ и популярных тематических онлайн-площадок [5-11]. Неудивительно, что сейчас наблюдается невиданный «бум» альтернативных проектов РН СЛК и мини-космодромов для их запуска.

Анализ тенденций развития разработок РН СЛК показывает два эволюционных подхода:

– модернизации существующих ракет космического назначения (как например, семейств «Pegasus», «Taurus», «Minotaur» (США), CZ, КТ-1 (Китай), PSLV (Индия), «Циклон» (Украина);

– разработки и проектирования новых высокоэффективных РКН (таких, как «Falcon-1e» (США), «Vega» (ЕКА), «Epsilon» (Япония), CZ-5-SSLV,- L (Китай), и другие);

Создание сверхлегких РН, рассчитанных на выведение на низкую околоземную орбиту грузов до 300 кг, предполагают проведение летных испытаний уже в ближайшие годы [1].

Разработкой РН СЛК в настоящее время занимается ряд компаний: Firefly Space Systems (США), Virgin Galactic (США), Interorbital Systems (США), Rocket Lab (США-Новая Зеландия), Orbital Sciences Corporation (США), НТЦ «Комплекс-МИТ» (Россия), ООО «Лин Индастриал» (Россия), PLD Space (Испания), Skyrora Limited (Европа) и многие другие. К тому же рыночные тренды для частных компаний уже набирают обороты, о чем свидетельствует широкая клиентура, заявленные договоренности и растущий спрос на услуги запуска малых КА [5-21].

К таким РН будут предъявляться требования широкого диапазона высот и наклонений целевых орбит, которые невозможно удовлетворить при попутном выведении, надежности, простоты подготовки к пуску, оперативности запуска для быстрого выведения на заданные орбиты, минимизации экологического воздействия на окружающую среду.

Предлагаемые на сегодняшний день разработки РН СЛК предполагают низкую стоимость выведения, высокую оперативность запуска, малые риски и затраты, возможность обеспечения индивидуального, не зависящего от других полезных нагрузок, выведения на заданные орбиты с минимальными ограничениями на окна запуска, окупаемость и рентабельность. Кроме того развитие РН СЛК позволит провести экспериментальную отработку перспективных технологических решений, в том числе применение 3D печати при изготовлении элементов конструкции, спасаемый блок первой ступени, многоразовое использование блоков РН, применение новых лёгких сплавов и композиционных материалов, сжигание отделяющихся элементов конструкции РН в процессе выведения (межступенных отсеков, головных обтекателей), подготовка и пуск РН с мобильной стартовой платформы в полуавтоматическом режиме, внедрение перспективных технологий по маршевым двигателям, системам управления, которые *могут* использоваться на РН более тяжелых классов и др.

Помимо прочего преимуществом РН СЛК является возможность более частых запусков, не привязанных к пускам тяжелых РН для решения задачи восполнения спутниковых группировок. К примеру, уже сейчас для восполнения состава системы глобальной широкополосной связи OneWeb планируется использовать сверхлегкую РН Launcher One (Virgin Galactic, США), а компания Planet (США) планирует осуществить замену отказавших спутников типа Flock (кубсат формфактора 3U) системы дистанционного зондирования Земли при помощи сверхлегкой РН Electron (Rocket Labs, США) [20] и т. д.

Анализ известных зарубежных исследований по созданию РН СНК показывает, что в настоящее время достигнуты определенные результаты в создании РН СЛК [14-24]. Среди них:

- РН SS-520 № 4 (японская твердотопливная трехступенчатая ракета) [18];

- РН Electron новозеландской компании Rocket Lab [20];
- сверхлегкая РН Alpha, стартап Firefly Space Systems (США) (2014 год) [19];
- двухступенчатая сверхлегкая РН Vector, ориентированная на коммерческий рынок микро- и наноспутников компании Vector Space Systems [21];
- сверхлегкая РН с многоразовой первой ступенью Arion 2 (Miura 5) испанской компании PLD Space, рассчитанная на выведение на НОО 150 кг полезного груза (с изменением конструкции ракеты и увеличением полезной нагрузки до 300 кг) [16];
- РН Skylark L компании Skyrora Limited прошла полномасштабное испытание, ее полет запланирован к середине следующего года [8];
- твердотопливная РН семейства «Старт», созданная на базе межконтинентальной баллистической ракеты «Тополь», способную вывести полезную нагрузку 490-1000 кг на орбиты высотой 200-1000 км [9-10];
- российская РН «Аквилон», предполагаемая грузоподъемность которой составляет до 450 кг [9];
- проект двухступенчатой РН космического назначения СЛК «Алдан» с полезной нагрузкой до 100 кг на экологически безопасных топливных компонентах. Проект получил положительную оценку экспертов Кластера космических технологий и телекоммуникаций фонда «Сколково» [11];
- модернизация существующего ракетного метеорологического комплекса МН-300 [38] и многие другие.

На сегодняшний день срочные запуски МКА практически невозможно осуществить из-за отсутствия ракеты. Производственные циклы расписаны на годы вперед, тем более каждая ракета делается под конкретную полезную нагрузку, поэтому внеплановые востребованные запуски затруднительны в коммерческих целях и привлекательны для военных задач [23]. Критичность срыва графика запусков чревата финансовыми потерями и задержкой отработки технологических решений. По мнению экспертов, срочные запуски востребованы для максимально оперативной съемки нужного региона даже при наличии надежных группировок долгоживущих спутников, все они могут оказаться либо недоступны, либо недостаточно эффективны. Накладываемые ограничения современного технологического процесса запуска РН включают также приоритет интересов владельца основного, а не попутного груза, которыми являются в своем большинстве малые КА. В таком случае привлекательность развития всевозможных проектов РН СЛК многократно возрасает.

Для срочных внеплановых запусков желательно не пользоваться основными космодромами — если это будет (пред-) военный период, то они, вероятно, либо будут заняты пополнением национальной группировки «больших» спутников (например, геостационарных спутников связи или спутников систем навигации), либо выведены из строя. В мирное же время они заняты плановой коммерческой и научной деятельностью, и прерывать ее по мелким поводам неприемлемо.

Для РН такого класса возможно создание мобильного стартового комплекса, способного производить запуски с более удобных позиций с точки зрения энергозатрат на выведение полезной нагрузки и выделения зон падения несгорающих частей РН: либо стационарного стартового комплекса с применением установщика, либо с передвижного наземного стартового комплекса (грузовой наземный транспорт с пусковым устройством, заправочной передвижной станцией и комплексом управления полетом [9, 24-26].

Преимуществом эксплуатации РН СЛК является возможность осуществления пусков с любого места, отвечающего требованиям безопасности и подходящего с точки зрения параметров целевой орбиты. Следовательно, мобильные стартовые комплексы для запусков РН СЛК в соответствии с Соглашением о природопользовании должны обеспечиваться нормами экологической безопасности, службами экологического контроля и мониторинга, мероприятиями по очистке районов падений от отработанных частей РН, нормативно-правовой документацией в части превышения лимитов по сбросам, эколого-экономической оценке ущерба и рисках и другими.

Выбор места для локализации мобильного космодрома обусловлен учетом таких факторов, как наличие зон отчуждения (участков незаселённой или малонаселённой местности) для падения отделяемых частей ракет в штатных и аварийных ситуациях, а также хорошо развитой сети транспортных и энергетических магистралей. Важно и географическое расположение места старта. Например, в зависимости от широты места старта, меняется добавка к характеристической скорости ракеты за счёт суточного вращения Земли: дополнительная линейная скорость (на экваторе 465 м/с, на широте Байконура — 316 м/с) при заданной мощности РН позволяет вывести на орбиту в восточном направлении полезный груз (ПГ) большей массы. Погодные условия в районе космодрома тоже имеют значение — большое число безоблачных и, по возможности, безветренных дней в году дают возможность более эффективно использовать оптические средства слежения за полётом РН.

Примером мобильного старта грунтового базирования является космический ракетный комплекс «Старт-1», в котором пуск твердотопливной РН осуществляется из транспортно-пускового контейнера, размещенного на колесном шасси высокой проходимости.

Каждый СК оснащён системами заправки носителя компонентами топлива, башней обслуживания ракеты, стоящей на ПУ, оборудованием предстартовой подготовки и центром управления пуском/полётом.

Компактное размещение комплексов космодрома и их группировка по классам носителей имеют большое значение для расширения диапазонов секторов азимутов пуска с каждого СК, централизованного использования оборудования и сооружений космодрома.

Исходя из анализа мировых тенденций развития ракет-носителей СЛК можно выявить основные актуальные направления исследований: прогнозные оценки экологической нагрузки в районах эксплуатации РН СЛК и проектно-поисковые проработки собственной независимой системы, обеспечивающей управляемый спуск отработавших ракетных блоков в заданные территориальные рамки.

Авторами предлагается принципиально новая концепция, предполагающая внедрение технологии управляемого спуска ракетного блока и эколого-экономическую и техническую оценку эффективности ее эксплуатации. Казахстанская и российская стороны заинтересованы в создании РН, которые оказывали бы наименьшую экологическую нагрузку на районы падения отделяющихся частей РН, расположенных на территории Республики Казахстан и соседних государств.

Учитывая многолетний российский опыт разработок и применения более чем 50 модификаций исследовательских метеорологических ракет предлагается

концепция обеспечения экологической безопасности эксплуатации РН СЛК на последних этапах жизненного цикла [27]. В основе предлагаемой концепции заложены принципы эффективной модернизации РН и организации соответствующего информационного обеспечения на этапе запуска и приземления с учетом требований экологической безопасности. Соответственно, предусматривается научно-методическая разработка её основных положений, включающих в себя:

– модели информационно-прогностической системы определения районов запуска и падения отделяющихся частей РН СЛК на основе системного анализа, включающего в себя анализ целей запуска, энергетических возможностей РН СЛК, координат районов падения с учётом минимизации экологического воздействия на окружающую среду;

– исследования в обеспечении создания бортовых систем, реализующих управляемый спуск отработавшей первой ступени РН СЛК в рекомендуемый район падения для различных направлений разработок (модернизация существующих РН СЛК на основе твердотопливных ускорителей первой ступени [26-27], перспективных разработок РН СЛК на основе жидкостных двигателей [28-29] и

- отработки технологии сжигания межступенного переходного отсека и створок головного обтекателя.

Реализация концепции на основе модернизации РН СЛК позволит:

– рассматривать РН СЛК как перспективный элемент для подготовки и переподготовки кадров для создаваемой казахской ракетно-космической отрасли;

– снизить экологическую нагрузку на природную среду, в том числе и в районах падения;

– создавать оперативные резервы точек запуска и приземления и вести мониторинг данных точек.

Таким образом, если использовать главный критерий – показатель функциональной (перспективы создания системы подготовки и переподготовки кадров для создаваемой казахстанской ракетно-космической отрасли) и экологической эффективности ракетно-космической системы на основе РН СЛК, учитывать затраты и финансовые потери на восстановление экологической обстановки в районах падения, то реализация проекта представляется целесообразной [30-31]. К тому же соблюдение принципов экологической безопасности для развития космической инфраструктуры гражданского и оборонного комплекса РК при реализации ракетно-космической деятельности [31], в частности, при эксплуатации и запускам малых космических аппаратов различного назначения, представляется актуальной задачей в соответствии со статьей 24 Закона РК «О национальной безопасности [30].

Результаты комплексных исследований, проведенные совместно с ведущими учеными России в рамках проекта AP05131162 «Теоретические и экспериментальные исследования инновационной технологии создания РН с улучшенными экологическими характеристиками на примере перспективных РН, запускаемых с космодрома Байконур», послужат основой разработки перспективных РН и позволят отработать проектные параметры РН для управляемого спуска отработавших ступеней [26-29, 32-42].

Литература

1. Давыдов П.А. Обоснование требований к ракете-носителю сверхлёгкого класса нового поколения с учётом мировых тенденций развития средств выведения и рынка пусковых услуг. // Космонавтика и ракетостроение. Изд.: ЦНИИМаш, ISSN: 1994-3210. – № 2(71). – 2013. - с. 67-72.

2. Смирнов В.И. Международные тенденции в создании и эксплуатации малых космических аппаратов. // Космонавтика и ракетостроение. - 2003, вып. 2 (31). - с. 160.

3. Колюбакин В. Состояние мирового рынка пусковых услуг. - https://telesputnik.ru/materials/tekhnika-i-tekhnologii/article/sostoyanie-mirovogo-rynka-puskovykh-uslug/ (10.09.2020)

4. Кузнецов А.Н., Осадченко А.С., Ромашкин А.М. Анализ сектора рынка малых спутников (наноспутников) и возможных схем их размещения в отсеках полезного груза средств выведения. // Космонавтика и ракетостроение. - 2003, вып. 2 (31). - с. 137.

5. Ермаков А. Мобильная космонавтика: зачем Китаю свои «морские старты. - https://iz.ru/887258/aleksandr-ermakov/mobilnaia-kosmonavtika (10.09.2020)

6. https://www.france24.com/en/20190713-macron-france-space-forc (30.08.2020)

7. https://twitter.com/Cosmic_Penguin/status/1203183000113958912

8. https://www.skyrora.com/

9. Е.В. Космодемьянский, А.В. Нагиев, Д.Ю. Изратов, В.А. Кирпичев, П.А. Давыдов, А.А. Маркарова, И.В. Козлова, А.Ю. Окутин, А.Ю. Пустовалов. Проект космического ракетного комплекса на базе ракеты-носителя сверхлёгкого класса // Онтология проектирования. – 2018. – Т. 8, №4(30). - С.523-539. – DOI: 10.18287/2223-9537-2018-8-4-523-539.

10.. https://ecoruspace.me/%D0%A1%D1%82%D0%B0%D1%80%D1%82+1.html

11. Сверхлегкая ракета «Алдан». - https://spacelin.ru/proekty/sverkhlegkaya-raketa-aldan/ (09.09.2020).

13. Костев Ю. В., Мезенова О. В., Позин А. А., Шершаков В. М. Система запуска малых космических аппаратов // Изв. вузов. Приборостроение. - 2016. - Т. 59, № 6. - С. 482—488.

14. Клюшников В.Ю. Ракеты-носители сверхлегкого класса: ниша на рынке пусковых услуг и перспективные проекты //Воздушно-космическая сфера. – 2019, №3. -С.58-71.

15. The Annual Compendium of Commercial Space Transportation: 2018. Federal Aviation Administration, January 2018, Washington. 255 p.

16. Arion-2 Miura-5. - URL: http://www.b14643.de/Spacerockets_3/PLDSpace/Description/Frame.htm (Дата обращения: 01.06.2020).

17. Сенькин В. С. Оптимизация проектных параметров ракеты-носителя сверхлегкого класса //Техническая механика. – 2009, № 1. - С. 80-88.

18. Japan's SS-520 CubeSat Launch Vehicle Achieves Success on Second Try [Электронный ресурс]. URL: http://spaceflight101.com/japanss-520-5-launch-success/ (Дата обращения: 06.06.2020).

19. Firefly Payload User's Guide. August 10, 2018. Austin (Texas): Firefly Aerospace Inc. 64 p.

20. Electron. Payload User's Guide. Version 6.2, Rocket Lab. New Zealand, 2018. 53 p.

21. Vector-H Forecasted Launch Service Guide – VSS-2017-023 - Version 2.0. Tucson (Arizona): Vector Space Systems, 2017. 14 p.

22. Данилюк А. Ю., Клюшников В. Ю., Кузнецов И. И., Осадченко А. С. Требования к облику и основным проектным параметрам микроракетного комплекса, предназначенного для запуска малых космических аппаратов размерностей “нано”, “пико” и “фемто” // Вестник НПО им. С. А. Лавочкина. – 2015. - Т. 29, № 3. - С. 107—113.

23. Ю.А. Матвеев, А.А. Позин, В.М. Шершаков. Системные вопросы создания ракет-носителей сверхлёгкого класса // Вестник НПО имени С.А. Лавочкина. - №2/44, 2019. - С. 37 – 43.

24. https://russiancouncil.ru/analytics-and-comments/analytics/novyy-etap-militarizatsii-kosmosa/

25. Космодромы: состав и виды. - https://sovkos.ru/cosmodrom/kosmodromy-sostav-i-vidy.html

26. Suimenbayev B.T., Trushlyakov V.I., Yermoldina G.T., Suimenbayeva Zh.B. and Bapyshev A.M. Development of a measures complex to reduce the technogenic impact of launches of the promising Irtysh launch vehicle in the impact areas of the Baikonur cosmodrome. //Mechanical Science and Technology Update IOP Conf. Series: Journal of Physics: Conf. Series1260. – 2019. –P. 11-22.//doi:10.1088/1742-6596/1260/11/112025.

27. Suimenbayev B.T., Trushlyakov V.I., Yermoldina G.T., Suimenbayeva Zh.B., Bapyshev A.M. Business-process development of the information analytical Systems of the Baikonur cosmodrom and launch vehicle design for ecological safety Improving in the impact areas of the worked-off stages. //News of The National Academy of Sciences of The Republic of Kazakhstan. Physico-Mathematical Series. – Volume 1, Number 323 (2019), 5 – 13 //https://doi.org/10.32014/2019.2518-1726.1.2019. – Vol.1,№323. – P.5-13.

28. V. Trushlyakov, Ya. Shatrov, B. Sujmenbaev, D. Baranov The designing of launch vehicles with liquid propulsion engines ensuring fire, explosion and environmental safety requirements of worked-off stages/Acta Astronautica. – 2017. – Vol. 131. – pp. 96-101. DOI: 10.1016/j.actaastro.2016.11.031

29. V. Trushlyakov, A. Novikov, I. Lesnyak Study of acoustic and low-pressure exposure on the temperature of the evaporation of a liquid with free interface before it freezes/ Journal of the Acoustical Society of America. - 2019. - Т. 146, № 5. - С. 3333-3338.

30. Закон Республики Казахстан «О национальной безопасности Республики Казахстан» (с изменениями и дополнениями по состоянию на 01.01.2020 г.)

31. Соглашение между правительством Российской Федерации и правительством Республики Казахстан по экологии и природопользованию на территории комплекса "Байконур" в условиях его аренды Российской Федерацией, Алма-Ата, 4 октября 1997 года.

32. Трушляков В.И., Новиков А.А., Лесняк И.Ю., Паничкин А.В. Исследование процесса испарения жидкости со свободной поверхностью в замкнутой ёмкости при понижении давления и акустическом воздействии // Теплофизика и аэромеханика. – 2019. – Т. 26, № 2. – С. 275 – 286.

33. Жариков К.И., Трушляков В.И. Моделирование процесса истечения парогазовой смеси из дренажной магистрали ступени ракеты-носителя. // Инженерно-физический журнал. –2019. – Т 92, № 3. – С. 1-13.

34. Суйменбаев Б.Т., В. Трушляков В.И., Ермолдина Г.Т., Суйменбаева Ж.Б., Бапышев А.М. Концепция снижения техногенного воздействия пусков перспективной ракеты-носителя «Иртыш» в районах падения космодрома Байконур. //Омский научный вестник. Серия авиационно-ракетное и энергетическое машиностроение. Том 3 № 2 2019. The concept of reducing the man-made impact of launches of the promising Irtysh launch vehicle in the impact areas of the Baikonur cosmodrome // Omsk scientific bulletin. Series aviation-rocket and power engineering vol. 3 no. 2 2019. С. 115-126. DOI: 10.25206/2588-0373-2019-3-2-115-126. (https://orcid.org/inbox#50%C2%A0274%C2%A0996).

35. Суйменбаев Б.Т., Ермолдина Г.Т., Суйменбаева Ж.Б., Бапышев А.М., Трушляков В.И. Разработка научно-методического обеспечения снижения техногенного воздействия пусков РН в районах падения космодрома Байконур //Вестник КазНТУ № 6 (130), 2018. - С. 501-505.

36. Ермолдина Г.Т., Бапышев А.М. Подготовка предложений по проведению экспериментальных исследований по испарению остатков компонентов топлива в баках отработавших ступеней РН // Вестник КазНИТУ. - №5 (135) 2019. - С. 759-764

37. Suimenbayev B.T., Trushlyakov V.I., Zhubatov Zh.K., Yermoldina G.T., Suimenbayeva Zh.B., Bapyshev A.M. Optimization of allocation of areas for the falling of the worked-off stages boosters of the launch vehicle based on zoning and classification of the existing impact areas of Baikonur cosmodrome /8TH European Conference for Aeronautics and Space Sciences. – Madrid, 2019. – P.89-102. 2019. DOI: 10.13009/EUCASS2019-220

38. Суйменбаев Б.Т., Трушляков В.И., Ермолдина Г.Т., Суйменбаева Ж.Б., Бапышев А.М. Разработка комплекса мероприятий по снижению техногенного воздействия пусков перспективной РН «Иртыш» в районах падения космодрома Байконур /Материалы III Междунар.науч.-техн.конф., Омск, 2019. –С. 177-185

39. Суйменбаев Б.Т., Трушляков В.И., Ермолдина Г.Т., Суйменбаева Ж.Б., Бапышев А.М. Предложения к концепции проектирования и эксплуатации перспективных РН с ЖРД и районов падения космодрома Байконур в рамках проекта Байтерек. /Материалы XIII Всерос.науч.-техн.конф. «Проблемы разработки, изготовления и эксплуатации ракетно-космической техники и подготовки инженерных кадров для авиакосмической отрасли», посв. Памяти гл. Конструктора ПО «Полет» А.С. Клинышкова, Омск, 2019. – С.36-43

40. Суйменбаев Б.Т., Трушляков В.И., Ермолдина Г.Т., Бапышев А.М. Информационно-аналитическая система для создания ракет-носителей с улучшенными экологическими характеристиками/Междунар. Сатпаевские чтения. – Алматы: КазНИТУ, 2018. – С. 894-898.

41. Суйменбаев Б.Т., Трушляков В.И., Ермолдина Г.Т., Суйменбаева Ж.Б., Бапышев А.М. Разработка бизнес-процесса информационно-аналитических систем космодрома Байконур и проектирования ракеты-носителя для повышения экологической безопасности в районах падения отработавших ступеней. /Матер. III Междунар. Науч. Конфер. «Информатика и прикладная математика», посв. 80-летнему юбилею проф. Бияшева Р.Г. и 70-летию проф. Айдарханова М.Б. – Алматы, 2018. – С.355-366.

42. Трушляков В.И., Суйменбаев Б.Т., Севоян В.А., Ермолдина Г.Т., Суйменбаева Ж.Б., Бапышев А.М. Методология экспериментальных исследований получения парогазовых смесей для управления движением отработавших ступеней ракет-носителей при спуске с траекторий выведения / IV междунар. Науч.-практ. Конф. «Информатика и прикладная математика», посв. 70-летнему юбилею проф. Биярова Т.Н., Вуйцика В.Ч. и 60-летию проф. Амиргалиева Е.Н., Алматы, 2019. – С.492-500.

РОЛЬ ВНЕШНИХ БАЗ ДАННЫХ ПРИ ПОДБОРЕ КОНТРАГЕНТОВ[1]

Бобров Л.К. Медянкина И.П., Михайленко Н.А., Семканова В.А., Утепбегенов И.Т.
e-mail: l.k.bobrov@edu.nsuem.ru, i.p.medyankina@edu.nsuem.ru, mih_nt@mail.ru, vsemkanova@gmail.com, i.utepbergenov@gmail.com
Новосибирский государственный университет экономики и управления, Россия
Новосибирский государственный университет экономики и управления, Россия
Новосибирский государственный университет экономики и управления, Россия
Новосибирский государственный университет экономики и управления, Россия
Институт информационных и вычислительных технологий КН МОН РК, Казахстан

Аннотация. *Подчеркнута актуальность задачи подбора контрагентов для инновационных организаций. Рассмотрена процедура и методы оценки и выбора контрагентов. Дана краткая характеристика некоторых ресурсов бизнес-информации. Показано, что использование бизнес-информации позволяет расширить географический охват при поиске потенциальных контрагентов и на начальном этапе отсеять заведомо не подходящих кандидатов, что снижает трудоемкость последующих работ. Дано краткое описание процедуры оценки и подбора контрагентов, предусматривающей использование мировых баз данных и показано, что использование бизнес-информации способствует снижению рисков выбора неблагонадежных контргентов.*

Ключевые слова: *инновационная деятельность, подбор контрагентов, методы оценки, процедура отбора, базы бизнес-информации.*

Введение

Вопросу обоснованного выбора различного рода контрагентов (поставщиков, дилеров, торговых представителей и т.п.) посвящено достаточно большое число публикаций, поскольку, при отсутствии должного внимания к этому вопросу, возможно возникновение негативных последствий, среди которых самыми распространенными являются:

[1] Работа поддержана грантом МОН РК (проект №AP05134019 «Разработка научно-методических основ и прикладных аспектов построения распределенной системы информационного обеспечения инновационной деятельности с учетом специфических особенностей каждого из этапов жизненного цикла инноваций»).

– приобретение некачественной продукции;

– нарушение сроков поставки товаров;

– неполучение или несвоевременное получение денежных средств за поставленные товары, выполненные работы, оказанные услуги и т. д.

Особенно актуален этот вопрос для инновационных предприятий. И не важно, идет ли в данном случае речь об инновационных предприятиях, развивающихся за счет собственных технологий, работающих в кооперации с внешними партнерами или приобретающих лицензии и патенты [1], поскольку, согласно результатам исследований, более 80% инновационно активных предприятий взаимодействуют с внешними организациями и более 63% высокотехнологичных предприятий сотрудничают с контрагентами с целью совместного проведения разработок и реализации инновационных проектов [2]. Кроме того, учитывая высокий уровень неопределенности и риска практически на всех этапах жизненного цикла инновационного проекта, можно утверждать, что для малых и средних инновационных предприятий, совместная деятельность с недобросовестными контрагентами может для этих предприятий закончиться банкротством.

В настоящей работе предпринята попытка показать, что трудоемкость реализации процедуры подбора контрагентов может быть существенно сокращена, а риски неправильного выбора уменьшены при условии использования соответствующих баз данных бизнес-информации.

Процедура и методы выбора контрагентов

В общем случае данная процедура включает следующие этапы:

– формирование исходного пула потенциальных контрагентов;

– проверка организаций из пула контрагентов на благонадежность;

– выбор метода для анализа потенциальных контрагентов;

– разработка системы критериев, исходя из выбранного метода анализа;

– формирование окончательного списка контрагентов;

– установление связи с контрагентом, проведение переговоров и оформление документов о сотрудничестве.

Как показывает практика, формирование исходного пула потенциальных контрагентов может осуществляться различным образом – от опроса коллег и знакомых до использования различного рода каталогов и проведения поисков по сайтам в интернете.

Например, на портале проекта Rusprofile.ru (www.rusprofile.ru) размещена подробная актуальная информация о более чем 10 миллионах российских юридических лиц и 12 миллионах индивидуальных предпринимателей России. Поиск информации о контрагентах на портале можно осуществлять, по названию организации, адресу, руководителю, учредителям, с помощью Справочник компаний на основе классификатора ОКВЭД и др.

Международная информационная система Kompass (ru.kompass.com) содержит данные по 34 442 311 компаний в более чем 64 странах мира. Поиск информации можно осуществлять по названию компании, производимым товарам и услугам, по стране, области, городу, по ключевым словам.

С точки зрения инновационной целесообразности, выбирать контрагентов можно с использованием Единой государственной информационной системы учета

результатов научно-исследовательских и опытно-конструкторских работ (https://www.rosrid.ru). В рамках этой системы осуществляется формирование и поддержка национального библиотечно-информационного фонда Российской Федерации в части открытых неопубликованных источников научной и технической информации – отчётов о НИОКР, кандидатских и докторских диссертаций, описаний результатов интеллектуальной деятельности и их использования [3].

Примером расширения географии поиска контрагентов может служить использование семейства баз данных свободного доступа «Wer liefer was», охватывающих европейские фирмы (www.wlw.de) и позволяющие проводить поиск как по названиям фирм, так и по продуктам.

В ряду крупнейших баз данных можно выделить базу «Бизнес-Карта» (http://www.biznes-karta.ru), представляющую информацию о 2.8 млн. зарубежных компаний по 56 странам мира и 310 тыс. предприятий по России и странам СНГ. Здесь представлены все основные сектора экономики, отрасли и подотрасли промышленности. Описание предприятия включает такие поля, как название, адрес, Ф.И.О. руководителя, контактные данные, численность работающих, номенклатура продукции, используемые сырье и материалы, экспорт, импорт, форма собственности, год основания. При поиске можно выбирать предприятия по территории, сектору рынка, продукции и услугам, по численности работающих, форме собственности, году основания и т.д., при этом обеспечивается экспорт данных в формате EXCEL, WORD или TXT.

Использование баз данных бизнес-информации при формировании исходного пула потенциальных контрагентов позволяет:

– с учетом глобализации рынка существенно расширить географию поиска подходящих контрагентов;

– выявить негативную информацию о фирмах;

– получить данные о платежах интересующих компаний и уровне их платежной дисциплины;

– получить информацию о топ-менеджерах компаний, и т.п.

Выявить негативную информацию и проверить контрагентов из пула на благонадежность, проанализировав различные аспекты их деятельности, инновационное предприятие может самостоятельно, воспользовавшись, например, такими базами, как "Риски бизнеса: проверь себя и контрагента" на сайте Федеральной налоговой службы (https://egrul.nalog.ru/index.html), «Единый федеральный реестр сведений о фактах деятельности юридических лиц» на сайте Федресурса (https://fedresurs.ru/), банк данных исполнительных производств на сайте ФСПП России, Сведения о юридических лицах, имеющих задолженность по уплате налогов на сайте ФНС (https://service.nalog.ru/zd.html) и др.

Кроме того, существуют сервисы, где проведут комплексную проверку контрагента по заявке предприятия. Из наиболее распространенных в России сервисов можно выделить следующие: «Контур.Фокус» – поиск информации для проверки контрагента осуществляется по базам России, Беларуси, Казахстана (https://focus.kontur.ru/); «СПАРК-Интерфакс» – поиск информации для проверки контрагента осуществляется по базам России, Украины, Беларуси, Казахстана, Киргизии и Кипра (http://www.spark-interfax.ru), «Прима-Информ» (https://www.prima-inform.ru/), «Интегрум» (https://integrum.ru/), «СБиС Контрагенты» (https://sbis.ru/contragents). Эти сервисы позволяют получить все

необходимые сведения о контрагенте: о его деятельности, актуальном составе руководства, выписках из ЕГРЮЛ и ЕГРИП, возможных долгах, судебных процессах и многом другом.

В отношении контрагентов из стран Евросоюза информацию можно получить на сайте Европейского бизнес реестра – European Business Register (https://www.ebr.org/).

Особо следует остановиться на решениях, предлагаемых LexisNexis (http://www.lexisnexis.ru/solutions).

Lexis® Diligence - интегрированная база данных для комплексной проверки организаций и физических лиц на благонадежность (due diligence). База данных позволяет проверить контрагента по 150 зарубежным базам данных компаний (Hoover's, Dun & Bradstreet, Worldscope и др.), базам данных санкций, спискам политиков и аффилированных лиц (politically exposed persons), архивам СМИ, биографическим данным и судебным делам.

Lexis® Diligence содержит:

– информацию о компаниях, включая сведения о юридической и кредитной истории, банковских счетах, бухгалтерской отчетности: проверка юридического лица, получение информации о бизнесе, структуре управления, и т.п.;

– архивы применения санкций, справки по PEP (politically exposed persons) и вотч-листы: проверка по черным спискам и историям санкций (OFAC, HM Treasury, FBI), база данных по 800 000 политическим деятелям;

– глобальный архив новостей с глубиной более 35 лет, позволяющий, в том числе, получить информацию, не доступную в Интернете: проверка по 23 000 международным, национальным и региональным СМИ и блогам;

– глобальную базу юридических прецедентов и справочной информации по судебным делам;

– биографии физических лиц, охватывающие примерно 500 биографических источников, включая Who's Who и Debrett's;

– информацию по странам: определение стран с высоким уровнем риска на основе отчетов мировых СМИ и углубленных аналитических докладов Economist Intelligence Unit.

Эксперты LexisNexis регулярно готовят и публикуют различного рода аналитические материалы, но и привлекаются для подготовки индивидуальных отчетов по заказам клиентов компании.

В составе ресурсов бизнес-информации LexisNexis большой интерес представляют справочники Company Dossier и Industry Dossier.

Company Dossier предоставляет обширные сведения о более чем 35 млн. компаний по всему миру. Эта информация позволяет пользователю самостоятельно подготовить отчеты, отражающие следующие аспекты деятельности потенциальных партнеров, заказчиков и конкурентов:

– структура и финансовые инструменты компаний;

– материнские и дочерние компании;

– товарные знаки;

– упоминания в новостях, и др.

Кроме того, использование Comany Dossier дает возможность сравнивать показатели деятельности компании-пользователя с показателями деятельности

четырех ближайших конкурентов, получать информацию о перспективах развития рынка и новых возможностях, а также управлять рисками путем получения важнейшей информации о благонадежности, деловых партнерах, судебных спорах и интеллектуальной собственности.

Industry Dossier предоставляет доступ к материалам и показателям, собранным из авторизованных деловых, финансовых, экономических, правовых и новостных источников и охватывающим более тысячи различных отраслей,

В качестве источников информации выступают Mergerstat, Integra, Market Guide, U.S. Congress Bill Text, Bill Tracking, U.S. Census Bureau Data и др.

Использование Industry Dossier дает возможность:

– мониторинга рыночной информации на уровне отрасли, компании или продукта;

– оценки и сравнения потенциальных партнеров, существующих альянсов, слияний и поглощений;

– идентификации и анализа возможностей рынка и конкретного продукта;

– исследования условий ведения бизнеса и анализа соответствующих статистических данных.

Полученная информация позволит исключить из списка потенциальных контрагентов неблагонадежные организации, что приведет к существенному уменьшению трудозатрат на последующий сбор необходимой информации о контрагентах и их детальный анализ.

Исключив на основе результатов анализа неблагонадежных контрагентов из пула, следует перейти к выбору критериев отбора и метода для анализа потенциальных контрагентов.

Выбор метода для анализа потенциальных контрагентов является непростой задачей ввиду большого множества таких методов и их вариаций. Свидетельством тому является обзорная статья Krishnendu Mukherjee «Supplier selection criteria and methods:past, present and future», посвященная методам и моделям оценки и выбора поставщиков как одного из вида контрагентов [4].

Следует отметить различия в понятиях оценки и выбора контрагента, они не являются синонимами.

Оценка — это многозначное понятие, обозначающее способ установления значимости чего-либо для действующего и познающего субъекта.

Оценку также можно трактовать как информацию, полученную в результате анализа тенденций, стратегического обзорного материала и ознакомления с материалами по внутренним и внешним условиям [5].

Соответственно, методы оценки контрагента и методы выбора контрагента имеют разное назначение. Методы можно разделить на методы оценки (метод множественной регрессии, метод главных компонент и др.) и методы выбора (например, метод аналитических сетей, метод анализа иерархий и др.).

Из методов оценки можно выделить количественные и качественные, а из количественных – параметрические и непараметрические.

При оценке контрагентов стараются использовать преимущественно числовые данные, характеризующие деятельность анализируемого объекта.

Наиболее распространенными методами, применяемыми в качестве инструмента для выбора контрагентов, являются: метод рейтинговых оценок, метод оценки затрат, метод доминирующих характеристик [6]. Несмотря на то, что еще

один из наиболее используемых методов - метод категорий предпочтения - относят к методам выбора контрагента, он, по своей сути, является методом оценки.

Охарактеризуем кратко перечисленные методы.

Метод рейтинговых оценок. Согласно этому методу, после сбора информации необходимо разработать систему критериев для выбора контрагента. Обычно основными критериями выбора контрагента являются цена, качество товара и надежность поставки [6]. Однако, в зависимости от ситуации, на первое место могут выходить [7]: производственные мощности, местоположение, технический потенциал, финансовое положение, возможность компромиссов и др.

После отбора критериев выбора контрагентов, экспертным путем устанавливается их значимость по выбранным показателям, а также оценивается вес каждого показателя. Далее рассчитывается рейтинг каждого контрагента посредством суммирования произведений веса показателя на его экспертную оценку. Сравнивая полученные значения рейтинга для разных контрагентов, определяют наилучшего партнера.

Метод оценки затрат. Рассчитываются все возможные издержки и доходы по контрагентам. Выбирается альтернатива с наименьшими расходами. Метод требует большого объема информации и проведения анализа по каждому поставщику.

Метод доминирующих характеристик. Метод состоит в сосредоточении на одном выбранном параметре (критерии) как основе для последующей оценки. Таким параметром может быть наиболее низкая цена, наилучшее качество, график поставок, внушающий наибольшее доверие, и т.п.

Метод категории предпочтения. В этом случае оценка контрагента, в том числе и выбор способа его оценки, зависит от информации, стекающейся из многих подразделений фирмы. Также анализируется информация, полученная из разговоров на профессиональных встречах, конференциях, данные СМИ [6]. Такой метод подразумевает наличие обширной и разнообразной информации из множества источников, которая позволяет рассматривать каждый фактор наравне с остальными.

Не останавливаясь далее на описании других методов, для иллюстрации их многообразия приведем классификационную схему методов подбора контрагентов, предложенную в работе [8], где автор подразделяет методы на две группы: атомарные (единичные, отдельные), и интегрированные (комплексные). Первые, в свою очередь, подразделяются на математические, статистические и методы с применением искусственного интеллекта (рис. 1).

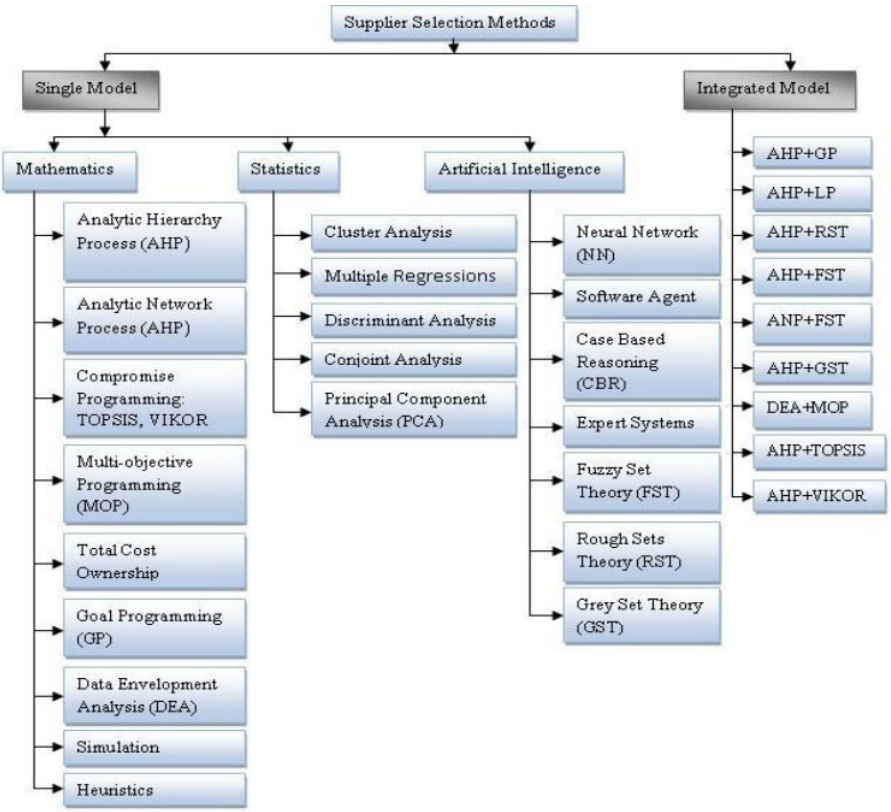


Рис. 1. Классификация методов отбора контрагентов

Однако, следует отметить, что представленная классификация, во-первых, охватывает далеко не все методы (напр., в ней отсутствуют методы ELECTRA). Во-вторых, часть методов используется лишь для оценки контрагентов, а не для выбора. Например, кластерный анализ, множественная регрессия, дискриминантный анализ, совокупная стоимость владения.

Для применения методов оценки и отбора необходимо разработать систему критериев. Количество критериев может варьироваться для каждого метода. Например, инновационных предприятий можно использовать такие критерии, как цена, размер минимальной партии, географическое положение, условия поставки, транспортные расходы, сроки поставки, качество продукции, надежность поставки.

На основании сформированной системы критериев применяется соответствующий метод для анализа контрагентов, в результате чего определяется окончательный список *контрагентов, после чего с ними* устанавливаются связи, проводятся переговоры и, по итогам переговоров, оформляются документы о сотрудничестве.

Таким образом, предлагаемая процедура оценки и подбора контрагентов, предполагающая использование информационных ресурсов, предлагаемых крупнейшими вендорами, может выглядеть следующим образом.

Этап 1. Формирование исходного пула потенциальных контрагентов. Используются базы данных, позволяющие найти кандидатов исходя из требуемого перечня нужных продуктов (услуг).

Этап 2. Проведение анализа, направленного на отсеивание из исходного пула кандидатов, не отвечающих некоему заданному набору общих требований. Здесь могут использоваться базы данных Dun&Bradstreet, Tomson Reuters, LexisNexis,

Интерфакс, и др., позволяющие проанализировать негативные отзывы о фирме, получить информацию о судебных разбирательствах (касающихся как собственно фирмы, так и ее топ-менеджеров), оценить финансовое состояние фирмы и уровень платежной дисциплины, а также многое другое. По завершении данного этапа формируется список кандидатов для последующего детального анализа в соответствии с наиболее подходящими критериями и методами.

Этап 3. Выбор критериев и метода анализа потенциальных контрагентов.

Этап 4. Проведение детального анализа потенциальных контрагентов и формирование финального списка потенциальных контрагентов. На данном этапе также может использоваться бизнес-информация, предоставляемая вендорами, упомянутыми выше (см. этап 2), причем некоторые из них предоставляют инструменты для формирования досье на интересующие фирмы.

Этап 5. Установление непосредственных контактов с потенциальными контрагентами, проведение необходимых переговоров и оформление документов о сотрудничестве.

Заключение

В практике работы инновационных организаций с различного рода контрагентами могут устанавливаться длительные, взаимовыгодные отношения, характеризуемые как «надежное партнёрство», либо временные взаимоотношения, связанные, например, с сезонными поставками, однако в каждом конкретном случае существует проблема поиска, оценки и подбора контрагентов.

С одной стороны, процесс глобализации мировой экономики, формирование единого информационного пространства предоставляют компании, действующей на рынке, практически неограниченные возможности, касающиеся поиска и выбора контрагентов. С другой стороны, усложняется задача их подбора и повышаются риски установления контактов с недобропорядочной фирмой.

В предлагаемой работе показано, что эти риски, равно и как трудоемкость процедуры выбора контрагентов, могут быть в значительной мере снижены при условии использования ресурсов бизнес-информации, предлагаемых крупными вендорами и доступных через сеть интернет. На предоставление метаинформации о таких информационных ресурсах ориентирован проект ИИВТ КН МОН РК «Разработка научно-методических основ и прикладных аспектов построения распределенной системы информационного обеспечения инновационной деятельности с учетом специфических особенностей каждого из этапов жизненного цикла инноваций».

Литература

1. Иванова, В.О. Рейтинговая система оценки контрагентов в условиях инновационного развития Госкорпорации «Росатом»/ В. О. Иванова // Вопросы инновационной экономики. – 2012. – № 4. – С. 21-29. – http://www.creativeconomy.ru/articles/26934/ (дата обращения: 08.09.2020).

2. Открытость российских инноваций / материал подгот. В.В. Власова, В.А. Рудь // Наука. Технологии. Инновации. – 2019. – 21 окт. – https://issek.hse.ru/data/2019/10/21/1528901491/NTI_N_149_21102019.pdf (дата обращения: 05.09.2020).

3. Инструкция // Единая государственная информационная система учета научно-исследовательских, опытно-конструкторских и технологических работ гражданского назначения: [сайт]. – https://www.rosrid.ru/resources/docs/instruction.pdf (дата обращения 05.09.2020).

4. Mukherjee, Krishnendu. Supplier Selection : An MCDA-Based Approach / by Krishnendu Mukherjee. - XX, 128 p. 43 illus. : online resource. - (Studies in Systems, Decision and Control). – https://pdfs.semanticscholar.org/4060/c7ff4dd1513eecbc35cc2409816a6ca26b11.pdf?_ga=2.189985576.249769656.1599912003-1380159785.1599912003 (дата обращения 02.09.2020).

5. Оценка // Википедия: [сайт]. – https://ru.wikipedia.org/wiki/Оценка (дата обращения 21.08.20).

6. Сергеев, В.И. Логистика снабжения : учебник для бакалавриата и магистратуры / В. И. Сергеев, И. П. Эльяшевич ; под общ. ред. В. И. Сергеева. – 2-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2014 – 523 с.

7. Линдерс, Майкл Р. Управление снабжением и запасами. Логистика : [пер. с англ.] / Майкл Р. Линдерс, Харольд Е. Фирон. – Санкт-Петербург : Victory, 2002. - 757 с. : ил.

8. Mukherjee, Krishnendu. Supplier selection criteria and methods:past, present and future / by Krishnendu Mukherjee [https://www.researchgate.net/publication/260250183_Supplier_selection_criteria_and_methods_past_present_and_future] (дата обращения 02.09.2020).

МЕТОДИКА УПРАВЛЕНИЯ ИННОВАЦИОННЫМ ПРОЦЕССОМ МЕНЕДЖМЕНТА КАЧЕСТВА ПРЕДПРИЯТИЯ

Тойбаева Ш.Д., Буранбаева А.И., Исабекова Л.С.
e-mail: shara_t@mail.ru, aburanbaeva@gmail.com, lyazzka07@mail.ru
Институт информационных и вычислительных технологий КН МОН РК, Казахстан
Институт информационных и вычислительных технологий КН МОН РК, Казахстан
Институт информационных и вычислительных технологий КН МОН РК, Казахстан

Аннотация. *Одним из важных стратегических инструментов в бизнесе является Качество. Большую значимость имеют вопросы по оценке эффективности СМК предприятия, учитывая специфику показателей качества, мультиуровневость системы, а также необходимость выбора оптимального числа показателей эффективности и оценку состояния системы, что связано с формированием рациональных решений при управлении СМК.*

Работа поддержана грантом МОН РК (проект №AP05134019 «Разработка научно-методических основ и прикладных аспектов построения распределенной системы информационного обеспечения инновационной деятельности с учетом специфических особенностей каждого из этапов жизненного цикла инноваций»).

Ключевые слова: *автоматизированная система управления, менеджмент качества, оценка результативности.*

Концепция устойчивого развития Государственной стратегии РК требует разработку методики устойчивого управления предприятием [1].

Устойчивость предприятия - состояние экономических и финансовых ресурсов, обеспечивающее постоянную прибыль, осуществление своих обязательств заинтересованным сторонам и достаточные условия для производственной деятельности, и учет внешних и внутренних факторов предприятия [2].

Разработка и внедрение СМК, является инновационным процессом, в целях повышения ее эффективности и результативности. За последние годы отмечается развитие систем на основе интеллектуального управления [3]. Основным направлением развития данных систем является использование аппарата нечеткой логики: нечеткого множества, нечеткого моделирования и т.п.

В данном исследовании опираются на труды отечественных и зарубежных ученых, представленных ниже.

В области стратегических методов управления предприятием в изменчивой среде бизнеса - сбалансированной системе показателей (ССП) уделено большое внимание авторами Капланом Р., Нортоном Д., в работе «Сбалансированная система показателей, определяющих эффективность работы организации» рассмотрен современный способ оценки деятельности предприятия. ССП используется для повышения эффективности внутренних и внешних коммуникационных процессов, контроля и совершенствования показателей деятельности предприятия [4,5] ССП не является инструментом формирования стратегии предприятия, она используется для описания существующей стратегии [6]. В трудах Качалова В.А. даны ответы на вопросы по разработке, внедрению, сертификации, а также совершенствованию СМК по экологическому управлению на базе моделей таких систем, которые регламентируются в ISO 9001:2015 и ISO 14001:2015. [7].

В области разработки технологии автоматизации систем управления менеджментом качества предприятия в Казахстане также рассматривается одна из распространенных современных методологий «Шесть сигм» [8] для улучшения производительности, где уделяется внимание на снижение количества браков, процессам и услугам [9,10]. В трудах Моисеевой А.В. выполнен анализ приложений ПО и приложений в сфере управления менеджментом качества, выполнен обзор специального программного обеспечения, распространяемого для улучшения основных этапов бизнес-процесса организации и автоматизация систем менеджмента качества [11]. В работе [12] изучено влияние ИТ-компетенции на систему менеджмента качества предприятия, что обеспечит большую эффективность программы СМК.

Информационные технологии способствуют изменению отношений между потреблением и производством, для их взаимодействия необходим обмен информацией, чтобы построить организацию и управление как для производителей, так и для потребителей [13].

В рамках онтологического моделирования представления и управления знаниями в системе менеджмента качества изучена монография Кубекова Б.С. «Организация и представление знаний планируемого обучения на основе онтологий» [14], в которой представлена методика моделирования знаниевых компонент, основанные на

онтологическом инжиниринге, введены новые определения. В работе [15] представлена методология моделирования бизнес-процессов от детального проектирования архитектуры до реализации бизнес-логики.

В области теории управления организационными системами Бурковым В.Н. [16], рассматривается модель управления организационными системами и технология решения соответствующих задач управления. В работе «Механизмы управления: мультифункциональное учебное пособие» [17] приводятся базовые механизмы управления организационными системами, представлены примеры по проектированию комплексных механизмов управления, а также математические модели теории управления организационными системами и их приложения. Так же уделяется внимание сложности вычислений решения задач оптимального управления в моделях функционирования активных систем, исследуются эффективные методы принятия решений, приведены примеры задач управления, с применением «распараллеливания» алгоритмов решения [18]. Концептуальные и методологические основы исследований в области систем управления.

Рассмотренные выше исследования имеют большую теоретическую и практическую значимость. Но существование ряда трудов по исследуемой теме не снимает надобности в дальнейшем развивать ее теоретические и методические основы, практическое применение в определенной области. Обзор работ, изданных по теме исследования, отражает, что обсуждаются только некоторые моменты изучаемой области. Например, общепринятой, стандартизированной методики оценки эффективности и результативности функционирования СМК не существует, и не решены многие проблемы данного направления автоматизации.

Имеется система управления менеджментом качества предприятия, которая включает: объект управления (предприятие), персонал, производственные и бизнес-процессы, аудиторов и показатели результативности предприятия. СМК влияет на показатели результативности предприятия через улучшение производственных и бизнес-процессов и может входить в состав показателей в виде оцениваемых показателей результативности СМК предприятия. Процесс СМК осуществляется путем оформления персоналом документированной информации и периодической оценки выполнения обязательств персонала, принятием КД/ПД и их последующего контроля. Данный процесс является очень трудоемким и отвлекает персонал предприятия от основной работы.

Требуется: автоматизировать управление СМК предприятия и разработать систему автоматизации менеджмента качества предприятия. Для этого следует рассмотреть следующие 3 этапа процесса автоматизации:

1) Интерактивный сбор информации, позволяющий автоматизировать процесс принятия управленческих решений для следующего этапа мониторинга;

2) На основании полученной информации построение нечетко-множественных моделей интеллектуального управления бизнес-процессами, представляющих зависимость качества СМК от характеристик процессов с использованием продукционной формы их представления;

3) Непрерывный мониторинг и визуализация управляемости процессов предприятия, позволяющий обеспечить статистическую управляемость и стабильность СМК предприятия;

4) Рассмотреть возможность реализации автоматизированного управления СМК предприятия на основе интеллектуальной информационной системы.

В соответствии с постановкой задачи предлагается следующая автоматизированная система управления МК предприятия с использованием модели интеллектуального управления качеством технологических процессов производства, которая представлена на рисунке 1.

Рисунок 1 – Структурная схема автоматизированной системы управления менеджментом качества предприятия

Автоматизированная система управления менеджментом качества предприятия состоит из следующих компонентов:

- {X}(t) – значение показателей по качеству бизнес-процессов;
- Объект управления - Предприятие;
- Автоматизированная система управления менеджментом качества;
- Y(t) - параметры оценки качества;
- P(t) – оценка результативности предприятия;
- U(t) – управляющее воздействие;
- Z(t) – возмущающие воздействия, знания экспертов для получения начальных количественных метрик.

Краткое описание функционирования АСУМК:

1) Входные данные {X}(t) поступают в объект управления, доступны для просмотра лицам, принимающим решения (ЛПР);

2) Объект управления «Предприятие» имеет следующие процессы: Основные процессы, управляющие процессы, процессы измерения и улучшения, а также поддерживающие процессы. Каждый из процессов содержит показатели количественной оценки результативности менеджмента качества предприятия.

3) Здесь Z(t) является положительными возмущающим воздействием, при котором в системе предусмотрено использование моделей «Расчет оцениваемых показателей качества по оценке результативности АСУМК предприятия» для ранжирования значимых показателей процессов и расчета результативности менеджмента качества предприятия, и «Статистическая управляемость процессов

СМК предприятия» для обеспечения статистической управляемости предприятия. Количественные показатели, полученные из исходных экспертных оценок, используются для последующей обработки в расчетных моделях.

4) Y(t) – определяет параметры оценки качества. Информация о текущих значениях поступает в СУ, с помощью нечетко-множественной модели интеллектуального управления производственными процессами СУ оказывает управляющее воздействие U(t) на ОУ рекомендательного характера, на выходе P(t) – оценка результативности предприятия.

Комплексная методика оценки результативности управления менеджментом качества предприятия

Основой нечетких моделей систем автоматизированного управления выделяют нечеткие логические регуляторы (НЛР), использующиеся для создания различных АСУТП, систем управления сложными динамическими системами и т.д. В основе НЛР лежат модели нечеткой логики: модели нечеткой логической связки и правил вывода [22]. Для НЛР на основе нечеткого продукционного процессора распространена следующая схема лингвистического описания: перевод в нечеткие значения (фаззификатор), нечеткая логическая связка, композиционные правила вывода и операторы преобразования в четкие значения (дефаззификаторы). Основным этапом проектирования интеллектуального нечеткого регулятора является создание «базы знаний», используя методы представлений и поиск знаний.

Одним из перспективных направлений теории нечеткого управления и НЛР можно выделить разработку адаптивных нечетких систем. «Нечеткое адаптивное управление – это метод управления, который позволяет приспособиться к изменениям параметров путем изменения алгоритма управления» [23].

По оценке устойчивости систем, известно несколько подходов, и распространенными подходами считаются оценки устойчивости системы управления по теориям Лагранжа и Ляпунова. «Устойчивость по Ляпунову – управление считается устойчивым, если при любом возмущении со стороны окружающей среды система способна за конечное время или в пределе приблизиться как угодно близко к той траектории движения в пространстве состояний, которую она имела до начала возмущения. Оценка устойчивости социально-экономических систем по Ляпунову практически невозможна из-за трудности описания ограничений на возможные возмущения и учета всех возможных возмущений» [24]. Так как система менеджмента качества предприятия относится однозначно к классу социально-экономических систем, данный вывод полностью применим к ней. «Система менеджмента качества организации является открытой социально-экономической системой, которая формируется, развивается и проходит все стадии развития (фазы роста самой организации)».

Поскольку целью исследования является обоснование и разработка методики автоматизированной управления системой менеджмента качества предприятия в Казахстане в условиях цифровой экономики, необходимо разработать систему автоматизации управления менеджментом качества предприятия. Для этого следует обосновать модель системы управления и исследовать ее на управляемость.

В отличие от рассмотренных выше компьютерных систем по сбору и анализу данных о качестве процессов предприятия на основе проведенного исследования предлагается следующая методика автоматизированного управления системой

менеджмента качества предприятия на основе интеллектуальной автоматизированной системы, включающей три модуля (рисунок 2).

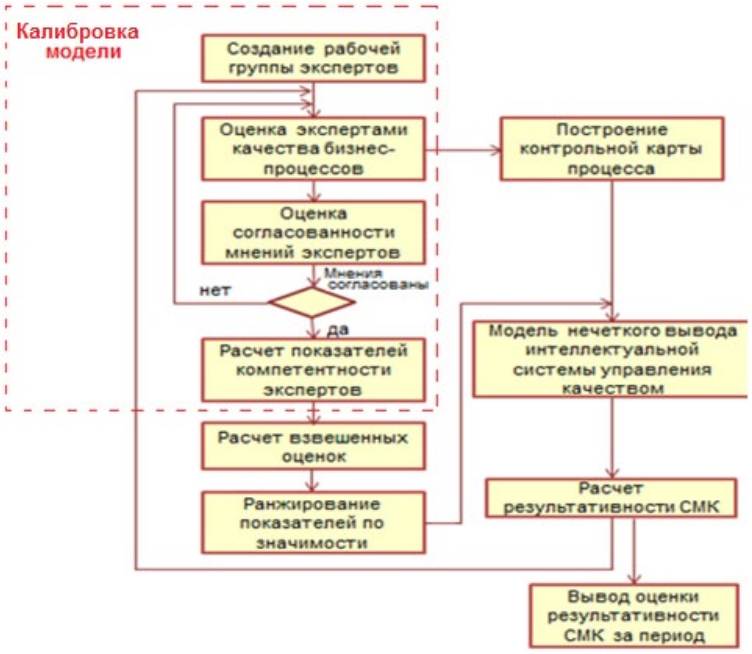


Рисунок 2 – Алгоритм автоматизированной системы управления МК

1) Расчет оцениваемых показателей количественной оценки результативности МК предприятия, позволяющий автоматизировать процесс принятия управленческих решений для следующего этапа мониторинга;

2) Мониторинг и визуализация управляемости процесса МК предприятия на основе его графического представления по отношению к его средней, нижней и верхней границам, позволяющие обеспечить статистически управляемость и стабильность предприятия;

3) На основании полученной информации строятся нечетко-множественные модели интеллектуального управления производственными процессами, представляющие зависимость качества процессов от их характеристик с использованием продукционной формы их представления.

Дальнейшее развитие отечественной автоматизированной информационной системы управления менеджментом качества предприятия по мере накопления данных предполагает также охват уровня высшего менеджмента предприятия – OLAP-системы и Data Mining системы для интеллектуального анализа данных.

Литература

1. О Концепции перехода Республики Казахстан к устойчивому развитию на 2007-2024 годы, Указом Президента Республики Казахстан от 13 апреля 2011 года № 47 // http://adilet.zan.kz/rus/docs/U060000216 20.04.2019

2. Сулейманов Н.Т. Инновационная модель всеобщего менеджмента качества (TQM), как объект интеллектуальной собственности// Уфа:ГАУ РНТИК «Баштехинформ», 2011. – С. 56-63.

3. Pupkov K.A. Intelligent Systems and Human Being// 13th International Symposium “Intelligent Systems 2018” (INTELS’18), 2019. V.150. – P. 540-543

4. Kalender Z., Vayvay Ö. The Fifth Pillar of the Balanced Scorecard: Sustainability // Procedia «Social and Behavioral Sciences», 2016, V. 235, P. 76-83

5. Tubis A., Werbińska-Wojciechowska S. Balanced Scorecard use in Passenger Transport Companies Performing at Polish Market // Procedia «Engineering», 2017, V.187, - P. 538-547.

6. Каплан Р.С., Нортон Д.П. Измерение стратегической готовности нематериальных активов // Российский журнал менеджмента, 2004. Т.2. №3. - С. 90 - 104.

7. Качалов В.А. Системы менеджмента на основе ISO 9001:2015 и ISO 14001:2015. Комментарии, рекомендации, практика внедрения// М.: ИздАТ, 2017. Т.4. - 477 с.

8. Albliwi S., Antony J., Arshed N., Ghadge A. Implementation of Lean Six Sigma in Saudi Arabian organisations: Findings from a survey// International Journal of Quality & Reliability Management, 2017. -34(4). – P. 508-529.

9. Gleesona F., Coughlanb P., Goodmana L., Newella A., Hargaden V. Improving manufacturing productivity by combining cognitive engineering and lean-six sigma methods// 52nd CIRP Conference on Manufacturing Systems (CMS), Ljubljana, Slovenia, 2019. V. 81. – P. 641-646

10. Deeb S., Haouzi H., Aubry A., Dassisti M. A generic framework to support the implementation of six sigma approach in SMEs// IFAC-PapersOnLine, 2018. V.51. - I.11, - P. 921-926

11. Моисеева А.В. Программное обеспечение системы менеджмента качества // Молодой ученый, 2017. - №10 (44). - С. 259-261.

12. Pérez-Aróstegui M., Bustinza-Sánchez F., Barrales-Molina V. Exploring the relationship between information technology competence and quality management// BRQ Business Research Quarterly, 2015. V.18, I.1, P. 4-17

13. Nakura Y., Ohashi M. The Impact of IT Technology on the QualityManagement Organization in Japan// CENTERIS 2013 - Conference on Enterprise Information Systems, 2013. V.9. - P. 209-214

14. Waldemar W., Kubekov B, Naumenko V., Narynov S, Toibaeva S., Utegenova A, A.Project - Competency based approach and the ontological model of knowledge representation of the planned learning// INTL Journal of electronics and telecommunications, 2018. V.65, № 1, - P. 45-49.

15. Barros O. Enterprise and Process Architecture Patterns// Business Process Management Journal, 2010. - 17(4). – P.598-618

16. Бурков В.Н., Коргин Н.А., Новиков Д.А. Введение в теорию управления организационными системами – М.: Либроком, 2009. – 264 с.

17. Бурков В.Н., Буркова И.В. Механизмы управления // Мультифункциональное учебное пособие. - М.: Ленанд, 2011. - 192 с.

18. Barkalov S.A., Burkov V.N., Poryadina V.L. Models of the competitive mechanism at the organization of mechanical engineering production// IOP Conf. Series: Materials Science and Engineering, 2019. 537. 042049. 10.1088/1757-899X/537/4/042049.

19. Муслимова А.К., Утепбергенов И.Т., Склярова Ю.В., Тойбаева Ш.Д. Формализация анализа функционирования и эффективности СМК для экспертной системы //Вестник КазНУ. Алматы, 2016. – №3/1 (90). – С. 87-96.

20. Жданов А.А., Караваев М.В. Применение нечеткой логики в имитационной системе автономного адаптивного управления// Труды Института Системного Программирования Российской Академии Наук – М.: ИСП РАН, 2002, Т.3. - С. 119-135.

21. Мухин В.И. Исследование систем управления: Учебник для вузов - М.: Издательство «Экзамен», 2003. - 384 с.

МАГНИТНАЯ ВОСПРИИМЧИВОСТЬ КАК ИНДИКАТОР ЗАГРЯЗНЕНИЯ СТРОИТЕЛЬНЫХ МАТЕРИАЛОВ

Атанов С.К., Искаков К.Т., Жораханов Н.Ә.
e-mail: zhorahanov@mail.ru
Евразийский национальный университет имени Л.Н. Гумилева, Казахстан

Согласно исследованиям ООН, зависимость показателей здоровья нации лишь на 8-10% определяется качеством медицинского обслуживания, на 20% — наследственными факторами, на 20%— экологической ситуацией окружающей среды и на **50%** — способом проживания то есть экологической ситуацией места проживания и места работы. Часто мы недооцениваем воздействие строительных материалов и конструкций, окружающих нас, на собственное здоровье и городской житель, по оценкам экспертов ВОЗ, до 80% своего времени проводит в помещениях. Поэтому материал стен (несущих конструкций) играет далеко не последнюю роль в обеспечении безопасности нашего здоровья [1]. Земля окутана магнитным полем и это поле являет собой часть той общей экосистемы, в которой существует человек, и вне которой его организм нормально функционировать не способен. Общеизвестный факт, что суточные изменения сердечного ритма, связанного с ним диастолического давления, а так же уровень лейкоцитов в крови прямо зависят от магнитных колебаний земного поля. Например, в дни, когда происходят так называемые магнитные бури, количество лиц, страдающих разнообразнейшими сердечно-сосудистыми проблемами, резко возрастает, а длительное пребывание в среде, где фиксируется высокое магнитное поле, повышает риск тромбообразования. Справедливо и обратное – при длительном нахождении в условиях низкого магнитного поля существенно снижается концентрация лейкоцитов, нарушается сердечный ритм, что вызывает за собой целый ряд других, отсроченных во времени последствий [2]. Пребывая, например, на 10-м этаже дома, мы оказываемся в ситуации, где низкочастотное магнитное поле Земли настолько мало, что может вызывать**"синдром дефицита магнитного поля человека".** Если блочная квартира на 10 этаже, уменьшено магнитное поле Земли примерно в 10 раз (0,18 э разделить на 10). Перенося это на современные реалии, можно смело утверждать, что жители многоэтажек, особенно обитатели верхних этажей, постоянно недополучают такого необходимого магнитного облучения.

В последнее время чётко проявляется тенденция к химизации технологических процессов в строительстве. В качестве добавок к строительным материалам, будь то бетон, керамический кирпич, железобетон, керамика и пр., применяют отходы металлургической и химической промышленности. Безусловно, это удешевляет

процесс их изготовления. Однако экономия на качестве и экологичности (безопасности) приводит к экономии на здоровье будущих жильцов. Но главным компонентом всех строительных материалов является песок и исследования магнитных его свойств посвящено данное исследование.

Цель работы — обобщить данные о магнитной восприимчивости основного компонента строительных материалов - карьерного песка и установить ее связь со степенью загрязнения тяжелыми металлами и его влиянием на **"синдром дефицита магнитного поля человека"**

Как известно [Kozhevnikov, Nikiforov, 1995; Кожевников, Никифоров, 1999], кирпичи и другие изделия из обожженной глины демонстрируют проявления магнитной вязкости вследствие магнитной восприимчивости основного компонента - минеральных компонентов. Исследуем влияние компонентов строительных материалом, и в частности песка с карьеров Акмолинской области на магнитную восприимчивость конечного изделия.

Карьерный песок — природный материал, который используется во многих сферах народного хозяйства и промышленности. Этот сыпучий материал добывается карьерным способом, как понятно из его названия. Песок в Астане поставляется с разных карьеров, которые соответственно предоставляют разные виды песка с разной структурой, зернистостью и составом (рисунок 1). На конечные свойства, которыми будет обладать карьерный песок, также влияют способы его добычи: промывание, просеивание и открытый способ добычи.

Рисунок 1 - Добыча песка карьерным способом

Внешнее магнитное поле, характеризуемое напряженностью H, действуя на магнитные атомные системы, индуцирует (наводит) в них магнитные моменты и ориентирует существующие магнитные моменты в направлении поля. В результате такого воздействия возникает собственное магнитное поле внутри вещества, т. е. вещество намагничивается. Степень намагничивания характеризуется вектором намагниченности J, который равен суммарному магнитному моменту единицы объема вещества:

$$\vec{J} = \frac{\sum_{\Delta V} \vec{P}_{ai}}{\wedge V},$$

где $\mathbf{P_{ai}}$ - наведенные и ориентированные магнитные моменты атомов; $\mathbf{\Delta V}$ — элементарный объем вещества, в пределах которого поле можно считать однородным. Между вектором намагниченности и вектором напряженности магнитного поля существует прямая связь:

$$\vec{J} = \chi \vec{H},$$

где χ — магнитная восприимчивость вещества, численно равная намагниченности при единичной напряженности внешнего поля.

Для измерения магнитной восприимчивости χ (каппа) наибольшее распространение получил индукционный способ, основанный на том, что при внесении магнитной среды или образца в рабочую область датчика (катушек, питаемых переменным током) изменяется поток магнитной индукции.

Каппаметрия - непосредственное измерение магнитной восприимчивости (χ) в полевых условиях является неотъемлемым элементом магниторазведочных исследований. Измерения подобного рода дают важнейшую априорную информацию о магнитных свойствах изучаемых объектов, что позволяет, например, решать прямую задачу (т.е. оценивать ожидаемые амплитуды магнитных аномалий от этих объектов). Как было сказано выше, распределение магнитной восприимчивости по вертикали позволяет изучить структуру почвенного покрова, выделить отдельные генетические горизонты, особенно те, которые характеризуются повышенными значениями магнитной восприимчивости.

Для экспериментального определения магнитной восприимчивости используется прибор каппаметр модели ПИВМ-32. Данный прибор предназначен для измерения магнитной восприимчивости в скважинах, а также возможно измерить восприимчивость образцов в лабораторных условиях.

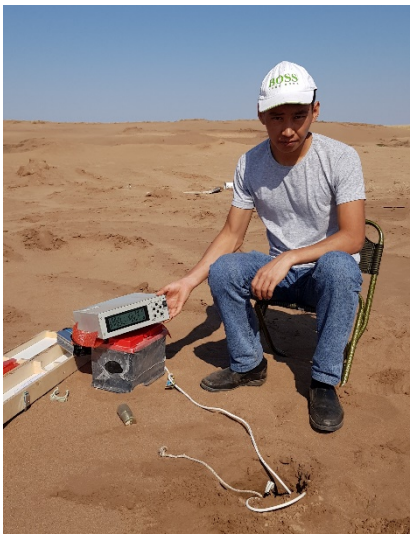
Портативный измеритель магнитной восприимчивости (каппаметр) ПИМВ-32 относится к современным приборам, в основе работы которых лежит принцип действия дифференциального магнитного моста. Данный прибор предназначен для измерения магнитной восприимчивости горных пород в полевых условиях на обнажениях, образцах, кернах буровых скважин. Также ПИМВ-32 используется при проведении геологического картирования, петромагнитных исследований и решает задачу дифференциации горных пород и руд по значению магнитной восприимчивости в диапазоне от -1 до 1 ед. СИ с чувствительностью до 1×10^{-5}ед. СИ.

Для повышения точности была предпринята попытка увеличить количество измерений, чтобы набором статистики уменьшить случайную составляющую погрешности измерений. Однако выяснилось, при многократных измерениях одного образца (больше 10) значения магнитной восприимчивости монотонно возрастают, что связано с остаточной намагниченностью.

Были проведены экспериментальные исследования в песчаном карьере, находящейся за пределами города Астаны, находящийся в 76 км северо-западном направлении. Исследована магнитная восприимчивость карьерного песка,

расположенных на объектах. С этой целью были вырыты серия скважин глубиной порядка 3 метров, показанная на рисунке 3а. На рисунке 3б представлен прибор в полной комплектации: зонд; регистратор; инвертор (12 вольт – 220 вольт); аккумулятор (12 вольт).

а) подготовка скважины



б) подготовка прибора к измерению

Рисунок 3– Подготовительные работы для проведения эксперимента

На рисунке 4 показаны этапы работы. Далее было произведено измерение коэффициента восприимчивости и запись результатов на ПК

а) измерение коэффициента восприимчивости

б) запись результатов на ПК

Рисунок 4 – Измерение коэффициентов восприимчивости

Прибор выдает истинное значение магнитной восприимчивости в виде частоты от 0 до 3000 Гц, что соответствует магнитной восприимчивости 0 … 3000 * 10^{-4}ед.СИ. Результаты измерения параметров магнитной восприимчивости и магнитной вязкости образцов многочастотным методом каппаметром приведены в таблице 1.

Таблица 1 – Результаты измерения магнитной восприимчивости образцов

№	kf1,10^{-5} СИ	kf2,10^{-5} СИ	kf3,10^{-5} СИ	FD(f1-f2), %	FD(f2-f3), %	FD(f1-f3), %

1	1625.9	1511.9	1378.2	7	8.8	15.2
2	416.18	397.18	377.08	4.6	5.1	9.4
3	524.97	504.24	484.12	3.9	4	7.8
4	380.23	366.53	354	3.6	3.4	6.9
5	386.91	370.97	355.28	4.1	4.2	8.2

Запись данных проводится в течение нескольких часов. Поскольку все измерения проходят на фоне псевдослучайных помех, обусловленных как явлениями в ионосфере, так и процессами, проходящими на поверхности и в земной коре, среднее квадратическое отклонение разности показаний магнитометров будет зависеть от временного сдвига моментов включения приборов и спектральной плотности возмущений геомагнитного поля.

Важно отметить, что параметр каппа является устойчивым во времени, не зависит от внешних условий (температуры, влажности, магнитных вариаций и т.п.). Достоинствами каппаметрии как метода являются: экспрессность, оперативность и большая дидактичность информации, опирающейся на результаты прямой фиксации параметра χ.

Измерения магнитной восприимчивости проводились в соответствии с инструкцией, методическими рекомендациями и по следующей методике - исследуемый образец помещался на датчик прибора в фиксированном положении, проводилось измерение в трехкратных повторениях для каждой пробы. Объем пробы и степень уплотнения материала во всех случаях были одинаковыми. После каждого замера пробы измерялся эталон в том же диапазоне. Результаты измерений выдавались в системе единиц СИ.

Для оценки целесообразности и эффективности исследования первоначально была проведена серия экспериментов на разных глубинах погружения зонда до 3 метров (таблица 3). Из представленных результатов видно, что магнитный профиль может быть важной характеристикой магнитных свойств песка. Как видно из рисунка 2, магнитная восприимчивость с поверхности до глубин 20 см меняется в пределах от 5x10"5 до 80x10"5 ед.Си, затем в диапазоне от 40 до 50 см она резко уменьшается в два раза, а далее меняется в небольших пределах от 5x10 5 до 25x10 5 ед.Си. Можно предположить, что граница резкой смены % отвечает переходному уровню (В), который отделяет соответственно почвенный слой песка (А) от материнской породы (С). Для других типов почв, например, суглинка, такой резкой границы не наблюдается, что возможно определяется меньшей степенью изменения материнской породы в процессе почвообразования.

Таблица 3 Данные измерения песчаном карьере

Глубина см	50	100	150	200	250	300	350	400	450	500
точка 1	60,359	58,133	58,489	56,712	60,544	58,947	59,266	57,972	62,867	58,346
Точка 2	63,306	60,691	56,865	61,655	58,508	63,793	59,871	60,637	61,134	63,547
Точка 3	62,988	58,287	60,537	57,394	63,432	56,684	60,633	57,861	61,423	61,452
Точка 4	59,153	57,027	61,186	56,988	57,697	60,813	61,718	59,593	56,768	56,834
Точка 5	58,865	59,637	57,682	62,108	58,318	56,715	61,719	60,344	60,648	56,692

Точка 6	57,324	61,670	60,665	57,842	58,319	60,461	63,009	63,543	63,805	59,733

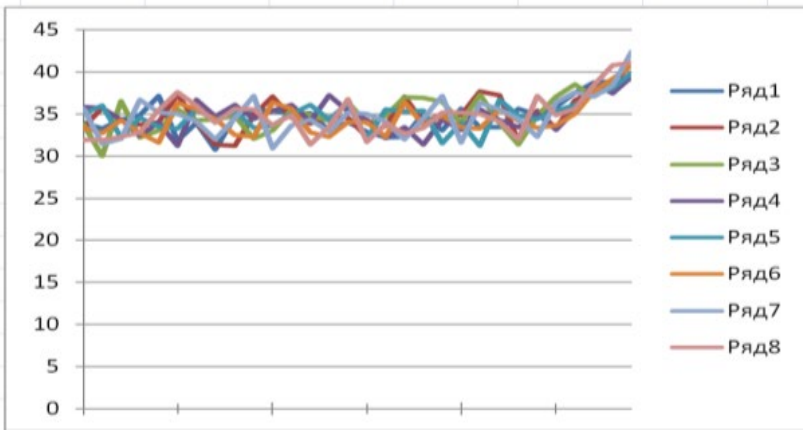


Рисунок 2 - Измерения магнитной восприимчивости карьерного песка от глубины залегания

Магнитная восприимчивость почв зависят от состава, размера зерна магнитных минералов и их источников, а также от методов их измерения. Измерения, проведенные в слабом переменном магнитном поле являются наиболее надежными [3].

Анализ данных показывает тенденцию роста магнитной восприимчивости, а значит и содержания тяжелых металлов в грунте по мере приближения к поверхности земли. В связи с этим все последующие измерения были проведены на глубине до 3 метров с использованием логарифмической шкалы по глубине с учащением измерения по мере приближения к поверхности земли.

При проведении численных расчетов берут грубое значение магнитной проводимости равное единице. С использованием этого прибора, имея измеренное значение коэффициента восприимчивости, можно принимать при расчетах точное значение магнитной проницаемости, причем вычисленных по слоям. В нашем случае для объекта «Песок карьерный», получены следующие данные: $\kappa_{песок} = 59{,}6 * 10^{-5}$.

Ниже в таблице 4 приведены среднее значение магнитной восприимчивости образцов строительных материалов, полученные лабораторных условия ЕНУ им. Л.Н. Гумилева и в полевых условиях.

Таблица 4 - Среднее значение магнитной восприимчивости образцов строительных материалов

Строительный материал	Температура, град Цельсия	Число измерений	Время измере-ния мин	χ * 10-5 ед. СИ
Песок	18-23	6	50-500	59,6
Цемент	18-23	6	50-500	89,3
Кирпич	18-23	6	50-500	61,2
Пескоблок	18-23	6	50-500	79,6
Газобетон	18-23	6	50-500	159,6

Заключение

Анализ полученных данных выявил закономерности, следующие из технологических особенностей производства. Так наибольшее значение магнитной

восприимчивости, а значит и наихудшие, несмотря на легкий вес и прочие преимущества проявил строительный газобетон. Это вполне объяснимо, так как при его производстве используется газообразователь - алюминиевая пудра. Из рассмотренных видов выгодно отличается материал - кирпич. И хотя он также содержит цемент - материал в относительно высокой магнитной восприимчивостью, но в ходе длительного и высокотемпературного обжига происходит частичное разрушение магнитных доменных структур цемента.

Таким образом, для строительных изделия типа "кирпич" влияние значение магнитной восприимчивости карьерного песка на общее значение магнитной восприимчивости незначительно. Это позволяет его рекомендовать как наиболее оптимальный строительный материал с точки зрения **"синдрома дефицита магнитного поля человека"** и можно использовать практически со всех карьеров Акмолинской области.

Литература

1. https://www.newsko.ru/articles/nk-528187.html
2. https://altay.land/article/5040/
3. *Magiera T., Goluchowska B., Jablonska M.* Technoge nic magnetic particles in alkaline dusts from power and cement plants // Water Air Soil Pollut. 2013. Vol. 224. P. 1389—1406.
4. *Meena N.K., Maitib S., Shrivastava A.* Discrimination between anthropogenic (pollution) and lithogenic magnetic fraction in urban soils (Delhi, India) using envirionmental mag netism // J. Appl. Geophis. 2011. Vol. 73. P. 121—129.

РАЗРАБОТКА ПРОГРАММНОГО МОДУЛЯ «AUTOMATED SYSTEM FOR VERIFICATION AND CHANGE OF PARAMETERS OF THE WRF MODEL – ASVC WRF 1.0» ДЛЯ РЕГИОНАЛЬНОЙ КЛИМАТИЧЕСКОЙ МОДЕЛИ WRF

Бостанбеков К.А.[1], Алимова А.Н.[1], Джамалов Д.К.[1], Юничева Н.Р.[2]
[1]*Казахский национальный исследовательский технический университет имени К.И.Сатпаева, Казахстан*
[2]*Институт информационных и вычислительных технологий, Казахстан*

Аннотация *В данной работе представлен программный модуль для автоматического скачивания и проверки целостности данных, запуска модулей препроцессинговой обработки и обеспечения непрерывной работы модели, а также внесение изменений во входные параметры модели. Описаны основные функциональные возможности. Расписан алгоритм работы программы. Подробно описана работа разработанной программы.*

Численное моделирование климатической системы с помощью региональных климатических моделей является главной методологической основой для решения задачи прогнозных оценок будущих параметров климата. Региональная климатическая модель WRF (Weather Research and Forecasting) это система для

прогнозирования погоды и моделирования атмосферных процессов, пригодная как для оперативных, так и для исследовательских целей. Система является эффективным инструментом для разработки методов ассимиляции данных, параметризации процессов подсеточного масштаба, прогноза погоды и моделирования регионального климата [1-3]. Модель WRF представляет собой систему взаимодействующих модулей: модуль, обеспечивающий подготовку начальных и граничных данных (WRF Preprocessing System); вычислительный модуль – решающее ядро (Advanced Research WRF); модуль обработки результатов вычислений (WRF Postprocessing System).

Для автоматического скачивания и проверки целостности данных ERA-Interim [4], запуска модулей препроцессинговой обработки и обеспечения непрерывной работы модели WRF, а также внесение изменений во входные параметры модели была разработана программа «Automated system for verification and change of parameters of the WRF model – ASVC WRF 1.0»**.**

Функциональные возможности: программный модуль производит автоматическое скачивание метеорологических данных (архив ERAInterim) для использования в качестве начальных и граничных условий в модели WRF. Данный модуль загружает с сайта ECMWF (Европейского центра среднесрочных прогнозов погоды) метеорологические данные реанализа (повторного анализа) атмосферной модели, которые интерполированы на изобарические поверхности, а также приземные и наземные данные.

Также имеется возможность проведения валидации скачанных метеорологических данных архива ERAInterim. Проверка данных осуществляется в 2 этапа. На первом этапе все файлы данных проверяются по фиксированному объему, параллельно происходит классификация файлов. На втором этапе для каждого класса файлов определяется список отсутствующих дат. Результатом проверки являются txt-файлы со списком недостающих файлов данных. В модуле автоматической загрузки реализована функция, которая считывает информацию с файлов проверки и автоматически скачивает недостающие данные.

Автоматически запускать модули препроцессинговой обработки (ungrib.exe и metgrid.exe). Перед запуском динамического блока климатической модели требуется подготовить исходные данные в требуемые форматы. Для этого используются программы ungrib.exe и metgrid.exe. Программа ungrib.exe предназначена для распаковки метеорологических данных, скачанных с архива ERAInterim, в бинарном формате grib. Программа metgrid.exe объединяет геофизические данные местности и метеорологические данные в один файл и проводит горизонтальную интерполяцию до указанного разрешения. Данная программа автоматизирует запуск данных препроцессинговых программ для набора скачанных метеорологических данных и формирует набор входных данных для климатической модели WRF.Обеспечивает непрерывную работу модели WRF (real.exe и wrf.exe).

Учитывая большой объем входных и выходных данных, а также возникновение счетной нестабильности, вызванной ошибками округления при проведении длительных модельных расчетов, был разработан специальный программный модуль, позволяющий контролировать ход выполнения численных экспериментов. Модуль разбивает эксперимент на моделируемые интервалы равные 1 месяцу (один шаг). На каждом шаге осуществляющий рестрарт модели, загружаются начальные и граничные данные. Данная программа запускает расчет на каждый месяц по всем годам начиная с указанной даты ${startdate} до ${enddate}.

Сначала запускается программа real.exe, предназначенная для вертикальной интерполяции входных метеорологических данных и формирование шаблона выходного файла. После того как real.exe завершилась, она возвращает код "SUCCESS COMPLETE REAL_EM INIT", что означает успешность выполнения программы и следом запускается основной модуль, программа wrf.exe.

В качестве граничных и начальных условий для региональной климатической модели применялись данные реанализа (повторного анализа) Era-Interim Европейского центра среднесрочных прогнозов погоды.

Описание общего алгоритма работы программы (ASVC WRF**)**

Программа ASVC WRF дает возможность автоматической закачки и верификации данных реанализа (повторного анализа) Era-Interim Европейского центра среднесрочных прогнозов погоды. Запускать модули препроцессинговой обработки. Разбивать эксперимент на моделируемые интервалы, вносить изменений во входные параметры модели и контролировать ход выполнения численных экспериментов.

Общий алгоритм решения задачи представлен на рисунке 1.

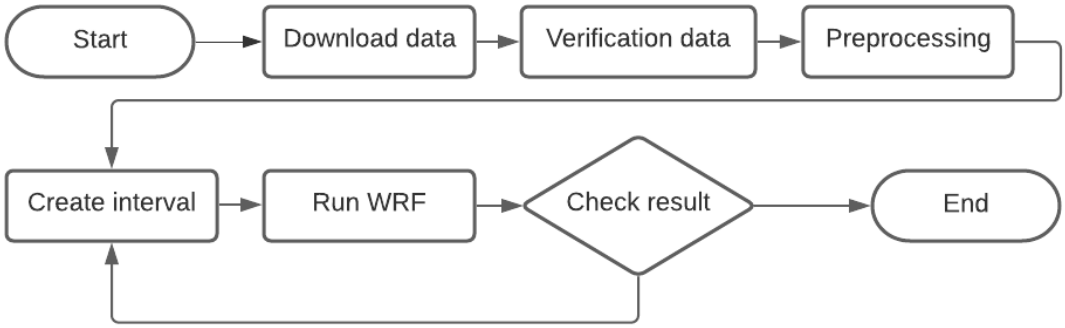


Рисунок 1 – Общая блок схема алгоритма

Описание программы «ASVC WRF 1.0» для ЭВМ

При первом запуске программу «ASVC WRF» можно запустить с помощью скрипта “start.sh”, набрав в терминале команду “sh start.sh *03 2010*”, где 03 – месяц, 2010 – год. Данный скрипт устанавливает все необходимые программы, скачивает данные и запускает расчет на указанный месяц и год.

Программу «ASVC WRF» можно запускать поэтапно, в следующей последовательности:

1. Программа «ASVC WRF» требует предварительной установки модели WRF. Для установки WRF необходимо запустить скрипт “installer.sh”. Скрипт автоматический скачивает все необходимые для работы зависимые библиотеки и компилирует программу WRF. Для запуска установщика наберите в терминале команду *“sh installer.sh”*.

2. После установки программы следующим шагом является скачивание метеорологических параметров для начальных и граничных условий климатической модели WRF. Для этого необходимо запустить скрипт “downloader.sh”. Данный скрипт скачивает метеоданные и проверяет целостность и полноту скаченных файлов. Для запуска требуется набрать команду “*csh downloader.sh 03 2010*”, где 03 – месяц, 2010 – год.

3. Чтобы модель WRF могла работать со скаченными файлами нужно провести предобработку данных с помощью программы WPS (WRF Preprocessing System). Автоматический запуск предобработки реализован в скрипте preprocessing.sh и запускается с терминала командой "*sh preprocessing.sh 03 2010*", где 03 – месяц, 2010 – год.

4. Запуск расчета осуществляется непосредственно из каталога эксперимента командой "*sh run_cordex.sh 03 2010*", где 03 – месяц, 2010 – год. При запуске на экране терминала Linux выводится информация о ходе эксперимента.

Все команды выполнять в терминале с каталога, где расположены данные скрипты. Завершение работы программы происходит при закрытии консоли Linux, либо по завершению программы.

Данная работа выполнена при поддержке грантового финансирования научных проектов КН МОН РК №AP05135848 «Моделирование будущего климата Центральной Азии в рамках международного проекта CORDEX (COordinated Regional climate Downscaling EXperiment)»

Литература

1 Skamarock W.C., Klemp J.B., Dudhia J., Gill D.O., Barker D.M., Wang W., and Powers J.G. A Description of the Advanced Research WRF Version 2 // https://arrc.ou.edu/~rockee/NRA_2007_website/WRF-weather-model-arw_v2.pdf: 30.01.2007.

2 Michalakes J., Dudhia J., Gill D., Henderson T., Klemp J., Skamarock W., and Wang W. The Weather Research and Forecast Model: Software Architecture and Performance // Use of High Performance Computing in Meteorology. – 2005. – PP.156–168.

3 Takle, E.S., et al. Project to Intercompare Regional Climate Simulations (PIRCS): Description and initial results // Journal of Geophysical Research, 1999. – V.104, N.D16. – pp.19443–19461.

4 ERA-Interim. https://www.ecmwf.int/en/forecasts/datasets/reanalysis-datasets/era-interim (20.10.2018).

КОМПЬЮТЕРНОЕ МОДЕЛИРОВАНИЕ ЧИСЛЕННО-АНАЛИТИЧЕСКОГО РЕШЕНИЯ ДИНАМИЧЕСКОЙ ЗАДАЧИ ПОРОУПРУГОСТИ.

А.С.Бердышев[12], Д. Н. Блиева[13], А.Асхатулы[13],
[1]*Институт информационных и вычислительных технологий КН МОН РК,*
[2]*Казахский национальный педагогический университет имени Абая,*
[3]*Казахский национальный университет им. Аль-Фараби*

Аннотация: *В данной работе вычисляется точное решение начально - краевой задачи пороупругости. Обратные преобразования Фурье и Лапласа были применены с использованием параллельных и последовательных вычислений для получения двумерного решения, зависящего также от времени. Визуализация*

примеров динамических решений представлена для нескольких фиксированных значений времени, которые подтверждают выполнение граничных условий.

***Ключевые слова**: пористые среды, преобразования Фурье-Лапласа, теория пороупругости, акустические волны.*

Компьютерное и математическое моделирование нестационарных физических процессов, протекающих в пористых средах, насыщенных жидкостью, играет важную роль в изучении течений жидкости в пористых структурах.

Это особенно важно в связи со сложностью как экспериментального, так и теоретического изучения внутренней структуры пористой среды. В то время как широкое применение компьютерного моделирования, основанного на реалистичных математических моделях, стимулирует дальнейшие исследования в этом направлении. Последние достижения в области такого математического моделирования и моделирования помогают развивать многие другие области исследований, включая науки о земле и материаловедение, механику, биотехнологию и медицину, теорию энергии и теорию фильтрации. Теории типа Био [Biot, 1956, 1962] часто используются для изучения динамических процессов в пористых средах. Однако существует относительно небольшое количество опубликованных исследований, в которых бы корректно сравнивались теоретические результаты, полученные на основе теории Био, с экспериментальными результатами, основанными на природных примерах. В своей работе [] Доровский приводит сравнение разработанной им модели, основанной на континуальной теории фильтрации с моделью Био-Френкеля. В обеих моделях учитывается три типа волн, распространяющихся в пористой среде: две продольные и одна поперечная. Но в отличие от модели Био, в модели Доровского пористая среда описывается с помощью трех упругих модулей вместо четырех.

Обратимся к математической постановке модели для двумерной динамической задачи. Управляющие уравнения основаны на законах сохранения импульса и Гука и согласуются с условиями термодинамики. Рассмотрим полуплоскость, заполненную пористой средой, насыщенной жидкостью, каждая из которых характеризуется соответствующими параметрами. Таким образом, распространение сейсмических волн в этих средах при отсутствии потерь энергии описывается следующей начально-краевой задачей в терминах скорости насыщающей жидкости, скоростей твердой матрицы, давления жидкости и тензора напряжений. Итак, рассматриваемая задача формулируется следующим образом:

Закон сохранения импульса для упругой среды:

$$\frac{\partial u_j}{\partial t}+\frac{1}{\rho_{0,s}}\left(\frac{\partial \sigma_{j1}}{\partial x_1}+\frac{\partial \sigma_{j2}}{\partial x_2}\right)+\frac{1}{\rho_0}\frac{\partial p}{\partial x_j}=F_j, \tag{1}$$

Закон сохранения импульса для жидкости:

$$\frac{\partial v_j}{\partial t}+\frac{1}{\rho_0}\frac{\partial p}{\partial x_j}=F_j, \tag{2}$$

Закон Гука для твердой матрицы (упругой среды):

$$\frac{\partial \sigma_{jk}}{\partial t} + \mu(\frac{\partial u_k}{\partial x_j} + \frac{\partial u_j}{\partial x_k}) + (\frac{\rho_{0l}}{\rho_0} K - \frac{2}{3}\mu)\delta_{jk} div\vec{u} - \\ -\frac{\rho_{0,s}}{\rho_0} K\delta_{jk} div\vec{v} = 0, \tag{3}$$

Закон Гука для жидкости :

$$\frac{\partial p}{\partial t} - (K - \alpha\rho_0\rho_{0,s}) div\vec{u} + \alpha\rho_0\rho_{0,l} div\vec{v} = 0, \tag{4}$$

Начальные условия :

$$u_j\Big|_{t=0} = v_j\Big|_{t=0} = \sigma_{jk}\Big|_{t=0} = p\Big|_{t=o} = 0, \tag{5}$$

Граничные условия на свободной поверхности в плоскости $x_2 = 0$

$$\sigma_{22} + p\Big|_{x_2=0} = \sigma_{12}\Big|_{x_2=0} = \frac{\rho_{0,l}}{\rho_0} p\Bigg|_{x_2=0} = 0, \tag{6}$$

Для двумерного случая $j = 1,2;\ k = 1,2$ и система (1)-(4) состоит из восьми уравнений в частных производных с восемью начальными условиями (5) при $t = 0$ и тремя граничными условиями (6) при $x_2 = 0$, где $\vec{u} = (u_1, u_2)^T$ и $\vec{v} = (v_1, v_2)^T$ - векторы скоростей упругой пористой среды и жидкости со следующими физическими параметрами:

$\rho_{0,s}$ - парциальная плотность упругой пористой среды;

$\rho_{0,s}$ - парциальная плотность насыщающей жидкости,

$\rho_0 = \rho_{0,s} + \rho_{0,l}$,

$\rho_{0,s} = \rho_{0,s}^f (1 - d_0)$,

где $\rho_{0,s}^f$ и $\rho_{0,l}^f$-соответственно физические плотности пористой среды и жидкости.,

d_0 - пористость

и p - поровое давление,

σ_{jk} - компоненты тензора напряжений,

δ_{jk} это символ Кронекера.

Причем, $K = \lambda + \frac{2}{3}\mu,$ где $\lambda > 0$ и $\mu > 0$ - коэффициенты Ламе $\alpha = \rho_0\alpha_3 + \frac{K}{\rho_0^2}$, $\rho_0^3\alpha_3 > 0$, - объемный модуль сжатия жидкой составляющей гетерофазной среды.

Упругие модули $K > 0$, $\mu > 0$ и $\alpha_3 > 0$ выражаются в терминах скорости распространения поперечных волн и двух скоростей продольных волн следующим образом:

$$\mu = \rho_{0,s} c_s^2,$$

$$K = \frac{\rho_0}{2}\frac{\rho_{0,s}}{\rho_{0,l}}\left(c_{p_1}^2 + c_{p_2}^2 - \frac{8}{3}\frac{\rho_{0,l}}{\rho_0} c_s^2 - \right.$$

$$\left. -\sqrt{(c_{p_1}^2 - c_{p_2}^2)^2 - \frac{64}{9}\frac{\rho_{0,l}\rho_{0,s}}{\rho_0^2} c_s^4} \right),$$

$$\alpha_3 = \frac{1}{2\rho_0^2}\left(c_{p_1}^2 + c_{p_2}^2 - \frac{8}{3}\frac{\rho_{0,s}}{\rho_0} c_s^2 - \right.$$

$$\left. -\sqrt{(c_{p_1}^2 - c_{p_2}^2)^2 - \frac{64}{9}\frac{\rho_{0,l}\rho_{0,s}}{\rho_0^2} c_s^4} \right).$$

Прямые преобразования Лапласа-Фурье по временной переменной t и пространственной переменной x_1 используются в качестве инструмента для преобразования исходной сложной двумерной граничной задачи для гиперболической системы дифференциальных уравнений в частных производных (1) - (6) в более простую граничную задачу системы обыкновенных дифференциальных уравнений относительно одной пространственной переменной x_2. Задача сводится к системе из шести дифференциальных уравнений относительно переменной x_2, которые могут быть представлены в нормальном виде следующим образом:

$$\hat{w}' = B_1 \hat{w} + B_2, \tag{7}$$

Где $\hat{w} = \hat{w}(\hat{u}_1, \hat{u}_2, \hat{v}_2, \hat{\sigma}_{12}, \hat{\sigma}_{22}, \hat{p})^T$.

Решение системы (7) в виде шести функций находится с помощью спектрального метода. Две оставшиеся функции решения выражаются в терминах нацденных шести решений следующим образом:

$$\hat{v}_1 = -\frac{1}{s\rho_0} i k_1 \hat{p} + \frac{\hat{F}_1}{s} \tag{8}$$

$$\hat{\sigma}_{11} = -\frac{1}{ik_1}\frac{\partial \hat{\sigma}_{12}}{\partial x_2} - \frac{\rho_{0,s}}{\rho_0}\hat{p} - \frac{s\rho_{0,s}}{ik_1}\hat{u}_1 + \frac{\rho_{0,s}}{ik_1}\hat{F}_1 \tag{9}$$

Спектр матрицы B_1 в системе (7) вычисляется с помощью программного обеспечения MATLAB и состоит из трех пар взаимно противоположных собственных значений следующим образом:

$$Sp(B_1)=\begin{pmatrix}\tau_1\\ \tau_2\\ \tau_3\\ \tau_4\\ \tau_5\\ \tau_6\end{pmatrix}=\begin{pmatrix}\tau_1\\ \tau_2\\ \tau_3\\ -\tau_1\\ -\tau_2\\ -\tau_3\end{pmatrix}$$

Компоненты спектра $Sp(B_1)$ вычисляются в символьной форме и зависят от физических значений упругих модулей K, α, μ, а также параметров ρ_0, $\rho_{0,l}$, $\rho_{0,s}$, характеризующих пористую среду. Причем данные параметры вычисляются с использованием физических входных параметров пористого материала, насыщающей жидкости $\rho^f_{0,s}$, $\rho^f_{0,l}$, d_0 и двух скоростей сейсмических продольных волн c_{p1}, c_{p2} и одной поперечной c_s, распространяющихся в пористой среде. Благодаря вычислительным экспериментам удалось установить существование таких значений параметров, при которых все шесть собственных значений τ_k, $k=1,...,6$ спектра $Sp(B_1)$ являются различными между собой значениями, что является важным фактом для возможности представления решения в явном виде. А матрица собственных векторов обозначается как $P=(z_1\,|\,z_2\,|\,z_3\,|\,z_4\,|\,z_5\,|\,z_6)\in M_{6\times 6}(\square)$ такая, что выполняется равенство $B_1 z_k=\tau_k z_k$, $k=1,\ldots,6$. Выражения элементов матрицы собственных векторов являются слишком длинными алгебраическими выражениями, и соответствующий код вычисления MATLAB включен в программный комплекс для решения этой динамической задачи.

Можно показать, что аналитическое решение может быть выражено в следующем виде:

$$\begin{aligned}
w_m(t,x_1,x_2)=&\int_0^\infty\int_{-\infty}^\infty\Big\{-\sum_{k=1}^{3}z_{mk}\mathrm{e}^{\tau_k x_2}\Big[\big(\mathrm{i}\,p_{k3}d_3+p_{k4}d_4\big)\times\\
&\times\int_{x_2}^\infty \mathrm{e}^{-\tau_k l}\hat{F}_1(l)dl+p_{k6}\rho_0\int_{x_2}^\infty \mathrm{e}^{-\tau_k l}\hat{F}_2(l)dl\Big]+\\
&+\sum_{k=4}^{6}z_{mk}\mathrm{e}^{-\tau_{k-3}x_2}\Big[-\sum_{j,q=1}^{3}p_{kj}r_{jq}\Big(\big(\mathrm{i}\,p_{q3}d_3+p_{q4}d_4\big)\times\\
&\times\int_0^\infty \mathrm{e}^{-\tau_q l}\hat{F}_1(l)dl+p_{q6}\rho_0\int_0^\infty \mathrm{e}^{-\tau_q l}\hat{F}_2(l)dl\Big)+\\
&+\big(\mathrm{i}\,p_{k3}d_3+p_{k4}d_4\big)\int_0^{x_2}\mathrm{e}^{\tau_{k-3}l}\hat{F}_1(l)dl+\\
&+p_{k6}\rho_0\int_0^{x_2}\mathrm{e}^{\tau_{k-3}l}\hat{F}_2(l)dl\Big]\Big\}dk_1\,ds,
\end{aligned}\tag{11}$$

где $m = 1,\ldots,6$

Обозначим I_k следующий Интеграл:

$$I_k = \int_0^\infty \mathrm{e}^{-\tau_k l} \hat{F}_1(l) dl \,, \qquad (12)$$

который мы можем сначала решить аналитически для определенного вида функции, чтобы сэкономить много вычислительных ресурсов для вычисления (11).

Для вычисления решений (11) возьмем следующие значения входных параметров и форму функции внешней силы, удовлетворяющую условиям разрешимости задачи:

$\rho_{0,s}^f$	1400.0	Kg / m^3
$\rho_{0,l}^f$	997.0	Kg / m^3
c_{p_1}	2000.0	m / s
c_{p_2}	1300.0	m / s
c_s	1300.0	m / s
d_0	0.3	

$$F(t, x_1, x_2) = \mathrm{e}^{-t^2 - x_1^2 - x_2^2}, (t, x_1, x_2) \in [0, \infty) \times \square \times [0, \infty). \quad (13)$$

Сначала мы применяем преобразование Лапласа-Фурье к функции $F(t, x_1, x_2)$ в (13). Далее подставляем полученное выражение в интеграл I_k в (12) для дальнейшей аппроксимации двойных интегралов в функциях решений (11). Мы можем аналитически решить полученный интеграл, что позволит значительно сэкономить на вычислительных ресурсах следующим образом:

$$\int_0^\infty \mathrm{e}^{-\tau_q l} \hat{F}_1(l) dl = \frac{\pi}{2} erfc(\frac{s}{2}) e^{\frac{s^2}{4} - \frac{k_1^2}{4}} \int_0^\infty e^{-\tau_k l} e^{-l^2} dl =$$

$$= \frac{\pi^{3/2}}{4} erfc(\frac{s}{2}) erfc(\frac{\tau_k}{2}),$$

где $erfc$ является функцией комплиментарной ошибки.

Визуализация полученных решений выполняется в виде 3-мерной анимации на PyPlot. При этом для целей настоящей работы в качестве примера приведены графики функций решений в различные фиксированные моменты времени при различном количестве интервалов по временной и пространственным переменным. В частности, для случаев $t = 1$ при $n = 32$ и $t = 53$ при $n = 64$ графики выглядят следующим образом:

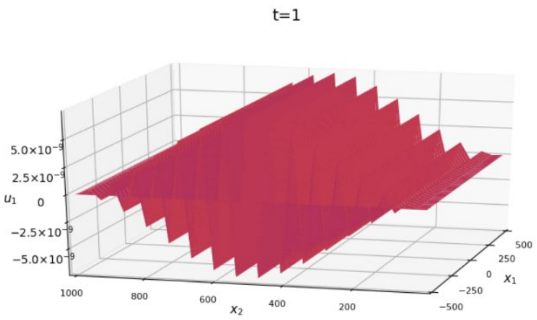


Рисунок 1. График функции решения $u_1(t, x_1, x_2)$ при $t = 1c$

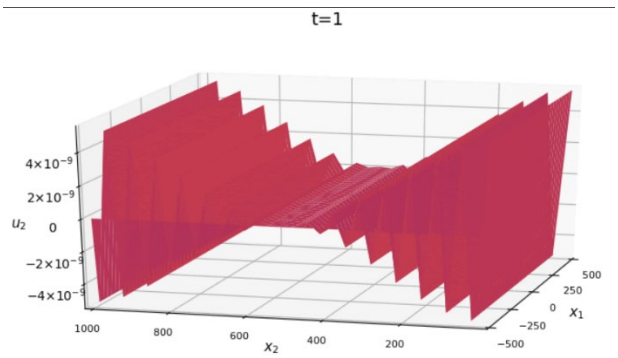


Рисунок 2. График функции решения $u_2(t_0, x_1, x_2)$ при $t = 1c$

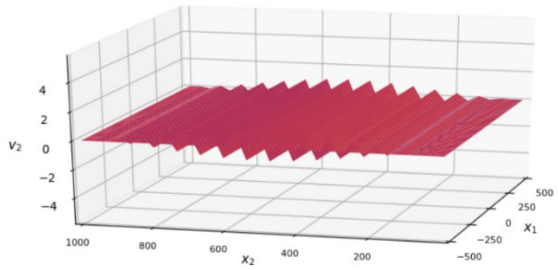


Рисунок 3. График функции решения $v_2(t, x_1, x_2)$ при $t = 1c$

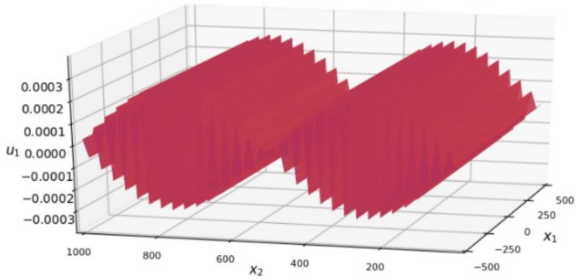


Рисунок 4. График функции решения $u_1(t, x_1, x_2)$ при $t = 53c$

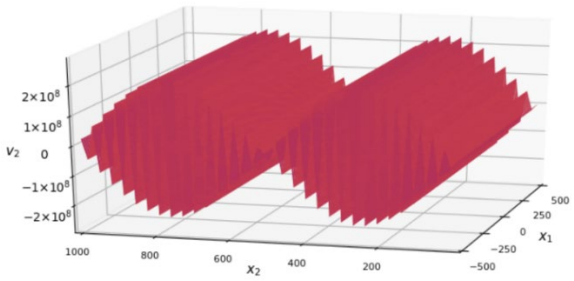


Рисунок 5. График функции решения $v_2(t, x_1, x_2)$ при $t = 53c$

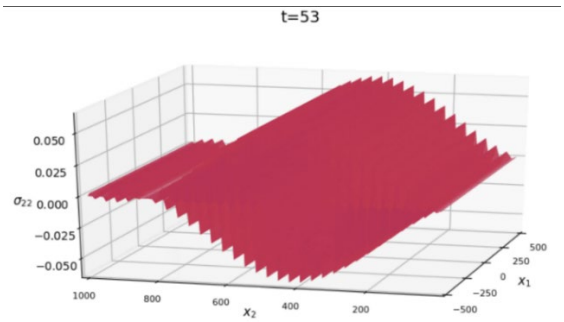


Рисунок 6. График функции решения $\sigma_{22}(t, x_1, x_2)$ при $t = 53c$

На приведенных графиках видно, что функции полученных решений удовлетворяют граничным условиям исходной задачи (1)-(6), то есть три функции затухают до нуля при $x_2 = 0$ и все при достаточно большом значении $x_2 \to \infty$.

Подтверждение Данное исследования проводились при поддержке гранта Комитета науки Министерства образования и науки Республики Казахстан Институту информационных и вычислительных технологий по проекту №AP05131026.

Литература

1. Frenkel I.I. “On theory of seismic and seismoelectrical phenomena in wet soil”, Izvestia AN SSSR. Ser.geogr. and geophys. Vol.8, No.4, PP.133-150, 1944. (In Russian)
2. Biot M.A. “Theory of propagation of elastic waves in a fluid-saturated porous solids”, J. Acoustic. Soc. Amer., - 1956, V. 28. PP. 168 - 186.
3. Berdyshev A.S., Imomnazarov Kh. Kh., Jian-Gang Tang, Mikhailov A. “The Laguerre spectral method as applied to numerical solution of a two dimensional linear dynamic seismic problem for porous media”, Open Comput.Sci., 6, PP.208-212, 2016
4. Sorokin K.E., Imomnazarov Kh.Kh. “Numerical solution of linear two-dimensional dynamic problem for porous medium”, Journal of Siberian Federal University, MathematicsI\&Physics, 3(2), PP.256-261, 2010 (In Russian)
5. Dorovskiy V.N., Perepechko Y.V., Romenskiy E. I., “Wave processes in saturated elastically deformable medium”, Physics of combustion and explosion, No 1, PP.100-111, 1993, (In Russian)
6. Blokhin A. M., Dorovsky V. N. Mathematical “Modelling in the Theory of Multivelocity Continuum”, Nova Sci., New York, MathSciNet, 1995
7. Dorovsky V. N. Imomnazarov Kh. Kh. A “Mathematical model for the movement of a conducting liquid through a conducting porous medium”, Mathl. Comput. Modelling, Printed in Great Britain, Vol. 20, No.7, PP.91-97, 1994
8. Imomnazarov Kh.Kh., Imomnazarov Sh.Kh., Mamatqulov M.M., Chernykh E.G. “The fundamental solution of the stationary two-velocity hydrodynamics equation with one pressure”, Bull. Of the Novosibirsk Computing Center, series: Mathematical Modeling in Geophysics, Novosibirsk, No.17, PP.5-12, 2014,.
9. Meirmanov A. “Mathematical Models for Poroelastic Flows”, Berlin : Springer, Vol. 1 of Atlantis Studies in distinctial Equations, 2014.
10. Berdyshev A.S., Imomnazarov Kh.Kh. “Direct and inverse problems for the system of equations of the theory of the two-velocity continuum” MES RK, Abai KazNPU, IICT. -Almaty, PP153, 2017. (In Russian)

11. Berdyshev A.S., Imomnazarov Kh.Kh., Kholmuradov A.E. “Optimizatsionnyi metod reshenia odnoi odnomrnoi obratnoi zadachi porouprugosti”, Sibirskie elektronnye matematicheskie izvestia. Vol 12., -PP284-293, 2015, http:semr.math.nsc.ru/v12/html (In Russian)

12. Berdyshev A.S., Imomnazarov Kh.Kh., Jian-Gang Tang, Tuchieva S. “The symmetric form of poroelasticity dynamic equations in terms of velocities, stresses, and pressure”, Open Engineering formerly Central European Journal of Engineering. Vol. 6, Issue 1. PP322-325, (2016)

13. 13. Berdyshev A.S., Bliyeva D.N. “Application of Laplace transformation to reduce differential system of poroelasticity equations to an elliptic system of equations”, Proceeds of the Scientific IICT Conference, MES RK "Modern problems of Computer Science and Computational Technologies", June 2-5, Almaty, PP.80-81, 2018

14. Berdyshev A.S., Bliyeva D.N. “On one study method of a mathematical model based on poroelasticity equations dynamic system”, Vestnik KazNITU, - №3, PP.527-233, 2019 (In Russian)

15. Berdyshev A.S., Bliyeva D.N. “Construction of fundamental solution system for dynamic poroelasticity problem using Laplace-Fourier transform”, Proceeds of IV International scientific and practical conference «Computer Science and Applied Mathematics», devoted to the 70-th anniversary of Prof.Biyarov T.N. and Wojcik Waldemar and 60th anniversary of Prof.Amirgaliyev, September 25-29, Almaty, PP.23-31, 2019.

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ДЛЯ ПОТОКА В ТРЕХМАСШТАБНОЙ СРЕДЕ С ТОНКИМИ ТРЕЩИНАМИ

Байшемиров Ж.Д.[1,2], Баймурзаев Д.Д. [2,3], Нуртас М.[4],
Адил Н.[1,2], Жанбырбаев А.Б. [1,2]
e-mail: zbai.kz@gmail.com
[1]*Казахский национальный педагогический университет имени Абая,*
[2]*Институт информационных и вычислительных технологий КН МОН РК,*
[3]*Военно-инженерный институт радиоэлектроники и связи,*
[4]*Международный университет информационных технологий, Казахстан*

Аннотация. *В данной работе рассматривается математическая модель осреднение течения сжимаемой жидкости в трехмасштабной среде с тонкими трещинами, представленные в блоках с условиями непрерывности потока и давления на границе раздела сред.*

Основное отличие сред с тонкими трещинами от сред с двойной пористостью состоит в том, что толщина трещин является новым малым параметром задачи. Это меняет структуру асимптотических разложений и, следовательно, макромасштабное поведение. В частности, высокая внутренняя проницаемость каждой трещины не обеспечивает ее доминирующей роли в процессе переноса, так как ее эффективная проницаемость может быть равной или даже меньшей, чем проницаемость плотных блоков. В частности, если локальная проницаемость трещины и блока равна 1 и ω соответственно, а толщина трещины равна h, то вклад трещин и блоков в процесс

переноса будет одинаковым, если $\omega \square h$. В этом случае среда ведет себя как однородная, то есть достаточно тривиально. Таким образом, режимы течения будут зависеть от соотношения между локальной проницаемостью блоков и эффективной проницаемостью трещин: ω / h. Соответственно, появление нелокальных эффектов, являющихся основным объектом изучения данного исследования, будет соответствовать случаю $\omega / h \square \varepsilon^2$, где ε - период

неоднородности среды. Это соответствует ситуации, когда $\omega \square \varepsilon^{2+\alpha}$ и $h \square \varepsilon^2$, где $\alpha > 0$.

Но в этом случае можно показать, что каждый блок будет возмущаться только в узком пограничном слое, непосредственно контактирующем с трещиной. В этом пограничном слое каждый блок работает как источник по отношению к течению в трещине. Это качественно меняет структуру функций Грина операторов, описывающих течение в блоке, и соответствующую структуру ядер в макроскопических уравнениях. Нами получены результат, что такой класс сред соответствует ядрам Абеля, что допускает аналитические решения соответствующих интегральных уравнений. Появление пограничного слоя и макроскопическая модель, соответствующая этому случаю, были получены в [1, 2] для двухмасштабной среды.

Уравнения течения сжимаемой жидкости в блоках $\Omega^{(1)}$ и трещинах $\Omega^{(2)}$ имеют вид:

$$b^{(1)} \frac{\partial p^1}{\partial t} = \varepsilon^{2+\alpha} \nabla_x \cdot \left(a^{(1)} \nabla_x p^1 \right), \quad x \in \Omega^1 \tag{1}$$

$$b^{(2)} \frac{\partial p^2}{\partial t} = \nabla_x \cdot \left(a^{(2)} \nabla_x p^2 \right), \quad x \in \Omega^2 \tag{2}$$

$$\frac{a^{(1)}}{a^{(2)}} = \varepsilon^{2+\alpha}, \quad \frac{h}{\varepsilon} = \varepsilon^{\frac{\alpha}{2}}, \quad \alpha > 1 \tag{3}$$

с условиями непрерывности потока и давления на границе раздела сред.

Если записать эти уравнения в локальных координатах $y = x/\varepsilon$, то на блоке множитель перед второй производной справа будет ε^{α}. Поэтому, когда $\varepsilon \to 0$, уравнение на блоке теряет вторую производную, то есть меняет тип. Из-за этого невозможно выполнить условия на границе раздела сред. Это означает, что внутри блока возникает тонкий пограничный слой, в котором сосредоточивается все возмущение.

Центральная часть блока остается невозмущенной в течение всего процесса. Осредненная модель течения в такой среде имеет форму системы двух уравнений:

$$\square B^{(2)} \frac{\partial P^1}{\partial t} = div\left(\square A^{(2)} gradP^2 \right) - \gamma\lambda \square B^{(1)} \int_0^t \frac{\partial P^1}{\partial t} \frac{1}{\sqrt{t-\tau}} d\tau \tag{4}$$

$$P^1 = P^2 - \int_0^t \frac{\partial P^2}{\partial t} K(t-\tau)\, d\tau, \qquad K(t) \equiv 1 - 2\varepsilon^{\frac{\alpha}{2}} \lambda \sqrt{t} \tag{5}$$

где P^1 и P^2 - осредненные давления в блоках и трещинах;

$$\lambda = \begin{cases} \dfrac{8\left(y_2^\Gamma y_3^\Gamma + y_3^\Gamma y_1^\Gamma + y_1^\Gamma y_2^\Gamma\right)}{\theta} \sqrt{\dfrac{a^{(1)}}{\pi b^{(1)}}}, & \textit{для случая осесимметричных трещин} \\ \dfrac{6}{\theta^{\frac{1}{3}}} \sqrt{\dfrac{a^{(1)}}{\pi b^{(1)}}}, & \textit{когда все переломы идентичны} \end{cases} \tag{6}$$

Формально, это подобно модели течения в среде с двойной пористостью, но ядро $K(t)$ определено иначе.

Рассмотрим среду такой де структуры как в [3 - 5], так что на самом большом масштабе мы имеет трещины и блоки, а каждый блок состоит из многих малых блоков и малых трещин. Все трещины тонкие. Нумерацию сред начнем с самой малой, так что Ω^1 - это самые маленькие и самые плотные блоки, Ω^2 - это мелкие трещины, которые разделяют мелкие блоки, Ω^3 - крупные трещины, которые образуют периодическую решетку с периодом ε.

Период сети мелких трещин - ε^2. Проницаемость сред растет от среды Ω^1 к среде Ω^3. Проницаемость крупных трещин – 1, мелких трещин - $\omega \le 1$. Отношение проницаемости сред Ω^1 и Ω^2 - $\varepsilon^{2+\alpha}$, подобно случаю двухмасштабной среды.

По ширине трещин намного меньше, чем период сети, так что:

$$h^{(i)} / \varepsilon^{4-i} = o(1), \; i = 3, 2$$

или

$$h^{(3)} \le \varepsilon, \qquad h^{(2)} \le \varepsilon^2.$$

Наряду с глобальной системой координат x, введем локальные координаты $y^{(1)}$ и $y^{(2)}$ для двух малых масштабов.

$$y^{(2)} = \frac{x}{\varepsilon}, \qquad y^{(1)} = \frac{x}{\varepsilon^2}.$$

Они варьируются внутри элементарных ячеек $Y^3 \cup \tilde{Y}^2$ и $Y^2 \cup Y^1$. Линейный размер каждой ячейки равен 1 в локальных координатах.

Модель потока, сформулированная через x для трехмасштабной среды выглядит в следующим образом:

$$b^1 \frac{\partial p}{\partial t} = \omega \varepsilon^{2+\alpha} \nabla \cdot \left(a^1 \nabla p \right), \tag{7}$$

$$b^2 \frac{\partial p}{\partial t} = \omega \nabla \cdot \left(a^2 \nabla p \right), \quad x \in \Omega^2 \tag{8}$$

$$b^3 \frac{\partial p}{\partial t} = \nabla \cdot \left(a^3 \nabla p \right), \quad x \in \Omega^3 \tag{9}$$

с граничными условиями

$$a^{(n+1)} \frac{\partial p}{\partial v}\bigg|_{\Gamma_+^{n+1,n}} = \omega a^{(n)} \frac{\partial p}{\partial v}\bigg|_{\Gamma_-^{n+1,n}}, \quad n = 1, 2 \tag{10}$$

где $\Gamma^{n+1,n}$ - граница между Ω^n и Ω^{n+1}; v - нормаль вектор к $\Gamma^{n+1,n}$; $\Gamma_+^{n+1,n}$ означает ту сторону границы $\Gamma^{n+1,n}$, которая касается области Ω^{n+1}; ∇ - оператор градиента, выраженный через переменную x.

Работа выполнена при финансовой поддержке гранта КН МОН РК №AP05132680.

Литература

1 L.Pankratov, V. Rybalko. Asymptotic analysis of a double porosity model with thin fissures. Mat. Sbornik, 2003,v.194, no. 1, pp 121–146

2 Panfilov M.B. Macroscale Models of Flow through Highly Heterogeneous Porous Media. -Kluwer Academic Publishers, 2000.

3 Байшемиров Ж.Д., Жанбырбаев А.Б., Баймурзаев Д.Д. Усредненная модель неравновесной двухфазной фильтрации несжимаемых жидкостей в двухмасштабной среде с сильно контрастными свойствами // Вестник КБТУ. - 2018. - №4. –С. 49-55.

4 Байшемиров Ж.Д., Жанбырбаев А.Б., Адил Н., Баймурзаев Д.Д. Об линеаризованной модели двухфазного течения // Материалы IV Международной научно-практической конференции «Информатика и прикладная математика», посвященной 70-летнему юбилею профессоров Биярова Т.Н., Вальдемара Вуйцика и 60-летию профессора Амиргалиева Е.Н. – Алматы, 2019. -С. 182-186.

5 Панфилов М.Б., БайшемировЖ.Д., Бердышев А.С. Макроскопическая модель двухфазного течения сжимаемых жидкостей в среде с двойной пористостью // Прикладная математика и механика. Том: 84 • Выпуск: 1, 2020. -С.44-63.

SOME APPROACH TO ECG SIGNALS PROCESSING, ANALYZING AND CLASSIFICATION

[1,2]Iurii Krak
E-mail: [1]krak@univ.kiev.ua, [2] yuri.krak@gmail.com
[1] Taras Shevchenko National University of Kyiv, Theoretical Cybernetics Dept., Kyiv, 01601, Ukraine
[2] Glushkov Cybernetics Institute, Intellectual communication information Lab., Kyiv, 03187, Ukraine

Abstract

The paper investigates statistical algorithms for ECG signal processing, such as correlation function estimation, spectral density (Fourier transform), estimation of R-R intervals distribution, and various variants of wavelet transform. The dynamics of the variation of the dispersion of the lengths of the R-R intervals were also investigated. To distinguish R-R intervals, an ECG approximation was used with the help of a piecewise polynomial continuous and differentiated curve developed by the authors, which has a continuous first derivative[1]. The algorithm for estimating the first derivative based on proposed splines is developed. The detection of the spline thresholds value for the effective isolation of R peaks in the ECG signal is investigated. Using the spline-approximation derivative allowed to increase the accuracy of R-R intervals selection up to 6% compared to the known numerical methods. Wavelet transforms were used for the spatial-temporal analysis of the ECG signal, which make it possible to use parts of signals in the systems of operational signal investigation. Also, on the basis of the inverse wavelet transform, the ECG signal was cleared of noise. These algorithms formed the basis for the creation of a smart system for monitoring and prompt evaluation of cardiac regimens. Combining different approaches to ECG analysis has increased the reliability of the recognition system. Among machine learning algorithms, convolutional neural networks (CNNs) have achieved significant performance in many pattern recognition tasks, along with traditional approaches such as Random Forest or Gradient Boosting. Wavelet transformations allow utilizing spectral components that are useful in ECG signal processing tasks [2]. The performance of the wavelet applications for signal classification was evaluated. The experiments show that wavelet transformations can achieve better accuracy than existing algorithms while having significantly fewer parameters than conventional CNNs. Experiments show that the use of a smart system allows you to diagnose abnormalities in the heart.

Keywords: *signal analysis, approximation, QRS complex, features extraction, sequential analysis, classification, expert systems*

Refrences

[1] Iurii Krak, Anatolii Pashko, Oleg Stelia, Olexander Barmak, Sergey Pavlov. “Selection Parameters in the ECG Signals for Analysis of QRS Complexes”. Proceedings of the 1st International Workshop on Intelligent Information Technologies & Systems of Information Security. Khmelnytskyi, Ukraine, June 10-12, CEUR Vol-2623. 2020. pp.1-13.

[2] O.A. Khorozov, I.V. Krak, A.I.Kulias, V.S.Kasianiuk, W.Wojcik, A.Tergeusizova. “Monitoring vital signs using fuzzy logic rules”. In monograph: Information technology in Medical Diagnostics II. Ed. by Waldemar Wojcik, Sergii Pavlov, Maksat Kalimoldaev. CRC Press. 2019. pp.237-243. [3

TRANSMISSION CAPACITY ANALYSIS OF DENSE RELAY-ASSISTED D2D CELLULAR NETWORKS

Amodu Oluwatosin[1], Mohamed Othman[1,2], Orken Mamyrbayev[3], Nor Kamariah Noordin[4], Idawaty Ahmad[1]
E-mail: amoduahmedtosin@gmail.com, mothman@upm.edu.my, morkenj@mail.ru, nknordin@upm.edu.my, idawaty@upm.edu.my
[1]*Department of Communication Technology and Network, Universiti Putra Malaysia, 43400 UPM Serdang, Selangor D.E., Malaysia*
[2]*Laboratory of Computational Science and Mathematical Physics, Institute of Mathematical Research (INSPEM), Universiti Putra Malaysia, 43400 UPM Serdang, Selangor D.E., Malaysia*
[3]*Institute of Information and Computational Technology, Almaty, Kazakhstan*
[4]*Department of Computer and Communication Systems Engineering, Faculty of Engineering, Universiti Putra Malaysia, 43400 UPM Serdang, Selangor D.E., Malaysia*

Abstract
The deployment of relay nodes is a promising approach to improve the coverage of traditional device-to-device (D2D) communication. Devices with poor connectivity find relay nodes to facilitate data transmissions which improve the transmission capacity (TC) of the network. However, some devices are not always willing to function as relays especially when there are no incentive mechanisms provided. Also, in a network consisting of highly dense potential relay nodes, relays may not provide a further increase in TC gain as they begin to cause interference. In this paper, we revisit existing TC analysis of relay-assisted D2D communication, giving computable expressions for the relay gains in the underlay and overlay modes. We identify a key challenge in dense relay deployments where a further increase in the density of relay nodes does not provide any increase in TC gains. In such scenarios, we show that the unwillingness of certain nodes to function as relays can be of advantage to improve the TC performance in both underlay and overlay modes. To this end, we present a model in which the number of willing relay nodes (wRNs) is modelled as a function of the total relays to capture the non-altruistic tendencies of most devices.

Keywords: *D2D; relay; poisson point process; stochastic geometry; transmission capacity*

STEADY FREE CONVECTION OF PARAFFIN WAX IN RECTANGULAR CAVITIES

Çağatay Yıldız , Müslüm Arıcı
e-mail: cagatayyildiz01@gmail.com, muslumarici@gmail.com,
Mechanical engineering department, Engineering faculty, Kocaeli University, Umuttepe campus, 41001, Kocaeli, TURKEY

Abstract. *Photovoltaic panels (PV), which are the devices that converts solar energy to electric energy, are drawing more attention day by day, due to the fact that solar energy is an abundant renewable energy type. Although the solar energy is plentiful and clean, the conversion efficiency of PV panels is so low that they only convert a small amount of*

solar energy to electrical energy, namely 5-20% in practical applications. Apart from the low efficiency PV panels already struggle, excessive temperature rise cause a significant drop in the efficiency, which can be around 0.4 to 6.5% per 1 °C of temperature rise. At this point, cooling applications, which can be implemented by active and passive methods, become crucial for hindering the efficiency drop of PV panels. One of the passive cooling methods for PV panels, meaning that no requirement for external energy, is the utilization of phase change materials (PCM) by mounting an enclosure filled with PCM to the back of PV panels, which is then called PV/PCM system. Due to the high heat absorption capacity of PCMs during melting, this method is proven to be useful for PV cooling applications by various studies. However, there are few studies investigating the natural convection behaviour of molten PCM, that is, once the melting process is completed. Furthermore, most studies considering natural convection in enclosures deal with isothermal boundary condition at cavity walls or heat flux at one wall and constant temperature at the other wall. In this study, natural convection of molten PCM in a rectangular enclosure is taken into account with heat flux on top and Robin boundary condition at the bottom wall of the enclosure, while the remaining side walls are considered adiabatic. Besides, the analysis is performed for different Biot numbers, Rayleigh numbers, and aspect ratios. The outcomes of the numerical computations are presented by streamline and isotherm contours for the visualization of flow and temperature fields, and local and mean Nusselt numbers for the evaluation of heat transfer performance. The results showed that variation of Biot number has remarkable impact on the flow structure. Compared to the case of isothermal boundary condition, the flow structure is considerably different at low Biot numbers, while this difference becomes insignificant as Biot number is increased. It is deduced from the outcomes of the study that the considered boundary condition and especially the Biot number has a remarkable effect on the natural convection, which reveals the importance of appropriate selection of boundary conditions in modelling of PV/PCM systems.

ИНТЕЛЛЕКТУАЛЬНАЯ СИСТЕМА УПРАВЛЕНИЯ ДОРОЖНЫМ ДВИЖЕНИЕМ В МЕГАПОЛИСЕ

А.С. Родионов[1], И.А. Мусихин, П.А. Карпик[2]
e-mail: alrod@sscc.ru (13 пт.)
[1]*Институт вычислительной математики и математической геофизики СО РАН*
[2]*Сибирский государственный университет геосистем и технологий*

Аннотация. *В докладе рассматриваются основные положения по разработке интеллектуальной системы управления дорожным движением в больших городах, включающей как адаптивную маршрутизацию, учитывающую прогнозную загрузку дорог, так и управление светофорами и управляемыми дорожными знаками*

Введение

То, что дорожное движение становится всё более интенсивным и сложным в оперативном (да и в стратегическом) управлении, давно стало очевидным. Стремительный рост автопарков в больших городах с одной стороны и

возможности, предоставляемыми современными цифровыми информационными технологиями с другой, естественным образом приводят к разработке многочисленных автоматизированных систем мониторинга и организации дорожного движения (МОДД). При этом, как правило, независимо развиваются системы маршрутизации (навигации), учитывающие оперативную обстановку в ближайшем окружении транспортного средства и перспективном маршруте, и системы управления светофорами и управляемыми дорожными знаками, также учитывающие оперативную информацию о интенсивности движения на конкретных перекрёстках и перегонах. Вместе с тем, совмещение этих систем может привести к существенным результатам по разгрузке дорог и предотвращению возникновения заторов (пробок).

Дорожное движение в больших городах обладает некоторыми специфическими особенностями, это:

- Большая плотность транспортных потоков;
- Наличие «спальных районов» и пригородных дач, определяющих цикличность потоков по времени суток и дням недели;
- Заведомое наличие «узких мест», как-то: мостов, межрайонных магистралей, въездов-выездов из города;
- Большое количество регулируемых перекрёстков и пешеходных переходов;
- Наличие общественного транспорта (ОТ) различного типа, включая рельсовый;
- Значимое количество спецтранспорта;
- Экологические проблемы, связанные с загрязнением атмосферы выхлопными газами.

Соответственно, при создании подобной интегрированной системы необходимы:

- Возможно более полный охват территории и участников ДД при минимизации затрат;
- Учёт различных прав участников движения (ОТ, спецтранспорт, электротранспорт, грузовые и легковые автомобили и пр.);
- Учёт возможности смены режимов работы светофоров и управляемых дорожных знаков.

Система МОДД призвана решать целый ряд задач:

Стратегические задачи:

- Определение маршрутов и расстановка остановок ОТ;
- Расстановка дорожных знаков, разметка, светофоры…
- Расстановка камер наблюдения и других придорожных устройств.

Оперативные задачи:

- Обновление статистики;
- Маршрутизация;
- Управление режимом работы светофоров;
- Добавочные ТС ОТ.
-

Основные допущения

Предполагается, что по большей части транспортных средств (ТС) в онлайн режиме доступна следующая информация:

- Текущее местоположение (посредством систем GLONASS/GPS, BeiDou, и т.д.);
- Тип ТС (известен из его персонального ID);
- Назначенный маршрут (по сообщениям с навигатора ТС).

Доли средств, предоставляющих эти данные, обозначим как $\alpha_i \in (0,1)$, соответственно.

Предполагаем, что а-приори скорость ТС зависит от его типа и текущего состояния дороги.

Под состоянием дороги понимаем её загрузку $l=L/Th$, где L – число ТС на 1000 м^2 дороги, а Th – её пропускная способность.

Для простоты используем шкалированную таблицу скоростей ТС, предполагая постоянной скорость v_{ij} ТС класса i на j-ом интервале загрузки дороги.

В случае постоянной загрузки дорог местоположение ТС в любой будущий момент времени легко определяется при наличии его заданного маршрута. Однако, очевидно, что и загрузка дорог, и маршруты ТС подвержены изменениям.

Для прогноза загрузки дорог и, соответственно, местоположения ТС, используем матрицы “источник-назначение” (origin-destination matrices, ODM) A(t), оценку которых можно проводить многими методами [1,2]. Использование этих матриц позволяет моделировать появление новых активных ТС на участках дорог.

Источники данных

Средства сбора оперативных данных:

- Расстановка видеокамер;
- Использование интернет приложений типа «Яндекс пробки»;
- Обратная связь с навигаторов;
- В перспективе - VANET.

Дополнительные средства сбора статистики для стратегического управления:

- Сводки ДТП (для определения потенциально аварийно-опасных участков);
- Данные от операторов мобильной связи;
- Данные от паспортных столов и организаций (для определения пассажиропотоков в ОТ);
- Данные от перевозчиков, как ОТ, так и грузового автотранспорта.

Цели управления

Рассматриваются две группы показателей, в какой-то мере отображающих противоположные интересы городской среды и участников движения.

С точки зрения участников движения:

- длина пути (l_{ij});
- время в пути (t_{ij});
- количество пересадок при поездках на ОТ (n_{ij});
- Необходимый пеший путь при поездках на ОТ (s_{ij}).

… … … … … .

С точки зрения «города», интегральные показатели:

- выбросы в атмосферу (P);
- пополнение бюджета (B);
- выполнение градостроительных норм и правил (GP);
- обеспечение «элитности» отдельных микрорайонов (El);
- … … … … … .

Противоречивость целей приводит к постановке задач многокритериальной оптимизации с заданием весов оптимизируемых показателей.

$$F = \alpha F_1 + (1-\alpha)F_2,$$

$$F_1 = \beta_1 \sum_{i=1}^{n}\sum_{j=1}^{n} E[l_{ij}] + \beta_2 \sum_{i=1}^{n}\sum_{j=1}^{n} E[t_{ij}] + \beta_1 \sum_{i=1}^{n}\sum_{j=1}^{n} E[n_{ij}] + \beta_1 \sum_{i=1}^{n}\sum_{j=1}^{n} E[s_{ij}] + \ldots,$$

$$F_2 = \gamma_1 E[P] + \gamma_2 E[B] + \gamma_3 E[GP] + \gamma_4 E[El] + \ldots.$$

Математические ожидания либо оцениваются на основе статистических данных, либо экспертно.

Параметр α определяет приоритеты жителей и властей, β_i и γ_i – служат для определения вклада показателей с одновременным обезразмериванием и приведением к одному масштабу.

Прогноз местоположения ТС

Предположим также, что нам известны средние значения загруженности дорог для разных интервалов времени и для разных типов дня (рабочий, праздничный, выходной и т.д.) и для разных погодных условий. Несложно предсказать, что в будущем, когда все активные машины будут сообщать о своем местонахождении через какую-то систему, такую информацию можно будет получить.

Таким образом, в любое время в будущем, то есть во времени $t = t_0 + \Delta t$, где t_0 – текущее время, мы можем предсказать загрузку L_iлюбой дороги R_i по следующему правилу:

$$L_i(t)=L_i(t_0)-dL_i(t, \Delta t)+\mathrm{aL_i}(t, \Delta t)+\mathrm{EL_i}(t, \Delta t).$$

Здесь $dL_i(t, \Delta t)$ – уменьшение загрузки дороги за счёт покидающих её ТС за время Δt, aL_i(t, Δt) – увеличение загрузки за счёт въезжающих на неё ТС за этот период, и EL_i(t, Δt) – дополнительное прогнозное увеличение загрузки за счёт новых участников движения, моделируемых на основе матриц ODM $A(t)$.

Стандартные решения по организации систем МОДД (данные и софт)

Как правило, для описания дорожной сети используют взвешенные графы, иногда несколько.

Более продвинутые системы используют понятия *слоёв*, привязанных к одним координатам, т.е. зная координаты можно получать информацию из графа, соответствующего конкретному слою. Если координаты получены при решении задачи на графе одного слоя (например, при решении задачи покрытия сети дорог регистраторами какого-либо вида), можно легко связаться с данными других слоёв по этим координатам. Также по этим координатам можно получать информацию из различных геоинформационных баз, например, кадастрового учёта.

Наиболее известны международные стандарты OGC WMS, WFS и WPS для формирования, обмена, предоставления и обработки пространственных данных.

По данным сайта https://live.osgeo.org/:

Стандарт OGC WMS (картографический веб-сервис) предоставляет простой интерфейс http-запросов для получения геопривязанных изображений карт нескольких распределённых пространственных баз данных. В ответе сервиса на

запрос будет одно или более изображений карты (в формате JPEG, PNG и др.), которые могут быть показаны в браузере или настольном приложении.

Стандарт WFS — веб-сервис пространственных объектов, определяющий интерфейсы и операции, которые позволяют запрашивать и редактировать векторные пространственные данные, такие, как дороги или береговые линии.

Стандарт WPS (веб-сервис геопроцессинга) описывает правила для входящих и исходящих данных (запросов и ответов на них) для сервисов геопроцессинга (геообработки), таких, как пересечение полигонов и др.

Из отечественных систем можно упомянуть, например, ГИС Сервер 2011 [3] – службу Windows Services, предназначенную для обеспечения удаленного круглосуточного доступа к пространственным данным пользователей программ ГИС Карта 2011, Панорама-Редактор, ГИС Навигатор 2011, Панорама 2011 Мини и других программ, разработанных в среде GIS ToolKit версии 11 или ГИС-Конструктор для Linux.

Этот сервер предоставляет удаленный многопользовательский доступ к различным видам пространственных данных: векторным, растровым и матричным.

Перечисленные системы предназначены, прежде всего, для простых отображения и реализации запросов, не затрагивая вопросы решения задач оперативного управления и решения различных оптимизационных задач.

Предлагаемая модель описания карт дорог и маршрутов

В качестве математической модели подобных многослойных карт наиболее удобно использовать *гиперсети* [4]. В этой модели рёбра первичной сети называются ветвями, а маршруты (пути) вкладываемых сетей – рёбрами. Таким образом, каждая вкладываемая сеть описывается графом, вершины которого соответствуют оконечным пунктам, и каждому ребру соответствует путь из ветвей первичной сети.

Нетрудно видеть, что гиперсети естественным образом могут служить формальной моделью для описания взаимодействия слоёв карт в отрыве от пространственного их изображения, т.е. быть промежуточным представлением между ГИС и решателями:

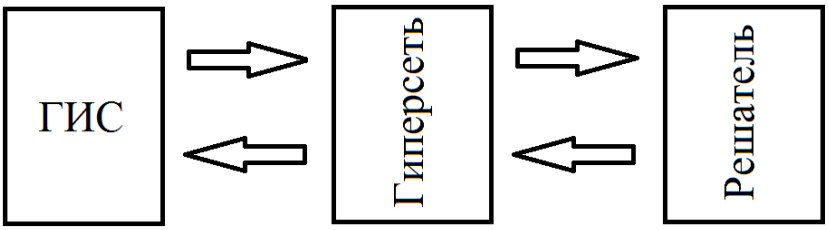


Рис. 1 Место гиперсети в моделировании системы МОДД

При программной объектно-ориентированной версии реализации модели МОДД для объекта, описывающего ветвь, очевидна необходимость реализации следующих методов:

Vehicles – формирование текущего списка ТС на ветви;

State – отчёт о состоянии ветви (загрузка, наличие препятствий, средняя скорость, наличие и характеристики пробок);

StateForecast – прогноз состоянии ветви на заданный момент времени;

… … …

Для объекта же описывающего ТС, необходимы следующие методы:

Route – определение оптимального маршрута от текущего местоположения до цели;

TimeForecast – прогноз оставшегося времени поездки;

FuelForecast – прогноз расхода топлива.

Остальные методы привязываются к конкретным типам ТС.

В условиях больших размерностей графов слоёв, характерных для мегаполисов, нецелесообразно реализовывать методы объектов ТС на оконечных (мобильных) устройствах, задачи выполнятся решателями на центральной супер ЭВМ (ЦС), методы же реализуют подготовку запросов и интерпретацию полученных результатов.

Что до гиперсети модели транспортной системы, то она, естественно, также формируется и поддерживается на ЦС.

1. Gaudry, Marc. The Four Approaches to Origin-Destination Matrix Estimation for Consideration by the MYSTIC Research Consortium // Bureau d'Economie Théorique et Appliquée, UDS, Strasbourg, Working Papers of BETA, 2000.

2. Reza Tolouei, Stefanos Psarras, Rawle Prince. Origin-Destination Trip Matrix Development: Conventional Methods versus Mobile Phone Data // Transportation Research Procedia, 2017. – Vol. 26, P. 39-52.

3. *ГИС Сервер x64 (ГИС Сервер)* – https://gisinfo.ru/products/gisserver.htm (15.09.2020).

4. В.К. Попков, Математические модели связности / Отв. ред. А. С. Алексеев. 2-е изд., испр. и доп. Новосибирск: ИВМиМГ СО РАН, 2006. 490 с.

ПОДХОД К ПОСТРОЕНИЮ ОНТОЛОГИЙ НАУЧНЫХ ПРЕДМЕТНЫХ ОБЛАСТЕЙ НА ОСНОВЕ СИСТЕМЫ ПАТТЕРНОВ ОНТОЛОГИЧЕСКОГО ПРОЕКТИРОВАНИЯ

Загорулько Ю.А.
e-mail: zagor@iis.nsk.su
Институт систем информатики им. А.П. Ершова СО РАН; Новосибирск; Россия

Аннотация

В докладе представлен подход к разработке онтологий научных предметных областей, базирующийся на использовании разнородных паттернов онтологического проектирования, объединенных в одну систему. В докладе дается краткий обзор паттернов онтологического проектирования, описывается система паттернов, включающая как универсальные паттерны, предназначенные для описания типовых конструкций онтологии, так и паттерны, ориентированные на представление научных знаний, обсуждается методика построения онтологии с использованием данной системы паттернов. Показано, что применение паттернов онтологического проектирования позволяет не только обеспечить согласованное представление всех сущностей онтологии научной предметной области и тем самым избежать многих ошибок онтологического моделирования, но и сэкономить ресурсы, затрачиваемые на разработку этой онтологии.

Ключевые слова: *Онтология, Научная предметная область, Научные знания, Паттерн онтологического проектирования, Методика построения онтологии*

ИСПОЛЬЗОВАНИЕ МЕТОДОВ КАЧЕСТВЕННОГО КОНТЕНТ-АНАЛИЗА ДЛЯ ИССЛЕДОВАНИЯ РАСПРЕДЕЛЕНИЯ ПРОТИВОПРАВНЫХ ТЕКСТОВ НА НОВОСТНЫХ САЙТАХ

Хайрова Н. Ф.[1], Мамырбаев О. Ж.[2], Колесник А. С.[3] , Мухсина К. Ж.[4]
[1]e-mail: nina_khajrova@yahoo.com
[3]e-mail: kolesniknastya20@gmail.com
Национальный технический университет «Харьковский политехнический институт», Украина
[2]e-mail: morkenj@mail.ru
Институт информационных и вычислительных технологий КН МОН РК, Казахстан
[4]e-mail: kuka_ai@mail.ru
Казахский Национальный университет им. Аль-Фараби, Казахстан

Для анализа огромное количество текстовой информации социальных сетей и медиа может быть применена информационная технология контент-анализа, изучающего документы в их социальном контексте. Использование методов контент-анализа позволяет исследовать смысловое содержания текстов и оценить их влияние на общество. В данном исследовании приводится анализ существующих подходов, методов и инструментов контент-анализа, а также обосновывается актуальность использования широкого спектра лингвистических категорий для проведения качественного контент-анализа. В статье показано использование методов качественного контент-анализа, базирующихся на инструментах и алгоритмах machine learning и разработанном трехъязычном словаре криминально окрашенных терминов. В качестве экспериментального корпуса рассматриваются тексты, собранные автоматически, с помощью разработанного программного продукта, с новостных сайтов Казахстана, Украины, Великобритании и США.

Введение.

Сегодня одним из самых популярных направлений исследования больших объемов текстовых данных становится использование методов и подходов контент-анализа. И, несмотря на то, что контент-анализ наиболее популярен в областях социальных и гуманитарных наук, этот подход становится все более универсальным.

Спектр применения подходов контент анализа является довольно широким. Наиболее часто он используется при проведении социальных исследований, опросов, для выявления шаблонов и поиска тенденций изменения в общественном мнении в хронологическом срезе. Полученные таким образом данные можно сравнивать в разных промежутках времени и выявлять изменения, происходящие в обществе, политике или культуре [1]. Также контент-анализ является одним из

самых простых способов, используемых для определения авторства. Его методы актуальны также при изучении документов в их социальном контексте, что позволяет выявить то, что может ускользнуть при традиционном изучении статей, публикаций СМИ, выступлений известных людей и т. д.

Целью контент-анализа является создание количественного описания смыслового и символического содержания текста документа, которое позволит фиксировать объективные признаки и осуществить их подсчет. Контент-анализ позволяет "вписать" содержание документа в социальный контекст, осмыслить его одновременно и как проявление, и как оценку социальной жизни. Такой анализ документа может:

–выявить действия и события, существовавшие до данного документа и получившие в нем свое отражение;

–показать существующие в настоящем документе особенности (например, характеристики формы - язык, структура, жанр сообщения ритм и тон речи);

–оценить результат или эффект воздействия данного документа на последующие события.

В целом, контент-анализ может быть использован как: основной, параллельный и контрольный (вспомогательный) метод. В качестве основного данный метод используется при определении тематической направленности изучаемого материала. Параллельный метод применяется в сочетании с другими методами, а контрольный или вспомогательный при классификации ответов на анкетные вопросы.

Важным отличием контент-анализа от других подобных методов является его четкость, формализованность и систематизированность, которые заключаются в необходимости конкретного определения категорий анализа (ключевых понятий документа). После определения системы категорий анализа необходимо выбрать единицу анализа текста, соответствующую этим категориям. Единицей анализа может быть слово, предложение, тема, идея, автор, персонаж, социальная ситуация и другие элементы. Следующим этапом контент-анализа является установление единицы счета, представляющей элемент количественной меры единицы анализа, который позволяет регистрировать частоту (регулярность) появления признака категории анализа в тексте (число печатных знаков, страниц, абзацев, авторских листов и т.д.). Заключительный этап представляет экспертный анализ полученных результатов исследования.

Такая по-этапность контент-анализа требует детального предварительного анализа цели метода, определения ее зависимости от выбранных категорий и их количественного или качественного значения.

Анализ возможностей использования контент-анализа в современных лингвистических и социальных исследованиях

Контент-анализ представляет собой универсальный метод для работы с информацией, используемый с различными источниками данных, таких как текстовые, визуальные, аудио- и другие виды данных [2]. Методика контент-анализа является очень гибкой и может быть использована как эмпирически так и теоретически [3].

В целом подходы контент-анализа можно разделить на качественные и количественные. В простейшем случае, количественный контент-анализ включает

подсчет слов или предложений. В сложном, — это процесс выделения категорий в имеющихся данных (репрезентативных образцов содержания) и их кодирование, что позволяет выявить или отобразить те или иные различия анализируемых данных и оценить точность кодирования. Собранные данные анализируются для описания шаблонов или характеристик контента или для идентификации связи между рассматриваемыми свойствами данных [4].

Количественный подход хорошо себя зарекомендовал, в так называемой, предиктивной полицейской деятельности, которая заключается в применении количественных аналитических методов для определения перспективных целей предотвращения преступлений. При таком анализе используются уже имеющиеся данные по преступлениям (записи допросов, архивные данные, протоколы и т. д.). В исследовании [5] показано, что данный подход позволяет с высокой вероятностью определить место и время правонарушения, а также выявить людей, находящихся в группе риска.

Следует отметить, что достаточно большое количество исследований посвящено использованию методов количественного контент-анализа в задачах криминалистики. Например, в исследовании [6] используются количественные лингвистические показатели для контент-анализа текстовых записей 30 человек, совершивших самоубийство или террористические преступления. Результат обработки позволил выявить тенденции (географические, наличие групповой принадлежности и др.), указывающие на преступление.

При выборе между количественным и качественным анализом, современные исследователи склоняются к качественному, так как он использует индуктивные рассуждения исследователя, формирующего категории [7, 8]. Например, количественный контент-анализ можно успешно использовать для определения близости тем произведений авторов, по частоте появления заданных слов и фраз, а качественный анализ позволяет осуществлять глубокий анализ текста, основанный на связи между понятиями. Исследования, которые используют качественный подход, фокусируются на характеристиках языка как объекте коммуникации. В этом случае контент-анализ не останавливается на простом подсчете слов, а переходит на уровень интенсивного изучения языка, целью которого является классификация большого количества категорий, отображающих явное или предполагаемое сообщение.

Можно выделить три подхода качественного анализа [9]. Первый подход является традиционным, при котором категории для кодирования выводятся из необработанных данных. Второй подход является направленным, когда категории для кодирования берутся из теории или результатов исследования, а затем исследователи используют эти данные и создают категории. И третий подход — это итоговый подход, который начинается с количественного контент-анализа, заключающегося в подсчете слов, а затем расширяется до качественного контент-анализа, используемого для определения и раскрытия темы [10].

Сам процесс контент-анализа является многоуровневым, одним из важных этапов которого является этап создания словаря, используемого для категоризации. Под словарем подразумевается список слов, ассоциируемых с той или иной категорией. Словарь может создаваться вручную большим количеством экспертов или автоматически с помощью различных методов machine learning и компьютерной лингвистики.

Так называемые мануальные, вручную созданные словари, широко применяются на маленьких текстах и незначительном объеме данных. Возможно использование уже существующих словарей, например, хорошо известных словарей положительных и отрицательных слов [11]. В то же время, наиболее удобным и быстрым способом создания словаря является его автоматическое создание. Для этого обычно необходим большой набор текстов (например, сообщения из соцсетей, статьи, твиты), размеченных по характеризуемым атрибутам человека (пол, возраст и т. д). Эти тексты разбиваются на слова или словосочетания с помощью токенизации, и определяются слова или фразы, наиболее связанные с результатом, например, с помощь стохастических методов.

Еще один способ создания словаря основывается на "краудсорсинге", позволяющем собирать большое количество слов без особых усилий и затрат по времени. Используя рейтинги создаются "взвешенные словари", в которых каждое слово имеет соответствующий вес в определенной категории (например, слово "потрясающий" может быть оценено как 4.6 по 5-балльной шкале положительных эмоций, тогда как слово "хороший" может получить только 3.5). Такая оценка, данная слову сотнями или даже тысячами людей, позволяет разработать рейтинговый словарь, охватывающий даже слова из категории общих и нейтральных.

Как количественный, так и качественный подходы контент-анализа имеют широкие спектры применения. Например, в исследовании [12] внимание уделяется контент и сентимент анализам, посвященным теме вируса Эболы в ленте новостей и Твиттере, которые осуществлялись с помощью словарного контроля собранных данных, а также с использованием n- граммного техники моделирования тем LDA и анализа сущностей. Результаты показали, что освещенность этой темы в Твиттере более была более размыта, чем в новостях. Кроме того, в новостных статьях больше внимания уделялось таким объектам, связанным с событиями как лицо, организация и местоположение, тогда как Twitter охватывает объекты, ориентированные на время.

Кроме социальной и криминальной сферы контент-анализ активно используется в различных других научных направлениях. Например, в исследовании [13] был осуществлен контент-анализ публикаций различных журналов, связанных с эколингвистикой, показавший резкое повышение внимания к данному направлению исследований.

Исследование подходов и алгоритмов NLP, используемых для автоматизированного контент-анализа

Задача контент-анализа решается в рамках общего подхода Natural Language Processing (NLP). Обработка естественного языка является очень широкой областью, позволяющей получать новую информацию из уже имеющихся текстовых данных. Существенная часть технологий NLP базируется на методах машинного обучения (machine learning), хорошо работающих при наличии заданных человеком входных признаков и оптимизации их весов; так же как на подходах глубинного обучения (deep learning), использующих алгоритмы автоматического выявления лучших признаков из сырых входных данных.

Стартовой точкой NLP задач часто является векторное представление или *Vector Space Model* (VSM). Направления *word embedding* и *text embedding* представляют важные методы NLP, при которых слова сопоставляются с векторами

действительных чисел. Метод *word embedding* позволяет формализовать значение слова в документе, выявить семантическое представление, а также определить связь и семантическое сходство с другими словами. Он применяется в задачах классификации текстов, следовательно, является незаменимым инструментом для контент-анализа.

Word2vec, использующий двухслойную нейронную сеть, является одним из самых популярных методов реализации *Word embedding*. На вход поступает текстовый корпус, а на выходе — набор векторов. Хорошо обученный набор векторов слов разместит похожие слова близко друг к другу в VSM пространстве. Например, слова "помидор", "огурец" и "овощи" могут объединяться в одном углу, а желтый, красный и синий — в другом. Многие исследователи считают, что развитие подхода *Word embedding* позволит преобразовывать естественный язык так, что он будет легко читаться компьютером при выявлении сходства между словами и текстами, с последующей возможностью реализации различных математических операций над векторами.

Word2vec использует два основных учебные алгоритма, один - *continuous bag of words* (*CBOW*), другой — *skip-gram*. Основное различие между этими двумя методами заключается в том, что *CBOW* использует контекст для прогнозирования целевого слова, тогда как *skip-gram* использует слово для прогнозирования целевого контекста. Как правило, метод *skip-gram* может иметь лучшую производительность по сравнению с методом *CBOW*, поскольку он может захватить два семантических значения одного слова.

Кроме *word2vec* для автоматической реализации контент-анализа может быть использована техника векторных представлений, например, такая как *GloVe*, которая стремится решить проблему увлечением значение одного *word embedding* со структурой всего обозримого корпуса. Для этого, модель ищет глобальные совпадения числа слов и используя статистику, минимизирует среднее отклонение. Такая схема позволяет отождествлять сходство слова с векторным расстоянием с достаточной степенью точности.

Использование перечисленных выше методов и алгоритмов обработки текстов (NLP) позволяет осуществлять автоматизированный контент-анализ текстовых данных с высокой точностью. Программные реализации этих алгоритмов доступны на языке Python в таких пакетах как scikit, Gensim и др.

Метод контент-анализа новостных сайтов по противоправному и географическому признаку.

В рамках нашего исследования, мы анализировали потоки новостей и формировали специализированные корпуса текстов на нескольких языках. Тексы корпусов являются материалами новостей с сайтов Казахстана (patrul.kz, Inform.kz, Azattyq.org), Украины (tsn.ua, criminal.tv, 24tv.ua), Великобритании (news.sky.com) и США (foxnews.com, cnn.com), посвященных криминальной тематике. Все перечисленные сайты являются достоверными источниками информации и содержат данные о противоправных (уголовные) действиях той или иной страны.

Для автоматического сбора данных было спроектировано приложение на языке Python, которое позволило считать статьи из указанных сайтов новостей и хранить их в БД [14].

id	head	url	text
5657	В Львове :	https://tsn.ua/ru/ukrayina/v-lvove-zya	Во Львове правоохранители задержа.
5658	В Австрал	https://tsn.ua/ru/svit/v-avstralii-polici	Австралийская полиция изъяла круп
5659	Луценко г	https://tsn.ua/ru/politika/lucenko-pri	Генеральный прокурор Украины Юр
5660	Праздков	https://tsn.ua/ru/ukrayina/prazdnovar	Украинские правоохранители зареги
5661	15 тысяч (	https://tsn.ua/ru/ukrayina/15-tysyach	За пять лет с 2013 по 2018 год в Украи
5662	lazyload c	https://tsn.ua/ru/ukrayina/iz-ukrainy-	Правоохранители Хмельницкой обла
5663	lazyload c	https://tsn.ua/ru/ukrayina/izbil-i-pyta	В селе Армашовка Ширяевского рай
5664	Минздрав	https://tsn.ua/ru/ukrayina/minzdrav-p	Гослекслужба на просьбу Министер
5665	Количеств	https://tsn.ua/ru/ukrayina/kolichestvc	В течение 26 дней предвыборной кам
5666	В Ивано-(	https://tsn.ua/ru/ukrayina/v-ivano-fra	В Ивано-Франковске в воскресенье,
5667	На Днепр	https://tsn.ua/ru/ukrayina/na-dnepro	На в Криничанск

Рисунок 1 - Пример фрагмента БД, в которой хранятся собранные тексты с сайтов новостей Украины.

На сегодня объем корпуса составляет 10 500 текстов, и корпус продолжает непрерывно пополняться. Тексты британских и американских сайтов представлены на английском языке, а тексты казахских и украинских сайтов на русском языке. Тексты корпуса распределены по 4 подкорпусам, отвечающим за каждую из стран. Корпуса используются для создания тематических словарей криминально-окрашенной лексики для двух языков.

В процессе контент-анализа все тексты новостей были проанализированы по видам преступлений. Согласно оценке экспертов, в нашем корпусе преобладают тексты о девяти видах преступления: убийство; похищение или пропажа человека; ДТП; преступления, связанные с несовершеннолетними; хулиганство; мошенничество; кража (грабеж); наркотики; похищение авто.

По перечисленным категориям был сформирован словарь криминально-окрашенных терминов в формате XML по трем частям речи: существительные, глаголы и прилагательные, выделенные типами элементов *<nouns>*, *<verbs>* и <adjectives>, которые сохраняют термы различных частей речи, выделенные тегом *<term>*. Атрибут *id* элемента *<term>* показывает индекс данного терма в под-словаре отдельной части речи (рис. 2).

В свою очередь, тег <term> имеет дочерние элементы *<lemma>* и, *<synset>*, с атрибутом *lang*, значение которого указывает язык. Элемент *<lemma>* показывает термин казахского, русского и английского языков для одного понятия. Элемент *<synset>* включает список синонимов для каждого термина каждого из трёх языков. Тим элемент<domain> указывает одну из подтем, определяющих девять видов преступлений.

```
  <?xml version="1.0" encoding="UTF-8"?>
- <vocabulary>
  - <nouns>
    - <term id="1">
        <lemma lang="ru">стрельба</lemma>
        <domain> MURDER </domain>
        <synset lang="ru">обстрел, выстрел </synset>
        <lemma lang="en">shooting</lemma>
        <synset lang="en">firing, fire, gunfire</synset>
        <lemma lang="ka">атыс</lemma>
        <synset lang="ka">ату, оқ жаудыру, атылыс</synset>
```

Рисунок 2 – Пример фрагмента созданного трех язычного словаря противоправной информации.

На рисунке 3 показано окно пользовательского интерфейса, предназначенного для работы с созданным словарем.

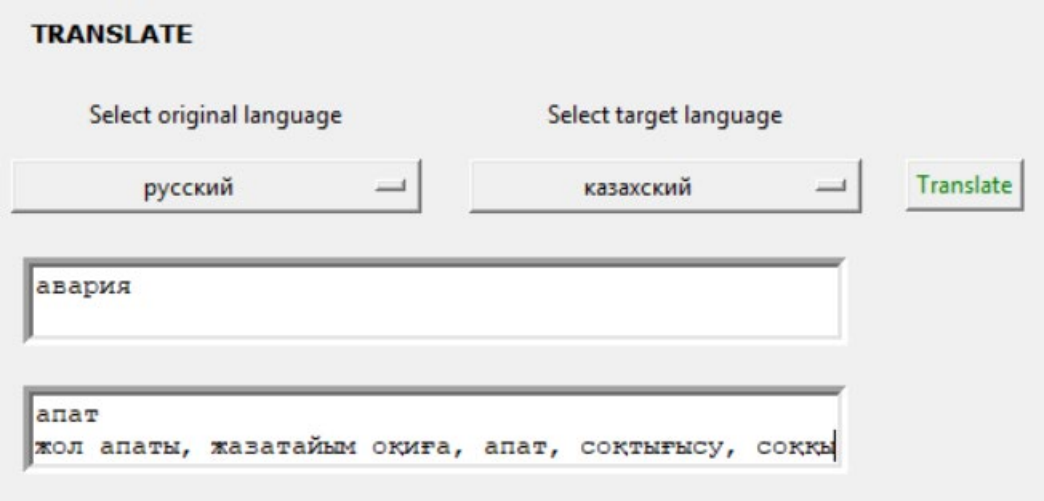


Рисунок 3 – Окно пользовательского интерфейса, предназначенного для работы с созданным словарем.

Мы выделили два вида задач контент-анализа, решаемых с помощью созданного словаря:

1) ранжирование документов по степени тематической схожести; вданном случае мы рассматриваем близость тематики входного текста к девяти определенным выше подтемам (или различным видам преступлений);

2) определение тематической направленности широко-известных новостных сайтов для построения "криминальной картины" той или иной страны и рассмотрения зависимости между преступлениями, их географическим расположением и временем. Мы планируем сопоставить уровни преступности четырех стран (Украина, Казахстан, Великобритания и США) и рассмотреть преступления в их временной зависимости.

Для решения вышеприведенных задач будут использоваться векторные модели слов (*Word2Vec*, *FastText* и т. д.). Для создания так называемых тематических моделей текстов используется пакет *Gensim* - библиотека обработки естественного языка, предназначенная для "Тематический моделирование". С помощью этой библиотеки планируется проанализировать тексты корпусов по криминально-

окрашенной лексике, с использованием словаря, созданного на данном этапе исследования.

Выводы

В последние годы средства массовой информации стали важным и неотъемлемым элементом современного общества. СМИ проникают во все области человеческой деятельности и захватывают все большее информационное пространство. Современное общество принимает средства массовой информации как важный и значительный источник получения знаний о мире и происходящих в нем событиях. В эпоху развития способов коммуникации, СМИ являются "социальным инструментом, обеспечивающим взаимодействие в текстовом формате с целью модификации картины мира индивида". Именно данные черты делают СМИ главным участником процесса формирования общественного мнения, культуры и мировоззрения людей и требуют изучения, глубокого анализа и осмысления роли языка СМИ.

Одним из современных и эффективных методов такого изучения является контент-анализ или так называемый анализ содержания. Он представляет собой процедуру анализа различных видов текстов (вербальных и визуальных), позволяющую анализировать взаимодействие, лежащее между коммуникатором и аудиторией. Проведенное исследование показывает, что контент-анализ является более результативным методом анализа средств массовой информации чем, например, опытный метод, поскольку он не вмешивается в то, что изучает, а позволяет анализировать большие объемы текстовой информации, выделяя в ней основные аспекты, которые не видны невооруженным глазом.

В результате проведенного анализа показано, что использование контент-анализа позволит получить достоверные результаты по определению картины противоправной информации, представленной на новостных сайтах Казахстана, Украины, Великобритании и США. А также осуществить последующий анализ текстов сайтов и их классификацию по временным, географическим и тематическим (уровень различных видов преступлений) критериям. Проводимый контент-анализ базируется на выделения криминально-окрашенной лексики новостных сайтов, включенной в разработанный словарь криминально-детерминированных термов, оформленный в формате XML. Словарь разработан для казахского, русского и английского языков, и включает синсеты для каждого термина каждого языка. Словарь дополнительно упорядочен по частям речи и видами преступлений.

Литература

1. Steven E. Stemler (2001), “An Overview of Content Analysis”, Practical Assessment, Research & Evaluation, 7(17)] Available online: http://PAREonline.net/getvn.asp?v=7&n=17.

2. Klaus H Krippendorff (2013), “Content Analysis - 3rd Edition: an Introduction to Its Methodology”, Thousand Oaks: SAGE Publications, Inc, 422 p.

3. Steven E. Stemler (2015), “Emerging Trends in Content Analysis”, Emerging Trends in the Social and Behavioral Sciences: An Interdisciplinary, Searchable, and Linkable Resource, pp. 1-14.

4. Daniel Riffe, Stephen Lacy and Frederick Fico (2014), “Analyzing Media Messages Using Quantitative Content Analysis in Research”, Routledge, 200 p.

5. Walter L. Perry, Brian McInnis, Carter C. Price, Susan Smith, John S. Hollywood (2013), “Predictive Policing Forecasting Crime for Law Enforcement”, RAND Corporation, 4 p.

6. Chelsea H. Smith, Adam Lankford (2016), “The linguistics of terror: a content analysis of suicide notes and martyr manifestos”, the Department of Criminal Justice in the Graduate School of The University of Alabama, 67 p.

7. Hossein Hashemnezhad (2015), “Qualitative Content Analysis Research: A Review Article”, Journal of ELT and Applied Linguistics (JELTAL), pp. 54-62.

8. Berg, B.L. (2001), “Qualitative Research, Message for the Social Sciences”, 4th Edition, Allin and Bacon, pp. 15-35.

9. Mayring P. (2000), “Qualitative Content Analysis”, Forum Qualitative Sozialforschung, 10 p.

10. Hsiu-Fang Hsieh, Sarah E Shannon (2005), “Three Approaches to Qualitative Content Analysis”, Qualitative Health Research, pp. 1277-1288.

11. H. Andrew Schwartz, Lyle H. Ungar (2015), “Data-Driven Content Analysis of Social Media”, The Annals of the American Academy of Political and Social Science, pp. 78-94.

12. Hea-Jin Kim, Yoo Kyung Jeong and Min Song (2015), “ Topic-based content and sentiment analysis of Ebola virus on Twitter and in the news”, Journal of Information Science, pp. 2-20.

13. Chen, S. (2016). “Language and ecology: A content analysis of ecolinguistics as an emerging research field”, Ampersand 3, pp. 108-116.

14. Khairova N., Kolesnyk A., Mamyrbayev O. and Mukhsina K., (2019), “The Aligned Kazakh-Russian Parallel Corpus Focused on the Criminal Theme.” COLINS, pp. 116-125.

TECHNIQUES FOR THE EXPLORATION OF PIEZOELECTRIC HARVESTERS

Erol Kurt
ekurt@gazi.edu.tr
Department of Electrical and Electronics Engineering, Technology Faculty, Gazi University, Ankara, Turkey,

Abstract

Analytical and numerical techniques for the design and optimization of piezoelectric harvester (PH) systems are considered. Initially the approaches on how to start with an initial design are explained. Later on, the techniques to improve the starting design are reported. Especially the applications of finite element analysis (FEA), and time-integration schemes are focused together with the required analytical methods. There exist many tools to implement the time integration, however from the point of engineering, MatLab tool is the most preferable. In the case of FEA, mainly the Maxwell 3D package programme is explained in the present chapter. A route to get the optimized harvester devices is discussed gradually. In the time integration method, the description of dimensionless equations of motion, electricity and magnetic equations are given for the future possible applications.

The cantilever structure of piezoelectric materials are widely considered in the literature. The time-dependent solutions of the systems are sampled and possible future applications are underlined. Following the mechanical design, the ferromagnetic and non-magnetic parts should be clearly identified for the electromagnetic design if the device uses a magnetic component. Each design has its own magnetic flux path, magnetic field density values and magnetic. In order to provide a concrete device, following the analytical description, 2D or/and 3D designs should be drawn under a package programme working with FEA. Magnetostatic and magnetodynamic solutions are required in order to get the voltage and current output from the system. Besides, a time-dependent solution via a MatLab code can be applied. Before any practical application, theoretical works on the considered harvesters give a chance to the engineers to use the budget and time efficiently.

Keywords*: piezoelectric, mode, Matlab, harvester, finite element, power, Maxwell*

CLASSIFICATION OF TEXURES ON THE BASE OF MACHINE LEARNING ALGORITHMS

[1]G. Taubayev, [2]A.L. Bychkov, [3]F.A. Murzin, [3]N.E. Russkikh, [2]E.I.Ryabchikova, [3]S.S. Khairulin, [1]G.B. Abdikerimova

E-mail: [1]galymzhan001@gmail.com, [2]bychkov_a@solid.nsc.ru, [3]murzin@iis.nsk.su, [3]russkikh.nikolay@gmail.com, [2]lenryab@niboch.nsc.ru, [3]s.khayrulin@gmail.com, [1]gulzira1981@mail.ru

[1] L.N. Gumilyov Eurasian National University, Department of Information Systems, Astana, Kazakhstan

[2] Institute of Solid State Chemistry and Mechanochemistry SB RAS

[3]A.P. Ershov Institute of Informatics Systems SB RAS, Novosibirsk, Russia

Abstract. *The aim of the research is to develop algorithms for analyzing images obtained from various sources. The paper analyzes images of the ultrastructure of plant cell walls, obtained by transmission electron microscopy of plant raw materials, after various physicochemical and/or mechanochemical processing. The main focus is on the development of classification methods based on machine learning models. There were used learning traditional classifiers and learning deep convolution neural networks. The question of the applicability of methods for learning neural networks with many hidden layers, united under one term "deep learning" is investigated. The optimal parameters of the classifiers were selected automatically using the GridSearch function of the Sklearn software package. The work was carried out for the Institute of Solid State Chemistry and Mechanochemistry of the Siberian Branch of the Russian Academy of Sciences. The study was supported by a grant from the Russian Science Foundation (project No. 16-13-10200).*

Keywords: *textural images, texture features, electronic microscopy, Deep learning, Random forest*

Introduction

Research is aimed at creating a scientific and technical groundwork in the field of image processing of texture type [1-4]. The aim of the research is to develop and search algorithms for analyzing images obtained from various sources, for example, using modern

electron microscopic methods. In particular, images of the ultrastructure of plant cell walls, obtained by transmission electron microscopy of plant materials, after various physicochemical and/or mechanochemical processing are analyzed.

The work was carried out for the Institute of Solid State Chemistry and Mechanochemistry of the Siberian Branch of the Russian Academy of Sciences. The study was supported by a grant from the Russian Science Foundation (project No. 16-13-10200).

For the moment, there is a need in the world for the development of new functional, curative and prophylactic and sports food containing biopolymers hydrolysates, especially proteins and carbohydrates, in a digestible form.

The scientific problem, the solution of which is assumed in the project, is that the methods of hydrolysis, segregation and purification currently used for the processing of agricultural products do not allow us to process raw materials comprehensively, to involve hardly hydrolysable and nonreactive substances in the process, and to increase the reactions selectivity in a number of cases.

The liquid-phase chemical and biotechnological approaches aimed at intensifying liquid-phase hydrolysis have largely exhausted the resource. The increase of temperature of liquid-phase hydrolysis leads to partial decomposition of amino acids and the production of by-products (often allergens), the use of pure enzyme preparations with high hydrolase activity increases the cost of the product, additional segregation and purification steps complicate the technology and adversely affect the environment (organic solvents, effluents, by-products).

The proposed project aims at studying the processes occurring during solid-phase mechanical activation and the subsequent heterogeneous enzymatic hydrolysis of protein plant material. Fundamental knowledge obtained is able form the basis for new technologies for effective processing of agricultural products, the creation of safe and high quality, including special (functional) food products.

The existence of this problem can be explained by the complicacy of studying plant raw materials. It has several levels of structural organization: "plant tissues - cells - cell walls - polymer components of cell walls". By the way, quantify specific character is made by heterogeneous reactions, which are adverse for classical solution chemistry and biotechnology, and which limit the rate of the process with low reactivity of polymers in the solid phase state, contribute to certain specificity.

This brings us to the study of texture-type images. Really in the current time, these investigations are in demand by scientists from various fields – chemists, biologists, technologists, but often such images are processed manually at a qualitative (rarely semi-quantitative) level [5-6]. The transition to algorithms that allow operating with large amounts of data would allow us the listed areas of science to take a significant step forward, to improve existing and create new technological processes.

In this work, we continue the research presented in [7-10], passing to new more modern methods. The tasks of understanding an image at a high level, one way or another, are related to the classification and categorization of the entire image, its parts or each pixel. Therefore, in the development of computer vision, machine learning and its universal algorithms for classification, clustering, as well as artificial neural networks played an important role [11-19]. To obtain good results in the accuracy of object recognition, machine learning algorithms require a large amount of labeled (marked) data for training (learning).

The progress we are making today with deep learning [17] is that it allows computational models with multiple processing layers to learn representations of data with

multiple levels of abstraction. Conventional machine learning methods tend to be limited in their ability to process raw data in its original form. Deep learning methods are learning methods with multiple layers of data analysis, obtained by composing simple but non-linear modules, each of which transforms data at one level into data at a higher, slightly more abstract level. By combining a sufficient number of such transformations, very sophisticated recognition methods can be "trained".

For classification tasks, higher levels of representation enhance input features that are important for discrimination and suppress irrelevant changes and noise. A key aspect of deep learning is that it learns from the raw data provided using a common known learning algorithm.

In our investigations, the learning algorithms use vectors containing sets of texture features (18 in total) or models using fragments (samples) of 64x64 pixels. In particular, microphotographs of sections of the straw cell wall are considered. Specialized software was developed that allows us to select fragments (samples) of 64x64 pixels in a photograph (Fig. 1) in order to create training samples.

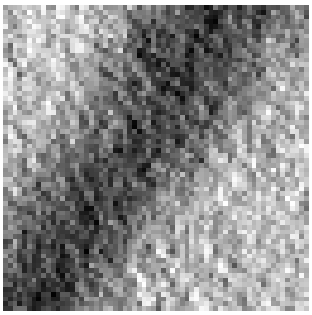


Figure 1. Example of sample

Each sample was assigned a corresponding class number. In total, 10 classes are considered, and their list is given below.

1. Gelatin.
2. Holes.
3. The grid.
4. Unformed material on the wall surface.
5. The cell wall is striped: the border between the electron-transparent layer and the layer of average electron density.
6. Cell wall: electron-transparent layers.
7. The wall is not striped.
8. Plant material that does not have an ordered (striped) structure (outside the walls).
9. Biological admixtures.
10. Resin without gelatin.

A total of 9979 samples were prepared. The diagram below shows the number of representatives of different classes (Fig. 2). Note that Type 3 samples were not prepared.

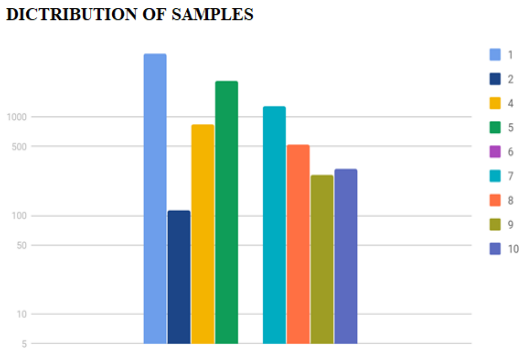


Figure 2. Distribution of samples in the training selection

It is planned that the characteristics of textural features obtained for various images (entropy, order/disorder ratio, proportion of zones with an "abnormal" texture, etc.) or fragments of images can be further correlated with values characterizing the physicochemical properties of the analyzed material: reactivity, porosity, diffusion coefficient, etc.

To carry out the correlation, also it will be possible to use machine learning algorithms, for example, based on a neurocomputer approach. So, having the learned system on a dataset, it will then be possible to make predictions regarding the physicochemical properties of materials in demand in the chemical industry. Application of machine learning methods, i.e. in fact, artificial intelligence methods in the classically applied methods of physicochemical analysis are the most interesting part of the project.

Software products that allow detailed analysis of textures can be successfully applied in various fields of science and industry. First of all, it is chemistry and materials science. You can analyze organic materials, sections of metals and minerals, ceramics, etc.

The range of tasks is not limited to the analysis of micrographs. So, when processing aerospace images, researchers also deal with different textures. It is possible to identify a coniferous or deciduous forest, fields sown with grain or legumes, etc. You can also distinguish a forest affected by pests, deserted areas.

Modfels based on traditional classifiers

Basic difference of ideas of our project from existing analogues consists in the correct application of mathematical methods and in their deeper study. For example, it is known more than two hundred textural features. In scientific reviews, usually about fifty are mentioned. During too time, in practice, as a rule, 3-4 features are used, for example, at processing of space photos. That is they remain not investigated to the full.

The same it is possible to tell about application of integral transformations. For example, at research of durability of metals under loadings Haar transformation is used to characterize cracks. The question, what information can be received on the basis of other transformations almost is not studied. In the literature in wood chemistry it is spoken about utility of the R/S-analysis and fractal analysis for corresponding researches, but data have a sketchy character.

In our project, it is offered to approach in a complex to the given questions, i.e. to consider a big number of features, big number of transformations and create algorithms and programs, applicable for the decision of a wide class of problems.

In particular based on the available samples, several traditional classifiers [11-19] were trained: Random forest classifier, Gradient boosting, KNN (K nearest neighbors method), Deep learning (based on a multilayer [20-29] convolution neural network).

Random forest is a machine learning algorithm based on the use of an ensemble of decision trees. The algorithm is used for classification, regression and clustering problems. The main idea is to use a large ensemble of decision trees, each of which by itself gives a very low quality of classification, but due to their large number, the result is good.

Gradient boosting. Most boosting algorithms consist of iterative learning of weak classifiers in order to assemble them into a strong classifier. When they are added, some weights are usually to them given that are usually related to learning accuracy. After the weak classifier is added, the weights are recalculated, which is known as "recalculation of weights". Incorrectly classified input gains more weight, and correctly classified instances lose weight. Thus, subsequent learning focuses more on examples where the previous weak learning gave a misclassification.

KNN (K Nearest Neighbor Method) is the algorithm for automatic feature classification or regression. In the case of using the method for classification, the object is assigned to the class that is most common among the neighbors of this element, whose classes are already known. In the case of using the method for regression, the object is assigned the average value over the objects closest to it, the values of which are already known. The algorithm can be applied to samples with a large number of attributes (multidimensional). To do this, before using it, you need to set the distance function. The classic version of such function is the Euclidean metric.

Deep learning (deep learning based on a multilayer convolutional neural network) is characterized as a class of machine learning algorithms that is based on the use of neural networks.

The algorithm uses a multilayer nonlinear filter system for feature extraction. Each subsequent layer receives the output of the previous layer as input. That is, the features are organized hierarchically; the characteristics of a higher level are derived from characteristics of a lower level. Layers correspond to different levels of abstraction, in other words, layers form a hierarchy of concepts. A deep learning system can combine supervised and unsupervised learning algorithms. Sample analysis can be interpreted as unsupervised learning and classification as supervised learning.

The first option we considered. The element of the training sample is a vector, each component of which is the value of the corresponding texture feature taken over the entire sample. A total, 18 features were used. Since the number of samples in some classes in the samples is insignificant, and the entire selection is not correctly formed (balanced) in terms of quantity, it was decided not to consider small classes and among the remaining classes to choose an equal number of samples in each. Thus, only classes remained in the training sample: 1, 4, 5, 7, 8, 9, 10.

The number of samples in each class was taken equal to 520. Each sample was divided into training – 80% and test – 20%. The optimal parameters of the classifiers were selected automatically using the GridSearch function of the Sklearn software package. At the same time, the algorithms showed the following accuracy in determining the classes.

Random forest – 0.76;

Gradient boosting – 0.75;

K nearest neighbors – 0.72.

Texture features

Below is a list of texture features that were used in the algorithms.

The standard approach for calculating texture features is as follows. It is necessary to select the so-called running (or sliding) window with an odd side: 3, 5, 7 pixels. The feature is calculated inside the running window. The size of a local fragment is important to reflect correctly the texture properties.

The value of feature is written into a new matrix of the same size as the original one. In the new matrix, the value is written to a point with coordinates equal to the coordinates of the center of the running window. The elements of the new matrix are obtained in some interval [A, B]. Further, usually this interval is linearly mapped into the interval [0, 255]. After that, it is possible to visualize the result of calculating the texture feature.

The standard approach in our case is not very informative. Therefore, it was decided to use a non-standard approach. Namely, texture features are calculated over large windows (including non-square ones), which the user can specify by selecting an area that may be of interest to him. That is, we are talking about calculating numerical characteristics related to vast areas, including various kinds of artifacts. The 18 most important texture features are considered, and all of them are implemented in the program.

Attributes based on statistical characteristics

As such features, statistical characteristics of spatial distributions can be used, calculated as measures of homogeneity from a one-dimensional histogram of signal values (characteristics of the 1st order) and from two-dimensional histograms of signal values (characteristics of the 2nd order). Thus, the following statistical characteristics can be used as numerical texture estimates from a one-dimensional histogram:

the k-th moment

$$T_1^k = n^{-2}\sum_{i=1}^{n}\sum_{j=1}^{n}[f(i,j)]^k ,$$

entropy

$$T_2 = -\sum_{g=0}^{N-1} F(g)\log_{10} F(g),$$

energy

$$T_3 = \sum_{g=0}^{N-1}[F(g)]^2 ,$$

variation

$$T_4 = -\sum_{g=0}^{N-1}(g-\mu)^2 F(g),$$

where n is a window size in pixels,
$f(i,j)$ is a pixel brightness at a point (i,j),
N is the number of image brightness gradations,
$F(g)$ is the number of pixels having a brightness g,
μ is average brightness in the window.

The analysis shows that the texture estimates given above and calculated from a one-dimensional histogram of frequencies do not take into account the mutual arrangement of neighboring pixels in the window and only allow us to estimate the group properties of the

pixels that are part of a particular image. Thus, these estimates are effective only for describing textures with unexpressed spatial regularity.

Features that take into account the relative position.

One aspect of texture is related to the spatial distribution and spatial interdependence of the brightness values of the local area of the image with increasing distance between the estimated points. In coarse-grained textures, the brightness distribution changes much more slowly than in fine-grained ones.

The statistics of spatial interdependence of the brightness values between the nearest neighboring points are used. The adjacency matrix (or co-occurrence matrix) of brightness levels is an estimate of the second-order probability density distribution obtained from the image under the assumption that the probability density depends only on the location of two pixels.

For the formation of texture features that take into account the mutual arrangement of pixels within the sliding window, an approach based on an adjacency matrix is used. Another name is a gradient distribution matrix. In what follows, we will use the name of an adjacency matrix.

Let the analyzed image be a rectangle and has N_x horizontal elements and N_y vertical elements. Further $G = \{1,2,...,N\}$ is a set of N quantized brightness values. Then the image is described by a function from the set G into the set of brightness values, that is, $f : L_x \times L_y \to G$ where $L_x = \{1,2,...,N_x\}$ and $L_y = \{1,2,...,N_y\}$ are the horizontal and vertical spatial regions, respectively.

For each pixel in the image, we define the concept of a neighbor. This is a pixel different from the considered one, the coordinates of which in sets L_x and L_y differs by no more than 1 from the coordinates of the considered pixel. Thus, all non-bordering pixels of the image have 8 neighbors (Fig. 3)

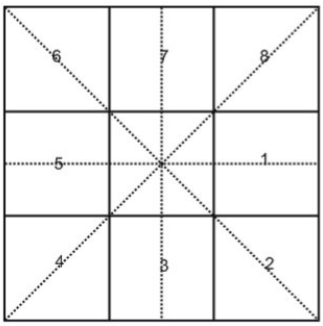


Figure 3. Adjacent pixels

Let us divide 8 adjacent pixels into 4 classes depending on how they border on the pixel in question. Neighbors numbers 1 and 5 will fall into the first class, numbers 4 and 8 in the second, numbers 3 and 7 in the third, numbers 2 and 6 in the fourth. The classes, respectively, can be called classes of directions 0, 45, 90 and 135 degrees.

The concept of a neighbor can be generalized to pixels located at a distance d from each other. We will be interested in pixels located at a distance $d = 1$ from each other and belonging to the same class of directions.

The adjacency matrix contains the relative frequencies p_{ij} of the presence in the image of neighboring elements located at a distance d from each other, with brightness $i, j \in G$. Usually there are horizontal ($\alpha = 0^\circ$), vertical ($\alpha = 90^\circ$) and cross-diagonal ($\alpha = 45^\circ$ and $\alpha = 135^\circ$) pairs of elements. It should be noted that these matrices are symmetric, namely $P(i, j, d, \alpha) = P(j, i, d, \alpha)$.

Since the number of such matrices can be very large, it is usually limited to only considering the pixels in close proximity, or the values of the elements in the matrices composed for different orientations are averaged.

Further it is shown an example (Fig. 4) of the formation of a matrix with parameters $d = 0$ and $\alpha = 0$. This is a methodological example, 8 gradations of brightness are used.

In general case, the matrix size is determined by the number of image brightness gradations. The value of each element of the matrix is equal to the number of occurrence of a pair of pixels with the corresponding values of the intensities in the given positions relative to each other.

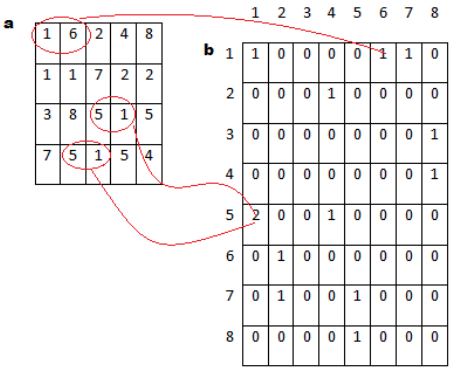


Figure 4. An example of forming an adjacency matrix

For example, the occurrence of a pair with the value (1,6) in the original image, provided that an adjacent pair is located on the same line, is equal to1, and the occurrence of a pair with a value of (5,1) is 2.

The resulting matrix is reduced to a normalized matrix:

$$p(i, j, d, \alpha) = \frac{P(i, j, d, \alpha)}{\sum_i \sum_j P(i, j, d, \alpha)}.$$

On the base of calculated adjacency matrices, it is possible to directly calculate the following texture features:

the average

$$T_5 = \mu_i = \mu_j = \sum_{i=0}^{N-1} \left[i \sum_{j=0}^{N-1} p(i, j) \right],$$

energy

$$T_6 = \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} [p(i, j)]^2,$$

variation

$$T_7 = \sigma_i^2 = \sum_{i=0}^{N-1} \left[(i - \mu_2)^2 \sum_{j=0}^{N-1} p(i, j) \right],$$

uniformity

$$T_8 = \sum_{i=0}^{N-1}\sum_{j=0}^{N-1} p(i,j)/(1+|i-j|),$$

where $p(i,j)$ is the frequency of appearance of two pixels in a window with brightness i and j at an angle α at a distance *d*. Note that here new notions of energy and variation are defined.

Let σ_i be the standard deviation of the brightness in the window.

Statistical moments make possible to form texture features that take into account the relative position of neighboring pixels in the window, and accordingly, are effective for describing textures with pronounced spatial regularity.

The second angular moment

$T_9 = \sum_{i=1}^{N}\sum_{j=1}^{N}(p(i,j)/M)^2$, where M is the total number of the pairs adjoining to each other of elements (for example, for *d*=1, $\alpha = 0$, $M = 2N_y(N_x - 1)$ is a measure of uniformity (homogeneity) of the image and accepts in this case the minimum value.

Contrast $T_{10} = \sum_{n=0}^{N-1} n^2 \left[\sum_{i=1}^{N}\sum_{j=1}^{N} p(i,j)/M\right]$, $|i-j| = n$, is defined by a size of local variations of brightness of the image. With increasing the number of local variations, contrast increases.

Correlation coefficient $T_{11} = \sigma_x^{-1}\sigma_y^{-1} = \sum_{i=1}^{N}\sum_{j=1}^{N}[ij(p(i,j)/M) - m_x m_y]$, where m_x, m_y, σ_x, σ_y are average values and root-mean-square deviations for $p_x(i) = \sum_{j=1}^{N} p(i,j)/M$ and $p_y(j) = \sum_{i=1}^{N} p(i,j)/M$ accordingly. T_{11} serves as a linearity measure of a regression dependence of a brightness on the image

Dispersion $T_{12} = \sum_{i=1}^{N}\sum_{j=1}^{N}(i-m)^2(p(i,j)/M)$ defines variations of brightness concerning average value.

Reverse moment $T_{13} = \sum_{i=1}^{N}\sum_{j=1}^{N}[1+(i-j)^2]^{-1}(p(i,j)/M)$ is closely connected with contrast and reflects a disorder degree of elements of a gradients matrix round the main diagonal. This feature is alternative to a contrast in a case of influence of regional structures, as rather big differences in values of brightness bring the minimum contribution to an end result.

Total average

$T_{14} = \sum_{n=2}^{2N} np_+(n)$, where $p_+(n) = \sum_{i=1}^{N}\sum_{j=1}^{N} p(i,j)/M$ at *i*+*j*=*n*, *n*=2,…,2*N* is the histogram of the sums of values of brightness. T_{14} is defined by the histogram of the sums of values of brightness $p_+(n)$ on pairs of elements of the image which is directly connected with a contiguity matrix.

Total dispersion $T_{15} = \sum_{n=2}^{2N} (n - T_{14})^2 p_+(n)$ serves as a measure of a variation of brightness concerning a total average.

Total entropy for the histogram of the sums of values of brightness $T_{16} = \sum_{n=2}^{2N} p_+(n) \log p_+(n)$ is defined by a classical measure of the statistical theory of the information and expresses the non-uniformity of a distribution brightness properties of elements of the image.

Entropy of Haralick $T_{17} = -\sum_{i=1}^{N} \sum_{j=1}^{N} (p(i,j)/M) \log(p(i,j)/M)$ is defined the same as also total entropy, but only for a contiguity matrix.

Difference dispersion $T_{18} = \sum_{n=0}^{N-1} \left[n - \sum_{m=0}^{N-1} p_-(m) \right]^2 p_-(n)$, $|i - j| = m$ is expressed through the histogram of differences of values of brightness $p_-(n) = -\sum_{i=1}^{N} \sum_{j=1}^{N} P(i,j)/M$ on steams of elements of the image

Difference entropy $T_{19} = -\sum_{n=0}^{N-1} p_-(n) \log p_-(n)$ pays off as total entropy and entropy for a contiguity matrix, but for the histogram of differences of values of brightness. Usually we do not use this characteristic, but in principal, it is interesting.

The problem of choosing informative features. It should be noted that not all considered texture characteristics are equally informative when classifying certain textures. Therefore, to increase the efficiency of algorithms, it is necessary to solve the problem of analyzing the information content and optimizing the system of features. The main issue when constructing a system of features is to determine which and how many features need to be selected for a reliable classification of objects in the image. In this case, one should be guided by the principle of taking into account the properties of the object's regularity. If the classified object has some regularity, then this regularity must be taken as the basis for the formation of a system of features. Moreover, it is necessary to ensure that this regularity is inherent in all objects belonging to a given class.

There is no formal procedure for selecting a system of features. The features used in solving certain problems are set only on the basis of the experience and intuition of a specialist. From the source system selected in this way, then in one formal way or another, a more economical and most informative subsystem of features for describing images is selected. The very process of specifying the initial system is not formalized in any way. There is an opinion that it is necessary to use everything that can only be suspected of being informative. But this is only true in principle. In practice, excessive inflation of the original system of features is not harmless. In the case of using some decision functions, adding features with a small learning sample may not only not improve, but even worsen the quality of learning.

Calculation examples
Random forest classifier

For the Random forest method, the number of decision trees parameter was varied. The optimal number was determined to be 200. The results of applying the Random forest classifier are shown below (Fig. 5, 6). The results of other algorithms are shown next to it (Fig. 7, 8).

To mark up the image (Fig. 6–8), the same colors are used as in the diagram (Fig. 2).

The algorithms showed the accuracy of determining the classes on the validation set equal to approximately 75%.

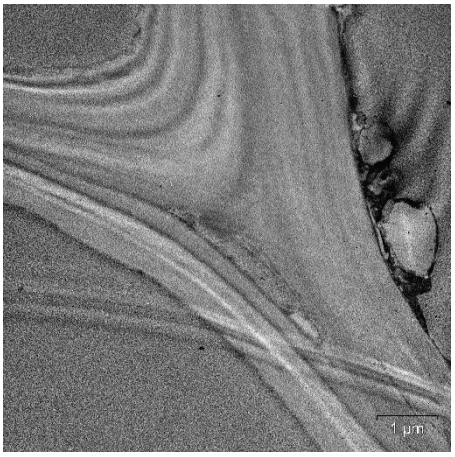


Figure 5. The initial image

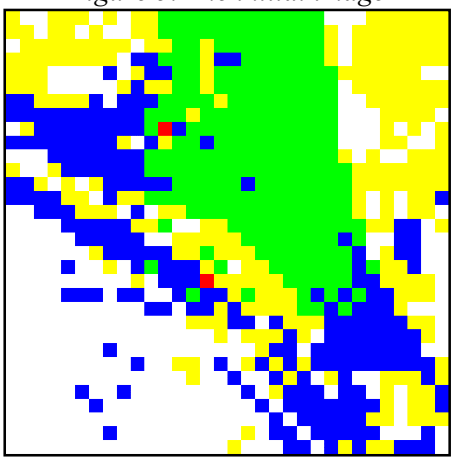


Figure 6. The result of marking a photo using the Random forest method

Gradient boosting

For gradient boosting, the parameter varied – the number of solvers.

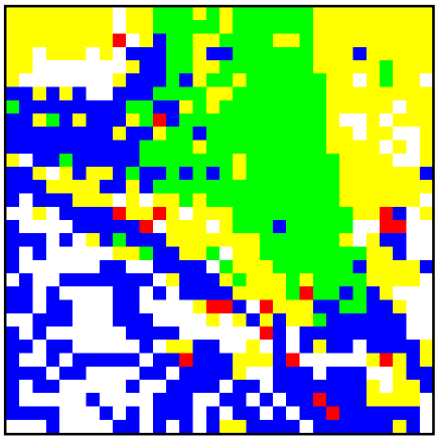


Figure 7. The result of marking the photo with the Gradient boosting classifier

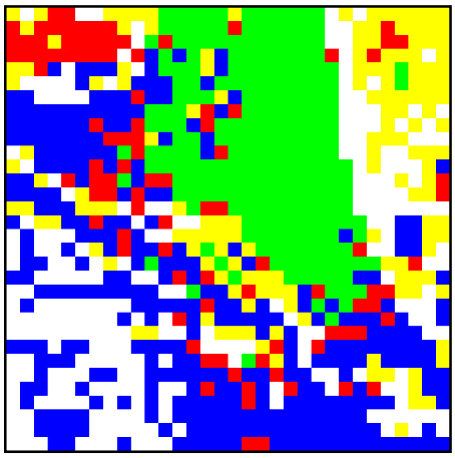


Figure 8. The result of marking the photo with the KNN classifier. The optimal number turned out to be 5.

Deep learning

A multilayer convolution neural network has been implemented. It allowed us to find the contours of the cell walls (Fig. 9).

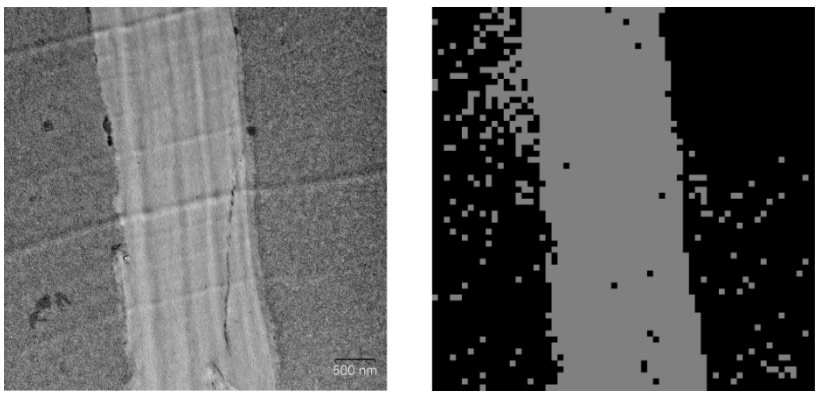


Figure 9. Results of working neural network

The architecture of the neural network is quite complex, so we will omit it from consideration. Below are examples of how the algorithm works.

Model on the base of convolution neural network

For classification, a neural network model was used, which has 5 convolution layers. The first layer contains filters of size 4, the rest – filters of size 16. On all layers, excepting the last one, there are 20 filters with ELU activation function. The last layer has 10 layers (according to the number of classes) and Softmax activation. Each layer uses the so-called batch normalization.

Data. For training the model, data consisting of 9598 samples of 64 by 64 pixels were used, as before, 10 classes were considered.

1. Gelatin (4137 samples).
2. Holes (111 samples).
3. Grid (0 samples).
4. Unformed material on the wall surface (819 samples).
5. The cell wall is striped: the border between the electron-transparent layer and the layer of average electron density (2243 samples).
6. Cell wall: electron-transparent layers (0 samples).
7. The wall is not striped (1274 samples).
8. Plant material without an ordered (banding) structure (outside the walls) (464 samples).
9. Biological admixtures (257 samples).
10. Resin without gelatin (293 samples).

The samples were divided into training and validation sets in a 3: 1 ratio so that the proportions within the classes were the same. The model was learned over 250 epochs with categorical cross-entropy as a loss function using the Adam optimizer with an initial learning rate of 0.0001. After each epoch, the learning rate multiplied by 0.99. The batch size was chosen equal to 64. Data augmentation was used during learning (reflections along the vertical and horizontal axes, transposition, rotations, brightness fluctuations and random Gaussian noise).

Data augmentation is an important step in training machine learning models. Data augmentation refers to increasing the data sample for training by modifying existing data.

We also used test-time augmentation – reflections and transposition. This is a way to improve the quality of the classifier through averaging. After learning, the model with the highest accuracy was selected on the validation set.

The algorithms showed the accuracy of determining the classes on the validation set equal to 79.4%. Since the model is fully convolution model, we have the ability to use it to classify each pixel in the entire image. Below is an example of the classification, and you can see the result in the following pictures (Fig. 10–12).

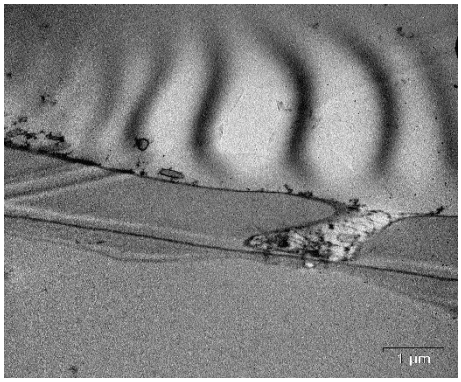


Figure 10. The initial Image

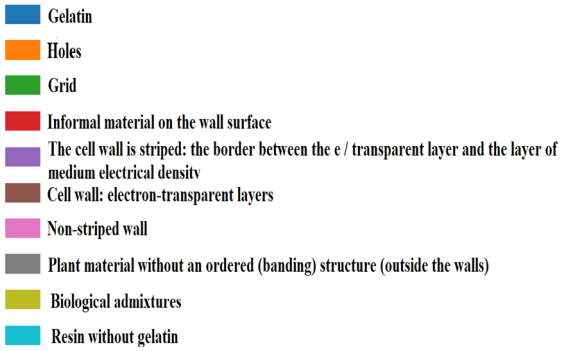


Figure 11. Color palette used to visualize result

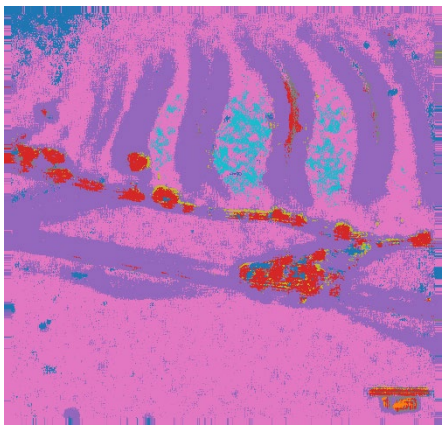


Figure 12. Results after applying neural network

Conclusion

The proposed project aims at studying the processes occurring during solid-phase mechanical activation and the subsequent heterogeneous enzymatic hydrolysis of protein plant material. The peculiarity approach is the consideration of natural polymers and plant materials – traditional objects for biotechnology – from the standpoint of solid state chemistry and materials science that to be applied [30-37].

Knowledge, experience and methods of studying heterogeneous processes occurring at the solid-liquid interphase and one often are the limiting stage are applied. The selected objects in this work is presented presented as a sophisticated and organized at the supramolecular level complex of polymers with a different chemical composition. Fundamental knowledge obtained is able form the basis for new technologies for effective processing of agricultural products, the creation of safe and high quality, including functional, food products.

The work is devoted to the study of texture images. The source is microphotographs of plant raw materials, ground by special mills. The work was carried out for the Institute of Solid State Chemistry and Mechanochemistry of the SB RAS.

The main result is two approaches to solving the problem of classifying and finding the contours of cell walls. Traditional classifiers and deep convolution neural networks were used, which assume a large number of training annotated data. The learning algorithms use vectors containing sets of texture features (18 in total) and models working with fragments (samples) of 64x64 pixels. During learning, data augmentation was used: reflections along the vertical and horizontal axes, transposition, rotations, brightness fluctuations and random Gaussian noise.

In this work, the following problems were solved.

1. Several traditional classifiers were learned: Random forest classifier, Gradient boosting, KNN (method of K nearest neighbors), Deep learning (based on a multilayer convolution neural network).

2. Deep convolution neural networks were learned using data, consisting of 9598 samples of 64 by 64 pixels. There were considered 10 classes.

3. Many computational experiments were carried out for the comparative analysis and evaluation of the results of the classifiers.

4. The developed methods made it possible to determine the classes with an accuracy of 79.4% and to find contours of the cell walls.

The results of work can be applied in the automated systems of the analysis of images applied in scientific researches and in the industry. Application in the industry allows us to reduce the price of the analysis of the quality of the production and in some cases to raise the quality. Implementation of obtained results in systems of gathering, processing and transferring information will promote a development of a scientific and technological complex. New effective algorithms and program systems will allow us to reach technical, technological, technical and economic successes.

References

[1] H.A. Andreev, O.V. Bazarskii, A.S. Hlauberman, A.I. Kolesnikov, Yu.V. Korzhik, Ya.L. Khliavich, Analysis and synthesis of random spatial textures. Foreign radio electronics. Vol. 2, 1984, pp. 3-33.

[2] R.M. Haralick, Statistical and structural approaches to the description of textures. TIIER. Vol. 67(5), 1979, pp. 98-119.

[3] A.A. Potapov, New information technologies based on probabilistic textural and fractal features in radar detection of low contrast targets. Radiotechnology and electronics. Vol. 48(9), 2003, pp. 1101-1119.

[4] N.V. Kolodnikova, Survey of texture attributes for image recognition problems. Reports of TUSUR: Automated systems for information processing, control and design. 2004, pp.117-118.

[5] A.P. Karmanov Lignin. Structural organization and self-organization. Syktyvkar:

Institute of Chemistry of the Komi Scientific Center of the Ural Branch of the Russian Academy of Sciences, Syktyvkar. 1999, pp. 66-67.

[6] A.P. Karmanov, D.V. Matveev, Problems of wood chemistry and wood chemistry. Institute of Chemistry of the Komi Scientific Center of the Ural Branch of the Russian Academy of Sciences, Syktyvkar. 2001, pp. 50-52.

[7] G.B. Abdikerimova, F.A. Murzin, A.L. Bychkov, W. Xinyu, E.I. Ryabchikova, T. Ayazbayev, The analysis of textural images on the basis of orthogonal transformations. Journal of Theoretical and Applied Information Technology. Vol. 96, Iss. 1, 2019, pp. 16-22.

[8] G.B. Abdikerimova, A.L. Bychkov, S.S. Khayrulin, F.A. Murzin, N.E. Russkikh , E.I. Rybchikova , W. Xinyu, Analysis of images obtained by the transmission electronic microscopy. Materials Today: Proceedings. Iss. 12, 2019, pp. 90-92.

[9] G.B. Abdikerimova, F.A.Murzin, A.L. Bychkov, S.S. Khayrulin, Wei Xinyu, N.E. Russkikh , E.I. Rybchikova, Software tools for cell walls segmentation in microphotography. Journal of Theoretical and Applied Information Technology. Vol.96, Iss. 15, 2018, pp. 4783-4793.

[10] G. Abdikerimova, A. Bychkov, W. Yu, F. Murzin, N. Russkikh, S. Khairulina, E. Ryabchikova, Algorithms and software for the analysis of disordering the structure of cellular walls. Bulletin of the Novosibirsk Computing Сепter. Series: Computer Science. Vol. 40, 2016, pp. 1-14.

[11] A. Smola, S.V.N. Vishwanathan, Introduction to machine learning. Cambridge Univ. Press. 2008, pp.150-151.

[12] X. Wu, V. Kumar, R. Quinlan, J. Ghosh, Y. Qiang, M. Hiroshi, G.J. McLachlan, Ng Angus, B. Liu, Ph. Yu, Zh. Zhou, Top 10 algorithms in data mining. Knowledge and Information Systems. No14 (1), 2008, pp. 1-37.

[13] L. Rokach, O. Maimon, Data mining with decision trees: theory and applications. World Scientific Pub Co Inc. 2008, 305 p.

[14] C. Cortes, V.N. Vapnik, Support-vector networks. Machine Learning. No. 20 (3), 1995, pp. 273-297.

[15] L. Breiman, Random Forests. Machine Learning. Vol. 45, No. 1, 2001, pp. 5-32.

[16] D.T. Larose, Discovering Knowledge in Data: An Introduction to Data Mining. Wiley-Interscience. 2004, 222 p.

[17] I. Sutskever, J. Martens, G. Dahl, G. Hinton, On the importance of initialization and momentum in deep learning. Journal of Machine Learning Research. Vol. 28, No. 3, 2013, pp. 1139-1147.

[18] D.E. Rumelhardt, G.E. Hinton, R.J. Williams, Learning Internal Representations by Error Propagation. Parallel Distributed Processing: Explorations in the Microstructure of Cognition. MIT, Cambridge. Vol 1, 1986, pp.318-362.

[19] D.E. Rumelhardt, G.E.Hinton, R.J. Williams, Learning representations by back-propagating errors. Nature, Vol. 323, 1986, pp.533-536.

[20] N. Srivastava, G. Hinton, A. Krizhevsky, I. Sutskever, R. Salakhutdinov, Dropout: A Simple Way to Prevent Neural Networks from Overfitting. Journal of Machine Learning Research, Vol. 15, 2014, pp.1929-1958.

[21] J.J. Hopfield, Neural networks and physical systems with emergent collective computational abilities. Proceedings of National Academy of Sciences of USA, Vol.79, No.8, 1982, pp. 2554-2558.

[22] Y. Bengio, Practical Recommendations for Gradient-Based Training of Deep Architectures. https://arxiv.org/abs/1206.5533v2

[23] I. Goodfellow, Y. Bengio, A.Courville, Deep Learning. MIT Press, 2016. http://www.deeplearningbook.org/

[24] A. Gibson, J. Patterson. Deep Learning. O'Reilly Media, Inc., 2017. https://www.safaribooksonline.com/library/view/deep-learning/9781491924570/

[25] K. He, X. Zhang, Sh. Ren, J. Sun. Deep Residual Learning for Image

Recognition. http://arxiv.org/abs/1512.03385v1

[26] L.A. Gatys, A.S. Ecker, M. Bethge. A Neural Algorithm of Artistic Style. http://arxiv.org/abs/1508.06576v1

[27] I.J. Goodfellow, J. Pouget-Abadie, M. Mirza, Bing Xu, D. Warde-Farley, Sh. Ozairy, A. Courville, Y. Bengio, Generative Adversarial Nets. http://arxiv.org/abs/1406.2661v1

[28] I. Goodfellow, NIPS 2016 Tutorial: Generative Adversarial Networks. https://arxiv.org/abs/1701.00160v4

[29] D. Foster, Generative Deep Learning: Teaching Machines to Paint, Write, Compose, and Play. O'Reilly Media. 2019, 330 p.

[30] A.L. Bychkov et al. Ultrastructural changes of cell walls under intense mechanical treatment of selective plant raw material. Biomass and Bioenergy. Vol. 47, 2012, pp. 260-267

[31] A.L. Bychkov, V.A. Buchtoyarov, O.I. Lomovsky Mechanical pretreatment of corn straw in a centrifugal roller mill. Cellulose Chemistry and Technology. Vol. 48 (5-6), 2014 pp. 545-551.

[32] E.M. Podgorbunskikh, A.L. Bychkov, et al. Pretreatment of rice husk in a pilot scale mill for further enzymatic hydrolysis. Catalysis in Industry. Vol. 8, 2016, pp. 274-279.

[33] V.A. Bukhtoyarov, A.L. Bychkov, O.I. Lomovskii, Effect of lignocellulose substrate on enzyme denaturation during joint mechanical treatment. Russian Chemical Bulletin. Vol. 64:4, 2015, pp. 948-951.

[34] A.L. Bychkov, V.A. Bukhtoyarov, O.I. Lomovskii, Stabilization of cellulosolytic enzymes by sorption on the plant raw materials surface. Russian Chemical Bulletin. Vol. 64:5, 2015, pp. 1189-1191.

[35] A.L. Bychkov, et al. Mechanically activated enzymatic hydrolysis of yeast biomass. Catalysis in Industry. Vol. 8, No. 4, 2016, pp. 354-360

[36] O. Lomovsky, A. Bychkov, I. Lomovsky, V. Logvinenko, A. Burdukov, Mechanochemical production of lignin-containing powder fuels from biotechnology industry waste: A review. Thermal Science. Vol. 19, No 1, 2015, pp. 219-229.

[37] O. Lomovsky, A. Bychkov, I. Lomovsky, Mechanical Pretreatment, in: Biomass Fractionation. Technologies for a Lignocellulosic Feedstock Based Biorefinery. Elsevier, 2016, pp. 23-55.

СЕКЦИЯ 3

Жасанды интеллект технологиялары. Интеллектуалды басқару жүйелері. Компьютерлік лингвистика және сөйлеу технологиялары. Бейнелерді танып білу және кескіндерді өңдеу. Биоинформатика және биометрикалық жүйелер. Адам-машиналық өзара әрекеттесуі. Машиналық оқыту. Интеллектуалды робототехникалық жүйелер

Технологии искусственного интеллекта. Интеллектуальные системы управления. Речевые технологии и компьютерная лингвистика. Распознавание образов и обработка изображений. Биоинформатика и биометрические системы. Человеко-машинное взаимодействие. Машинное обучение. Интеллектуальные робототехнические системы

Technologies of artificial intelligence. Intelligent control systems. Speech technologies and computer linguistics. Image recognition and image processing. Bioinformatics and biometric systems. Human-machine interaction. Machine learning. Intelligent Robotic Systems

ОБЗОР МЕТОДОВ ГЛУБОКОГО ОБУЧЕНИЯ ДЛЯ ВЫЯВЛЕНИЯ КОРРЕЛЯЦИЙ МЕЖДУ СОСУДИСТОЙ СТРУКТУРОЙ СЕЧАТКИ И ДРУГИМИ СЕРДЕЧНО-СОСУДИСТЫМИ ЗАБОЛЕВАНИЯМИ.

Рахымбекулы Ж., Пак А.А., Тукешев К.С., Джаксылыкова А.Б.
e-mail: rzhanik@gmail.com, alexpak1983@gmail.com, tukeshev.kuanysh@mail.ru, aselya17.89@mail.ru
Институт информационных и вычислительных технологий КН МОН РК, Казахстан
Институт информационных и вычислительных технологий КН МОН РК, Казахстан
Казахский научно – исследовательский институт глазных болезней
Институт информационных и вычислительных технологий КН МОН РК, Казахстан

Аннотация. *Системные заболевания, влияющие на кровообращение, могут привести к прогрессирующим морфологическим изменениям сосудистой сети сетчатки. Метод офтальмоскопии является неинвазивным диагностическим исследованием структуры сосудов сечатки. Доступность к неинвазивному осмотру и визуализации делает сосуды глазного дна наиболее информативными для анализа и прогностически значимыми в оценке состояния всего организма. В связи с этим накоплен большой фактический материал по изучению, разработке и внедрению в медицинскую практику методов исследований изображений глазного дна. Выявление связей между изменениями в сосудах сечатки с многочисленными видами заболеваний представляет практический и научный интерес. Например, изменения калибра сосудов артерий и вен сетчатки связаны с гипертонией, атеросклерозом и повышенным риском инсульта и инфаркта миокарда. Действительно, болезнь эндокринной систем, такая как сахарный диабет и болезнь сердечно сосудистой системы (гипертонии различной этиологии) имеют явно выраженное влияние на структуры сосудистого русла глазного дна [1]. Качество жизни пациента зависит от таких диагностических параметров как точность, достоверность, а также ширины охвата диагностическим методом различных нозологических групп. Таким образом, в настоящем исследовании предлагается совершенствование диагностического метода офтальмоскопии при помощи аппарата нейрокомпьютинга, с целью расширения охвата на новые нозологии, включая прогнозирование возникновения заболеваний и раннюю диагностику.*

Рядом исследовании было показано,как рисунок сосудов глазного дна может быть связан такими заболеваниями, как хроническим заболеванием почек, сердечно-сосудистыми заболеваниями, анемией, нарушением кровооброщения головного мозга и др.

Авторы [2] исследовали связи между аномалиями сосудистой сети сетчатки и повышенным риском развития хронической болезни почек (ХБП), что подтверждает гипотезу о том, что отклонения от оптимальной микрососудистой архитектуры

могут быть связаны с заболеваниями различной этиологии. Исследователи использовали математический аппарата фрактального анализа для построения глобального показателя геометрической сложности и оптимальности сосудистых сетей. Методологически был использован подход популяционного исследования «случай-контроль». Размер клинической базы составил 261 пациента с ХБП.

Следующая работа [3] рассматривает патологии глазного дна в когортном исследовании хронической почечной недостаточности (Chronic Renal Insufficiency Cohort, CRIC), в нем участвовали люди с различными стадиями хронической болезни почек (ХБП). Визуализации глазного дна были получены с использованием немидриатической глазной камеры Canon CR-DGI у 1936 человек, участвовавших в исследовании CRIC. Фотографии оценивались офтальмологом-клиницистом по сетчатке глаза в центральном центре чтения фотографий. Среди 1936 пациентов, которые были сфотографированы, 1904 (98%) имели оцениваемые фотографии по крайней мере на один глаз. обнаружили высокую распространенность патологии глазного дна у пациентов с ХБП. Эти данные подтверждают рекомендации по регулярному полному обследованию глаз у пациентов с ХБП.

В работе [4] исследовалась корреляция между острыми нарушениями мозгового кровообращения (ОНМК) и патологиями сечатки. Целевой группой исследования являются пациенты, страдающие распространенными возрастными заболеваниями головного мозга, включая нейродегенеративные (например, деменция) и цереброваскулярные (например, инсульт). Поскольку современные методы нейровизуализации, такие как магнитно-резонансная томография, могут быть не в состоянии обнаружить тонкие субклинические изменения (разрешение <100-500 мм) при деменции и инсульте, существует острая необходимость в других дополнительных методах для исследования патофизиологии этих заболеваний. Сетчатка - из-за ее анатомического, эмбриологического и физиологического сходства с мозгом - предлагает уникальное и доступное «окно» для изучения коррелятов и последствий субклинической патологии в головном мозге. Компоненты сетчатки, такие как микрососуды и аксоны ганглиозных клеток сетчатки, теперь могут быть визуализированы неинвазивно с использованием различных методов визуализации сетчатки, например, фотографии глазного дна и оптической когерентной томографии. Достижения в области визуализации сетчатки могут дать новое и потенциально важное понимание цереброваскулярных нейродегенеративных процессов в дополнение к тому, что в настоящее время возможно с помощью нейровизуализации.

Из-за инвазивности диагностических тестов на анемию и затрат, связанных с ее скринингом, это состояние часто не обнаруживается. Авторы [5] показали, что анемию можно обнаружить с помощью алгоритмов машинного обучения, обученных с использованием изображений глазного дна сетчатки и дополнительной информации о пациенте, включая расу и\или этническую принадлежность, возраст, пол и артериальное давление. В целевой группе исследования насчитывается 11 388 пациентов, медицинские данные взяты из UK Biobank. Автоматический скрининг на анемию на основе изображений глазного дна может особенно помочь пациентам с диабетом, которым регулярно проводят визуализацию сетчатки, и у которых анемия может повысить риск заболеваемости и смертности.

В работе [6] рассматривается вопрос прогнозирования атеросклероза с использованием изображений глазного дна сетчатки при помощи методов глубокого обучения. Методология работы предполагает проверку его клинических последствий путем проведения ретроспективного когортного анализа.

Использовалась база данных Центра укрепления здоровья больницы Сеульского национального университета (HPC-SNUH). Модель глубокого обучения была обучена с использованием 15 408 изображений для прогнозирования атеросклероза сонной артерии, рабочая абревиатура модели (DL-FAS). Ретроспективная когорта была сформирована из участников в возрасте 30-80 лет, прошедших выборные медицинские осмотры в HPC-SNUH. Используя DL-FAS в качестве основного воздействия, участники отслеживались для определения основного исхода смерти от сердечно-сосудистых заболеваний до 31 декабря 2017 г.

Для верификации прогностической силы модели атеросклероза сонной артерии когорта состояла из 32 227 участников, 78 умерших от сердечно-сосудистых заболеваний (ССЗ) и медиана контрольных посещений через 7,6 года. Полученный DL-FAS был независимым предиктором смерти от сердечно-сосудистых заболеваний с поправкой на FRS и добавил прогностическую ценность по сравнению с FRS.

Мы благодарим Институт Информационных и Вычислительных Технологий за финансовую поддержку. (Грант AP05132760, Казахстан).

Литература

1. Ильясова Н. Ю. Диагностический комплекс анализа изображений сосудов глазного дна //Биотехносфера. – 2014. – №. 3 (33).
2. C. C. A. Sng et al., “Fractal analysis of the retinal vasculature and chronic kidney disease,” Nephrol. Dial. Transplant., vol. 25, no. 7, pp. 2252–2258, 2010, doi: 10.1093/ndt/gfq007.
3. J. E. Grunwald et al., “Prevalence of ocular fundus pathology in patients with chronic kidney disease,” Clin. J. Am. Soc. Nephrol., vol. 5, no. 5, pp. 867–873, 2010, doi: 10.2215/CJN.08271109.
4. E. Stefánsson et al., “Retinal Oximetry Discovers Novel Biomarkers in Retinal and Brain Diseases,” Invest. Ophthalmol. Vis. Sci., vol. 58, no. 6, pp. BIO227--BIO233, 2017, doi: 10.1167/iovs.17-21776.
5. A. Mitani et al., “Detection of anaemia from retinal fundus images via deep learning,” Nat. Biomed. Eng., vol. 4, pp. 18–27, 2020, doi: 10.1038/s41551-019-0487-z.
6. P. De Boever, T. Louwies, E. Provost, L. Int Panis, and T. S. Nawrot, “Fundus photography as a convenient tool to study microvascular responses to cardiovascular disease risk factors in epidemiological studies,” J. Vis. Exp., no. 92, pp. 1–9, 2014, doi: 10.3791/51904.

ИССЛЕДОВАНИЕ ПОДХОДОВ ПО ИЗВЛЕЧЕНИЮ КЛЮЧЕВЫХ СЛОВ ИЗ ТЕКСТА

Рахимова [1]Д.Р., Турганбаева [2]А.О., Сатыбалдиев[1] А.
e-mail: diana.rakhimova@kaznu.kz, turganbaeva.aliya@bk.ru, nba_abilay.99@mail.ru
[1]Казахский Национальный Университет имени аль Фараби, Казахстан
[2]Институт информационных и вычислительных технологий КН МОН РК, Казахстан

Аннотация. *В настоящее время объемы и динамика информации, которая подлежит обработке в лексикографии и информационном поиске, делают особенно актуальной задачу автоматического извлечения ключевых слов и словосочетаний, которые могут использоваться для создания и развития терминологических ресурсов, а также для эффективной обработки документов: индексирования, реферирования, кластеризация и классификации. В данной работе представлены обзоры современных методов по извлечению ключевых слов из электронных текстов. Представлен разработанный алгоритм извлечения ключевых слов, основанного на лингвистических свойствах и статистических данных казахского языка. Практическое применение алгоритма было апробировано на текстах различного жанра и тематик на казахском языке.*

Введение.

Анализ огромного количества данных может быть упрощен, если у нас будет ключевые слова или словосочетания, которые могут предоставить нам основные характеристики, концепцию и т. д. документа. Соответствующие ключевые слова и словосочетания могут служить кратким изложением документа и помогают нам легко упорядочивать документы и извлекать их на основе их содержания [1]. Необходимо различать два основных подхода к решению проблемы автоматизации выделения ключевых слов и словосочетаний: назначение ключевых слов и словосочетаний (keyphrase assignment) и их извлечение (keyphrase extraction) [2-3]. Главное отличие заключается в том, что первый подход позволяет выделять только те ключевые слова и словосочетания, которые содержатся в некотором предусмотренном словаре, а второй подход предполагает выбор ключевой информации непосредственно из текста.

Ключевые слова могут быть назначены вручную или автоматически, но первый подход очень трудоемкий и дорогой. Таким образом, существует необходимость в автоматизированном процессе, который извлекает ключевые слова из документов. Есть готовые программные решения этой задачи для распространенных языков (английский, русский, испанский и т.д.), а для казахского языка только единицы и они не в открытом доступе.

1. Исследование подходов по извлечению ключевых слов

Методы назначения ключевых слов можно условно разделить на две категории: (1) назначение ключевых слов и (2) извлечение ключевых слов [4-7]. Оба вращаются вокруг одной и той же проблемы - выбора лучшего ключевого слова. Слова, встречающиеся в документе, анализируются с целью выявления наиболее представительных слов, обычно исследуя свойства источника (то есть частоту, длину) [8]. Существующие методы для автоматического извлечения ключевых слов по предложению Ping-I и Shi-Jen можно разделить на [9]: статистические подходы и подходы машинного обучения.

Необходимо так же акцентировать на четырех категориях, предложенных авторами Zahang и др. в работе [8]: 1) простые статистические подходы; 2) лингвистические подходы; 3) подходы машинного обучения; 4) другие подходы.

Простые статистические подходы включают в себя простые методы, которые не требуют данных обучения. Кроме того, методы не зависят от языка и домена. Статистика слов из документа может быть использована для идентификации

ключевых слов: статистика n-граммы, частота слов, TF-IDF, совпадения слов, дерево PAT (дерево Патрисии; дерево суффиксов или дерево позиций) и т.д. Недостатком является то, что в некоторых профессиональных текстах, таких как здоровье и медицина, наиболее важные ключевые слова могут появляться только один раз в статье. Использование статистически уполномоченных моделей может непреднамеренно отфильтровать эти слова [8].

В работе [9] предлагается способ оценки терминологичности на базе контрастного подхода. Способ берет за основу известную формулу взвешивания слов TF-IDF, согласно которой вес слова в документе тем выше, чем выше частота его использования в этом документе и чем ниже его разброс по всей коллекции. В новом варианте формулы, который авторы называют «term frequency – inverse domain frequency», оценивается вес слова не в документе, а в целевой коллекции. Согласно новой формуле вес слова тем выше, чем выше относительная частота его использования в целевой коллекции и чем ниже его относительный разброс по всем коллекциям:

$$TF * IDF = TF(t, D) * IDF(t) = \frac{n_{t,D}}{\sum_k n_{k,D}} * \log\left(\frac{|TS|}{|\{d: t\epsilon d\}|}\right), \quad (1)$$

где $n_{t,D}$ – это число вхождений слова t в целевую коллекцию D, $\sum_k n_{k,D}$ – это сумма вхождений всех слов в целевую коллекцию D, |TS| – это количество документов во всех используемых коллекциях, $|\{d: t \in d\}|$ – это количество всех документов, в которые слово t входит хотя бы один раз. Таким образом, авторы считают терминами все слова с высокой концентрацией в пределах узкого подмножества документов.

Авторы работы [10] также предлагают оценивать терминологичность слов на базе формулы TF-IDF. Собственный вариант этой формулы они называют контрастным весом (contrastive weight) и определяют его как меру, которая тем выше, чем выше частота употребления слова в целевой коллекции и чем ниже относительная частота его употребления в контрастных коллекциях:

$$Contrastive\ Weight = TF(t, D) * IDF(t) = loglog(f_t^D) * \log\left(\frac{F_{JC}}{\sum_j f_t^i}\right) \quad (2)$$

где f_t^D – частота употребления слова в целевой коллекции, $\sum_j f_t^j$ – сумма частот всех употреблений слова в контрастных коллекциях, $F_{TC} = \sum_{i,j} f_i^j$ – сумма частот употреблений всех слов во всех коллекциях, включая целевую. Как отмечают сами авторы, контрастный вес значительно лучше оценивает терминологичность слов, чем чистые частоты, однако общая эффективность метода, определенная с помощью F-меры, по их словам, не бросается в глаза.

В работе [11] также развивается идея штрафов и вознаграждений, заложенная в базовой конструкции формулы TF-IDF, и предлагается новый вариант этой формулы, получивший название “term frequency – disjoint corpora frequency”. В качестве вознаграждения используется абсолютная частота употребления слова в

целевой коллекции, а в качестве штрафа – произведение абсолютных частот употреблений слова в контрастных коллекциях:

$$TF * DCF = \frac{f_t^D}{\prod_{g \epsilon G} 1 + \log\left(1 + f_t^g\right)} \quad (3)$$

где $f_t{}^D$ и $f_t{}^g$ – частоты употреблений данного слова t в целевой и контрастной коллекциях соответственно, G – множество всех контрастных коллекций.

Подходы лингвистики используют лингвистическую особенность слов в основном, предложений и документа. Лексический, синтаксический, семантический и дискурсивный анализ являются одними из наиболее распространенных, но сложных анализов.

Подходы машинного обучения рассматривают контролируемое или неконтролируемое обучение на примерах, но связанная работа по извлечению ключевых слов предпочитает контролируемый подход. Подходы контролируемого машинного обучения создают модель, которая обучается на основе набора ключевых слов. Они требуют ручной аннотации в наборе данных обучения, которая является чрезвычайно утомительной и непоследовательной (иногда запрашивает предопределенную таксономию). К сожалению, авторы обычно присваивают ключевые слова своим документам только тогда, когда они вынуждены это делать. Таким образом, индуцированная модель применяется для извлечения ключевых слов из нового документа. Этот подход включает в себя наивный метод Байеса, *SVM, C4.5, Bagging* и т.д. Таким образом, методы требуют данные обучения и часто зависят от предметной области. Системе необходимо заново изучать и устанавливать модель каждый раз при изменении домена [12-13]. Индукция модели может быть очень сложной и длительной для массивных наборов данных.

Другие подходы для извлечения ключевых слов в целом объединяют все методы, упомянутые выше. Кроме того, иногда для объединения они включают эвристические знания, такие как положение, длина, особенности компоновки терминов, HTML и аналогичные теги, форматирование текста и т.д.

Модель векторного пространства (МВП) хорошо известна и является наиболее используемой моделью для представления текста в подходах интеллектуального анализа текста [14, 15]. В частности, документы, представленные в виде векторов признаков, расположены в многомерном евклидовом пространстве. Эта модель подходит для захвата частоты простых слов, однако структурная и семантическая информация обычно не учитывается. Следовательно, из-за простоты модель векторного пространства имеет несколько недостатков :1) значение текста и структуры не могут быть выражены, 2) каждое слово не зависит от другого, последовательность появления слов или другие отношения не требуются, 3) если два документа имеют одинаковое значение, но имеют разные слова, сходство не может быть легко вычислено.

Текстовое представление на основе графа известно, как одно из лучших решений, эффективно решающих эти проблемы. График представляет собой математическую модель, которая позволяет очень эффективно исследовать взаимосвязи и структурную информацию.

Граничное отношение между двумя терминами может быть установлено на многих принципах, использующих различную область текста или отношения для построения графа: 1) слова, встречающиеся вместе в предложении, абзаце, разделе

или документе, добавленные в граф в виде клики; 2) пересекающиеся слова из предложения, абзаца, раздела или документа; 3) слова, встречающиеся в фиксированном окне в тексте; 4) семантические отношения - соединяющие слова, имеющие одинаковое значение, слова, написанные одинаково, но имеющие разное значение, синонимы, антонимы, и т.д.

2. Разработка алгоритма извлечения ключевых слов, основанного на лингвистических и статистических данных

Алгоритм на рисунке 3 извлечения ключевых слов из документов на казахском языке включает в себя 3 этапа: 1. нахождение кандидатов в ключевые слова; 2. выделение признаков; 3. ранжирование.

На первом этапе решаются 2 задачи: предварительная обработка слов; и разделение текста на отдельные слова и словосочетания.

Первая задача является языко-зависимой, поэтому здесь учитывается морфологическая особенность казахского языка. Для решения этой задачи задействованы система полных окончаний казахского языка (через морфологический анализатор казахского языка, разработанный на платформе Apertium выполняем разметку документа), алгоритм стемминга и лемматизации для казахского языка (реализованные на языке программирования Python3). А для второй использован простой подход - процедура токенизации, с помощью которой весь текст разбивается на отдельные слова.

На втором этапе для каждого найденного кандидата в ключевые слова выделяются признаки, по которым оценивается степень его важности. Выделяемые признаки можно разбить на 3 категории: синтаксические признаки, статистические признаки, структурные признаки.

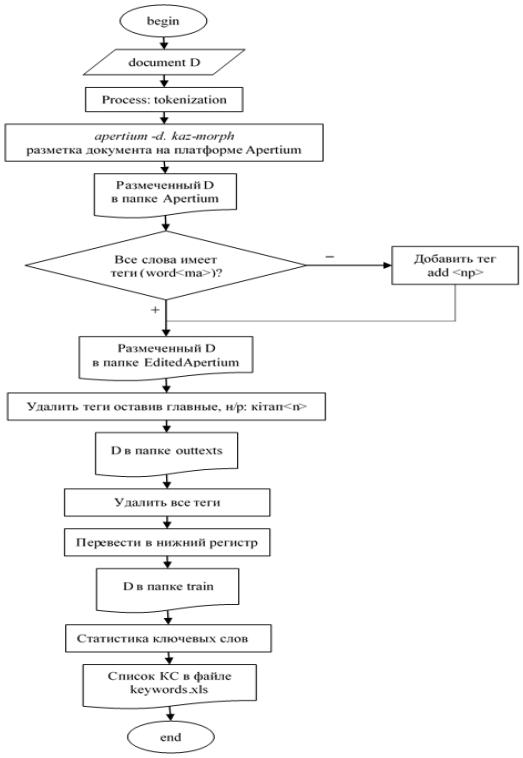


Рис. 1 Блок-схема алгоритма извлечения ключевых слов из документов на казахском языке

Для выделения синтаксического признака мы использовали морфологический анализ казахского языка. И алгоритм TF-IDF (Term Frequency – Inverse Document Frequency) для определения частотности, то есть для выделения статистических признаков. В программе для биграммного слово указали следующие признаки: существительное+существительное (N+N), прилагательное+существительное (Adj+N), существительное+глагол (N+V), имя собственное+существительное (Np+N), числительное+существительное (только некоторые слова) (Num+SomeWordsOfTime).

На третьем этапе ранжируем результаты по статистическому признаку и в соответствующей мере к объему текста.

3. Применение подходов по извлечению ключевых слов к текстам на казахском языке

Реализация алгоритма выполнено на языке программирования Python3. Программа тестировалась на подготовленных корпусах различных тематик, приведенные в таблице 1.

Полученные результаты экспериментов, выполненных на корпусах, приведенных в таблице 3 проанализированы учитывая граничный коэффициент находки по объему и выявлено что ключевые слова и словосочетания подобраны правильно. Результаты анализа приведены в таблице 1.

Таблица 1. Экспериментальные результаты разработанного алгоритма по определению ключевых слов для казахского языка

Название документа	Объем документа (предложениий)	Граничный коэффициент ключевых слов	Количество ключевых слов	Точность нахождения
futbol.txt	558	3-8	8	85,71%
boks.txt	659	3-8	8	75%
Samsung.txt	167	3-8	8	87,5
7tarihitulga.txt	275	3-8	8	97%
LG.txt	97	9-11	10	90%
ginnes.txt	103	9-11	10	80%

Заключение

По итогам научно исследовательской работы были получены следующие результаты: Исследованы методы и современные подходы по извлечению ключевых слов и словосочетание из текстов; Разработан модифицированный подход по извлечению ключевых слов и словосочетаний, который будет применен для решения прикладных задач обработки естественных языков (реферирования текстов на казахском языке, информационный поиск).

Благодарность

Исследование выполнено при поддержке Министерства образования и науки Республики Казахстан в рамках научного проекта AP 05132950.

Литература

1. Шереметьева С.О., Осминин П.Г. Методы и модели автоматического извлечения ключевых слов // Вестник Южно-Уральского государственного университета. – 2015. – № 1, Т. 12. – С. 76-81.

2. Effective Approaches for Extraction of Keywords // http://www.ijcsi.org/papers/7-6-144-148.pdf: 25.07.2020.

3.Keyword extraction a review of methods and approaches - http://langnet.uniri.hr/papers/beliga/Beliga_KeywordExtraction_a_review_of_methods_and_approaches.pdf: 05.07.2020.

4. Witten I.H., Paynter G.W., Frank E., Gutwin C., NevillManning C.G. Kea: Practical Automatic Keyphrase Extraction // Proceedings of the 4th ACM Conference of the Digital Libraries. – Berkeley, CA, USA, 1999. – P. 254-255.

5. Turney P.D. Learning to Extract Keyphrases from Text // Technical Report, National Research Council of Canada. – Institute for Information Technology, 1999. – P. 325-328.

6. Medelyan O., Witten I.H. Thesaurus Based Automatic Keyphrase Indexing // Proceedings of the 6th ACM/IEEE-CS JCDL 2006. – NY, USA, 2006. – P. 296-297.

7. Feldman R., Sanger J. The Text Mining Handbook - Advanced Approaches in Analyzing Unstructured Data. – NY: Cambridge University Press, 2007. – P. 258-305.

8. Zahang C., Wang H., Liu Y., Wu D., Liao Y., Wang B. Automatic Keyword Extraction from Documents Using Conditional Random Fields // Journal of CIS. – 2008. – №4:3. – P. 1169-1180.

9. Chen P., Lin S. Automatic keyword prediction using Google similarity distance // Expert System Application. – 2010. – Vol. 37, issue 3. – P. 1928-1938.

10. Kim S.N., Baldwin T., Kan M-Y. An unsupervised approach to domain-specific term extraction // Proceedings of the Australasian Language Technology Association Workshop. – 2009. – P. 94-98.

11. Basili R. A contrastive approach to term extraction // Proceedings of the 4th Terminological and Artificial Intelligence Conference. – 2001. – P. 154-166.

12. Lopes L., Fernandes P., Vieira R. Estimating term domain relevance through term frequency, disjoint corpora frequency-tf-dcf // Knowledge-Based Systems. – 2016. – Vol. 97. – P. 156-187.

13. Sebastiani F. Machine learning in automated text categorisation // Journal ACM Computing Surveys. – 2002. – №34(1). – P. 1-47.

14. Jones K.S. Informaion retrieval and artificial inteligence // Artificial Intelligence. – 1999. – №114(1-2). – P. 257-281.

15. Berry M.W., Survey of Text Mining II: Clustering, Classification, and Retrieval. – Springer Science & Business Media, 2007. – P. 138-143.

ИССЛЕДОВАНИЕ ПРИМЕНЕНИЯ BERT МОДЕЛИ ДЛЯ ЭКСТРАКТИВНОЙ СУММАРИЗАЦИИ ОФИЦИАЛЬНЫХ ПРАВОВЫХ ДОКУМЕНТОВ

Уалиева И.М., Мусабаев Р.Р.
e-mail: i.ualiyeva@ipic.kz
Институт информационных и вычислительных технологий КН МОН РК, Казахстан

Аннотация. *Автоматическое реферирование текстов или суммаризация для официальных документов – один из методов отбора ключевых фраз и предложений, наиболее полно отражающих официальные тексты. Рассматриваются методы экстрактивной суммаризации текстов для официальных правовых документов. В данное время появились новые архитектуры, позволяющие провести суммаризацию путем кластеризации векторов, полученных алгоритмами глубокого обучения. Исследуется применение BERT модели для реферирования текстов государственных программ РК.*

Введение

Задача суммаризации (summarization) или автоматического реферирования текстов – одна из ключевых тем в области обработки естественных языков (Natural Language Programming (NLP)). Она состоит в сжатии большого объема текста до связного краткого содержания, отражающего основные идеи исходного текста. Всего существует два типа суммаризации: абстрактивная (abstractive) и экстрактивная (extractive). Абстрактивная суммаризация сходна с тем, как человек резюмирует текст, применяя обобщающие слова, которых нет в исходном тексте [1]. Экстрактивная суммаризация составляет резюме исходя из имеющейся структуры, предложений и словосочетаний исходного текста и ранжирует их по степени их значимости.

В своем исследовании мы применяем задачу суммаризации к текстам офицальных правовых документов (legal documents), к которым также относятся государственные программы РК. Государственные программы, являются официальными документами, в которых правительство доводит до граждан важные значимые проблемы общества, какие задачи выдвигаются для общества в целом, как для юридических, так и для отдельных граждан. И, если юридические лица имеют аппарат юристов для изучения программ, то обычные люди лишены этого преимущества. Суммаризация позволяет предоставить важную информацию в более доступной и понятной форме для обычного человека. Задача суммаризации для официальных документов – сложная задача, так как официальные документы имеют ряд таких особенностей как слишком длинные тексты, сложную структуру и наличие сложных для понимания рядовым гражданином специфических слов [2]. И суммаризация – это мощный инструмент, с помощью которого можно из текста можно извлечь ключевые идеи без ручного вмешательства. В данное время существует много исследований, пытающихся решить проблему суммаризации для официальных документов [2]–[4]. В последние годы появилось много подходов, основанных на глубоком обучении [4], [5]. Мы исследуем метод суммаризации, основанный на методологии BERT и его применение к задаче суммаризации текстов

официальных документов. Далее в работе будет обзор исследований в области суммаризации официальных текстов, описана методология суммаризации на примере текстов официальных государственных программ, представлены результаты работы модели и примеры суммаризации для некоторых документов.

Обзор существующих работ

Всего, согласно исследованиям [6], существует шесть основных техник или методов суммаризации. Это подходы, основанные на нечеткой логике, на машинном обучении (включая глубокое обучение), статистике, графический подход, тематическое моделирование и основанный на правилах.

Для суммаризации официальных правовых текстов исследователи применяют широкий диапазон подходов. Детальный обзор методов проведен в работе [2]. Большинство методов опирается на знания специалистов в области права и политологии, лингвистов, чтобы разметить данные или получить информацию о структуре и особенностях документов, т.е. большинство подходов основано на обучении с учителем.

Размеченные ручным способом данные имеют высокую себестоимость, поэтому исследователи активно стали изучать и предлагать подходы, основанные на обучении без учителя. Некоторые подходы основаны на тематическом моделировании и латентном семантическом анализе (Latent Semantic Analysis, LSA) [7]. Подходы, основанные на извлечении признаков, также показали свою эффективность, в таких методах каждое предложения представляется как набор признаков. Для извлечения признаков из предложений используется метод взвешенных графов, основанный на извлечении признаков методом tf-idf. Для определения значимости предложений используются классические методы машинного обучения [8].

Автоматическая генерация помеченных обучающих данных для сегментации юридических текстов с использованием знаний предметной области была предложена в (Wagh and Anand, 2020). В работах [9], [10] показаны подходы, основанные на глубоком обучении, применяемые для экстрактивной суммаризации официальных правовых текстов.

Для суммаризации формируется вектор методом BERT [11]. Далее векторы кластеризуются алгоритмом k-means. Далее опишем каждый из компонентов метода.

Экстрактивная суммаризация текста с BERT и k-means

Для проведения суммаризации в качестве датасета мы используем государственные программы РК. Корпус госпрограмм собран с правительственных сайтов РК, в него отобраны госпрограммы «Программа Рухани Жангыру», Стратегия «Казахстан-2050», Стратегический план развития Республики Казахстан до 2025 года, Государственная программа «Цифровой Казахстан», Государственная программа развития образования и науки Республики Казахстан на 2020-25 гг., Новая программа развития здравоохранения на 2020-25 гг. и другие, всего одиннадцать программ. Все тексты корпусов проходят предобработку и лемматизацию. Тексты госпрограмм очищаются от формул, таблиц, рисунков, содержания. При предобработке мы удаляем цифры и знаки пунктуации, стоп-слова и слова длиной менее трех символов. Лемматизируем слова с помощью библиотеки MyStem [12]. Слова, которые встретились в корпусе реже 10 раз, не включаем в датасет.

Прошедший предобработку текст проходит токенизацию и разбивается на предложения. Первоначально удаляются слишком короткие и слишком длинные предложения. Предложения, которые начинаются с союзов, также не включаются. Чистые предложения поступают в BERT модель для формирования векторов, далее кластеризуются алгоритмом k-means. k-means отбирает те предложения, которые расположены наиболее близко к центроидам.

BERT для формирования векторов

BERT – это двунаправленная мультиязычная модель, основанная на архитектуре Transformer. Модель предварительно обучена без учителя на двух NLP-задачах: предсказание закрытых маской слов и предсказание, является ли следующее предложение логическим продолжением предыдущего.

BERT работает по принципу векторного представления слов, основанном на контекстной близости, когда слова, встречающиеся в тексте рядом с одинаковыми словами (а, следовательно, имеющие схожий смысл), в векторном представлении будут иметь близкие координаты векторов.

При подаче текста на вход BERT-модели сначала выполняется его токенизация — разбиение на более мелкие единицы (токены): абзацы делятся на предложения, предложения на слова и пр. Входной текст разбивается на список токенов, доступных в словаре. Если в словаре отсутствует слово, то оно постепенно разбивается на более мелкие части, которые уже находятся в словаре. Таким образом контекст нового слова будет комбинацией смыслов его частей. Как, например, для русского языка слово «пришел» разбивается на «при» и «##шел».

Таким образом, BERT является автокодировщиком (autoencoder, AE), который скрывает и изменяет некоторые слова, пытаясь восстановить изначальную последовательность слов из контекста.

Для экспериментов была использована многоязыковая модель BERT-Base. Многоязыковая модель реализована для 104 языков, имеет 12 слоев, 768 узлов, 12 выходов, 110M параметров, библиотеку pytorch-pretrained-BERT и OpenAI GPT-2 PyTorch модель – сеть, которая расширяет оригинальную архитектуру BERT.

Выводы и обсуждение

Реферирование официальных текстов – специфическая задача в области NLP и BERT может строить конспекты автоматически, с учетом специфики исходного материала. На следующем этапе планируется провести сравнительное исследование алгоритма с известными алгоритмами суммаризации текстов как TextRank и XLNet, преодобученной ML-модели многослойной transformer-архитектуры.

Поддержка исследований.

Работа проводится в рамках ПЦФ «Разработка информационных технологий и систем для стимулирования устойчивого развития личности как одна из основ развития цифрового Казахстана».

Литература

[1] P.-E. Genest and G. Lapalme. Framework for Abstractive Summarization using Text-to-Text Generation / P.-E. Genest and G. Lapalme. // Proc. 49th Annu. Meet. Assoc. Comput. Linguist., pp. 64–73, Jun. 2011.

[2] A. Kanapala, S. Pal, and R. Pamula. Text summarization from legal documents: a survey / A. Kanapala, S. Pal, and R. Pamula. // Artif. Intell. Rev., vol. 51, no. 3, pp. 371–402, Mar. 2019, doi: 10.1007/s10462-017-9566-2.

[3] B. Hachey and C. Grover. Extractive summarisation of legal texts / B. Hachey and C. Grover // Artif. Intell. Law, vol. 14, no. 4, pp. 305–345, Apr. 2007, doi: 10.1007/s10506-007-9039-z.

[4] D. Anand and R. Wagh. Effective deep learning approaches for summarization of legal texts / D. Anand and R. Wagh // J. King Saud Univ. - Comput. Inf. Sci., p. S1319157819301259, Dec. 2019, doi: 10.1016/j.jksuci.2019.11.015.

[5] D. Miller. Leveraging BERT for Extractive Text Summarization on Lectures. / D. Miller // ArXiv190604165 Cs Eess Stat, Jun. 2019, Accessed: Sep. 15, 2020. [Online]. Available: http://arxiv.org/abs/1906.04165.

[6] A. P. Widyassari et al. Review of automatic text summarization techniques & methods / A. P. Widyassari et al. // J. King Saud Univ. - Comput. Inf. Sci., p. S1319157820303712, May 2020, doi: 10.1016/j.jksuci.2020.05.006.

[7] A. John, P. S. Premjith, and M. Wilscy. Extractive multi-document summarization using population-based multicriteria optimization / A. John, P. S. Premjith, and M. Wilscy // Expert Syst. Appl., vol. 86, pp. 385–397, Nov. 2017, doi: 10.1016/j.eswa.2017.05.075.

[8] M. Saravanan, B. Ravindran, and S. Raman. Automatic identification of rhetorical roles using conditional random fields for legal document summarization / M. Saravanan, B. Ravindran, and S. Raman // 2008.

[9] M. Allahyari et al. Text Summarization Techniques: A Brief Survey / M. Allahyari et al. // ArXiv170702268 Cs, Jul. 2017, Accessed: Sep. 15, 2020. [Online]. Available: http://arxiv.org/abs/1707.02268.

[10] A. Sinha, A. Yadav, and A. Gahlot. Extractive Text Summarization using Neural Networks / A. Sinha, A. Yadav, and A. Gahlot // ArXiv180210137 Cs, Feb. 2018, Accessed: Sep. 15, 2020. [Online]. Available: http://arxiv.org/abs/1802.10137.

[11] J. Devlin, M.-W. Chang, K. Lee, and K. Toutanova. BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding / J. Devlin, M.-W. Chang, K. Lee, and K. Toutanova // ArXiv181004805 Cs, May 2019, Accessed: Sep. 15, 2020. [Online]. Available: http://arxiv.org/abs/1810.04805.

[12] I. Segalovich. A Fast Morphological Algorithm with Unknown Word Guessing Induced by a Dictionary for a Web Search Engine / I. Segalovich // 2003.

КЛАССИФИКАЦИЯ НЕГАТИВНЫХ ПУБЛИКАЦИЙ В СМИ С ИСПОЛЬЗОВАНИЕМ ТЕМАТИЧЕСКОГО МОДЕЛИРОВАНИЯ

Якунин К.[1,2], Мухамедиев Р.И.[1,2,3], Кучин Я.[1,2], Мусабаев Р.[1], Булдыбаев Т.[4], Мурзахметов С.[3], Сымагулов А.[1,3]
e-mail: Yakunin.k@mail.ru
[1]*Институт информационных и вычислительных технологий КН МОН РК, Казахстан*
[2]*Сатпаев Университет (КазНИТУ), Казахстан*
[3]*ISMA университет, Рига*
[4]*Информационно-аналитический центр, Казахстан*

Аннотация. *В работе предложен метод оценки текстовых документов по произвольным критериям с использованием тематической модели корпуса документов. Оценка формируется следующим образом: после формирования тематической модели корпуса рассчитывается условное вероятностное распределение документов по темам, свойствам и классам. Для оценки каждого документа могут быть применены веса, присвоенные экспертами каждой теме. Предложенная методика была применена к корпусу документов, состоящему из более чем 800 тысяч новостных публикаций из общедоступных казахстанских источников, опубликованных в 2018-2019 годах. Выполнена классификация документов с выявлением негативной информации по общественно значимым темам. Эксперименты подтверждают общую возможность оценки тональности публикаций с использованием тематической модели текстового корпуса.*

1 Введение

Исследователи концентрируют свои усилия на оценке медийного контента в связи с его практической значимостью для информационных агентств, рекламных компаний и государственного сектора. Анализ медиаконтента позволяет прогнозировать вероятную популярность новостных статей [2], предоставлять качественные статьи пользователям, планировать PR-стратегию по продвижению товаров или услуг [3, 4]. Государственный сектор получает инструмент для продвижения и пропаганды инноваций, PR-планирования и выявления контента, запрещенного законом. Пользователи могут быстро и эффективно отфильтровывать большие объемы информации.

Предложенный нами метод основан на тематическом моделировании и байесовских правилах, что снижает затраты на маркировку корпуса документов. В то же время метод показывает результаты, сравнимые с более трудоемкими подходами, основанными на контролируемом обучении.

Помимо введения, статья состоит из следующих разделов:

Второй раздел включает в себя описание тематического моделирования.

В третьем разделе описывается предлагаемая модель оценки текстов.

В четвертом разделе описаны обработанная корпорация, свойства и классы, а также результаты верификации метода по задаче выявления негативной информации по значимым темам.

В заключении мы обсуждаем полученные результаты, преимущества и недостатки предлагаемого алгоритма, а также намечаем направления дальнейших исследований.

2 Тематическое моделирование

Тематический анализ или тематическое моделирование является одним из активно применяемых методов NLP. Тематическое моделирование — это метод, основанный на статистических характеристиках коллекций документов, который используется для обобщения текста, извлечения информации, поиска и классификации информации [5]. Суть данного подхода заключается в интуитивном понимании того, что документы в коллекции образуют группы, в которых различается частота слов или словосочетаний.

Тематическое моделирование используется как попытка преодолеть ограничения BERT [6] и других NLP-моделей глубокого обучения, таких как необходимость больших объемов ручной маркировки и значительная вычислительная сложность, а также сохранить идею переноса обучения путем

передачи знаний из большого массива немаркированных данных для получения знаний о скрытых структурах корпуса.

Тематическое моделирование хорошо развито с точки зрения алгоритмов и методов, основанных на статистической модели языка, а использование кластеров документов, связанных с набором тем, позволяет решать проблемы синонимии и полисемии терминов [7]. Вероятностные тематические модели описывают документы (M) дискретным распределением по совокупности тем (T), а темы дискретным распределением по совокупности терминов [8]. Иными словами, тематическая модель определяет, к какой теме принадлежит каждый документ и какие слова образуют каждую тему. Для построения тематической модели корпуса документа используются вероятностно-латентный семантический анализ (Вероятностный латентный семантический анализ (PLSA), достаточно популярный метод латентного распределения по Дирихле (LDA) [9] и его расширение BigARTM [10].

В данной работе тематическая модель BigARTM используется для расчета условных распределений вероятностей документов по темам, свойствам и одному или нескольким классам. Агрегирование влияния тем на итоговую оценку осуществляется с помощью байесовского метода, который в конечном итоге позволяет рассчитать ожидаемые гипотезы по отдельным характеристикам публикаций СМИ.

3 Метод

В предлагаемой модели оценка каждой публикации рассматривается в трех формах:

- Темы, полученные с помощью тематического моделирования. Например, спорт, образование, экономика, несчастные случаи и т.д.

- Свойства - можно использовать произвольный список свойств. Необходимо иметь процесс для получения оценок влияния каждой темы на каждое из выбранных свойств. Примеры таких процессов описаны в разделе 4. Примерами свойств являются тональность, социальная значимость, объективность, манипулятивность, политизация и др.

- Классы. Идентификация статей, относящихся к каждому классу, в целом является конечной целью предлагаемого метода. Выбранные свойства должны иметь некоторую корреляцию или влияние на конечные классы. В случае статьи конечным классом является негативная информация по социально значимым темам.

Следует отметить, что в данной работе рассматривается только одно свойство - негативная тональность. Другие свойства и составной класс будут рассмотрены в дальнейших исследованиях.

Основная идея многокритериальной оценки и агрегирования субъективных и объективных свойств была первоначально описана в [11].

Применение тематической модели, полученной в результате кластерного анализа (неконтролируемое обучение), в сочетании с классами и атрибутами, определенными экспертами, заслуживает внимания в связи с предлагаемым подходом. Таким образом, семантика распределения определяется пользователем (экспертом), а исходное тематическое моделирование зависит от корпорации документов.

Применение Байесовского подхода позволяет оценить вероятность выдвижения гипотезы на основе неполной информации с частью текстового корпуса. Другими словами, он позволяет получить оценки для документов по указанным модальностям путем обработки только части текстового корпуса, хотя и с пониженной точностью.

Сначала мы генерируем тематическую модель, а затем вычисляем значения условных вероятностей p1, ..., p6 (см. далее). Есть несколько вычислительных деталей, которые стоит упомянуть в контексте байесовской агрегации.

Если субъективная вероятность $p(e|h)$ равна 0.5, то она не повлияет на целевую гипотезу $p(h|e)$ и может быть интерпретирована как неубедительная или несущественная. Следовательно, если $p(e|h)$ выше 0.5, то это влияние на целевую гипотезу будет положительным, а если ниже 0.5 - отрицательным.

Эта особенность подразумевает, что нормализация на каждом шаге вычислительного процесса должна быть скорректирована соответствующим образом. Например, если признак/событие имеет положительное влияние 0.8, но оно применяется только к определенному объекту с весом 0.5, неправильно просто перемножать эти два числа и затем использовать его, так как результат умножения будет равен 0.4, что является небольшим отрицательным влиянием, которое не соответствует действительному влиянию признака/события в 0.8 (положительное).

Следует также уточнить, что вес (0,5) в предыдущем примере обычно соответствует той степени, в которой документ соответствует теме, которой было присвоено определенное значение воздействия (0,8). Однако, как будет отмечено ниже, этот показатель может меняться с одного этапа модели на другой.

Для решения этой проблемы был введен специальный процесс нормализации взвешенного воздействия, который осуществляется по следующей формуле:

$$(p - 0.5) * w + 0.5 \tag{1}$$

где p - влияние объекта/события/темы, а w - вес (или степень, в которой объект относится к данному объекту/событию/теме). После этого применяется байесовский процесс агрегации. Последним шагом является нормализация каждой строки результирующей матрицы, которая также настраивается - все значения ниже 0.5 нормализуются отдельно к диапазону [0; 0.5], а все значения выше 0.5 нормализуются к [0.5; 1]. Такая нормализация позволяет предотвратить снижение значений, чтобы удержать значения на адекватном уровне насыщения вдоль множественных матричных преобразований (p1->p6).

Теперь рассмотрим процесс вычисления P матриц:

Матрица P1 описывает связь между темами и критериями оценки. Ее можно получить различными способами, в том числе с помощью генерации словаря, ручной маркировки и (полу)автоматической маркировки с использованием мультикорпусного подхода [12].

Матрица P2 описывает связь между документами и темами и получается с помощью моделирования тем (в моделях тем на основе LDA она соответствует матрице тета).

Матрица P3 получается из выполнения первого этапа AHP - сокращения парной матрицы сравнения критериев оценки до столбцового вектора важности каждого критерия.

P4 описывает связь между темами и целевыми классами. Матрица P4 вычисляется как пользовательское умножение матрицы p1 на p3. По

пользовательскому умножению матриц мы ссылаемся на пользовательское взвешенное воздействие с индивидуальной нормализацией, как описано выше.

P5 описывает оценки отношений каждого документа к каждому целевому классу и вычисляется с помощью пользовательского умножения матриц.

P6 описывает оценки отношений каждого документа к каждому критерию оценки, а также вычисляется с помощью пользовательского умножения матриц.

Основным результатом всего процесса является матрица P5, которая описывает отношения каждого документа к целевым классам, состоящим из критериев оценки.

Матрица P6 также может иметь некоторую полезность в зависимости от того, насколько независимыми являются критерии оценки.

4 Данные и верификация

Матрица P2 была получена путем тематического моделирования BigARTM на корпусе из 804829 новостных публикаций из 40 казахстанских источников, опубликованных с 01.01.2018 по 31.12.2019.

Модель BigARTM была рассчитана с помощью гладкого "разреженного регуляризатора тета" (tau=0.15), "регуляризатора декоратора phi" (tau=0.5) и "регуляризатора улучшенной когерентности phi" (tau=0.2), количество тем - 200. Параметры были выбраны в ходе оптимизации поиска по сетке.

Отрицательные значения тональности по каждой теме были получены путем ручной маркировки двумя экспертами, которые были перепроверены на несоответствия, скорректированы и усреднены. Каждая тема была представлена 25 основными словами/фразами, и каждому эксперту было предложено дать оценку тональности этой темы по шкале от 0 до 10, 5 - нейтрально, 0 - очень положительно и 10 - очень отрицательно. Следует отметить, что обозначение настроений может не отражать мнение автора в каждом тексте, а скорее отражать негативность или позитивность события, описанного в данной новостной публикации.

Топовые новости по негативной тональности (Таблица 1) в основном состоят из убийств, запланированных расследований террористической деятельности, катастроф (таких, как взрыв в Арыси в 2019) и вопросов, связанных с правами человека (митинги, свобода собраний, полицейский произвол и т.д.).

Таблица 1. Лучшие новости по негативной тональности

Sentiment_m4a	**Дата**	**Заголовок**	**Источник**
0,857	2019-11-01	У жителя Алматы был конфискован целый арсенал оружия.	24.kz/ru
0,857	2019-05-06	В Арысе произошел взрыв боеприпасов	nur.kz
0,853	2018-03-13	Движение "Демократический выбор Казахстана", признанное экстремистским	365info.kz
0,851	2020-05-28	Еще одного активиста вызвали на допрос после запрета движения "Кеше Партиясы".	rus.azattyq.org

0,846	2020-01-05	Подозреваемый в покушении на убийство задержан в Темиртау.	today.kz

Таблица 1 показывает, что главные новости по оценочным значениям действительно соответствуют соответствующим критериям. Однако такая ручная проверка, естественно, не может быть использована для проверки результатов модели. Поэтому была предложена методология перекрестной проверки новостей:

1) Подгруппа в 20% новостных публикаций была случайным образом сформирована для тестирования.

2) Расчет проводился, начиная со стадии моделирования темы, без учета новостей в тестовом наборе.

3) Затем, когда были получены все необходимые веса (матрицы P1-P4), матрицы P5 и P6 были рассчитаны для всего корпуса, как тестового набора, так и тренировочного.

4) Случайная подвыборка из 1000 новостей, помеченных как тестовый набор, была выбрана случайным образом из верхних 10 процентов и нижних 10 процентов в соответствии с расчетными оценками. Причина рассмотрения только верхних и нижних новостей заключается в том, что эксперименты показали, что значительная часть новостей не может быть ясно помечена ни экспертом, ни системой, поскольку не все новости, например, являются определенно позитивными или негативными, тем более, что мы имеем дело с профессиональной журналистикой, которая должна быть нейтральной и беспристрастной. Следует отметить, что 20 процентов корпуса - это по-прежнему значительный объем новостей - около 160000. Следовательно, цель проверки - убедиться в том, что точность модели высока, в то время как полнота не считается критическим в соответствии с предложенной методикой.

5) Эти подвыборки были вручную маркированы экспертами. Экспертам были предоставлены название, дата, url и медиа-источник.

6) Были рассчитаны показатели качества в сравнении с экспертной разметкой.

Таблица 2. Результаты проверки модели

Критерий	MAE	F1	ROC AUC
Негативная тональность	0.14	0.93	0.93

В таблице 2 приведены результаты проверки модели. Отрицательные настроения были предсказаны с ROC AUC 0,93, с точностью 0,94 и полнотой 0,94. Следует отметить, что такие результаты были получены простой моделью (без применения глубокого обучения) и все необходимые расчеты весов/параметров требовали минимальной ручной маркировки.

5 Заключение

В работе предложен метод, позволяющий классифицировать публикацию по любому семантически сложному критерию без необходимости создания большого размеченного корпуса документов. В частности по новостным публикациям отрицательной тональности

Предложенная модель была проверена как на основе списков ведущих новостных изданий по негативной тональности, которые выглядят логически последовательными, так и на основе стандартных метрик ML, таких как F1 Score и

ROC AUC, рассчитанных на подвыборке из 1000 новостей, помеченных экспертами вручную.

Отметим, что описанный подход имеет ряд ограничений:

- Тематическое моделирование, применяемое для получения векторных представлений текстов, работает с так называемыми мешками слов и не учитывает более тонкую семантику текстов, порядок слов n-грамм и т.д., что существенно ограничивает качество алгоритма.

- Экспертные оценки тем отличаются субъективностью.

- Описанный подход лучше всего подходит для больших корпусов (не менее 50-100 тыс. текстов) длинных текстов (не менее 100-150 слов и более). Предварительные эксперименты показали, что применение предложенной модели к меньшим корпусам, показывает значительно худшие результаты.

Для преодоления этих недостатков в дальнейших исследованиях предлагается применять модели, использующие методы дистрибутивной семантики для формирования тематической модели, либо перенести проблему высокоуровневой маркировки в текстовое пространство. Предполагается, что при таком подходе будет учитываться семантическое содержание текста, в отличие от подсчета количества слов.

Предложенная модель была реализована в как часть информационной системы мониторинга и оценки СМИ [13]. Разработанная система позволяет решать как классические задачи, такие как простые отчеты или анализ настроений, так и имеет ряд уникальных примеров использования, отличающих ее от существующих решений, таких как анализ на уровне тем и возможность выполнять анализ сущностей без поиска по ключевым словам.

Финансирование

Работа финансировалась за счет гранта BR05236839 Министерства образования и науки Республики Казахстан.

Литература

1. Bushman B. J., Whitaker J. Media Influence on Behavior //Encyclopedia of Human Behavior: Second Edition. – Elsevier Inc., 2012. – С. 571-575.

2. Mishra S., Rizoiu M. A., Xie L. Feature driven and point process approaches for popularity prediction //Proceedings of the 25th ACM international on conference on information and knowledge management. – 2016. – С. 1069-1078.

3. Tatar A. et al. Ranking news articles based on popularity prediction //2012 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining. – IEEE, 2012. – С. 106-110.

4. Bandari R., Sitaram A., Huberman B. A. 2012. The pulse of news in social media: Forecasting popularity //Proceedings of the Sixth International Conference Weblogs and Social Media, Palo Alto, CA: Association for the Advancement of Artificial Intelligence.

5. Mashechkin I. V., Petrovskiy M. I., Tsarev D. V. Metody vychislenija relevantnosti fragmentov teksta na osnove tematicheskix modelej v zadache avtomaticheskogo annotirovanija [Methods of text fragment relevance estimation based on the topic model analysis in the text summarization problem] //Vychislitel'nye Metody i Programmirovanie [Numerical Methods and Programming]. – 2013. – Т. 14. – С. 91-102.

6. Devlin J. et al. Bert: Pre-training of deep bidirectional transformers for language understanding //arXiv preprint arXiv:1810.04805. – 2018.

7. Пархоменко П. А., Григорьев А. А., Астраханцев Н. А. Обзор и экспериментальное сравнение методов кластеризации текстов //Труды Института системного программирования РАН. – 2017. – Т. 29. – №. 2. – С. 161-200.

8. Воронцов К. В., Потапенко А. А. Регуляризация, робастность и разреженность вероятностных тематических моделей //Компьютерные исследования и моделирование. – 2012. – Т. 4. – №. 4. – С. 693-706.

9. Vorontsov K. et al. Bigartm: Open source library for regularized multimodal topic modeling of large collections //International Conference on Analysis of Images, Social Networks and Texts. – Springer, Cham, 2015. – С. 370-381.

10. Blei D. M., Ng A. Y., Jordan M. I. Latent dirichlet allocation //Journal of machine Learning research. – 2003. – Т. 3. – №. Jan. – С. 993-1022.

11. Mukhamediev R. I. et al. Multi-criteria spatial decision making supportsystem for renewable energy development in Kazakhstan //IEEE Access. – 2019. – Т. 7. – С. 122275-122288.

12. Мухамедиев Р. И. и др. Эксперименты по оценке средств массовой информации на основе тематической модели корпуса текстов //Cloud of Science. – 2020. – Т. 7. – №. 1. – С. 87-103.

13. Barakhnin V. B. et al. The design of the structure of the software system for processing text document corpus //Бизнес-информатика. – 2019. – Т. 13. – №. 4 (eng).

ПРАКТИЧЕСКИЕ РАССУЖДЕНИЯ В БАЙЕСОВСКИХ СЕТЯХ

Шаяхметова А.С., Литвиненко Н.Г., Литвиненко Г.Г.
E-mail: asemshayakhmetova@mail.ru
Институт информационных и вычислительных технологий КН МОН РК, Алматы. Казахстан

Аннотация

Статья посвящена некоторым вопросам, возникающим при разработке алгоритмов для решения расчетных задач в байесовских сетях. Коротко рассмотрена теория потенциалов применительно теории байесовских сетей. На примере показаны возможности использования потенциалов. Проблемам использования нескольких байесовских сетей при исследовании прикладных задач. Существуют прикладные задачи, которые достаточно сложно адекватно описать моделью, представляющей из себя единственную байесовскую сеть. В тоже время в исследуемой задаче могут существовать блоки с различными видами неопределенностей, которые хорошо описываются байесовскими сетями.

Ключевые слова: *Байесовские сети, Ориентированный граф, теория потенциалов*

Практические алгоритмы обновления вероятностей в байесовских сетях

В данной статье мы рассмотрим алгоритмы обновления вероятностей в байесовских сетях. Эффективный алгоритм обновления имеет основополагающее значение для применимости байесовских сетей так как объединенная таблица вероятностей увеличивается экспоненциально с числом переменных. К сожалению,

ни один из известных методов не гарантирует гибкий вычислительный процесс. Дальше будет рассмотрен один из наиболее известных методов [1].

Для описания расчетов в байесовской сети более удобно использовать потенциалы, по сути являющиеся эквивалентом условных вероятностей. Использование потенциалов позволяет формализировать многочисленные свойства алгебры умножения и маргинализации таблиц. Для байесовских сетей потенциал — это аналог таблиц совместных, условных вероятностей, однако потенциал вовсе не обязан представлять собой вероятности.

Потенциал **φ** является вещественной функцией над некоторой областью конечных переменных **X**:

$\boldsymbol{\varphi : sp(X) \to R}$

Область определения переменной X обозначается и записывается как dom (X) и обозначает состояния, которые может принимать X.

Область потенциала обозначается через **dom(φ)**. Например, область потенциала **P (A, B|C)** есть **dom(P (A, B|C)) = {A, B, C}**.

Два потенциала можно умножить. Иногда умножение обозначатся точкой [2]. В случае байесовских сетей, когда потенциалы соответствуют таблицам условных вероятностей, эта операция соответствует декартову произведению таблиц.

Умножение потенциалов имеет следующие свойства:

1. $\mathbf{dom(\varphi_1\varphi_2) = dom(\varphi_1) \cup dom(\varphi_2)}$.
2. Коммутативный закон: $\boldsymbol{\varphi_1\varphi_2 = \varphi_2\varphi_1}$.
3. Ассоциативный закон: $\boldsymbol{(\varphi_1\varphi_2)\varphi_3 = \varphi_1(\varphi_2\varphi_3)}$.
4. Существование единицы: потенциал единицы 1 — это потенциал, который содержит только 1 и определяется для любой области, таким образом, что $\mathbf{1 \cdot \varphi = \varphi}$, для всех потенциалов **φ**.

Одна из важнейших операций, которую можно проводить с потенциалами, — это маргинализация. Проиллюстрируем её на примере. Общая идеология применения теории потенциалов к байесовским сетям такова [3]: потенциал — это таблица условных вероятностей вида

$\mathbf{P(X_1, X_2, \ldots, X_k \mid Y_1, Y_2, \ldots, Y_n)}$.

Маргинализация позволят уменьшить количество переменных.

$$\mathbf{P(X_1, X_2, \ldots, X_{j-1}, X_{j+1}, \ldots, X_k | Y_1, Y_2, \ldots, Y_n)} = \sum_{\mathbf{X_j}} \mathbf{P(X_1, X_2, \ldots, X_k | Y_1, Y_2, \ldots, Y_n)}$$

Оператор маргинализации может быть обобщен на потенциалы таким образом, что:

$\sum_A \boldsymbol{\varphi}$ есть потенциал над **dom (φ) \ {A}**.

Маргинализация является коммутативной:

$$\sum_A \sum_B \boldsymbol{\varphi} = \sum_B \sum_A \boldsymbol{\varphi}$$

Для потенциалов вида **P (A | V),** где **V** - множество переменных, имеем:

5. $\sum_{\mathbf{A}} \mathbf{P(A \mid V) = 1}$.

Для маргинализации справедливо следующее:

6. Дистрибутивность. Если $\mathbf{A \notin dom(\varphi_1)}$ тогда $\sum_A \boldsymbol{\varphi_1 \varphi_2} = \boldsymbol{\varphi_1} \sum_A \boldsymbol{\varphi_2}$,

Дистрибутивный закон обычно известен как ab + ac = a (b + c), и предыдущая формула фактически является тем же законом, который применяется к таблицам. Для проверки рассмотрим расчеты в таблицах.

B \ A	a_1	a_2
b_1	x_1	x_2
b_2	x_3	x_4

φ_1(A, B)

B \ C	a_1	a_2
b_1	y_1	y_2
b_2	y_3	y_4

φ_2(C, B)

B \ A	a_1	a_2
b_1	(x_1y_1, x_1y_2)	(x_2y_1, x_2y_2)
b_2	(x_3y_3, x_3y_4)	(x_4y_3, x_4y_4)

φ_1(A, B)·φ_2(C, B)

B \ A	a_1	a_2
b_1	$(x_1y_1 + x_1y_2)$	$(x_2y_1 + x_2y_2)$
b_2	$(x_3y_3 + x_3y_4)$	$(x_4y_3 + x_4y_4)$

$\sum_C \boldsymbol{\varphi_1}(\mathbf{A},\mathbf{B}) \cdot \boldsymbol{\varphi_2}(\mathbf{C},\mathbf{B})$

B	
b_1	$(y_1 + y_2)$
b_2	$(y_3 + y_4)$

$\sum_C \boldsymbol{\varphi_2}(\mathbf{C},\mathbf{B})$

B \ A	a_1	a_2
b_1	$x_1(y_1 + y_2)$	$x_2(y_1 + y_2)$
b_2	$x_3(y_3 + y_4)$	$x_4(y_3 + y_4)$

$\boldsymbol{\varphi_1}(\mathbf{A},\mathbf{B}) \sum_C \boldsymbol{\varphi_2}(\mathbf{C},\mathbf{B})$

Также используется термин проекция для маргинализации. Например, если **A** и **B** изолированы от **φ(A, B, C),** можно сказать, что **φ** спроецирован на **C**, и мы используем обозначение $\boldsymbol{\varphi}^{\downarrow C}$. В этой записи свойства маргинализации выглядят следующим образом (**V** и **W** обозначают наборы переменных):

7. Коммутативный закон. $(\boldsymbol{\varphi}^{\downarrow V})^{\downarrow W} = (\boldsymbol{\varphi}^{\downarrow W})^{\downarrow V}$
8. Дистрибутивный закон. Если $\mathbf{dom}(\boldsymbol{\varphi_1}) \subseteq \mathbf{V}$, то $(\boldsymbol{\varphi_1}\,\boldsymbol{\varphi_2})^{\downarrow V} = \boldsymbol{\varphi_1}\,(\boldsymbol{\varphi_2}^{\downarrow V})$

Кратко рассмотрим алгоритмы обновления вероятностей. Эффективный алгоритм обновления имеет основополагающее значение для применимости байесовских сетей так как объединенная таблица вероятностей увеличивается экспоненциально с числом переменных. К сожалению, ни один из известных методов не гарантирует гибкий вычислительный процесс. Дальше будет рассмотрен один из наиболее известных методов [4-5].

Для описания расчетов в байесовской сети более удобно использовать потенциалы, по сути являющиеся эквивалентом условных вероятностей. Для алгебры таблиц вероятностей для удобства обозначений будем использовать функциональные обозначения. То есть произведение P(A | pa (A)) P(B | pa (B)) рассматривается как произведение двух функций φ1(A, pa (A))*φ2(B, pa (B)).

Алгоритм обновления вероятностей рассмотрим на учебном примере.

Рассмотрим байесовскую сеть (рисунок 1) над множеством переменных U. Потенциалы, заданные для данной байесовской сети BN: **φ1 = P (A1), φ2 = P (A2 | A1), φ3 = P (A3 | A1), φ4 = P (A4 | A2), φ5 = P (A5 | A2, A3) и φ6 = P (A6 | A3).**

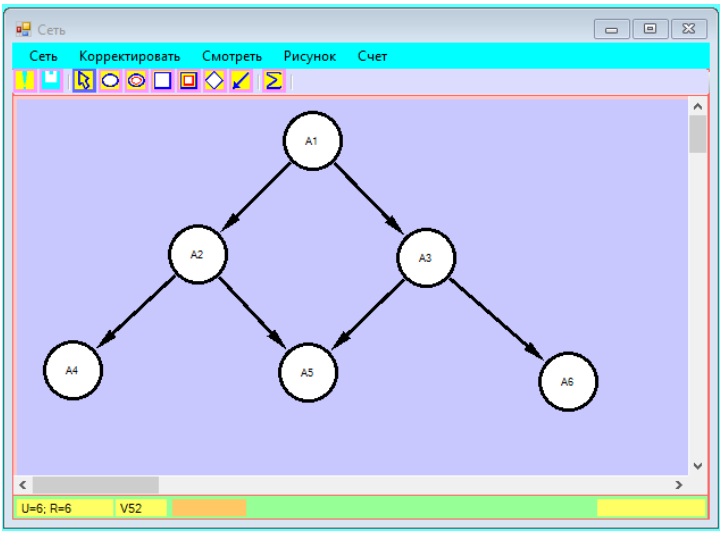


Рисунок 1 - Байесовская сеть

Предположим, что мы хотим вычислить P(A4). Из правила цепочки имеем:

$\mathbf{P(U)=\varphi1\varphi2\varphi3\varphi4\varphi5\varphi6}$ **и** $\mathbf{P(A4)} = \sum_{\mathbf{A1,A2,A3,A5,A6}} \boldsymbol{\varphi}\mathbf{1}\boldsymbol{\varphi}\mathbf{2}\boldsymbol{\varphi}\mathbf{3}\boldsymbol{\varphi}\mathbf{4}\boldsymbol{\varphi}\mathbf{5}\boldsymbol{\varphi}\mathbf{6}$

Используя закон распределения, получим:

$$\mathbf{P(A4)} = \sum_{\mathbf{A1}} \boldsymbol{\varphi}\mathbf{1(A1)} \sum_{\mathbf{A2}} \boldsymbol{\varphi}\mathbf{2(A2,A1)}\boldsymbol{\varphi}\mathbf{4(A4,A2)} \sum_{\mathbf{A3}} \boldsymbol{\varphi}\mathbf{3(A3,A1)}$$
$$\sum_{\mathbf{A5}} \boldsymbol{\varphi}\mathbf{5(A5,A2,A3)} \sum_{\mathbf{A6}} \boldsymbol{\varphi}\mathbf{6(A6,A3)}$$

Вначале вычисляем $\boldsymbol{\sigma}\mathbf{6(A3)} = \sum_{\mathbf{A6}} \boldsymbol{\varphi}\mathbf{6(A6,A3)}$. Очевидно, $\boldsymbol{\sigma}\mathbf{6(A3)}$ не зависит от переменной **A6**. Получим

$$\mathbf{P(A4)} = \sum_{\mathbf{A1}} \boldsymbol{\varphi}\mathbf{1(A1)} \sum_{\mathbf{A2}} \boldsymbol{\varphi}\mathbf{2(A2,A1)}\boldsymbol{\varphi}\mathbf{4(A4,A2)} \sum_{\mathbf{A3}} \boldsymbol{\varphi}\mathbf{3(A3,A1)} \sum_{\mathbf{A5}} \boldsymbol{\varphi}\mathbf{5(A5,A2,A3)}\, \boldsymbol{\sigma}\mathbf{6(A3)}$$

Затем вычисляем $\boldsymbol{\sigma}\mathbf{5(A2,A3)} = \sum_{\mathbf{A5}} \boldsymbol{\varphi}\mathbf{5(A5,A2,A3)}\boldsymbol{\sigma}\mathbf{6(A3)}$. $\boldsymbol{\sigma}\mathbf{5(A2,A3)}$ уже не зависит от переменной **A5**. В итоге получаем

$$\mathbf{P(A4)} = \sum_{\mathbf{A1}} \boldsymbol{\varphi}\mathbf{1(A1)} \sum_{\mathbf{A2}} \boldsymbol{\varphi}\mathbf{2(A2,A1)}\boldsymbol{\varphi}\mathbf{4(A4,A2)} \sum_{\mathbf{A3}} \boldsymbol{\varphi}\mathbf{3(A3,A1)}\, \boldsymbol{\sigma}\mathbf{5(A2,A3)}$$

Затем вычисляем

$$\boldsymbol{\sigma}\mathbf{3(A1,A2)} = \sum_{\mathbf{A3}} \boldsymbol{\varphi}\mathbf{3(A3,A1)}\boldsymbol{\sigma}\mathbf{5(A2,A3)}.$$

$$\mathbf{P(A4)} = \sum_{\mathbf{A1}} \boldsymbol{\varphi}\mathbf{1(A1)} \sum_{\mathbf{A2}} \boldsymbol{\varphi}\mathbf{2(A2,A1)}\boldsymbol{\varphi}\mathbf{4(A4,A2)}\, \boldsymbol{\sigma}\mathbf{3(A1,A2)}$$

Затем вычисляем

$$\boldsymbol{\sigma}\mathbf{2(A1,A4)} = \sum_{\mathbf{A2}} \boldsymbol{\varphi}\mathbf{2(A2,A1)}\boldsymbol{\varphi}\mathbf{4(A4,A2)}\boldsymbol{\sigma}\mathbf{3(A1,A2)}.$$

$$\mathbf{P(A4)} = \sum_{\mathbf{A1}} \boldsymbol{\varphi}\mathbf{1(A1)}\, \boldsymbol{\sigma}\mathbf{2(A1,A4)} = \boldsymbol{\sigma}\mathbf{1(A4)}$$

Затем вычисляем $\mathbf{P(A4)} = \boldsymbol{\sigma}\mathbf{1(A4)}$.

Это типичная схема расчета вероятности какой-либо переменной байесовской сети. Мы постепенно избавлялись от переменных, пока не осталась переменная, которую необходимо рассчитать. Однако есть много нюансов, некоторые из этих нюансов рассмотрим далее.

Причиной использования закона распределения является уменьшение размера таблиц для обработки. Для полного представления **P(U)** требуется пространство, включающее все шесть переменных. Для процесса, показанного на рисунке 2, самый большой потенциал для обработки содержит три переменные. Потенциалы обозначены в эллипсах, домены потенциалов обозначены в прямоугольниках. Можно отметить, что здесь незримо используется свойство марковости байесовской сети – если знаем настоящее, то для расчетов будущего не нужно знать прошлого.

Постепенное избавление в расчетах от переменных есть суть маргинализации переменных при расчетах в байесовской сети.

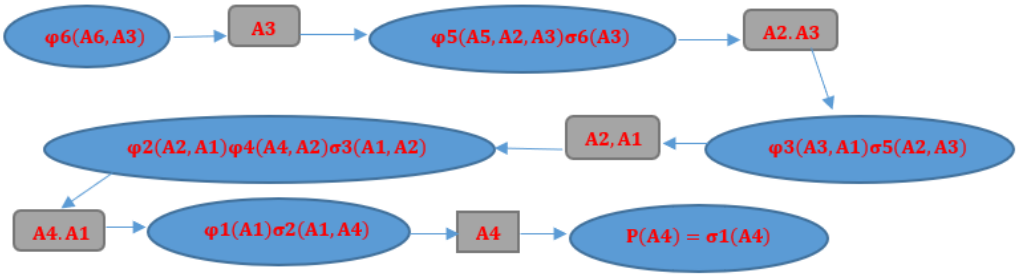


Рисунок 2 - Маргинализация переменных при расчетах в байесовской сети

В предыдущих расчетах мы выполняли маргинализацию в определенном порядке, а именно**: A6, A5, A3, A2, A1,** и это отражено в структуре на рисунке 2. Поскольку маргинализация является коммутативной, она может быть выполнена в любом порядке. Обычно используется термин «порядок исключения», а не «порядок маргинализации». Если мы используем обратный порядок исключения, мы получаем структуру на рисунке 3**.**

$$\mathbf{P(A4) = \sum_{A6,A2,A3} \varphi 6(A6,A3) \sum_{A5} \varphi 5(A5,A2,A3) \sum_{A2} \varphi 4(A4,A2) \sum_{A1} \varphi 3(A3,A1) * \sum_{A1} \varphi 2(A2,A1) \sum_{A1} \varphi 1(A1)}$$

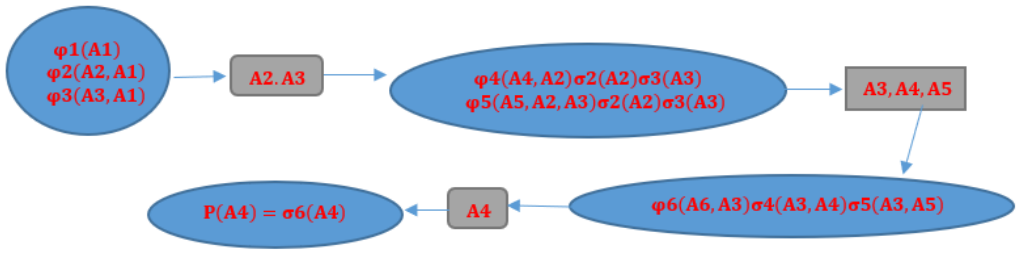


Рисунок 3 - Структура маргинализация

Расчеты в байесовской сети достаточно объемны и объемны, в первую очередь по данным. Объемность по вычислениям или вообще отсутствует или играет второстепенную роль. Основная проблема при разработке алгоритмов – где и как хранить данные. Поскольку размер обрабатываемых доменов является хорошей мерой сложности, необходимо решить задачу поиска порядка исключения с наименьшими обрабатываемыми доменами.

В предыдущих расчетах мы предполагали, что никаких свидетельств не было введено в сеть. Анализируя процесс, показанный на рисунке 2, мы понимаем, что можно сделать некоторые упрощения. Поскольку **φ5 = P (A5 | A2, A3) и φ6 = P (A6 | A3),** мы имеем

$$\boldsymbol{\sigma 6(A3) = \sum_{A6} \varphi 6(A6, A3) = \sum_{A6} P(A6\,|A3) = 1}$$

$$\boldsymbol{\sigma 5(A2, A3) = \sum_{A5} \varphi 5(A5, A2, A3)\sigma 6(A3) =}$$

$$\boldsymbol{= \sum_{A5} \varphi 5(A5, A2, A3) * 1 = \sum_{A5} P(A5|A2, A3) = 1}$$

Продолжая дальше, получим:

$$\boldsymbol{\sigma 3(A1, A2) = \sum_{A3} \varphi 3(A3, A1)\sigma 5(A2, A3)}$$

$$\boldsymbol{= \sum_{A3} \varphi 3(A3, A1) * 1 = \sum_{A3} P(A3|A1) = 1}$$

Таким образом весь процесс

$$\boldsymbol{P(A4) = \sum_{A1} \varphi 1(A1) \sum_{A2} \varphi 2(A2, A1)\varphi 4(A4, A2) \sum_{A3} \varphi 3(A3, A1)}$$

$$\boldsymbol{\sum_{A5} \varphi 5(A5, A2, A3) \sum_{A6} \varphi 6(A6, A3)}$$

сводится к вычислению

$$\boldsymbol{P(A4) = \sum_{A1} P(A1) \sum_{A2} P(A2|A1)P(A4|A2)}$$

Узлы **A3, A5** и **A6** являются примерами так называемых бесплодных узлов (barren nodes). Узел **A** называют бесплодным, если ни **A,** ни кто-либо из его потомков не получили свидетельств. Потенциал условной вероятности, прикрепленный к бесплодному узлу, влияет только на узлы-потомки**.**

Если у нас есть свидетельства **A5 = a5** и **A6 = a6,** и свидетельства имеют два состояния, то справедливо следующее:

$$\boldsymbol{P(A4, e) = \sum_{A1,A2,A3,A5,A6} \varphi 1\varphi 2\varphi 3\varphi 4\varphi 5\varphi 6e5e6}$$

$$\boldsymbol{P(A4|e) = \frac{P(A4, e)}{\sum_{A4} P(A4, e)}}$$

Эффект состоит в том, что переменные **A5** и **A6** создаются в потенциалах **φ5 и φ6,** а маргинализации **A5** и **A6** являются избыточными, то есть **φ5 = P (A5 = a5 | A2, A3) и φ6 = P (A6 = a6 | A3).** Процесс, описанный в данном разделе, достаточно общий, чтобы охватить все типы сценариев свидетельств. Задача состоит в том, чтобы дополнить этот общий процесс методами, использующими преимущества упрощений для конкретного сценария свидетельств, таких как идентификация бесплодных узлов.

Предположим, что мы хотим вычислить **P(Ai, e)** для всех i. Не используя преимущества специального вида сценария свидетельств, мы можем для каждого узла использовать метод, рассмотренный ранее (рисунок 2). Предположим, что мы

вычисляем **P(A2, e)** через порядок исключения **A6, A5, A3, A1, A2.** Тогда схема потенциалов выглядит так, как показано на рисунке 4.

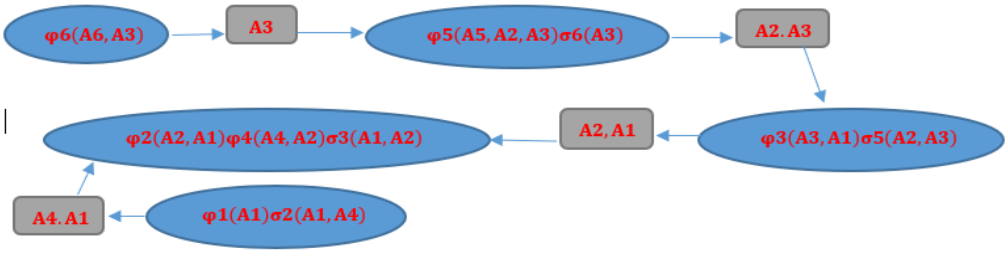


Рисунок 4. Схема потенциалов

Выводы

Как видно, схема на рисунке 4 очень похожа на схему на рисунке 2. Только две стрелки перевернуты. То есть многие вычисления из расчета **P(A4, e)** могут быть повторно использованы. Дальше мы покажем общую идею систематического способа повторного использования частных результатов при расчете всех маргиналов**.**

Литература:

1 Pearl J. Artificial Intelligence Applications // How to Do with Probabilities what people say you can't,/ Editor Weisbin C.R., IEEE, North Holland, 1985, 6–12 p.

2 Gorodetskiy V., Tulupiev A. Formation of consistent knowledge bases with uncertainty // RAS. Proceedings of the Academy of Sciences. Theory and control systems, 1997, - №.5, 33–42 p.

3 Gorodetskiy V. Modeling of underdetermined knowledge // SCM'98: SPb, 1998. - Vol.1. - 98–102 p.

4 Litvinenko A., Litvinenko N., Mamyrbayev O., Shayakhmetova A., Turdalyuly M. “Clusterization by the K-means method when K is unknown,” Inter. conf. «Applied Mathematics, Computational Science and Systems Engineering». Rome, Italy, 2019, - Vol. 24. - 1-6 p.

5 Tulupiev A. Algebraic Bayesian networks // Logical-probabilistic approach to modeling knowledge bases with uncertainty, SPb.: SPIIRAS, 2000, - 292 p.

ҚАЗАҚ ТІЛІ СӨЙЛЕУІН ТАНУДАҒЫ ӨЗЕКТІ МӘСЕЛЕЛЕРДІ ТАЛДАУ

[1]Мамырбаев Ө.Ж., [2] Қамзабек А.Н., [3] Абдуллахан С.А.
[2](e-mail: kamzabekaray@gmail.com)
[3](e-mail: saltanat.abd@icloud.com)
[1](e-mail: morkenj@mail.ru)
[1]Ақпараттық және есептеуіш технологиялар институты, 050000 Алматы, Қазақстан
[2]Қазақ Ұлттық Аграрлық Университеті 050010 Алматы, Қазақстан
[3]Қазақ Ұлттық Аграрлық Университеті 050010 Алматы, Қазақстан

Аннотация. *Осы мақалада ұсынылған тақырып қазіргі әлемде өте өзекті. Тану технологияларын кеңінен енгізу әртүрлі білім салаларындағы адамдардың дағдыларын жақсартуға мүмкіндік береді, олардың арасында шет тілдерін оқыту ерекше орын алады. Бұл мақалада бейнені тану технологиясына қысқаша шолу, қазіргі жағдайда сөйлеуді танудың маңыздылығын анықтау, сонымен қатар сөйлеушінің ерекшеліктерін ескере отырып, шет тілдерін оқытудың лингвистикалық тренажерын құрудың өзектілігі келтірілген.*

Сөйлеу сигналдарын танудағы басты мәселе спикердің екпіні мен сөйлеу ерекшеліктерінің болуы екендігі анықталды. Осыған байланысты осы мәселені барынша азайтып, студенттерге айтылымды жақсартуға көмектесетін тілдік тренажер жобасы жасалды. Мұндай тренажердің жұмысы шет тілін үйренуге кешенді тәсілге негізделген, өйткені ол төрт маңызды компонентті біріктіреді: жазу, тыңдау, оқу, сөйлеу.

1. Кіріспе

Жасанды интеллект (AI) саласындағы зерттеулер қазіргі уақытта адамзат үшін үлкен қызығушылық тудырады. Атап айтқанда, AI бағыттарының бірі – машиналық оқыту іс жүзінде кеңінен қолданылады және үлгіні тану (Pattern Recognition) мәселелерін шешеді.

Үлгіні тану – бұл объектілерді бірнеше санаттарға немесе сыныптарға жіктеуге бағытталған ғылыми пән. Нысандар суреттер деп аталады[1].

Соңғы бірнеше онжылдықта тану жүйелері компьютерлік өңдеудің айтарлықтай жетістіктерінің арқасында қол жетімді болды. Алайда, осы жаңа автоматтандырылған әдістердің көпшілігі бастапқыда жүздеген, тіпті мыңдаған жылдар бұрын жасалған идеяларға негізделген.

Тану дәлдігі бар әмбебап алгоритмдерді құру 100 % - бұл өте көп уақытты қажет ететін процесс және қазіргі уақытта іс жүзінде мүмкін емес көрінеді, қазірдің өзінде жоғары пайызды көрсететін тану жүйелері бар, тану адам қызметінің әртүрлі салаларында белсенді қолданылады[2] (сурет. 1).

Тану жүйелері өте кеңінен қолданылуда, ең көп тараған тану жүйелері:

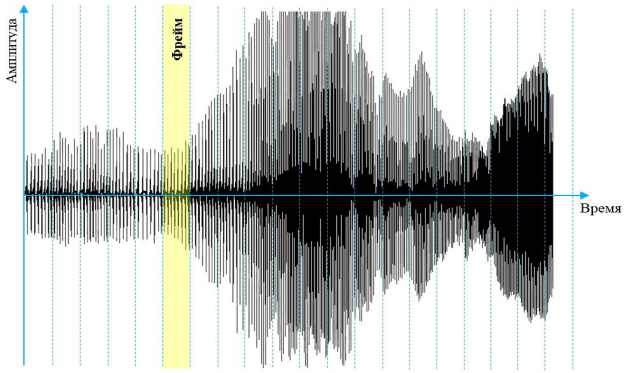
1. втокөлік нөмірін тану;
2. Символдарды тану;
3. Штрих-кодты тану;
4. Компьютерлік диагностика;
5. Дауысты тану;
6. Ақпараттық қауіпсіздік;
7. ДНК;
8. Құжаттарды топтастыру.

Сурет 1. Үлгіні тану теориясын практикада қолдану

2. Сөйлеуді тану технологиясы

Шет тілдерін үйрену кезінде тыңдау, оқу және жазу дағдыларын жетілдіруге арналған көптеген ақпараттық технологиялар бар, бірақ сөйлеу дағдыларын жетілдіруге жеткілікті көңіл бөлінбейді. Бірақ сонымен бірге білім алушы үшін дыбыстарды, әріптерді және тұтас сөздерді дұрыс айтуды үйрену маңызды, өйткені бұл оқытылатын тілдің ана тілімен қарым-қатынас жасау үшін негіз болып табылады. Бүгінгі таңда бұл мәселені шешудегі ең перспективалы бағыт-оқушының дауысының ерекшеліктеріне негізделген сөйлеуді тану технологияларын енгізу [3].

Сөйлеуді сәтті тану үшін әдетте жақтаулар деп аталатын бірнеше ондаған миллисекундтық дыбыстық сигналдың бөліктері қарастырылады (сурет. 2) [4]. Бұл тапсырманы орындау өте қиын, өйткені кейбір фонемалар бір-біріне өте ұқсас, бірақ сіз оны "ықтималдық"тұрғысынан шеше аласыз. Кейбір фонемалар бұл сигнал үшін ықтимал, ал басқалары аз. Акустикалық модель құрылады, ол кішкентай дыбыстық сигналдың (кадрдың) бөлігін қабылдайтын және осы кадрдағы әртүрлі фонемалардың ықтималдық үлестірімін беретін функция болып табылады. Акустикалық модельге сүйене отырып, белгілі бір дәрежеде айтылған нәрсені қалпына келтіруге болады.



Сурет 2. Сөйлеу сигналын фреймдарға бөлу

Осы тұрғыдан мәселені қарастыра отырып, сіз сөйлеуді танудың жалпы моделіне келе аласыз, ол қазіргі кезде жиі қолданылады – Жасырын Марков Моделі (ЖММ).

2.1 ЖММ арқылы сөйлеуді тану жүйесінің құрылымы

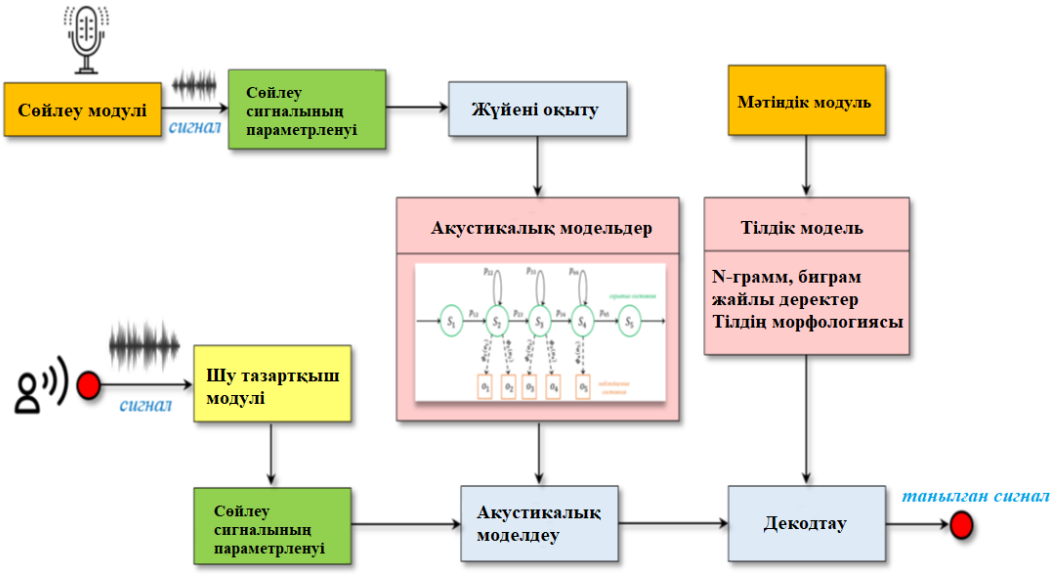
Жалпы жағдайда жасырын Марков модельдеріне негізделген сөйлеуді тану жүйесінің құрылымы келесі элементтерден тұрады (сурет. 3):

* акустикалық модель-қабылданған сөйлеу сигналын сөйлеудегі белгілі бір дыбыстарды (әріптер, сөздер) сипаттайтын алдын-ала жасалған көптеген дыбыстық модельдермен (СММ) салыстырады;

* тілдік модель-мүмкін болатын ауызша тізбекті анықтайды; әр түрлі тілдер үшін бұл модель басқаша көрінеді: мысалы, орыс тілі үшін жүйені қиындататын бір сөздің көптеген формаларын ескеру қажет, ал ағылшын тілінде статистикалық модельдерді (N-грамм) қолдану жеткілікті);

* шуды тазарту модулі және пайдалы сигнал бөлімі;

* декодер-акустикалық және тілдік модельдерден тану процесінің деректерін салыстырады және танылған сөйлеу сигналының алынған тізбегін шығарады[5].

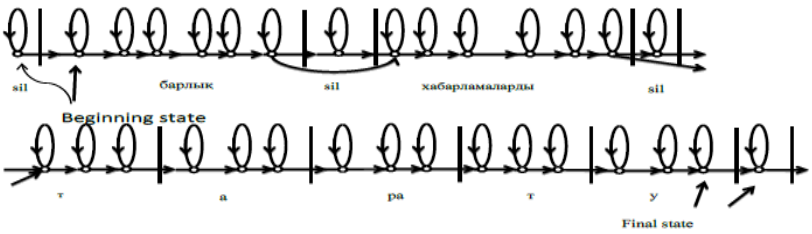


Сурет 3. ЖММ негізінде сөйлеуді тану жүйесінің сұлбасы

Сипаттамасы 60-шы жылдардың соңында жарияланған жасырын Марков модельдері (ЖММ) жақында танымал болды. Біріншіден, СММ-нің математикалық құрылымы өте бай және ғылымның әртүрлі салаларындағы математикалық мәселелерді шешуге мүмкіндік береді. Екіншіден, сауатты жобаланған модель іс жүзінде жақсы жұмыс нәтижелерін береді.

ЖММ сөйлеу сигналының едәуір өзгерістерін және статикалық модельдеу аппаратындағы ауызекі сөйлеу тілі құрылымын модельдеуге мүмкіндік береді. ЖММ сөйлемдегі фонемаларды іс жүзінде көптеп қолдануды сипаттау үшін Марков тізбегін пайдаланады.

4 суретте сөз бөліктерінің әртүрлі контекстік – тәуелді модельдерінен құрастырылған аяққы қалыптардағы «барлық хабарламаларды тарату» сөйлемдері үшін жасырын Марков моделінің жұмыс сызбасы көрсетілген:



4 сурет. Жасырын Марков моделінің жұмыс сызбасы

3. Қазақ тілін танудағы кездесетін проблемалар

Сөйлеуді танудың көптеген әдістері мен алгоритмдері белгілі бір тілге тәуелді емес екеніне қарамастан, сөйлеуді тану жүйесін жасау кезінде қарастырылып отырған тілдің ерекшелігін ескеру қажет. Әр тілдің фонетикалық немесе грамматикалық құрылымына қатысты өзіндік ерекшеліктері бар.

Қазақ тілі түркі тілдер отбасынан шыққан және Қазақстанда кириллицамен жазылады, дегенмен басқа елдердегі қазақтар әліпбидің араб және латын вариацияларын бейімдеді. Қазіргі қазақ кирилл алфавитінде 42 әріп бар, олардың 15-і номиналды түрде дауысты дыбыстарға, 27-сі дауыссыз дыбыстарға жатады[6]. Алайда, қазақтың байырғы дауысты дыбыстарының нақты саны және олардың жіктелуі әлі күнге дейін пікірталас тақырыбы болып табылады. Қазақ тілінің фонетикасы бойынша Мемлекеттік стандарт жоқ екенін, ал қазақ тілі бойынша қазіргі заманғы оқулықтар мен оқу құралдарының авторлары бұл мәселе бойынша бірыңғай пікір қалыптастырмағанын атап өткен жөн

Сондықтан, бірінші проблема – бұл сөйлеу сигналын ұсынудың фонетикалық тәсілін пайдаланатын, біріктірілген сөйлеуді тану жүйесін құру үшін аса маңызды қазақ тілінің фонетикалық құрылысының бірыңғай және келісілген сипаттамасының болмауы.

Қазақ тілінің дыбыстарына толық талдау жүргізу үшін әр түрлі жыныстағы, жастағы және аймақтардағы қазақ тілінің сөйлеушілерінің айтылуын қамтитын нақты сөйлеу сигналдарының өкілді акустикалық базасының болуы талап етіледі. Осыған байланысты тағы бір мәселені атауға болады – бұл акустикалық-өкілдік мәліметтер базасының болмауы. Акустикалық мәліметтердің болуы қазақ тілінің дыбыстарын фонетикалық-акустикалық талдауға және жіктеуге мүмкіндік беріп қана қоймай, сонымен қатар қазақ тілін тану жүйесі үшін акустикалық модельдерді құруға негіз болады.

4. Қорытынды

Қорыта келгенде, қазақ тілін танудағы басты проблемалардан басқа, елдің әртүрлі аймақтарында және одан тыс жерлерде нақты диалектілермен байланысты проблемалар бар. Мысалы, жергілікті қазақтардың сөзі Моңғолияда тұратын этникалық қазақтардың сөзінен біршама ерекшеленеді. Тіпті Қазақстанның өзінде елдің оңтүстігінде тұратын халықтың сөзі елдің солтүстігінде немесе батысында тұратын халықтың сөзінен біршама ерекшеленеді. Мәселе біздің еліміздің екі тілділігімен күрделене түседі, өйткені орыс сөздері қарапайым және тіпті әдеби сөйлеуде араласуы мүмкін.

Қазақ тілін танудың практикалық жүйесін құру кезінде барлық көрсетілген проблемаларды ескеру қажет. Мақалада біз осы мәселелерді қандай да бір тәсілмен шешуге әр түрлі жол бар екенін көрсеттік.

Әдебиеттер

1. Мамырбаев О.Ж., Қыдырбекова А.С., Турдалыұлы М., Мекебаев Н.О. Дауыс бойынша пайдаланушыны идентификациялау және аутентификациялау әдістеріне шолу // “Инновациялық АТ және ақылды технологиялар” ғылыми конф. материалдары, 2019. – Б. 315-321.

2. Карабалаева М.Х. Система распознавания целых слов с использованием динамического выравнивания времени // Қазақстан Республикасы Ұлттық ғылым академиясының хабаршысы. – 2009. – №6. – С. 7-11.

3. Калимолдаев М.Н., Мамырбаев О.Ж., Қыдырбекова А.С., Миекебаев Н.О. I-векторлы бейнелеуді пайдаланып дауысты тексеру және идентификацияла// “Халықаралық математика және физика журналы” , 2019. – Б. 12-15.

4. Мамырбаев О.Ж., Тұрдалыұлы М, Мекебаев Н.О., Қыдырбекова А.С. Сандық жүйке желілерін қолданып сөйлеуді автоматты түрде тану// ACIIDS, Индонезия, Іс жүргізу, 2019 - II бөлім.

5. Gaikwad S.K., Gawali B.W., and Yannawar P., A review on speech recognition technique// International Journal of Computer Applications IJCA, 2018. - Vol. 10, No. 3, - P 16-24.

6. Torekhanov S., Sharipbayev A. The mathematical model of the set of Kazakh vowels // L.N. Gumilyov Eurasian National University Bulletin, Astana. – 2002. – Vol. 3-4. – P. 30–33.

MEL КӨМЕГІМЕН СӨЙЛЕУДІ ТАНУ ЖҮЙЕСІН ҚҰРУ КЕПСТРАЛДЫҚ ЖИІЛІК КОЭФФИЦИЕНТІ ӘДІСІ

[1]Мамырбаев Ө.Ж., [2]Қамзабек А.Н, [3]Абдуллахан С.А.
(e-mail: kamzabekaray@gmail.com)
(e-mail: saltanat.abd@icloud.com)
[3](e-mail: morkenj@mail.ru)
[1]Ақпараттық және есептеуіш технологиялар институты, 050010 Алматы, Қазақстан
[2]Қазақ Ұлттық Аграрлық Университеті 050010 Алматы, Қазақстан
[3]Қазақ Ұлттық Аграрлық Университеті 050010 Алматы, Қазақстан

Аннотация. *Сөйлеуді тану жүйелері теледүкендер, телебанк, ақпараттық қызметтер, үйді автоматтандыру, дауыстық хабарламалардың қауіпсіздігі және т. б. сияқты қосымшаларда кеңінен қолданыс тапты. Одан бөлек жүргізушіге қозғалыс кезінде қауіпсіз қоңырау шалуға мүмкіндік беретін дауыстық қоңыраулар жиынтығына айналды. Бұл жоба адам дауысының моделін қолдану арқылы сөйлеуді танудың жоғары тиімді жүйесін дамыту болып табылады. Адамның*

құлағының мінез-құлқын тану арқылы, Мэл - кепстралдық (Cepstral Coefficient MFCC) коэффициенттер жиілігі сипаттамалық қабілетін дамыту үшін қолданылады. Бұл мақалада адам сөйлеуі мен дыбыс сигналдарының ерекшеліктерін ажырата отырып, сөйлеу сигналдарын таниды қарастырамыз.

1. Кіріспе

Сөйлеуді тану - бұл сөйлеу сигналын танымал сөздерге немесе әріптерге статистикалық түрлендіру процесі болып табылады. Технология мүмкіндігі шектеулі адамдарға арналған қосалқы коммуникациялар, яғни телефон қоңыраулары, хабарламаларға жауап беру, қызмет көрсету кезінде автоматтандырылған көмек көрсету үшін сөйлеуді тану қажеттілігінен туындады. Сонымен қатар, сөйлеуді тану қызмет көрсету және қосалқы салаларда адам ресурстарын басқару құралына айналды. Сөйлеу үшін тану сәтті болуы керек, миллиондаған сөйлеу үлгілері бар үлкен анықтамалық мәліметтер базасы болу қажет, ал оны жаһандық коммуникациялардың әртүрлілігін ескере отырып, әр уақыт қолданып және кеңейтіліп отыруы керек. Сөйлеуді тану - бұл компьютерлік өзара әрекеттесу және үлгіні тану саласындағы тұрақты зерттеу тақырыбы болып табылады[1].

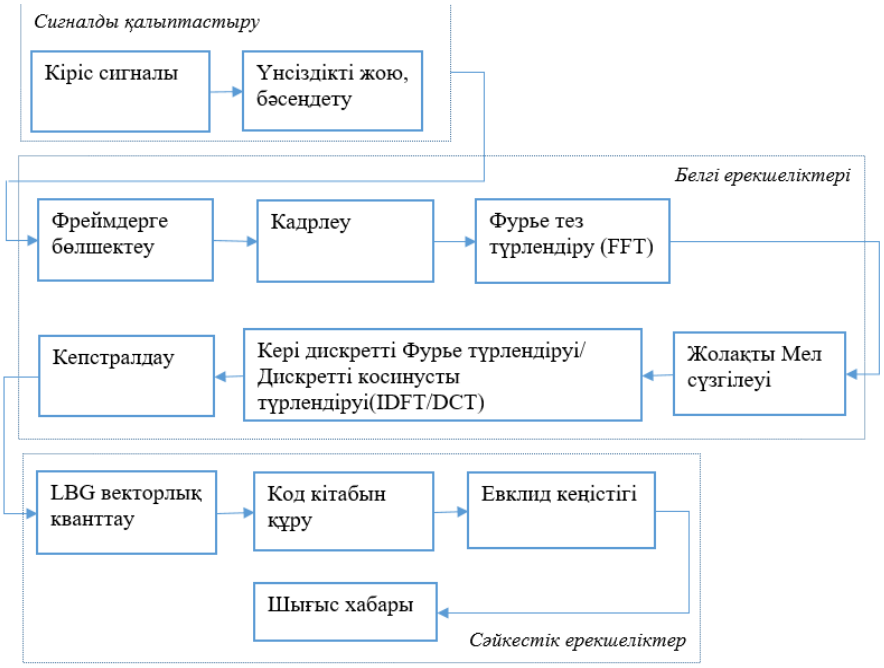
Нақты уақыт режимінде сөйлеуді нақты талдый алатын жүйелерге сұраныстың артуы байқалады. Мұндай жүйелерді үлкен мәліметтер базасына қойылатын талаптар, сөйлеу сигналдарының шуылға осалдығы және төмен өнімділік, жоғары есептеу талаптарына байласнысты кіріктірілген платформа арқылы басқару қиын.

Сөйлеуді тану технологиясы дегеніміз не, ол қалай жұмыс істейді және Мел – кепстралдық коэффициенттер жиілігі көмегімен сөйлеуді тану жүйесін құру әдісінің артықшылғы қандай? Осы мақалада біз жауап беруге тырысатын бірнеше сұрақтар бар[2].

2. Сөйлеуді тану блоктары

Сөйлеуді тану соңғы онжылдықта маңызды зерттеу саласына айналды. Осы қызығушылықтың нәтижесінде көптеген жаңа тәсілдер пайда болды. Әр техниканың белгілі бір тәсілді - белгілі бір кәсіпорын үшін құнды ете алатын тура дәлдікпен, өнімділік деңгейлеріне байланысты өзіндік ерекшеліктері бар. Адамның дауысы мен есту моделінің биометриясына ең жақын КЖКӘ әдісі.

Адамның құлағы 1 – 4 кГц жиіліктерге сезімтал, бірақ 8 килогерцке дейінгі де жиілікті қабылдай алады. У. Гайквад, М. Ахмедтің зерттеуілері бойынша [3] адамның құлағының мінез-құлқы сызықтық емес, бірақ сигналдағы қуат сызықтық парадигманы орындай алатынын болжайды. Сызықтық шкала сөйлеуді тану өнімділігін жақсарту үшін адамның биометриясына сәйкес болуы керек. Содан кейін алынған нысандар, мәтіндегі сөздермен салыстырылады. Сөйлеуді танудың әр жүйесіндегі ең бірінші процесс - белгілерді алу болып табылады. Белгілерді алудың ерекшелігі объектіні анықтау үшін қажетті дыбыстық сигналдардың компоненттерін оқшаулап, лингвистикалық мазмұнын ескере отырып, үнсіздікті жоққа шығарады.



1- сурет. Сөйлеуді танудың құрылымдық

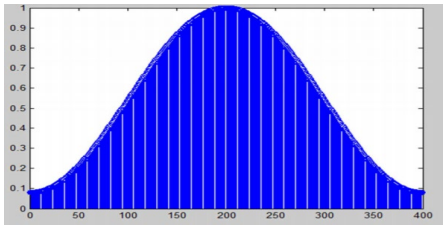
2.1 Кадр және терезе

Дыбыстық сигналдар үнемі өзгеріп отырады, бірақ зерттеушілер қысқа уақыт мерзімінде сигнал тұрақты екенін болжауы қажет. Шын мәнінде, дыбыстық сигнал 20-40 МС қысқа кадрларда талдануы керек. L. Muda, M. Begam және I. Elamvazuthi зерттеулерінде [4] кадрлардың кең ауқымы 5-тен 100 мс-қа дейінгі аралықта пайдалануға болмайды.

Егер қарастырылған кадрлар тым қысқа болса, онда бір кадр сенімді спектрлік бағалау үшін үлгілер жеткіліксіз болады.Егер кадрлар тым ұзақ болса, тағайындалған кадр кезінде сигнал өте көп өзгеріске ұшырайды. Сигнал 16 кГц жиілікте таңдалынса, және таңдалған кадр өлшемі стандарт 25 мс тең болады делік. Бір кадрдағы үлгілерді 0.025 x 16000 = 400 үлгі ретінде есептеуге болады, ал кадр қадамының өлшемі шамамен 10 мс (160 үлгі) болады. Бірінші кадр 0-ден 400-ге дейін және одан кейінгілері 160-тан 400 үлгіге дейін жалғасады. Сондықтан кадр және Де-кадр [5] процессі екі көрші кадр арасында корреляцияны қолдап, яғни ақпараттың жоғалуын азайту үшін кадрларды қабаттастыруды қажет етеді. Жүйенің бастапқы және кадрдың соңғы нүктелерінде сабақтастықты сақтау үшін *терезе фунциясы* қажет. Бұл жоба терезе фунциясы мақсаттары иілуінің тегістігінің күштілігіне байланысты Хемминг терезесін пайдаланады. Әр кадр Хемминг терезесіне көбейтілуі қажет. Терезені фунциясының қолдану мақсаты - әр кадрдың шеткі нүктелерінде сигналды нөлге тарту арқылы спектрлік бұрмалануды азайту болып табылады. Хемминг терезесі 2 суретте көрсетілген және 1 теңдеуімен жүзеге асырылады.

$$M(n) = X(n)' * W(n), \quad 0 \le n \le N-1, \text{ онда}$$
$$W(n)=0,54-0,46\cos(2\pi n/n-1), \; 0 \le n \le N-1 \qquad (1)$$

Терезе функциясы бойынша өңдегеннен кейін, әр кадрдың қуат спектрі есептеледі. Бұл процесс алынған бойлық толқындардың жиілігіне байланысты, әр түрлі жылдамдықпен дірілдейтін cochlea (адамның құлағындағы орган – ұлу тәрізді іспеттес) алынады. Cochlea қай нүктеде дірілдейтініне байланысты, белгілі бір дыбыстық толқында әртүрлі нервтер миға белгілі бір жиіліктерде сигнал жібереді.

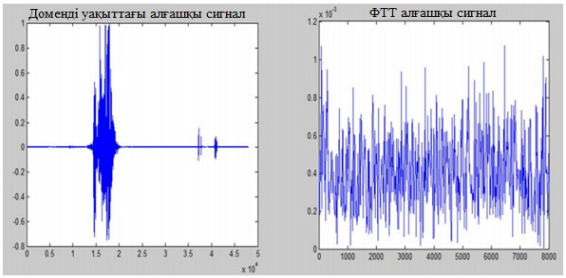


2- сурет. Хемминг терезесі.

2.2 Фурье тез түрлендіруі (FFT)

Сөйлеу сигналдары уақыттық аралығында өте тез және шұғыл өзгереді, ал егер уақыт аралығындағы сөйлеу сигналдарын жиілік шамасына айналдырсақ, онда тиісті спектрлік айқын көрінісін таба аламыз. Сөйлеу сигналдан кейін, жүйе сигналдарды фреймдерге бөледі, кадрдағы сөйлеу сигналдарының үздіксіздігін арттыру үшін терезе функциясын шақырады. Сандық сигналдарды спектрдің деректеріне түрлендіру үшін Фурье тез түрлендіруді.

Дыбыстық сигналды уақыт аймағынан жиілікке түрлендіру және жиілік спектрі бойынша энергияны бөлу 3 суретте көрсетілген. Есептеу уақытының төмендеуіне байласнысты ФТТ DFT – мен салыстырғанда 100 еседен астам жақсартылған өнімділік көрсетеді. DFT орнына ФТТ қолдану күрделі есептеулердің мөлшерін азайтады: $N^2 to(N/2)loglog_2N$. ФТТ жиілік спектрі бойынша энергияның бөлінуін білдіреді. Энергия спектрі сүзгілеу кезінде қолайлы және энергия тығыздығын бағалайды [5]. ФТТ коэффициенттерін 2 теңдеуді қолдана отырып есептеуге болады.

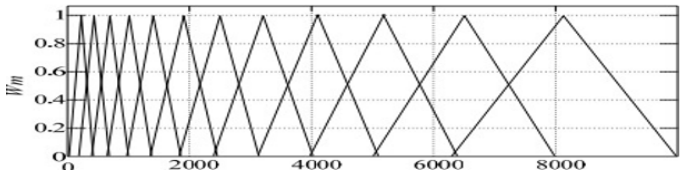


3 - сурет. Акустикалық кіріс сигналы және оның ФТТ көрінісі

2.3 Мел-сүзгілердің тарамы (MFW), Кепстр коэффициенті, Векторлық кванттау

Мел - сүзгілердің тарамы үшбұрышты қабаттасып жасалған ауырлық функциялары көмегімен орындалады. Бұл үшбұрышты ауырлық функциялары Мел-шкаладағы бірдей өтпелі жолақтың 50% бөгей отырып жабады (яғни Мел- сүзгі көршілес сүзгілердің орталық жиіліктері арасындағы жиіліктерді қамтиды). Сондықтан олар Мел-шкалада бірдей аймақ болып көрінеді, ал жиілік

диапазонындағы ені логарифмдік жиілікте өседі. Фильтрлердің ені мел-шкалада біркелкі болуы мүмкін. 4-суретте жиілік осіндегі 12 жолақтық мел-сүзгілердің жиынтығынан тұратын үшбұрышты ауырлық функцияларының үлгісі көрсетілген.



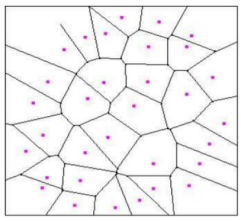
4 - сурет. 12 жолақты Мел-жиілік сүзгілерінің тарағы

Автоматтандырылған талдау кезінде спектрдің энергиясын әр мел-жолақта (сүзгі) бағалау қажет. Әрбір мел-сүзгідегі жиілік бойынша ажыратымдылықтың барлық элементтерінің энергиясынан тұратын *вектор – мел-спектр* болып табылады.

Мел-сүзгіштерінің үшбұрышты ауырлық функцияларын бөгейтініне байланысты, мел-спекторлы вектордың көршілес компоненттері бір-бірімен өзара байланысады. Логарифмдік мел-спектрде дискретті косинус түрлендіруін қолдану негізінде көршілес компоненттер арасындағы өзара корреляция айтарлықтай азаяды. Цифрлық сигналдарды өңдеу кезінде мел-жиілік *кепстралды коэффициенттері* пайда болады [6].

Векторлық кванттау (Vector Quantization (VQ)) - $A = \{a1, \dots, an\}$ бұл - кіріс векторларының желілік тізбегі үшін $W = \{w1, w2 \dots, wn\}$ коды бар векторларын векторлық кванттау міндеті болып табылады, оның өзі Q-ға сәйкес келетін кодтық векторынан алынған әрбір вектордың орнын басқан жағдайында ауытқушылықты минималдау міндеті болып қойылады[7].

Бұл берілген әдісте сөйлеу сигналының белгілерінің векторларының кіріс желілік тізбегінен алынған кодтары бар векторлардың көптеген жиыны пайдаланушы моделі болып табылады. Бұл көп жиынды құру үшін белгілер векторларының бастапқы желілік тізбегі L кластерлерге бөлінеді, сөйтіп кодтары бар векторлар ретінде олардың орта нүктелері алынады. *Векторлық кванттау әдісі* жүзеге асыруда – жеңіл және сөйлеушінің мәтінге тәуелсіз танып анықтау міндетінде қолданыла береді, алайда ол әр кезде тану дәлдігін бере алмайды. Егер код кітабының қажетті мөлшері 2 болса, онда процесс осы қадамда тоқтайды. Егер жоқ болса, онда бұл процесс қажетті код кітабын алу үшін жалғастыру керек.



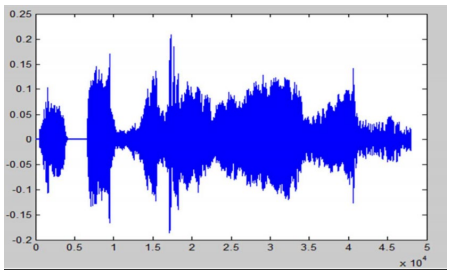
5 - сурет. Екі өлшемді кеңістіктегі векторлық кванттау

Сөз дерекқоры кіріс сигналын үйлестіру үшін жасалады. Кіріс сигналы жүйеге кірген уақытта, ол бұрын түсіндірілген барлық блоктардан өтеді. Код кітабы сигналдық және кодтық кітаптары кіріс сигналдарының кодтық кітабы арасындағы

ең аз Евклид кеңістігін тудырады. Шығатын қажетті сөз деректер базасынан кіріс сигналына дейінгі ең аз қашықтықтағы сөз болады.

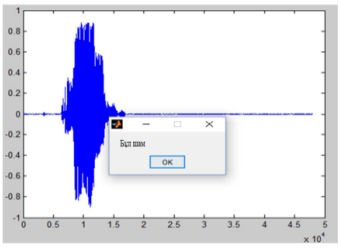
3. Нәтижелер мен тәжірибелер

Келесі нәтижелер сөйлеуді тану жүйесі арқылы танылған сөздер немесе сөз тіркестерін көрсетеді. Жүйе жұмысының тиімділігін талдау үшін қоршаған орта жағдайларының үш түрі қарастырылды: 1) үнсіз 2) тырнау дыбысы бар 3) және музыкалық шу. "Шам" сөзі барлық үш жағдайда бағаланады.

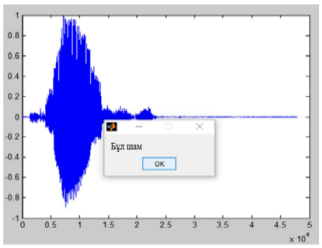


6 - сурет. Сигнал мысалы (музыкалық шу).

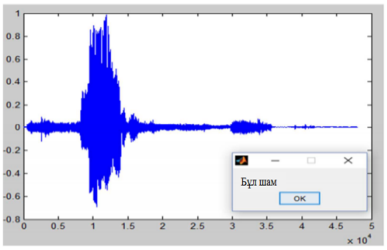
Сигналдың кедергісіз формасы айтылған сөздің конвертін көрсетеді, үлгілермен салыстырғанда сөйлеу сигналының мәні бар. Кіріс сигналы шуылға ұшыраған кезде, бастапқы кіріс сигналына шу коэффициенттері қосылады. Бұл сандар үлгілермен салыстырғанда шуылға қосылатын сөйлеу сигналының мөлшерін (егер бар болса) көрсетеді. 7 Сурет хабарлама терезесінде берілген кіріс сигналы сәйкес келетін танылған сөз көрсетілген.



Сурет 7. Шуы жоқ "шам" сөзі.



Сурет 8. Тырнау дыбысы бар "шам" сөзі.



Сурет 8. Музыкалық шуы бар "шам" сөзі.

Көріп отырғанымыздай жүйе сөзді таниды. Тәжірибе бойынша тек сөздер емес, сөздер жиынтығын және сөз тіркестерін айтып, әр түрлі жылдамдықпен сөйлеген жағдайлады да қарастырды. Деректерге статистикалық талдау жасалынған кезде әр түрлі қоршаған орта жағдайларында сөздер мен сөз тіркестері бойынша жүргізіледі. Нәтижелер үш жағдайда жиналды: 1) үнсіз 2) тырнау шу 3) музыкалық шу. Бұл тіркестер жұмыстың тиімділігін бағалау үшін енгізіледі жүйесі. Алынған мәліметтер жеке сөздерді, сондай-ақ фразаларды жүйенің ажырата алатындығын көрсетеді.

4. Қорытынды

Осы жоба аясында сөйлеуді тану жүйесі сәтті енгізілді. Мұндай жүйе байланыс, автоматтандыру саласында, биоинженерия, адам-машиналық өзара әрекеттесу және қауіпсіздік, тағы да басқа көптеген салада қолданыс табуы мүмкін.

Сөйлеу сигналының сипатын шығару үшін Мел – кепстралдық коэффициенттер жиілігі әдісі қолданылды. MFCC – Мел кепстралды коэффициенті әдісі сөйлеуді тану үшін тиімді екендігі дәлелденді. Өйткені ол адамның тыңдау моделіне сәйкес жасалған Mel шкаласын қолданылды.

Тәжірибелік нәтижелерді статистикалық талдауы, жүйенің шу болмаған жағдайда тану жылдамдығын 90%-нан астам екенін көрсетеді. Тәжірибелер сонымен қатар жүйенің жеке сөздерді тануда сәтті (90% сәттілік), үздіксіз сөздермен салыстырғанда фразалар (70% сәттілік) үлкенірек екенін көрсетеді. Сыртқы шудың болуы жүйенің жұмысына теріс әсерін тигізетінін де бақыладық. Әсіресе, тырналған шу болған жағдай кезінде (яғни шу тұрақсыз болған уақытта). Тәжірибелер көрсеткендей, баяуүздіксіз сөз тіркестерін тануда сөйлеу жылдамдығы теріс фактор болып табылады (30%-35%) пайдалану сипаттамаларының нашарлауын байқадық).

Болашақ зерттеулерің тақырыптары: спикерлердің үні мен дауыс деңгейінің өзгеруінің салдары, бір сөзді танудағы екпін параметрлері, сөз тіркестерін танудағы сөйлеу жылдамдығының әсері, және төмен жиілікті шудың әсері (адамның сөйлеуіне ұқсас) алуға болады.

Әдебиеттер

1. Мамырбаев О.Ж., Қыдырбекова А.С., Турдалыұлы М., Мекебаев Н.О. Дауыс бойынша пайдаланушыны идентификациялау және аутентификациялау әдістеріне шолу // “Инновациялық АТ және ақылды технологиялар” ғылыми конф. материалдары, 2019. – Б. 315-321.

2. Gaikwad U., Ahmed M. Enhanced Speaker Recognition System using MFCC and LGB algorithm // International Journal of Electronics and Communication Systems, 2014. - Vol.
5, No. 3. – P. 17-19.

3. Калимолдаев М.Н., Мамырбаев О.Ж., Қыдырбекова А.С., Миекебаев Н.О. I-векторлы бейнелеуді пайдаланып дауысты тексеру және идентификацияла// “Халықаралық математика және физика журналы” , 2019. – Б. 12-15.

4. Мамырбаев О.Ж., Тұрдалыұлы М, Мекебаев Н.О., Қыдырбекова А.С. Сандық жүйке желілерін қолданып сөйлеуді автоматты түрде тану// ACIIDS, Индонезия, Іс жүргізу, 2019 - II бөлім.

5. Gaikwad S.K., Gawali B.W., and Yannawar P., A review on speech recognition technique// International Journal of Computer Applications IJCA, 2018. - Vol. 10, No. 3, - P 16-24.

6. Linguistic Data Consortium [Электрондық ресурс]. 2016. URL: https://www.ldc.upenn.edu/ (online; accessed: 2020).

7. Automatic Speech Recognition. Slideshare. [Электрондық ресурс]. Available: http://www.slideshare.net/richiebmthimmaiah/automatic-speech-recognition-4721204

HANDWRITING RECOGNITION DEVELOPMENT SYSTEM SOFTWARE

[1,2] Mamyrbayev Orken, [1]Nawida Najmee,
(E-mail: 1nawida.najmee111@gmail.com)
(E-mail: morkenj@mail.ru)
Institute of Information and Computational Technologies, Kazakh National Agrarian University, Faculty of "IT technologies, automation and mechanization of agro-industrial complex" 7M06102 Almaty kazakhstan

Abstract

Handwriting recognition is said to be growing rapidly in the current globalization. This handwriting recognition ensures an accurate medical care and it also reduces storage costs. There are many ways that this handwriting recognition works. Handwriting recognition is a method where a computer system can recognize characters. Handwriting recognition is an electronic device that is able to determine what is person is writing. This handwriting recognition is a technology that is used to identify certain things and also it is used on devices. Handwriting recognition plays a big role in the technology world now. Handwriting technology's aim is to mainly let people to write what they normally write and it eventually digitize the writing that they made. NestorWriter was the first handwriting recognition device found. Handwriting recognition is something that is able to describe the ability of computer to translate the human writing to text writing. Handwriting recognition is a technology that has been in this technology world since the 1980's but only now it has been used rapidly. This process is done by turning the words into conventional type on a computer and other than that, it also can be done by reflecting the person's handwriting on the computer. In this era of globalization, technologies continue to improve and improve more in no time. But most of the companies failed, but the devices didn't improve that much as they wanted. It also plays an important role in the storage and in the recovery of critical handwriting information. It also can recognize other symbols written by hand which is natural handwriting.

Keywords: recognition | handwriting | system | software | text | computer | data | character | advantage | electronic |

Introduction

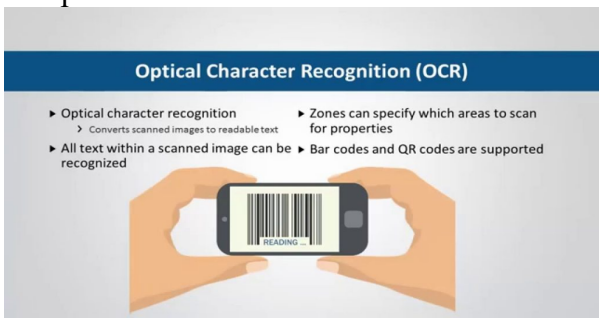
Automatic handwriting recognition aims at transforming this information into a processable electronic format, which gives us the opportunity to store, organise, retrieve and analyse knowledge electronically. As well as the general benefits of handwriting recognition systems, this can have other significant impacts for science and engineering fields that have maths as a core part, such as automatic generation of lecture notes. The motivation behind this research is to support the scientific community in tackling the automation of transformation of mathematical handwritten images into processable formats. Automatic recognition of handwriting allows easier access to an increased amount of information, making it available not only to millions of users but also amenable to electronic search, data mining, etc.

Style of paper

There are two types of handwriting recognition techniques; Optical Character Recognition (OCR) and Online Recognition.

Optical character recognition

Optical character recognition (OCR) is process of classification of optical patterns contained in a digital image. The character recognition is achieved through segmentation, feature extraction and classification. This chapter presents the basic ideas of OCR needed for a better understanding of the book. The chapter starts with a brief background and history of OCR systems. Then the different techniques of OCR systems such as optical scanning, location segmentation, pre-processing, segmentation, representation, feature extraction, training and recognition and post-processing. The different applications of OCR systems are highlighted next followed by the current status of the OCR systems. Finally, the future of the OCR systems is presented.



Online Recognition

This is the second type of the handwriting recognition, Online Recognition. This Online Recognition experienced a flow in popularity. Apple Computers released a handheld device called the Newton in the 1990s. This Newton device was made use of the first widely available handwriting recognition interface. A small stylus was used to write on the Newton's screen and this Newton device will recognize the letters that are written and convert as a text document. This made the Newton device to have more popularity than expected.

Later as years pass by, the Palm Company tried a new handwriting recognition system. The Palm Company named the system Graffiti. The Graffiti system didn't only rely on the tradition Roman alphabet but the Graffiti system defined more on its own system by using much simpler line-strokes as a stand-in for each and every letter. This was an advantage for the Graffiti system as it allowed a higher success rate in identifying letters and also in learning a user's variations. At the same time it made a steep for learning curve which kept most mainstream users at bay.

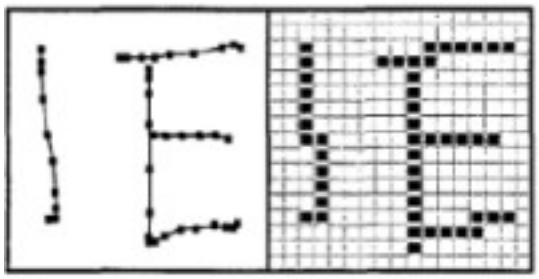
Other than that, the Microsoft Corporation's Tablet PCs also make use of the handwriting recognition system. The Tablet PCs didn't take an attempt to learn the user's shading whereas the Tablet PCs draw an extensive database of character variation. This system appeared to have a higher success rate than the other adaptive system because of its extensive database of character variation. Handwriting Recognition software became more useful because of the mainstreaming of PDAs and cellular phones with the stylus inputs. This made the handwriting recognition system to be more useful and grow rapidly from time to time.

Handwriting Recognition has many advantages that made it grow rapidly in the technology word now. There is much different kind of technologies that abide to enable others to take advantage of the handwriting recognition. The way this work was when

people write letters a different way and they let the computer know what the intended letter was and change in to a text document. But the problem with this was the different way that the letters are written and this could make unnatural feel to the person who is writing it. Another way of appreciating this technology is that just write and the computer changes it to a text document but at the same time, the computer doesn't always get the right word and sometimes it insert the wrong letters.

Tables and figures

However, in offline handwriting recognition, all which is available to the recognition system is the two-dimensional spatial information, In online handwriting recognition, data are collected while they are being generated on a digitising surface whether online or offline – is generally not an easy task. Naturally, the lack of dynamic information has made offline handwriting recognition a more difficult task than online.



(a) (b)

Comparing handwriting recognition systems – whether online or offline – is generally not an easy task. This is predominantly due to the fact that to be able to directly compare systems, you would need to test the systems on the same database; with the same lexicon size, writers, writing tools, etc. which is not the case all the time. The other factor that makes this comparison difficult is that systems are usually designed and built with a specific purpose. For instance, only in the case of offline recognisers systems deal with different problems such as different languages, handwritten versus machine-printed, word versus character, forms and diagrams versus text versus mathematics, and they even extend to the writing surface i.e. paper versus whiteboard and others.1

However, what is easy to see is that systems that deal with machine-printed text can outperform the ones dealing with handwriting. These systems, widely regarded as OCR or Optical Character Recognition, have managed to reach accuracy levels of 99% for many languages such as English [CMUV97]. In addition, online systems also generally perform better than their offline counterparts [PS00]. Online recognisers have long managed to

achieve results of over 90 − 95% [GLF+09, Oh01, TSW90], while only offline recognisers

that deal with a very limited number of lexicons have been nearly as successful [Pan12, PSH11, KSS03, Vin02].

But, many methods and techniques have been introduced to help tackle this complicated task, such as, Feature Extraction Methods and Pattern Recognition Methods. Although these methods have made offline handwriting recognition systems more accurate, offline recognition of handwriting still remains an open and challenging task.

Equations

In a nutshell , Handwriting Recognition software became more useful because of the mainstreaming of PDAs and cellular phones with the stylus inputs. This made the

handwriting recognition system to be more useful and grow rapidly from time to time. Handwriting Recognition software became more useful because of the mainstreaming of PDAs and cellular phones with the stylus inputs. Handwriting Handwriting recognition is said to be growing rapidly in the current globalization. This made the handwriting recognition system to be more useful and grow rapidly from time to time. Later as years pass by, the Palm Company tried a new handwriting recognition system. This is how handwriting recognition software helps in saving the old files or important document. Handwriting recognition software allows the old files to be saved in a proper electronic format. This handwriting recognition system is so useful. This is how handwriting recognition software helps in saving the old files or important document. Handwriting recognition software allows the old files to be saved in a proper electronic format. But still sometimes, these historical papers might be damaged or corrupted due to some accidents and there is when handwriting recognition software is really very helpful. Later as years pass by, the Palm Company tried a new handwriting recognition system. There is much different kind of technologies that abide to enable others to take advantage of the handwriting recognition. Additionally, there are many more advantages of handwriting recognition system. Certain cell phones have the handwriting recognition system in it. Handwriting recognition is used when there are certain people who prefer writing on the screens rather than writing it on a paper.

Refrences

[1] Arica, N., Vural, F. T. Y., An Overview of Character Recognition focused on Offline Handwriting, IEEE Transactions on Systems, Man and Cybernetics – Part C: Applications and Reviews, 31(2), pp 216–233, 2001.

[2] Bunke, H., Wang, P. S. P. (Editors), Handbook of Character Recognition and Document Image Analysis, World Scientific, 1997.

[3]Chaudhuri, A., Some Experiments on Optical Character Recognition Systems for different Languages using Soft Computing Techniques, Technical Report, Birla Institute of Technology Mesra, Patna Campus, India, 2010.

[4] Cheriet, M., Kharma, N., Liu, C. L., Suen, C. Y., Character Recognition Systems: A Guide for Students and Practitioners, John Wiley and Sons, 2007.

[5] Dholakia, K., A Survey on Handwritten Character Recognition Techniques for various Indian Languages, International Journal of Computer Applications, 115(1), pp 17–21, 2015.

[6] Mantas, J., An Overview of Character Recognition Methodologies, Pattern Recognition, 19(6), pp 425–430, 1986.

[7] Rice, S. V., Nagy, G., Nartker, T. A., Optical Character Recognition: An Illustrated Guide to the Frontier, The Springer International Series in Engineering and Computer Science, Springer US, 1999.

[8] Schantz, H. F., The History of OCR, Recognition Technology Users Association, Manchester Centre, VT, 1982.

[9] Scurmann, J., Reading Machines, Proceedings of International Joint Conference on Pattern Recognition, Munich, pp 1031–1044, 1982.

[10] Singh, S., Optical Character Recognition Techniques: A Survey, Journal of Emerging Trends in Computing and Information Sciences, 6 (4), pp 545–550, 2013.

[11] Young, T. Y., Fu, K. S., Handbook of Pattern Recognition and Image Processing, Academic Press, 1986.

[12] Yu, F. T. S., Jutamulia, S. (Editors), Optical Pattern Recognition, Cambridge University Press, 1998.

[13] Robert H. Anderson. Syntax-Directed Recognition of Hand-Printed Two-dimensional Mathematics. PhD thesis, Harvard University, Jan- uary 1968.

[14] Josef B. Baker. A Linear Grammar Approach for the Analysis of Math- ematical Documents. PhD thesis, School of Computer Science, June 2012.

[15] Orit Baruch. Line thinning by line following. Pattern Recognition Letters, 8:271–276,1988.

[16] Mary K. Babcock and Jennifer J. Freyd. Perception of dynamic infor- mation in static handwritten forms. American Journal of Psychology, 101:111–130, 1988.

[17] Richard Buse, Zhi-Qiang Liu, and Terry Caelli. A structural and re- lational approach to handwritten word recognition. IEEE TRANSAC- TIONS ON SYSTEMS, MAN, AND CYBERNETICS, 27(5):847–861,October 1997.

[18] Horst Bunke and P.S.P.Wang, editors. Handbook of Character Recog- nition and Document Image Analysis. World Scientific, 1997

[19]Radmilo M. Bozinovic and Sargur N. Srihari. Off-line cursive script word recognition. IEEE Trans. on Pattern Analysis and Machine In- telligence, 11:68–83, 1989.

[20]Josef B. Baker, Alan P. Sexton, and Volker Sorge. A linear grammar approach to mathematical formula recognition from pdf. In Mathe- matical Knowledge Management, 8th International Conference, LNCS 5625. Springer Verlag, 2009.

ПРИМЕНЕНИЕ СКРЫТЫХ МАРКОВСКИХ МОДЕЛЕЙ В РАСПОЗНАВАНИИ РЕЧИ

Мухтар Д. А.
Институт информационных и вычислительных технологий
КН МОН РК, Казахстан

Аннотация

Приведены результаты разработки программных модулей, реализующих систему распознавания речи на основе скрытых Марковских моделей и основанная на использовании кепстральных коэффициентов (MFCC) и коэффициентов линейного предсказания (LPC).

Обосновывается структура системы распознавания речи, использующая скрытые марковские модели, состоящая из четырех модулей:модуль выделения слов из звукового потока, модуль анализа признаков слова, модуль обучения скрытых марковских моделей и модуль распознавания слов. Приводятся алгоритмы формирования скрытых марковских моделей.

Приведены результаты оценки точности распознавания для различных параметров модели.

Ключевые слова: *скрытая марковская модель, кепстральные коэффициенты (MFCC), коэффициенты линейного предсказания (LPC)*

Введение. На сегодняшний день распознавание речи является динамично развивающимся направлением в области искусственного интеллекта. Этому свидетельствует достигнутые за последние полвека успехи благодаря которому

распознавание речи получила широкое проникновение в различные сферы человеческой деятельности.

Распознавание речи является одним из мощных инструментов для обмена информацией с помощью акустического сигнала. Не удивительно, но речевой сигнал уже несколько столетий является предметом исследований. Распознавание речи — это технология, которая позволяет вычислительной машине уловить слова, произнесенные человеком с помощью микрофона. Данная технология полезна для людей с ограниченными возможностями, которым в противном случае потребовались бы помощники. Автоматическое распознавание речи долгое время была сложной задачей. Первые статьи датируется с 1950 года. В течении этого время использовались различные модели для распознавания речи. Из всех подходов в настоящее время скрытые Марковские модели (СММ) дают наилучшую производительность [1].

Прогресс в области создания машин, способных воспринимать и создавать (синтезировать) человеческую речь, идет вместе с общим прогрессом науки и техники в первую очередь с прогрессом в области микроэлектроники. Для решения их необходимо обладать знаниями в филологии, лингвистике, цифровой обработке сигналов, распознавании образов, акустике, статистике и т.д.

В распознавании речи задействованы процессы создания (обучения) и распознавания на основании этих данных речь. Создание описании базы данных собирает имеющиеся примеры говорящих и извлекает из выбранных слов необходимые признаки. В процессе распознавания происходит идентификация говорящего в этот момент человека, которые сравнивается с сохраненными записями голосов. В реальном времени при распознавании сначала он находит вероятность произнесенного слова в предварительно сохраненной базе данных известных слов. Далее он принимает решение слова с выбором слова максимально подходящего. Распознавание речи имеет две категории: зависимый и независимый от текста. Распознавании речи по категории зависимость от текста определяет слова со словами, которые ему были даны во время сбора базы данных. Вторая категория при использовании в распознавании речи определяет слова независимо от слов. Также помимо категории в распознавании речи есть понимание такое как классификация. Классификация в распознавании речи делится как зависимое и независимое от говорящего [2].

Архитектура системы распознавания речи

Речевой сигнал в первую очередь передает произносимые слова или сообщения. Сфера распознавания речи связана с определением основного смысла высказывания. Успех в распознавании речи зависит от извлечения и моделирования характеристик, зависящих от речи, которые могут отличаться друг от друга [3].

Типичная архитектура системы распознавания речи состоит из следующих компонентов:

1. Обработка сигнала и функция извлечения
2. Акустическая модель
3. Языковая модель
4. Поиск гипотез

Первый компонент обработки сигнала и функция извлечения признаков принимает на вход аудио сигнал, которые улучшают речь, удаляя шумы и искажения

канала, преобразуя сигнал из временной области в частотную, и извлекает характерные векторы, которые подходят для следующих акустических моделей. Акустическая модель объединяет знания об акустике и фонетике. Данная модель принимает на вход функцию, созданную из компонента извлечения признаков и генерирует оценку для своей модели. Далее языковая модель оценивает вероятность предполагаемой последовательности слов или изучая взаимосвязь между словами (обычно текст) [4].

Рис. 1. Архитектура системы распознавания речи

Скрытые Марковские модели

СММ является одной из самых важных моделей машинного обучения в обработке речи и языке. В ее основе лежит конечный автомат, который состоит из N-состояний. С помощью СММ составляют статистические модели фонем, слов и целых фраз. Выбор конкретного языкового объекта зависит от задач, которые должна решать разрабатываемая система распознавания речи.

Начнем с формального определения скрытой марковской модели, сосредоточив внимание на том, как СММ отличается от цепи Маркова. СММ определяется следующими компонентами:

Q = q1q2...qN - набор из N состояний A = a11a12...an1...ann - матрица вероятности перехода A, каждое aij представляет вероятность перехода из состояния i в состояние j. O = o1o2...oT - последовательность из T наблюдений, каждое из которых взято из словаря V = v1, v2, ..., vV.

B = bi (ot) последовательность вероятностей наблюдения, также называемые вероятностями выбросов, каждая из которых выражает вероятность того, что наблюдение будет произведено из состояния i.

q0,qF - q0, qF - специальное начальное и конечное состояние, которое не связаны с наблюдениями, вместе с вероятностями перехода a01a02..a0n из начальное состояние и a1Fa2F ... anF в конечное состояние [5].

Структурно это можно описать как дискретную систему, имеющую конечное множество из N состояний —S={s1, . . . , sN}, в каждом из которых она может принимать одно из M значений из набора наблюдаемых параметров V={v1, . . . , vM}— алфавита. Состояние системы qt в момент времени t, принимающее одно из N значений множества S, зависит только от её состояния qt−1 в момент времени t−1, а значение наблюдаемого параметра Ot в момент времени t зависит только от состояния qt, т. е. не зависит от времени.

Вероятности переходов между состояниями системы задаются матрицей A. Вероятности выпадения каждого из M значений наблюдаемого параметра системы в каждом из N состояний системы задаются набором векторов B. Вероятность появления некоторого начального состояния системы задаётся вектором Pi. При этом последовательность состояний, в которых пребывает система Q=q1, . . . , qT, внешнему наблюдателю не видна, а видит он только последовательность

наблюдений O=o1, . . . , oT (здесь T— длина последовательности), т. е. система ведёт себя как «чёрный ящик».

На текущий момент можно выделить следующие подходы к составлению СММ:

1. На СММ составляют модели фонем – звуковых букв языка, которые можно объединять в слова.

2. Фонемы моделируются с помощью трех состояний – начального, среднего и конечного (рис. 2). Это связано с тем, что речевой тракт не может менять свои характеристики мгновенно, и при переходе от фонемы к фонеме происходит его «переключение» через промежуточные состояния.

3. Известно, что фонемы звучат по-разному в окружении разных фонем. Этот эффект называется коартикуляцией. В зависимости от того, будет ли учитываться или игнорироваться это явление, существует два типа моделей фонем:

1) монофоны – коартикуляция игнорируется, составляются модели отдельно стоящих фонем. Этот подход имеет важное преимущество: фонем в языке совсем немного (например, в русском языке их 43), и из них можно составить любые слова, так что распознавание будет сводиться к определению цепочки произнесенных фонем, и словарь такой системы фактически неограничен. Есть, однако, и серьезный недостаток: такая модель имеет невысокую точность;

2) трифоны – коартикуляция учитывается путем составления отдельных моделей для фонем в окружении других фонем. Рассмотрим слово «назад»: используя Международный фонетический алфавит, его можно описать цепочкой фонем «n-a-z-a-t». Здесь фонема /a/ встречается дважды, но из-за коартикуляции для нее потребуется составить две отдельные модели: «na+z» и «z-a+t». Это гораздо более сложный подход, но и точность распознавания выше, чем при использовании монофонов.

4. Составляют отдельные СММ для каждого слова из словаря и при распознавании выбирают «наиболее подходящую». Такой подход подойдет для распознавания отдельно стоящих слов.

5. Составляют одну СММ, склеивая СММ для слов через промежуточные состояния (например, тишину), согласно грамматике языка. Это необходимо для распознавания слитной речи.

В режиме обучения элементы системы распознавания речи имеют следующее функциональное назначение:

- речевая база содержит записи слов, повторяющихся несколько раз для обеспечения адекватности получаемых СММ, которые будут доступны для распознавания;

- выделение последовательности одинаковых слов из файла речевой базы с помощью предварительной обработки (подавление шума, фильтрация и т. д.);

- анализ признаков и определение алфавита слова V, по которому формируется последовательность наблюдений O;

- обучение СММ — подбор параметров СММ, чтобы она как можно лучше описывала реальную наблюдаемую последовательность O символов алфавита V анализируемого слова;

- сохранение СММ в базе — словаре.

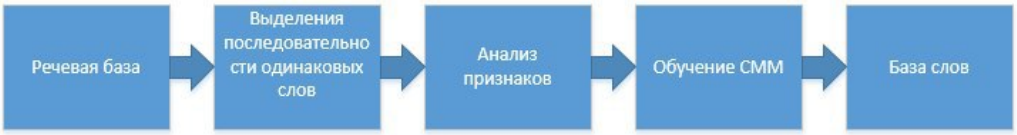


Рис. 2. Обучение

В режиме распознавания:

- выделение слова из входного звукового потока с помощью предварительной обработки;
- анализ признаков распознаваемого слова и формирование соответствующей последовательности наблюдений O;
- распознавание слова с использованием базы СММ и генерация кода распознаваемого слова.

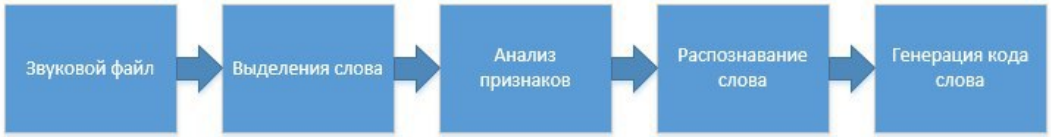


Рис. 3. Распознавание

Таким образом, для реализации данной структуры необходимо всего 4 модуля: модуль выделения слов из звукового потока, модуль анализа признаков слова, модуль обучения СММ с базой моделей, модуль распознавания слов.

Применения СММ

Наиболее широкое применение СММ нашли при решении таких задач, как распознавание раздельной и слитной речи, анализ изображений, видео, последовательностей ДНК и ряда других [6]. На сегодняшний день исследование, распознавание и применение распознавании речи является перспективным научно-техническим направлением. Многие научно-исследовательские центры такие как Массачусетский технологический университет, Стэндфордский университет, Исследовательский центр речевых технологий IBM. Центр речевых технологий и многие другие активно участвуют в работах. На текущий момент успешно работают системы распознавания речи в таких компаниях как Google, Apple, Yandex, Тинькофф и многие другие.

Заключение. В работе рассмотрен аппарат скрытых Марковских моделей применительно к решению задачи распознавания звуковых последовательностей (задача распознавания раздельной речи). Скрытые Марковские модели (СММ) - это способ связать последовательность наблюдений с последовательностью скрытых классов или скрытых состояний, которые объясняют наблюдения. Процесс обнаружения последовательности скрытых состояний с учетом последовательности наблюдений называется декодированием или выводом. Параметрами СММ являются матрица вероятности перехода A и матрица B матрица правдоподобия

наблюдения. СММ могут быть обучены с помощью алгоритма Баума-Велча или forward-backward алгоритма.

Так же рассмотрены вопросы создания программного модуля, который позволяет эффективно подготавливать необходимые исходные данные на основе кодирования признаков звукового сигнала, использующего линейные предсказания.

Как результат реализована и протестирована экспериментальная система, основанная на использовании кепстральных коэффициентов (MFCC) и коэффициентов линейного предсказания (LPC). Получены практические оценки точности распознавания для различных параметров модели.

Литература

1. SD.B.Paul,"Speech Recognition using Hidden Markov Model."

2. M.A.Anusuya , S.K.Katti "Speech Recognition by Machine: A Review" International journal ofcomputer science and Information Security 2009

3. Ms. Rupali S Chavan, Dr. Ganesh. S Sable "An Overview of Speech recognition Using HMM"

4. Dong yu, Li Deng "Automatic Speech recognition" Springer-Yerlag London 2015 688 p.

5. Daniel Jurafsky, James Martin "Speech and Language Processing" 2nd Edition 329 p.

6. Vaseghi, Saeed V. Advanced digital signal processing and noise reduction. – 3ed. – Chichester, 2006.

CONSIDERATION OF THE STATE OF SPEECH RECOGNITION TECHNOLOGY

[1]Amirgaliyev Ye., [2]Sadykova A.
e-mail: sadykova.akmanat@gmail.com
[1]Institute of Information and Computational Technologies CS MES RK, Kazakhstan
[2]Al-Farabi Kazakh National University, Kazakhstan

Abstract. *At this point in time, speech recognition has gone beyond its scope. Until that time, speech recognition systems had a small vocabulary and an application for users. By the research and development in this area, today this technology offers various products with a large vocabulary, a high degree of user convenience, high accuracy in a noisy environment and the ability to connect to any existing computer application. As you know, the voice of each may differ and for these purposes speech recognition systems include much higher individual performance and accuracy. Also, the ability to integrate input modes from a computer by a user is also included for convenience and alternative. This article provides a literature review and examines the state of knowledge and application of speech recognition technologies. A classification of existing recognition systems is given and each case is described separately. The final part describes the prospect of these types of technologies in the world and their capabilities.*

Key words: *speech recognition, speech control, speech to text conversion.*

Introduction. Since the advent of the first computers, one of the most important issues in the development of computer technology has been the process of human-machine interaction. For a long time it was available only to narrow specialists - technologists “communicated” with the machine through an intermediary programmer. This situation lasted until the appearance of the dialog interface, when the user was able to personally enter the command addressed to the machine from the keyboard and get a meaningful answer. The further appearance of the graphical interface, in which the person no longer needed to know any commands, led to the widespread spread of personal computers.

However, man has always sought a more universal and natural way of interacting with computers. Back in the era of punch cards in science fiction novels, a man with a computer talked as if he were an equal. Then the first steps were taken to implement the speech interface [1]. In 1971, the development of the largest project ever undertaken at that time in the field of speech recognition began, after the Advanced Research Project Agency (ARPA) of the US Department of Defense adopted a 5-year project to create machines that allow you to "understand" the words all together sentences and vocabulary of which amounted to 1000 words. At the end of 1976, several systems were introduced, one of which was HARPY. This system correctly understood 95% of sentences spoken by five operators, using a dictionary of 1011 words and a strictly limited grammar of sentences.

Modern speech recognition systems Currently, speech recognition is finding more and more applications, ranging from applications that convert speech information into text and ending with on-board car control devices. The whole variety of existing speech recognition systems can be divided into the following groups:

1. Software cores for hardware implementations of speech recognition systems;
2. Sets of libraries, utilities for developing applications that use speech recognition;
3. Independent user applications performing voice control and / or speech to text conversion;
4. Specialized applications using speech recognition;
5. Devices that perform recognition at the hardware level;

Let's consider each of these groups in more detail.

1. Software cores for hardware implementations. The basis of any speech technology is the so-called "engine" or the core of the program - a set of data and rules by which data is processed. Depending on the purpose of this core, there are TTS and ASR engine. The TTS (Text-to Speech) engine provides the ability to synthesize speech by text, and the ASR (Automatic Speech Recognition) engine - for speech recognition.

There are several large manufacturers involved in the creation of ASR cores, and among them are companies such as SPIRIT, Advanced Recognition Technologies, IBM.

SPIRIT company is creating software for digital telephony, voice compression, speaker identification, for VoIP and GPS technologies [2]. The SPIRIT ASR engine is designed to recognize voice commands and is used in various applications, such as voice control of devices, voice dialing in hands-free devices, and the entry of personal identification codes (PIN) in security systems. This kernel is embedded in any DSP or RISC platform and comes in the form of object code.

IBM has been involved in automatic speech recognition for more than 30 years and has made great strides in this area. Thus, ProVox Technologies, based on the ViaVoice® software core from IBM [3], created a system for dictating the reports of VoxReports radiologists [4]. According to the test results, this system with an accuracy of 95-98% recognizes continuous speech at a normal rate (up to 180 words per minute), regardless of the announcer. However, the vocabulary of the system is limited to a set of specific medical terms.

Opera Software has agreed with IBM to integrate Embedded ViaVoice speech recognition technology into Opera's browsers [5]. Using Embedded ViaVoice will allow users to control the browser not only with the mouse and keyboard, but also with voice.

Speech recognition technology is increasingly used in mobile communications. Thus, Advanced Recognition Technologies created the smARTspeak NG system, which is built into mobile phones [6]. Now the smARTspeak NG system is used in Siemens keyboardless phones [7], Panasonic TDMA phones in the USA and others.

Sakrament ASR Engine is a software development of the Belarusian company Sacrament [8], designed for use in various hardware systems and software applications using speech recognition technology. Declared characteristics: recognition accuracy 95-98%; speaker independence; language independence; recognition of continuous speech in the form of expressions and small sentences. However, in this system there is no possibility of training - additional dictionaries are created by order of the Sacrament company itself.

2. Sets of libraries for application development. With the development of speech technologies and the increasing introduction of mobile devices, the idea arose of using voice control in building network applications. To do this, it was necessary to develop a unified standard for the integration of speech technologies.

One of the open standards based on the XML language is VoiceXML (Voice eXtensible Markup Language), the first version published in May 2000 by the World Wide Web (W3 Consortium) is intended for the development of Interactive Voice Response (IVR) control media resources. The purpose of creating the standard is to bring all the advantages of web programming to the development of IVR applications [9].

However, interest in multimodal applications combining speech recognition with other forms of information input (using the keyboard, pen, or a set of numeric buttons) prompted a number of companies, including Microsoft, to support the SALT Forum project (Speech Application Language Tags - speech language application tags). And now, around SALT and VoiceXML of the W3C consortium, two different camps are being formed [10, 11]. Until now, companies cannot agree on the choice of the main standard, and now both directions are developing equally.

Various companies are developing packages for creating voice applications, the so-called Software Development Kit (SDK), supporting one or another standard. So Philips created the Speech SDK. This package supports the Voice XML specification and is designed to communicate with the C / C ++ API [12].

CompTek [13] and Philips jointly created SpeechPearl, a product consisting of a set of software modules, libraries, and utilities for developing speech recognition systems with Russian language support for telephone applications. In June 2004, the Telepath service, which manages WebMoney Transfer electronic wallets using mobile and landline phones, launched a speech recognition system based on SpeechPearl.

On the other hand, Microsoft is distributing its product, the Microsoft Speech SDK. It contains a set of components that describe the corresponding Windows Speech API, documentation, the source code of the blank program (it is enough to supplement it only with its own recognition algorithm), as well as Microsoft Speech Recognition and Microsoft Text-to-Speech [Speech Recognition and Translation Systems [14].

3. Independent user applications. Currently, the market for software speech recognizers is represented by many applications. Consider the most famous of them.

Dragon NaturallySpeaking Preferred by Dragon Systems [15] is the only program that has come close to meeting stated specifications. In general, he comes very close to

achieving the declared recognition accuracy of 95%. Although the Dragon package is inferior to some of its competitors in terms of moving around the screen, editing and formatting, it is superior to all in the main thing - the ability to correctly record spoken words the first time. Initially, this package does not work with Russian.

Company M.S. Technology [16] has developed the Microservice program for managing the functions of the Windows 98 / Me / 2000 / XP operating systems and entering text into any editor. The program supports Russian and English languages and contains a dictionary of about 10,000 words. Also created a simplified version - "Microservice" Light. Here the volume of the dictionary is limited to 300 words and 100 commands. 1C Company acquired the rights to this software and releases it under the name “Dictograph”.

However, according to testing, "Microservice" from M.S. Technology showed unsatisfactory results - 30–50% of correctly recognized words and commands [17].

4. Specialized applications. Speech recognition can be used not only for entering text or issuing commands, but also for more specific purposes. So the company “Center for Speech Technologies” develops and produces software products, technologies and equipment samples for the departments of the Ministry of Internal Affairs, Ministry of Justice, Ministry of Emergencies, Moscow Region, emergency services, call centers and other users, in whose activity particular importance is attached to the recording and processing of voice information [eighteen].

The company created the following applications: “IKAR Lab” - a tool kit for forensic investigation of phonograms of speech, “Tral” - an automated complex for recognizing speakers in phonograms of telephone conversations, “Territory” - an automated system for diagnosing dialects and accents of Russian spoken language.

The German institute DFKI, engaged in the development of artificial intelligence, has developed a system called Verbmobil, capable of translating spoken language from German to English or Japanese and vice versa, directly delivered to the microphone [19].

The system is designed as an independent Verbmobil Server. Thanks to this, Verbmobil was able to connect with a network of mobile phones standard GSM. Now multilingual subscribers, having connected to Verbmobil Server, can communicate with each other directly, accepting already translated speech, while Verbmobil automatically adjusts to the speaker’s language. According to experiments, translation accuracy is 90%, which was tested on 25,000 test phrases....

5. Devices that perform hardware recognition. To use the speech recognition functions in various devices, robots, toys, hardware methods for solving this problem are developed. So the American company Sensory Inc. developed an integrated circuit Voice Direct ™ 364 providing speaker-dependent recognition of a small number of teams (about 60) after preliminary training [20]. Before starting operation, the module must be trained in all the commands used in the work. Commands are saved to external memory as 128-byte images. During operation, the image of the next command is compared with the reference ones from the memory in the neural network module and a decision is made on the match.

Taiwanese technology corporation Primestar Technology Corporation has developed its own chip VP-2025, designed for speech recognition [21]. This device performs recognition using the neural network method.

In addition, American scientists decided to create a specialized microprocessor for speech recognition. Research in this direction will be carried out by employees of Carnegie Mellon University in Pittsburgh (PA) and the University of California at Berkeley. It is expected that the efficiency of speech recognition by such a chip will have to be 100-1000 times higher than that of the software and hardware systems used today [22].

Conclusion. Prospects for the development of speech recognition systems. As you can see, speech recognition technologies have found their application in various fields. However, in this area many problems still remain unresolved, many ideas require further development. So, programs that work with isolated words have achieved high accuracy in command systems - in the most common modern applications, recognition accuracy is on average 95-99% and depends mainly on the noise level. At the same time, the task of recognizing continuous speech has not been sufficiently solved, although in the case of a limited dictionary, systems of this type exist (VoxReports [4] on the ViaVoice [3] core, Verbmobil) and show high results in accuracy. Currently, many works are devoted to the problem of continuous speech recognition (IPU RAS [23], Istra-Soft [25], IBM [3]), because it is this type of speech interaction that is considered the most promising.

The most important stage of speech processing in the recognition process is the selection of informative features that uniquely characterize the speech signal. There are a number of mathematical methods that analyze the speech spectrum. Here the most widely used is the Fourier transform, known from the theory of digital signal processing. This mathematical apparatus has proven itself in this area, there are many signal processing techniques that use the Fourier transform as a basis. Despite this, work is ongoing to find other ways to parameterize speech. One of these new areas is wavelet analysis, which has been used to study speech signals relatively recently. The theory of this method is now being developed by scientists around the world, and many researchers have high hopes for using the wavelet analysis tool for speech recognition.

If we consider speech recognizers from the point of view of classification according to the functioning mechanism, the overwhelming majority of them relate to systems with probabilistic network methods for deciding whether the input signal matches the standard signal - this is the hidden Markov modeling (SMM) method, the dynamic programming method and the neural network method (Fig. 1) . For example, neural networks can be used to classify the characteristics of a speech signal and make a decision about belonging to one or another group of standards [27]. The neural network has the ability to statistical averaging, i.e. The problem with the variability of speech is solved. Many neural network algorithms perform parallel processing of information, i.e. all neurons work simultaneously. This solves the problem with the recognition speed - usually the operating time of a neural network is several iterations. Now many developers use the apparatus of neural networks to build recognizers [19, 24, 27].

However, if we compare the performance of modern recognition systems with the performance of systems from the beginning of its inception, these are areas of science, we can say that over the past decades, researchers have not made much progress. This makes some experts doubt the possibility of implementing a speech interface in the near future [28]. Others believe that the task is almost solved. Most experts agree that it will take some time to develop speech recognition. As part of its Super Human Speech Recognition project, IBM hopes to develop commercial systems by 2010 that translate speech into printed text more accurately than humans [29].

References

1. Xuedong, H., Li, D. (2009). An Overview of Modern Speech Recognition, Indurkhya/Handbook of Natural Language
2. Processing C5921_C01, 339 -344, Microsoft Corporation.

3. Xuedong, H., Li, D. (2009). An Overview of Modern Speech Recognition, Indurkhya/Handbook of Natural Language
4. Processing C5921_C01, 339 -344, Microsoft Corporation.
5. Xuedong, H., Li, D. (2009). An Overview of Modern Speech Recognition, Indurkhya/Handbook of Natural Language
6. Processing C5921_C01, 339 -344, Microsoft Corporation.
7. Xuedong, H., Li, D. (2009). An Overview of Modern Speech Recognition, Indurkhya/Handbook of Natural Language
8. Processing C5921_C01, 339 -344, Microsoft Corporation.
9. Xuedong H., Li D. An Overview of Modern Speech Recognation. Handbook of Natural Language Processing, 2009. pp. 339-344.
10. Anusuya M.A., Katti S.K. Speech Recognition by Machine. A Review of IJCSIS. 6(3), 2009.
11. Simon K., Joe F. Recognition ,Speech production knowledge in automatic speech recognition. Journal of Acoustic Society of America, 2006.
12. Masanobu N., Koji I., Sadaoki F. The Effect Of Spectral Space Reduction In Spontaneous Speech On Recognition Performances, 2007.
13. Jen-TZung et.al. Factor Analysed Subspace modeling And Selection IEEE transactions on Audio, speech and Language Processing. 16(1), 2008.
14. Preeti S., Parneet K. Automatic Speech Recognition. A Review of IJITT. 4(2), 2013.
15. Santosh K.G., Bharti W.G., Pravin Y. A Review of Speech Recognition Technique. IJCA. 10(3), 2010.
16. Manoj K.S., Omendri K. Speech Recognition. A Review, Special Conference Issue: NCCC&BD, 2015.
17. Gaikwad S.K., Gawali B.W., Yannawar P. A Review of Speech Recognition Technique. IJCA. 10(3), 2010.
18. Ghai W., Singh N. A Literature Review of Automatic Speech Recognition. IJCA. 41(8), 2012.
19. Srivastava N. Speech Recognition using Artificial Neural Network. IJESIT. 3(3), 2014.
20. Rashed A. Fast Algorithm for Noisy Speaker Recognition Using ANN. IJCET. 5(2), 2014.
21. Lee T., Ching Ch. Isolated Word Recognition Using Modular Recurrent Neural Networks. Pattern Recognition. 31(6), 1998.
22. Katagiri S. Speech pattern recognition using neural networks. W.Chou and B.H.Juang (Eds.) Pattern Recognition in Speech and Language Processing. CRC Press. pp.115-147, 2003.
23. Juang B.H., Furui S. Automatic speech recognition and understanding: A first step toward natural human machine communication. Proc.IEEE. 88(8). pp.1142- 1165, 2000.
24. Shinoda K. Lee C.H. A structural Bayes approach to speaker adaptation. IEEE Trans. Speech and Audio Proc. 9(3). pp. 276-287, 2001.
25. Liu Y. Structural metadata research in the EARS program. Proc. ICASSP. 957, 2005.
26. Soltau H. The IBM 2004 conversational transcription. Proc. ICASSP. I-205-208, 2005.
27. Furui S. Recent progress in corpus-based spontaneous speech recognition. IEICE Trans. Inf. & Syst.. E88-D(3). pp. 366-375, 2005.

28. Furui S. Speech-to-text and speech-to-speech summarization of spontaneous speech. IEEE Trans. Speech & Audio Processing. 12(4). pp. 401-408, 2004.

29. Lee C.H. Statistical confidence measures and their applications. Proc. ICSP. pp.1021-1028. 2001

30. Jerome R. B. Large Vocabulary Speech Recognition with Multispan statistical Language Models. 76 IEEE Transactions On Speech & Audio Processing. 8(1), 2000.

31. Eduardo L. Utterance Verification In Decoding And Training Procedures. IEEE Transactions On Speech And Audio Processing. 8(2), 2000.

32. Rita S., Bhiksha R. Automatic Generation of Subword Units for Speech Recognition Systems. EEE Transactions On Speech And Audio Processing. 10(2), 2002.

33. Jen-Tzung Ch. Linear Regression Based Bayesian Predictive Classification for Speech Recognition. IEEE Transactions On Speech And Audio Processing. 11(1), 2003.

34. Mohamed A., Olivier S. Sequential Estimation With Optimal Forgetting for Robust Speech Recognition. IEEE Transactions On Speech And Audio Processing. 12(1), 2004.

35. Mohamed A., Feng L., Hui J. A New Verification-Based Fast-Match for Large Vocabulary Continuous Speech Recognition. IEEE Transactions On Speech And Audio Processing. 13(4), 2005.

36. Giuseppe R. Active Learning: Theory and Applications to Automatic Speech Recognition. IEEE Transactions On Speech And Audio Processing. 13(4), 2005.

37. Frank W., Hermann N. Unsupervised Training of Acoustic Models for Large Vocabulary Continuous Speech Recognition. EEE Transactions On Speech And Audio Processing, 13(1), 2005 .

TASKS OF POST-EDITING MACHINE TRANSLATION FOR TURKIC LANGUAGES

[1]Rakhimova D., [2]Turarbek A., [3]Zhunussova A.
e-mail: [1]diana.rakhimova@kaznu.kz, [2]turarbekasem@kaznu.kz,
[3]alia_94-22@mail.ru
[1]Kazakh National University named after Al-Farabi, Казахстан
[2]Kazakh National University named after Al-Farabi, Казахстан
[3]Institute of Information and Computational Technologies SC MES RK, Kazakhstan

Annotation.*The article considers the issues of post-editing the text of a machine translation with Turkish languages. It was shown that Turkic languages are more susceptible to errors due to the peculiarities of their linguistic structure.*

In order to improve the quality of translation, the system is constantly updated and checked, which greatly simplifies and speeds up the work of translators. The work of modern machine translation technologies is analyzed. Previously, the work of online translators was translated into Kazakh and vice versa. Translation errors are identified, general advantages and disadvantages of an online machine translation system into Kazakh are given. A model for the development of a machine translation post-processing

system for the Kazakh language is proposed. The alignment method and the maximum entropy method were used, and the post-processing process was analyzed.

Key words: *machine translation, post-editing, entropy method.*

Introduction

In a rapidly changing world to support high professionalism in its field, it is necessary to be constantly in the flow of information, but in most cases, Turkic-speaking languages have little information. This often requires access to information in a foreign language. And ignorance of languages, in which science develops (English, German, Russian, etc.), leads to difficulties.

But in the modern world, electronic dictionaries and translators are an indispensable tool for accessing foreign information. In such cases, the first place is occupied by the machine translation system, which can perform the translation in a shorter period of time than the translator. As a rule, the machine (automatic) translation program automatically translates the text from one natural language to another.

However, when translating from the Turkic languages into English or Russian or vice versa, the text obtained when translating between the Turkic languages is sometimes incomprehensible, and finally, the presence of a translator is necessary. And the translation has been edited.

Post-editing is a form of processing an automatic translation product with the participation of a translator in order to obtain a quality translation with minimal effort. As a rule, post-editors are professional linguists-translators who know all the intricacies of machine translation. This allows them to determine what needs to be changed as a result of MT(machine translate), thereby improving the translation process [1].

The most popular and widely used machine translations today are Yandex Translator, Promt and Google Translator. "Promt" refers to the categories of systems based on grammatical rules (Rule-Based Machine Translation, RBMT) [2].

Features of the structure of Turkic languages

Türkic-speaking languages are agglutinative languages with complex nominative (morphological and syntactic) participation of polysynthetics. Due to the global development of our country from year to year and the growth of external relations, various translation programs are widely used when translating into Turkish or other languages. Various machine translation systems (MTS) still cannot translate correctly and there are translation errors, but the field of machine translation is much more developed than in previous years. The most popular machine translation systems were selected to analyze MT errors. When translating from Turkish or, conversely, from Russian and English into Turkish, various errors may occur, because the structure of the Turkic languages differs from other languages, has its own characteristics [3]:

- closeness of lexical structure;
- the law of synharmonism;
- series of affixes-agglutinations;
- lack of categories;
- Absence of auxiliary words (prepositions);
- special order of words
- harmony of sound
- connection of suffixes and suffixes to the word for each other changes the word format

To illustrate the closeness of the Turkic languages, the following (in terms of population) are given examples from several important languages:

Table 1. words in Turkic languages

Ancient Turkic	Turkish	In Turkmen	Tartar	English	Kyrgyz	Uzbek	Uighur	Tuvasha
ana	ana/anne	ene	ana	ана /ana/	ene	ona	ana	ава
burun	burun	burun	borın	мұрын /murın/	murun	burun	burun	думчук
qol	kol	qol	qul	қол /qol/	qol	qo‘l	kol	хол
yol	yol	ýol	yul	жол /jol/	jol	yo‘l	yol	орук (чол)
semiz	semiz	semiz	simez	семіз /semiz/	semiz	semiz	semiz	семис

As an example, we will consider errors in the text of Turkic languages (Kazakh) when translating.

Review of the modern system of machine translation for the Kazakh language and classification of errors

To determine the errors that arise in the machine translation, a comparative analysis of the translation of simple descriptive sentences in the machine translation systems was conducted.

Table 2. Examples of translating English and Russian texts into Kazakh on Yandex and Google

Genre	The original text is in Russian / Kazakh	Google Translate	Yandex
Scientific	В качестве примеров таких задач могут служить задачи распознавания технического состояния объекта и классификации этого состояния (нормального или аномального), обнаружения факта передачи или отсутствия единственного сигнала, нормального или патологического состояния органа.	Мұндай тапсырмалардың мысалы ретінде объектінің техникалық күйін тану және осы күйді жіктеу (қалыпты немесе қалыптан тыс), бір сигналдың таралуы немесе болмауы, мүшенің қалыпты немесе патологиялық күйін анықтау міндеттері жатады.	Мұндай міндеттердің мысалы ретінде объектінің техникалық күйін тану және осы күйді жіктеу (қалыпты немесе қалыпты емес), жалғыз сигналдың берілу немесе болмауы фактісін, органның қалыпты немесе патологиялық жағдайын анықтау Міндеттері болуы мүмкін.
	They are served as features in our d-gram model replacing the traditional n-gram model.To obtain dependency parse trees, we first applied TreeTagger for tokenization and POS-tagging. Next, we fed the tagged output to the MaltParser that we had	Олар дәстүрлі n-грамм моделін алмастыратын d-gram моделінің ерекшеліктері ретінде қызмет етеді. Тәуелділікті талдау үшін біз алдымен TreeTagger-ді токенизация және POS-тегтеу үшін	Олар біздің d-грамм моделімізде дәстүрлі N-грамм моделін алмастыратын функция ретінде қызмет етеді. Тәуелділіктің синтаксистік талдау ағаштарын алу үшін алдымен treetagger-ті

	trained on the Russian National Corpora.	қолдандық. Содан кейін біз Ресейдің ұлттық корпорациясында оқыған MaltParser-ге шығарылған өнімдерді жібердік.	токенизация және POS тегтеу үшін қолдандық. Содан кейін біз Ресейдің ұлттық корпустарында оқыған MaltParser - дің белгіленген нәтижесін тамақтандырдық.
Publicistic	Среди придуманных Каплевичем холодных, безжизненных, монументальных мраморных столбов протекает жизнь профессора Хигинса. Такое впечатление, что выдающийся филолог, истинный джентльмен живет на вокзале.	Каплевич ойлап тапқан суық, жансыз, ескерткіш мәрмәр тіректердің ішінде профессор Хиггинстің өмірі жалғасуда. Бекетте көрнекті филолог, нағыз джентльмен өмір сүретін көрінеді.	Каплевич ойлап тапқан суық, жансыз, монументалды мәрмәр тіректердің ішінде профессор Хигинстің өмірі жалғасуда. Бұл керемет филолог, нағыз джентльмен станцияда тұрады.
	Some have taken the anti-Obama ad as a reference to a “Stop Obama!” video posted last week that showed dozens of Russian students falling to the floor as if dead, revealing a lone girl with a sign claiming that the “president of the United States kills 875 people every week”	Кейбіреулер Обамаға қарсы жарнаманы «Обаманы тоқтат!» Деген сілтеме ретінде қабылдады. Өткен аптада жарияланған ондаған ресейлік студенттердің «АҚШ президенті апта сайын 875 адамды өлтіреді» деген жазуы бар жалғыз қызды еденге өлгендей құлап жатқанын көрсететін видео	Кейбіреулер антиобамдық жарнаманы " Обаманы тоқтатыңыз!өткен аптада видео жарияланды, онда ондаған ресейлік студенттер еденге өлі сияқты түсіп," Америка Құрама Штаттарының Президенті апта сайын 875 адамды өлтіреді " деген белгісі бар жалғыз қызды көрсетті”

The machine translation programs have their own advantages and disadvantages, as shown in Table 3. Analyzing the work of each of them, we were able to identify possible errors in translation from the Kazakh language and vice versa. Based on the errors, we are trying to find out in which cases MTS (machine translation systems) made mistakes when translating from Russian into Kazakh.

Table 3. Comparative description of the work of online machine translation systems in the Kazakh language

№	MTS	Disadvantages	Advantages
1	Google translator	There are some inconsistencies in the large proposals, but in most cases they are very small. Some place names, water names and regular expressions have been fixed by the post editor.	Complex scientific texts are translated well and qualitatively, there are some differences.
2	Yandex Translator	Some negative sentences have morphological problems.	Translates very large sentences, complex scientific texts.

3	Tridentsoftware	When translating many simple sentences, it was not possible to find a translation of many words.	There were only simple words translated.
4	Prof-translate	Translations of some names have not been found at all.	You can get good results when translating short sentences and phrases.

Below is the evaluation of the translation of the examples presented in 4 different MTS:

- The well-formed sentences (with the beginning, with the narrator) were well translated by Google, Yandex.Translator. Tridentsoftware brought the sentence back to its original form. prof-translate.ru led from a single sentence to a single sentence.
- Only the Google translator correctly translated the phrase “I am at the university” consisting of only the beginning and the narrator.
- Personal names, ie land and water names, were translated correctly by 3 MTS without errors, except for Google translation.
- Regular expressions were re-translated by all MAS literally or in Russian.
- Yandex, Google MTS translates at a very high level compared to other MTS.

Development of a post-editing system for machine translation

Translation of sentences from one language into another is closely related to machine translation. As a result of machine translation, there are always certain deficiencies that can be eliminated after editing. Post-processing is the processing of human text after machine translation. Today, many suppliers of linguistic services are actively developing this direction, developing methods of training editors and editing methods. The main purpose of this work is to increase the quality of the Anglo-Kazakh, Russian-Kazakh machine translation system. The developed model with the subsequent editing should be implemented in the form of experimental machine translation systems. This article suggests a post-processing method based on two-step procedures: the first detects text errors with the help of memory technology translations, and the second uses a model of maximum entropy, so that the second definition is determined. When it comes to machine translation, the computer does not understand the meaning of the text and the nuances of the language. Each new sentence structure, sentence, idiom is included in the program. Depending on the style and purpose of the text, a word can have several meanings.

At this time, the machine translation software can recognize the style of the text and choose the right translation accordingly. The program itself can offer the translator several translations. The main idea of this work is to find the wrong words in the Kazakh language in the translation of English sentences and to correct the wrong Kazakh words. It is recommended to use the technology of memory for translation of incorrect words in the translated text and to use the model of maximum entropy for correction of incorrect words [4]. Earlier the system was applied to "trained" and "working" texts in parallel cases. Preliminary training systems can increase the accuracy of translation, make terminology more convenient and reduce costs for post-processing.Figure 1 shows the machine translation model after editing.

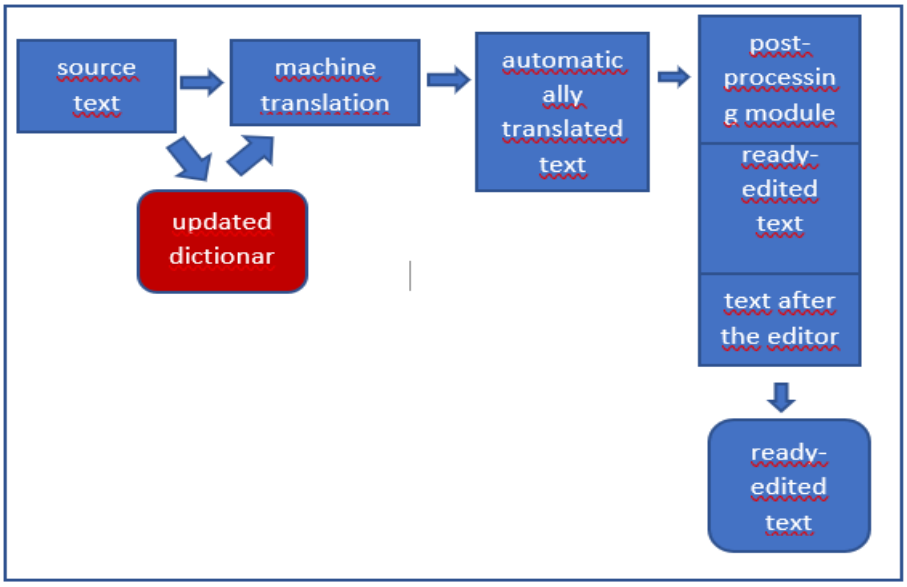


Fig.1 Post-editing model of machine translation

Figure 1 shows the post-edited architecture: the text is presented in a specific language (source), then the text is copied into a machine translation and updated dictionary, in the next step the automatically translated text is checked by a post-editor and the finished text is obtained [5].

Word processing methods. The approach presented in the article consists of two modules. The post-editor function detects incorrect words, then identifies the text after translation to apply the analysis and module to them. The method of maximum entropy is used to process words and phrases in English-Kazakh, Russian-Kazakh sentences. The main purpose of the learning model is determined by the first stage - finding the wrong words and correcting these words. Initially, we take English and Russian sentences, translate them with Google Translate, and then manually write the correct translation of Kazakh sentences. We have two files: from the translator and individually translated Kazakh sentences. These sentences from the two files (Google Translate and expected correct translation) are aligned with the matrix phrase alignment method (Koehn, Statical Machine Translation, p. 113) [6] and with inconsistent segments and words.

The main goal of the second stage is to correct the sentence in advance with incorrect words. Parallel sentences in about two languages (approximately 100,000) are used to analyze the original data. These suggestions are used to create tables for system training. We use the maximum entropy to create cubic tables. That is, the system is trained using the earlier creation of cubic tables. The table is based on a bilingual parallel body and a bilingual dictionary. Indicators show that only the first level is activated, multiplied by two for the second level, and the remaining part of the division is transferred to a number of other levels. This approach is not necessary for the introduction of the classifier, but for the understanding of the theory it is necessary to understand the difference between the sign and the indicator, as well as the difference in their numbering.

Classification is carried out according to the formula:

$$p(c|d,\lambda) = \frac{exp\sum_{i}^{n*k}\lambda_i f_i(c,d)}{\sum_{\tilde{c}\in C} exp\sum_{i}^{n*k}\lambda_i f_i(\tilde{c},d)} \quad (1)$$

In this formula [7]:

f_i – i-th classification indicator (0 or 1);

λ_i - weight of the indicator f_i of the i-th classification;
c – class hypothesis;
C - the sum of all possible classes;
D - classified document

Each indicator f_i has its own weight λ_i, which describes the relationship between the relevant classification criteria and the class. The heavier the weight, the stronger the bond. Thus, the fractional charge describes the weight exponent for the class - the hypothesis, and normalizes the allocated value in units. The most difficult part of this formula is the set of weights, which must be determined by numerical optimization, which we will talk about later [8].

Application of the method in the post-processing system. The method of maximum entropy is closely related to another common machine learning algorithm - logistic regression. That is, when using this method, we get an alternative word that is described above and has a meaning close to the context. The result of this approach is not just a classification decision, but a probability for a particular class. One of the advantages of this classification is the specification of the possible distribution of classes. If you use a machine translation from English into Kazakh, if the sentence contains incorrect words, the incorrect words should be edited later. Then, after finding the wrong, erroneous words in the sentence, we check their translation one by one, find and enter the correct translation to use it based on the method of maximum entropy. The general description of the method is as follows [9]:

$$f_i^j = \begin{cases} 1, \ if\ d = w_i, c = AW_j \\ 0, \ for\ other\ cases \end{cases} \quad (2)$$

$W_j -$ alternative words (class), $d -$ classified document, f_i- i-th classification indicator (0 or 1), $j - \overline{1,n}$;

A database of ambiguous dictionaries and TM (Translation Memory) are used to correct incorrect words, for example, the following elements are given (Table 4).

For the experiment, the text was obtained, consisting of short sentences. In this text, the word "liver" is incorrectly interpreted and indicated its equivalents:

Table 4. Examples of English synonyms and alternative words found in the texts.

Alternative words	Examples of phrases
Бауырмашыл	Бауырмашыл адамдарды
Бауыр	Бауыр - адам мүшесі.
Бауыр басу	бауыр баспа
Бауыр жіп	бауыр жіп
Бауыр алу	"бауыр алу" ырымын

1Бауырмашыл адамдарды қатты сыйлаймын. (Я очень уважаю людей-баурсаков).

2Бауыр - адам мүшесі. (Печень-это человек).

3 Ешкімге бауыр баспа (Никому печатать печень)

4 Бауыр жіп — түйе жабуының бауырбауы (Печеночные нитейно-верблюжье покрытие).

5 Кеше қонақтар "бауыр алу" ырымын өткізді. (Вчера гости провели обряд "получение печени").

We used the maximum entropy:

$$f^1 = \begin{cases} 1, \ if\ d = "f_3 \wedge f_4 \wedge f_5", c = AW_1 \\ 0, \ for\ other\ cases \end{cases} \quad (3)$$

$$f^2 = \begin{cases} 1, \ if\ d = "f_1 \wedge f_2 \wedge f_5", c = AW_2 \\ 0, \ for\ other\ cases \end{cases} \quad (4)$$

$$f^3 = \begin{cases} 1, \ if\ d = "f_2 \wedge f_5", c = AW_3 \\ 0, \ for\ other\ cases \end{cases} \quad (5)$$

$$f^4 = \begin{cases} 1, \ if\ d = "f_2 \wedge f_3 \wedge f_4", c = AW_4 \\ 0, \ for\ other\ cases \end{cases} \quad (6)$$

$$f^5 = \begin{cases} 1, \ if\ d = "f_4 \wedge f_5", c = AW_5 \\ 0, for\ other\ cases \end{cases} \quad (7)$$

Suggestions translated by experts are compared with sentences processed in the system. As a result, the translation of experts and our methods was in second place. By learning to agree, it is possible to say more accurately about the proposed system and improve the quality of translation.

Conclusion

Thus, as a result of our study, we came to the following conclusions:

• Linguistic structure and features of Turkic languages are considered

• Translation errors are identified, the general advantages and disadvantages of the online machine translation system in the Kazakh language are given.

• A model for the development of a post-processing machine translation system for the Kazakh language is proposed.

• The method of alignment and the method of maximum entropy were used, the analysis of the post-processing process was performed.

Thank you

This work was carried out under the research project AP08052421 "Research and development of the post-editing system of the Kazakh language in machine translation" with the support of the Ministry of Education and Science of the Republic of Kazakhstan

Literature

1. Андреева А. Д., Меньшиков И. Л., Мокрушин А. А. Обзор систем машинного перевода // Молодой ученый. — 2013. — № 12 (59). — С. 64—66.

2. Бабина О. И. Языковая личность переводчика и машинный перевод // Вестн. ЧелГУ. — 2011. — № 24.

3. Вопияшина С. М., Мурдускина О. В. Обучение редактированию перевода как способ повышения качества подготовки лингвистов-переводчиков // БГЖ. — 2016. — № 4 (17).

4. Зубов А. В., Зубова И. И. Информационные технологии в лингвистике. — М. : Академия, 2004. — 208 с.

5. Кочеткова Н. С., Ревина Е. В. Особенности машинного перевода // Филологические науки. Вопросы теории и практики. — 2017. — № 6-2 (72).

6. Максютина О. В. К вопросу об обучении редактированию и саморедактированию перевода // Филологические науки. Вопросы теории и практики. — 2014. — № 4-3 (34). — С. 121—124.

7. Максютина О. В. Редактирование перевода как неотъемлемая часть современного стандарта качества // Вестн. Том. гос. пед. ун-та. — 2014. — № 4 (145). — С. 106—111.

8. Марчук Ю. Н. Проблемы машинного перевода. — М. : Наука, 1983. — 201 с.

9. Nal Kalchbrenner, Phil Blunsom. Recurrent Continuous Translation Models. Proceedings of the 2013 Conference on Empirical Methods in Natural Language Processing, Seattle, Washington, USA, p. 1700–1709(2013)

LINK GRAMMAR PARSER И ФОРМАЛЬНЫЙ АНАЛИЗ ПЕРЕФРАЗИРОВАННЫХ ПРЕДЛОЖЕНИЙ НА ЕСТЕСТВЕННОМ ЯЗЫКЕ

А.С. Еримбетова[1,4], Ф.А. Мурзин[2,3], Ф. Озодов[3], А. Жанабеков[1]
e-mail: aigerian@mail.ru
[1]Институт информационных и вычислительных технологий КН МОН РК,
[2]Институт систем информатики им. А.П. Ершова СО РАН, Россия,
[3]Новосибирский государственный университет, Россия,
[4]Казахская академия транспорта и коммуникаций им. М. Тынышпаева, Казахстан

Аннотация. *Целью работы является создание базы знаний, содержащей информацию о перефразированных предложениях, в том числе содержащих временные и пространственные понятия, встречающиеся в текстах естественного языка. Содержание базы: важнейшие понятия из толкового словаря С. И. Ожегова; перефразированные предложения; результаты анализа лексических статей (толкований) и примеров из литературы с помощью Link Grammar Parser и набора программных комплексов и др. Результаты работы могут быть использованы в интеллектуальных информационно-поисковых системах. Диаграммы, полученные на выходе синтаксического анализатора Link Grammar Parser и систем DIALING, представляют собой чрезвычайно интересный материал для дальнейших исследований. Целесообразно исследовать возможность использования ряда конструкций и понятий математической логики в компьютерной лингвистике, таких как: построение Л. Хенкина, реализуемость и пропуск типов, полнота модели, форсирование, а также ряд неклассических логик.*

1. Введение

Основная цель состоит в исследовании конструкций в естественном языке, содержащих различные понятия в семантическом плане.

Создана база знаний, содержащая информацию о перефразированных предложениях, в том числе содержащих временные и пространственные понятия. База знаний содержит: наиболее важные понятия из толкового словаря С. И. Ожегова [10]; перефразированные варианты некоторых предложений; результаты анализа записей (интерпретации) и примеров использования в художественной литературе соответствующих понятий из словаря С. И. Ожегова с помощью программных систем Link Grammar Parser и DIALING [3].

Далее предполагается изучить диаграммы, полученные на выходе систем Link Grammar Parser и DIALING с помощью математической логики. Речь идет об исследовании возможностей применения в компьютерной лингвистике некоторых конструкций и понятий математической логики, таких как: построение Хенкина, реализация и опущение типов, полнота модели, форсирование, а также некоторых неклассических логик.

Предполагается провести анализ с помощью математической логики свойств лексических функций И.А. Мельчука [1] в контексте определения смысла и теоретико-множественных моделей языка, предложенных С. Маркусом.

В дальнейшем работа будет включать также исследования комбинаторных свойств лингвистических определений и конструкций, возможностей применения в компьютерной лингвистике понятий из теоретико-множественной и алгебраической топологии и исследования географических понятий.

Результаты работы могут быть использованы в интеллектуальных системах информационного поиска. А именно, для определения релевантности текста поисковому запросу и для определения тематики текстов. Она также представляет интерес для ученых, работающих в области теоретической лингвистики.

2. Формальные методы исследования семантики текстов

Семантика-раздел лингвистики, изучающий семантическое значение единиц языка: отдельных слов, словосочетаний, предложений, фрагментов текста. В настоящее время существует ряд машинно-ориентированных методов представления смысла предложений [1-9].

Например, И.А. Мельчук ввел понятие лексических функций, разработал понятия синтаксических и семантических валентностей и рассмотрел их в контексте толково-комбинаторного словаря [1]. В.С. Рубашкин и Д. Г.Лахути [5, 6] ввели иерархию синтаксических связей для более эффективной работы семантического анализатора. Подход И. А. Мельчука поддерживается в программной системе набора номера [3].

Появилось понятие универсального языка для представления знаний. Это может быть удобный инструмент для получения новых знаний из уже имеющихся. Вполне вероятно, что в будущем исследования будут развиваться в направлении создания таких семантических языков. Например, сейчас система под названием Knowledge Vault содержит 1,6 миллиарда фактов. Система NELL, разработанная в рамках проекта ReadTheWeb Университетом Карнеги-Меллона, содержит более 50 миллионов утверждений, дополнительно характеризующихся различной степенью доверия.

Еще одним подходом является использование системного синтаксического анализатора Link Grammar Parser [11-13], разработанного в Университете Карнеги-Меллона и основанного на некоторой специальной теории синтаксиса. Можно

заметить, что данная теория, вообще говоря, отличается от классической теории синтаксиса. Имея полученное предложение, система приписывает ему некоторую синтаксическую структуру, которая состоит из множества отмеченных соединителей (звеньев), соединяющих слова.

Полученные диаграммы, по сути, являются аналогами так называемых деревьев представления предложений. В деревьях подчинения можно задать вопрос от главного слова в предложении к второстепенному. Таким образом, слова выстраиваются в древовидную структуру. Основной причиной, по которой анализатор называется семантической системой, можно назвать уникальный по полноте набор ссылок. В наличии имеется около 100 базовых ссылок, при этом некоторые из них дополнительно имеют 3-4 варианта.

Наши исследования проводятся в соответствии со следующими пунктами.

1. Выбор наиболее важных понятий, касающихся времени и пространства, из толкового словаря С. И. Ожегова.

2. Создание набора перефразированных вариантов различных предложений и методов оценки их сходства.

3. Анализ записей (интерпретация) и использование примеров в художественной литературе, содержащих соответствующие понятия из словаря С. И. Ожегова, с помощью программных систем Link Grammar Parser и DIALING.

4. Анализ диаграмм, полученных на выходе систем

3. Синтаксический анализатор Link Grammar Parser

Link Grammar Parser – это синтаксический анализатор английского языка, разработанный в 1990 годы в Университете Карнеги-Меллона, США, основанный на некоторой теории. Заметим, что в целом данная теория отличается от классической теории синтаксиса. Получив предложение, система связывает его с синтаксической структурой, которая состоит из набора отмеченных связей, соединяющих пары слов. Подробное описание системы можно найти в [11-13].

Синтаксический анализатор Link Grammar Parser включает в себя около 60000 словарных форм. Он позволяет анализировать огромную часть синтаксических конструкций, в том числе многочисленные редкие выражения и идиомы. Работа синтаксического анализатора стабильна; он может пропустить часть предложения, которую он не может понять, и определить некоторую структуру для остальной части предложения. Он способен обрабатывать неизвестную лексику и делать обоснованные предположения о синтаксической категории неизвестных слов из контекста и письма. Он содержит данные о различных именах, числовых выражениях и различных знаках препинания.

Правила соединения слов описаны в наборе словарей. Для каждого слова в словаре фиксируется, какими соединителями оно может быть связано с другими словами в предложении. Соединитель имеет имя, с которым рассматриваемая единица (слово) может входить в предложение. Например, знак S соответствует связи между субъектом и предикатом, O-соединителю между объектом и предикатом. Только основных, наиболее важных разъемов, насчитывается более ста. Для обозначения направления соединителя знак "+" используется для обозначения правого соединителя, а знак "–" - для обозначения левого соединителя. Левый и правый разъемы одного типа образуют соединение (линк).

1. Практическая апробация системы показывает, что при анализе сложных

предложений, длина которых превышает 25-30 слов, возможен комбинаторный взрыв, и результатом работы анализатора становится "панический" граф, как правило, имеющий случайный вариант синтаксической структуры, неадекватный с лингвистической точки зрения.

2. Применение описанных выше идей затруднено для таких флективных языков, как русский, в представление о значительно увеличивающемся объеме словарей, которое возникает в связи с морфологическим развитием флективных языков. Каждая морфологическая форма должна быть описана отдельной формулой, где нижний индекс имени соединителя должен обеспечивать процедуру согласования. Это приводит к увеличению количества разъемов. Для агглютинативных языков (например, тюркских) эта система становится еще более сложной.

Ниже приведены примеры разбора двух предложений.

1. Уборщица убирает дом раз в неделю.

```
                        +--------MVs-------+
                        +-----Os----+      +---Mp--+
  +--Ds--+----Ss---+     +--Ds-+      |  +-NSa+
  |      |         |     |     |      |  |    |
 the cleaner.s cleans.v the house.n once a week.i
```

2.The house is cleaned by the cleaner once a week.

$Ss(cleaner,\ cleans) \wedge Os(cleans,\ house) \leftrightarrow Ss(house,\ is) \wedge Pv(is,\ cleaned) \wedge MVp(cleaned,\ by) \wedge Js(by,\ cleaner)$

```
                        +-----------MVs----------+
                        |      +----Js---+       +---Mp--+
  +--Ds-+--Ss--+--Pv--+--MVp-+  +--Ds--+       |  +-NSa+
  |     |      |      |      |  |      |       |  |    |
 the house.n is.v cleaned.v by the cleaner.s once a week.i
```

4. Перефразированные предложения

Известно, что естественные языки обладают разнообразием способов выражения смысла, можно передать одну и ту же мысль разными словами. Эта особенность значительно усложняет анализ текстов на естественном языке, и проблема выявления сходного смысла в разных высказываниях трудно формализуема. Формализация анализа временных и пространственных концептов текстов позволяет хотя бы частично приблизиться к решению этой задачи. В данном разделе рассматривается процесс выявления перефразированных предложений, содержащих впереди, сзади, сбоку, раньше, позже, еще, уже; с точки зрения их перефразирования.

Существуют две формы эквивалентности:

1) $x_1 \approx x_2 \leftrightarrow x_1 = x_2 \vee Syn(x_1, x_2)$

2) $x_1 \equiv x_2 \leftrightarrow Norm(x_1) = Norm(x_2)$.

Предположим, что даны два предложения. Интересно рассмотреть функции такие, что с дополнительными свойствами формы: и, и другие подобные.

При сравнении двух предложений, точнее, при анализе их близости, проводится проверка некоторых логических свойств. Например, пусть примеры

таких свойств приведены ниже.

1. Инвариантность коннектора

$\bar{x} \models P(x_{i_1}, x_{i_2}) \to \bar{y} \models P(y_{j_1}, y_{j_2})$

2. Замена соединителя на дизъюнкцию других

$\bar{x} \models P(x_{i_1}, x_{i_2}) \to \bar{y} \models \bigvee_t Q_t(y_{j_1}, y_{j_2})$

3. Разделение разъема на два разъема

$\bar{x} \models P(x_{i_1}, x_{i_2}) \to \exists k\ (\bar{y} \models Q(y_{j_1}, y_k) \wedge R(y_k, y_{j_2}))$

4. Разделение разъема на два разъема с инверсией

$\bar{x} \models P(x_{i_1}, x_{i_2}) \to \exists k\ (\bar{y} \models Q(y_{j_2}, y_k) \wedge R(y_k, y_{j_1}))$

Учитывая, что это обозначение для соответствующей модели, формулу из третьего пункта можно переписать в виде

$\bar{x} \models P(x_{i_1}, x_{i_2}) \to \bar{y} \models \exists y Q(y_{j_1}, y) \wedge R(y, y_{j_2})$

Аналогично формула из четвертого пункта может быть записана в аналогичной форме.

Подводя итог можно сказать что существуют правила формы

$R_i : \bar{x} \models \varphi_i(x_1, x_2) \to \bar{y} \models \psi_i(y_1, y_2)$

Заметим, что для английского языка мы зафиксировали более тридцати таких правил. Для русского и других языков этот вопрос менее изучен. Для системного набора номера также могут быть сформулированы аналогичные правила, но это более сложный вопрос.

Рассмотрим множество всех таких пар, на которых выполняется одно из правил. Обозначим это множество ПО и пусть его кардинальности . Заметим, что анализатор Link Grammar Parser предполагает наличие только одного соединителя между двумя словами. Поэтому будет выполнено не более одного правила.

5. Примеры перефразированных предложений на английском языке

1. Усложнение расширенного определения.

1.1. The flowers that he has bought were beautiful.

```
                 +-----------------Spx-----------------+
                 +--------------Bp--------------+       |
   +--Dmc-+-----R----+---Cr--+-Ss+---PP--+       +---Pa---+
   |      |          |       |   |       |       |        |
 the flowers.n that.misc-r he has.v bought.v were.v beautiful.a
```

1.2. The flowers that have been bought by him were beautiful.

Cr(*that, he*) ∧ *Ss*(*he, has*) ∧ *PP*(*has, bought*) ↔ *RS*(*that,have*) ∧ *PPf*(*have, been*) ∧ *Pv*(*been, bought*) ∧ *MVp*(*bought,by*) ∧ *J*(*by,him*).

```
          +-----------------------Spx----------------------+
          +---------Bp---------+                            |
   +--Dmc-+-----R----+----RS---+--PPf-+---Pv--+-MVp-+-J+     +---Pa---+
   |      |          |         |      |       |     | |     |        |
 the flowers.n that.misc-r have.v been.v bought.v by him were.v beautiful.a
```

2. A synonymic series expressing target relationships

2.1. You had put on that costume for making fun.

(*MVp* + ((*Mgp* + *Os*) *or Js*), etc.

```
            +--------------MVp-------------+
            +----------Osn---------+       |
 +-Sp-+--PP-+--K-+      +----D*u---+       +--Mgp--+--Os--+
 |    |     |    |      |          |       |       |      |
you had.v put.v on that.misc-d costume.n for.p making.v fun.n
```

2.2. You had put on that costume for make fun.

Mgp(*for, making*) ∧ *Os*(*making*, *fun*) ↔ *Jp*(*for*, *fun*).

2.3. You had put on that costume so that you could make fun.

```
            +--------------MVp-------------+
            +----------Osn---------+       |
 +-Sp-+--PP-+--K-+      +----D*u---+       +-----Jp-----+
 |    |     |    |      |          |       |            |
you had.v put.v on that.misc-d costume.n for.p [make] fun.n
```

Mgp(*for*, *making*) ↔ *IDC* (*so*, *that*) ∧ *Cs*(*that*, *you*) ∧ *Sp*(*you*, *could*) ∧ *I*(*could*, *make*).

```
            +---------------MVs---------------+
            +----------Osn---------+          |
 +-Sp-+--PP-+--K-+      +----D*u---+      +IDC+-Cs+--Sp-+---I---+--Os-+
 |    |     |    |      |          |      |   |   |     |       |     |
you had.v put.v on that.misc-d costume.n so that you could.v make.v fun.n
```

5. Примеры перефразированных предложений на русском языке

Давайте рассмотрим предложение «Вблизи ветер дул сильнее» (*Near the wind blew stronger*).

Существует 4 варианта синтаксического анализа этого предложения с помощью Link Grammar Parser

```
    +------------------------Xp-----------------------+
    +--------------Wd--------------+                   |
    |        +----EI---+----Sm3----+-----E-----+       |
    |        |         |          |          |       |
LEFT-WALL вблизи.e ветер.ndmsi дул.vnpdpms сильнее.as .
```

```
    +------------------------Xp-----------------------+
    +--------------Wd--------------+                   |
    |        +----------EI---------+                   |
    |        |         +----Sm3----+-----E-----+       |
    |        |         |          |          |       |
LEFT-WALL вблизи.e ветер.ndmsi дул.vnpdpms сильнее.as .
```

```
    +------------------------Xp---------------------+
    +-------------------Wd------------------+        |
    |                  +---------Sm3---------+        |
    |        +----EI---+----Mg----+          |        |
    |        |         |          |          |        |
LEFT-WALL вблизи.e ветер.ndmsi дул.ndnpg сильнее.as .
```

```
    +------------------------Xp-----------------------+
    +--------------Wd--------------+                   |
    |        +----EI---+----MVIv---+-----E-----+       |
    |        |         |          |          |       |
LEFT-WALL вблизи.e ветер.ndmsv дул.vnpdpms сильнее.as .
```

Здесь принимаются следующие обозначения.

Xp – ссылка для соединения начала предложения с точкой (в конце предложения).

Wd – ссылка указывает на начало предложения.

EI – связь с наречием, обозначающим пространственное понятие.

Sm3 – связывает подлежащее с глаголом (строчные буквы дополняют информацию о роде и лице).

E – связь между глаголом и изменяющим его наречием.

Mg – связь между существительным и причастием.

MVIv – объединяет предикат с дополнением.

Мы видим, что соединение Xp присутствует во всех схемах. Можно сказать, что она инвариантна. Слово вблизи (рядом), относящееся к пространственным понятиям, рассматривается в нашей сигнатуре как константа. Относительно других неинвариантных отношений, используя логические формулы, мы можем записать существующие эквивалентности.

$$x_1 = ветер$$

$$x_2 = дул$$

$$\varphi_1 = EI(вблизи, x_1) \wedge Sm3(x_1, x_2)$$

$$\varphi_2 = EI(вблизи, x_2) \wedge Sm3(x_1, x_2)$$

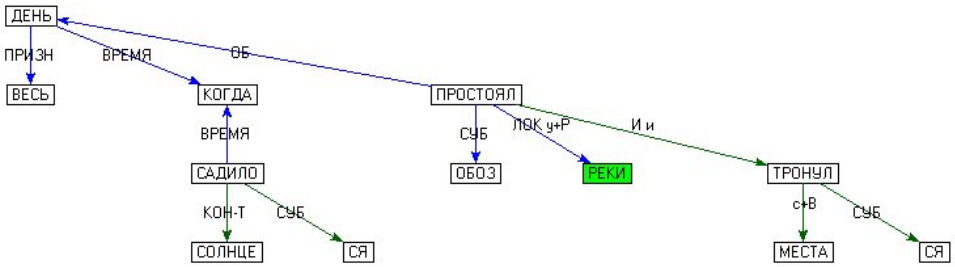
$$\varphi_3 = EI(вблизи, x_1) \wedge Mg(x_1, x_2)$$

$$\varphi_4 = EI(вблизи, x_1) \wedge MVIv(x_1, x_2)$$

$$\varphi_1 \leftrightarrow \varphi_2 \leftrightarrow \varphi_3 \leftrightarrow \varphi_4.$$

5. Система DIALING.

Идеи, рассмотренные в предыдущих разделах, могут быть применены для анализа перефразированных предложений, а именно для оценки их близости, также на основе диаграмм, полученных на выходе системы набора номера. Система набора номера разрабатывалась как система русско-английского перевода с 1999 по 2002 год на базе ООО "набор" (Москва) [3]. В разное время в работе над системой принимали участие более 20 специалистов, большинство из которых были известными учеными-лингвистами. Как и все современные системы обработки текстов, набор номера включает в себя все основные этапы анализа текста.



Let us consider some examples.

1. Обоз весь день простоял у реки и тронулся с места, когда садилось солнце.

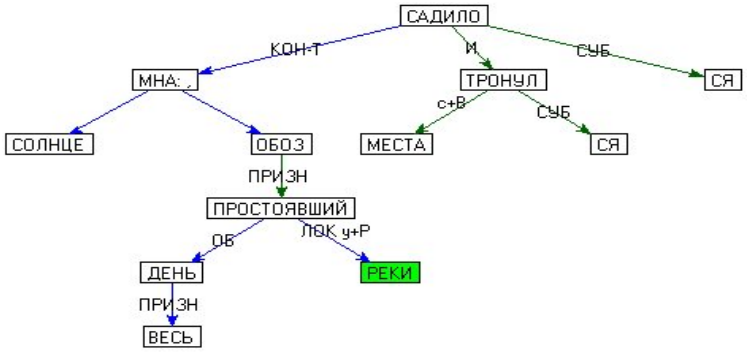
The convoy stood all day by the river and set off when the sun was setting.

2. Садилось солнце, обоз, простоявший весь день у реки, тронулся с места.

The sun was setting, the convoy, which stood all day by the river, began to move

2.1. Syntactic parsing result.

2.2. Semantic analysis result



6. Заключение

В работе описан процесс создания базы знаний, содержащей информацию о временных и пространственных понятиях, появляющихся в текстах на естественном языке. Формально описан процесс обнаружения перефразированных предложений, содержащих некоторые пространственные и временные понятия. Сейчас ведется работа по наполнению базы знаний. В результате проведенного исследования был сделан вывод о целесообразности применения таких инструментов, как синтаксический анализатор ссылок и набор номера для решения рассматриваемой задачи.

Link Grammar Parser – это достаточно необычная система, основной причиной, по которой анализатор называет семантическую систему, является то, что ее можно считать уникальным по полноте набором ссылок. Например, выделяются следующие классы наречий: ситуативные наречия, которые относятся ко всему предложению в целом (клаузальное наречие); временные наречия; вводные наречия, которые стоят в начале предложения и разделяются запятой (открыватели); наречия, модифицирующие прилагательные и др. Из достоинств системы следует отметить, что организация процедуры нахождения вариантов синтаксического представления очень эффективна.

Отметим также и негативные моменты. Практическое тестирование системы показывает, что при анализе сложных предложений, длина которых превышает 25-30 слов, возможен комбинаторный взрыв, а "панический" граф, как правило, случайный вариант синтаксической структуры становится результатом работы анализатора, с лингвистической точки зрения неадекватным. Использование этой системы затруднено для флективных языков, таких как русский, в связи с увеличением объемов словарей, возникающих в связи с морфологическим развитием флективных языков.

Для случая английского языка было проведено тестирование [15]. Основной

целью является определение релевантности текста поисковому запросу. В этом случае был найден минимальный вариант, дающий достаточно хорошие результаты, когда рассматривалось всего 8 звеньев. Для английского языка определен список наиболее важных ссылок системного синтаксического анализатора Link Grammar Parser. Он содержит 35 ссылок. Были обнаружены ссылки, которые существенно портили ситуацию в случае неполных предложений. Таких ссылок 8. Для русского языка такой детальный анализ ссылок не проводится. Возможности системного набора номера изучены еще меньше.

Тем не менее, следует отметить, что диаграммы, полученные на выходе систем Link Grammar Parser и DIALING, представляют чрезвычайно интересный материал для дальнейших исследований; в том числе для исследований временных и пространственных понятий; как с точки зрения приложений, так и для теоретической лингвистики.

Работа выполнена в рамках грантового финансирования по научным и (или) научно-техническим проектам на 2018-2020 годы МОН РК № AP05133550

Литература

1. I.A. Melchuk “Experience of Theory of Linguistic Models like Sence ↔ Text”, *Moscow*: *Nauka*, 1974.
2. U.D. Apresyan “Experimental Semantic Investigation of a Russian Verb”, *Moscow*: *Nauka*, 1967.
3. A.V. Sokirko “Semantic dictionaries in automatic word processing”, *Cand. Diss. (PhD Thesis), MGPII, Moscow*. 2000.
4. E.V. Paducheva “Dynamic models in semantics of lexic”, *Moscow: Languages of Slavic culture*, 2004.
5. D.G. Lakhuti “The automatic analysis of texts in a natural language”, *Information Processes and Systems,* Vol 11, 2003, pp. 18-25.
6. V.Sh. Rubashkin “Meaning Representation and Analysis in Intelligent Information Systems”, *Moscow*: *Nauka*, 1989.
7. S. Markus “Set-theoretical Models of Languages”, *Moscow*: *Nauka*, 1970.
8. T. Batura and F. Murzin “Logical Methods for Representing Meaning of Natural Language Texts”, *Proceedings ICCS,* Vol. 3038, 2004, pp. 545-551.
9. T.V. Batura and F.A. Murzin “The Machine-Oriented Logic Methods of Representation of Semantics of the Text in Natural Language”, *Novosibirsk*: *Publishing Company of NGTU*, 2008.
10. S.I. Ozhegov “Explanatory dictionary of the Russian language”, *Moscow*: *Mir i obrasovaniye*, 2014.
11. D. Temperley, D. Sleator and J. Lafferty “Link Grammar Documentation”, 1998, http://www.link.cs.cmu.edu/link/dict/index.html
12. “Link Grammar Documentation”, 2015, http://www.abisource.com/projects/link-grammar
13. “The CMU Link Grammar natural language parser”, 2018, https://github.com/opencog/link-grammar/
14. T.V. Batura, F.A. Murzin, A.A. Perfliev and T.V. Shmanina “Methods of the Increase of the Efficiency of Information Search on the Basis of Syntactic Analysis”, *Novosibirsk*: *Publishing Company of SB RAS*, 2014.

15. T.V. Batura, A.M. Bakieva, A.S. Yerimbetova, F.A. Murzin and S.K. Sagnayeva "Link grammar, relevance and definition of themes of texts", *Novosibirsk*: *Publishing Company of SB RAS*, 2018.
16. T.V. Batura, F.A. Murzin, D.F. Semich, A.M. Bakiyeva, A.S. Yerimbetova and S.K. Sagnayeva "Estimation of the Degree of Similarity of Sentences in a Natural Language Based on Using the Link Grammar Parser Program System", *Journal of Theoretical and Applied Information Technology,* Vol.86, 2016, Iss. 1, pp.68-77.
17. A.S. Yerimbetova, S.K. Sagnayeva, F.A. Murzin and J.A. Tussupov "Creation of tools and algorithms for assessing the relevance of documents", *Proceedings RPC,* 2018, Electronic publication: 9781538675311. Paper № 8482202.
18. F. Murzin, A. Yerimbetova, M. Tussupova and K. Aleksandrov "Development and analysis of technologies of searching information relevant to the search query using linguistic support", *Proceedings DAMDID/RCDL,* 2018, pp 207-214.
19. S. Tazhibayeva and B. Yeskeldiyeva. "A comparison of equality in Kazakh and Turkic Languages of Siberia", *Mediterranean Journal of Social Sciences,* Vol.6, Iss. 4S2, 2015, pp. 398-408, http://www.mcser.org/journal/index.php/mjss
20. S. Tazhibayeva and B. Yeskeldiyeva. "Multilingualism in modern Kazakhstan: New challenges", *Asian Social Science,* Vol. 11, Iss. 6, 2015, pp. 56-64.
21. J. Tussupov, M.A. Sambetbayeva, A.M. Fedotov, O.A. Fedotova, S.K. Sagnayeva, A.A. Bapanov and S.Z. Tazhibaeva "Classification model and morphological analysis in multilingual scientific and educational information systems", *Journal of Theoretical and Applied Information Technology*, Vol.86, Iss. 1, N 10, 2016, pp.96-111

СЕГМЕНТАЦИЯ РУКОПИСНЫХ СИМВОЛОВ С ИСПРАВЛЕНИЕМ НАКЛОНА ТЕКСТА

Елеусинов А.И., Бурибаев Ж.А.
e-mail: armankaznu@mail.ru
Институт информационных и вычислительных технологий КН МОН РК,
Казахский Национальный университет имени аль-Фараби

Аннотация. *Распознавание рукописного текста один из сложных задач в компьютерном зрении. В большинстве исследований распознавание текста осуществляется путем передачи каждой небольшой части сегментированного текста непосредственно в модель на основе нейронной сети.*

Наклонная коррекция - это метод предварительной обработки для повышения точности сегментации и распознавания при распознавании рукописных слов. Все обычные методы коррекции наклона выполнялись путем оценки среднего угла наклона и преобразования сдвига. Предлагаемая здесь методика представляет собой простой и уникальный набор алгоритмов для распознавания текста, который в первую очередь фокусируется на сегментации символов с помощью наклонной коррекции. Эксперименты проводились для текстов, написанных на казахском языке.

Ключевые слова: *наклонная коррекция, сегментация строк, сегментация слов, сегментация символов, преобразование Хафа.*

Введение

Задача распознавания рукописного текста состоит из этапов, а именно оцифровки, предварительной обработки, сегментация слов, сегментация символов, выделения признаков и классификации. Люди могут читать тексты независимо от стиля, в котором они написаны. Разные стили написания текстов затрудняют определить, что написано. По этой причине рекомендуется сделать систему инвариантной к стилю. Одним из основных источников изменчивости, характеризующей стиль письма, является угол наклона. Стиль письма может представлять важные различия между писателями и обычно демонстрирует различия для одного и того же писателя, в зависимости от настроения и скорости письма [1]. В основном стиль письма характеризуется некоторыми общеизвестными особенностями: наклон, уклон и размер символов. Наклон - это угол линии, в которой слово выровнено относительно горизонтального направления, а наклон - это угол по часовой стрелке между вертикальным направлением и доминирующим направлением вертикальных штрихов.

Многие методы были разработаны в попытке удовлетворить потребность в системах распознавания текстов, которые существуют в различных приложениях, таких как автоматическое считывание почтовых адресов и банковских чеков, обработка документов, оцифровка исторических документов и т. д. [2]. Типичными модулями системы распознавания являются предварительная обработка. затем возможная фаза сегментации или фрагментации, извлечение признаков, распознавания и постобработка. Предварительная обработка обычно включает нормализацию, снижение уровня шума, опорную линию, и вывод либо контур или скелет трассировку, если это необходимо.

Многие алгоритмы пытаются улучшить проблемы распознавания рукописного ввода, главным образом, для исправления наклонных букв. Предыдущие исследователи, использующие букву вертикального разделения после скелетирования букв, вычисляют количество слов пикселей, которые будут точкой разделения кандидатов [3].

Основная часть

В литературе существует несколько подходов к коррекции наклона, которые можно условно разделить на три группы. Первый, также исторический, определяет угол наклона, обнаруживая почти вертикальные штрихи и принимая средний угол из них в качестве угла сдвига. Этот подход был начат авторами [4], и несколько других последовали их примеру, используя различные способы выбора штрихов.

Второй подход оценивает функцию измерения изображения в диапазоне углов сдвига и выбирает угол с наибольшим значением меры. Мера чаще всего вычисляется из вертикальной гистограммы, основанной на идее, что у незапланированного письма будет более интенсивная гистограмма, то есть с более высокими и более выраженными пиками, чем у наклонного письма [5].

Третий подход отличается от первых двух неравномерным исправлением наклона. Приведенные выше методы срезают слово (или более крупные единицы) равномерно, то есть под одним углом, следовательно, никогда не могут полностью справиться с наклонно-вариативными словами, которые довольно распространены в обычном почерке. В [6] описан метод неравномерного наклона слов с

использованием методов динамического программирования. Чтобы применить разные углы сдвига в разных точках слова, нужно разбить слово на интервалы и срезать каждую из них по отдельности. Чтобы определить, какие интервалы выбрать и под каким углом сдвигать каждый интервал, оптимизируется критерий, который оценивает последовательности интервалов и углов одновременно. Такой метод имеет большой потенциал, так как он может справиться с наклонно-вариативными словами. Результаты действительно многообещающие, хотя есть больше проблем с надежностью, поскольку алгоритм имеет большую свободу делать ошибки в слове.

Коррекция наклона. Чтобы сделать распознавание букв более эффективным, мы исправили угол наклона изображения. Для коррекции наклона мы сначала рассчитываем угол для максимальных линий относительно вертикальной линии, используя метод преобразования Хафа (Hough Lines) [7]. Преобразование Хафа - это глобальное преобразование, которое используется для отображения точек в пространственном пространстве (x, y) в параметрическое пространство в (ρ, θ) через параметрическое представление линии: $\rho = x \cos\theta + y \sin\theta$. Переменная ρ - расстояние от начала координат до линии по вектору, вертикальному линии. Кроме того, измеренный угол перекоса θ - это угол между осью и этим вектором, который задается при применении преобразования Хафа для коррекции перекоса документа. Таким образом, метод автоматически обнаруживает строки в документе.

После нахождения угла изображение поворачивается на тот же угол в противоположном направлении вокруг базовой линии текста. Результат исправление наклона представлен на Рис. 1.

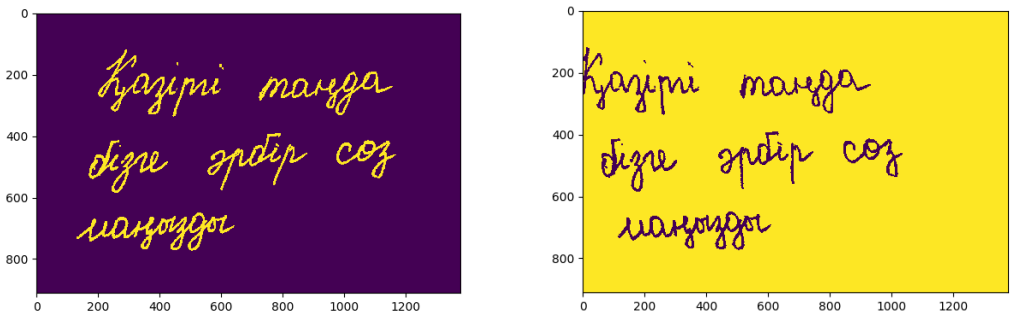


Рис. 1. Коррекция наклона текста

Сегментация строк. Учитывая, что строки текста расположены горизонтально, строки текста выделяются путем извлечения последовательных черных пикселей. Результат сегментации линии представлен ниже на Рис. 2.

Рис. 2. Сегментация строк

Сегментация слов. После выделения строк текста изображение расширяется, чтобы присоединиться к удаленному соседнему пикселю или удалить небольшое пространство между двумя буквами. После этого мы попытались использовать контурную трассировку для точного сегментирования пересекающихся компонентов. Затем на контуры накладывается ограничительная рамка для извлечения слов. Эти изображения слов затем отправляются на предварительную обработку. Результат сегментации слов представлен ниже на Рис. 3.

Рис. 3. Сегментация слов

Предварительная обработка. Первым шагом к анализу любого документа является предварительная обработка. Сначала образец изображения преобразуется в изображение в оттенках серого. Из этого изображения в градациях серого создается двоичное изображение, и один битовый двоичный шум удаляется с помощью эрозии. Все последующие шаги предназначены для нормализации данных по общей оси. При нормализации изображения различного размера изменяют размер изображения до фиксированного размера, сохраняя соотношение сторон без изменений.

Извлечение верхней контурной точки. Верхние точки контура извлекаются путем взятия первого черного пикселя каждого столбца сверху (Рис. 4).

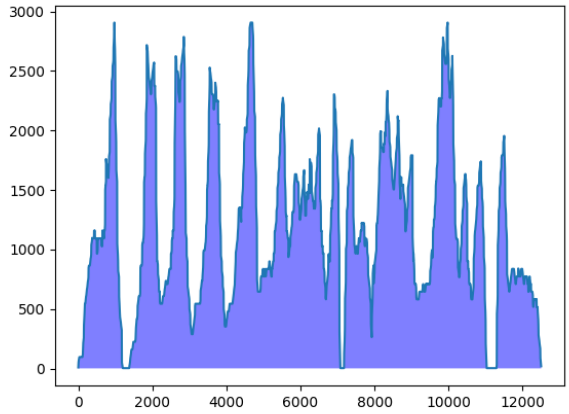


Рис. 4. Верхние точки контура

Сегментация символов. Мы предложили два подхода к сегментации символов:

1. Локальные максимумы и минимумы

- проходим через каждую верхнюю точку контура слева направо
- измеряется вертикальное расстояние каждой точки контура с ее следующей точкой контура
- если это расстояние больше определенного порогового значения, мы рассматриваем этот регион как «возможную» отрезок (Рис. 5)

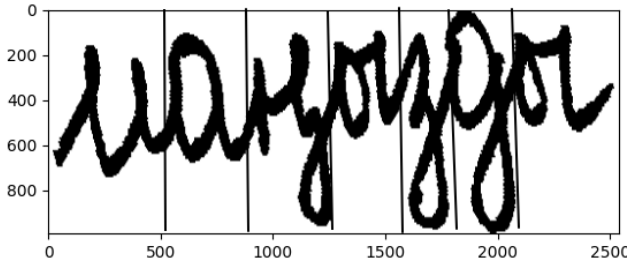


Рис. 5. Результат сегментации символов

2. Метод средней линии разреза

В этом методе извлекаются точки верхнего контура и точки нижнего контура. Затем вычисляется среднее значение, как для верхней, так и для нижней точки контура. Это среднее значение дает нам приблизительную верхнюю базовую линию и нижнюю базовую линию. Рассматривая эти две строки, находим среднюю линию и вырезаем слово из этой средней линии.

После вырезания изображения из средней линии пересекаем эту линию и находим полные пробелы. Эта область может рассматриваться как точка сегмента. Точки сегмента затем применяются к исходному слову для сегментации.

Обработка сегментации. В процессе сегментации из-за плохого качества изображений слова становятся более сегментированными. Мы попытались минимизировать проблему чрезмерной сегментации, установив некоторый порог. Если расстояние между двумя линиями сегмента меньше порогового значения, эта линия сегмента будет развернута и рассмотрит следующую линию сегмента. Порог

был установлен методом проб и ошибок изначально, его можно изменить на гораздо более конкретную формулу.

Выводы

В этой статье мы предложили простые методы для коррекции наклона и извлечения символов из изображения рукописного текста. Сначала мы преобразуем изображение в оттенках серого в двоичное изображение. После этого извлекаются текстовые строки, и корректируется базовая линия путем грубой и точной настройки. Этот метод может повернуть угол изображения от -45 до 45 градусов, а затем выбрать лучший угол. Углы, которые считают лучшими, это гистограмма с самым высоким пиком. Чрезмерная сегментация обычно происходит из-за геометрического искажения изображения. Это также появляется на некоторых букв перекрытия. В результате возникают ошибки при разделении. В будущем мы планируем включить в эту работу систему распознавания рукописного текста на казахском языке, которую включает такие операции, как сегментирование строк, слов и символов, распознавание символов и определение слов.

Литература

1. Bhowmik S., Malakar S., Sarkar R., Basu S., Kundu M., Nasipuri M., Off-line Bangla handwritten word recognition: a holistic approach // Neural Computing and Applications, 2018, 1–16 с.
2. Fitrianingsih, Sarifuddin Madenda, Suryarini Widodo, Rodiah, Slant Correction and Detection for Offline Cursive Handwriting using 2D Affine Transform // IJERT, vol. 5, no. 8, 2016.
3. Neeta Nain Subhash Panwar. Handwritten Text Recognition System Based on Neural Network // Journal of Computer and Information Technology, Vol 2, No.2. 2012
4. R.M. Bozinovic and S.N. Srihari, Off-line Cursive Script Word Recognition // IEEE Trans. PAMI, vol. 11, no. 1, pp. 68–83, 1989.
5. E. Kavallieratou, N. Fakotakis, and G. Kokkinakis. Slant estimation algorithm for OCR system // *Pattern Recognition*, vol. 34, no. 12, 2001, 2515–2522 с.
6. E. Taira, S. Uchida, and Hiroaki Sakoe, Nonuniform slant correction for handwritten word recognition // IEICE Transactions on Information & Systems, vol. E87-D, no. 5, 2004, 1247–1253.
7. Singh, Chandan and Bhatia, Nitin and Kaur, Amandeep, Hough transform based fast skew detection and accurate skew correction methods // Pattern Recognition, 41, 2008, 3528-3546 с.

ИНТЕЛЛЕКТУАЛЬНЫЕ РОБОТОТЕХНИЧЕСКИЕ СИСТЕМЫ С МУЛЬТИЯЗЫЧНЫМ РАСПОЗНАВАНИЕМ ГОЛОСОВОЙ РЕЧИ И ВЕРБАЛЬНЫМ КОМАНДНЫМ УПРАВЛЕНИЕМ

А.В.КИМ[1], Г.М.АЯЗБАЕВ[2]
akim.almaty@mail.ru
[1] *Институт информационных и вычислительных технологии (ИИВТ), г.Алматы, Республика Казахстан*
[2] *Казахский Национальный Университет им. аль-Фараби, г.Алматы, Республика Казахстан*

***Аннотация**: В данной статье рассматриваются основные подходы и методы вербального управления интеллектуальными роботами. Показана архитектура построения систем голосовых команд в комплексе вербального управления роботами. Приведены результаты разработки программно-аппаратного комплекса вербального робота. Результаты представлены на симуляторах роботов с применением программных пакетов трехмерного моделирования.*

***Ключевые слова**: робототехника, андроидные, гуманоидные, мобильные, коллаборативные роботы, программирование, симулятор, искусственный интеллект, искусственная нейронная сеть, интеллектуальные робототехнические системы.*

Современная робототехника далеко шагнула вперед. Роботы стали неотъемлемой частью нашей повседневной жизни. Сегодня они способны быть не только физическими, но и интеллектуальными помощниками человека. Все больше мест и профессий, где их присутствие и применение значительно улучшило многие производственные, технологические процессы, сделав их более технологичными и безопасными. Новым трендом для современных роботов является их использование в сферах: образования, медицины, развлечений, рекламной, торговой деятельности, в космической, в военных областях, а также при возникновении чрезвычайных ситуаций.

В повседневной жизни все чаще можно встретить антропоморфные (андроидные и гуманоидные) роботы, способные к интерактивному общению вербального и невербального характера с людьми. Многие из них обладают элементами искусственного интеллекта, способные понимать, отвечать на вопросы, говорить и даже вести светские разговоры. Однако, как правило, все они ориентированы главным образом на английский язык общения, в меньшей степени на японский, китайский, русский и др. языки.

В Казахстане также активно ведутся научные исследования в данном направлении. В ИИВТ МОН РК на сегодняшний день разработаны методика и программное обеспечение для интеллектуальных робототехнических систем (ИРС), способных распознавать, понимать, а также воспроизводить речь на казахском языке. Разработаны компьютерные модели и проводятся экспериментальные исследования по практическому применению вербального (голосового) командного управления различными типами ИРС: антропоморфными, манипуляционными и мобильными роботами [2-4].

Целью данного исследования является разработка универсального программно-аппаратного комплекса (АПК) для вербального командного управления ИРС на основе автоматического распознавания мультиязычной голосовой речи [4]:

1) для управления ИРС различных типов:
- антропоморфными (андроидными и гуманоидными) роботами;
- манипуляционными (промышленными и коллаборативными) роботами;
- мобильными (наземными колесными и гусеничными) роботами.

2) для вербального командного управления ИРС, с автоматическим распознаванием голосовых команд, произнесенных на одном из трех языков:
- английском;
- казахском;
- русском;

3) для выполнения управляемых движений ИРС от управляющих голосовых команд в вербальном режиме на одном из трех языков:
- английском;
- казахском;
- русском;

Распознавание голосовой речи человека – это достаточно сложная техническая задача, в которой звуковые (акустические) сигналы анализируются и структурируются в иерархию слов, фраз и предложений. Основными проблемами распознавания речи являются: акустическая и временная изменчивость, когда в разные моменты времени одни и те же речевые аудиофайлы имеют различные характеристики по амплитуде, частоте, тональности, длительности и др. [2,3].

Существуют основные методы распознавания речи [5]:
1. Скрытые Марковские модели;
2. Динамическая деформация времени;
3. Искусственные нейронные сети.

Методика расчета.

Диапазон человеческой речи составляет 20Гц - 20 КГц [3,4,5].

Исходный речевой сигнал представлен в дискретном виде как:

$$x[n], 0 \leq n < N$$

Применяем к нему преобразование Фурье:

$$X_a[k] = \sum_{n=0}^{N-1} x[n] e^{\frac{-2\pi i}{N} kn}, \qquad 0 \leq k < N$$

Вычисляем значения частоты в мел-шкале:

$$B^{-1}(b) = 700(\exp(b/1125)\text{-}1)$$

Вычисляем энергию сигнала:

$$S[m] = \ln(\sum_{k=0}^{N-1} |X_a[k]|^2 H_m[k]), \qquad 0 \le m < M$$

Применяем ДКП и получаем набор признаков сигнала, коэффициентов MFCC:

$$c[n] = \sum_{m=0}^{M-1} S[m]\cos(\pi n(m + 1/2)/M), \qquad 0 \le n < M$$

Результатом анализа сигнала является последовательность 10 мили секундных речевых кадров и содержащие информацию об этих участках, коэффициентов MFCC. Для улучшения качества распознавания, в кадры может быть добавлена информация о первой или второй производной значений их коэффициентов для описания динамики изменения речи [3,4,5].

Акустические единицы – Фонемы, Аллофоны, Дифоны, Трифоны [3].

Этапы акустической обработки:

- Сегментация,
- Выделение признаков,
- Моделирование акустических единиц,

Мел (от древнегреческого μελος — звук) — психофизическая единица высоты звука, количественная оценка звука по высоте основана на статистической обработке большого числа данных о субъективном восприятии высоты звуковых тонов. Результаты исследований показывают, что высота звука связана главным образом с частотой колебаний, но зависит также от уровня громкости звука и его тембра [2,3].

В распознавании речи используют комбинацию следующих моделей:

1. Акустическая модель, которая содержит информацию о звуковых параметрах (признаках) каждого сенона; бывают как контекстно-зависимые, так и контекстно-свободные. Обозначим набор признаков как *O*, тогда для слова *W* вероятность встретить набор *O – P(O|W)* [5,6].

2. Фонетический словарь, содержащий отображение из слов в фонемы. Можно заметить, что представление в виде словаря не является обязательным: это может быть некая функция, полученная в результате алгоритма машинного обучения. Обозначим произношение слова *W* как *Q(W)* [5,6].

3. Языковая модель, которая ограничивает слова для поиска. Она определяет, какое слово может следовать за данным и с какой вероятностью, таким образом, отсекая невозможные варианты. Наиболее часто используются n-граммные языковые модели. Обозначим вероятность встретить слово *W* как *P(W)* [5,6].

Если обозначить исходный аудиосигнал за X, а множество всех слов за W, то задача распознавания речи формализуется следующим образом [5,6].

$$W^* = \underset{W \in \mathrm{W}}{\operatorname{argmax}} P(W|X) = \underset{W \in \mathrm{W}}{\operatorname{argmax}} P\big(O\big|Q(W)\big)P(W)$$

В данной работе для определения эффективности систем распознавания речи используется метрика Word Error Rate(WER), основанная на подсчёте вставок, замен и удалений слов. [3]

$$WER = \frac{S + D + I}{N}$$

где

S – количество заменённых слов

D – количество удалённых слов

I – количество вставленных слов

То есть, чем выше WER, тем менее качественно произошло распознавание. Обычно выражается в процентах.

Существует несколько известных систем распознавания речи с открытым исходным кодом: CMUSphinx, HTK, Kaldi, Julius [3].

Эксперименты.

Данные для анализа были предоставлены лабораторией «Компьютерная инженерия интеллектуальных систем». Набор данных состоит из 1480 аудиозаписей из 20 колонок с 74–75 записями. Каждая аудиозапись состоит из фраз на казахском языке средней продолжительностью 6 секунд. Для идентификации говорящего, были собрали следующие данные: имя, пол, место рождения, год рождения [4].

Все аудио материалы имеют одинаковые характеристики:

- расширение файла: wav;
- метод цифрового преобразования: PCM;
- дискретная частота: 44,1 кГц;
- разрядность: 16 бит;
- количество аудиоканалов: один (моно).

Звук и запись одного динамика занимали в среднем 40–50 минут, включая время, необходимое для подготовки динамика, оборудования и удвоений, что соответствует 74–75 полученным файлам, общей продолжительностью 7–8 минут для каждого оратора [4].

Для проведения научного исследования и проверки работоспособности разработанных алгоритмов и программного обеспечения был использован программный симулятор трёхмерного моделирования Robo DK (Рис 2-4).

CMUSphinx реализован на языке C/C++ [1]. Интеллектуально вербальный комплекс был разработан на языке Python с модулем связи CMUSphinx и графическим симулятором выполнения команд PyOpenGL. Модел робота за основы трёхмерного моделирования были выбраны работы фирмы ABB. Графические результаты исследования показаны в рисунках 3-6.

В основе методики работы лежит техника среднего объединения акустических фонем для трех языков (казахского, русского, английского). Принципиально методика работы не отличаются между собой, что для английского, русского или казахского языков [2][3]. Целью исследования была проверка методики и качества

распознавания голосовой речи на трех языках. Полученные результаты WER показали колебание в диапазоне ~ 61-65 %, что довольно неплохой результат для первых работ по интеграции языков.

В системном модуле управления роботом реализованы блоки программ распознавания голосовых команд на: казахском, русском и английском языках.

Блок схема управления эксперимента показано в рисунке 1.

Ключевые командные слова в базе данных блоков управления показаны в Таблице 1.

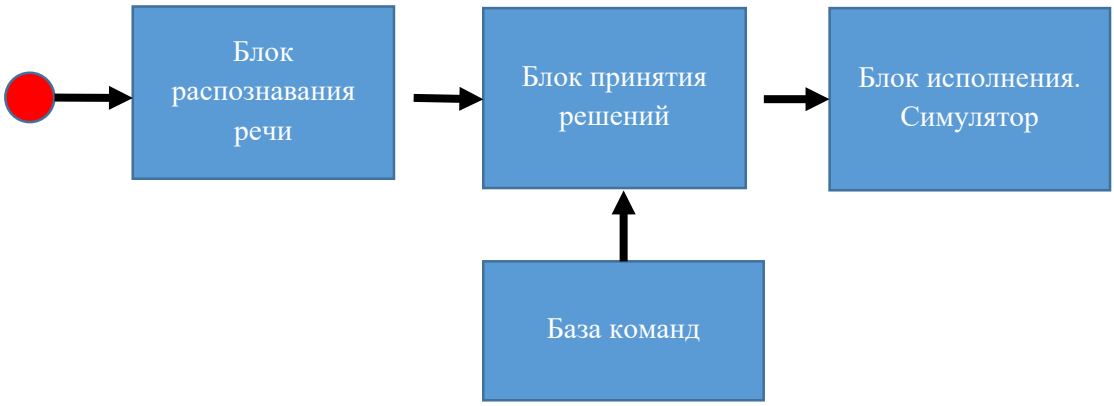


Рисунок 1. Блок схема управления эксперимента

Таблица 1. Основные команды управления роботом:

№	*Казахский*	*Русский*	*Английский*
1	**Алға**	вперед	go
2	**Артқа**	назад	back
3	**Оңға**	направо	right
4	**Солға**	налево	left
5	**Тоқта**	стоять	stop
6	**Көтеру**	поднять	catch up
7	**Төмендету**	опустить	let go
8	**Алу**	схватить	catch
9	**Қою**	положить	put down

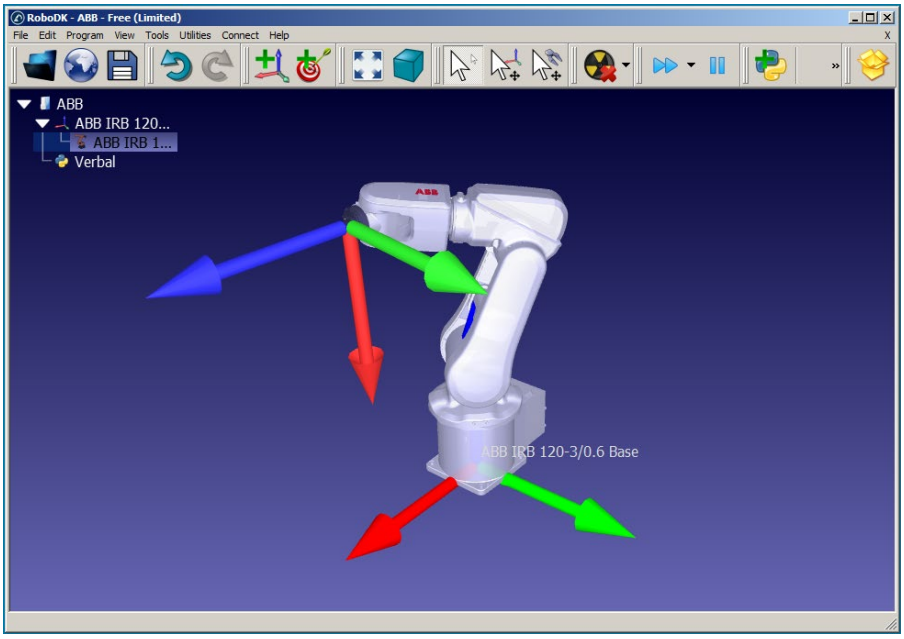


Рисунок 2. Симулятор коллаборативного робота для команд: «**налево», «направо»**

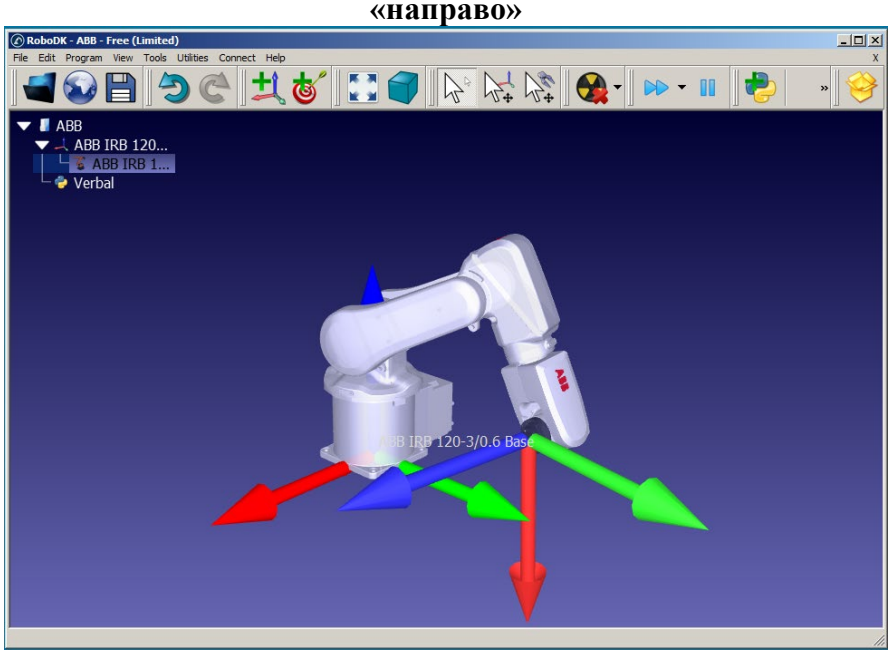


Рисунок 3. Симулятор коллаборативного робота для команд: **«опустить», «захватить»**

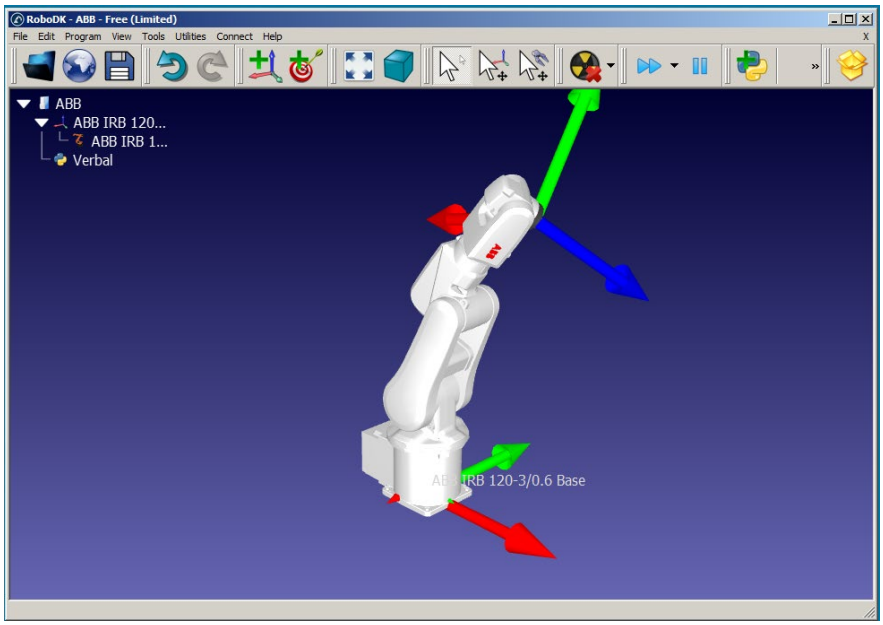


Рисунок 4. Симулятор коллаборативного робота для команд: **«поднять», «положить»**

Заключение.

В данной статье приведены результаты проведенных исследований в институте информационных и вычислительных технологий (ИИВТ) МОН РК (г. Алматы) по разработке программно-аппаратного комплекса для построения движений вербальных антропоморфных роботов. На базе трехмерных симуляторов, разработанных для исследования андроидных, манипуляционных и мобильных типов роботов, представлены результаты компьютерного моделирования голосового командного управления на казахском, русском и английском языках.

Кроме того, в будущем планируется провести дальнейшие исследования в этом направлении, для технической реализации данного универсального программно-технического комплекса для вербального командного управления различными типами роботов: манипуляционными, мобильными, антропоморфными.

Особенно актуальным и интересным для многих разработчиков и специалистов в области робототехники, роботизации в последнее время является режим коллаборативного (группового) управления бизнес-процессами в различных сферах услуг и интеграции технологических производств в технологические коллаборации.

Литература

1. CMU Sphinx Project by Carnegie Mellon University. http://cmusphinx.sourceforge.net/

2. Orken Mamyrbayev, Mussa Turdalyuly, Nurbapa Mekebayev, Keylan Alimhan, Aizat Kydyrbekova, Tolganay Turdalykyzy. Automatic Recognition of Kazakh Speech Using Deep Neural Networks // Asian Conference on Intelligent Information and Database Systems, 2019

3. Orken Mamyrbayev, Mussa Turdalyuly, Nurbapa Mekebayev, Kuralay Mukhsina, Alimukhan Keylan, Bagher BabaAli, Gulnaz Nabieva, Aigerim Duisenbayeva, Bekturgan Akhmetov. Continuous Speech Recognition of Kazakh Language // ITM Web of Conferences №24, 2019

4. Ayazbaev G.M., Kim A.V., Kunelbayev M. Development of software and hardware systems verbal intelligent robot. International Journal of Mechanical and Production Engineering Research and Development (IJMPERD) ISSN(P): 2249–6890; ISSN(E): 2249– 8001 Vol. 10, Issue 3, Jun 2020, 1839–1850 © TJPRC Pvt. Ltd.
5. Xuedong Huang, Alex Acero, Hsiao-Wuen Hon, Spoken Language Processing: A Guide to Theory, Algorithm, and System Development, Prentice Hall, 2001
6. Mikhailov Dmitrii. Analysis of CMUSphinx system performance // Saint-Petersburg 2016
7. Simulate Robot Applications https://robodk.com/

ВНЕДРЕНИЕ ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМ НА ТРАНСПОРТЕ

Утепбергенов И.Т., Ахмедиярова А.Т., Касымова Д.Т.
e-mail: aat.78@mail.ru
Институт информационных и вычислительных технологий КН МОН РК, Казахстан

Аннотация. *Статья посвящена вопросам повышения транспортной доступности крупных городов. Внедрение интеллектуальных транспортных систем позволит снизить уровень загруженности автомобильных дорог и увеличить их пропускную способность, оптимизировать использование автомобильного транспорта и повысить доступность услуг транспортного комплекса в целом. В городских условиях для получения возможности интеллектуального управления дорожным движением необходимо иметь полную информацию о распределении транспортных потоков, особенно на пересечениях, оборудованных техническими средствами управления дорожным движением. Для получения необходимых сведений может быть использованы видеокамеры, позволяющие производить замеры поведения транспортных потоков при минимальном использовании человеческих ресурсов и небольших материальных вложениях.*

Ключевые слова: *интеллектуальная транспортная система, автомобильный транспорт, умный город, безопасность движения, видеокамеры, «Сергек».*

Умный город является и, безусловно, будет одной из самых важных задач в ближайшие несколько десятилетий. Предполагается, что с настоящего времени до 2050 года более шести миллиардов человек будут жить в городской среде, то есть почти 75% населения Земли. Массовая концентрация людей в городах создает много возможностей, но также несет с собой свою долю проблем городского управления: загрязнение окружающей среды, безопасность, прожиточный минимум, мобильность и т.д.

Сегодня городским жителям нужен качественный общественный транспорт, чтобы этот транспорт минимально влиял на экологию и бюджет. В Алматы 80% выбросов в воздух происходит от автомобильных пробок. Ежедневно в городе

передвигаются порядка 700 тыс. автомобилей со средней скоростью в час пик 19 км в час. Согласно экспертным оценкам, ежедневные потери экономики Алматы от пробок составляет более 600 млн тенге.

Мировая практика для решения данной проблемы в последние десятилетия направляет усилия на создание проектов умного города. «Умным» город делают не только инфраструктурные, но и аналитические проекты. Более того – таким город становится в результате создания проектов, востребованность которых появляется как раз в результате исследования огромных массивов с виду разрозненных данных. Иными словами, именно большие данные являются драйвером всех мегапроектов в транспорте – будь это внедрение беспилотных автомобилей или глобальная аналитика дорожного движения.

При рассмотрении показателей дорожного движения следует выделить те из них, которые являются первичными. К ним следует отнести показатели, определяемые потребностями в перевозках пассажиров и грузов, а также в пешеходных сообщениях. К основным характеристикам транспортного потока относятся: *интенсивность движения; состав транспортного потока; плотность потока транспортных средств; скорость движения; продолжительность задержек движения.* Ряд факторов влияет на время поездки и ее изменчивость. Периодическая перегрузка вызвана ежедневными задержками в пиковые часы, которые возникают, когда спрос превышает пропускную способность шоссе, в то время как единовременные из-за нетипичных причин, таких как инциденты, отключенные транспортные средства, рабочие и строительные зоны, неблагоприятные погодные явления и специальные события. В такой ситуации водители точно не знают, когда они прибудут в пункт назначения.

В Казахстане активно идет процесс создания интеллектуальных транспортных систем, использующих инновационные разработки в моделировании транспортных систем и автоматизированном регулировании транспортных потоков, предоставляющая конечным потребителям большую информативность и безопасность, а также качественно повышающая уровень взаимодействия участников движения по сравнению с обычными транспортными системами. В интеллектуальных транспортных системах могут применяться технологии предсказывания на основе моделирования и накопленной ранее информации. Основные цели создания интеллектуальных транспортных систем представлены на рисунке 1.

Рис.1 Цели создания интеллектуальных транспортных систем

Видеокамеры - одни из самых простых, привычных и действенных средств, используемых в мониторинге. Преимущество видеокамер перед другими системами слежения в том, что есть возможность непосредственно увидеть всё, что находится в обзоре камеры. Современное специализированное программное обеспечение обработки изображений от видеокамер позволяет измерять параметры движущегося потока (например, скорость движения автомобилей, плотность потока движения), определять государственные регистрационные знаки автомобилей, выявлять нарушения правил дорожного движения. В дальнейшем эта информация может быть использована также в самых различных целях.

Развитие облачных сервисов хранения данных дает возможность организовать видеонаблюдение за любым объектом через интернет. Основной плюс облачного сервиса — возможность хранить информацию с камер на удаленном сервере и просматривать ее с любого компьютера или мобильного устройства. Разработано немало программ для видеонаблюдения. Они позволяют просматривать видео в режиме реального времени или обращаться к архивам записей, а также скачивать их фрагменты. Для монтажа бытовой системы видеонаблюдения достаточно приобрести простой комплект оборудования — IP-камеры, плату видеозахвата, встраиваемую в компьютер, или видеорегистратор. Чтобы организовать видеонаблюдение онлайн, нужно выбрать провайдера подобных услуг и подключить камеры к плате или видеорегистратору. Как правило, услуги провайдера предоставляют те же компании, что и продают «коробочное» оборудование для видеонаблюдения через интернет.

Все аппаратно-программное обеспечение для систем видеонаблюдения условно можно разделить на две группы — это пакетные облачные решения бюджетного класса, которые обычно востребованы только в частных домовладениях и малых офисах, и профессиональные многофункциональные решения для среднего и крупного бизнеса. Первые, как правило, включают оборудование и ПО, совместимое только с устройствами определенного бренда, они плохо масштабируются или не расширяются вовсе, не имеют систем самодиагностики, не

способны интегрироваться в другие системы безопасности. Вторые предоставляют пользователю широкий функционал, отвечают высоким стандартам безопасности, надежности, гибкости в настройках и стабильности в работе. Применение последних практически исключает программные и аппаратные сбои — компьютерная самодиагностика в случае их обнаружения автоматически дает сигнал на включение резервного оборудования и каналов связи.

Профессиональное ПО для видеонаблюдения поставляется в линейках Standard и Advance. Стандартный вариант обычно уже интегрирован в микросхемы видеокамер и центральные панели управления производителем; расширенный приобретается за отдельную плату и может работать с оборудованием любых брендов.

С развитием цифровой техники и удешевлением видеокамер появилась возможность организовывать видеонаблюдение (с последующим развитием ИТС) в городах с применением минимального количества камер при условии наиболее полного наблюдения за городской транспортной сетью.

Для построения адекватной модели требуется некоторая начальная информация о проблемных участках в городе, скоростные ограничения, средняя загруженность отдельных участков в зависимости от времени суток, времени года. Кроме этого, требуется карта города и знание расстояния от одной точки до другой.

На первом шаге территория города визуально делится на районы области с густой дорожной сетью, соединённые с другими районами магистральными дорогами. Размещение камер в одном районе не будет зависеть от размещения в другом. Таким образом, задача несколько упрощается, делится на несколько подзадач меньшей размерности. По тому же принципу можно произвести разбиение района на микрорайоны. Следующим шагом является определение дорог в районе, на которых сосредоточена основная масса транспортного потока, а также аварийных участков. Из наблюдения следует исключить дороги, которые не дают существенного вклада в поток. К ним относятся дороги с малой загрузкой, на которых возникновение аварийных ситуаций не меняет характера движения, внутренние дороги жилых зон. Не следует исключать участки, непосредственно примыкающие к магистралям. Далее на полученной территории определяется места возможного расположения камер. Удобно располагать их так, чтобы в круге обзора находилось как можно больше участков, которые требуется прослеживать. Такими точками служат прежде всего перекрёстки, повороты, крыши или углы зданий, высотные сооружения. После того, как основные точки размещения определены, нужно разделить всю требуемую территорию на множества участков, просматриваемых каждой камерой, и при необходимости добавить или убрать камеры.

Частичное прослеживание характерна для длинных промежутков между перекрёстками камеры покрывают участок частично. Если требуется прослеживать участок по всей длине, то нужно добавить точки размещения камер в зависимости от длины участка. Самым простым вариантом в таком случае является размещение через расстояние, как показано на рисунке 2, равное двум радиусам обзора камеры (или одному радиусу, если камера не может совершать круговое вращение).

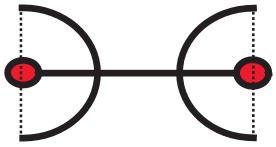


Рис.2 Частичное прослеживание

Если данный участок не является аварийным или не требует прослеживания по всей длине, то двух камер будет достаточно, так как о возникшей аварийной ситуации внутри промежутка можно судить по второстепенным признакам (например, сравнивая плотность потока на концах промежутка).

На длинных неаварийных участках магистралей, к которым примыкают только второстепенные дороги, также не требуется полное прослеживание и камеры удобно размещать либо на поворотах, либо через определённое расстояние, которое может быть много больше, чем радиус обзора камеры.

Частичное перекрытие. Один и тот же участок может в разной степени прослеживаться двумя и более камерами. При незначительном перекрытии (незначительность перекрытия может определяться, например, в процентном соотношении или в единицах длины и её конкретное значение зависит от рассматриваемого участка) можно разделить покрываемый участок на нужное количество подучастков и указать для каждой камеры наблюдаемые ей территории. Если перекрытие существенное, то можно считать, что обе камеры прослеживают участок целиком. Примеры таких ситуаций показаны на рисунке 3.

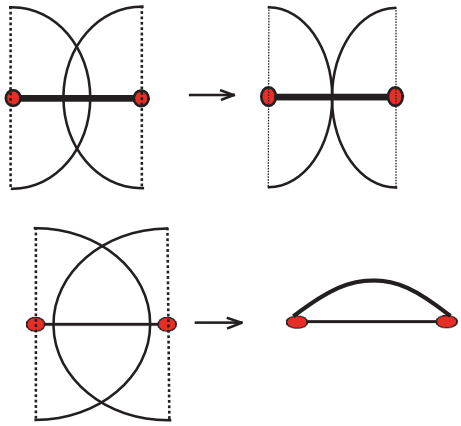


Рис. 3 Незначительное и существенное перекрытия

Для закруглённых участков дороги применяется либо осцилляция, либо есть точка внутри закругления, с которой беспрепятственно прослеживается весь поворот (рисунок 4).

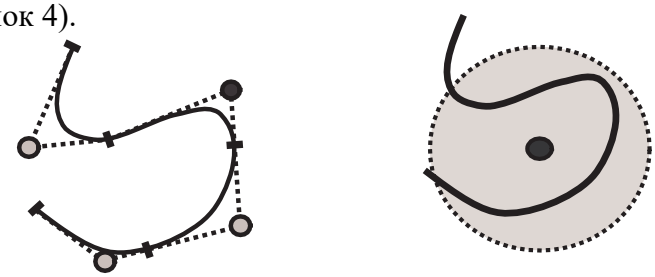


Рис. 4 Закругления

Также из всего множества возможных точек размещения нужно выделить те, в

которых камеры должны находиться обязательно. Такие точки могут находиться, например, на мостах, в тоннелях, на особо аварийных участках. После проделанного анализа задача формализуется следующим образом.

Пусть $I = \{1,...m\}$ - множество всех возможных мест размещения камер;

$J = \{1,...n\}$ - множество всех наблюдаемых участков;

$$a_{ij} = \begin{cases} 1, & \text{если камера i контролирует участок j} \\ 0, & \text{в противном случае} \end{cases}$$

Переменные задачи:

$$x_i = \begin{cases} 1, & \text{если на участке i устанавливается камера} \\ 0, & \text{в противном случае} \end{cases}$$

Тогда математическая модель решаемой задачи принимает вид

$$\min \sum_{i \in I} x_i$$

при ограничениях: $\sum_{i \in I} a_{ij} x_i \geq 1$, $j \in J$;

$x_i \in \{0,1\}$, $i \in I$

Данная задача известна в целочисленном программировании как задача о минимальном покрытии (ЗМП).

Результаты работы полученного комплекса мероприятий и программы, реализующие для данной задачи приближённый и адаптированный точный алгоритмы приведены в исследованиях авторов [*PrzeglądElektrotechniczny*].

Всего единую систему в Астане (Нур-Султан) объединяют 13 тысяч камер фото и видеофиксации. 124 (258 камер) автоматических систем фото-видеофиксации нарушений контролируют общественный порядок на 400 участках дорог и перекрестках. Из них 62 стационарных скоростомеров «Red Speed» и 21 аппаратно-программных комплексов «Vocord» фиксирующие скоростной режим, 12 систем Контроля дорожного движения «Интегра» (117 камер). Все они следят за тем, чтобы водители соблюдали ПДД. Не остаются без внимания и такие правонарушения как пересечение стоп-линии и проезд на запрещающий сигнал светофора. Аналогичные работы ведутся и в городе Алматы.

«Сергек» – это интеллектуальная система видеоконтроля, анализа и прогнозирования, включающая:

— сеть модулей видеофиксации, контролирующих ключевые зоны городского пространства – автотрассы, площади, транспортные развязки, придомовые территории и т. д.;

— систему записи и распознавания изображений;

— интеллектуальную систему обработки и анализа информации.

Стандартный модуль видеофиксации «Сергек» представляет собой камеру, устанавливаемую на опорах уличного освещения, коммутационный блок, источник бесперебойного питания и модуль беспроводной связи. Камера может оснащаться высокоэффективным допплеровским радаром собственной разработки, а также набором разнообразных датчиков (рис.5).

Рис.5 - Состав оборудования стандартный модуля видеофиксации «Сергек»

Особенности модуля видеофиксации «Сергек»:

Модуль видеофиксации в режиме реального времени фиксирует и распознает номера попадающих в зону обзора автомобилей, а также параметров их движения и экологические показатели.

Экологические датчики позволяют производить постоянный онлайн мониторинг состояния окружающей среды, в том числе:

- концентрацию CO_2;
- уровень шума;
- атмосферное давление;
- влажность;
- температуру.

Информация с видеокамер и датчиков по беспроводному каналу передается на серверы для последующей обработки.

Сергек располагает вычислительными мощностями и специальным программным обеспечением, позволяющими в режиме реального времени обрабатывать значительные объемы информации.

Функционал системы Сергек, в частности, включает:

- фиксацию и прогнозирование автомобильного потока;
- выявление и отслеживание перемещения автомобилей с заданными параметрами движения, в том числе нарушителей правил дорожного движения (скорость, разметка);
- оперативное информирование о важных событиях;
- сохранение и протоколирование объективной информации о важных событиях;
- трансляцию в режиме реального времени изображения с камер на мобильные устройства;
- сбор и анализ информации о параметрах автомобильных потоков и движении отдельных автомобилей.

Система «Сергек» позволяет подсчитать количество автомобилей, проезжающих по участку в единицу времени. Это даёт очень хорошую статистику

по загруженности дорог и может служить источником информации для системы интеллектуальных светофоров.

Актуальными проблемами контроля городского пространства с использованием больших данных являются:

— загруженность городских магистралей, необходимость оптимизировать транспортные потоки;

— необходимость оптимизировать использование автотранспорта городских служб;

— необходимость оптимизировать движение городского пассажирского транспорта;

— необходимость визуального контроля ключевых зон (места проведения массовых мероприятий, транспортные развязки, площади, торговые центры, придомовые территории, т.д.);

— необходимость оперативного реагирования на непредвиденные и чрезвычайные ситуации.

Более подробное ознакомление с технической документацией и функционированием системы «Сергек» показало, что на настоящее время при эксплуатации системы не решены до конца некоторые задачи, связанные с формированием и обработкой больших данных:

1) накопленная большая база данных, формируемая на протяжении 3-4 лет, требует обработки для выявления противоречий и избыточности данных;

2) система не сконфигурирована для работы с большими данными в реальном времени, чтобы предоставить операторам изменения времени движения в рамках текущего инцидента.

Более распространенным источником противоречий являются объединенные данные из нескольких источников, таких как обмен данными, объединение данных и хранилище данных.

Выводы.

В интеллектуальных транспортных системах применяются технологии предсказывания на основе моделирования и накопленной ранее информации. Преимущество видеокамер перед другими системами слежения в том, что есть возможность непосредственно увидеть всё, что находится в обзоре камеры. Развитие облачных сервисов хранения данных дает возможность организовать видеонаблюдение за любым объектом через интернет. С развитием цифровой техники и удешевлением видеокамер появилась возможность организовывать видеонаблюдение в городах с применением минимального количества камер при условии наиболее полного наблюдения за городской транспортной сетью.

Оптимизация и эффективный контроль работы городского транспорта и своевременное реагирование на непредвиденные ситуации означает снижение бюджетных расходов, а также повышение безопасности и комфорта городской жизни. Но, настоящее время при эксплуатации системы Сергек не решены до конца некоторые задачи, связанные с формированием и обработкой больших данных.

Литература

1. ООН: население Земли к 2050 году превысит 9,8 млрд человек. [Электронный ресурс]: https://tass.ru/obschestvo/4357817

2. Алматы ежедневно теряет более 600 млн. тенге из-за пробок. [Электронный ресурс]: https://kapital.kz/economic/67073/almaty-ezhednevno-teryaet-bolee-600-mln-tenge-iz-za-probok.html

3. Современные программы для организации видеонаблюдения онлайн. [Электронный ресурс]: https://www.kp.ru/guide/videonabljudenie-onlain.html

4. Ахмедиярова А.Т., Утепбергенов И.Т. Касымова Д.Т. Метод анализа транспортной сети для выявления узких мест // Интеллектуальные технологии на транспорте. – 2016. - №3. - С.9-14.

5. Семенов В.В. Математическое моделирование динамики транспортных потоков мегаполиса. – М., 2004. - 44 с.

6. Waldemar Wójcik, Akhmediyarova A.T., Mamyrbayev O., Kassymova D.T., Utepbergenov I.T. Development and research of the algorithm for determining the maximum flow at distribution in the network // PrzeglądElektrotechniczny. – 2017. – Vol.93, Issue 6. – P.137-140

7. Сергек. [Электронный ресурс]: http://sergek.kz/city-authorities

БИОМЕТРИЯЛЫҚ ТЕХНОЛОГИЯЛАРДЫ ҚОЛДАНАТЫН ДАУЫСТЫ ТАНУ ҚАУІПСІЗДІК ЖҮЙЕСІН ҚҰРУ

[1,2]Мамырбаев Ө.Ж., [1,2]Кыдырбекова А.С., [3]Осман М., [2]Жумажанов Б.Ж.
(e-mail: kas.aizat@mail.ru)
[3](e-mail: morkenj@mail.ru)
[1]әл-Фараби атындағы Қазақ ұлттық университеті, 050040 Алматы, Қазақстан
[2]Ақпараттық және есептеуіш технологиялар институты, 050010 Алматы,
[3]Коммуникациялық технологиялары және желілері бөлімі, Малайзия, Путра университі, 43400 UPM Serdang, Selangor D.E.

Аннотация. *Биометриялық технологиялар адамдарды тану үшін физикалық ерекшеліктері мен жеке қасиеттерін пайдалану арқылы алаяқтық пен ұрлықты азайту үшін қорғаныс ретінде тез танымал болып келеді. Биометриялық сәйкестендірудің алғашқы әдістері саусақ іздері мен қолжазбаны қамтыса, қазіргі заманғы әдістеріне көз қарашығын сканерлеу, бетті сканерлеу, дауыстық тану және қол іздері жатады. Биометриялық дауысты тану және идентификациялау технологиясы жүйені адамның дауысының ерекше сипаттамаларын тануға үйретуге бағытталған (яғни дауыстық басып шығару). Бұл технология әртүрлі қолдану мен қосымшаларға, соның ішінде ұялы телефондарға қауіпсіз қол жетімділікті басқаруға ыңғайлы (алаяқтықтың алдын алу үшін), банкомат өндірушілері (PIN-алаяқтықты жою үшін) және автомобиль өндірушілер (ұрлық пен көлік ұрлауды айтарлықтай азайту үшін). Бұл мақалада кіруді басқару(управления доступом) кілті ретінде дауыстық идентификацияға негізделген қауіпсіздік жүйесінің орындалуын ұсынамыз. Тексеру алгоритмі MATLAB функционалдық блоктарының көмегімен жасалады, олар адамның жеке басын оның дауысы бойынша растауға қабілетті. Дауыстық сәйкестік логикалық*

«1» -ге, ал сәйкессіздік «0» -ге әкеледі. Есікке кіруді бақылаудың микроконтроллер схемасы осы дауыстық белсенді жүйенің сенімділігін тексеруге арналған.

1. Кіріспе

Біз бір-бірімізбен сөйлесу үшін дауыстарымызды үнемі қолданамыз. Қарым-қатынас - бұл біздің күнделікті өміріміздің ажырамас бөлігі, сондықтан біз бір-бірімізбен сөйлесудің әртүрлі тәсілдерін қолданамыз. Алайда, адамның дауысынан маңызды ештеңе жоқ. Сөйлеу және тыңдау барлық басқа қарым-қатынастардың негізі болып табылады. Сізге сөйлеу және тыңдау үшін электронды құрылғы қажет емес; сізге қағаз бен қаламның да қажеті жоқ. Сізге тек сіздің дауысыңыз қажет. Басқа байланыс құралдарымен салыстырғанда ең қарапайым және жеңіл түрі. Қарым-қатынас пен әңгімелесу құралы болып табылатын дауыс - адам биометриясының бір түрі. Әр адамның дауысы тек сол дауысқа ғана тән ерекше сипаттамаларға ие болғандықтан, бұл дауысты биометриялық идентификация үшін қолдануға болады. Әңгімелесу - ақпаратты жеткізудің ең оңай және қарапайым тәсілі. Бұл сондай-ақ сәйкестендірудің қарапайым құралдарының бірі болуы мүмкін. Компьютерлік технологияның соңғы жетістіктері дауысты тануды - адам дауысының ерекше сипаттамаларына негізделген биометриялық технологияны бұрынғыдан да ыңғайлы, қауіпсіз және қауіпсіз етті. Бұл мақалада біз дауысты тану технологиясының қазіргі жағдайына көз жүгіртеміз және қазіргі жасанды интеллект технологиясының өзегі - биометрияның күшін ашудың кілті қаншалықты терең болатындығын көрсетеміз [1]. Сондай-ақ, біз терең нейрондық желілердің (DNN) технологиясын қол жетімді және сенімді ету бойынша жаһандық күш-жігердің басында тұрған дауысты тану технологиясы бойынша жұмысын мұқият қарастырамыз. Соңында, біз дауысты тану технологиясына арналған қоғамдық қауіпсіздік шешімдері сияқты әлеуетті өндірістік қосымшаларды талқылаймыз. Дауысты танудың дамыған бағдарламалық жасақтамасы есікті ашу механизмін сәтті іске қосқан, тек авторизацияланған адамға жұмыс істейтін дауыстық команда. Жүйе қауіпсіздіктің қол жетімділігін орташа деңгейде қамтамасыз ете алатындығы дәлелденген және дауысты анықтаған сайын дауыстың өзгеруіне сәйкес келетін конфигурацияланатын қауіпсіздік деңгейі бар.

Дауысты тану пайдаланушыларды жеке идентификациялаудың қарапайым және оңай әдісін ұсынады. Оның үстіне, аутентификацияның бұл түрі арнайы жабдықты қажет етпейді; кәдімгі микрофондар мен телефондарды қолдануға болады және қымбат арнайы сенсорлық құрылғы да қажет емес. Дауысты тану жүйесін орнату қарапайым және салыстырмалы түрде арзан.

Дауысты тану технологиясы дегеніміз не, ол қалай жұмыс істейді және оның жасанды интеллекттің негізгі заманауи технологияларының бірі болып табылатын терең білімге қатысы бар ма? Осы мақалада біз жауап беруге тырысатын бірнеше сұрақтар бар. Біз сондай-ақ DNN –нің осы саладағы жұмысын және әлемдік деңгейдегі дауысты тану технологиясын және қоғамдық қауіпсіздік шешімдері сияқты дауысты тану технологиясының әлеуетті өндірістік қосымшаларын қарастырамыз [2].

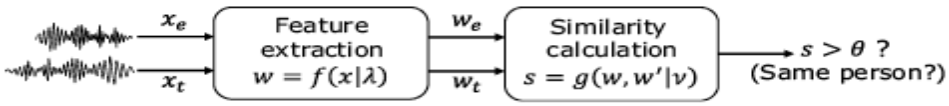
2. Дауысты тану технологиясы

Барлығымыз сөйлеушіні көрмесек те, кімнің дауысын тыңдайтынымызды болжауға дағдыланғанбыз. Егер сіз адамды танитын болсаңыз, онда сіз дұрыс болжай аласыз. Әр адамның дауысының ерекше сипаттамалары әр түрлі физикалық ерекшеліктерімен анықталады, мысалы, дауыс сымдары мен ауыз қуысының пішіні

(физикалық ерекшеліктер), сонымен қатар әрқайсымызға тән сөйлеу әдеттері (мінез-құлық ерекшеліктері). Дауысты тану технологиясы дауыс иесін жеке физикалық және мінез-құлық сипаттамаларына байланысты ерекшеліктерді оқшаулау және талдау функциялары арқылы идентификациялайды.

2.1 Дауысты танудың технологиялық компоненттері

Техникалық тұрғыдан дауысты тану дауыс иесін тану немесе дауыс иесін тексеру деп аталады. Көп жағдайда бұл екі дауысты салыстырып, олардың бір адам екенін анықтау үшін жеке-жеке өңдеуді қолданатын технологияға қатысты. Дауысты идентификациялау бұл белгісіз адамды дауыспен анықтауға тырысу, яғни «бірдің –көпке» өңдеуді жүзеге асыруы. Бірақ бұл, сайып келгенде, бір-бірін салыстырудың бірнеше рет қайталануына байланысты орындалады. Сонымен, өңдеудің негізгі бірлігі суретте көрсетілгендей жеке өңдеу болып табылады. 1.сурет



Сурет: 1 Дауысты тану жүйесінің негізгі конфигурациясы (бір-біріне салыстыру): ерекшеліктерді шығаруға және ұқсастықты есептеуге арналған модельдер (λ, ν) жаттығу кезінде мәліметтермен анықталады.

Қазіргі кезде объектілерді шығаруға арналған ең танымал құрылым - бұл i-вектор деп аталатын фрейм

1). Көптеген динамикалық дауыстардан (әр түрлі дауысты және дауыссыз) тұратын фонеманың стандартты моделін қолданып, i-векторы функция ретінде стандартты модель мен кіріс дауыстың айырмашылықтарын бөліп көрсетеді. Алайда, егер барлық айырмашылықтар алынып тасталса, онда функция үлкен болар еді, мүмкін жүздеген мың өлшемдер. Бұл проблеманы болдырмау үшін, i-вектор факторлық талдаудың көмегімен 400-ге жуық өлшемге дейін осындай үлкен функцияны қысады. Ұқсастықты есептеу үшін ықтимал сызықтық дискриминантты талдау (PLDA) [3].

2) PLDA сызықтық дискриминантты анализді (LDA) пайдаланып, теңдеулерді стохистикалық түрде қайта құрып, дәстүрлі машиналық оқыту әдісін қолданады және 400-өлшемді i-векторлық функция негізінде динамикті анықтау үшін ең қолайлы функцияны автоматты түрде таңдайды. Деректерді талдағаннан кейін ұқсастық ықтималдылық коэффициенті ретінде есептеледі.

i-вектор да, PLDA да Гаусс үлестіріміне (қалыпты үлестірім) негізделген ықтимал модельдер көмегімен тұжырымдалған. Дауысты тану, i-вектор және PLDA үшін де-факто стандарттарға әртүрлі машиналық оқыту әдістері кіреді. Автоматты түрде оқуға қабілетті, олар үлкен көлемдегі мәліметтерден оңтайлы модель параметрлерін жасай алады[4].

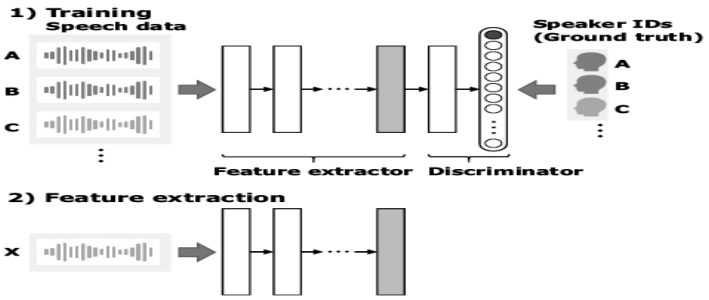
2.2 Дауысты тануда терең оқытуды пайдалану

Соңғы зерттеулерде сурет пен сөйлеуді тану саласындағы зерттеушілер терең оқытуды қолдану арқылы дәлдікті жақсартуға тырысуда. Дауысты тану осы тенденциядан тыс емес; терең оқытуға арналған зерттеулер 2014 жылдан басталды

және қазіргі уақытта осы саладағы парадигмалық өзгерісті бастан кешіруде, бұл дауысты тануды негізгі ағымға жеткізуге уәде береді [5].

Бұл ауысым дауысты танудың дәлдігін экспоненциалды түрде арттыратын динамикті терең ендіру немесе x-vector деп аталатын жүйенің пайда болуымен ерекшеленеді. Бұл саланың зерттеушілері x-vector-ді дәстүрлі i-vector [6]

3) 2-суретте x-векторлық жүйе түсінігі көрсетілген. Біріншіден, ерекшелік экстрактордан және дискриминатордан тұратын терең жүйке жүйесі (DNN) сөйлеушілерді дауыстарынан дұрыс шығаруға үйретілген. DNN Feature Extractor тек қана сөйлеушілерді олардың дауыстарынан анықтауға жарамды ақпаратты шығаратын етіп жасалған.



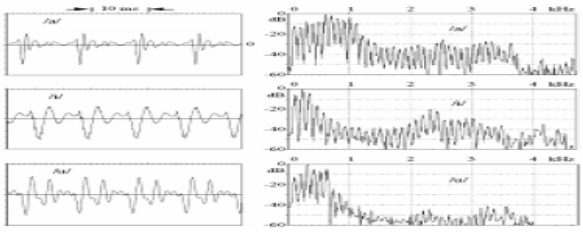
Сурет: 2 Терең оқытуға негізделген ерекшеліктерді бөлу тұжырымдамасы (x-вектор).

Сөйлеу өзгермелі ұзындықтағы уақыт қатарының деректері болғандықтан, нейрондық желіге енгізілген мәліметтер де өзгермелі болады. Бұл факт кескінге қарағанда дауысты өңдеуді қиындатады. Алайда, x-векторының көмегімен объектіні шығарғыштың соңында уақытша бағытта деректерді жинақтайтын бассейн қабатын енгізу арқылы белгіленген өлшемдері бар объект туралы қорытынды жасауға болады [7].

Дауысты тану үшін терең оқытуды жүзеге асыруға арналған сынақтар тек қана ерекшеліктер шығарумен шектелмейді және алдыңғы жағынан (сөйлеуді/сөйлеуді емес тану және шулы ортадағы сөйлеуді жақсарту) екінші деңгейге дейін (ұқсастықты есептеу). Сондай-ақ, барлық техникалық компоненттерді нейрондық желіге алмастыратын бүкіл жүйені оқытатын ұштық жүйе пайда болды. Бұл үрдіс болашақта жалғасуы мүмкін.

2.3 Дауысты тану жүйесін проектілеу

Сөйлеуді өңдеу және тілдік технологиялар көптеген арнайы ұғымдар мен терминологияларды қамтиды. Әр түрлі сөйлеу синтезі мен талдау әдістері қалай жұмыс істейтінін түсіну үшін біз сөйлеу өндірісі, артикуляциялық фонетика және басқа да кейбір терминологияны білуіміз керек. Үш дыбыстың сөйлеу сигналдары (/a/ /i/ /u/) 3-суреттегі уақыт пен жиілік аймағында көрсетілген. Негізгі жиілік барлық жағдайда 100 Гц құрайды, ал f_1, f_2 және f_3 /a/ дауысты формант жиіліктері шамамен 600 құрайды. Тиісінше Гц, 1000 Гц және 2500 Гц. Дауысты дыбыстар үшін /i/ алғашқы үш формант 200 Гц, 2300 Гц және 3000 Гц, ал /u/ үшін - 300 Гц, 600 Гц және 2300 Гц. Қозудың гармоникалық құрылымын жиіліктің домендік көрінісінен де байқауға болады.

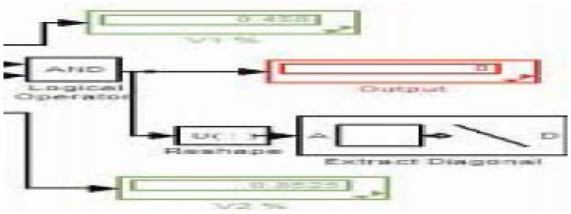


3-сурет Үш дыбыстың сөйлеу сигналдары (/a/ /i/ /u/)

3-суреттен көріп отырғанымыздай, айтылатын әр дауыстың жиілігі мен биіктігі бірдей емес. Бұл дауысты тану жүйелері үшін маңызды проблеманы тудырады, яғни дауысты сәйкестендіру пайда болған сайын дауыстың өзгеруін қалай есепке алу керек. Сонымен қатар, олар фондық шу мен басқа айнымалыларға байланысты жалған қабылдамаудың жоғары жылдамдығына ие. Бұл жобада қарапайым, бірақ дауысты танудың қарапайым жүйесі (бағдарламалық жасақтама) құрылды. Жүйе MATLAB-та блоктарының көмегімен жасалған. Негізінен «дауыстық сілтеме шаблоны» оны келесі дауыстық идентификациямен салыстыруға болатындай етіп жасалады. «Анықтама шаблонын» құру үшін адам өзінің атын айтуы керек және бұл .wav файлы ретінде жазылады.

Сурет 4. Дауысты тану жүйесі.

Дауысты тану жүйесі дауыстық/сөйлеу үлгісін танудың бірнеше айнымалысын немесе параметрлерін қамтиды, соның ішінде дауыс тонының биіктікті, динамикасын және толқын формасын. Осы параметрлерді қамтитын тексеру алгоритмі 4-суретте көрсетілгендей қол жетімді функционалды блоктар көмегімен жүзеге асырылады. Сөйлеу сигналын өңдеудің бірнеше кезеңі бар. Біріншісі - тыныштықтың энергетикалық деңгейіне қарсы қысқа мерзімді сигналдың энергия деңгейлерін өлшеу. Екіншіден, ол сандық FIR өткізгіш сүзгісі ретінде қызмет ететін және сонымен қатар сигналдың жиіліктік компоненттерін шығаратын Digital Filter Design блогы арқылы өтіп, шу мен кез келген қажетсіз сигналдарды жояды. Келесі қадам - ерекшеліктерді шығару. Оларға қысқа уақыт аралығында автокорреляцияны есептеу арқылы биіктік контурын анықтау, 1, 2 және 3 форматтардың жиіліктерін анықтау және автокорреляция мен FFT көмегімен орташа спектрлік энергия тығыздығын анықтау кіреді. Салыстыру процедурасы анықтамалық және енгізу шаблондарының өлшемдерін теңестіру арқылы жүзеге асырылады. Соңғы нәтижені тексеру үшін стандартты ауытқулар және ковариация сияқты әр түрлі статистикалық параметрлер есептелді.



Сурет 5. Енуді басқаруға арналған функционалды блоктар

Әзірленген дауысты тану жүйесінің басты артықшылығы - жүйенің пайдаланушының ыңғайлылығы үшін қауіпсіздіктің реттелетін деңгейін қамтамасыз етуі. Мысалы, оның ауруы кезінде адамның дауысының қалыпты өзгеруі үшін 15% ауытқу (85% кездейсоқтық) жеткілікті деп саналады. Мұндай үлкен ауытқуға қауіпсіздік пен қауіпсіздіктің қалыпты деңгейі қажет болатын уақыт пен қатысушылық жүйелер жағдайында да жол беруге болады. Әйтпесе, қауіпсіздік параметрін қажет болғанда жоғары сәйкестік мәніне қоюға болады; яғни құпия ақпаратқа қол жеткізу. 5-суретте енуді басқаруға арналған функционалды блоктар көрсетілген. Пайдаланушының дауыстық кірісі дауыстық нұсқаулық үлгісімен салыстырылады. Егер ауытқу белгіленген қауіпсіздік деңгейінен аз болса, логикалық «1» пайда болады, бұл рұқсат берілген дегенді білдіреді. Әйтпесе, '0' логикасы шығарылады, бұл қол жеткізуге тыйым салынған дегенді білдіреді. Алынған логикалық нәтиже параллель порт арқылы микроконтроллер тізбегіне келесі тапсырмаға (есікті ашу немесе керісінше) сәйкесінше беріледі.

3. Нәтижелер мен тәжірибелер

Адам өзінің аты сияқты қарапайым сөз сөйлегенде, оның дауысы толқын тудырады. Бұл толқын формасы дауыс үлгісі ретінде белгілі. Саусақ іздері сияқты, адамдардың дауысы бір-бірінен ерекшеленеді. Демек, дауыстық үлгілерді жеке сәйкестендіру үшін пайдалануға болады.

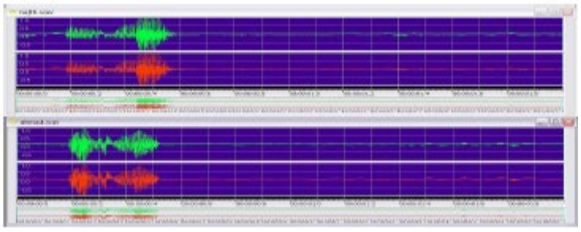
Сурет: 7. Бір адамның дауысының үлгілері

7-суретте «A1» сөзін сөйлейтін адамның екі дауыс үлгісі көрсетілген. Біреуі дауыстық нұсқаулық үлгісі ретінде қолданылады. Екі дауыс үлгісі де әр уақытта жазылған. Дауысты тану жүйесі екі үлгідегі айырмашылықтарды есептеу үшін қолданыла алады. Дауыстық және дауыстық идентификатор - бұл дауыстық қуат спектрлерінің параметрлік емес бағалары. Анықтамалық дауыс мәні 5,28 құрайды, ал Voice ID 5,959 мәнін береді. Демек, осы екі үлгінің арасындағы айырмашылық (∂) 0,6792 құрайды. V_1 және V_2 стандартты ауытқулары эталондық дауыспен салыстырғанда сәйкесінше 12,79% және 11,33% дауыстық идентификатор үшін.

Кесте 1. Дауысты тану нәтижелері

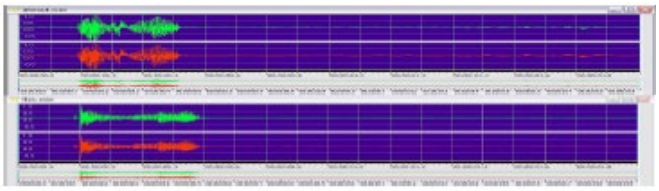
сілтеме үлгісі	екінші енгізу	анықтамалық дауыс	Voice ID	*Diff(∂) =|анықтамалық дауыс-Voice ID|*	*V_1%= (Diff(∂/анықтамалық дауыс)x 100%*	*V_2%= (Diff(∂/ Voice ID)x100%*	Шығыс
A1	өзі	5.28	5.959	0.6792	12.79	11.33	1
A2	басқа адам бір жынысты	5.28	2.846	2.434	45.8	85.25	0
B1	басқа адам бір жынысты	0.1292	0.0995	0.0297	22.95	29.79	0
B2	басқа адам басқа жынысты	5.959	0.1394	5.82	97.17	41.75	0

Екі айырмашылықта 15% -дан аз болғандықтан, дауыстар бір дауысқа тиесілі деп танылады. 6-суретте шығыс толқынының формалары көрсетілген. Егер V_1 және V_2 кірістерінің екеуі де 15% -дан төмен айырмашылықты көрсетсе (осы жоба үшін белгіленген қауіпсіздік деңгейі), логикалық нәтиже «1» болады, демек, рұқсат берілген. 8 және 9 суреттерде әртүрлі ерлер мен әйелдердің дауыстық іздері көрсетілген. V_1% және V_2% екеуі де 15% -дан асады, логикалық «0» құрайды, сондықтан енуге тыйым салынады. 10-суретте әр түрлі жыныстың толқын формасы көрсетілген. 1 кестеде Дауысты тану жүйесі сенімділігі мен тиімділігін тексеру үшін бірнеше дауыстық үлгілерден алынған нәтижелер көрсетілген. Қателік шегі 15% деңгейінде орнатылған кезде, жүйе толық аутентификация дәлдігін қамтамасыз етеді. Жоғарыда айтылғандай, қауіпсіздікті бақылауды енгізу үшін төзімділік маңызды болмауы мүмкін.



Сурет: 8. Әр түрлі ерлер дауыстық модельдері

Сурет 9. Әйелдер дауысының әр түрлі модельдері



Сурет 10. Ер мен әйел дауысының үлгілері

4. Қорытынды

Дауысты тану - бұл ең қарапайым биометриялық схемалардың бірі және қолданылуы. Енді, дауысты тану жүйелеріне тереңдетілген оқытуды енгізудің арқасында бұл технология әлдеқайда сенімді әрі қауіпсіз бола бастады.

Биометриялық технологиялар қазір саусақ іздері, көз қарашығын сканерлеу, дауыстық тану, беттер, қолтаңбалар немесе қолдың геометриясы сияқты бірегей физикалық сипаттамаларды идентификациялау және тексеру механизмі ретінде қолданудың арқасында танымал бола бастады. Бұл технология бизнес пен үкіметтерге жеке тұлғаны ұрлау және алаяқтықпен күресуге, транзакцияларды қорғауға, құпия ақпаратты қорғауға, шығындарды азайтуға және қызмет көрсету деңгейлерін жақсартуға көмектеседі. Биометриялық дауысты идентификациялау технологиясы көптеген нарықтарда баяу таралуда. Бір себебі, олар басқа биометриялық технологиялар сияқты дәл емес, бұл фондық шу мен басқа айнымалыларға байланысты жалған қабылдамаудың жоғары жылдамдығына байланысты. Алайда, микропроцессорлар мен сигналдарды өңдеу технологиялары дамыған кезде, күрделі алгоритмдерді қолдана отырып, дауысты дәлірек өлшеуге болады және оларды дауыстық баспаға айналдыруға болады - бірегей сандық көрініс. Дауысты тану жүйесі ол рұқсатты басқару механизмі үшін қауіпсіздік функцияларын толеранттылықпен толық дәлдікпен қамтамасыз етілген 15% деңгейіндегі дәлдікті ортада жұмыс істеді және орындалды

Бұл жобаны сәтті деп атауға болады, алайда дауысты басқаруды дербес, дербес микропроцессорлық қол жетімділікті басқару құрылғысында қолдану сияқты жетілдіруге мүмкіндік бар. Бұл жақсарту осы жобаның, яғни дауысты тану жүйесінің нарықтық құнын арттыру үшін қажет.

Бұл жұмыс Қазақстан Республикасы Білім және ғылым министрлігінің қолдауымен өтті. IRN AP05131207 терең нейрондық желілерді қолдана отырып, көп тілді автоматты түрде сөйлеуді тану технологияларын жасау.

[1] Мамырбаев О.Ж., Қыдырбекова А.С., Турдалыұлы М., Мекебаев Н.О., «Дауыс бойынша пайдаланушыны идентификациялау және аутентификациялау әдістеріне шолу», «Инновациялық АТ және ақылды технологиялар» ғылыми конференциясының материалдары, 2019, 315-321 бб.

[2] Дэвид Снайдер и др. «*x*-векторы: надежные встраивания DNN для распознавания говорящих», IEEE Международная конференция по акустике, речи и обработке сигналов (ICASSP), апрель 2018 г.

[3] М.Н.Калимолдаев, О.Ж.Мамырбаев, А.С.Қыдырбекова, Н.О.Миекебаев “i-векторлы бейнелеуді пайдаланып дауысты тексеру және идентификациялау”, Халықаралық математика және физика журналы 10, № 1, 66 (2019)1.

[4] О.Ж.Мамырбаев, М.Тұрдалыұлы, Н.О.Мекебаев, А.С.Қыдырбекова, «Сандық жүйке желілерін қолданып сөйлеуді автоматты түрде тану», ACIIDS, Индонезия, Іс жүргізу, II бөлім, 2019 ж.

[5] Георг Хейгольд и др., «Сквозная текстовая проверка говорящего», IEEE Международная конференция по акустике, обработке речи и сигналов (ICASSP), март 2016 г.

[6] Хитоси Ямамото и др., «Надежное извлечение i-вектора, тесно связанное с обнаружением голосовой активности с использованием глубоких нейронных сетей», Ежегодный саммит и конференция Азиатско-Тихоокеанской ассоциации обработки сигналов и информации (APSIPA ASC), декабрь 2017 г.

[7] Shivangi Mahto и др., «Преобразование i-вектора с использованием нового дискриминационного автошифровщика с шумоподавлением для надежного распознавания шума», INTERSPEECH, август 2017 г.

ПОДГОТОВКА СПЕЦИАЛИСТОВ И АДАПТАЦИЯ IT-ОБРАЗОВАНИЯ В УСЛОВИЯХ ЦИФРОВОЙ ЭКОНОМИКИ

Кубеков Б.С., Утегенова А.У., Науменко В.В., Ибраимкулов А.К.
e-mail: b.kubekov@mail.ru, utegenova77@mail.ru naumenko.v5@mail.ru, aibek_ibraimkulov@mail.ru
Институт информационных и вычислительных технологий КН МОН РК, Казахстан

Аннотация

В разделе 3.4 «Развитие человеческого капитала» Государственной программы «Цифровой Казахстан» 2018-2022г. отмечается, что цифровизация значительно опережает существующую систему требований производства к составу профессий, занятых на рынке труда. Отсутствие оперативной связи между рынком труда и системой образования может привести одновременно к подготовке уже не востребованных кадров и высвобождению кадров по «умирающим» профессиям. Поэтому необходимо полностью пересмотреть содержание всех уровней образования через развитие цифровых навыков всех специалистов.

Четвертая технологическая революция, цифровая трансформация предприятий, связанных с ИТ-производством, и развитие цифровой экономики беспрецедентно увеличивают темпы обновления имеющихся на рынке информационных технологий. Смена технологий приводит к быстрому изменений требований к навыкам, востребованным на рынке рабочей силы, и угрожает увеличением уже существующего разрыва между требованиями предприятий и уровнем подготовки выпускников вузов.

Такому положению способствует ряд причин, среди которых следует особо отметить несовершенство и негибкость образовательных программ; нехватка квалифицированных кадров преподавателей; неопределенность в логике

построения образовательной траектории обучения; невозможность удовлетворения жестким требованиям к аккредитации образовательной деятельности и необходимости гибкого реагирования на изменения требований профессионального рынка.

Введение

В газете «Казахстанская правда» от 14 января 2020г., Министр МОН РК отметил, что «Перед системой образования стоит задача обеспечения рынка труда специалистами, способными адекватно отвечать на современные вызовы, обладающими новыми знаниями, способными их применять и, главное, способными их непрерывно обновлять. С другой стороны, система образования по своей сути является инерционной, когда принятые сегодня решения дадут результаты через 5-10 лет. А рынок труда нуждается в специалистах с новыми навыками и компетенциями сегодня. Внедрение системы квалификаций потребует смены парадигмы образования от знаниевого подхода к компетентностному, где определяющую роль будут играть результаты обучения, показывающие знания, навыки и компетенции, что будет удобно и работодателю, и обучающемуся. Министерство, отойдя от централизованно управляемого учебного процесса для конкретных образовательных программ, предоставило университетам право самостоятельно разрабатывать этот процесс наиболее эффективными способами, адаптированными к возможностям, потребностям и интересам обучающихся студентов. Тем самым обеспечивается гибкость образовательных программ с учетом требований экономики региона и страны, а также сближение процесса подготовки специалистов к нуждам и ожиданиям трудовой сферы. Поэтому задача вузов заключается в том, чтобы максимально гармонизировать образовательные программы с принимаемыми отраслевыми рамками квалификаций и профессиональными стандартами».

Цифровая трансформация образования - неизбежный процесс изменения содержания, методов и организационных форм учебной работы. Данный процесс разворачивается в быстроразвивающейся цифровой образовательной среде и направлен на решение задач социально-экономического развития в условиях четвертой промышленной революции и становления цифровой экономики.

В этих условиях перед образованием ставятся следующие задачи по созданию современной и безопасной цифровой образовательной среды, обеспечивающей высокое качество и доступность образования всех видов и уровней; внедрению новых методов обучения и воспитания, образовательных технологий, обеспечивающих усвоение обучающимися базовых навыков и умений, повышение их мотивации к обучению и вовлеченности в образовательный процесс; модернизации профессионального образования посредством внедрения адаптивных, практико-ориентированных и гибких образовательных программ; формированию системы непрерывного обновления работающими гражданами своих профессиональных знаний, и приобретения новых профессиональных навыков, включая овладение компетенциями в области цифровой экономики.

Таким образом, суть цифровой трансформации образования заключается в достижении каждым обучаемым необходимых образовательных результатов за счет персонализации образовательного процесса, на основе развития в учебных заведениях цифровой образовательной среды, использования методов искусственного интеллекта, средств виртуальной реальности, обеспечения

общедоступного широкополосного доступа к Интернету и работу с большими данными.

Неизбежность переосмысления традиционного содержания образования подчеркивается в итоговых разделах Второй Российско-Китайской конференции [1], в которых отмечается, что успешность реализации проблем и задач по цифровой трансформации образования предусматривает овладение обучающимися ограниченного набора *ключевых* или *базовых понятий*, что позволит избежать поверхностного изучения большого количества не всегда связанных между собой вопросов, что является распространенным недостатком образовательных программ. Выделение *базовых понятий* позволяет сформировать у обучающихся понятийную структуру, которая облегчает приобретение новых знаний. Основательное изучение *базовых понятий* и участие в реализации проектов будет способствовать глубокому и осознанному усвоению естественных представлений при усвоении естественно-научных и специальных дисциплин и курсов. Кроме того, сокращение объема фактически изучаемого материала высвобождает время для того, чтобы обучающиеся могли выстраивать собственные знания, усваивать базовые компетентности, которые профессиональные сотрудники ИТ-производства используют в своей практической работе; рефлексивно осмысливать усваиваемый материал и глубже понимать природу изучаемых процессов и явлений, связанных с производством программных продуктов.

Указанные особенности и требования по совершенствованию инженерного образования, в соответствии с современными тенденциями по цифровизации образования, взяты в качестве основополагающих принципов по разработке методики и при реализации информационно-образовательного портала, проводимых в рамках проекта AP05134973 «Исследование и разработка моделей и методики представления и организации знаний с применением онтологического подхода и инструментальных средств Smart-технологии, при реализации образовательных программ и процессов».

1. Базовые концепции и возможности методики

В качестве базовых концепций методики служат концепции онтологического инжиниринга и проектно-компетентностного подхода, реализация которых направлена на формирование знаниевых компонент и последующего их использованием как для проектирования знаниевого контента дисциплин образовательной специальности, так и сценариев индивидуальной траектории обучения [].

Данные концепции реализованы в информационно-образовательном портале, предоставляющем следующие возможности:

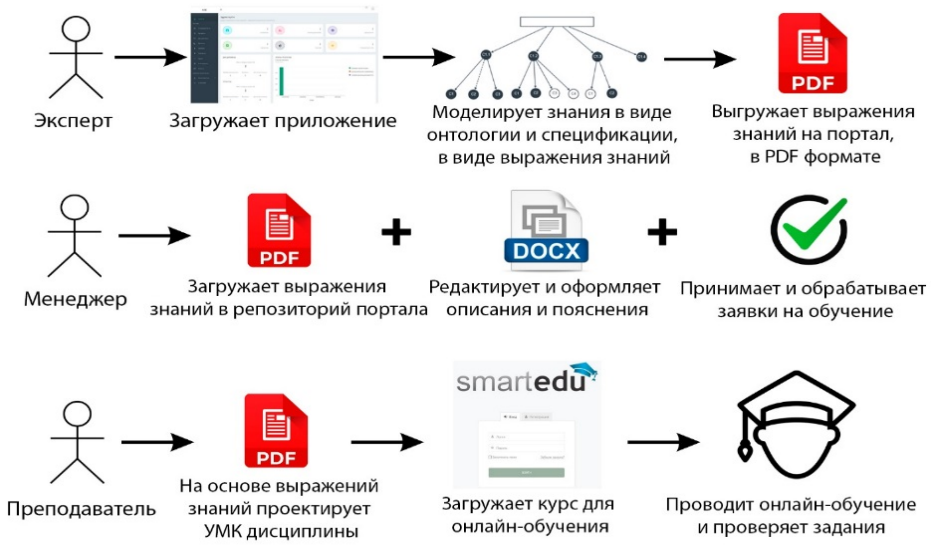


Рисунок 1- Возможности информационно-образовательного портала

Первая возможность – традиционно формировать знаниевый контент дисциплин учебного плана образовательной программы (в первую очередь «Обязательного модуля по специальности» и «Модуля по специальности»). Такая возможность предоставит заведующему кафедрой, совместно с Экспертом, в лице представителя ИТ-производства:

- определять требования по содержанию знаниевого контента дисциплин;
- формировать и управлять знаниевым контентом дисциплин;
- адаптировать знаниевый контент, в соответствии с развитием новых технологий и инструментальных средств специальности;
- контролировать релевантность содержания знаниевого контента рабочих программ дисциплин требованиям рынка труда и профессиональных стандартов.

Вторая возможность - в том, что используя проектно-ориентированную технологию обучения, планировать знаниевый тренд и формировать знаниевый контент, в первую очередь, профилирующих и базовых дисциплин образовательной программы специальности, в соответствии с компетентностными моделями этапов CDIO. В этом случае, распределение дисциплин по семестрам связывается с этапами CDIO, и с необходимостью получения требуемых знаний и умений для разработки проекта(ов), по каждому из этапов.

Третья возможность - в том, что используя проектно-ориентированную технологию обучения, планировать знаниевый тренд и формировать знаниевый контент сценария индивидуальной траектории обучения. В этом случае, для конфигурирования сценария обучения используются знаниевые компоненты и их интерфейсы, в виде smart-контракта. На рисунке 2. представлены возможности информационно-образовательного портала по индивидуальной форме обучения.

Рисунок 2- Возможности информационно-образовательного портала по индивидуальной форме обучения

2. Основные концепции образовательной среды портала

Всемирная инициатива MIT - CDIO и проектно-ориентированная технология обучения (*Conceive, Design, Implement, Operate).*

Онтологический инжиниринг - ядро концепции «*Управление знаниями»,* связанное с наиболее цельным представлением сведений о понятиях, в едином знаниевом формате, взаимосвязями между понятиями, определениями одних понятий посредством других с учетом типа взаимосвязей. Онтологический инжиниринг предоставляет возможность более лучшей *восприимчивости* (*Receptivity*) *и воспроизводимости* понятий.

Компетентностная модель этапа CDIO - композиция *профессиональных, базовых и дополнительных компетенций*, каждая из которых отображается необходимым и достаточным набором *опорных понятий* предметной области.

Форматы организации и представления знаний: *модель онтологии,* характеристическая модель, *выражение знания, знаниевый компонент, знаниевый тренд*.

CDIO Syllabus – перечень планируемых результатов обучения и требований работодателей к инженерному образованию, сформулированных в виде компетенций.

Компонентные технологии и smart-контракт. Свойства общности и изменчивости.

Выражение компетенций:

$$ec.PrC.Conceive <= *PrC_1(*P_1*P_2)*PrC_2*PrC_3; \quad (1)$$

с помощью которого происходит моделирование и конфигурирование сценария обучения.

Моделирование сценария обучения - основано на smart-контрактах знаниевых компонент, из которых формируется *знаниевый тренд* траектории обучения:

$$\{P\} <KC,Col,Lev> \{Q\} \quad (2)$$

Знаниевый тренд – *знаниевая модель*, являющаяся *композицией профессиональных, базовых и дополнительных* компетенций компетентностной

модели этапа CDIO, усвоение каждой из компетенций модели, предполагает изучение и освоение необходимого и достаточного набора *опорных понятий*.

Сигнатуры *профессиональных, базовых и дополнительных компетенций* знаниевого тренда определяют рамочные знания плана CDIO Syllabus - *плана планируемых результатов обучения*.

$$\{P\} < \text{CDIO Syllabus} > \{Q\} \qquad (3)$$

Знаниевый контент – спецификация онтологии *опорных понятий профессиональных, базовых и дополнительных компетенций,* в формате выражений знаний. Знаниевый контент, таким образом, определяет знаниевое содержание дисциплин образовательной программы, либо индивидуальной траектории обучения.

На рисунке 3 представлены компоненты и процессы образовательной среды портала:

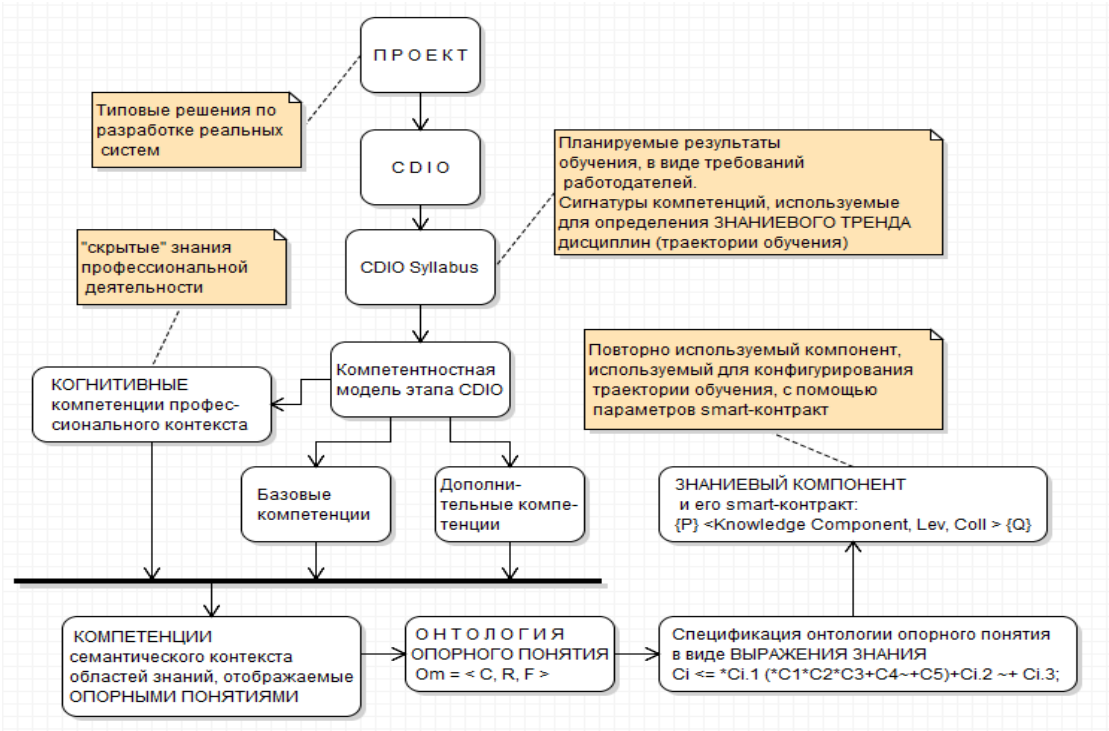


Рисунок 3 - Компоненты и процессы образовательной среды портала

Заключение

Таким образом, в данной статье обобщены основные результаты исследований и разработок, связанные с инновационной методикой формирования знаниевого контента, на базе онтологического инжиниринга и проектно-компетентностного подхода. Разработанная для этих целей образовательная среда, в рамках информационно-образовательного портала, позволяет формировать и адаптировать знания современных технологий и инструментальных средств ИТ-производства, обладает возможностями по конфигурированию этих знаний для проектировании знаниевого контента дисциплин образовательной программы либо формирования сценария индивидуальной траектории обучения, в соответствии с профессиональными потребностями обучающихся.

Практическая значимость проводимых исследований будет способствовать содействию и развитию цифровой трансформации образования, путем продвижения:

- проектно - компетентностной парадигмы и основанной на ней инновационной модели отображения знаний, позволяющей релевантно отображать семантический контекст образовательных ресурсов наборами опорных понятий;
- методики формирования и реализации знаниевых компонент, основанной на проектно-ориентированной технологии обучения, стандартов и принципов всемирной инициативы CDIO; эпистемологической функции компетентностного подхода уровневого инженерного образования; онтологическом инжиниринге и компонентном подходе;
- системности представления и формализации знаниевых компонент для проектирования знаниевого контента рабочих программ дисциплин, на основе smart-контракта;
- семантического анализа образовательных ресурсов с целью выделения опорных (ключевых) понятий и предоставления возможности конфигурирования знаниевых компонент, в соответствии с требуемым сценарием и результатами обучения, а также воспроизводимостью и повторным использованием знаниевых компонент;
- навыков и рациональных приемов «сжатия» информации с когнитивно-графическим представлением знаний;
- возможности для преподавателей использовать удобное и доступное инструментальное средство для создания и визуального представления онтологии опорных понятий, их редактирования и использования в простой и наглядной форме;
- возможности формирования повторно используемых знаниевых компонент, их конструирования и адаптации для широкого спектра образовательных программ и услуг, что будет способствовать академической мобильности студентов и конкурентоспособности учебного заведения на рынке образовательных услуг.

Результаты исследований и разработок представлены в виде монографии «Организация и представление знаний планируемого обучения на основе онтологии», изданной в издательстве «LP-Zhasulan» и переведенной на казахский и английский языки, с дальнейшим изданием; многочисленных публикациях в базе цитирования Scopus, изданиях, рекомендованных ККСОН и в международных конференциях. По программному обеспечению образовательной среды получено авторское свидетельство США № 610144435, от 06.04.2019г. Intelligent educational environment (Интеллектуальная образовательная среда) // «Международная компания по защите авторского права, США, Нью-Йорк», гарантированное Бернской конвенцией / Kubekov Bulat. На базе данной методики защищены докторская диссертация Утегеновой А.У., подготавливаются диссертации докторантов Науменко В. и Ибраимкулова А.; защищены магистерские диссертации: Жаксыбаевой Н., Плотникова Д., Ибрайхан Р., Резцова Н., Магаметовой А., Рудаковой Ю., Касеновой А.

Благодарности:

Данные исследования и разработки стали возможными благодаря гранту ИРН 05134973 «Исследование и разработка моделей и методики представления и

организации знаний с применением онтологического подхода и инструментальных средств Smart-технологии, при реализации образовательных программ и процессов», выполняемому в Институте информационных и вычислительных технологий КН МОН РК.

Литература

1. Государственная программа «Цифровой Казахстан» 2018-2022г.

2. Вторая Российско-китайская конференция исследователей образования. «Цифровая трансформация образования и искусственный интеллект», 26-27 сентября 2019г. - https://aiedu.hse.ru/2019/program

СЕКЦИЯ 4

Деректерді қорғау және ақпараттық қауіпсіздік. Ақпаратты қорғаудың бағдарламалық-техникалық құралдары. Күрделі жүйелердің ақпараттық қауіпсіздігін камтамассыз етудің математикалық әдістері.

Информационная безопасность и защита данных.
Программно-технические средства защиты информации.
Математические методы обеспечения информационной безопасности сложных систем

Information security and data protection. Software and hardware for information protection. Mathematical methods of ensuring information security of complex systems

AL01 АЛГОРИТМІНЕ ИНТЕГРАЛДЫҚ КРИПТОГРАФИЯЛЫҚ ТАЛДАУ

Д.С. Дюсенбаев
e-mail: dimash_dds@mail.ru
ҚР БҒМ ҒК «Ақпараттық және есептеуіш технологиялар институты»
«Ақпараттық қауіпсіздік» зертханасы

Аннотация. *Қандай да бір симметриялы блокты криптографиялық алгоритмге интегралдық криптоталдау бойынша талдау жасау үшін, алдымен оның сызықтық емес функциялық бөліктеріне арнайы интегралдық криптанализдың талаптарына сай талдаулар қарастырылады. Көп жағдайларда сызықтық емес функцияның қызметін S-блоктар атқарады. Сондықтан, талдаулар алдымен блокқа жүргізіліп, нәтижелері статикалық кесте құрайды. Интегралдық криптоталдау белгілі бірнеше ашық және жабық мәтіндердің жұптарының негізінде статистикалық талдау ретінде жүргізіледі.*

S-блокқа интегралдық криптанализ

S-блокқа талдау жасаудан бұрын жалпы алгебрадағы ақырлы өріске (немесе Галуа өрісіне) шолу жасайық. Қарастырылатын өрісіміз $GF(2^n)$ екілік жүйедегі ақырлы өріс болсын және осы өрісте $K = GF(2)[x]/(f(x))$ факторлық сақина құрастырайық. Мұндағы $f(x)$ - $GF(2)$ өрісіндегі келтірілмейтін көпмүшелік. K факторлық сақинасын $GF(2)$ өрісіндегі көпмүшеліктердің сақинасы деп атап, оны $K[x]$ түрінде белгілейді.

Ескерту. m айнымалы көпмүшеліктер үшін $K[x_1, x_2, \dots, x_m]$ түрінде белгілейді.

Ескерту. $K[x]$ сақинасының элементтерін $(p_{n-1}, p_{n-2}, \dots, p_1, p_0)$ вектор ретінде қарастырамыз. Мұндағы вектор көпмүшеліктің коэффиценттері $p(x) = p_{n-1}x^{n-1} + p_{n-2}x^{n-2} + \dots + p_1x + p_0 = \sum_{i=0}^{n-1} p_i x^i$ және $p_i \in GF(2)$. Мақалада белгілеуге қолайлы болу үшін жоғарыда айтылған векторларды екілік жүйедегі сан ретінде қабылдаймыз. $K[x] \to Z_p$ түрлендіруі биективті, $p = 2^n$. Біз түрлендірген екілік жүйедегі ақырлы сандар жиынында қолданылатын қосу амалының орнына разрядтық биттік қосу (xor) деп аталатын математикалық амалын және көбейту амалы да разрядтық биттік қосу амалының ережесі бойынша орындалады. $K[x]$ және Z_p ақырлы жиындары осы амалдар бойынша $< K[x], \oplus, \otimes >$ - сақинасын және $< Z_p, \oplus >$ - абель тобын құрайды.

Ескерту. Z_p ақырлы жиынның ақырлы сандар жиыны ретінде емес, екілік жүйедегі векторлық жиын ретінде қараймыз.

Ескерту. Жазуға ықшамдырақ болу үшін төменгі теңдіктердегі модулді көрсетпейміз.

Көпмүшеліктегі бейнесі	Векторлық бейнесі	Сандық бейнесі
0	(0,0,…,0,0,0)	0
1	(0,0,…,0,0,1)	1
x	(0,0,…,0,1,0)	2
x+1	(0,0,…,0,1,1)	3

x^2	(0,0,…,1,0,0)	4
x^2+1	(0,0,…,1,0,1)	5
…	…	…
$x^{n-1}+x^{n-2}+\cdots+x$	(1,1,…,1,1,0)	2^n-2
$x^{n-1}+x^{n-2}+\cdots+x+1$	(1,1,…,1,1,1)	2^n-1

1-кесте. $GF(2)[x]/(f(x))$ факторлық сақинасына қатысты кесте.

Лемма 1. Ақырлы жиынның барлық элементтерінің қосындысы нөлге тең.

Дәлелдеуі. Ақырлы жиынның барлық элементтерінің қосайық. Сонда көпмүшеліктің сәйкесінше коэфиценттері модуль 2 бойынша қосылады. Басқаша айтқанда қосу $GF(2)$ өрісінде орындалады. Көпмүшеліктердің әрбір бірмүшелігіндегі 1-лердің саны 2^{n-1} тең. Сондықтан барлық коэфиценттер нөлге тең.

Лемма 2. Ω ақырлы жиын және оның $\Omega_1, \Omega_2: \Omega = \Omega_1 \cup \Omega_2, \Omega_1 \cap \Omega_2 = \emptyset$ шарттарды қанағаттандыратын ішкі жиындары болсын. Егер $\forall(x,k) \in \Omega_1: x \oplus k \in \Omega_1$ және $\forall(x,k) \in \Omega_2: x \oplus k \in \Omega_1$ болса, онда $\Omega_1 = \{x_1, x_2, \dots, x_r\}$ және $\Omega_2 = \{y_1, y_2, \dots, y_r\}$ үшін $\oplus \sum_{i=1}^{r} S(x_i \oplus k) \equiv \oplus \sum_{i=1}^{r} S(y_i \oplus k) \equiv s$ қосындысы кілттің кез келген мәнінде тұрақты мән береді.

Дәлелдеуі: Ω ақырлы жиын барлық элементтерінің қосындысы теорема 1 бойынша нөлге тең. Сондықтан, қосынды нөл болуы үшін қосылғыштар тең болады. Енді қосылғыштар кілттің кез келген мәнінде бірдей мән қабылдайтынын көрсетейік. $\forall(x,k) \in Z_1: x \oplus k \in Z_1$ шарты үшін кілттің Z_1 жиында жататын мәндері үшін тұрақты болады, өйткені Z_1 жиынның элементерінің орындарын ауыстырғанмен бірдей болады.

$$x_1 \oplus k \oplus x_2 \oplus k \oplus \dots \oplus x_{r-1} \oplus k \oplus x_r \oplus k$$
$$\Rightarrow S(x_1 \oplus k) \oplus S(x_2 \oplus k) \oplus \dots \oplus S(x_{r-1} \oplus k) \oplus S(x_r \oplus k)$$

Кілттің Ω_2 жиында жататын мәндері үшін келесі қасиеттер орындалады: $\forall k \in \Omega_2, \forall x \in \Omega_1: x \oplus k \in \Omega_2$. Ω_2 жиынның элементерінің орындарын ауыстырғандай болады.

$\forall x \in \Omega_2$ және кілттің Ω_1 жиында жататын мәндері үшін $\forall k \in \Omega_1$: $x \oplus k \in \Omega_2$. Ω_2 жиынның элементерінің орындарын ауыстырғандай болады.

$\forall x \in \Omega_2$ және кілттің Ω_2 жиында жататын мәндері үшін $\forall k \in \Omega_2$: $x \oplus k \in \Omega_1$. Ω_1 жиынның элементерінің орындарын ауыстырғандай болады.

Лемма 3. Бірдей қосылғыштардың саны жұп болса, онда қосынды нөлге тең.

Дәлелдеуі: $x \oplus k \oplus x \oplus k \equiv 0 \Rightarrow S(x \oplus k) \oplus S(x \oplus k) \equiv 0$.

1-мысал. Мысалға төмендегідей блок берілсін.

											0	1	2	3	4	5
(x)		4				1	3	0			5		2			

2-кесте. S-блок алмастыру кестесі.

Ескерту. S-блок алмастыруы кездейсоқ болғандықтан, оған көпмүшеліктердің сақинасын таңдағанда қарастырып отырған алгоритмдегі жиындарды және оған қолданылатын амалдарды бір өрістің төңірегіне түрлендіруіне қатысты.

Z_p жиынның барлық элементтерінің қосындысы $s \equiv \oplus \sum_{i=0}^{2^{m+1}-1} i \equiv 0$ нөлге тең болғандықтан, қосындыларды қиылпайтын екі қосындыға жіктесек, онда олардың мәні тең болады. Ол қосындыларды теорема 2-нің шарттарын қанағаттандыратындай жіктесек, онда кілттің кез келген мәнінде S-блокқа қатысты тұрақты мән қабылдайды.

Егер $x_1 \oplus k \oplus x_2 \oplus k \oplus \ldots \oplus x_7 \oplus k \oplus x_8 \oplus k$ қосындысындағы x_i-лар $(i = \overline{1,8})$ мен k-ның әртүрлі мәндерін беріп, олардың сәйкесінше S-блок алмастырудан кейінгі қосындысын есептейік: $S(x_1 \oplus k) \oplus S(x_2 \oplus k) \oplus \ldots \oplus S(x_7 \oplus k) \oplus S(x_8 \oplus k)$. Сонда төмендегі өрнектерді көреміз:

Егер $x_i \equiv i, (i = \overline{0,7})$ және $k \equiv 0$ болғанда, өрнектеріміз келесі мәндерді қабылдайды: $0 \oplus 1 \oplus 2 \oplus 3 \oplus 4 \oplus 5 \oplus 6 \oplus 7 \equiv 0 \Rightarrow$
$S(0) \oplus S(1) \oplus S(2) \oplus S(3) \oplus S(4) \oplus S(5) \oplus S(6) \oplus S(7) \equiv 7.$

Дәл осылай $k \equiv 1$ болғанда, өрнектеріміз: $1 \oplus 0 \oplus 3 \oplus 2 \oplus 5 \oplus 4 \oplus 7 \oplus 6 \equiv 0 \Rightarrow$
$S(1) \oplus S(0) \oplus S(3) \oplus S(2) \oplus S(5) \oplus S(4) \oplus S(7) \oplus S(6) \equiv 7.$

$k \equiv 2$ болғанда, өрнектеріміз: $2 \oplus 3 \oplus 0 \oplus 1 \oplus 6 \oplus 7 \oplus 4 \oplus 5 \equiv 0 \Rightarrow$
$S(2) \oplus S(3) \oplus S(0) \oplus S(1) \oplus S(6) \oplus S(7) \oplus S(4) \oplus S(5) \equiv 7.$

…

$k \equiv 7$ болғанда, өрнектеріміз: $7 \oplus 6 \oplus 5 \oplus 4 \oplus 3 \oplus 2 \oplus 1 \oplus 0 \equiv 0 \Rightarrow$
$S(7) \oplus S(6) \oplus S(5) \oplus S(4) \oplus S(3) \oplus S(2) \oplus S(1) \oplus S(0) \equiv 7.$

$k \equiv 8$ болғанда, өрнектеріміз: $8 \oplus 9 \oplus 10 \oplus 11 \oplus 12 \oplus 13 \oplus 14 \oplus 15 \equiv 0 \Rightarrow$
$S(8) \oplus S(9) \oplus S(10) \oplus S(11) \oplus S(12) \oplus S(13) \oplus S(14) \oplus S(15) \equiv 7.$

…

$k \equiv 15$ болғанда, өрнектеріміз: $15 \oplus 14 \oplus 13 \oplus 12 \oplus 11 \oplus 10 \oplus 9 \oplus 8 \equiv 0 \Rightarrow$
$S(15) \oplus S(14) \oplus S(13) \oplus S(12) \oplus S(11) \oplus S(10) \oplus S(9) \oplus S(8) \equiv 7.$

Егер $x_i \equiv 2i, (i = \overline{0,7})$ және $k \equiv 0$ болғанда, өрнектеріміз:
$0 \oplus 2 \oplus 4 \oplus 6 \oplus 8 \oplus 10 \oplus 12 \oplus 14 \equiv 0 \Rightarrow$
$S(0) \oplus S(2) \oplus S(4) \oplus S(6) \oplus S(8) \oplus S(10) \oplus S(12) \oplus S(14) \equiv 12.$

$k \equiv 1$ болғанда, өрнектеріміз: $1 \oplus 3 \oplus 5 \oplus 7 \oplus 9 \oplus 11 \oplus 13 \oplus 15 \equiv 0 \Rightarrow$
$S(1) \oplus S(3) \oplus S(5) \oplus S(7) \oplus S(9) \oplus S(11) \oplus S(13) \oplus S(15) \equiv 12.$

$k \equiv 2$ болғанда, өрнектеріміз: $2 \oplus 0 \oplus 6 \oplus 4 \oplus 10 \oplus 8 \oplus 14 \oplus 12 \equiv 0 \Rightarrow$
$S(2) \oplus S(0) \oplus S(6) \oplus S(4) \oplus S(10) \oplus S(8) \oplus S(14) \oplus S(12) \equiv 12.$

…

$k \equiv 15$ болғанда, өрнектеріміз: $15 \oplus 13 \oplus 11 \oplus 9 \oplus 7 \oplus 5 \oplus 3 \oplus 1 \equiv 0 \Rightarrow$
$S(15) \oplus S(13) \oplus S(11) \oplus S(9) \oplus S(7) \oplus S(5) \oplus S(3) \oplus S(1) \equiv 12.$

Егер $x_i \equiv 4i, (i = \overline{0,7})$ және $k \equiv 0$ болғанда, өрнектеріміз:
$0 \oplus 4 \oplus 8 \oplus 12 \oplus 0 \oplus 4 \oplus 8 \oplus 12 \equiv 0 \Rightarrow$
$S(0) \oplus S(4) \oplus S(8) \oplus S(12) \oplus S(0) \oplus S(4) \oplus S(8) \oplus S(12) \equiv 0.$

$k \equiv 1$ болғанда, өрнектеріміз: $1 \oplus 5 \oplus 9 \oplus 13 \oplus 1 \oplus 5 \oplus 9 \oplus 13 \equiv 0 \Rightarrow$
$S(1) \oplus S(5) \oplus S(9) \oplus S(13) \oplus S(1) \oplus S(5) \oplus S(9) \oplus S(13) \equiv 0.$

$k \equiv 2$ болғанда, өрнектеріміз: $2 \oplus 6 \oplus 10 \oplus 14 \oplus 2 \oplus 6 \oplus 10 \oplus 14 \equiv 0 \Rightarrow$
$S(2) \oplus S(6) \oplus S(10) \oplus S(14) \oplus S(0) \oplus S(6) \oplus S(10) \oplus S(14) \equiv 0$

…

$k \equiv 15$ болғанда, өрнектеріміз: $15 \oplus 11 \oplus 7 \oplus 3 \oplus 15 \oplus 11 \oplus 7 \oplus 3 \equiv 0 \Rightarrow$
$S(15) \oplus S(11) \oplus S(7) \oplus S(3) \oplus S(15) \oplus S(11) \oplus S(7) \oplus S(3) \equiv 0.$

Егер $x_i \equiv i + 8, (i = \overline{0,7})$ және $k \equiv 0$ болғанда, өрнектеріміз:
$8 \oplus 9 \oplus 10 \oplus 11 \oplus 12 \oplus 13 \oplus 14 \oplus 15 \equiv 0 \Rightarrow$
$S(8) \oplus S(9) \oplus S(10) \oplus S(11) \oplus S(12) \oplus S(13) \oplus S(14) \oplus S(15) \equiv 7.$

Бұл жағдайда $k \equiv \overline{0,7}$ үшін осы қосылғыштардың орын ауысуымен жіктеледі, ал $k \equiv \overline{8,15}$ үшін қиылыспайтын жиынның қосылғыштарымен жіктеледі.

Егер $x_i \equiv 4 + i, (i = \overline{0,7})$ және $k \equiv 0$ болғанда, өрнектеріміз:
$4 \oplus 5 \oplus 6 \oplus 7 \oplus 8 \oplus 9 \oplus 10 \oplus 11 \equiv 0 \Rightarrow$
$S(4) \oplus S(5) \oplus S(6) \oplus S(7) \oplus S(8) \oplus S(9) \oplus S(10) \oplus S(11) \equiv 9$

$k \equiv 1$ болғанда, өрнектеріміз: $5 \oplus 4 \oplus 7 \oplus 6 \oplus 9 \oplus 8 \oplus 11 \oplus 10 \equiv 0 \Rightarrow$
$S(5) \oplus S(4) \oplus S(7) \oplus S(6) \oplus S(9) \oplus S(8) \oplus S(11) \oplus S(10) \equiv 9$

$k \equiv 2$ болғанда, өрнектеріміз: $6 \oplus 7 \oplus 4 \oplus 5 \oplus 10 \oplus 11 \oplus 8 \oplus 9 \equiv 0 \Rightarrow$
$S(6) \oplus S(7) \oplus S(4) \oplus S(5) \oplus S(10) \oplus S(11) \oplus S(8) \oplus S(9) \equiv 9$

$k \equiv 3$ болғанда, өрнектеріміз: $7 \oplus 6 \oplus 5 \oplus 4 \oplus 11 \oplus 10 \oplus 9 \oplus 8 \equiv 0 \Rightarrow$
$S(7) \oplus S(6) \oplus S(5) \oplus S(4) \oplus S(11) \oplus S(10) \oplus S(9) \oplus S(8) \equiv 9$

$k \equiv 4$ болғанда, өрнектеріміз: $0 \oplus 1 \oplus 2 \oplus 3 \oplus 12 \oplus 13 \oplus 14 \oplus 15 \equiv 0 \Rightarrow$
$S(0) \oplus S(1) \oplus S(3) \oplus S(4) \oplus S(12) \oplus S(13) \oplus S(14) \oplus S(15) \equiv 9$

$k \equiv 5$ болғанда, өрнектеріміз: $1 \oplus 0 \oplus 3 \oplus 2 \oplus 13 \oplus 12 \oplus 15 \oplus 14 \equiv 0 \Rightarrow$
$S(1) \oplus S(0) \oplus S(3) \oplus S(2) \oplus S(13) \oplus S(12) \oplus S(15) \oplus S(14) \equiv 9$

…

$k \equiv 8$ болғанда, өрнектеріміз: $12 \oplus 13 \oplus 14 \oplus 15 \oplus 0 \oplus 1 \oplus 2 \oplus 3 \equiv 0 \Rightarrow$
$S(12) \oplus S(13) \oplus S(14) \oplus S(15) \oplus S(0) \oplus S(1) \oplus S(2) \oplus S(3) \equiv 9$

$k \equiv 9$ болғанда, өрнектеріміз: $13 \oplus 12 \oplus 15 \oplus 14 \oplus 1 \oplus 0 \oplus 3 \oplus 2 \equiv 0 \Rightarrow$
$S(13) \oplus S(12) \oplus S(15) \oplus S(14) \oplus S(1) \oplus S(0) \oplus S(3) \oplus S(2) \equiv 9$

…

$k \equiv 14$ болғанда, өрнектеріміз: $10 \oplus 11 \oplus 8 \oplus 9 \oplus 6 \oplus 7 \oplus 4 \oplus 5 \equiv 0 \Rightarrow$
$S(10) \oplus S(11) \oplus S(8) \oplus S(9) \oplus S(6) \oplus S(7) \oplus S(4) \oplus S(5) \equiv 9$

$k \equiv 15$ болғанда, өрнектеріміз: $11 \oplus 10 \oplus 9 \oplus 8 \oplus 7 \oplus 6 \oplus 5 \oplus 4 \equiv 0 \Rightarrow$
$S(11) \oplus S(10) \oplus S(9) \oplus S(8) \oplus S(7) \oplus S(6) \oplus S(5) \oplus S(4) \equiv 9$

Көп жағдайларда қосындылар бірдей мәнге ие бола бермейді.

$$0 \oplus 6 \oplus 12 \oplus 2 \oplus 8 \oplus 14 \oplus 4 \oplus 10 \Rightarrow S(0) \oplus S(6) \oplus S(12) \oplus S(2) \oplus S(8) \oplus S(14) \oplus S(4) \oplus S(10)$$

$$1 \oplus 7 \oplus 13 \oplus 3 \oplus 9 \oplus 15 \oplus 5 \oplus 11 \Rightarrow S(1) \oplus S(7) \oplus S(13) \oplus S(3) \oplus S(9) \oplus S(15) \oplus S(5) \oplus S(11)$$

… т.б.

Енді осы интегралдық мән ретінде қарастырып отырған қосындылардың санын есептейік. Егер S-блок алмастыруының кіріс және шығыс биттерінің саны 8 болса, онда қарастырып отырған қосындылардың саны $C_{128}^{256} = \frac{256!}{128!128!} \approx 2^{251}$ терумен пара-пар. Ондай теруді қарастыруға компьютердің есептеу күші жеткіліксіз. Сондықтан интегралдық мәндердің санын анықтау үшін келесі алгоритмді пайдаланамыз.

Топтарға ажырату бойынша топтастыру арқылы жиындарды іздеу немесе санау.

$GF(2)$ өрісінде екі элементтен тұратын {0; 1} жиыны үшін лемма 2-ні қанағаттантыратын жиындардың саны екеу. Теру $C_2^1 = 2$ тең. Мүмкін болатын жалпы саны 2.

$GF(2^2)$ өрісіндегі элементердің саны 4 және жиынды {0; 1; 2; 3} белгілеп алайық. Лемма 2-ні қанағаттантыратын жиындардың саны 6 және олар мыналар: {(0; 1); (2; 3); (0; 2); (1; 3); (0; 3); (1; 2)}. Теру $C_4^2 = 6$. Жалпы саны $4^2 = 16$.

$GF(2^3)$ өрісіндегі элементердің саны 8 және жиын {0; 1; 2; 3; 4; 5; 6; 7} болады. Лемма 2-ні қанағаттантыратын жиындардың саны 14 және олар: {(0; 1; 2; 3); (4; 5; 6; 7); (0; 1; 4; 5); (2; 3; 6; 7); (0; 1; 6; 7); (2; 3; 4; 5); (0; 2; 4; 6); (1; 3; 5; 7); (0; 2; 5; 7); (1; 3; 4; 6); (0; 3; 4; 7); (1; 2; 5; 6); (0; 3; 5; 6); (1; 2; 4; 7)}. Теру $C_8^4 = 70$. Жалпы саны $8^4 = 4096$.

Интегралдық мәндерді қабылдайтын «S-блоктің кірісінің саны 14 × (4!) = 14 × 24 = 336.

$GF(2^4)$ өрісіндегі элементердің саны 16: {0; 1; 2; 3; 4; 5; 6; 7; 8; 9; 10; 11; 12; 13; 14; 15}. 2-теореманы қанағаттантыратын жиындардың саны 26 және олар: {(0; 1; 2; 3; 4; 5; 6; 7); (8; 9; 10; 11; 12; 13; 14; 15); (0; 1; 2; 3; 8; 9; 10; 11); (4; 5; 6; 7; 12; 13; 14; 15); (0; 1; 2; 3; 12; 13; 14; 15); (4; 5; 6; 7; 8; 9; 10; 11); (0; 1; 4; 5; 8; 9; 12; 13); (2; 3; 6; 7; 10; 11; 14; 15); (0; 1; 6; 7; 8; 9; 14; 15); (2; 3; 4; 5; 10; 11; 12; 13); (0; 2; 4; 6; 8; 10; 12; 14); (1; 3; 5; 7; 9; 11; 13; 15); (0; 2; 5; 7; 8; 10; 13; 15); (1; 3; 4; 6; 9; 11; 12; 14); (0; 2; 4; 6; 9; 11; 13; 15); (1; 3; 5; 7; 8; 10; 12; 14); (0; 2; 5; 7; 9; 11; 12; 14); (1; 3; 4; 6; 8; 10; 13; 15); (0; 3; 4; 7; 8; 11; 12; 15); (1; 2; 5; 6; 9; 10; 13; 14); (0; 3; 5; 6; 8; 11; 13; 14); (1; 2; 4; 7; 9; 10; 12; 15); (0; 3; 4; 7; 9; 10; 13; 14); (1; 2; 5; 6; 8; 11; 12; 15); (0; 3; 5; 6; 9; 10; 12; 15); (1; 2; 4; 7; 8; 11; 13; 14)}. Теру $C_{16}^8 = \frac{16!}{8!8!} = 12870 \approx 2^{13}$. Жалпы саны $16^8 = 4294967296 = 2^{32}$. Интегралдық мәндерді қабылдайтын S-блоктің кірісінің саны 26 × (8!) = 26 × 40320 = 1048320 ≈ 2^{19}.

$GF(2^5)$ өрісіндегі элементердің саны 32: {0; 1; 2; 3; … 27; 28; 29; 30; 31}. Лемма 2-ні қанағаттантыратын жиындардың саны 50. Теру $C_{32}^{16} = \frac{32!}{16!16!} \approx 2^{29}$. Жалпы саны $32^{16} = 2^{80}$. Интегралдық мәндерді қабылдайтын S-блоктің кірісінің саны 50 × (16!) ≈ 2^{49}.

$GF(2^6)$ өрісіндегі элементердің саны 64: {0; 1; 2; 3; … 59; 60; 61; 62; 63}. Лемма 2-ні қанағаттантыратын жиындардың саны 98. Теру $C_{64}^{32} = \frac{64!}{32!32!} \approx 2^{60}$. Жалпы саны $64^{32} = 2^{192}$. Интегралдық мәндерді қабылдайтын S-блоктің кірісінің саны 98 × (32!) ≈ 2^{124}.

$GF(2^7)$ өрісіндегі элементердің саны 128: {0; 1; 2; 3; … 125; 126; 127}. Лемма 2-ні қанағаттантыратын жиындардың саны 194. Теру $C_{128}^{64} = \frac{128!}{64!64!} \approx 2^{124}$. Жалпы саны $128^{64} = 2^{448}$. Интегралдық мәндерді қабылдайтын S-блоктің кірісінің саны 194 × (64!) ≈ 2^{303}.

$GF(2^8)$ өрісіндегі элементердің саны 256: {0; 1; 2; 3; … 253; 254; 255}. Лемма 2-ні қанағаттантыратын жиындардың саны 386. Теру $C_{256}^{128} = \frac{256!}{128!128!} \approx 2^{251}$. Жалпы саны $256^{128} = 2^{1024}$. Интегралдық мәндерді қабылдайтын S-блоктің кірісінің саны 386 × (128!) ≈ 2^{724}.

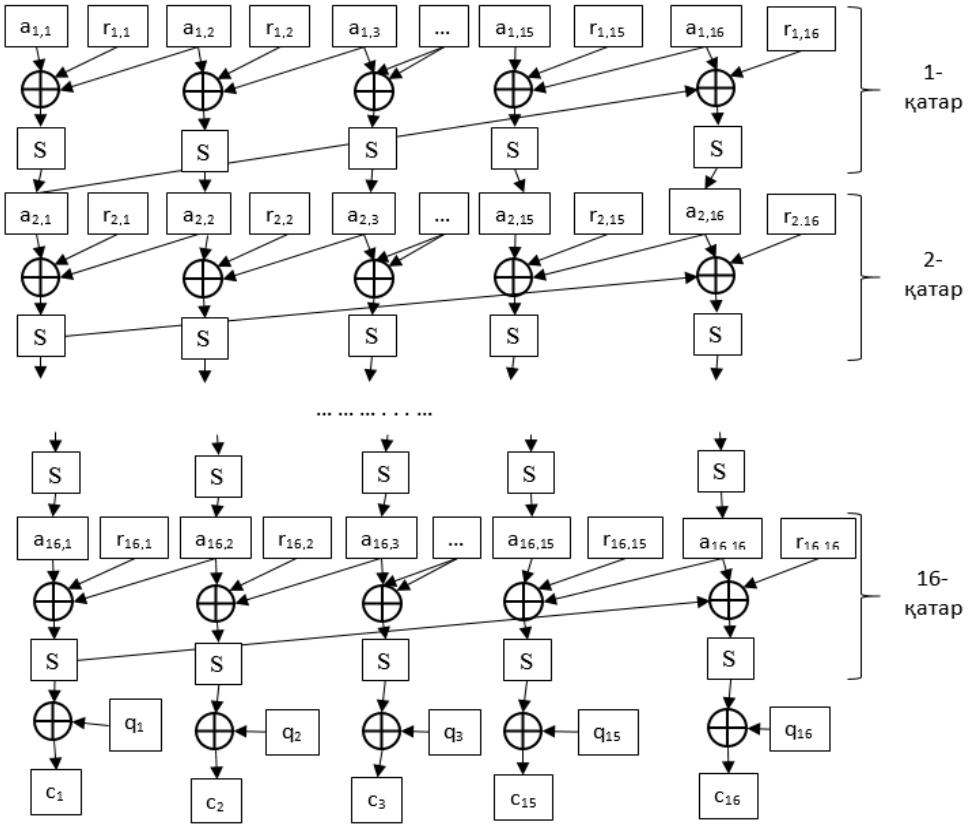
AL01 алгоритміне интегральдық криптоанализ

Алдымен алгоритмнің ішкі құрылысын еске түсіреміз және бір раунд үшін интегралдық талдау жазайық. Ол үшін 128 ашық және жабық мәндердің жұптарының қосындысы таңдалады. Жоғарыдан бағалау үшін, таңдалған ашық мәндердің интегралдық қосындысының біреуі нөлге тең емес, ал қалғандары нөлге тең болатындай шартпен аынады. Сондықтан, А қосымшадағы «AL01» алгоритмінің

1-суретте көрсетілген схема бойынша бірінші қатардан кейінгі нәтижелердің (мәндерінің) ақиқаттығының ықтималдылығы 1-ге тең болады. Қалған қадамдардан кейінгі нәтижелердің ықтималдылығын есептеу үшін S-блок алмастыруының кіріс және шығыс мәндерінің қосындыларына қатысты интегралдық мәндердің анықталуының ықтималдылығын есептеуін қажет етеді.

Егер барлық мүмкін болатын жағдайлардың саны $256^{128} = (2^8)^{128} = 2^{1024}$ және интегралдық мәндердің саны мен шығысы нөл болатын жағдайлардың санының қосындысы $2^{724} < 2^{724} + 2^{512} = 2^{512}(2^{212} + 1) < 2^{725} \Rightarrow 2^{724} + 2^{512} \approx 2^{725}$ болады. Сонда шығысы анықталған мән болуының ықтималдылығы $2^{725} / 2^{1024} = 2^{-299}$ тең болады.

Сондықтан әрі қарай қарастырудың қажеттілігі жоқ.



1-сурет. «AL01» алгоритмінің бір раундтық жұмыс істеу схемасы

Әдебиеттер

1. Joan Daemen, Lars Knudsen, Vincent (January 1997). “The Block Cipher Square” (PDF) in 4th International Workshop on Fast Software Encryption (FSE ’97), Volume 1267 of Lecture Notes in Computer Science.: 149-165, Haifa: Springer-Verlag.

2. Lars Knudsen and David Wagner. Integral Cryptanalysis (Extended Abstract). – 2003.

3. Материал из Википедии: - ru.wikipedia.org/wiki/Интегральный_криптоанализ.

АЛГОРИТМ АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЯ НА ОСНОВЕ ВТОРОГО ФАКТОРА В ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ СИСТЕМАХ

Усатова О.А.[1], Нысанбаева С.Е.[1], Вуйцик В.[2]
e-mail: uoa_olga@mail.ru, sultasha1@mail.ru, waldemar.wojcik@pollub.pl
Институт информационных и вычислительных технологий
КН МОН РК, Казахстан
Люблинский технологический университет, Люблин, Польша

Аннотация. *Предлагается алгоритм аутентификации пользователя на основе второго фактора. Рассмотрены типы аутентификации пользователей. Предложено и исследовано клиент-серверное приложение разработанного алгоритма двухфакторной аутентификации. Приведены результаты разработанной программной реализации.*

Ключевые слова: *алгоритм аутентификации, информационно-коммуникационные системы, безопасность данных, протоколы аутентификации, мобильное приложение, серверная часть.*

Введение

Одними из основных средств защиты информационных систем от постороннего вмешательства являются идентификация и аутентификация, так как механизмы защиты информации рассчитаны на работу с поименованными субъектами и объектами. Аутентификация и идентификация информационной системы являются взаимозависимыми действиями распознавания и проверки подлинности. Основной целью аутентификации является снижение угроз безопасности, а именно нарушение конфиденциальности и целостности информации. Аутентификация используется для доступа к социальным сетям, электронной почте, интернет магазинам, интернет–банкингу, платежным системам и т.д. Несанкционированный доступ – один из самых распространенных видов нарушений, представляющий непосредственную угрозу работоспособности системы.

1. Система аутентификации пользователя на основе генерации одноразового пароля

В настоящее время использование парольной аутентификации является доступным и распространенным из–за простоты применения. Этот метод защищенности направлен на увеличение прочности концепции защиты информации. Одним из эффективных методов защиты информации является двухфакторная аутентификация для входа в систему. Она предполагает двойную защиту данных посредством привязки аккаунта к системе защиты. После привязки пользователю необходимо будет взаимодействовать с этой системой для верификации данных.

Двухфакторная аутентификация позволяет обеспечивать более высокую степень защиты по сравнению с однофакторной аутентификацией, при которой пользователь предлагает только один фактор, обычно пароль, который используется

для контроля доступа к чувствительным системам и данным. В данной статье рассмотрен алгоритм аутентификации пользователя на основе второго фактора для обеспечения защиты информации в информационно–коммуникационных системах. Проведен обзор и анализ существующих систем защиты информации в информационно–коммуникационных системах и алгоритмов многофакторной аутентификации. Рассмотрены принципы построения защиты информации в базе данных при аутентификации пользователя и классификация распространенных методов двухфакторной аутентификации, используемых в информационных системах, рассмотрены недостатки и достоинства этих методов. Рассмотрены алгоритмы и протоколы аутентификации с использованием одноразового кода, проведен анализ систем защиты информации и их характеристики на основе двухфакторной аутентификации и статистические данные компаний, специализирующихся в области обеспечения информационной безопасности и анализ кибератак [1].

Предлагаемая система двухфакторной аутентификации состоит из двух этапов. На первом этапе аутентификации пользователь вводит свой логин и пароль. При успешном прохождении этого этапа необходимо пройти второй этап, на котором рассматривается генерация одноразового пароля на основе программы аутентификации и мобильного телефона [2].

Большинство современных систем аутентификации основываются на применение функций вычисления хеш, которые вычисляют хеш на основе входной строки для дальнейшего использования в системе кодирования. В качестве входной строки для хеш–функции могут быть использованы учетные данные пользователя (логин, пароль), текущее время, дополнительная секретная строка и т.д. Для реализации алгоритма двухфакторной аутентификации используется функция SHA256. Эта функция использовалась для вычисления хеша в виду ее особенностей. Изменение одного бита входной строки влияет на все биты вычисляемого хеша, что позволяет исключить вычисляемую зависимость получаемого хеша от входной строки [3].

В ходе исследования были рассмотрены методы аутентификации пользователя на основе генерации одноразового пароля для проведения эффективности работы алгоритмов.

Использование одноразовых паролей для прохождения двухфакторной аутентификации осуществляется следующим образом:

1. производится ввод учетных данных пользователя (логин/пароль);
2. учетные данные посылаются на сервер аутентификации;
3. производится проверка введенных пользователем данных на сервере аутентификации;
4. на стороне сервера формируется запрос, который генерирует одноразовый код и отправляет его на устройства;
5. одноразовый пароль вводится пользователем и передает его на сервер;
6. сервер производит проверку сходства паролей;
7. проверка удовлетворительная, аутентификация считается успешной.

Алгоритм двухфакторной аутентификации для защиты информации в информационно-коммуникационных системах, позволяющий использовать комбинацию постоянного и временного (одноразового) паролей. Постоянный пароль пользователь выбирает сам. Временный пароль генерируется по определенным алгоритмам и действует в течение определенного времени.

Для получения одноразового пароля используется дополнительное программное обеспечение. Генерация одноразового пароля возможна в режиме онлайн. В данном режиме дополнительное программное обеспечение посылает запрос на сервер авторизации для генерации временного пароля [4].

Одноразовый пароль генерируется на стороне сервера и представляется пользователю в дополнительном программном обеспечении. Одноразовый пароль может содержать определенный срок действия до одной минуты.

Генерация одноразового пароля выполняется на основе результата выбранной определенной тригонометрической функции, которая имеет ряд переменных параметров. Функции объединяются в массив значений размерностью 256 на 256, их количество равно 65536. Выбор тригонометрической функции и ее начальных параметров осуществляется на основе результата вычисления хеш– функции SHA256. Также для вычисления тригонометрической функции и ее начальных параметров может быть использован любой тип хеш–функции.

Входной строкой для вычисления хеш–функции является комбинация учетных данных пользователя, текущего момента времени и дополнительной секретной строки.

Полученная хеш–функция разделяется на отдельные числа, которые будут являться индексами для выбора тригонометрической функции и начальными данными [5, 6].

Для оптимизации данного алгоритма проведен анализ стойкости генератора с использованием метода полного перебора, в котором учитывается длина строки и скорость перебора в секунду. На скорость перебора влияют характеристики программного обеспечения и оборудования. К характеристикам программного обеспечения относятся антивирусные программы, защита экранов, операционные системы и т.д. К характеристикам оборудования относятся, пропускная способность шины данных, скорость работы накопителей информации, пропускная способность сети, наличие виртуализации и т.д. Данные характеристики существенно влияют на скорость работы алгоритма и не могут превышать скорости перебора 1000000 в секунду. 64 ядерный процессор может перебрать 1000000 слов в сукунду.

В разработанном алгоритме аутентификации пользователя на основе второго фактора, генератор секретных слов работает по описанному выше алгоритму и генерирует слова, состоящие из 5 символов. Скорость перебора была взята 100000 слов в секунду, которую может перебрать 4 ядерный процессор, что для использования обработки на персональном компьютере является оптимальным [7].

Новизна алгоритма двухфакторной аутентификации пользователя на основе программы – аутентификатора и мобильного телефона, состоит в генерации тригонометрических функций путем усложнения масштабирования функций при вычислении одноразового пароля. Масштабирование выполняется матричным представлением вариантов тригонометрических функций и использованием хеш–функций для вычисления координат и параметров, генерируемой тригонометрической функцией по текущему времени, секретной строке, логину и паролю первого аутентификационного пароля.

2. Программная реализация системы аутентификации

Осуществлена компьютерная реализация системы защиты информации при аутентификации пользователя на основе одноразового пароля и проведено исследование корректности выполнения предложенного алгоритма.

Для реализации разработанного алгоритма было создано клиент-серверное приложение «Security Code of the 2FA», состоящая из 3 взаимодействующих модулей: пользователя, мобильного приложения и серверной части [7].

Пользователь при входе в информационную систему должен пройти регистрацию для осуществления дальнейшего взаимодействия с сервисом. При регистрации пользователю необходимо создать логин и пароль, пароль желательно создать сильный, следуя рекомендуемым стандартам.

При входе в информационную систему пользователь авторизуется, вводя свои учетные данные и одноразовый пароль. Для получения одноразового пароля пользователь должен иметь мобильный телефон и установленное на него приложение [8].

Мобильное приложение – клиентская часть защиты информационной системы с использованием двухфакторной аутентификации. Оно позволяет пользователю взаимодействовать с системой путем регистрации собственных информационных ресурсов или выбора одного из доступных и генерировать одноразовый временный пароль для входа.

Серверная часть – основополагающий модуль в работе проекта, в котором реализован алгоритм генерации одноразового пароля для осуществления защищенного входа в подключенные информационные ресурсы.

Для безопасного хранения информации используются криптографические алгоритмы защиты баз данных и стандартные средства защиты, такие как подключение к базе данных с помощью логина и пароля администратора базы данных. В работе [9] подробно рассмотрены структуры каждого из этих модулей.

Исследование производительности разработанного приложения позволяет значительно уменьшить период обработки и расходы на поддержание работоспособности. Автоматизация процесса тестирования позволит уменьшить время обработки данных в информационной системе. Одной из важных характеристик применения программного продукта является скорость его выполнения. В связи с этим рассмотрены результаты исследования скорости выполнения программной реализации алгоритма двухфакторной аутентификации на основе генерации одноразового пароля. Данное клиент-серверное приложение Security Code of the 2FA имеет размер 0,687 Мбайт, что является оптимальным для реализации предложенного алгоритма.

Также не маловажным является то, что разработанная система может быть внедрена в закрытую сеть.

Выводы

Разработан алгоритм двухфакторной аутентификации на основе программы – аутентификатора и мобильного телефона, который генерирует усложненный набор функций одноразового пароля для каждой отдельной информационно-коммуникационной системы. Для предложенного алгоритма аутентификации пользователей информационно–коммуникационных систем на основе второго фактора разработано и реализовано клиент – серверное приложение.

Полученные результаты являются новыми, имеют теоретическую и практическую значимость. Проведенные научно-исследовательские работы по разработке и анализу систем защиты информации при идентификации и аутентификации пользователя на основе двухфакторной аутентификации направлены на решение задач по обеспечению информационной безопасности.

Возможность дальнейшего развития предложенной системы двухфакторной аутентификации заключается в расширении компонентов (например, используется уже такая терминология, как «Композитная аутентификация»), применении отечественных криптографических алгоритмов, разработке дополнительных инструментов и оптимизации решений с целью повышения производительности.

Литература

1 Нысанбаева С.Е., Усатова О. А. «Способы обеспечения безопасности информации в базах данных»// Вестник КазНИТУ им. Сатпаева.– Алматы, 2018. – № 2. – С. 66–70.

2 Нысанбаева С.Е., Усатова О.А. «Двухфакторная аутентификация в автоматизированной системе управления»// III Междунар. науч. конф. «Информатика и прикладная математика». – Алматы, 2018. – С. 239–242.

3 S. Nyssanbayeva, W. Wojcik, O. Ussatova «Algorithm for generating temporary password based on the two–factor authentication model»// Przegląd Elektrotechniczny. – Polan, 2019. –№ 5. – P. 101–106.

4 Olga Ussatova, Saule Nyssanbayeva «Generators of one-time two-factor authentication passwords»// Informatyka, Automatyka, Pomiary w Gospodarcei Ochronie Środowiska. – Poland, 2019. № 2. – P. 60–64.

5 O. Ussatova, S. Nyssanbayeva, W. Wojcik «Development of an authentication model based on the second factor in an automated control system»// Вестник КБТУ. – Алматы, 2019. –Т.16. – С.115–118.

6 O. Ussatova, S. Nyssanbayeva, W. Wojcik «Two-factor authentication algorithm implementation with additional security parameter based on mobile application »// International Conference on Wireless Communication, Network and Multimedia Engineering (WCNME2019). –Guilin, China, 2019. – Vol. 89. – P. 84–86.

7 Begimbayeva Yenlik, Ussatova Olga, Biyashev Rustem, Nyssanbayeva Saule «Development of an automated system model of information protection in the cross-border exchange»// Cogent Engineering Journal. – 2020. DOI: 10.1080/ 23311 916. 2020.1724597. –P. 1–13.

8 O. Ussatova, S. Nyssanbayeva, W. Wojci. « Software implementation of two-factor authentication to ensure security when accessing an information system» // Вестник КазНУ им.аль-Фараби. –Алматы,2019. – С.87–95.

9 Усатова О.А. «Клиент-серверная система защиты информации на основе двухфакторной аутентификации»// междунар. науч.– практ. конф. «Актуальные проблемы информационной безопасности в Казахстане». – Алматы, 2020. – С. 243–248.

ЖЕЛІЛІК ТОПОЛОГИЯНЫҢ ҚАУІПСІЗДІК МОДЕЛІ МЕН ӘДІСТЕРІН ӘЗІРЛЕУ

Ордабаева Г.К.
e-mail: gulzi200988@mail.ru
Әл-Фараби атындағы Қазақ ұлттық университеті, PhD докторант, Қазақстан

***Аннотация**: Бүгінгі таңда, ақпараттық жүйелерге қауіп төндіретін модельдерді құрудың көптеген тәсілдері белгілі. Бұл тәсілдер нормативтік актілерде және стандарттарда, әртүрлі компаниялардың құжаттарында және ғылыми зерттеулерде сипатталған.*

Мақалада қауіптерді анықтауда және қауіпсіздікті бағалауда қолданылатын компьютерлік желілердің модельдерін құру тәсілдері мен әдістері қарастырылды.

Кіріспе

Ақпараттық технологиялардың қарқынды дамуы үшін желі топологиясының сенімділігін арттыру өзекті міндеттердің бірі. Мұндай мәселелерді шешу үшін қолданыстағы желілік архитектураларды әзірлеу, желі арқылы ақпараттық ресурстарды тарату кезіндегі қауіптерді зерттеу қажеттігі туындайды.

Компьютерлік желілер модельдері қарастыратын бөліміне байланысты келесі топтарға бөлінеді [1]:

- тұжырымдамалық (концептуальдық) модельдер [2, 3];
- функционалды модельдер [4];
- математикалық модельдер [5].

Тұжырымдамалық модельдер сипатталған жүйенің құрылымын, оның элементтерінің қасиеттерін, бейресми тілде модельдеу мақсаттарына жету үшін маңызды себеп-салдарлық байланыстарды анықтайды. Бұл үшін әдетте графиктер, кестелер, диаграммалар және т.б. қолданылады.

Сипаттамалық графикалық модельдер өзара әрекеттесетін және өзара байланысты блоктар жиынтығын қолдана отырып, функционалды модельдер ұйымның жұмыс істеуі аясында қалай жасалатынын көрсетеді.

Математикалық модельдер формулалар, графиктер, мысалдар және т. б. арқылы сипатталады, сонымен қатар, әлеуметтік, техникалық және жаратылыстану ғылымдарында, әртүрлі дизайн мәселелерін шешуде қолданылады [6].

Негізгі бөлім

Ашық жүйелердің өзара байланысының (Open System Interconnection, OSI) Халықаралық стандарты бойынша компьютерлік желі жеті деңгейге бөлінеді: қолданбалы, көрсету, сеанстық, транспорттық, желілік, арналық және физикалық. OSI моделінің физикалық, арналық және желілік деңгейлеріне проекцияда таратылған есептеу жүйесі объектілерінің өзара әрекеттесу моделі [7] жұмыста сипатталған. Нақты желілік шарттарға, қызметтер үстемділігіне және басқа факторларға байланысты жіберуші мен қабылдаушы компьютерлер арасындағы бағыт анықталады. Таратылған есептеу жүйелері моделінің негізгі міндеті берілген кіріс параметрлері арасында байланыс орнату.

Проекциядағы OSI физикалық деңгейінің моделі таратылған есептеу жүйесінің объектілері арасындағы физикалық байланысты анықтайды. OSI арналық деңгейіне проекциядағы желілік адаптерлердің аппараттық адрестері деңгейіндегі объектілердің өзара әрекеттесуін орнатады. Проекциядағы OSI объектілерінің желілік деңгейге байланысы логикалық адрестер деңгейінде анықталады.

OSI моделінің физикалық деңгейінде желілік кабель арқылы жіберілетін әрбір биттің ұзақтығы және оның сәйкес электрлік немесе оптикалық импульсқа көшірілуі анықталады. OSI моделінің арналық деңгейіне проекциядағы желілік адаптерлердің аппараттық адрестері деңгейіндегі объектілердің өзара әрекеттесуін орнатады. Желілік деңгейге проекцияда OSI моделі объектілерінің байланысы логикалық адрестер деңгейінде анықталады.

Жұмыста әмбебап *KS* желісі енгізіледі, ол физикалық немесе арналық OSI деңгейінің байланыс сызығы ретінде түсініледі, өйткені, физикалық және арналық деңгейлердің проекциядағы моделдерінде айырмашылық жоқ. Физикалық деңгейдегі объектілер - хост немесе роутердің желілік адаптері, арналық деңгейдегі объектілер – желілік адаптердің аппараттық адресі.

Берілген таратылған есептеу жүйесінде *N* өзара байланысқан *KS* (физикалық және арналық деңгейдегі байланыс желілері) және *LS* (желілік деңгейдегі байланыс желілері) объектілер мен роутерлерді қамтиды, яғни:

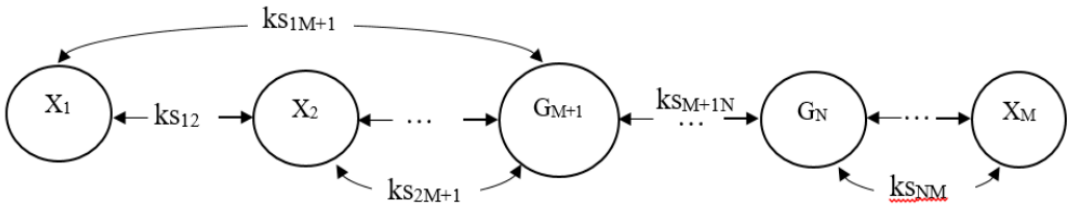
$X=\{x_i|i=1..M\}$ – хостар жиыны,
мұнда $i=1..M$ –хостар саны.

$G=\{g_i|j=M+1..N\}$ –роутерлер жиыны,
мұнда $j=M+1..N$ –роутерлер саны.

Физикалық немесе арналық деңгейінде әр хост тек бір ғана жақын роутермен байланысады. Барлық нысандар *K* объектісін *L* объектісімен байланыстыратын қос бағытты байланыс желілері ks_{KL} арқылы өзара әрекеттеседі.

$KS=\{ks_{KL}|k=1..N,L=1..N\}$,
мұнда *KS* - OSI моделінің физикалық немесе арналық деңгейіндегі байланыс желілерінің жиынтығы.

Проекциядағы ақпараттық жүйенің OSI моделінің арналық немесе физикалық деңгейінің граф моделі 1- суретте көрсетілген.

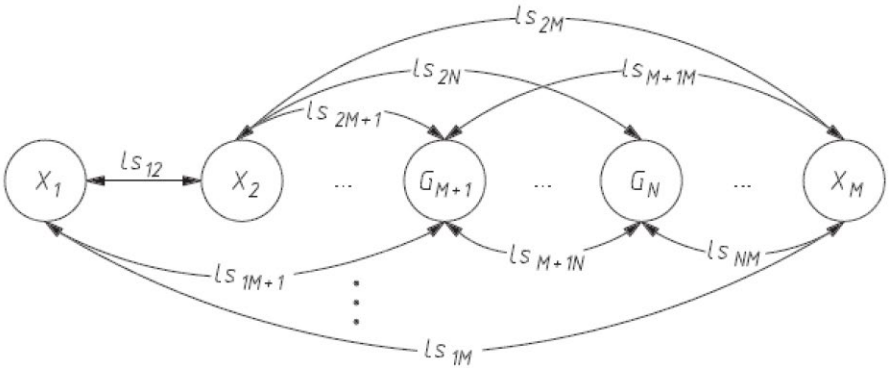


1- сурет. Проекциядағы OSI моделінің физикалық немесе арналық деңгейінің граф моделі

Желілік деңгейде әр объект басқа объектімен (кез - келгенімен) бір-екі бағытты ls_{KL} байланыс желісінің көмегімен өзара әрекеттесе алады, ол *K* объектісін *L* объектісімен байланыстырады. Бұл деңгейде хосттың немесе маршрутизатордың желілік адресі объект болып табылады.

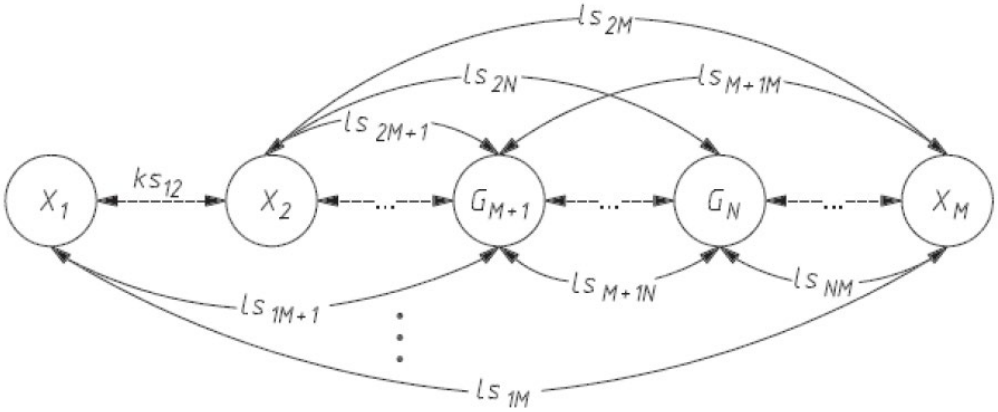
$LS=\{ls_{KL}|k=1..N, L=1..N\}$,
мұнда *LS* – желілік деңгейдегі объектілердің көптеген байланыс сызықтары.

Граф көмегімен ұсынылған проекциядағы ақпараттық жүйенің желілік деңгейдегі моделі 2-суретте көрсетілген.



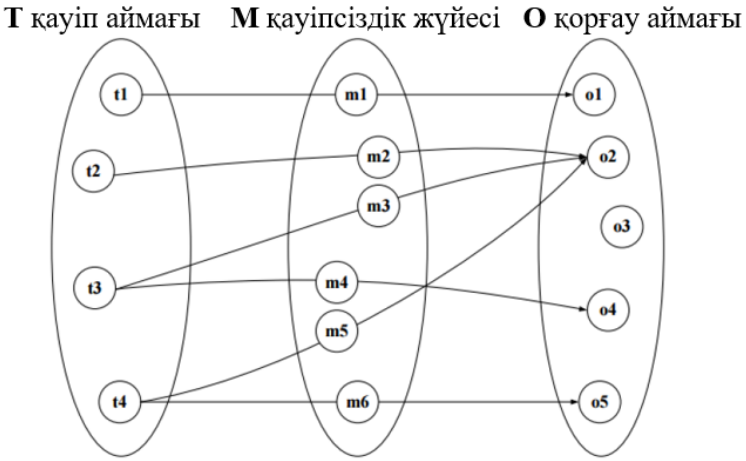
2-сурет. OSI желілік деңгейіне проекциядағы граф моделі

OSI моделінің физикалық және желілік деңгейлеріне проекциядағы объектілердің өзара әрекеттесу моделі 3- суретте көрсетілген.



3-сурет. OSI физикалық және желілік деңгейлеріне проекциядағы граф моделі

Королёва О.Ю., өз жұмысында ақпараттық қауіпсіздік жүйесін сипаттау үшін 4-суретте берілген үш жақты граф моделін қолданған [8]. Қауіп-объект қатынастар жиыны екі жақты графикті {T, O} құрайды. M үшінші жиынын енгізу бағандағы барлық мүмкін беттерді жабады. Нәтижеде -S= {T, M, O} үш жақты граф моделі құрылады.

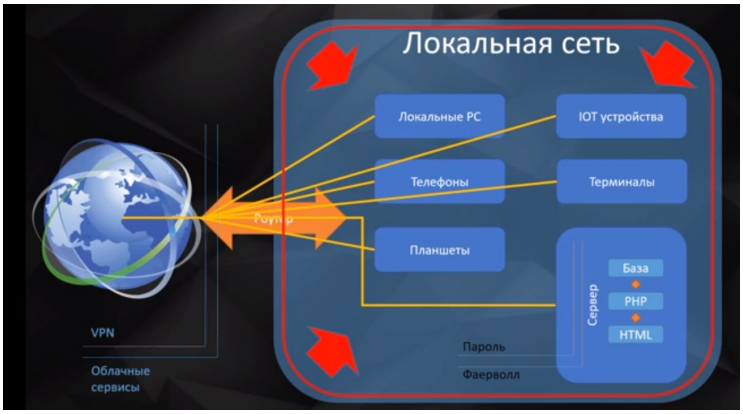


4-сурет. Ақпараттық қауіпсіздікті қамтамасыз ету жүйесінің граф моделі

Ақпараттық қауіпсіздік туралы мәліметтер нормативтік құжаттардан және ақпаратты қорғау мәселелерімен айналысатын компаниялардың зерттеулері мен есептерінен алынады [9, 10].

Бүгінде компьютерлік желінің қауіпсіздігін анықтаудың бірнеше әдістері бар. Қарапайым әдістің бірі ретінде – Nessus Vulnerability Scanner негізінде желінің осалдығын анықтау жолдарын қарастырдық. Желі осалдығын анықтаудың негізгі мақсаты – желіні қорғаудағы әлсіз буынды анықтау [11].

5-суреттегі желі мысалында, роутер арқылы бүкіләлемдік байланысқа шығамыз, сонымен қатар, барлық ішкі құрылғылар өзара ешқандай құпия сөздерсіз (пароль) байланыс жасай алады.

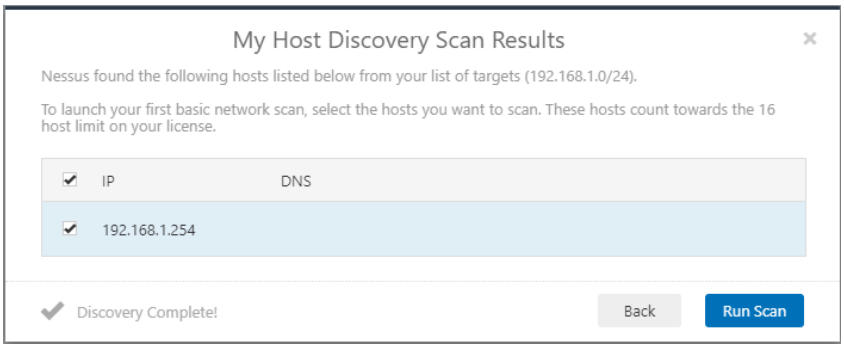


5-сурет. Локальды желі байланысы [12]

Осалдықты анықтаудағы міндеттер:

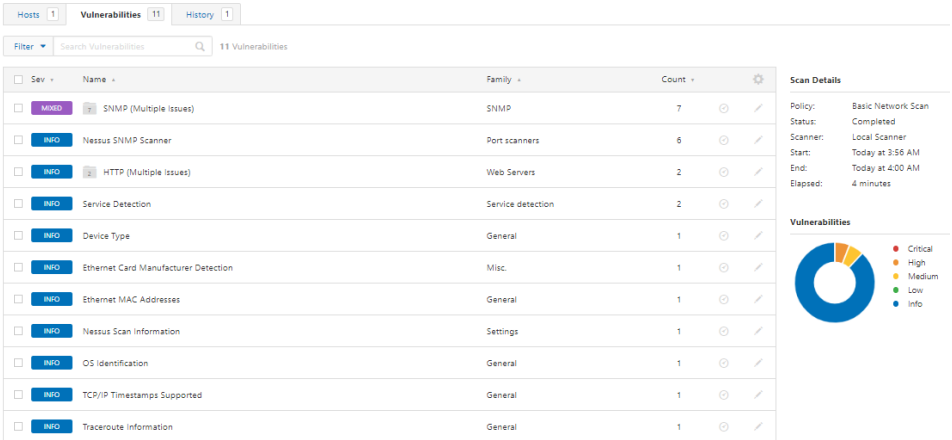
- желілік инфрақұрылымда, бағдарламалық және аппараттық құралдарда, қосымшаларда кездесетін осалдықтарды анықтау;
- анықталған «қауіпсіздік саңылауларының» гипотетикалық сценарийінің салдарын түсіндіру;
- анықталған қатерлермен күресу стратегиясын әзірлеу;
- компанияның қауіпсіздігін жақсарту және қауіпсіздік тәуекелдерін жою бойынша ұсыныстар беру.

Nessus Vulnerability Scanner толықтай орнатылғаннан соң ашылған сұқбаттық терезеде 192.168.1.0/24 IP адресінің барлық ішкі желісін сканерлейміз.



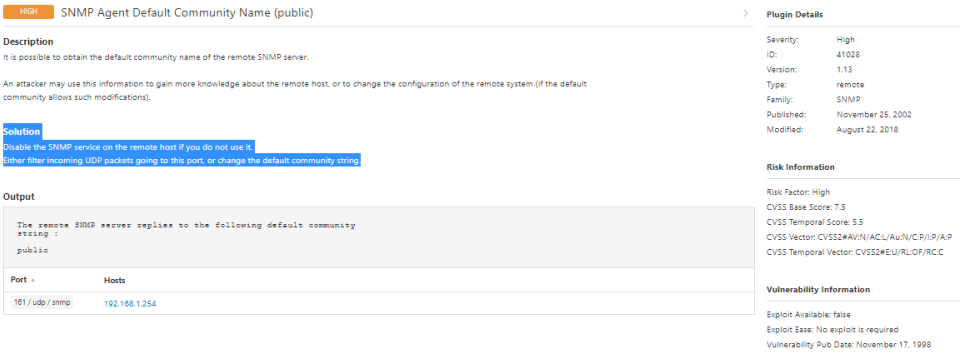
6 – сурет. Ішкі желіні сканерлеу [11]

Сканерлеу нәтижелері бойынша біз IP адрестер тізімін және осы адрестерге байланысты осалдықтарды аламыз. Осалдықтар түрлі түстермен берілген (7-сурет).



7-сурет. Сканерлеу нәтижесінде анықталған осалдықтар

Қажетті осалдықты белгілей отырып толық ақпарат алуға болады және осы есепті қалаған форматта сақтай аламыз. Мысалы, SNMP Agent Default Community Name (public) осалдығына берілген талдау және осалдықты жою жолдары 8 - суретте көрсетілген.



8-сурет. Анықталған осалдыққа талдау

Қорытынды

Мақалада OSI моделінің физикалық, арналық және желілік деңгейіндегі таратылған есептеу жүйесі объектілерінің өзара әрекеттесуін сипаттайтын бағытталған графты қолдана отырып жасалған ақпараттық жүйенің моделі берілген.

Қолданылуы қарапайым Nessus Vulnerability Scanner негізінде желінің осалдығын анықтау әдісі келтірілді. Nessus Vulnerability Scanner осалдықты анықтаудағы үздік сканер болып табылады. Басты артықшылығы – деректер базасындағы қауіпті моделдер негізінде желіні тез әрі сапалы тексереді.

Әдебиеттер

1. Загинайлов Ю.Н. Теория информационной безопасности и методология защиты информации: учебное пособие // Ю. Н. Загинайлов. – М. Берлин: Директ-Медиа, 2015. – 253с.

2. Бова В.В. Концептуальная модель представления знаний при построении интеллектуальных информационных систем // Известия ЮФУ. Технические науки. – 2014. – № 7 (156). – С. 109–117.

3. Коломейцева А.Д., Загинайлов Ю.Н. Разработка концептуальной модели системы защиты государственной информационной системы // Анализ современных тенденций развития науки: сборник статей Международной научно - практической конференции, Волгоград, 5 июля 2017 г. – Уфа: АЭТЕРНА. В 2 частях. – Ч.1 – С. 41–44.

4. Симонова М.В., Атрощенко В.А. Особенности построения различных алгоритмов и функциональных моделей в системе мониторинга умного дома // VII международная научно-практическая конференция молодых ученых, посвященная 56-й годовщине полета Ю.А. Гагарина в космос: Сборник научных статей, Краснодар, 12-13 апреля 2017 г. - Краснодар: Общество с ограниченной ответственностью "Издательский Дом - Юг". – С. 420–424.

5. Shangytbayeva G. A., Karpinski M. P., Akhmetov B. S., Yerekesheva M. M. Zhekambayeva M. N. Mathematical Model of System of Protection of Computer Networks against Attacks DOS/DDOS [Электронный ресурс]. – Режим доступа: https://doi.org/10.5539/mas.v9n8p106, свободный (дата обращения: 31.08.2020 г.).

6. Новохрестов А.К. Модель угроз информационной безопасности программного обеспечения компьютерных сетей на основе атрибутивных метаграфов. Диссер.канд. техн. Наук. - Томск, 2018. – 114 с.

7. BugTraq.Ru: Модели механизмов реализации типовых угроз безопасности РВС [Электронный ресурс]. – Режим доступа: https://bugtraq.ru/library/books/attack/chapter03/02.html?k=9, свободный (дата обращения: 31.08.2020 г.).

8. Королёва О.Ю. Модель и метод оценки эффективности системы обеспечения информационной безопасности корпоративного хранилища данных кредитных организаций Российской Федерации // Автореф. дис. канд. техн. наук [Электронный ресурс]. – Режим доступа: http://aspirantura.ifmo.ru/file/other/ktyaZl1TkI.pdf, свободный (дата обращения: 31.08.2020 г.).

9. СТ РК ISO/IEC 27013-2017. Информационные технологии. Методы и средства обеспечения безопасности. Руководство по интегрированному внедрению ISO/IEC 27001 и ISO/IEC 20000-1. [Электронный ресурс]. – Режим доступа: https://online.zakon.kz/Document/?doc_id=37992086#pos=0;0, свободный (дата обращения: 01.09.2020 г.).

10. KZ-CERT. Компьютерлік инциденттерге әрекет ету қызметі. [Электронды ресурс]. – https://cert.gov.kz, (01.09.2020 г.).

11. THE NESSUS FAMILY. [Электронный ресурс]. – https://www.tenable.com/products/nessus, (07.09.2020 г.).

12. Безопасность. Локальная сеть. [Электронный ресурс]. – https://www.youtube.com/watch?v=oLyo1FFQjKs, (07.09.2020 г.).

КРИПТОГРАФИЯЛЫҚ ХЕШ АЛГОРИТМДЕР ЖАСАУДЫҢ ӘРТҮРЛІ ЖОЛДАРЫН ҚАРАСТЫРУ

Сақан Қ.С.[1,2], Алғазы К.Т.[1,2]
e-mail: kairat_sks@mail.ru, kunbolat@mail.ru,
[1]ҚР БҒМ ҒК Ақпараттық және есептеуіш технологиялар институты, Қазақстан
[2]*Әл-Фараби атындағы Қазақ ұлттық университеті, Қазақстан*

Аңдатпа. *Қарастырылған жұмыста қазіргі ақпараттық технологиялар саласында өзекті мәселенің бірі болып саналатын ақпараттық қауіпсіздік жүйелерінің құрамдас бөлшегі болып есептелінетін хеш-функциялары жайында баяндалған. Оның негізгі функциясы, элементтері, әзірлеу барысындағы ерекшеліктер, сондай-ақ оны жасаудың алдағы уақыттағы негізгі бағыттары мен зерттеу жүргізу аясы көрсетілген.*

Түйінсөз. *Хеш-функция, хештеу алгоритмдері, коллизия, хеш алгоритмдеріне шабуыл, көпитерациялық хештеу.*

Кіріспе. Қазіргі таңда ақпараттың қауіпсіздігін қамтамасыз ету үшін хэш-функциялардың осал тұстарын одан әрі азайту жолдарын зерттеу мәселелері өте өзекті, өйткені қазіргі заманғы технологияның дамуы, есептеудің тиімді жолдарының ғылыми тұрғыда негізделе түсуі, есептеу құралдарының қуаты мен жылдамдығының тұрақты өсуі кезінде сәтті шабуылдардың өнімділігі де артып келеді. Сондықтан жоғары төзімділікті қажет ете отырып, жылдам есептеулер жүргізетін қарапайым хэш алгоритмдер әзірлеп шығару – заман талабының негізгі мәселелерінің бірі болып қалып отыр. Айта кететіні, белгілі MD5 және SHA топтамалары хэш функциялары анықталған осалдықтарға қарамастан, жоғары жылдамдыққа ие болуы себепті кейбір практикалық қосымшаларда әлі де қолданыла қала беріп отыр.

Негізгі терминдері, талаптары, қасиеттері, шабуыл жолдары. Криптографиялық хеш-функция – криптографиялық бағытта ақпаратты қорғау мақсатында пайдаланатын, ерекше қосымша қасиеттерге ие хеш-функциялардың классы. Ол ақпараттарды қорғауды, ақпараттардың негізгі меншік иесін анықтауды (аутентификациялау), ақпараттардың көшірмелерін табуды, зиянды бағдарламаларды анықтауды орындау үшін қолданылатын кең таралған математикалық аппарат ретінде қолданылады.

l_M биттік ұзындықтағы X ақпараты (хабарламасы) үшін l_h биттік ұзындықтағы қысылған біртекті h бейнесін

$$h = H(X)$$

хеш-функциясы арқылы анықтауға болады. Егерде h бейнесі $V_{\text{н}}$ бастапқы векторымен және/немесе K кілтінің қолданылуы арқылы алынатын болса,

$$h = H(X, V_{\text{н}}, K)$$

арқылы өрнектеледі.

Жақсы жасалынған хеш-функция мына қасиетттерге ие болу керек:

өзара анықталғандық. Бірдей кіріс хабарламалармен алынған хэш-функциясының нәтижелері бірдей болады (бірдей хабарлама әрқашан бірдей хэш мән береді);

кез-келген хабарлама үшін хэш функциясының мәнін жылдам есептеу мүмкіндігі;

көшкін әсерінің болуы, яғни хабарламалардағы өте аз өзгеріс өзгеріске дейінгі және өзгерістен кейінгі есептелінген хэш мәндер өте үлкен өзгеріс әкелуі керек;

коллизия санының аз болуы, яғни бірдей хэш мәндері бар екі түрлі хабарламаны оңай таба алмау.

Криптографиялық хэш-функция бірқатар талаптарды қанағаттандыруы керек [1-5]:

– прототипті есептеуге төзімділік – кез-келген алдын-ала берілген хэш-мәндері үшін белгісіз прототипті таба алмау мүмкіндігі, яғни берілген $h=H(X)$ хэш-функциясы үшін кез-келген X мәніне сәйкес алдын-ала берілген хэш мәні кезінде X белгісіз прототипін есептеп табу мүмкін емес;

– екінші прототипті есептеуге төзімділік – берілген хэш мәнін беретін кез-келген басқа прототипті таба алмау, яғни берілген h хэш-функциясы мен X прототипі үшін $H(X)=H(X')$ шарты орындалатын $X' \neq X$ басқа прототипін табу мүмкін еместігі;

– коллизияға қарсы төзімділік – бірдей мән шығарылатын екі прототипті таба алмау мүмкіндігі, яғни берілген h хэш-функциясы үшін $H(X)=H(X')$ шарты орындалатын X және X' екі прототипін табу мүмкін емес.

Криптографиялық хеш-функцияларына келесідегідей бағытта шабуылдар типтері жасалынады:

– берілген $h=H(X)$ мәні арқылы прототипті іздеу;

– берілген X арқылы $H(X)=H(X')$ шартын орындайтын X' прототипін іздеу арқылы.

Сонымен қатар хеш-функцияларды зерттеу барысында осы екі бағытта басты базалық шабуылдар ретінде төмендегі шабуылдарды қарастыруға болады:

«Дөрекі күш» әдісі негізіндегі шабуылы берілген хеш мәні бойынша алдыңғы прототипті табу үшін қолданылады. Шабуылдың мәні төмендегідей: кіріс хабарламаларын тізбектелген немесе кез-келген кездейсоқ ретте пайдалана отырып, оларды алдын-ала берілген хеш мәнімен салыстыра отырып қажетті прототипті іздеу мүмкіндігі. Бұндай шабуылдың күрделілігі хеш мәнді есептеуге кететін 2^{l-1} - операциялар санына тең, мұндағы l – хеш мәнінің ұзындығы.

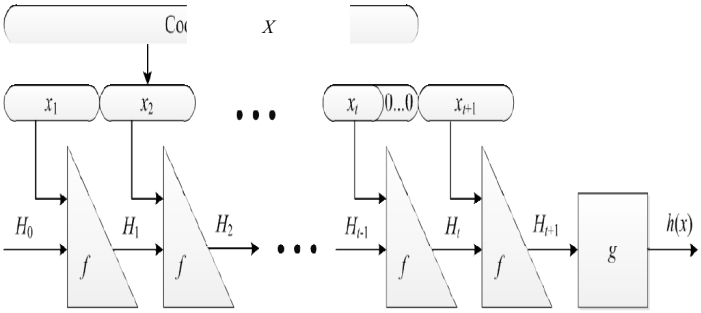
«Туған күндер» әдісі негізіндегі шабуылы – криптоталдауда туған күн парадоксы негізінде хеш-функциялардың коллизияларын іздеу әдісі үшін қолданылатын тәсіл. Былайша айтқанда, бір хеш мәнді беретін бір-бірінен өзгеше кіріс хабарламаларын табу. n_1 және n_2 элементттерден тұратын екі хеш мәндердің жиынында бір-біріне сәйкес келетін екі элементтің табылуының ықтималдылығы төмендегі формула бойынша табылады:

$$p \approx 1 - e^{\frac{n_1 n_2}{2}}.$$

Әдетте, «дөрекі күш» және «туған күндер» әдістерімен жасалынатын шабуылдарға тиімді қарсы тұру үшін хэш мәнін құру мақсатында қажетті операциялардың санын арттыруға мүмкіндік беретін көпитерациялы хэшті қолдану (көпитерациялы хештеу) пайдаланылады. Келесі кезекте, көпитерациялы хештеу жоғарғы аталған шабуылдарды жүргізудің мүмкіндіктерін қиындатады [6]. Көпитерациялы хештеудің негізі болып 1979 жылы Ральф Меркл әзірлеген құрылым болып есептелінеді. Қазіргі қолданыстағы көптеген хеш-функциялар, соның ішінде

SHA топтамасы, MD5, ГОСТ Р 34.11-94 стандарты осы принцип негізінде құрастырылған.

Меркл-Дамгард құрылымының жұмыс процессі кезекті итерациялық түрлендірудің кіріс мәндері ретінде хабарламаның кезекті бөлшегі (блогі) және алдыңғы итерацияның шығыс мәні қарастырылатын итерациялық процестен тұрады. Хабарлама X кіріс ұзындықтары бірдей t санындағы x_i блоктарға бөлінеді. Ескере кететіні, егер соңғы блок толық ұзындықта болмаса, ол қажетті ұзындықта қандайда бір алдын-ала белгіленген мәндермен толықтырылады. x_i блогының ұзындығы r-ге тең болсын. r блогының ұзындығы f қысу функциясының кіріс блогының ұзындығына сәйкес келуі керек. Әдетте, $(t+1)$-ші блокта X хабарламасының ұзындығы және H_0 – инициализация векторы жайында ақпарат қамтылады. Меркл-Дамгард құрылымының сызбасы 1-суретте көрсетілген.



1-сурет. Меркл-Дамгард құрылымы

Симметриялы шифрлау алгоритмдері негізінде құрастырылған хеш-функцияны құрастырудың бір жолы

Іс жүзінде симметриялық шифрлау алгоритмдерін хеш алгоритмі негізінде қарастыру барысында негізгі құрылымдық моменті ретінде шифрблоктардың бір-біріне тіркелу режимдерін пайдалануға болады. DES, IDEA, ГОСТ-28147 шифрлеу стандарттарындағы криптографиялық түрлендірулер біршама хеш-функциялардың жасалуының негізін қалады. 1-суретте көрсетілген f сығу функциясы ретінде шифрлау алгоритміндегі криптографиялық примитивтерді қарастыратын боламыз. Жалпы жағдайда 1-суреттегі сызбадағы x_i-лер орнында хабарламаның шифрлеу алгоритміндегі блок ұзындығына тең етіп алынған кезекті блоктар, ал H_i-лер орнында шифрлеу кілттері мен алдыңғы итерациядан алынған хеш мәндерінен құралған кіріс мәндер қарастырылады: $H_i = f(x_i, H_{i-1}),\ i = \overline{1..t}$. Осындай жолмен жасалынған хеш-функциялардың жұмыс істеу жылдамдығы мен төзімділігі қолданылған шифрлау алгоритмінің осы сипаттамаларымен сәйкес келеді. Алайда, бұл барлық жағдайда орындала бермейді. Блоктік шифрлауды пайданып шифрленген хабарламаларды дешифрлеуден гөрі осы блоктік шифрлеу алгоритмін қолданып жасалған хеш мәндерге криптоталдау жүргізу оңай жолмен жүзеге асырылады [7].

Алдағы уақыттағы жұмыстың бағыты Меркл-Дамгард құрылымын пайдаланып, хеш-функцияларды жасау барысында зерттелетін бағыт болып f шифрлау алгоритмін позициялық емес полиномиалды санау жүйесінде қарастыру болып табылады. Қарастырылатын $GF(2^n)$ ақырлы өрісінде $p_1(x), p_2(x), \dots, p_s(x)$ - екілік коэффициентті келтірілмейтін көпмүшеліктер жұмыс негіздері ретінде алынатын болады, ал N хабарламасын екілік коэффициентті $N(x)$ көпмүшелігі

ретінде өрнектейтін боламыз. m_i – $p_i(x)$ көпмүшеліктерінің дәрежелері болсын. Сонда $m = m_1 + m_2 + \cdots + m_s$ дәрежелі $P(x) = p_1(x) \cdot p_2(x) \cdots p_s(x)$ көпмүшелігі позициялық емес полиномиалды санау жүйесінде негізгі жұмыс диапазоны болып есептелінеді. $\alpha_i = N(x) \, mod \, p_i(x), i = \overline{1..s}$ ескерсек, $N(x)$ көпмүшелігі мынандай түрде жазыла алады: $N(x) = \left(\alpha_1(x), \alpha_2(x), \ldots, \alpha_s(x)\right)$ [8].

Әрі қарай, қытайдың қалдықтар туралы теоремасын ескере отырып, N хабарламасын түрлендіруде келесідегілей формулаларды пайдаланатын боламыз:

$N(x) = \sum_{i=1}^{s} \alpha_i(x) \cdot B_i(x)$, мұндағы

$B_i(x) = (\prod_{i=1}^{s} p_i(x))/p_i(x) \cdot M_i(x) \equiv 1(mod \, p_i(x))$,

ал $M_i(x)$ осы тепе-теңдік орындалатындай етіп таңдалып алынатын көпмүше.

Хеш-функциясын жасау кезіндегі ерекшелік – шифрлау алгоритмдеріндегідей кері шифрлеу процедурасын қарастыруды қажетсінбейді. Сол себепті, позициялық емес полиномиалды санау жүйесінде кері орнына келтірудің формулаларын қарастырмайтын боламыз.

Қорытынды. Алдағы ғылыми жұмыстарда хеш-функцияларды жасау барысында позициялық емес полиномиалды санау жүйесінде блокті шифрлеу алгоритмдерін зерделейтін боламыз. Алынған теориялық және тәжірибелік нәтижелерді ескере отырып, хеш-функциялардың негізгі қасиетттерімен оларға қойылатын талаптарды қанағаттандыратындай тиімді жолдарды іздестіреміз. Осы мақсатты кіретін параметрлерді мен f шифрлау алгоритмінің криптографиялық примитивтерін тиісінше өзгерте отырып жүзеге асырамыз. Сонымен қатар, ҚР БҒМ ҒК ақпараттық және есептеуіш технологиялар институтының «Ақпараттық қауіпсіздік» зертханасында әзірленген әртүрлі шифрлеу алгоритмдерін де (соның ішінде Qamal, AL01, EM шифрлеу алгоритмдерін) қажетті өзгерістер енгізе отырып, хеш-функцияларды жасау кезінде қолданылатын боламыз.

Әдебиет:

1. Вервейко В.Н., Пушкарев А.И., Цепурит Т.В. Функции хэширования: классификация, характеристика и сравнительный анализ. – http://bezopasnik.org/article/book/94.pdf. (қарау күні: 01.09.2020).
2. Schneier B. One-Way Hash Functions // Dr. Dobb's journal. 1991. vol. 16. no. 9. 148–151.
3. Biham E., Shamir A. Differential cryptoanalysis of FEAL and NHash // In Advances in Cryptology (Eurocrypt ’91). 1990. pp. 1–16.
4. Biham E. On the Applicability of Differential Cryptoanalysis to Hash Functions // In E.I.S.S Workshop on Cryptographic Hash Functions. 1992. pp. 25–27.
5. Quisquater J.-J., Delescaille J.-P. How Easy is Collision Search. New results and applications to DES // In Advances in Cryptology (CRYPTO’89). 1990. vol. 435. 408–415.
6. Лёвин В.Ю. О повышении криптостойкости однонаправленных хеш-функций / Фундаментальная и прикладная математика. 2009. Т. 15:5. С. 171–179.
7. Горбенко И.Д., Штанько И.А. Горбенко Иван Дмитриевич, Штанько Игорь Анатольевич Функции хеширования. Понятия, требования, классификация, свойства и применение // Радиоэлектроника и информатика. 1998. №1 (2). – https://cyberleninka.ru/article/n/funktsii-heshirovaniya-ponyatiya-trebovaniya-klassifikatsiya-svoystva-i-primenenie (қарау күні: 01.09.2020).

8. Amerbayev V.M., Biyahev R.G., Nyssanbaeva S.E. Use of nonpositional notations in cryptographic protection // Izv National Academy of Scienes Resp. Kazakhstan, Series Phisical Materials, 2005, (3), 84-89.

ПРИНЦИПЫ ПОСТРОЕНИЯ БЛОЧНЫХ ШИФРОВ И ТРЕБОВАНИЯ К НИМ

К. Алгазы, К. Сакан
e-mail: kunbolat@mail.ru, kairat_sks@mail.ru
Институт информационных и вычислительных технологий КН МОН РК, Казахстан

Аннотация: *Современные криптосистемы можно однозначно разделить по способу использования ключей на криптосистемы с секретным ключом и с открытым ключом. Если для зашифрования и расшифрования используется один и тот же ключ, такая криптосистема называется симметричной. К современным алгоритмам блочного шифрования предъявляют достаточно жесткие требования, связанные с областью применения, возможностью реализации на различных вычислительных платформах и другими факторами.*

Ключевые слова: *криптография, блочные шифры, S-блок, сеть Фейстеля, хэширование.*

Введение

К симметричным криптосистемам относятся DES, AES, ГОСТ 28147-89 и т.д. Новым направлением в криптографии стало изобретение асимметричных криптосистем с открытым ключом, таких, как RSA, DSA или Эль-Гамаль.

Практика показала, что чем больше известен алгоритм, чем больше людей работало с ним, тем более проверенным, а значит, и надежным он становится. Так, публично известные алгоритмы сейчас выдерживают борьбу со временем, а вот засекреченные государственные шифры обнаруживают в себе множество ошибок и недочетов, т. к. всего учесть невозможно[1-4].

Общепринятая схема построения симметричных криптосистем представляет собой циклические перестановки и подстановки битов в блоке фиксированной длины, алгоритм которых определяется секретным ключом. В таблице 1 приведен современные симметричные методы шифрования.

Таблица 1. Обзор симметричных методов шифрования

Метод	**Длина ключа, бит**	**Размер блока, бит**	**Затраты на подбор ключа, х лет**	**Примечание**
DES	56	64	$5\ 10^2$	Разработан в 1977 г. фирмой IBM. За 20 лет не найдено способа взломать шифр, кроме полного перебора в среднем 25% всех ключей, но при современных возможностях он позволяет достичь успеха
Triple DES	128 (112)	64	10^{18}	Трехкратное повторение алгоритма DES с разными ключами. Эффективная длина ключа 112 бит.

IDEA	128	64	10^{21}	Разработан в 1992 г. Lai и Massey. Не взломан до настоящего времени
ГОСТ 28147-89	256	64	нет данных	Является Государственным стандартом в России
Blowfish	до 448	64	нет данных	Разработан Шнайером (Schneier) в 1993 г. Это шифр Файстела был создан специально для 32-битовых машин и существенно быстрее DES
AES (Rijndael)	Длина ключа и длина блока могут быть 128, 192 или 256 бит, независимо друг от друга			Предложен криптоаналитиками Joan Daemen и Vincent Rijmen. Алгоритм не имеет известных слабостей в защите (по данным NIST).

Принципы построения блочных шифров.

Блочные криптосистемы разбивают текст сообщения на отдельные блоки и затем осуществляют преобразование этих блоков с использованием ключа. Согласно работам Шеннона, к современным блочным шифрам выдвигают следующие требования [5, 6]:

- *рассеивание* информации – распространение влияния одного знака открытого текста на почти все знаки шифротексты. Это затрудняет статистический анализ и не позволяет восстановить ключ по частям;
- *перемешивание* информации для усложнения зависимости между ключом и шифрованным текстом.

Схемы, решающие такие задачи, называют *SP - сетями* (от первых букв англ. substitution – подстановка и permutation – перестановка).

Основные операторы блоковых шифров:

1) операторы перестановки, называемые *P* -боксами;
2) операторы подстановки, называемые *S* -боксами;
3) операция исключающего ИЛИ;
4) циклический сдвиг;
5) замена;
6) разбиение и объединение блока.

Комбинация этих операторов в современных шифрах позволяет рассеять и перемешать информацию.

В отличие от шифроблокнота, где длина ключа равна длине сообщения, блочный шифр способен зашифровать одним ключом одно или несколько сообщений, суммарной длиной больше, чем длина ключа. Передача малого по сравнению с сообщением ключа по зашифрованному каналу — задача значительно более простая и быстрая, чем передача самого сообщения или ключа такой же длины, что делает возможным его повседневное использование. Однако, при этом шифр перестает быть не взламываемым. От поточных шифров работа блочного отличается обработкой бит группами, а не потоком. При этом блочные шифры надёжней, но медленнее поточных. Симметричные системы обладают преимуществом над асимметричными в скорости шифрования, что позволяет им оставаться актуальными, несмотря на более слабый механизм передачи ключа (получатель должен знать секретный ключ, который необходимо передать по уже налаженному зашифрованному каналу. В то же время, в асимметричных шифрах открытый ключ, необходимый для шифрования, могут знать все, и нет необходимости в передачи ключа шифрования).

К достоинствам блочных шифров относят сходство процедур шифрования и расшифрования, которые, как правило, отличаются лишь порядком действий. Это упрощает создание устройств шифрования, так как позволяет использовать одни и те же блоки в цепях шифрования и расшифрования. Гибкость блочных шифров позволяет использовать их для построения других криптографических примитивов: генератора псевдослучайной последовательности, поточного шифра, имитовставки и криптографических хэшей.

Сеть Фейстеля

Раунд, организованный по сети Фейстеля имеет следующую структуру. Входной блок делится на несколько частей равной длины. Эти части блока называются ветвями. Так, например, если блок имеет длину 64 бита, используются две ветви по 32 бита каждая. Ветви обрабатываются по отдельности, после чего осуществляется циклический сдвиг всех ветвей влево. В случае двух ветвей каждый раунд имеет структуру, показанную на рис 1.

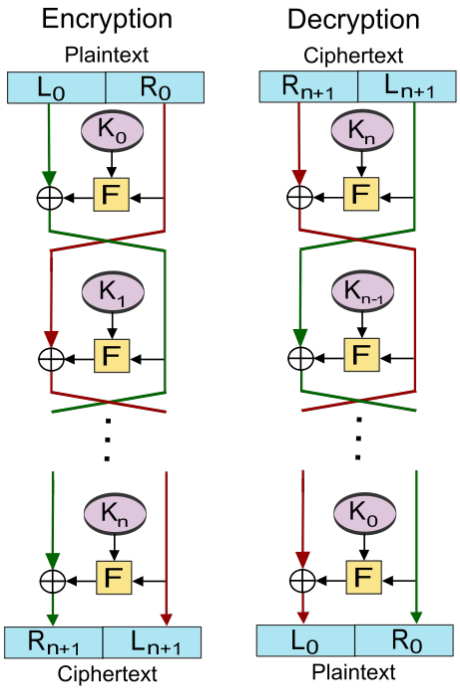


Рис. 1 – Структура сети Фейстеля

В последнее время все чаще используются различные разновидности сети Фейстеля для 128-битного блока с четырьмя ветвями. Увеличение количества ветвей, а не размерности каждой ветви связано с тем, что наиболее популярными до сих пор остаются процессоры с 32-разрядными словами, следовательно, оперировать 32-разрядными словами эффективнее, чем с 64-разрядными.

Свойства сети Фейстеля:

1. Сеть Фейстеля можно сконструировать так, что для зашифрования и расшифрования будет использоваться один и тот же алгоритм – отличие между этими операциями будет состоять лишь в порядке применения раундовых ключей; такое свойство алгоритма наиболее полезно при его аппаратной реализации или на платформах с ограниченными ресурсами.

2. В одном раунде меняется только половина битов блока -> для стойкости шифра надо увеличивать число раундов.

Требования к блочному алгоритму шифрования

К современным алгоритмам блочного шифрования предъявляют достаточно жесткие требования, связанные с областью применения, возможностью реализации на различных вычислительных платформах и другими факторами [7, 8]. Рассмотрим основные из требований.

1. Алгоритм должен обеспечивать высокий уровень стойкости, и эта стойкость не должна основываться на сохранении втайне самого алгоритма.
2. Незначительное изменение исходного сообщения должно приводить к существенному изменению зашифрованного сообщения даже при использовании одного и того же ключа.
3. Алгоритм должен успешно противостоять атакам по выбранному тексту, то есть таким, чтобы нельзя было узнать ключ, даже зная достаточно много пар (зашифрованное сообщение, незашифрованное сообщение), полученных при шифровании с использованием данного ключа.
4. Алгоритм шифрования должен иметь возможность быть реализованным на различных платформах, которые предъявляют различные требования. Для наиболее быстрых приложений используется специальная аппаратура. Несмотря на это, программные реализации применяются также достаточно часто. Поэтому алгоритм должен допускать эффективную программную реализацию на универсальных микропроцессорах. Алгоритм должен также работать на микроконтроллерах и других процессорах среднего размера.
5. Алгоритм должен использовать простые операции, которые эффективны на микропроцессорах, т.е. исключающее или, сложение, табличные подстановки, умножение по модулю. Не должно использоваться сдвигов переменной длины, побитных перестановок или условных переходов.
6. Алгоритм должен эффективно реализовываться на специализированной аппаратуре, предназначенной для выполнения операций шифрования и расшифрования, то есть реализация алгоритма в виде электронных устройств должна быть экономичной.
7. Алгоритм шифрования должен быть применим во многих приложениях. Алгоритм должен быть эффективен при шифровании файлов данных или большого потока данных, при создании определенного количества случайных битов, а также должна быть возможность его использования для формирования односторонней хеш-функции[1].
8. Алгоритм должен быть простым для написания кода, чтобы минимизировать вероятность программных ошибок. Также это дает возможность анализа и уменьшает закрытость алгоритма.
9. Алгоритм должен допускать любую случайную строку битов нужной длины в качестве возможного ключа (это называется *иметь плоское пространство ключей*). Не должно быть "слабых" ключей, облегчающих криптоанализ.
10. Алгоритм должен легко модифицироваться для различных уровней безопасности и удовлетворять как минимальным, так и максимальным требованиям.

Проектирование S блоков .

Выбор хороших S-блоков - не простая задача, существует множество различных идей, как лучше сделать это. Можно выделить четыре главных подхода [9].

1. Случайно выбрать. Ясно, что небольшие случайные S-блоки небезопасны, но большие случайные S-блоки могут оказаться достаточно хороши. Случайные S-блоки с восемью и более входами достаточно сильны. Еще лучше 12-битовые S-блоки. Устойчивость S-блоков возрастает, если они одновременно являются и случайными, и зависящими от ключа. В IDEA используются большие зависящие от ключа S-блоки.

2. Выбрать и проверить. В некоторых шифрах свойства S-блоков, генерированных случайным образом, проверяются.

3. Разработать вручную. При этом математический аппарат используется крайне незначительно: S-блоки создаются с использованием интуитивных приемов. Барт Пренел (Bart Preneel) заявил, что "... теоретически интересные критерии недостаточны [для выбора булевых функций S-блоков] ...", и что "... необходимы специальные критерии проектирования" .

4. Разработать математически. S-блоки создаются в соответствии с математическими законами, поэтому они обладают гарантированной надежностью по отношению к дифференциальному и линейному криптоанализу, а также хорошими диффузными свойствами.

Существует ряд призывов объединить "математический" и "ручной" подходы, но реально, по-видимому, конкурируют случайно выбранные S-блоки и S-блоки с определенными свойствами. Конечно преимуществом последнего подхода является оптимизация против известных методов вскрытия - дифференциального и линейного криптоанализа - но обеспечиваемая этим подходом степень защиты от неизвестных методов вскрытия также неизвестна. Разработчикам DES было известно о дифференциальном криптоанализе, и его S-блоки были оптимизированы соответствующим образом. Скорее всего, о линейном криптоанализе они не знали, и S-блоки DES очень слабы по отношению к такому способу вскрытия. Случайно выбранные S-блоки в DES были бы слабее против дифференциального криптоанализа, но сильнее против линейного криптоанализа.

С другой стороны случайные S-блоки могут не быть оптимальными по отношению к данным способам вскрытия, но они могут быть достаточно большими и, следовательно, достаточно надежными. Кроме того, они, скорее всего, будут достаточно устойчивы и против неизвестных способов вскрытия. Спор все еще кипит, но лично мне кажется, что S-блоки должны быть такими большими, насколько это возможно, случайными и зависеть от ключа.

Заключение

Общепринятым подходом в криптографии считается такое построение шифра, при котором его секретность определяется только секретностью ключа K_S (правило Керкоффа). Таким образом, шифр должен быть устойчивым к взлому, даже если потенциальному криптоаналитику известен весь алгоритм шифрования, кроме значения используемого ключа, и он располагает полным текстом перехваченной шифрограммы.

В блочных алгоритмах, построенных на основе сети Фейстеля, основной операцией является вычисление образующей функции F. Эта функция использует подключ раунда и одну ветвь входного блока для вычисления результата. Именно тем, как определяется функция F, системы шифрования и отличаются друг от друга.

В некоторых алгоритмах введены также начальные преобразования входного блока данных, придающие некоторую "случайность" входному тексту (это называется *рандомизацией* данных.) Рандомизация производится для того, чтобы уменьшить естественную избыточность входного сообщения.

Сила большинства сетей Фейстела - и особенно их устойчивость к дифференциальному и линейному криптоанализу - непосредственно связана с их S-блоками. Это явилось причиной потока исследований, что же образует хороший S-блок.

Литература

1. Б. Шнайер, Прикладная криптография, 2-е изд: Пер. с англ. –Триумф, 2002. – 816 с.
2. В. Столлингс, Криптография и защита сетей: принципы и практика. 2-е изд./Пер. с англ. – М: Вильямс, 2001, - 672 с.
3. Л.К. Бабенко, Е.А. Ищукова. Современные алгоритмы блочного шифрования и методы их анализа // Москва. Гелиос АРВ – 2006, - 376 с.
4. М.А. Иванов Криптографические методы защиты информации в компьютерных системах и сетях. М.:КУДИЦ-ОБРАЗ, 2001-368 с.
5. Габидулин Э.М., Кшевецкий А.С., Колыбельников А.И., Владимиров С.М., Защита информации, учебное пособие — М.: МФТИ, 2011. — 225 с.
6. K. Nyberg. Differentially uniform mappings for cryptography. Advances in cryptology – Eurocrypt'93, Springer-Verlag, Berlin, 1993.
7. Гатченко Н.А., Исаев А.С., Яковлев А.Д. «Криптографическая защита информации» – СПб: НИУ ИТМО, 2012. – 142с.
8. Ященко В. В., Введение в криптографию, 4-е изд., доп. М.: МЦНМО, 2012. - 348 с.
9. Токарева Н. Н. Симметричная криптография, НГУ, Новосибирск, 2012. - 234 с.

РЕГЛАМЕНТАЦИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ФИНАНСОВОМ СЕКТОРЕ РК

Айтхожаева Е.Ж., Жоламан Б.Р.
E-mail: ait_djam@mail.ru, 13olkproduction@gmail.com
Satbayev University/Казахский Национальный Технический Университет имени К.И.Сатпаева, Алматы, Казахстан

Аннотация. *Отмечается основополагающая роль международных и национальных стандартов в определении требований к обеспечению информационной безопасности, в том числе и в финансовом секторе. Особое внимание уделяется стандартам ISO/IEC 27001 и ISO/IEC 27002 из системы стандартизации ISO/IEC 27k на системы управления информационной безопасности, а также ISO/IEC 15408. Делается акцент на нормативные правовые акты основных регуляторов финансовой отрасли – НБРК и АРРФР. Отмечается необходимость разработки методологии обеспечения информационной безопасности финансового сектора Республики Казахстан для обеспечения*

системного подхода к информационной безопасности критичных инфраструктур финансовой отрасли.

Ключевые слова: *стандарты информационной безопасностью, нормативные правовые акты финансового сектора.*

Введение. При решении проблем информационной безопасности (ИБ) первостепенное значение имеют вопросы регламентации. Особенно это важно в отношении объектов критичной информационно-коммуникационной инфраструктуры, нарушение функционирования которых приводит к чрезвычайным ситуациям, представляющим угрозу национальной безопасности. К таким объектам относится большинство объектов финансовой отрасли, успешное функционирование которых напрямую зависит от безопасности информационно-коммуникационной инфраструктуры.

Банки всегда были в фокусе внимания злоумышленников. А использование информационно-коммуникационных технологий (ИКТ) определило тренд постоянного роста объема финансовых средств в киберпространстве, что повышает вероятность рисков ИБ.

Цель международных стандартов в области ИБ состоит в том, чтобы продвигать передовые методы и практики обеспечения информационной безопасности, наработанные мировым сообществом. Национальные стандарты по ИБ обычно разрабатываются путем гармонизации и адаптации международных стандартов, с сохранением оригинального шифра и названия стандарта.

В 2017 году постановлением Правительства Республики Казахстан была утверждена Концепция кибербезопасности («Киберщит Казахстан»), составленная с учетом текущей обстановки в области кибербезопасности, в том числе в финансовом секторе [1]. В соответствии с Концепцией, Национальный Банк Республики Казахстан (НБРК) и Агентство Республики Казахстан по регулированию и развитию финансового рынка (АРРФР), учитывая отраслевые и международные требования, должны обеспечивать нормативными правовыми актами требования по ИБ банковских информационных систем.

Международные и национальные стандарты. Комитет ISO/IEC JTC 1/SC 27 на постоянной основе разрабатывает семейство международных стандартов на Системы Управления (Менеджмента) Информационной безопасностью (СУИБ или СМИБ) ISO/IEC 27k [2]. Наиболее известными и применяемыми являются стандарты ISO/IEC 27001 и ISO/IEC 27002. Данные стандарты содержат требования по созданию, внедрению, поддержанию и постоянному совершенствованию системы управления ИБ (ISO/IEC 27001) и практические правила управления ИБ (ISO/IEC 27002 – критерии для оценки механизмов безопасности организационного уровня), применимы для любых видов деятельности, типов и масштаба организаций. Такие отрасли, как банковская деятельность, финансы, страхование широко используют данные стандарты.

В Казахстане оба эти стандарта гармонизированы и адаптированы, наряду со стандартом ISO/IEC 27000 (СТ РК ISO/IEC 27000-2019), посвященному общему обзору и словарю семейства стандартов ISO/IEC 27k:

– Государственный стандарт Республики Казахстан СТ РК ИСО/МЭК 27001-2015. Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования;

– Государственный стандарт Республики Казахстан СТ РК ИСО/МЭК 27002-2015. Методы обеспечения защиты. Свод правил по управлению защитой информации.

Информационная безопасность банков начинается с аудита. В настоящее время аудит информационных технологий (ИТ) и системы управления информационной безопасностью (СУИБ) практически всегда является дополнением к финансовому аудиту. В семейство международных стандартов ISO/IEC 27k входят стандарты, содержащие требования к органам аудита и сертификации СУИБ:

– ISO/IEC 27006:2015 Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems. Аналогичный гармонизированный стандарт РК – СТ РК ISO/IEC 27006-2017 «Информационные технологии. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности»;

– ISO/IEC 27007:2020 Information security, cybersecurity and privacy protection – Guidelines for information security management systems auditing (Руководство по проведению аудита систем менеджмента информационной безопасности (СМИБ)), содержит рекомендации по эффективному аудиту СМИБ;

– ISO/IEC 27008:2019 Information technology – Security techniques – Guidelines for auditors on information security controls (Руководство для аудиторов средств управления информационной безопасностью).

Американским Институтом Сертифицированных Публичных Бухгалтеров (American Institute of Certified Public Accountants (AICPA)) и Канадским Институтом Общественных Бухгалтеров (Canadian Institute of Chartered Accountants (CICA)) был разработан стандарт SysTrust для проведения ИТ аудита, который является дополнением к финансовому аудиту. SysTrust содержит требования для оценки надежности и безопасности информационных систем, которые используются финансовыми аудиторами при проведении финансового аудита. Данный стандарт отражает бухгалтерское видение проблемы ИБ.

В РК гармонизирован также международный стандарт ISO/IEC 15408 "Common Criteria for Information Technology Security Evaluation" (3 части), в котором представлены критерии для оценки механизмов безопасности программно-технического уровня. Общие критерии оценки безопасности информационных технологий определяют функциональные требования безопасности (security functional requirements) и требования к адекватности реализации функций безопасности (security assurance requirements).

Государственный стандарт Республики Казахстан на основе ISO/IEC 15408 введен в действие в 2017 году:

– СТ РК ИСО/МЭК 15408-1. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель;

– ИСО/МЭК 15408-2. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности;

– ИСО/МЭК 15408-3. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности.

Для хищения финансовых средств все активнее используются дистанционные финансовые услуги, онлайн-банкинг. Переход на технологии 5G только усугубит ситуацию с угрозами. Международный Совет по стандартам безопасности индустрии платежных карт (Payment Card Industry Security Standards Council, PCI SSC) разработал стандарт безопасности данных платежных карт PCI DSS – Payment Card Industry Data Security Standard. Требования стандарта обязательны для всех компаний, которые передают, хранят и обрабатывают в своих информационных системах данные о держателях платежных карт Visa и MasterCard, независимо от страны, формы собственности, типа организации и т.д. В стандарте определено более 200 требований по обеспечению безопасности этих данных, но количество выполняемых требований, проверяемых при обязательной сертификации, зависит от уровня организации. Уровень определяется в зависимости от количества транзакций, а требования к обязательной сертификации зависят от типа проверяемой организации.

Обыденным явлением в киберпространстве стали утечки персональных данных. Этой угрозе подвержены практически все организации и частные лица, но особенно она актуальна для сектора здравоохранения и финансового сектора. На противодействие этой угрозе направлен международный стандарт ISO/IEC 29151:2017 Information technology – Security techniques – Code of practice for personally identifiable information protection (Информационные технологии – Методы обеспечения безопасности – Свод практики по защите персональных данных).

В Республики Казахстан этот стандарт не адаптирован, но в 2013 году принят Закон Республики Казахстан «О персональных данных и их защите» (с изменениями и дополнениями по состоянию на 03.07.2020 г.).

В Европе с 2018 года действует общий регламент по защите персональных данных GDPR – General Data Protection Regulation (Регламент ЕС 2016/679), который применяется ко всем компаниям, обрабатывающим персональные данные резидентов и граждан Европейского союза, независимо от местонахождения такой компании.

Стратегия кибербезопасности финансового сектора Республики Казахстан. В соответствии с Указом Президента Республики Казахстан от 11 ноября 2019 года №203 «О дальнейшем совершенствовании системы государственного управления Республики Казахстан», НБРК реорганизован путем выделения из него АРРФР.

В этой связи, функции отраслевого центра информационной безопасности финансового рынка и финансовых организаций, а также функции проведения анализа информации об инцидентах информационной безопасности банков и организаций, осуществляющих отдельные виды банковских операций, включая сведения о нарушениях, сбоях в информационных системах переданы НБРК в АРРФР для их осуществления [3].

Государственное регулирование финансового рынка с 2020 года стало осуществляться двумя государственными органами – НБРК и АРРФР, что предопределяет их роль в регламентации ИБ финансового сектора Республики Казахстан. Ниже представлены основные нормативные правовые документы в этом направлении.

В 2001 году было принято постановление Правления НБРК №80 «Об утверждении Правил по обеспечению безопасности информационных систем банков второго уровня и организаций, осуществляющих отдельные виды

банковских операций». В этом постановлении были определены требования к ИБ банковских информационных систем.

В 2014 году в постановлении Правления НБРК №29 «Об утверждении Правил формирования системы управления рисками и внутреннего контроля для банков второго уровня» было введено понятие риска ИБ и закреплена необходимость в проведении его оценки. С 2015 года банки второго уровня представляют отчеты по понесенным убыткам, связанным с реализацией рисков информационной безопасности.

В настоящее время около 73% банков второго уровня Республики Казахстан предоставляют услуги мобильного банкинга для физических лиц. Развитие электронных банковских услуг привело к необходимости принятия в 2016 году Правлением НБРК постановления №34 «Об утверждении Требований к безопасности и беспрерывности работы информационных систем банков и организаций, осуществляющих отдельные виды банковских операций», в котором были определены требования по безопасности и непрерывности работы информационных систем банков для оказания электронных банковских услуг. С 2017 года ежеквартально банки второго уровня представляют отчеты о простоях информационной системы более одного часа.

В соответствии с Законом Республики Казахстан от 31 августа 1995 года «О банках и банковской деятельности в Республике Казахстан» в 2018 году было принято постановление Правления НБРК №47 «Об утверждении Правил и сроков представления банками сведений о наличии систем управления информационной безопасностью, а также о соблюдении требований к обеспечению информационной безопасности в Национальный координационный центр информационной безопасности». Правила устанавливают порядок и сроки представления банками сведений о наличии систем управления информационной безопасностью, а также о соблюдении требований к обеспечению информационной безопасности в Национальный координационный центр информационной безопасности.

В 2018 году в целях повышения уровня безопасности банковских операций и эффективности реагирования на инциденты было принято постановление Правления НБРК №48 «Об утверждении Требований к обеспечению информационной безопасности банков и организаций, осуществляющих отдельные виды банковских операций, Правил и сроков предоставления информации об инцидентах информационной безопасности, включая сведения о нарушениях, сбоях в информационных системах».

Имеются и другие нормативные правовые документы, регламентирующие ИБ в финансовом секторе Республики Казахстан.

По состоянию на 11 сентября 2020 года АРРФР разработал ряд проектов постановлений, направленных на повышение уровня обеспечения информационной безопасности финансового рынка Республики Казахстан, такие как:

– проект постановления Правления АРРФР «Об утверждении Требований к службам реагирования на инциденты информационной безопасности, проведению внутренних расследований инцидентов информационной безопасности». Данный проект постановления позволит систематизировать работу центров реагирования на инциденты ИБ крупных финансовых институтов, а также описывает необходимые процедуры этапов мониторинга, реагирования и проведения расследований инцидентов ИБ;

– проект постановления Правления АРРФР «Об утверждении требований к компетенциям руководителей и работников подразделений информационной безопасности, включая требования по повышению квалификации лиц, ответственных за обеспечение информационной безопасности». Требования содержат минимально необходимый перечень компетенций, знаний и навыков, необходимых для исполнения функциональных обязанностей работников финансовых организаций Республики Казахстан, задействованных в информационной безопасности.

В НБРК совместно с АРРФР утверждено совместное Постановление «Об утверждении Стратегии кибербезопасности финансового сектора Республики Казахстан на 2020-2022 годы» от 20 июля 2020 года (№89 НБРК, №69 АРРФР) (далее – Стратегия кибербезопасности). Стратегия кибербезопасности является основополагающим документом по информационной безопасности финансового сектора Республики Казахстан.

В Стратегии кибербезопасности определяется шесть основных направлений по созданию эффективной системы обеспечения кибербезопасности финансового сектора к 2022 году:

– совершенствование регулирования систем обеспечения кибербезопасности субъектов финансового рынка;

– развитие отраслевого центра информационной безопасности финансового рынка;

– кибербезопасность платежных систем, рынка платежных услуг и цифровых финансовых услуг;

– сотрудничество в сфере борьбы с киберпреступностью в глобальном масштабе;

– повышение уровня киберграмотности населения;

– совершенствование системы управления информационной безопасностью в НБРК и АРРФР [4].

Реализация Стратегии кибербезопасности позволит увеличить уровень и качество предупреждения, реагирования и устранения инцидентов ИБ финансового сектора Республики Казахстан.

К тем информационно-коммуникационным инфраструктурам в финансовом секторе, которые относятся к критичным (а таких большинство), применимы также и нормативные правовые документы РК, действующие в сфере ИБ для объектов критичной информационно-коммуникационной инфраструктуры.

Выводы. В 2019 году Казахстан вошёл в список стран с высоким уровнем готовности противостояния угрозам ИБ, имея 40 место из 193 стран мира в Глобальном индексе кибербезопасности. В Республике Казахстан необходимость обеспечения ИБ банковской тайны, коммерческой информации, персональных данных закреплена законодательно.

Существует нормативная правовая база в области ИБ финансового сектора. Практически все принятые нормативные правовые акты содержат правила и/или требования, направленные на повышение уровня безопасности объектов финансовой отрасли по отдельным направлениям их деятельности. Стратегия кибербезопасности содержит анализ текущего состояния и направления деятельности по созданию эффективной системы обеспечения кибербезопасности в финансовом секторе.

Но для успешного достижения целей Стратегии кибербезопасности необходима методология обеспечения информационной безопасности финансового

сектора, которая будет служить методологической базой управления информационной безопасностью, исключению разрозненности и фрагментарности нормативных правовых документов и повышению их эффективности, реализации возможностей системного подхода.

Методология должна быть разработана в соответствии с требованиями нормативных руководящих документов РК, на основе стандартов ИБ (ISO/IEC 27k и др.), анализа структуры, угроз ИБ, информационных рисков и защищенности информационных ресурсов финансового сектора РК.

Литература

1. Концепция кибербезопасности («Киберщит Казахстана») (2017). http://adilet.zan.kz/rus/docs/P1700000407 (30.01.2020);

2. Standards by ISO/IEC JTC 1/SC 27. Information security, cybersecurity and privacy protection. https://www.iso.org/ru/committee/45306/x/catalogue (03.02.2020);

3. Указ Президента Республики Казахстан от 11 ноября 2019 года №203 «О дальнейшем совершенствовании системы государственного управления Республики Казахстан»;

4. Совместное Постановление НБРК и АРРФР «Об утверждении Стратегии кибербезопасности финансового сектора Республики Казахстан на 2020-2022 годы» от 20 июля 2020 года (№89 НБРК, №69 АРРФР);

КРИПТОГРАФИЯЛЫҚ ХАТТАМАЛАРДЫҢ ЛОГИКАЛЫҚ ДҰРЫСТЫҒЫН BAN ЛОГИКАСЫ НЕГІЗІНДЕ ТАЛДАУ

Капалова Н.А., Сулейменов О.Т.
e-mail: suleimenov97@gmail.com
ҚР БҒМ ҒК Ақпараттық және есептеуіш технологиялар институты, Қазақстан

Аңдатпа: *Бұл мақалада аутентификация хаттамаларына талдау жасау барысында кеңінен қолданылатын, білім мен сенімділікті талдаудың формальды логикалық моделі – BAN логикасына талдау жүргізілген. Криптографиялық хаттамаларға BAN логикасы арқылы талдау қалай жасалынатыны келтірілген. Талдауды автоматтандыруға арналған бағдарлама нәтижесі көрсетілген.*

Кілттік сөздер*: аутентификация, криптографиялық хаттама, BAN логикасы.*

Ақпараттық қауіпсіздік саласында криптографиялық хаттамалар маңызды рольге ие. Криптографиялық хаттамалар ақпараттық процесстерде криптографиялық түрлендірулер мен алгоритмдерді қолдану ережелерінің жиынтығына негізделген. Олар аутентификация, қол жетімділікті басқару, құпиялықты қаптамасыз ету және т.б. мақсаттарда қолданылады. Криптографиялық хаттамаларға оларды пайдалану объектілеріне қарай әртүрлі талаптар қойылады.

Қазіргі таңдағы қолданыстағы хаттамалардың және жаңадан құрылып жатқан хаттамалардың қауіпсіздік деңгейін зерттеу және талдау үшін арнайы формальды әдістер мен формальды емес, интуитивті әдістер қолданылады.

Криптографиялық хаттамаларды талдаудың формальды әдістерін төрт түрге бөлуге болады [1]:

1. Білу мен сенімді талдауға арналған модальды логикаға негізделген әдістер (BAN логикасы, Мао и Бойда логикасы, Мозер логикасы);
2. Сараптамалық жүйелерге негізделген әдістер, олардың көмегімен криптографиялық хаттамаларды жасаушы әртүрлі шабуыл сценарийлеріндегі хаттаманың әрекетін зерттей алады;
3. Криптографиялық хаттамаларды талдау үшін әзірленбеген талдау спецификациялары мен құралдарының тілдерін пайдалана отырып хаттамаларды модельдеу мен талдауға негізделген әдістер;
4. Криптографиялық хаттамалардың алгебралық және логикалық қасиеттеріне негізделген формальды модельдерге негізделген әдістер (алгебралық модельдеу).

Бүгінгі таңда криптографиялық хаттамалардың дұрыстығын талдаудың ең көп қолданылатын әдістері модальды логикаға негізделген әдістер болып табылады. Атап айтқанда, модальды логикаға негізделген криптографиялық хаттамаларды талдаудың ең тиімді әдістері BAN логикасы және оның кеңейтімдері (GNY логикасы, Сиверсон логикасы және т.б.)

Бэрроуз-Абади-Нидхэм логикасы немесе BAN логикасы – бұл аутентификация хаттамаларына талдау жасау барысында кеңінен қолданылатын, білім мен сенімділікті талдаудың формальды логикалық моделі [2].

BAN логикасының негізгі идеясы бұндай хаттамаларды талдау кезінде, ең алдымен, аутентификация процесіне қатысатын тараптардың мәліметтерді қалай қабылдайтыны маңызды. Олардың сенім ретінде қандай ақпаратты қабылдайтыны және оларға белгілі немесе сенімді фактілерге сүйене отырып логикалық жолмен шығарылуы мүмкін ақпаратқа назар аудару қажет [3].

Әдетте аутентификация хаттамалары хаттамаға қатысушылар арасында жіберілетін хабарламаларды дәйекті түрде тізімдеу арқылы сипатталады. Әрбір қадамда хабарламаның мазмұны сипатталады, сонымен қатар оны жіберуші мен алушы көрсетіледі. BAN логикасы хабарламаның түпнұсқалығын оның тұтастығы мен жаңашылдығының функциясы ретінде қарастырады, хаттама барысында осы атрибуттардың күйін бақылау үшін логикалық ережелерді қолданады [4].

BAN логикасында объектілердің 3 түрі анықталған: хаттамаға қатысушылар (A, B, S), симметриялы шифрлеу кезіндегі кілттер (K_{AB}, K_{AS} және K_{BS}) немесе асимметриялы шифрлеу кезіндегі кілттер (ашық кілттер: K_A, K_B, K_S және құпия кілттер K_A^{-1}, K_S^{-1}, K_B^{-1}), және оларды байланыстыратын формулалар. Сондай-ақ, келесідей белгілеулер қолданылады: арнайы сандық белгілеулер (уақыт белгілері және т.б.) – N_A, N_B, N_S, формулалар мен пікірлерге арналған жалпы белгілеулер – X, Y. Хаттаманы талдау барысында жіберілген әрбір хабарлама формулаға айналады, содан кейін логикалық формулалар пікірлермен байланыстырылады [5]. Бұл логикада қолданылатын жалғыз логикалық операция – конъюнкция болып табылады. Сондай-ақ әр түрлі предикаттар енгізіледі, мысалы, қатысушылар мен мәлімдемелер арасындағы қарым қатынасты орнату (сенім, юрисдикция және т.б.) немесе мәлімдемелердің қандай да бір қасиеттерін білдіру (мысалы, жаңашылдық, яғни мәлімдеме жуық арада алынғанын көрсету).

Кез-келген формальды логика секілді, BAN логикасында аксиомалар мен қорыту ережелері болады. Хаттаманы талдау – қорыту ережелерін қолдана отырып, BAN логика формулаларымен көрсетілген кейбір мәлімдемелер жиынтығын дәлелдеуден тұрады. Мысалы, кез-келген аутентификация хаттамасына кем дегенде

келесідей талаптар қойылады: екі қатысушы да бір-бірімен ақпарат алмасудың құпия кілтін тапқанына сенуі қажет.

Негізгі предикаттар және олардың белгіленуі:

- $P| \equiv X$ – бұл P, X пікіріне сенетінін білдіреді. Бұл P хабар алмасушы тарабы, X пікірін шынайы ақпарат ретінде қабылдап, әрекет ете бастайды дегенді білдіреді.
- $P \lhd X$ – P тарабы X хабарламасын оқыды немесе қабылдады деген мағына береді. Яғни P тарабы X хабарламасында не жіберілгенін оқи алады.
- $P|\sim X$ – дегеніміз уақыттың бір бөлігінде P тарабы X пікірін айтқан, яғни X хабарламасын жіберген.
- $P| \Longrightarrow X$– X пікірі P тарабының юрисдикциясына кіреді.
- $\#X$ – X хабарламасының жаңашылдығын білдіреді. Яғни, X хабарламасы ағымдағы хаттама орындала бастағаннан бергі уақытта жіберілгенін білдіреді.
- $P \overset{k}{\longleftrightarrow} Q$ – P және Q хабарлама алмасу үшін k ортақ кілтін қолданады.
- $\{X\}_K$ – X хабарламасының деректері K кілтімен шифрланғанын білдіреді.

Конъюнкция операторы үтір арқылы, ал олардың қорытындысы көлденең сызық ретінде жазылады. Мысалы, $A \wedge B \Rightarrow C$ логикалық өрнегі BAN логикасында $\frac{A,B}{C}$ ретінде жазылады.

BAN логикасының аксиомалары:

1. Уақыт екі кезеңге бөлінеді: өткен шақ және осы шақ. Осы шақ хаттама басталған уақыттан бергі кезең.
2. Хаттамаға қатысушы P, кез-келген X хабарламасын жіберген болса, онда ол жіберілген хабарламаның шынайылығына сенеді.
3. Хаттама барысында пайдаланылатын шифрлеу алгоритмдері абсолютті сенімді деп саналады: шифрленген хабарламаны кілтті білмейтін қолданушылар кез-келген жағдайда оқи алмайды.

Қорыту ережелері:

Хабарламаның мәні туралы ереже *(The message-meaning rule):*

$$\frac{A| \equiv A \overset{K}{\longleftrightarrow} B, A \lhd \{X\}_K}{A| \equiv B| \sim X}$$

Ереженің мағынасы: A тарабы B тарабы арқылы хабар алмасу барысында K кілтін қолданатынына сенеді және A тарабы K кілтімен шифрланған X хабарламасын көреді деген жорамалдар қорытындысы бойынша A тарабы X хабарламасын B тарабы жібергеніне сенеді.

Сандық қосымшалардың бірегейлігін тексеру ережесі *(The nonce-verification rule):*

$$\frac{A| \equiv \#X, A| \equiv B| \sim X}{A| \equiv B| \equiv X}$$

Егер A тарабы X пікірінің жаңашылдығына сенетін болса және B тарабы уақыттың кез-келген бөлігінде X пікірін айтқан болса, онда A тарабы B тарабының X хабарламасына әлі де сенетініне сенеді.

Юрисдикция ережесі (*The jurisdiction rule):*

$$\frac{A| \equiv B| \Rightarrow X, A| \equiv B| \equiv X}{A| \equiv X}$$

Егер ***A*** тарабы ***B*** тарабының ***X*** хабарламасы бойынша юрисдикциясы болса және ***B*** тарабының ***X*** хабарламасына сенетініне ***A*** тарабы да сенетін болса, онда ***A*** тарабы да ***X*** хабарламасына сенетін болады.

BAN логикасының негізгі мағынасы көрсетілген 3 қорыту ережелері төңірегінде шоғырланған. Сонымен қатар, түрлендірулер барысында басқа да ережелер қолданылады.

Тәжірибе тұрғысынан алғанда, кез-келген хаттаманы талдау келесідей алгоритм арқылы жүзеге асады [5]:

- Бастапқы хаттама идеалды түрге түрлендіріледі, яғни BAN логикасының терминдері арқылы жазылады.
- Хаттаманың бастапқы күйі туралы болжамдар қосылады.
- Әрбір хабарламамен логикалық формулалар байланыстырылады, яғни әрбір мәлімдемеден кейін хаттаманың жай-күйі туралы логикалық мәлімдеме алынады.
- Хаттаманың болжамдары мен пікірлеріне хаттаманың жұмысы аяқталғаннан кейін хаттамағы қатысушы тараптардың сенім жағдайын анықтау үшін қорыту ережелері мен аксиомалар қолданылады.

Осы уақытқа дейін BAN логикасындағы идеализация процесі ең көп сынға ұшырады, себебі идеализацияланған хаттама тәжірибе жүзінде жұмыс жасау барысында өзгеше жұмыс жасауы мүмкін [6]**.** Сонымен қатар, BAN логикасын қолдана отырып хаттаманы талдау нәтижесін оның қауіпсіздігінің дәлелі деп санауға болмайды, себебі бұл формальды логика тек хаттаманың жұмыс істеу логикасының дұрыстығын тексеруге арналған.

Аутентификация хаттамаларының мақсаты.

BAN логикасының терминдерінде аутентификация хаттамаларының мақсаты келесідей болады:

$$A| \equiv A \overset{K}{\leftrightarrow} B, \;\; B| \equiv A \overset{K}{\leftrightarrow} B,$$

Яғни, хаттамаға қатысатын тараптар өзара хабарламалар алмасу барысында тек бір ғана құпия кілтті қолданатынына сенуі тиіс. Дегенмен, хаттамаға басқа да талап қойса болады:

$$A| \equiv B| \equiv A \overset{K}{\leftrightarrow} B, \;\; B| \equiv A| \equiv A \overset{K}{\leftrightarrow} B.$$

Яғни, кілтті қабылдағанды растауды талап ету.

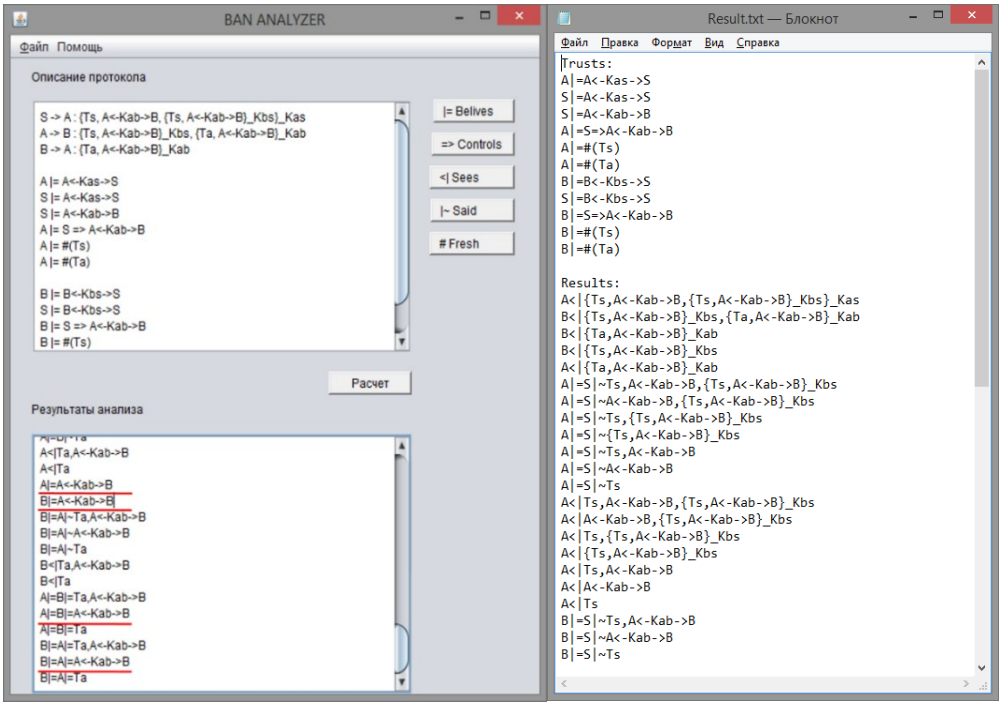
BAN логикасы арқылы хаттамаларды талдау процесін автоматтандыратын «BAN Analyzer» бағдарламасы әзірленді. Бағдарлама арқылы «Kerberos», «The Andrew Secure RPC Handshake», «The Needham-Schroeder public key», «The CCIT X.509» аутентификация хаттамаларына автоматтандырылған талдау жасалынды. Бұл хаттамалардың талдауы алдымен қолмен жасалынды. Сонымен қатар бағдарлама арқылы жасалынған талдау нәтижелерімен салыстырылды.

1-суретте «Kerberos» хаттамасына жасалынған талдау нәтижесі көрсетілген, хаттаманың қосымша сенімдерді қолданбастан симметриялық кілт алмасу барысында қойылған мақсаттардың барлығы орындалғанына көз жеткізуге болады.

Бағдарлама кіріс деректері ретінде талдау жасалынатын хаттаманың BAN логика шеңберінде идеализация жасалынған қадамдарын және хаттама жұмысы басталмай тұрып бізге белгілі болатын сенімдер енгізіледі. Хаттамадағы әрбір

қадамға талдау жасау үш кезеңнен тұрады. Әр кезеңде қорыту ережелері қолданылады: хабарламаның мәні туралы ереже, сандық қосымшалардың бірегейлігін тексеру ережесі, юрисдикция ережесі, қажет болған жағдайда қойылған мақсатқа жету үшін қосымша ережелер де пайдаланылады. Шығыс деректері ретінде қорытынды келесідей мәтіндік файл алынады: алғашқы болып хаттама хабарламалары, яғни BAN логикасына сәйкес әрбір қадам, хаттама басталмай тұрып белгілі болған сенімдер, одан кейін жүргізілген талдау нәтижесі.

Симметриялы және асимметриялы криптографиялық хаттамаларға талдау бір ережелерді пайдалана жүргізілгенмен, оларды қолдану принциптері әртүрлі болады.



1-сурет. «BAN Analyzer» бағдарламасының қорытындысы

Ақпараттық жүйелерде қолданылатын криптографиялық хаттамаларды әзірлеу қиындығымен қатар, оларды талдау да маңызды мәселелердің бірі. Сенімді деп қолданылып жүрген криптографиялық хаттамалардың уақыт өте әртүрлі шабуылдарға осалдық танытқан жағдайлар тарихта өте көп кездеседі**.** Сондықтан криптографиялық хаттаманың дұрыстығын дәлелдеу үшін қолданыстағы талдау әдістерінің тек біреуін ғана қолдану жеткіліксіз.

Қорытынды

Криптографиялық хаттамаларды талдаудың қолданыстағы әдістерін зерттеу барысында келесі қорытынды шығаруға болады. Аутентификация хаттамаларына талдау жасау барысында автоматтандырылған жүйелерін қолдану орынды.

Жұмыс барысында BAN логикасын қолдану негізінде кілттерді таратуға арналған криптографиялық хаттамалардың логикалық дұрыстығына формальды тексеру жүргізуге арналған автоматтандырылған «BAN Analyzer» бағдарламасы әзірленді. Бағдарлама арқылы «Kerberos», «The Andrew Secure RPC Handshake», «The Needham-Schroeder public key», «The CCIT X.509» аутентификация хаттамаларына автоматтандырылған талдау жасалынды. Талдау нәтижелері

бағдарлама жұмысының оң нәтижелерін және хаттамалардың логикалық дұрыстығын көрсетті. Хаттамаларды талдауды BAN логика әдістерімен жүзеге асыратын бағдарламалар – кілттермен алмасудың криптографиялық хаттамаларының жұмыс қабілеттілігі мен қауіпсіздігін тестілеу үшін, сонымен қатар хаттамаларды талдауды үйрену мақсаттары үшін де пайдалы болуы мүмкін, себебі кез-келген сенім логикасын зерттеу BAN логикасы әдістерімен талдау дағдыларына негізделген. Басқа да криптографиялық хаттамаларға талдау жасау жұмыстары жүргізілетін болады. Болашақта басқа да сенім логикаларына негізделген алгоритмдерді бағдарламалық жүзеге асыру көзделіп отыр. Сонымен қатар, криптографиялық хаттамалардың дұрыстығын талдау үшін криптографиялық хаттамаларды талдаудың қолданыстағы және тиімді формальды әдістерін әлі де жетілдіру қажет деп есептейміз.

Атқарылған жұмыс Қазақстан Республикасы Білім және ғылым министрлігінің AP05132568-OT-18 «Разработка системы управления криптографическими ключами» гранттық қаржыландыру бағдарламасы аясында орындалды.

Әдебиеттер

1. Черемушкин А.В., Криптографические протоколы: основные свойства и уязвимости / А.В. Черемушкин. – Москва. Ин-т криптографии, 2009. – 272 с.
2. M. Burrows, M. Abadi, R. Needham, «A Logic of Authentication», – P. 19.
3. B. Schneier, «Applied Cryptography», – 66 c.
4. Л.К. Бабенко, О.Б. Макаревич, В.В. Остапенко. Логика ban для спецификации и анализа криптографических протоколов – https://cyberleninka.ru/article/n/logika-ban-dlya-spetsifikatsii-i-analiza-kriptograficheskih-protokolov (10.08.2020)
5. Могилевская Н.С. Программное средство логической проверки корректности криптографических протоколов распределения ключей на основе BAN логики. Вестник Донского государственного технического университета. – 2012. – № 1. – 5-14 с.
6. D.M. Nessett, «A Critique of the Burrows, Abadi, and Needham Logic», – P. 35-38.

СХЕМА ЭЛЬ-ГАМАЛЯ НА ОСНОВЕ НЕПОЗИЦИОННЫХ ПОЛИНОМИАЛЬНЫХ СИСТЕМ СЧИСЛЕНИЯ

Нысанбаева С.Е., Капалова Н.А., Варенников А.В.
e-mail: snyssanbayeva@gmail.com, kapalova@ipic.kz, avarennikov@gmail.com
Институт информационных и вычислительных технологий КН МОН РК, Казахстан

Аннотация. *В данной работе рассматриваются модифицированные алгоритмы генерации ключей, шифрования и электронной цифровой подписи криптосистемы Эль-Гамаля с использованием непозиционных полиномиальных систем счисления.*

Введение

После того, как в 1975 году Диффи и Хеллман [1] представили концепцию криптографии с открытым ключом, были разработаны многочисленные методы её реализации. В качестве примера можно привести систему Ривеста-Шамира-Адлемана (RSA) [2], зависящую от сложности факторизации больших целых чисел, и схему Эль-Гамаля [3], основанную на сложности вычисления дискретных логарифмов над конечными полями, получившие наиболее широкое распространение.

Числовая схема шифрования и электронной подписи Эль-Гамаля может быть обобщена для работы в любой конечной циклической группе G. Группа G должна удовлетворять следующим условиям [4]:

– эффективность, то есть групповые операции в G должны вычисляться относительно просто;

– криптографическая стойкость, то есть решение проблемы дискретного логарифма в G должно быть практически неосуществимым.

Ниже приведены некоторые из групп, удовлетворяющие этим условиям:

– мультипликативная группа $\mathbb{Z}_p^*$ целых чисел по модулю простого числа p;

– группа обратимых элементов $\mathbb{Z}_n^*$, где n есть составное целое число;

– мультипликативная группа $\mathbb{Z}_q^*$ конечного поля $\mathbb{F}_q$, где $q = p^s$, p есть простое число, s есть положительное число;

– группа точек эллиптической кривой над конечным полем и другие.

В данной статье в качестве циклической группы G с перечисленными выше свойствами рассматривается мультипликативная группа конечного поля $\mathbb{F}_2[x]/\big(f(x)\big)$, являющегося полной системой вычетов по модулю неприводимого полинома $f(x)$ над полем $GF(2)$, то есть с двоичными коэффициентами.

В следующих разделах описываются модифицированные алгоритмы генерации ключей, шифрования/расшифрования, создания и проверки цифровой подписи с использованием непозиционных полиномиальных систем счисления.

Генерация ключей.

Особенностью описываемых алгоритмов шифрования и электронной цифровой подписи является то, что длина ключа может быть произвольной.

1) Сначала выбирается длина ключа L (в битах).

2) Затем производится формирование непозиционной полиномиальной системы счисления (НПСС). В качестве рабочих оснований НПСС выбираются неприводимые двоичные полиномы $p_1(x), p_2(x), \dots, p_n(x)$ со степенями $d_1, d_2, \dots, d_n$, соответственно, при этом сумма степеней рабочих оснований должна совпадать с длиной ключа, то есть $\sum_{i=1}^{n} d_i = L$. Для выполнения китайской теоремы об остатках все основания должны быть различными.

3) Для каждого рабочего основания $p_i(x)$ выбирается примитивный полином $\alpha_i(x) \in \mathbb{F}_2[x]/\big(p_i(x)\big)$, являющийся генератором элементов поля $\mathbb{F}_2[x]/\big(p_i(x)\big)$ порядка $\varphi\big(p_i(x)\big) = 2^{d_i} - 1$, где функция φ является обобщением функции Эйлера применительно к полиномам.

4) Затем для каждого рабочего основания $p_i(x)$ выбирается случайное целое число k_i такое, что $1 \le k_i < \varphi\big(p_i(x)\big) - 1$. Значения k_i должны храниться в секрете.

5) Наконец, для каждого рабочего основания $p_i(x)$ вычисляется выражение $\beta_i(x) = \alpha_i(x)^{k_i} \bmod p_i(x)$.

Таким образом, ключом K является пара $K = \langle CK, OK \rangle$, где $CK = (k_1, k_2, \dots, k_n)$ – это закрытый (секретный) ключ, а OK – это открытый ключ, состоящий из следующих элементов:
$K = \langle (p_1(x), p_2(x), \dots, p_n(x)), (\alpha_1(x), \alpha_2(x), \dots, \alpha_n(x)), (\beta_1(x), \beta_2(x), \dots, \beta_n(x)) \rangle$.

Алгоритм ассиметричного шифрования

Для того, чтобы зашифровать сообщение M длиной L битов, отправителю необходимо получить открытый ключ получателя и выполнить следующие действия:

1) Разбить битовую последовательность, представляющую сообщение M, на n частей длиной $d_1, d_2, \dots, d_n$ бит, соответственно, после чего преобразовать полученные битовые последовательности в полиномы $m_1(x), m_2(x), \dots, m_n(x)$ с двоичными коэффициентами.

2) Для каждого $i = \overline{1, n}$ выбрать случайное целое число r_i такое, что $1 \le r_i < \varphi(p_i(x)) - 1$.

3) Для каждого $i = \overline{1, n}$ вычислить первую часть шифртекста:
$\gamma_i(x) = \alpha_i(x)^{r_i} \bmod p_i(x)$.

4) Для каждого $i = \overline{1, n}$ вычислить вторую часть шифртекста:
$\delta_i(x) = (m_i(x) \times \beta_i(x)^{r_i}) \bmod p_i(x)$.

Таким образом, шифртекст C представляет собой следующую структуру:

$$C = \langle (\gamma_1(x), \gamma_2(x), \dots, \gamma_n(x)), (\delta_1(x), \delta_2(x), \dots \delta_n(x)) \rangle$$

Для расшифрования шифртекста получатель должен использовать свой закрытый ключ и выполнить следующие действия:

1) Для каждого $i = \overline{1, n}$ вычислить выражение:
$m_i(x) = \left(\gamma_i(x)^{-k_i} \times \delta_i(x)\right) \bmod p_i(x)$.

2) Преобразовать двоичные полиномы $m_i(x)$ в битовые последовательности длиной $d_1, d_2, \dots, d_n$ бит и соединить их вместе, получая на выходе битовую последовательность, представляющую текст открытого сообщения M.

Алгоритм цифровой подписи

Для того, чтобы подписать сообщение M длиной L битов электронной цифровой подписью, отправителю необходимо использовать свой закрытый ключ и выполнить следующие действия:

1) Разбить битовую последовательность, представляющую сообщение M, на n частей длиной $d_1, d_2, \dots, d_n$ бит, соответственно, после чего преобразовать полученные битовые последовательности в целочисленные значения $m_1, m_2, \dots, m_n$.

2) Для каждого $i = \overline{1, n}$ выбрать случайное целое число r_i такое, что $1 \le r_i < \varphi(p_i(x)) - 1$ и НОД$(r_i, \varphi(p_i(x)) - 1) = 1$.

3) Для каждого $i = \overline{1, n}$ вычислить первую часть цифровой подписи:
$\sigma_i(x) = \alpha_i(x)^{r_i} \bmod p_i(x)$.

4) Для каждого $i = \overline{1, n}$ преобразовать двоичные полиномы $\sigma_1(x), \sigma_2(x), \dots, \sigma_n(x)$ в целочисленные значения $\sigma_1, \sigma_2, \dots, \sigma_n$.

5) Для каждого $i = \overline{1, n}$ вычислить вторую часть цифровой подписи:
$s_i = r_i^{-1}(m_i - k_i\sigma_i) \bmod (\varphi(p_i(x)) - 1)$.

Таким образом, цифровая подпись S представляет собой следующую структуру:

$S = \langle(\sigma_1(x),\ \sigma_2(x),\ \dots\ ,\ \sigma_n(x)), (s_1, s_2, \dots s_n)\rangle.$

Для проверки цифровой подписи получатель должен использовать свой открытый ключ и выполнить следующие действия:

1) Разбить битовую последовательность, представляющую сообщение M, на n частей длиной $d_1, d_2, \dots, d_n$ бит, соответственно, после чего преобразовать полученные битовые последовательности в целочисленные значения $m_1, m_2, \dots, m_n$.

2) Для каждого $i = \overline{1,n}$ преобразовать двоичные полиномы $\sigma_1(x), \sigma_2(x), \dots, \sigma_n(x)$ в целочисленные значения $\sigma_1, \sigma_2, \dots, \sigma_n$.

3) Для каждого $i = \overline{1,n}$ вычислить первую часть проверочного значения:

$$\vartheta_i(x) = (\beta_i(x)^{\sigma_i} \times \sigma_i(x)^{s_i}) \bmod p_i(x)$$

4) Для каждого $i = \overline{1,n}$ вычислить вторую часть проверочного значения:

$\omega_i(x) = \alpha_i(x)^{m_i} \bmod p_i(x).$

Если для каждого $i = \overline{1,n}$ выполняется условие $\vartheta_i(x) = \omega_i(x)$, цифровая подпись принимается. В противном случае цифровая подпись отклоняется.

Заключение

Все операции умножения и возведения в степень двоичных полиномов производятся в непозиционной полиномиальной системе счисления, поэтому вычисление этих операций может выполняться параллельно по модулям полиномов, выбранных в качестве оснований системы.

Результаты исследования модифицированной системы ассиметричного шифрования по схеме Эль-Гамаля с использованием полиномиальных систем счисления опубликованы в работах [5-7].

Описанные алгоритмы шифрования и электронной цифровой подписи были реализованы в системе управления криптографическими ключами «CKMS Crypto 1.0».

Данная работа выполняется в рамках проекта AP05132568 «Разработка системы управления криптографическими ключами» Министерства образования и науки Республики Казахстан.

Литература

1. Diffie W. and Hellman M. New directions in cryptography // IEEE Transactions on Information Theory, 1976. – vol. IT-22(6). – pp. 472-492.
2. Rivest R., Shamir A. and Adleman L. A method for obtaining digital signatures and public key cryptosystems // Communications of the ACM, 1978. – vol. 21(2). – pp. 120-126.
3. ElGamal T. A public-key cryptosystem and a signature scheme based on discrete logarithms // IEEE Transactions on Information Theory, 1985. – vol. IT-31(4). – pp. 469-472.
4. Авдошин С. М., Набебин А. А. Дискретная математика. Модулярная алгебра, криптография, кодирование // М: ДМК Пресс, 2017. – 351 с.
5. Нысанбаева С.Е. Разработка и исследование криптографических систем на базе непозиционных полиномиальных систем счисления: дисс. докт. техн. наук. – Алматы, 2009. – 240 с.

6. Капалова Н. А. Исследование криптостойкости алгоритма шифрования Эль-Гамаля на базе непозиционных полиномиальных систем счисления // Информационная безопасность. Матер. XII Межд. науч.-практ. конф. – Таганрог, ТТИЮФУ, 2012. – Ч. 1 – С. 253-258.

7. Капалова Н. А. Модифицированный алгоритм шифрования Эль-Гамаля на базе непозиционных полиномиальных систем счисления // Известия Национальной академии наук РК. – Алматы, 2013. – № 1. – С. 22-26.

О РАЗРАБОТКЕ МОДЕЛИ СИСТЕМЫ КАЗАХСТАНСКОГО СЕГМЕНТА ЗАЩИЩЕННОГО ТРАНСГРАНИЧНОГО ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ

Бегимбаева Е.Е.[1], Бияшев Р.Г.[1]
e-mail: enlik_89@mail.ru, brg@ipic.kz
Институт информационных и вычислительных технологий
КН МОН РК, Казахстан

Аннотация. *Предлагается модель системы автоматизированного трансграничного информационного обмена. Рассмотрены типы возможных конфликтных ситуаций в этой системе. Предложено и исследовано программная реализация разработанного алгоритма формирования и проверки цифровой подписи. Приведены результаты разработанной программной реализации.*

Ключевые слова: система трансграничного информационного обмена, информационная безопасность, электронная цифровая подпись, конфликтные ситуаций.

Введение

В процессе создания Таможенного союза стран ЕАЭС согласно Договору о Евразийском экономическом союзе (с изменениями на 14.05.2018 г.) сформировалось понятие и значимость «трансграничного пространства доверия» [1].

Создание интегрированной информационной системы пространства доверия ЕАЭС будут способствовать обеспечению доверия в условиях межгосударственного обмена данными и электронной документацией уполномоченных органов государств-членов ЕАЭС. Это позволит повысить уровень информационных взаимодействий в рамках трансграничного пространства [2].

Интегрированное информационное взаимодействие в трансграничном пространстве доверия представляет собой комплекс, сформированный правовыми, организационными и техническими условиями, согласованными странами — членами ЕАЭС для межгосударственного обмена данными и электронными документами между уполномоченными органами [3].

В августе 2019 года была утверждена концепция трансграничного информационного взаимодействия межправительственным советом ЕАЭС на уровне премьер-министров (Казахстан, России, Киргизии, Армения, Беларусь) [4].

В ЕАЭС пришли к соглашению об единых подходах к реализации электронного информационного взаимодействия между субъектами бизнеса

и государственного органа. Предполагается, что реализация концепции даст возможность субъектам трансграничного взаимодействия стран ЕАЭС взаимодействовать друг с другом в электронном виде с использованием электронной цифровой подписи. Применение единых подходов предполагает упрощение взаимодействия участников и усиление коммуникационных составляющих между ними. Таким образом, формируется юридически значимая система документооборота межгосударственного уровня для информационного обеспечения органов государственной власти и управления государств — членов ЕАЭС [5].

Единый подход к реализации электронного взаимодействия противоречит условию «трансграничного пространства доверия». Поскольку пространство может называться «трансграничным пространством доверия», если государствами ЕАЭС обеспечиваются:

1) цифровой суверенитет и нейтралитет государств-членов, а также невмешательства стран в информационные ресурсы друг друга, в принципы информационной безопасности;

2) согласованные условия принятия решений и общие подходы к использованию институциональных форм доверительного трансграничного пространства;

3) криптографические меры защиты информаций и согласованные условия использования услуг серверов, предоставляемых операторами национальной информационной инфраструктуры.

Важной составляющей обеспечения информационной безопасности любого государства является разработка и использование отечественных средств защиты информации. Разрабатываемая система защищенного трансграничного обмена позволит использовать отечественные разработки и стандарты криптографической защиты информации. Применение отечественных разработок позволит повысить надежность и безопасность казахстанского сегмента защищенного трансграничного обмена.

1. Разработка системы защиты информации в информационной системе трансграничного обмена

Одной из задач корректного функционирования любой информационной системы передачи данных, а именно при трансграничном обмене является обеспечение защищенной передачи данных.

Модель защиты информации в информационной системе трансграничного обмена (ИСТО) разрабатывается с учетом существования множества подсистем, включая:

- криптографические подсистемы, обеспечивающие конфиденциальность, целостность данных и неотказуемость авторства, путем использования алгоритмов шифрования и электронной цифровой подписи;

- подсистема управления доступом, обеспечивающие идентификацию и аутентификацию при входе в систему, доступ субъектов к различным объектам и ресурсам с использованием заданных политик и процедур;

- подсистема регистрации и учета, которые обеспечивают регистрацию: входа (выхода) субъектов доступа в (из) системы; действия субъектов над объектами; статуса объекта; конфликтных ситуаций в системе.

Научные работы по разработке систем защищенного трансграничного обмена были выполнены в рамках проекта грантового финансирования МОН РК на тему «Разработка системы казахстанского сегмента защищенного трансграничного информационного взаимодействия». Это система состоит из блоков (подсистем): шифрования, электронной цифровой подписи и разграничения доступом.

Для блоков шифрование и электронной цифровой подписи разработаны модели модифицированных алгоритмов зашифрования и расшифрования, алгоритмы формирования и проверки ЭЦП на базе модулярных систем счисления. Проведены работы по улучшению модели модифицированных алгоритмов зашифрования и расшифрования на основе симметричного блочного шифрования, который использует блоки длиной по 128 бит и сеть Фейстеля [6]. Разработан расширенный алгоритм формирования и проверки электронной цифровой подписи на базе непозиционных полиномиальных систем счисления. Построена обобщенная схема функционирования автоматизированной системы целиком.

Разработаны программные модули для алгоритмов зашифрования и расшифрования, а также алгоритмов формирования и проверки ЭЦП. Усовершенствован пользовательский интерфейс программных модулей для алгоритмов зашифрования и расшифрования, алгоритмов формирования электронной цифровой подписи и ее проверки [7].

Ведутся работы по разработке рекомендаций по усилению параметров надежности модифицированных криптографических алгоритмов.

Для систем ЭЦП рассмотрен перечень конфликтных ситуаций, относительно разрабатываемой системы защищенного трансграничного обмена. Приведена система разрешения возможных конфликтных ситуаций. Были рассмотрены существующие методы, процедуры и инструментальных средства обеспечения бесконфликтного взаимодействия программных средств защиты информации. Сформулирован перечень конфликтных ситуаций, возможных в разрабатываемой системе. Разработана архитектура модели разрешения конфликтных ситуаций [8].

Проведены работы по разработке компьютерной программы, реализующей модуль системы разграничения доступа [9]. Поскольку система аутентификации является одним из ключевых элементов инфраструктуры защиты от несанкционированного доступа любой информационной системы, была рассмотрена возможность использования аутентификации на основе второго фактора [10].

Выводы

По результатам исследований:

- опубликованы 13 статей, из них 2 - в зарубежном научном журнале входящий в базу Web of Science Core Collections и Scopus, 1 - в журнале входящий в список журналов, рекомендованных ККСОН МОН РК.
- получены 2 свидетельства о внесении сведений в государственный реестр прав на объект, охраняемые авторским правом.

Полученные результаты по проекту являются новыми, имеют теоретическую и практическую значимость. Рассматривается возможность дальнейшего расширение блоков составляющих защищенную систему трансграничного информационного обмена, а именно применение композитной аутентификаций для систем разграничения доступом.

Литература

1. Соглашение о применении информационных технологий при обмене электронными документами во внешней и взаимной торговле на единой таможенной территории Таможенного союза 2010 г., которое прекратило действие с 01.01.2015 г. на основании международного договора от 29.05.2014 г. № 349н.
2. Решение Коллегии Евразийской экономической комиссии от 27.01.2016 г. № 105 «О Стратегии развития трансграничного пространства доверия».
3. Ступаков Н.В. Цифровая интеграция стран ЕАЭС и СНГ: политико-правовые основы развития интегрированной информационной системы евразийского сотрудничества // Международное Сотрудничество Евразийских Государств: Политика, Экономика, Право, №1 2019, с. 15-25.
4. Концепция трансграничного информационного взаимодействия, утв. Решением Евразийского межправительственного совета от 9 августа 2019 года № 7.
5. ИТ-проекты ЕАЭС https://www.tadviser.ru/a/394495.
6. Дюсенбаев Д., Сақан Қ., Алғазы К., Хомпыш А., «MODNPSS14» шифрлау алгоритміне криптографиялық талдау, Хабаршы КазККА №3, 2019ж., - 235-243 б.
7. Begimbayeva, Y.Y., Ussatova O.A., Nyssanbayeva, S.E., Biyashev, R.G. Development of an automated system model of information protection in the cross-border exchange // Cogent Engineering, Volume 7, Issue 1, 2020, DOI: 10.1080/23311916.2020.1724597 (SJR 0.272, Q2, процентиль 68).
8. Бегимбаева Е.Е. О модели разрешения конфликтных ситуаций в автоматизированной системе защищенного информационного взаимодействия // Актуальные проблемы информационной безопасности в Казахстане: Матер. Межд. науч. – практ. конф. (15 января 2020 г.). – Алматы, 2020. – С. 105-107.
9. Калимолдаев М.Н., Бияшев Р.Г., Рог О.А. Уровни определения модели типизированного атрибутного разграничения доступа // Актуальные проблемы информационной безопасности в Казахстане: Матер. Межд. науч. – практ. конф. (15 января 2020 г.). – Алматы, 2020. – С. 148-154.
10. Усатова О.А. Клиент-серверная система защиты информации на основе двухфакторной аутентификации // Актуальные проблемы информационной безопасности в Казахстане: Матер. Межд. науч. – практ. конф. (15 января 2020 г.). – Алматы, 2020. – С. 242-247.

МОДИФИЦИРОВАННЫЙ МЕТОД ДИНАМИЧЕСКОГО ПРОГРАММИРОВАНИЯ ДЛЯ ОПРЕДЕЛЕНИЯ АКТИВНОГО СОСТАВА СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Ахметов С.С.[1], Калижанова А.У.[2], Lakhno V.[3], , Набиева Г.С.[4]
e-mail: kalizhanova_aliya@mail.ru, gulnaz_nc@mail.ru
[1, 2] Институт информационных и вычислительных технологий КН МОН РК, Казахстан
[2]Алматинский университет энергетики и связи, Алматы, Казахстан
[1]Казахский национальный университет имени аль-Фараби, Казахстан
[2] Department of Computer systems and networks, National University of Life and Environmental Sciences of Ukraine, Kyiv, Ukraine
[4] Казахский Национальный медицинский университет имени С.Д. Асфендиярова, Казахстан

Аннотация. *В статье предложена многокритериальная оптимизационная модель, предназначенная для вычислительного ядра системы поддержки принятия решений (СППР), принимаемых в процессе анализа вариантов размещения средств защиты информации (СЗИ) по узлам распределенной вычислительной сети (РВС) предприятия или организации. В отличие от существующих, модель позволяет автоматизировать анализ различных вариантов размещения СЗИ. Также модель позволяет учитывать, как отдельные факторы, влияющие на показатели защищённости РВС, так и их комбинации.*

Введение.

Многие исследования в области проблематики обеспечения кибербезопасности (КБ) и защиты информации (ЗИ) в распределенных вычислительных сетях (РВС) [1–3] показали, что не существует универсальных методов и моделей, которые способны дать специалистам служб информационной безопасности и КБ инструментарий для решения задачи по оптимизации размещения средств ЗИ (далее СЗИ). Особенно это заметно в условиях роста масштабов или изменения первоначально заданной архитектуры сети. И это связано, прежде всего, с постоянно меняющимся ландшафтом киберугроз. Эффективное решение подобной многокритериальной оптимизационной задачи возможно лишь при использовании систем поддержки принятия решений (СППР), обладающих мощным вычислительным ядром на основе различных математических моделей для решения подобных задач.

В связи с вышеизложенным можно сделать вывод, о том, что исследования по разработке моделей, методов и информационных технологий, например, СППР по оптимизации размещения СЗИ и КБ для РВС, является актуальной научной и технической задачей.

Обзор и анализ литературы по тематике исследования

Для решения задачи по оптимизации размещения СЗИ в РВС различными авторами использовались следующие модели и методы:

1) методы и модели на основе теории нечеткой логики [4, 5, 6];

2) методы и модели количественной оценки показателей от несанкционированного доступа в ИС [13]. Недостатком данных моделей можно считать большое количество эмпирических коэффициентов, а также некоторую неопределённость в процессе принятия решения;

3) экономические подходы [7, 8] при расчёте стратегий инвестирования в системы кибербезопасности. Однако в данных публикациях авторы делают упор именно на экономические аспекты задачи. При этом не принимается во внимание вопрос, связанный с оценкой качества защиты РВС;

4) модели, связанные с оцениванием защищенности информации [9, 10]. В этих публикациях главными параметрами являются время безопасного функционирования ИС и показатели функциональной устойчивости системы [9]. Недостатками данных методик является отсутствие элементов модели, которые делают возможным рассмотрение работы ИС в условиях разных классов кибератак;

5) комбинаторные методы [11, 12]. В данных работах ставятся задачи по минимизации затрат на СЗИ при ограничениях на заданный уровень эффективности. Авторы дополнили модель и алгоритм решения новой процедурой поиска

максимальных элементов в матрице, которая содержит показатели эффективности для каждого СЗИ.

Методы и модели.

В данном параграфе статьи описан метод определения активного состава СЗИ для узла РВС. Метод основан на модификации метода динамического программирования для решения многокритериальных оптимизационных задач по выбору СЗИ. Также используются экспертные оценки параметров, обобщаемые за счет применения метода Т. Саати (метод анализа иерархий). Такой подход дает возможность оперативно реагировать на изменение перечня угроз для объекта защиты и принимать решения в режиме реального времени.

Решая задачу многокритериальной оптимизации структуры СЗИ по контурам кибербезопасности РВС следует выделить следующие ключевые моменты:

1. Определенные классы киберугроз в текущий момент времени воздействуют не целиком на РВС, а на ее отдельные узлы или элементы. Следовательно, необходимо определять состав индивидуальных наборов СЗИ, таким образом, чтобы минимизировать размер потенциального ущерба для всей РВС;

2. Показатели эффективности одного и того же средства защиты могут быть разными. Это зависит от места размещения данного СЗИ, например, ряд антивирусного ПО рассчитан именно на применение на серверах (Антивирус Kaspersky Small Office Security 7 лицензия на 1 год для защиты 50 рабочих станций, 1 файлового сервера и 50 мобильных устройств (KL4541XCQFS)). Следовательно, целесообразно представлять показатели эффективности соответствующих контрмер, исходя из критериев оценивания класса СЗИ, к которому анализируемая контрмера относится;

3. СЗИ из некоторых классов не могут (или нецелесообразно) быть размещены на определённых узлах РВС. Например, песочницы не обязательно применять для мобильных устройств;

4. По отношению к угрозам одного типа можно применять СЗИ из разных классов. Например, для недопущения проникновений несанкционированных лиц в РВС и для обеспечения проверки подлинности пользователей можно использовать как традиционные средства аутентификации и идентификации пользователей (пароли, электронные подписи, биометрия), так и ПО для определения клавиатурного почерка. Таким образом, подходы с применением критериев оценивания контрмер и связей между критериями и киберугрозами, дает возможность находить решение с учётом эквивалентности СЗИ;

5. Руководствуясь предположением, что дублирование СЗИ на ряде узлов лишено смысла, в многокритериальной оптимизационной модели можно применить коэффициенты, учитывающие иерархию узлов в сети. Тогда, если обеспечена высокая степень защиты информации и кибербезопасность на узлах более высокого уровня, нет необходимости дублировать защиту на узлах более низкого уровня.

В процессе решения многокритериальной оптимизационной задачи в качестве «рюкзаков» выступают точки размещения СЗИ. К таковым можно отнести серверы, рабочие станции, коммутаторы, маршрутизаторы и др. В качестве предметов, которые находятся в рюкзаках выступают антивирусное ПО, межсетевые экраны и др. Тогда задача с точки зрения обеспечения КБ формулируется так: необходимо размесить в «рюкзаке» как можно больше СЗИ.

При это следует [13–18]: 1) обеспечить лучшую эффективность предметов; 2) не превысить заданных ограничений, например, на стоимость «рюкзака».

То есть, имеем постановку задачи с мультивыбором. Суть задачи с мультивыбором заключена в том, что все предметы разделяются на классы. Классы объединяют в себе только эквивалентные предметы, которые схожи по назначению. Обязательно реализовать выбор предмета из каждого имеющегося класса. То есть, например, для рассматриваемого с помощью СППР решения, обязательно необходимо, например, выбрать одну антивирусную программу их класса аналогичного программного обеспечения (ПО).

Следует отметить, что параметры (критерии CR_i), характеризующие эффективность различных СЗИ, принадлежащие к разным классам, как правило отличаются. Например, антивирусное ПО, если не принимать во внимание стоимость, можно охарактеризовать такими параметрами: «Полнота идентифицируемых видов киберугроз»; «Качество обнаружения вирусов»; «Влияние антивируса на производительность системы»; «Удобство их использования»; «Качество отчетов»; «Гибкая конфигурация»; «Регулярность обновления ядра антивируса»; «Поддержка средств архивирования»; и др. [17–22]:

Файерволы (программные межсетевые экраны), напротив характеризуют такими параметрами: совместимость с антивирусным ПО; контроль и нежелательного блокировка трафика; легкая настройка правил; автоматическая блокировка загрузки вредоносных файлов; предотвращение сканирования портов; др.

Свои собственные параметры, используемые в процессе выбора, и исходя из потребностей и стоимости имеют и другие СЗИ, т.е. криптографические средства шифрования; средства аутентификации и идентификации пользователей; средства контроля доступа; средства протоколирования и аудита и др.

В основном, при сравнении объектов, имеющих различные частичные критерии, применяются количественные оценки. Для этого каждой качественной оценке критерия ставится в соответствие определенный балл. Когда объект состоит из большого количества частных критериев используются обобщенные (глобальные, интегральные, синтетические, агрегированные, комплексные) оценки. Для расчета интегральной оценки в основном используется арифметическая сумма частных критериев: $IA_{\sum} = CR_1 + CR_2 + ... + CR_n$, где $IA_{\sum}$ – интегральная оценка кибернетической защищенности РВС, и CR_i – оценка i – того критерия.

Однако, использование интегральной оценки, в таком виде, имеет один существенный недостаток, связанный с невозможностью учета важности каждого из критериев, поэтому для решения данной задачи вводятся весовые коэффициенты важности [3, 18, 23]. Каждому критерию методом экспертных оценок задается весовой коэффициент важности. Данный коэффициент отражает вес анализируемого критерия в каждой отдельной ситуации. Расчет интегральной оценки осуществляется по формуле: $CR_{\sum} = w_1 \cdot CR_1 + w_2 \cdot CR_2 + ... + w_n \cdot CR_n$, где w_i – коэффициент важности i – того критерия. Чем больше вес w_i критерия CR_i тем больше его влияние на общую интегральную оценку средства защиты и КБ узла РВС $CR_{\sum}$ [2, 23-27].

Критерии считаются одинаково важным если $w_1 \cdot = w_2 = ...w_n = \frac{1}{n}$.

Особой задачей при расчете обобщенного критерия является способ добавления его частных критериев. На практике различают однородные и неоднородные критерии. Однородными считаются критерии, которые имеют одинаковую (единую, общую) шкалу оценок и могут быть сопоставимыми. Такие критерии легко сравниваются, поскольку для выяснения большей важности критерия, или же их эквивалентности, не нужно делать никаких дополнительных операций. Обязательным условием однородности является то, что каждая шкала градаций должна отражать одинаковый уровень преимуществ для каждого из критериев.

На практике существует большое количество задач, связанных с кибербезопасностью РВС, в которых используются неоднородные критерии. Например, критерии могут выражаться: 1) в количестве обнаруженных вирусов (для антивирусного ПО); 2) в количестве выявленных попыток получения НСД к ресурсам РВС (для систем обнаружения вторжений); 3) во времени, затраченном на обнаружение атак или обнаружении вируса; 4) в техническом состояние РВС до атаки и после ее успешной реализации (например, в баллах); и другое.

В таком случае для построения обобщенного критерия $CR_{\sum}$, все частичные критерии должны быть приведены к общей шкале оценивания (обычно такая шкала является безразмерной), то есть другими словами данные нужно нормировать [21]. Часто применяется так называемая "быстрая" нормализация.

Стоит отметить, что такое нормирования данных может привести к неверным рекомендациям. Поэтому для приведения всех критериев к одной шкале оценивания на интервале $[\alpha, \beta]$, целесообразно использовать линейное преобразование. Для реализации данного преобразования должно быть выполнено следующее условие $0 \le \alpha < \beta$, где $\alpha, \beta -$ левая и правая границы оценивания критерия. Значение нормированного критерия CR_i определяется по формуле:

$$\overline{CR}_i = \frac{CR_i - CR_i^+}{CR_i^+ - CR_i^-} \cdot (\beta - \alpha) + \alpha,$$

где $CR_i^+ = \max, CR_i^- = \min, CR_i^+ \ne CR_i^-, \quad i \in [1, m].$

Таким образом на первом этапе решения многокритериальной оптимизационной задачи по формированию наборов СЗИ для узлов РВС можно использовать результаты опросов экспертов. Анализ многих последних исследований в области решения оптимизационных задач в сфере выбор наборов СЗИ для ОИБ [7–18] показывает эффективность применения метода Т. Саати (метода анализа иерархий) для определения весовых коэффициентов важности при исчислении эффективности отдельных компонентов контуров защиты информации на узлах РВС.

Далее более детально остановимся на предлагаемых дополнениях метода динамического программирования для выбора СЗИ по узлам РВС.

В основе метода динамического программирования лежит принцип оптимальности Беллмана: "Каким бы ни было состояние системы перед следующим шагом, нужно выбирать так, чтобы выигрыш на этом этапе плюс оптимальный выигрыш на всех последующих шагах был оптимальным" [17]. Проще говоря оптимальное решение в *i*-м шаге находится, основываясь на найденных на предыдущих шагах оптимальных решениях. Отсюда, для того чтобы найти

оптимальное решение на последнем шаге нужно сначала найти оптимальное решение для всех предыдущих шагах, начиная с первого.

Анализ исследований методов динамической оптимизации (таблица 1) показал целесообразность использования метода динамического программирования, поэтому в работе за основу выбран именно этот метод. Он обеспечивает наилучшее быстродействие при больших объемах данных.

Применение метода динамического программирования для решения задачи упаковки рюкзака при определении активного состава СЗИ узла РВС, позволяет из множества средств защиты по параметрам (критериям):

1) эффективность (степень защищенности), которую, необходимо обеспечить, например, шкала 1–10, или иная);

2) минимальные затраты на СЗИ для РВС (Далее критерий стоимость СЗИ, например, шкала 1–100, или иная), отобрать определенное количество таким образом, чтобы получить максимальную суммарную эффективность СЗИ для РВС при одновременном соблюдении требований по суммарной максимальной стоимости защиты РВС в целом. То есть решение должно содержать такой набор предметов (средств защиты информации – СЗИ) суммарный «вес» (эффективность в предотвращении угроз и атак) которых должен быть максимально близкой к емкости рюкзака.

Выводы

Таким образом, в статье предложена многокритериальная оптимизационная модель, предназначенная для вычислительного ядра системы поддержки принятия решений (СППР), принимаемых в процессе системного анализа вариантов оптимального размещения средств кибербезопасности (КБ) и СЗИ распределенной вычислительной сети (РВС) предприятия или организации. В отличие от существующих, модель позволяет автоматизировать анализ различных вариантов СЗИ и КБ. Также модель позволяет учитывать, как отдельные факторы, влияющие на показатели защищённости РВС, так и их комбинации. К числу рассматриваемых в модели факторов можно отнести: варианты архитектур РВС; характеристики конкретного оборудования РВС организации или предприятия; классы угроз КБ; параметры угрозы, например, потенциальный ущерб от угрозы и/или вероятность ее возникновения; др. Подобный подход позволил реализовать как принципы эквивалентности СЗИ конкретной угрозе, так и системный комплексный подход к формированию высокоэффективной системы защиты для РВС.

На основе предложенной модели разработан и протестирован модифицированный алгоритм динамического программирования для определения активного состава СЗИ для узла РВС. Данный алгоритм может быть реализован в модуле адаптивной СППР по оптимизации наборов СЗИ и КБ для РВС.

Литература

1. Lakhno, V.A. (2020). Algorithms for Forming a Knowledge Base for Decision Support Systems in Cybersecurity Tasks, Advances in Intelligent Systems and Computing, 938, pp. 268–278.

2. Akhmetov, B. et al. (2019). Development of sectoral intellectualized expert systems and decision making support systems in cybersecurity, Advances in Intelligent Systems and Computing, 860, pp. 162–171.

3. Kartbayev, T., Akhmetov, B., Doszhanova, A. Et al. (2019). Development of decision support system based on feature matrix for cyber threat assessment, International Journal of Electronics and Telecommunications, 65 (4), pp. 545–550.

4. Sallam, H. (2015). Cyber security risk assessment using multi fuzzy inference system. IJEIT, 4(8), pp. 13–19.

5. Alali, M., Almogren, A., Hassan, M. M., Rassan, I. A., & Bhuiyan, M. Z. A. (2018). Improving risk assessment model of cyber security using fuzzy logic inference system. Computers & Security, 74, 323–339.

6. Abdenov, A. Z., Trushin, V. A., & Abdenova, G. A. (2018, January). Complex method to calculate objective assessments of information systems protection to improve expert assessments reliability. In Journal of Physics: Conference Series (Vol. 944, No. 1, p. 012001). IOP Publishing.

7. Akhmetov, B.S., Akhmetov, B.B. et al. (2019). Adaptive model of mutual financial investment procedure control in cybersecurity systems of situational transport centers, News of the National Academy of Sciences of the Republic of Kazakhstan, Series of Geology and Technical Sciences, 3 (435), pp. 159–172.

8. Adranova, A., Lakhno, V., Akhmetov, B. et al. (2019). Modeling of cyber threats in information networks of distance education systems, Journal of Theoretical and Applied Information Technology, Vol. 97, Iss., pp. 4921–4933.

9. Tse, D., Pan, X., Zong, Y., Liu, J., & Yang, Q. (2018, December). Assessing Information Security Risk Using Markov Chain. In 2018 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM) (pp. 808–813). IEEE.

10. Ma, D., Wang, L., Lei, C., Xu, Z., Zhang, H., & Li, M. (2017, April). Quantitative Security Assessment Method based on Entropy for Moving Target Defense. In Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security (pp. 920–922). ACM.

11. Mousavi, S. M., Moghadasi, M., & Fazekas, G. (2017, September). Dynamic resource allocation using combinatorial methods in Cloud: A case study. In 2017 8th IEEE International Conference on Cognitive Infocommunications (CogInfoCom) (pp. 000073–000078). IEEE.

12. Simos, D. E., Kampel, L., & Ozcan, M. (2018, June). Combinatorial Methods for Testing Communication Protocols in Smart Cities. In International Conference on Learning and Intelligent Optimization (pp. 437–440). Springer, Cham.

13. Akhmetov B., Lakhno V., Akhmetov B., Myakuhin Y., Adranova A., Kydyralina L. (2019) Models and Algorithms of Vector Optimization in Selecting Security Measures for Higher Education Institution's Information Learning Environment. Advances in Intelligent Systems and Computing, CoMeSySo 2018: Intelligent Systems in Cybernetics and Automation Control Theory, vol 860, pp. 135–142. Springer, Cham.

14. Mahanta, H. J., Khan, A. K., & Mukhopadhyay, S. (2019). Modular exponentiation with inner product to resist higher-order DPA attacks. Innovations in Systems and Software Engineering, pp. 1–11.

15. Augusto, A. A., Do Coutto Filho, M. B., de Souza, J. C. S., & Guimaraens, M. A. R. (2018). Branch-and-Bound Guided Search for Critical Elements in State Estimation. IEEE Transactions on Power Systems, 34(3), pp. 2292–2301.

16. Daniele, P., Maugeri, A., & Nagurney, A. (2017). Cybersecurity investments with nonlinear budget constraints: analysis of the marginal expected utilities. In Operations research, engineering, and cyber security (pp. 117-134). Springer, Cham.

17. Katzan, H. (2016). Contemporary Issues in Cybersecurity. Journal of Cybersecurity Research (JCR), 1(1), pp. 1–6.

18. Rodger, J. A., & George, J. A. (2017). Triple bottom line accounting for optimizing natural gas sustainability: A statistical linear programming fuzzy ILOWA

optimized sustainment model approach to reducing supply chain global cybersecurity vulnerability through information and communications technology. Journal of cleaner production, 142, pp. 1931–1949.

19. Lu, Q., Lin, Z., Liu, S., Zhu, Y., Yang, Y., & Cai, Q. (2018, October). DG Capacity Assessment in Distribution Network Considering Uncertainties Using Multi-Parametric Programming. In 2018 2nd IEEE Conference on Energy Internet and Energy System Integration (EI2) (pp. 1–4). IEEE.

20. Jana, D. K., & Ghosh, R. (2018). Novel interval type-2 fuzzy logic controller for improving risk assessment model of cyber security. Journal of information security and applications, 40, pp. 173–182.

21. Sarala, R., Zayaraz, G., & Vijayalakshmi, V. (2016). Fuzzy cognitive map-based reasoning for prediction of multi-stage attacks in risk assessment. International Journal of Intelligent Engineering Informatics, 4(2), pp. 151–167.

22. Sun, C. C., Hong, J., & Liu, C. C. (2016, June). A coordinated cyber attack detection system (CCADS) for multiple substations. In 2016 Power Systems Computation Conference (PSCC) (pp. 1–7). IEEE.

23. Yan, D., Liu, F., Zhang, Y., Jia, K., & Zhang, Y. (2018, August). Characterizing the Optimal Attack Strategy Decision in Cyber Epidemic Attacks with Limited Resources. In International Conference on Science of Cyber Security (pp. 65–80). Springer, Cham.

24. Lee, Y., Choi, T. J., & Ahn, C. W. (2019). Multi-objective evolutionary approach to select security solutions. CAAI Transactions on Intelligence Technology, 2(2), pp. 64–67.

25. Fielder, A., Panaousis, E., Malacaria, P., Hankin, C., & Smeraldi, F. (2016). Decision support approaches for cyber security investment. Decision Support Systems, 86, pp. 13–23.

26. Saurabh, P., Verma, B., & Sharma, S. (2012, October). Biologically inspired computer security system: the way ahead. In International Conference on Security in Computer Networks and Distributed Systems (pp. 474–484). Springer, Berlin, Heidelberg.

27. Erdogmus, D., & Principe, J. C. (2002). Generalized information potential criterion for adaptive system training. IEEE Transactions on Neural Networks, 13(5), pp. 1035–1044.

КЛЮЧЕВОЕ РАСПИСАНИЕ АЛГОРИТМА ШИФРОВАНИЯ ДАННЫХ «ВС-2»

Капалова Н., Хаумен А., Ержанов А.
e-mail: kapalova@ipic.kz, haumen.armanbek@gmail.com
Институт информационных и вычислительных технологий КН МОН РК, Казахстан

Аннотация. *Свойства ключевого расписания алгоритма шифрования являются определяющими при оценке стойкости алгоритма, так как при определенных условиях плохо подобранное ключевое расписание (или использование так называемых слабых и частично слабых ключей) может ослабить криптографические свойства итеративного блочного шифра. В данной работе приведены способы построения ключевого расписания алгоритма блочного шифрования «ВС-2» и описаны их свойства.*

Введение

Криптографическая стойкость (или криптостойкость) – это свойство криптографического алгоритма быть устойчивым к криптографическому анализу. Устойчивым называется тот алгоритмический код, успешное криптоаналитическое вскрытие которого предписывает заинтересованному лицу иметь в своѐм распоряжении настолько колоссальные вычислительно-алгоритмические или временные ресурсы на дешифровку перехваченных сообщений, что задачу решить либо практически невозможно, либо к тому времени, когда она будет решена, засекреченная информация утратит свою ценность для злоумышленников.

Ключевое расписание блочного шифра является важным компонентом его строения, определяющим его криптографическую стойкость. Применение многих методов криптоанализа затруднено, если алгоритм развертывания ключа обеспечивает сложную нелинейную зависимость битов раундовых ключей от битов основного ключа [1].

Свойства ключевого расписания, характеризующие взаимосвязи основного ключа с раундовыми ключами являются определяющими при оценке стойкости итеративного блочного шифра относительно ряда методов криптоанализа: согласования, дифференциального и др. Например, нежелательным является ключевое расписание, при котором генерируемая из основного ключа последовательность раундовых ключей содержит определенное число повторяющихся элементов. Так, по отношению к основному ключу при криптографическом анализе алгоритма DES введено понятие слабого ключа, то есть основного ключа, порождающего 16 одинаковых раундовых ключей [2].

Одной из причин ненадежности криптосистем является использование слабых ключей. Фундаментальное допущение криптоанализа, впервые сформулированное О.Кирхгоффом, состоит/ в том, что секретность сообщения всецело зависит от ключа, т.е. весь механизм шифрования, кроме значения ключа, известен противнику. Слабый ключ– это ключ, не обеспечивающий достаточного уровня защиты или использующий в шифровании закономерности, которые могут быть взломаны.

Алгоритм шифрования не должен иметь слабых ключей. Если это невозможно, то количество слабых ключей должно быть минимальным, чтобы уменьшить вероятность случайного выбора одного из них; все слабые ключи должны быть известны заранее, чтобы их можно было отбраковать в процессе создания ключей.

Генераторы случайных чисел - еще один источник угрозы для стойкости криптосистемы. Если для генерации ключей используется криптографический слабый алгоритм, независимо от используемого шифра вся система будет нестойкой. Качественный ключ, предназначенный для использования в рамках симметричной криптосистемы, представляет собой случайный двоичный набор. Если требуется ключ разрядностью n, в процессе его генерации с одинаковой вероятностью должен получаться любой из 2^n возможных вариантов. Важной частью для безопасности ключа является наличие рандомных входных данных на стадии генерации ключа. Если в этих входных данных недостаточно энтропии, то атакующий сможет их угадать и получить таким образом секретный ключ без мучительной факторизации числа N.

Отсюда с однозначностью вытекает принципиальная важность формирования ключей: ключи должны выбираться случайно, чтобы исключалась возможность их отгадывания на основе каких-либо ассоциаций.

Неудачное построенное ключевое расписание блочного шифра может заметно ослабить криптографические свойства алгоритма шифрования. Поэтому особое внимание должно уделяться на ключевое расписание создаваемого шифра [3].

Ключевое расписание алгоритма шифрования «BC-2»

В институте информационных и вычислительных технологий по руководством Р.Бияшева и С.Нысанбаевой созданы симметричные блочные алгоритмы шифрования данных. Один из этих алгаритмов является алгоритм «BC-2» (сокращенное от слова BlockCipher).

Алгоритм шифрует данные блоками по 256 бит, длина ключа составляет 512 бит.

Алгоритм BC-2 разработан на основе SP-сети. Использование SP-сети позволяет выполнить преобразования над всем входным блоком целиком, а не только над его половиной.

Процесс шифрования состоит из нескольких раундов, каждый из которых включает в себя несколько преобразований, а именно три:

- *AddKey* –сложение по модулю 2 (xor) с раундовым ключом;
- *Conversion-S* – замена с помощью таблиц подстановок;
- *Conversion-MB* (MixBlcok) – линейное преобразование.

Количество раундов шифрования 10. В каждом раунде над шифруемыми данными поочередно выполняются перечисленные выше преобразования [4].

Генерация раундовых ключей

Пусть K— ключ итеративного блочного алгоритма шифрования. Тогда ключевым расписанием называется система функций $\{\theta_1,\theta_2,\ldots, \theta_r\}$, при помощи которой ключ K расширяется до r ключей $k_1,\ldots, k_r$. В большинстве случаев r - число раундов итеративного блочного шифра.

Раундовые ключи получаются путем определенных преобразований на основе мастер-ключа, длина которого, составляет 512 бит. Этот процесс начинается с разбиения мастер-ключа пополам, так получается первая пара раундовых ключей. Для генерации каждой последующей пары раундовых ключей применяется 10 итераций сети Фейстеля, в каждой итерации используются функции преобразования **S, MB и ROL** (Рис. 1). Преобразования **S** и **MB** используются в самом алгоритме «BC-2».

Преобразование S

Нелинейное преобразование S использует операции с байтами. К каждому байту применяется нелинейная биективная *подстановка*, задаваемая одномерным массивом, состоящих из 256 элементов. 256-битный блок данных поступает на вход преобразования S и разбивается на 32 байтов. Каждый байт входного блока – это индекс значения, находящегося в таблице подстановок. Таким образом, на выходе преобразования S будет набор байтов, находящихся по соответствующим индексам в заданном таблице подстановок:

$c_i = S[b_i],\ i = \overline{0,31}.$

Далее этот блок подается на вход линейного преобразования MB, в котором блок разбивается на 32 байта.

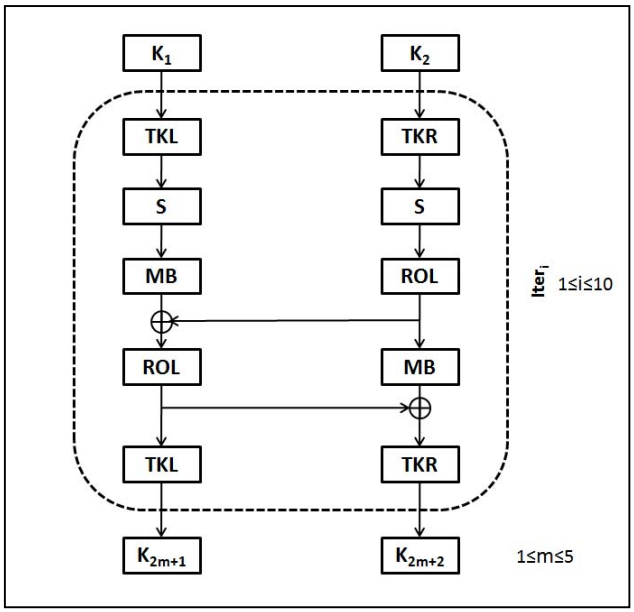


Рис. 1 Схема генерации раундовых ключей

Преобразование MB

Это линейное преобразование алгоритма BC-2. Преобразование **MB** (MixBlock) перемешивает байты в блоке.

Преобразование **MB** осуществляется следующим образом:

1. Каждый байт в блоке умножается на соответствующий ему коэффициент в поле GF(2^8) по модулю $x^8 + x^4 + x^3 + x^2 + 1$. Коэффициенты являются элементами блока-констант **C**. После операции умножения выполняется операция сложения всех 32-хбайтов между собой по модулью 2 (битовое сложение).

2. Полученное число записывается 32-ым байтом, а все остальные байты сдвигаются на один байт вправо, тем самым вытесняя самый крайний правый байт. Подобные расчеты проводятся 32 раза, в результате получаем новое 32-х байтное значение (Рис. 2).

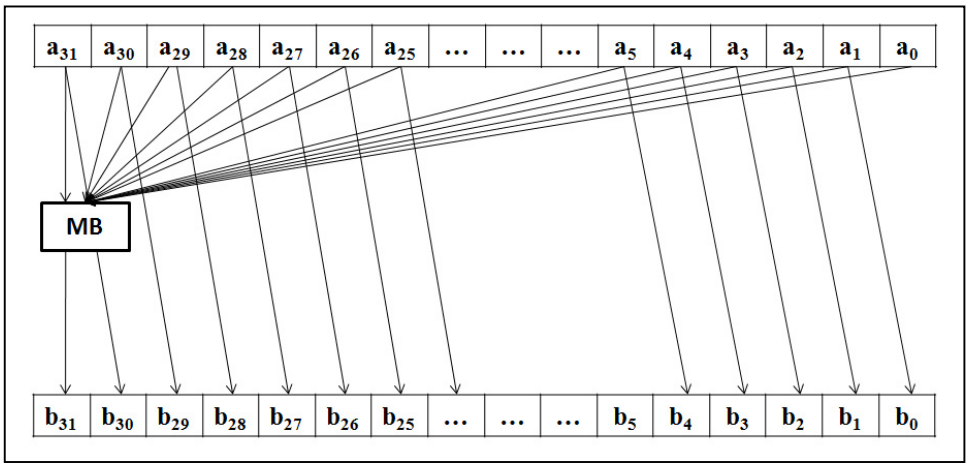


Рис.2 Схема линейного преобразования MB

Блок-констант **C**состоит из 32 элементов.

C(32) = (17, 39, 191, 203, 67, 173, 43, 197, 61, 13, 59, 131, 227, 7, 101, 83, 41, 149, 71, 127, 19, 137, 113, 53, 157, 241, 73, 181, 223, 109, 157, 23).

Преобразование **ROL**–есть циклический сдвиг битов блока налево на одну позицию.

Для изучения свойства ключевого расписания алгоритма «BC-2», была разработана компьютерная программа на языке программирования Delphi.

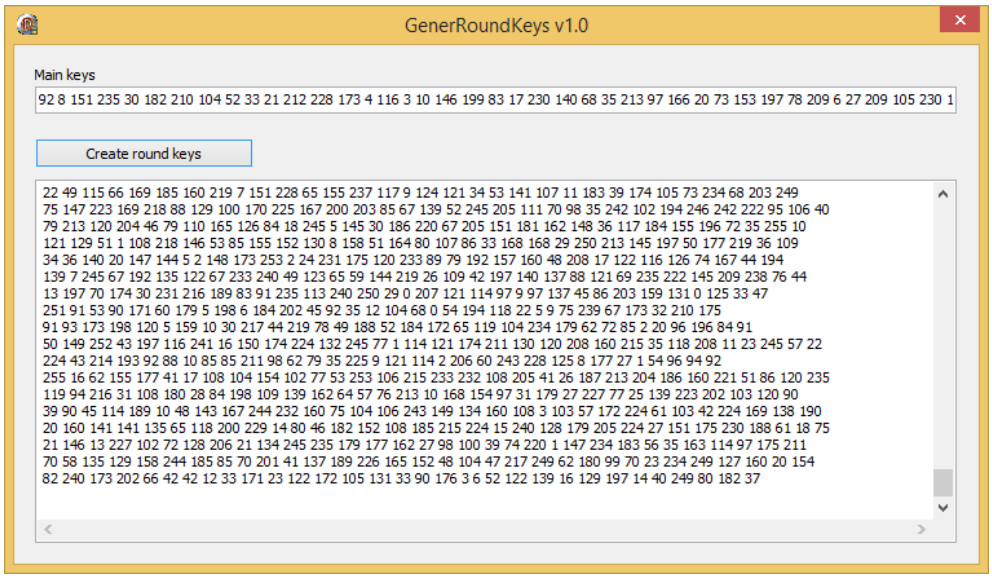


Рис. 3 Скриншот экрана программы для генерации раундового ключа

С помощью данной компьютерной программы мы можем получит ключевые последовательности любой длины. Результатом программы будет бинарный файл, который содержит последовательности байтов (Рис. 3).

Идеальными считаются ключевые последовательности, похожие на случайную последовательность. Поэтому ключевую последовательность алгоритма «BC-2»нужно тестировать различными тестами для ПСП.

На первом этапе полученные файлы тестировались с помощью графических тестов. На рисунках 4 и 5 представлены результаты этих тестов.

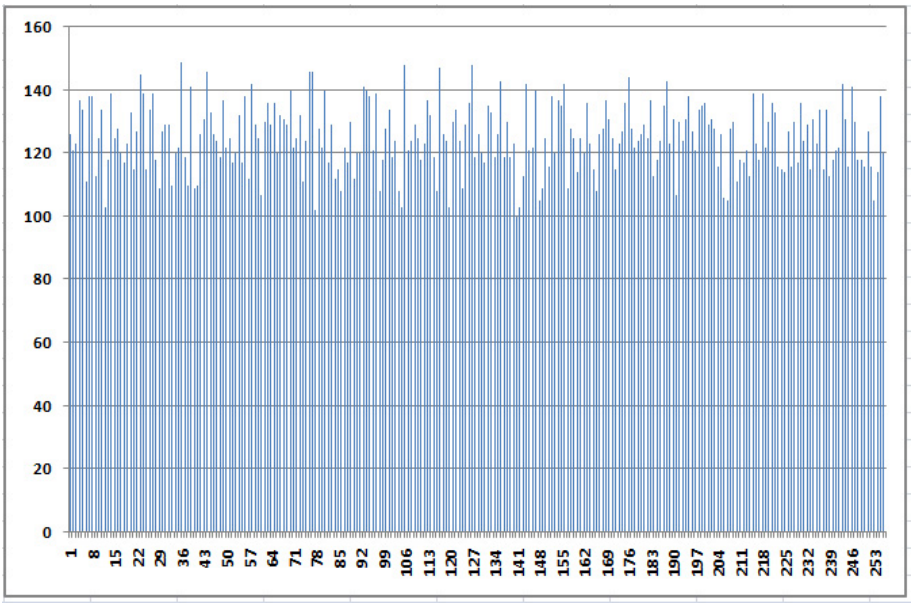


Рис. 4 Результат графического теста (распределение байтов)

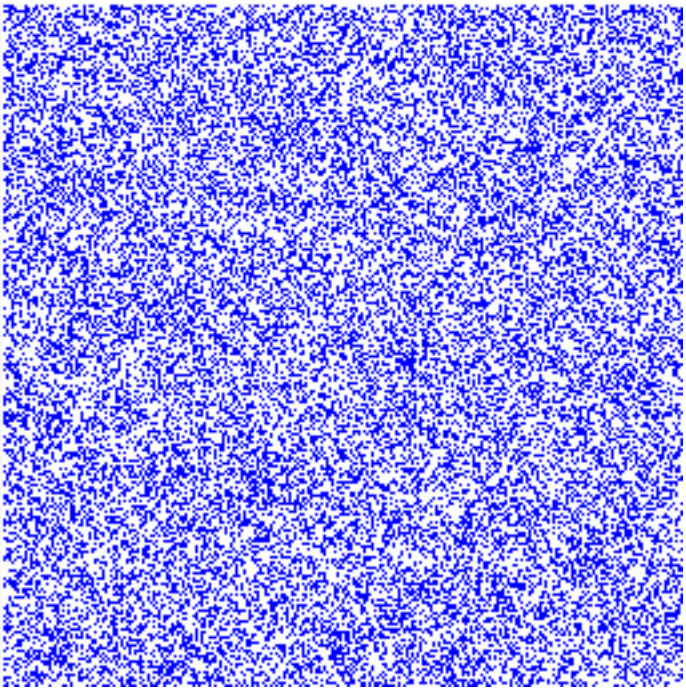


Рис. 5 Результат графического теста (расположение байтов на плоскости)

На данном этапе результаты многих экспериментальных тестов дают полижительные результаты.

Заключение

Следующим этапом данной работы является тестирование ключевых последовательностей, получаемых в результате ключевого расписания на известных тестах ПСП, определения недостатков и поиск методов устранения их.

Благодарность

Научно-исследовательская работа выполнена в рамках проекта BR05236757- «Разработка программных и программно-аппаратных средств для криптографической защиты информации при ее передаче и хранении в инфокоммуникационных системах и сетях общего назначения» в Институте информационных и вычислительных технологий.

Литература

1. Фомичев В.М., Коренева А.М., Тулебаев А.И. О параметрах генератора раундовых ключей алгоритма 2-ГОСТ // Прикладная дискретная математика. Приложение, 2019. – № 12.-С.137-141.
2. Фомичев В. М. О ключевом расписании блочных шифров без слабых ключей // Томский государственный университет. Прикладная дискретная математика. Приложение, 2016 –№ 9. С. 70–73.
3. Фомичев В. М. Дискретная математикаи криптология / М.: Диалог-МИФИ, 2003.– С.302-306.
4. Капалова Н.А., Хаумен А. Симметричный блочный алгоритм шифрования данных «ВС-2»// «Безопасные информационные технологии». Сборник трудов Десятой международной научно-технической конференции – М.: МГТУ им. Н.Э. Баумана, 2019.- С. 161-166.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И КИБЕРБЕЗОПАСНОСТЬ В КАЗАХСТАНЕ

Калимолдаев М.Н., Бияшев Р.Г., Нысанбаева С.Е., Капалова Н.А.
e-mail: mnk@ipic.kz, brg@ipic.kz, kapalova@ipic.kz, sultasha1@mail.ru
Институт информационных и вычислительных технологий КН МОН РК
Казахстан

Аннотация. *В данной работе приведены основные характеристики о защите информации – информационной безопасности и кибербезопасности, а также основные направления проводимых научно-исследовательских работ в Институте информационных и вычислительных технологий (ИИВТ) КН МОН РК по разработке и исследованию систем криптографической защиты информации.*

Введение

Информационная безопасность - показатель гарантированной защиты как отдельной личности, так и каждой организации (государства) и их разносторонних интересов от любых деструктивных угроз и/или воздействий в информационном пространстве. Принято считать, что информационная безопасность - это комплекс мероприятий, обеспечивающий следующие факторы:

- конфиденциальность;
- целостность;
- доступность.

Целостность информации (или данных) - означает, что данные не были изменены при выполнении любой операции над ними, будь то передача, хранение или представление. Целостность подразумевает под собой возможность передачи

информации и работы с ней без ее потери или видоизменения. Возможностью изменения информации должны обладать уполномоченные лица.

Конфиденциальность (от англ. confidence - доверие) - необходимость предотвращения утечки (разглашения) какой-либо информации. Чаще всего такой информацией может, является служебная тайна или «ноу-хау».

Доступность - это открытость информации пользователям или объектам в соответствии с предоставленными им правами доступа.

Об информационной безопасность и кибербезопасности в Казахстане

Информационная безопасность имеет дело с информацией и данными как онлайн, так и офлайн. Она определяется как защита информации от несанкционированного использования, раскрытия, разрушения, изменения и т. д. С информационной безопасности, как с основы безопасности защищаемых данных, начинают создание защиты информационных систем от нежелательных воздействий.

Кибербезопасность же связана исключительно с цифровой сферой и касается всего, что связано с Интернетом. Это включает в себя все учетные записи в Интернете, интернет-соединения, фишинг, травлю, взлом данных и т. Д. Кибербезопасность связана с киберпространством, а также включает данные и информацию в этой сфере. В этом состоит суть разницы: кибербезопасность связана исключительно с цифровой сферой и касается всего, что связано с Интернетом, а информационная безопасность имеет дело с информацией и данными. Таким образом, разница между информационной безопасностью и кибербезопасностью заключается в том, что информационная безопасность защищает физическую и цифровую информацию, а кибербезопасность защищает только цифровую информацию. Или, информационная безопасность предотвращает несанкционированный доступ любого рода, в то время как кибербезопасность предотвращает несанкционированный цифровой доступ.

В последние годы различные аспекты обеспечения информационной безопасности в области информатизации и связи нашли свое отражение и развитие в Уголовном кодексе Республики Казахстан, Кодексе Республики Казахстан "Об административных правонарушениях", законах Республики Казахстан "О государственных секретах", "О персональных данных и их защите", "Об электронном документе и электронной цифровой подписи", "О связи", и целом ряде подзаконных актов, разработанных в реализацию новой редакции Закона Республики Казахстан "Об информатизации", вступившего в силу с 1 января 2016 года.

Подтверждается это и Постановленим Правительства Республики Казахстан от 30 июня 2017 года № 407 об утверждении Концепции кибербезопасности ("Киберщит Казахстан"), далее Концепция. Она основана на оценке текущей ситуации в сфере информатизации государственных органов, автоматизации государственных услуг, перспектив развития "цифровой" экономики и технологической модернизации производственных процессов в промышленности, расширения сферы оказания информационно-коммуникационных услуг. Концепция определяет основные направления реализации государственной политики в сфере защиты электронных информационных ресурсов, информационных систем и сетей телекоммуникаций, обеспечения безопасного использования информационно-коммуникационных технологий (ИКТ).

Для последних десятилетий характерна общемировая тенденция использования достижений информационно-коммуникационных технологий по сравнению с темпами формирования культуры их использования. В Концепции указывается на необходимость единства подходов к мониторингу обеспечения информационной безопасности государственных органов, физических и юридических лиц, а также выработку механизмов предупреждения и оперативного реагирования на инциденты информационной безопасности, в том числе в условиях чрезвычайных ситуаций социального, природного и техногенного характера, введения чрезвычайного или военного положения.

В ней также указывается на то, что

- наиболее чувствительная для безопасности государства информация в электронной форме передается только через сети телекоммуникаций специального назначения, физически отделенные от Интернета и использующие криптографические средства защиты информации;
- необходимо преодоление проблемы не высокой востребованности отечественных разработок, т.к. кибербезопасность в конечном итоге зависит от уровня развития отечественной IT-отрасли и электронной промышленности. Одной из причин этого является отсутствие обязательности приоритетного использования их продукции в государственных органах.

В Концепции кибербезопасности «Киберщит Казахстана» укатывается также и на то, что необходимо осуществлять «Предоставление приоритета исследованиям и собственной школе прикладной математики, по разработке средств криптографической защиты информации, криптологии, разработок по программируемым логическим интегральным схемам, квантовой криптографии и разработке защиты систем передачи, обработки и хранения информации, а также систем информационной безопасности».

Разработка систем защиты информации в ИИВТ КН МОН РК

В нашем Институте проводятся научно-исследовательские работы по разработке, исследованию криптографических систем (шифрования, электронной цифровой подписи, управления ключами) и создание на их основе систем криптографической защиты информации. Достигается это путем

- разработки систем симметричного блочного шифрования при хранении и передаче информации, в том числе с использованием модулярных систем счисления;
- анализа надежности и эффективности разработанных систем шифрования;
- создания **программных средств для расчёта и** хранения параметров разработанных криптосистем;
- программной реализации разработанных систем шифрования;
- разработки системы защиты хранимой и передаваемой информации на основе разработанных систем шифрования;
- сертификация разработанных компьютерных программ, подача заявок на получение авторских свидетельств.

Институт имеет государственную лицензию «На осуществление деятельности по разработке и реализации (в том числе иной передаче) средств криптографической защиты информации», выданную Комитетом национальной безопасности РК 03 июля 2017 г., номер лицензии 549.

В Казахстане в настоящее время в действующих системах защиты электронных данных используются зарубежные криптографические алгоритмы и

стандарты. Стандарты шифрования приняты во многих зарубежных государствах: США, России, Беларуси, Украине, Узбекистане:

1. ГОСТ Р 34.12-2015. Информационная технология. Криптографическая защита информации. Блочные шифры. – Москва, 2016;
2. FIPS 46-3. Data Encryption Standard (DES). - USA, NIST, 1977;
3. FIPS PUB 197. Advanced Encryption Standard (AES). – USA, NIST, 2002;
4. ГОСТ 28147-89. Система обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. – М.: Госстандарт СССР, 1989;
5. ДСТУ 4145-2002. [электронный ресурс]: Режим доступа: http://ru.wikipedia.org/wiki/ ДСТУ 4145-2002, свободный (дата обращения: 7.07.2014);
6. BelT [электронный ресурс]: Режим доступа: http://ru.wikipedia.org/wiki/BelT, свободный (дата обращения: 7.07.2014);
7. O.z DSt 1105:2006. Информационная технология. Криптографическая защита информации. Алгоритм шифрования данных // Государственный стандарт Узбекистана. - Дата введения 01.10.2006.

Проводимые исследования нацелены на создание отечественных алгоритмов криптографической защиты информации, в том числе с использованием современного алгебраического подхода на базе модулярных систем счисления. Разработка систем криптографической защиты информации для обеспечения надежной защиты информации при ее хранении и передаче проводиться на основе разработанных алгоритмов шифрования и средств программной/ программно-аппаратной реализации.

Основные полученные результаты представлены в следующих публикациях:

1. Biyashev, R.G., Kalimoldayev M.N., Nyssanbayeva, S.E., Kapalova N.A., Dyusenbayev, D.S., Algazy K.T., Development anod analysis of the encryption algorithm in nonpositional polynomial notations // Eurasian Journal of Mathematical and Computer Applications. – 2018. - № 6(2). - С.19-33.
2. Капалова Н.А., Дюсенбаев Д.С., Алгазы К.Т., Хаумен А. Линейный криптоанализ для одного раунда алгоритма «KazCipher с использованием SP сети» // Матер. XIV Междунар. Азиатской школы-семинара "Проблемы оптимизации сложных систем". - Кыргызская Республика. с. Кара-Ой, 2018. – Ч.1. – С. 283-290.
3. Дюсенбаев Д., Сақан Қ. «AL01» шифрлау алгоритміне криптографиялық талдау // Материалы IV международной научно-практической конференции «Информатика и прикладная математика» -Ч.2. – Алматы, 2019. – С. 561-569.
4. Нысанбаева С.Е., Варенников А.В. Формирование базы данных неприводимых многочленов над конечным полем $GF(2)$ // Материалы IV международной научно-практической конференции «Информатика и прикладная математика» -Ч.2. – Алматы, 2019. – С. 630-638.
5. Бияшев Р.Г., Алгазы К.Т., Дюсенбаев Д.С., Ержанов Е.Б. Результаты проверки «лавинного эффекта» алгоритма «AL01» // Материалы IV международной научно-практической конференции «Информатика и прикладная математика» -Ч.2. – Алматы, 2019. – С. 602-607.
6. Капалова Н.А., Хомпыш А., Алгазы К.Т. ЕМ түрлендіру әдісі негізінде жасалған блокты шифрлеу алгоритміне жүргізілген бағалау тесттері // Материалы IV международной научно-практической конференции «Информатика и прикладная математика» -Ч.2. – Алматы, 2019. – С. 580-587.

7. Сақан Қ., Алғазы К. Программная реализация алгоритма симметричного блочного шифрования «Qamal» для исследования его криптографических свойств // Матер. науч. конф. ИИВТ МОН РК «Современные проблемы информатики и вычислительных технологий». – Алматы, 2019. - С. 269-275.

8. Хомпыш А., Криптостойкости S-блоков в алгоритме шифрования на основе EM // Материалы XXIII молодёжной международной научно-практической конференции студентов, аспирантов и молодых учёных. - Санкт-Петербург, 2019. - С. 15-19

9. Пирожников А.Г., Дюсенбаев Д.С., Некоторые следствия теоремы Вильсона // Материалы IV международной научно-практической конференции «Информатика и прикладная математика» -Ч.1, – Алматы, 2019. – С. 301-304

10.Бегимбаева Е.Е., Усатова О.А., Бияшев Р.Г., Нысанбаева С.Е., Вуйцик В. Разработка модулей для защиты информации в автоматизированной системе с применением разграничения доступа // Материалы IV международной научно-практической конференции «Информатика и прикладная математика» -Ч.2. – Алматы, 2019. – С. 595-602.

11.Абдикаликов К.А. Криптостойкость системы шифрования RSA // Материалы IV международной научно-практической конференции «Информатика и прикладная математика» -Ч.2. – Алматы, 2019. – С. 587-592.

12.А. с. 4211. Объект авторского права под названием «Sandyq v 1.02» (программа для ЭВМ) / Нысанбаева С. Е., Капалова Н. А., Хаумен А.; опубл. 25.06.2019, МЮ РК

13.А. с. 5200. Объект авторского права под названием «Qamal v 1.0.1» (программа для ЭВМ) / Бияшев Р.Г., Капалова Н. А., Алгазы К.Т., Дюсенбаева Д.С., Сақан Қ.С.; опубл. 06.09.2019, МЮ РК

14.А. с. 5450. Объект авторского права под названием «Программа шифрования файлов «CryptoEM v1.0.1»» (программа для ЭВМ) / Капалова Н. А., Хомпыш А.; опубл. 24.09.2019, МЮ РК.

КОМПЬЮТЕРЛІК ЖҮЙЕЛЕРДЕГІ (КЖ) КИБЕРШАБУЫЛДАРДЫ АНЫҚТАУДЫҢ ЗАМАНАУИ ЖҮЙЕЛЕРІН ТАЛДАУ

Ахметов Б.С., Лахно В.А., Ыдырышбаева М.Б.
e-mail: moldir.ydyryshbaeva@gmail.com
Әл-Фараби атындағы Қазақ Ұлттық Университеті, Қазақстан

Аңдатпа. *Ақпараттық жүйелердегі (АЖ) немесе компьютерлік жүйелердегі (КЖ) күрделі мақсатты кибершабуылдардың артуы, ақпараттық қауіпсіздік (АҚ) және оның құрамдас бөлігі киберқауіпсіздік (КҚ) болып табылатын қоғамның маңызды мәселелерін тудырады. Шабуылдар кезінде киберқылмыскерлер бірегей зиянды бағдарламалар мен АЖ-ға ену әдістерін жиі қолданады. АЖ-де көпкезеңді мақсатты кибершабуылдарды жүзеге асырудың күрделі формализацияланған типтік емес жағдайларында КҚ басқару үшін ШҚҚЖ модельдері мен бағдарламалық қамтамасыз етілуін дамыту қажеттілігі туындайды. Осыған сәйкес, олардың қалыпты жұмыс істеуін қамтамасыз ету және басып кіруді болдырмау үшін арнайы қауіпсіздік құралдары қажет. Ақпараттық қауіпсіздік*

саласында белсенді дамып келе жатқан бағыт кибершабуылдарды анықтау және ақпараттық жүйелерде басып кіруді болдырмау болып табылады. Компьютерлік жүйеде басып кіруді болдырмау үшін әртүрлі әдістер, модельдер, құралдар қолданылады. Нәтижесінде компьютерлік жүйелердегі кибершабуылдарды анықтаудың қазіргі заманғы жүйелеріне талдау жасалынды.

Ақпараттық жүйелер (АЖ) мен ақпараттық технологиялардың (АТ) жаһандық қарқынды дамуы қоғам қызметінің барлық салаларына жан-жақты әсер етеді. Бүгінде экономикаларды цифрландыру жағдайында қазіргі заманғы мемлекеттік және жеке компаниялардың басым көпшілігі өндірістік және бизнес процестерді басқару, шешімдер қабылдауды қолдау, қажетті деректерді іздеу және т.б. үшін АЖ-ны іске қосты. Ақпараттық технологиялардың дамуына сәйкес компьютерлік жүйелер

Сонымен қатар, АЖ және АТ компанияларының бизнес процестеріне терең интеграциялау ақпараттандыру объектілері үшін кибернетикалық қауіптердің санын ұлғайтты. Сонымен қатар, біз сыртқы және ішкі қауіптердің өсуі туралы айтып отырмыз. Сондықтан компаниялардың қалыпты жұмыс істеуін қамтамасыз ету, олардың АЖ және басып кіруді болдырмау үшін қатерлерді жоюға арналған барабар ұйымдастырушылық және техникалық шаралар қажет. Ең алдымен, кибернетикалық шабуылдар сценарийлерінің күрделілігінің өсуі жағдайында арнайы кибернетикалық қауіпсіздік құралдарына (КҚ) назар аудару керек.

Соңғы онжылдықта АҚ және КҚ саласында белсенді дамып келе жатқан өзекті бағыттардың бірі кибершабуылдарды анықтау және авторланбаған тарап тарапынан АЖ-ға басып кіруді болдырмау болып табылатынын атап өткен жөн.

КҚ мәселелеріне маманданған жетекші компаниялардың [1, б. 7-10, 2, б. 12, 3, б. 7, 9] жыл сайынғы талдамалық есептері көрсетіп отырғандай, бөлінген АЖ-ға шабуылдар жыл сайын жетілдіре түсуде. Қазіргі кибернетикалық шабуылдар жаһандық сипатқа [5, б. 7] ие болып отыр.

Жаппай кибернетикалық шабуылдар АҚ және КҚ әртүрлі ақпараттандыру объектілерін (АҚҚе) қамтамасыз ету саласындағы инновациялық зерттеулердің тұтас толқынын тудырды. Сонымен қатар, арнайы техникалық шешімдер – шабуылдарға қарсы іс-қимыл құралдары мен жүйелерін әзірлеуге және жасауға бағыт берді

Желілік шабуылдарды анықтау үшін бүгінгі таңда КҚ мамандары заманауи әдістердің [4-6], модельдердің[7-8], құралдардың [9, 10], бағдарламалық қамтамасыз ету құралдардың (БҚ) [11, 12] барлық мүмкіндігін қолданады. Кешенді техникалық шешімдер де кеңінен қолданыла бастады [13, 14]. Сонымен қатар, бұл шешімдердің ажырамас бөлігі ретінде басып кіруді анықтау жүйелері (БКАЖ) қарастырылады [15, 16]. БКАЖ қолдану қазіргі заманғы шабуылдардың көпшілігін болдырмауға мүмкіндік береді және киберқауіптер мен шабуылдардың жаңа немесе өзгертілендірілген түрлері пайда болған кезде олар айтарлықтай тиімді жұмыс істей алады.

[17, 18] жұмыстарда AAFID, ASAX, Bro, NetSTAT, Prelude SIEM, Shadow, Snort и SnortNet, SolarWinds NPM бағдарламалық құралдары туралы толық сипаттама берілген. БАКЖ класына жататын заманауи бағдарламалық өнімдерді

объективті бағалау үшін төменде тиісті іске асырудың аппараттық-бағдарламалық құралдары Cisco IPS,Cisco IPS, OSSEC, Kaspersky Anti Targeted Attack Platform, InfoWatch ASAP, Tipping Poing NGIPS, Arbor Networks Spectrum, DefensePro DDoS Defense & DDoS Prevention Device және т.б. көрсетілген. Талдау кезінде алынған деректерді жүйелеу үшін 1.2 және 1.3 кестелер жасалды, бұл БКАЖ үшін бірқатар критерийлер бойынша артықшылықтар мен белгілі бір шектеулерді жалпылауға мүмкіндік береді. 1.2-кестеде БКАЖ ашық жүйелері көрсетілген. 1.3-кестеде БКАЖ жабық жүйелері көрсетілген.

1-кесте. БКАЖ ашық жүйелерін талдау нәтижесі, ([19, б. 17-20, 20, б. 205] әдебиеттері негізінде)

	КАЖ	Аномалиялар мен шабуылдарды анықтау әдістері											Жүйені басқару		Масштабталулық	Ба қылау деңгейі		Кибершабуылға немесе аномалияға	Қауіпсіздік	Опе рациялық жүйелерді (ОЖ) қолдау			БКАЖ бейімділік	Шешімдерді қодау
		Сараптамалық	Статистикалық	Сигнатуралық	Сценарий графтары	Өзгерістерді бақылау	Кластерлік	Динамикалық	Машиналық оқыту	Мінездік талдау	Эвристикалық	Анық емес логика	Орталықтандырылған	Үлестірілген		Жүйелік	Желілік			Unix & Linux	Windows	MacOS		
	AFID																							
	nort																							
	relude IEM							+																
	etSTAT																							
	SAX																							
	ro																							
	SSEC											/+											/+	
	uricata																							
	amhain																							
0	ecurity nion											/+												

Белгілеу: (+) – параметрдің болуы; (-) – параметрдің болмауы; (-/+) – параметрдің ішінара болуы

2-кесте. Басып кіруді анықтау құралдарын талдау нәтижелері, ([19, б. 22-27, 20, б. 206] әдебиеттері негізінде)

	КАЖ	Аномалиялар мен шабуылдарды анықтау әдістері																					
		Сараптамалық	Статистикалық	Сигнатуралық	Сценарий графтары			Динамикалық			Эвристикалық	Анық емес логика	Орталықтандырылған	Үлестірілген	Масштабталулық	Жүйелік	Желілік	Кибершабуылға немесе ақылау деңгейі	Қауіпсіздік	Unix & Linux	Windows	MacOS	БКАЖ бейімділік	Шешімдерді қодау
	Shadow																							
	Cisco IPS																							
	Arbor NetSp																							
	InfoWatch ASAP																							
	Symantec DTMS																							
	IPS																							
	Tipping Poing NGIPS																							/+
	Axoft invGUARD																							
	DefensePro																							
0	KATA P																							

	latform																						

Қазіргі заманғы рұқсатсыз басып кіруді анықтау әдістері мен БКАЖ талдауға арналған көптеген мақалалар мен зерттеулер бар. 1, 2 кестелерінде ұсынылған деректерді талдау көрсеткендей, қазіргі заманғы БКАЖ-де әртүрлі математикалық әдістерді қолданады. Талдау нәтижесі көрсеткендей, қазіргі заманғы БКАЖ-нің көпшілігінде талдауға арналған модульдер бар және күрделі мақсатты шабуылдарды шешуге қолдау көрсетеді. Осы тұрғыда бізге интеллектуалды ШҚҚЖ әлеуетін пайдалану туралы айтуға болады, оның алгоритмдері өз кезегінде деректерді талдаудың математикалық әдістеріне, Data Mining, болжауға және т.б. негізделген.

Соңғы жылдары АҚҚе-ге жасалған кибершабуылдар санының өсуі тиімді БКАЖ жасауға қызығушылық тудырды. Осы саладағы зерттеулердің перспективалы және жеткілікті жаңа бағыты АҚ және КҚ саласындағы ШҚҚЖ [21] және сараптамалық жүйелердің (СЖ) [22] әдістерін, модельдері мен бағдарламалық кешендерін дамыту жөніндегі жұмыстар болды.

Осылайша, қарастырылған жұмыстардағы қарама-қайшылықты ескере отырып, АҚҚе КҚ саласындағы ШҚҚЖ үшін іс жүзінде жүзеге асырылатын шешімдер бойынша зерттеулерді жалғастыру қажет екені анық. Мұндай зерттеулер, атап айтқанда, БКАЖ үшін күрделі форматталған типтік емес мәселелерді шешуге бағытталуы керек (мысалы, көп сатылы бағытталған кибершабуылдарды жүзеге асыру процестерінде).

Аталған мәселе өзекті болғандықтан, ғалымдар мен зерттеушілер компьютерлік жүйелерде киберқауіпсіздікті анықтайтын әмбебап және болашақта қолданылатын әдістерді іздеуді жалғастыруда.

Әдебиеттер

1. Годовой отчет компаний Cisco по информационной безопасности - https://www.cisco.com/c/dam/global/ru_ru/assets/offers/assets/cisco_2018_acr_ru.pdf (04.04.2020)

2. Отчет «Понимание кибер-угроз 2020» - https://www.cloudav.ru/upload/iblock/b58/PandaLabs%20-%20Threat-Insights-2020.pdf (10.01.2020)

3. Итоги внутренних пентестов – 2020 - https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/internal-pentests-2020-rus.pdf (05.03.2020)

4. Стасюк, А. И., & Корченко, А. А. (2012). Метод выявления аномалий порожденных кибер атаками в компьютерных сетях. Захист інформації, 14(4), 127-132.

5. Корченко, А. (2014). Метод фаззификации параметров на лингвистических эталонах для систем выявления кибератак. Безпека інформації, (20, № 1), 21-28.

6. Корченко, А. (2014). Метод определения идентифицирующих термов для систем обнаружения вторжений. Безпека інформації, (20,№ 3), 217-223.

7. Корченко, А. А. (2012). Модель эвристических правил на логико-лингвистических связках для обнаружения аномалий в компьютерных системах. Захист інформації, 14(4), 109-115.

8. Бекетова, Г. С., Ахметов, Б. Б., Корченко, О. Г., & Лахно, В. А. (2016). Розробка моделі інтелектуального розпізнавання аномалій і кібератак з

використанням логічних процедур, які базуються на покриттях матриць ознак. Безпека інформації, 22(3), 242-254.

9. Корченко, А., Щербина, В., & Вишневская, Н. (2016). Методология построения систем выявления аномалий, порожденных кибератаками. Захист інформації, (18, № 1), 30-38.

10. Терейковский, И., & Корченко, А. (2017). Система выявления кибератак. Безпека інформації, (23, № 3), 176-180.

11. Мусихина, Д. А., Яньков, П. А., & Елизарова, А. А. (2017). Выявление комплексных кибератак на критически важных объектах. Успехи современной науки, 4(2), 60-64.

12. Lakhno, V. (2016). Creation of the adaptive cyber threat detection system on the basis of fuzzy feature clustering. Eastern-European journal of enterprise technologies, 2(9), 18-25.

13. Петренко, С. А., Ломако, А. Г., Амельченкова, О. Н., & Зотова, А. В. (2012). Вычисления с памятью критически важных информационных систем в условиях кибератак. Защита информации. Инсайд, (6), 58-69.

14. Корченко, А. А., & Жумангалиева, Н. К. (2018). Структурная модель системы выявления вторжений. In Новые информационные технологии и системы (pp. 171-173).

15. Shenfield, A., Day, D., & Ayesh, A. (2018). Intelligent intrusion detection systems using artificial neural networks. ICT Express, 4(2), 95-99.

16. Papamartzivanos, D., Mármol, F. G., & Kambourakis, G. (2019). Introducing deep learning self-adaptive misuse network intrusion detection systems. IEEE Access, 7, 13546-13560.

17. Zhumangaliyeva, N., Korchenko, A., Doszhanova, A., Shaikhanova, A., Gulmira, S., Smagulov, S., & Erzhan, S. (2019). Detection Environment Formation Method for Anomaly Detection Systems. Journal of Theoretical and Applied Information Technology, 97(16), 4239-4250.

18. Rubio, J. E., Alcaraz, C., Roman, R., & Lopez, J. (2017, July). Analysis of Intrusion Detection Systems in Industrial Ecosystems. In SECRYPT (pp. 116-128).

19. Borowik, B., Petrov, O., Karpiski, M., Korchenko, O., & Lakhno, V. (2018). Immune and Defensive Corporate Systems. 222 p.

20. Корченко, А. А., & Жумангалиева, Н. К. (2018). Структурная модель системы выявления вторжений. In Новые информационные технологии и системы (pp. 171-173).

21. Berik, A., Valeriy, L., Yuliia, B., & Andrii, M. (2017). Разработка системы поддержки решений в слабо формализуемых задачах обеспечения кибербезопасности. Восточно-Европейский журнал передовых технологий, 1(2 (85)).

22. Массель, А. Г., & Гаськова, Д. А. (2018). Методы и подходы к обеспечению кибербезопасности объектов цифровой энергетики. Энергетическая политика, (5), 62-72.

«AL01» ШИФРЛЕУ АЛГОРИТМІНІҢ ҚАСИЕТТЕРІН ЗЕРТТЕУ

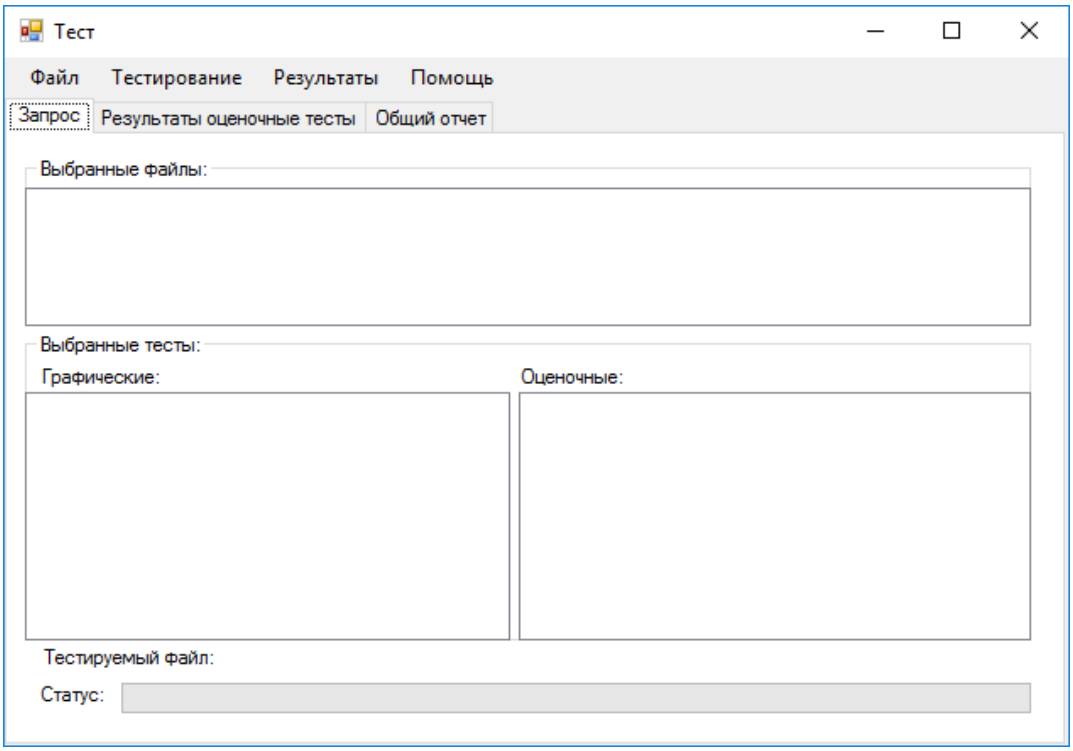
Самрат С.М., Әлиасқар М.С.
e-mail: sanzhar.samrat@gmail.com, 87019931011@mail.ru
ҚР БҒМ ҒК «Ақпараттық және есептеуіш технологиялар институты», Қазақстан

Аңдатпа. *Бұл мақалада статистикалық тесттер жинағын қолдана отырып «AL01» шифрлеу алгоритмінің статистикалық қасиеттеріне зерттеу, талдау жасалды және сапасы бағаланды.*

Бүгінгі таңда жүргізіліп жатқан зерттеу жұмыстарының негізгі мақсаты «AL01» шифрлеу алгоритмінің статистикалық қауіпсіздігін бағалау. «AL01» шифрлеу алгоритмі төрт раундтан тұрады. Бұл алгоритмде шифрлау блогының ұзындығы негізгі кілт ұзындығына тең және 128 битті құрайды [1,2].

Ұсынылатын криптоалгоритмге қойылатын талаптардың бірі, псевдокездейсоқ тізбек генераторы ретінде пайдалану жарамдылығы болып табылады. Ол үшін шифрмәтіндерді (алынған тізбектерді) статистикалық тесттерден өткізіп, нәтижелерін талдау керек. Тест үшін 20 түрлі файлды 5 түрлі кілттер тобымен шифрлеп, 100 шифрмәтін алынды.

Алынған 100 тізбектің статистикалық қауіпсіздігін зерттеу үшін «Д.Кнуттың статистикалық тесттерді және графикалық тесттерді таңдаудың автоматтандырылған жүйесі» (Автоматизированная система подборки статистических тестов Д.Кнута и графических тестов) бағдарламасы қолданылады.



1-сурет. «Д.Кнуттың статистикалық тесттерді және графикалық тесстерді таңдаудың автоматтандырылған жүйесі» бағдарламасының басты терезесі

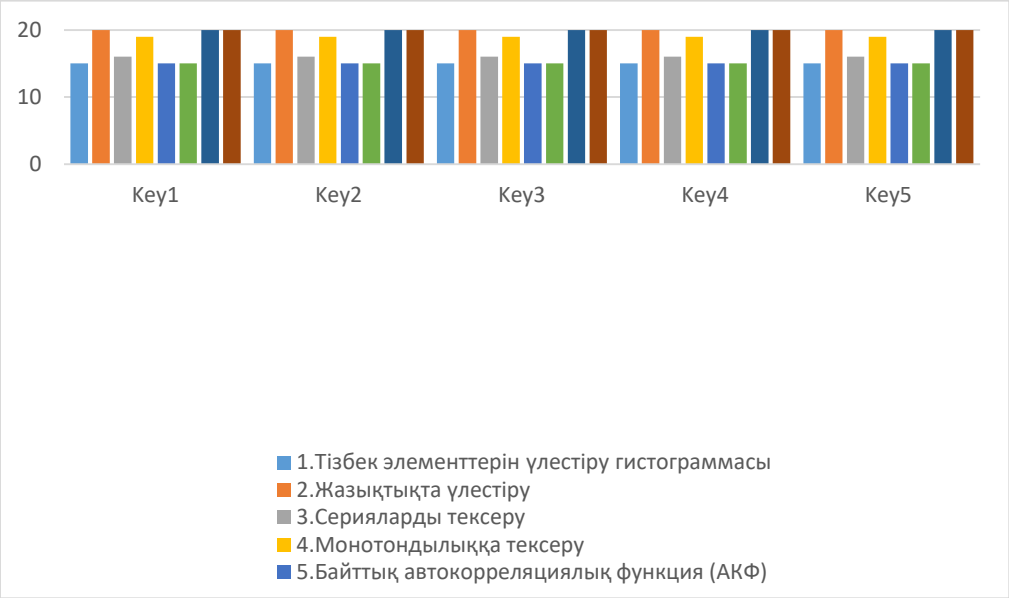
Псевдокездейсоқ тізбекті зерттеу үшін, екі тест тобы қолданылады [3-5].

- **Графикалық тесттер.** Тізбектің статистикалық қасиеттері графикалық тәуелділік түрінде көрсетіледі. Графикке қарап зерттелетін тізбек қасиеттеріне қорытынды жасалады. Графикалық тесттер: тізбек элементтерін үлестіру гистограммасы; жазықтықта үлестіру; серияларды тексеру; монотондылыққа тексеру; автокорреляциялық функция (АКФ), графикалық спектрлі тест, сызықтық күрделілік профилі.
- **Бағалау тесттері.** Тізбектің статистикалық қасиеттері сандық сипаттамалармен анықталады. Бағалау тесттері беретін сандық сипаттама арқылы тесттен өткенін немесе өтпегенін нақты айтуға болады. Бағалау тесттері: 0 мен 1-ге тексеру, байланыссыз серияларды тексеру, символ бойынша тексеру, интервалдарды тексеру, комбинацияларды тексеру, купондарды жинаушының тесті (тест собирателя купонов), орын ауыстыруларды тексеру, корреляцияны тексеру.

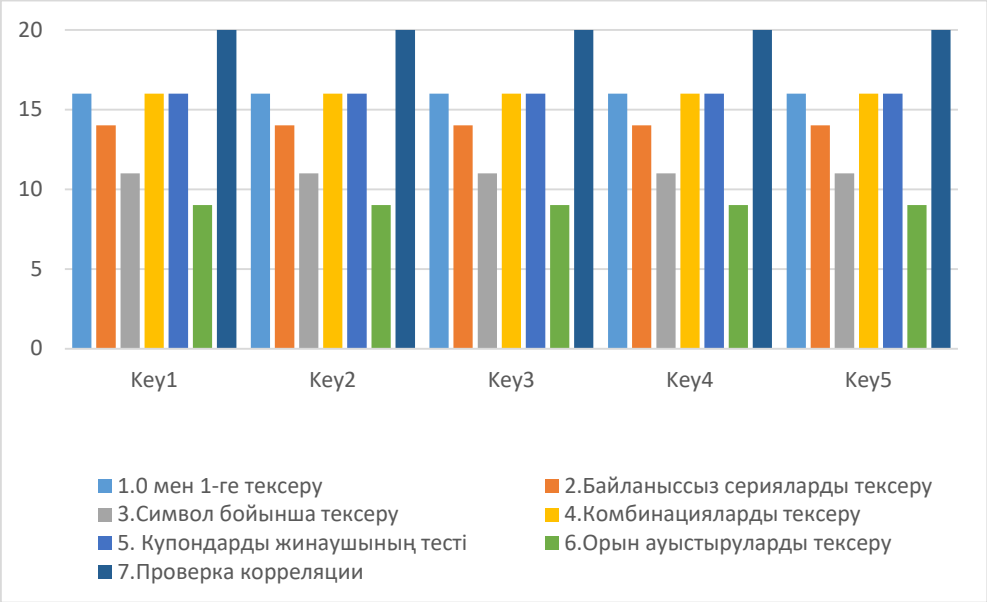
1-кесте. Шифрмәтіндерді зерттеу нәтижелері

Тест түрі	Тесттер	Key1	Key2	Key3	Key4	Key5
Графикалық тесттер	1.Тізбек элементтерін үлестіру гистограммасы	15	15	15	15	15
	2.Жазықтықта үлестіру	20	20	20	20	20
	3.Серияларды тексеру	16	16	16	16	16
	4.Монотондылыққа тексеру	19	19	19	19	19
	5.Байттық автокорреляциялық функция (АКФ)	15	15	15	15	15
	6.Биттік автокорреляциялық функция (АКФ)	15	15	15	15	15
	7.Графикалық спектрлі тест	20	20	20	20	20
	8.Сызықтық күрделілік профилі	20	20	20	20	20
Бағалау тесттері	1.0 мен 1-ге тексеру	16	16	16	16	16
	2.Байланыссыз серияларды тексеру	14	14	14	14	14
	3.Символ бойынша тексеру	11	11	11	11	11
	5.Комбинацияларды тексеру	16	16	16	16	16
	6. Купондарды жинаушының тесті	16	16	16	16	16
	7.Орын ауыстыруларды тексеру	9	9	9	9	9
	8.Проверка корреляции	20	20	20	20	20

1-кестеде әр тесттен сәтті өткен тізбектер саны көрсетілген. 2 және 3-суретте Графикалық және бағалау тесттер нәтижелері көрсетілген.



2-сурет. Графикалық тесттер нәтижелері



3-сурет. Бағалау тесттер нәтижелері

Графикалық және бағалау статистикалық тесттерінен алынған тізбектің статистикалық сипаттамаларын талдау нәтижелері алынды.

Графикалық тесттер нәтижелері 2-сурете көрсетілген. Жалпы тест нәтижелері – жақсы. Бірақ, нәтижелер шифрленетін файл түріне байланысты болады. .xls және .txt форматтағы файлдар тізбек элементтерін үлестіру гистограммасы, байттық автокорреляциялық функция, биттік автокорреляциялық функция тесттерінде нашар нәтиже көрсетті.

Бағалау тесттер нәтижелері 3-сурете көрсетілген. Тізбектердің көбісі символ бойынша тексеру, орын ауыстыруларды тексеру тесттерінен өтпеді. Бұл тесттерде дәлірек нәтиже алу үшін тізбек ұзындығын көбейтіп, қосымша тестілеу жасау керек.

Әдебиеттер

1. Дюсенбаев Д., Сақан Қ. «AL01» шифрлау алгоритміне криптографиялық талдау // Материалы IV международной научно-практической конференции «Информатика и прикладная математика» (Часть II). – Алматы, 2019. – с. 561-569.

2. Бияшев Р.Г., Алгазы К.Т., Дюсенбаев Д.С., Ержанов Е.Б. Результаты проверки «лавинного эффекта» алгоритма «AL01» // Материалы IV международной научно-практической конференции «Информатика и прикладная математика» (Часть II). – Алматы, 2019. – с. 602-607.

3. Нысанбаева С.Е., Капалова Н.А., Дюсенбаев Д.С., Алгазы К.Т. Исследования статистических свойств разработанного генератора псевдослучайных последовательностей // Материалы научной конференции Института информационных и вычислительных технологий МОН РК «Современные проблемы информатики и вычислительных технологий». – Алматы, 2018. – С. 210-217.

4. Капалова Н.А., Алгазы К.Т., Самрат С.М. Криптоалгоритмдердің статистикалық қауіпсіздігін зерттеу // Материалы научной конференции Института информационных и вычислительных технологий МОН РК «Современные проблемы информатики и вычислительных технологий (29-30 июня 2017 г.)». – Алматы, 2017. – С. 108-113.

5. Иванов М.А., Чугунков И.В. Теория, применение и оценка качества генераторов псевдослучайных последовательностей. – М.: «КУДИЦ-ОБРАЗ», 2003. – 240 с.

Содержание

Секция 1. Современные проблемы прикладной математики, информатики и теории управления. Моделирование и оптимизация сложных систем и бизнес процессов. Вычислительная математика, численный анализ и программирование, математическая логика. Теория статистики. Статистические методы		6
Мазаков Т.Ж., Айпанов Ш.А, Kisala P., Зиятбекова Г.З., Әлиасқар М.С.	ГИДРОТЕХНИКАЛЫҚ ҚҰРЫЛЫСТАРДАҒЫ СУ ДЕҢГЕЙІН КЛИМАТТЫҚ МӘЛІМЕТТЕР АРҚЫЛЫ БАҚЫЛАУДЫ АВТОМАТТАНДЫРУ ЖӘНЕ ОНЫҢ МАҢЫЗДЫЛЫҒЫ	7
Амирханов Б.С., Мазаков Т.Ж., Мазакова А.Т., Исимов Н.Т., Жолмагамбетова Б.Р., Әбдіразақ Б.К.	ДИСТАНЦИОННЫЙ МЕТОД МОНИТОРИНГА ЖИЗНЕННЫХ ПОКАЗАТЕЛЕЙ ЧЕЛОВЕКА	13
Амиргалиев Е.Н, Кунелбаев М.М, Орманов Т.А.	МОДЕЛИРОВАНИЕ ТЕРМОСИФОННОЙ СИСТЕМЫ СОЛНЕЧНОГО КОЛЛЕКТОРА	22
Есмагамбетова М.М., Сонькин М.А., Клюева Е.Г., Касымова Д.Т., Яворский В.В.	РАЗРАБОТКА ПРОЦЕДУР ПРИНЯТИЯ РЕШЕНИЙ ПО ПРЕДУПРЕЖДЕНИЮ АВАРИЙНЫХ СИТУАЦИЙ С УЧЕТОМ ВЗАИМОСВЯЗИ ФАКТОРОВ РАЗВИТИЯ ПРОБЛЕМЫ	28
A. Kalizhanova, S. Amirgalieva, A. Kozbakova, G. Kashaganova, Zh. Aitkulov,	RESEARCH OF NEW STRUCTURES OF THE TILT FIBER BRAGG GRATINGS AND THEIR PROPERTIES	38
Калимолдаев М.Н., Клюева Е.Г., Яворский В.В., Есмагамбетова М.М.	ПРИЛОЖЕНИЕ ДЛЯ МОНИТОРИНГА ДАННЫХ СЛОЖНЫХ СИСТЕМ, ПРЕДСТАВЛЕННЫХ МАТРИЦАМИ БОЛЬШОЙ РАЗМЕРНОСТИ	47
Ахметкалиевва А.С., Мамырбаев О.Ж., Алимхан К	УАҚЫТЫ КЕШІККЕН ЖОҒАРЫ РЕТТІ АНЫҚТАЛМАҒАН СЫЗЫҚТЫ ЕМЕС ЖҮЙЕЛЕР ҮШІН БЕЛГІЛЕНГЕН ӨТПЕЛІ ӨНІМДІЛІГІ БАР КЕҢ АУҚЫМДЫ ПРАКТИКАЛЫҚ ІЗГЕ ТҮСІРУ МӘСЕЛЕСІ	54
Есмагамбетова М.М., Бобров А.К., Утепбергенов И.Т., Клюева Е.Г., Ахмедиярова А.Т	АЛГОРИТМ ФОРМИРОВАНИЯ ПРОГРАММ ПРЕДУПРЕЖДЕНИЯ ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЙ	59

А.У. Калижанова, И.М. Кемельбекова	АНАЛИЗ СУЩЕСТВУЮЩИХ МЕТОДОВ И МОДЕЛЕЙ ПРОГНОЗИРОВАНИЯ И ИХ СРАВНЕНИЕ	66
Казыхан Р., Ташев А.	МОДЕЛИРОВАНИЕ В СКАЛЯРНОЙ ФУНКЦИИ С ПОМОЩЬЮ ТРЕХМЕРНОГО СИМПЛЕКС ЭЛЕМЕНТА	71
Akhmet M., Tleubergenova M., Nugayeva Z.	POINCARE CHAOS IN IMPULSIVE SYSTEMS	75
Амиргалиев Е.Н, Сундетов Т.Р, Кунелбаев М.М.	РАЗРАБОТКА СИСТЕМЫ ПИТАНИЯ, АЛГОРИТМА УПРАВЛЕНИЯ И АРХИТЕКТУРЫ ВЕРБАЛЬНОГО РОБОТА	81
Мусабаев Р.Р., Козбагаров О.Б.	НАЧАЛЬНОЕ ПРИБЛИЖЕНИЕ ПРИ ПОИСКЕ ОПТИМАЛЬНОГО РЕШЕНИЯ В ТЕМАТИЧЕСКОМ МОДЕЛИРОВАНИИ КАК ЗАДАЧЕ МАТРИЧНОГО РАЗЛОЖЕНИЯ	89
Ширяева О.И.	СИНТЕЗ СИСТЕМЫ УПРАВЛЕНИЯ НЕФТЕГАЗОВОЙ ОТРАСЛИ НА ОСНОВЕ ИСКУССТВЕННЫХ ИММУННЫХ СИСТЕМ И АЛГОРИТМА НЕГАТИВНОЙ СЕЛЕКЦИИ	100
Самигулина Г.А., Масимканова Ж.А.	РАЗРАБОТКА БАЗЫ ЗНАНИЙ ДЛЯ МУЛЬТИАГЕНТНОЙ СИСТЕМЫ НА ОСНОВЕ КООПЕРАТИВНОГО АЛГОРИТМА РОЯ ЧАСТИЦ С ВЕСОМ ИНЕРЦИИ	106

Секция 2. Информационно-телекоммуникационные технологии. Системы и сети передачи данных. Интернет-технологии. Облачные технологии. Параллельные вычисления. Распределённые вычисления. Суперкомпьютерные и кластерные системы. Обработка больших объёмов данных (Big-data). Геоинформационные системы и технологии. Инновационные образовательные технологии 113

Г. А. Амирханова, А.Ю. Горчаков	ВЕРИФИКАЦИЯ ОДНОЙ МОДЕЛИ ПЛОСКОЙ КРИСТАЛЛИЧЕСКОЙ РЕШЕТКИ	114
Anarbay Kudaykulov, Azat Tashev, Mukaddas Arshidinova., Begaliyeva Kalamkas	INVESTIGATION OF THE THERMOMECHANICAL STATE OF A ROD OF VARIABLE CROSS-SECTION UNDER THE INFLUENCE OF DISSIMILAR HEAT SOURCES.	119
Мамырбаев О.Ж., Оралбекова Д.О.	ОНЛАЙНОВЫЕ МОДЕЛИ НА ОСНОВЕ ВНИМАНИЯ ДЛЯ ИНТЕГРАЛЬНЫХ (END-TO-END) СИСТЕМ РАСПОЗНАВАНИЯ РЕЧИ	135
Demesinova S., Alipbayev K.	USE OF SPHTS AS A MEANS OF PROTECTION IN AIRCRAFT.	141

Ибраимкулов А.Е., Еримбетова А.С., Кубеков Б.С.	ВСПОМОГАТЕЛЬНЫЕ ТЕХНОЛОГИИ ДЛЯ УЧАЩИХСЯ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ	143
Терехов А.Г.	СПУТНИКОВЫЙ МОНИТОРИНГ ГИДРОТЕХНИЧЕСКИХ ОБЪЕКТОВ КИТАЙСКОЙ ЧАСТИ БАССЕЙНА РЕКИ ИЛИ В СЕЗОНЕ 2020 ГОДА	149
Вуйцик В., Кисала П., Калижанова А.У., Козбакова А.Х., Айткулов Ж.С., Оразбеков Ж., Искакова М., Арсланова С.	ЭКСПЕРИМЕНТАЛЬНО-МОДЕЛЬНЫЕ ИССЛЕДОВАНИЯ ПЕРИОДИЧЕСКИХ СТРУКТУР ДЛЯ СИСТЕМЫ ИНТЕРРОГАЦИИ	153
Ж.Б. Садирмекова, М.А. Самбетбаева.	РАЗРАБОТКА ТЕХНОЛОГИИ ИНТЕЛЛЕКТУАЛЬНЫХ НАУЧНО-ОБРАЗОВАТЕЛЬНЫХ ИНТЕРНЕТ-РЕСУРСОВ	165
Ермолдина Г.Т., Трушляков В.И., Утегенова А.У., Алипбаев К.А., Суйменбаева Ж.Б., Бапышев А.М., Аден А.Е., Гусейнов С.Р.	ОБЕСПЕЧЕНИЕ ЭКОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ ПРИ ЭКСПЛУАТАЦИИ РАЙОНОВ ЗАПУСКА И ПАДЕНИЙ ПЕРСПЕКТИВНЫХ РАКЕТ-НОСИТЕЛЕЙ СВЕРХЛЕГКОГО КЛАССА	171
Бобров Л.К. Медянкина И.П., Михайленко Н.А., Семканова В.А., Утепбегенов И.Т.	РОЛЬ ВНЕШНИХ БАЗ ДАННЫХ ПРИ ПОДБОРЕ КОНТРАГЕНТОВ	179
Тойбаева Ш.Д., Буранбаева А.И., Исабекова Л.С.	МЕТОДИКА УПРАВЛЕНИЯ ИННОВАЦИОННЫМ ПРОЦЕССОМ МЕНЕДЖМЕНТА КАЧЕСТВА ПРЕДПРИЯТИЯ	187
Атанов С.К., Искаков К.Т., Жораханов Н.Ә.	МАГНИТНАЯ ВОСПРИИМЧИВОСТЬ КАК ИНДИКАТОР ЗАГРЯЗНЕНИЯ СТРОИТЕЛЬНЫХ МАТЕРИАЛОВ	194
Бостанбеков К.А., Алимова А.Н., Джамалов Д.К., Юничева Н.Р.	РАЗРАБОТКА ПРОГРАММНОГО МОДУЛЯ «AUTOMATED SYSTEM FOR VERIFICATION AND CHANGE OF PARAMETERS OF THE WRF MODEL – ASVC WRF 1.0» ДЛЯ РЕГИОНАЛЬНОЙ КЛИМАТИЧЕСКОЙ МОДЕЛИ WRF	200

А.С.Бердышев, Д. Н. Блиева, А.Асхатулы	КОМПЬЮТЕРНОЕ МОДЕЛИРОВАНИЕ ЧИСЛЕННО-АНАЛИТИЧЕСКОГО РЕШЕНИЯ ДИНАМИЧЕСКОЙ ЗАДАЧИ ПОРОУПРУГОСТИ.	203
Байшемиров Ж.Д., Баймурзаев Д.Д. , Нуртас М., Адил Н., Жанбырбаев А.Б.	МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ДЛЯ ПОТОКА В ТРЕХМАСШТАБНО Й СРЕДЕ С ТОНКИМИ ТРЕЩИНАМИ	211
Iurii Krak	SOME APPROACH TO ECG SIGNALS PROCESSING, ANALYZING AND CLASSIFICATION	215
Amodu Oluwatosin, Mohamed Othman, Orken Mamyrbayev, Nor Kamariah Noordin, Idawaty Ahmad	TRANSMISSION CAPACITY ANALYSIS OF DENSE RELAY-ASSISTED D2D CELLULAR NETWORKS	216
Çağatay Yıldız , Müslüm Arıcı	STEADY FREE CONVECTION OF PARAFFIN WAX IN RECTANGULAR CAVITIES	216
А.С. Родионов, И.А. Мусихин, П.А. Карпик	ИНТЕЛЛЕКТУАЛЬНАЯ СИСТЕМА УПРАВЛЕНИЯ ДОРОЖНЫМ ДВИЖЕНИЕМ В МЕГАПОЛИСЕ	217
Загорулько Ю.А.	ПОДХОД К ПОСТРОЕНИЮ ОНТОЛОГИЙ НАУЧНЫХ ПРЕДМЕТНЫХ ОБЛАСТЕЙ НА ОСНОВЕ СИСТЕМЫ ПАТТЕРНОВ ОНТОЛОГИЧЕСКОГО ПРОЕКТИРОВАНИЯ	222
Хайрова Н. Ф., Мамырбаев О. Ж., Колесник А. С., Мухсина К. Ж.	ИСПОЛЬЗОВАНИЕ МЕТОДОВ КАЧЕСТВЕННОГО КОНТЕНТ-АНАЛИЗА ДЛЯ ИССЛЕДОВАНИЯ РАСПРЕДЕЛЕНИЯ ПРОТИВОПРАВНЫХ ТЕКСТОВ НА НОВОСТНЫХ САЙТАХ	223
Erol Kurt	TECHNIQUES FOR THE EXPLORATION OF PIEZOELECTRIC HARVESTERS	231
G. Taubayev, A.L. Bychkov, F.A. Murzin, N.E. Russkikh, E.I.Ryabchikova, S.S. Khairulin, G.B. Abdikerimova	CLASSIFICATION OF TEXURES ON THE BASE OF MACHINE LEARNING ALGORITHMS	232

Секция 3.Технологии искусственного интеллекта. Интеллектуальные системы управления. Речевые технологии и компьютерная лингвистика. Распознавание образов и обработка изображений. Биоинформатика и биометрические системы. Человеко-машинное взаимодействие. Машинное обучение. Интеллектуальные робототехнические системы 249

Рахымбекулы Ж., Пак А.А., Тукешев К.С., Джаксылыкова А.Б.	ОБЗОР МЕТОДОВ ГЛУБОКОГО ОБУЧЕНИЯ ДЛЯ ВЫЯВЛЕНИЯ КОРРЕЛЯЦИЙ МЕЖДУ СОСУДИСТОЙ СТРУКТУРОЙ СЕЧАТКИ И ДРУГИМИ СЕРДЕЧНО-СОСУДИСТЫМИ ЗАБОЛЕВАНИЯМИ.	250
Рахимова Д.Р., Турганбаева А.О., Сатыбалдиев А.	ИССЛЕДОВАНИЕ ПОДХОДОВ ПО ИЗВЛЕЧЕНИЮ КЛЮЧЕВЫХ СЛОВ ИЗ ТЕКСТА	252
Уалиева И.М., Мусабаев Р.Р.	ИССЛЕДОВАНИЕ ПРИМЕНЕНИЯ BERT МОДЕЛИ ДЛЯ ЭКСТРАКТИВНОЙ СУММАРИЗАЦИИ ОФИЦИАЛЬНЫХ ПРАВОВЫХ ДОКУМЕНТОВ	259
Якунин К., Мухамедиев Р.И., Кучин Я., Мусабаев Р., Булдыбаев Т., Мурзахметов С., Сымагулов А.	КЛАССИФИКАЦИЯ НЕГАТИВНЫХ ПУБЛИКАЦИЙ В СМИ С ИСПОЛЬЗОВАНИЕМ ТЕМАТИЧЕСКОГО МОДЕЛИРОВАНИЯ	262
Шаяхметова А.С., Литвиненко Н.Г., Литвиненко Г.Г.	ПРАКТИЧЕСКИЕ РАССУЖДЕНИЯ В БАЙЕСОВСКИХ СЕТЯХ	269
Мамырбаев Ө.Ж., Қамзабек А.Н., Абдуллахан С.А.	ҚАЗАҚ ТІЛІ СӨЙЛЕУІН ТАНУДАҒЫ ӨЗЕКТІ МӘСЕЛЕЛЕРДІ ТАЛДАУ	275
Мамырбаев Ө.Ж., Қамзабек А.Н, Абдуллахан С.А.	MEL КӨМЕГІМЕН СӨЙЛЕУДІ ТАНУ ЖҮЙЕСІН ҚҰРУ КЕПСТРАЛДЫҚ ЖИІЛІК КОЭФФИЦИЕНТІ ӘДІСІ	280
Mamyrbayev Orken, Nawida Najmee,	HANDWRITING RECOGNITION DEVELOPMENT SYSTEM SOFTWARE	287
Мухтар Д. А.	ПРИМЕНЕНИЕ СКРЫТЫХ МАРКОВСКИХ МОДЕЛЕЙ В РАСПОЗНАВАНИИ РЕЧИ	291
Amirgaliyev Ye., Sadykova A.	CONSIDERATION OF THE STATE OF SPEECH RECOGNITION TECHNOLOGY	296
Rakhimova D., Turarbek A., Zhunussova A.	TASKS OF POST-EDITING MACHINE TRANSLATION FOR TURKIC LANGUAGES	302
А.С. Еримбетова, Ф.А. Мурзин, Ф. Озодов, А. Жанабеков	LINK GRAMMAR PARSER И ФОРМАЛЬНЫЙ АНАЛИЗ ПЕРЕФРАЗИРОВАННЫХ ПРЕДЛОЖЕНИЙ НА ЕСТЕСТВЕННОМ ЯЗЫКЕ	310

Елеусинов А.И., Бурибаев Ж.А.	СЕГМЕНТАЦИЯ РУКОПИСНЫХ СИМВОЛОВ С ИСПРАВЛЕНИЕМ НАКЛОНА ТЕКСТА	319
А.В.Ким, Г.М.Аязбаев	ИНТЕЛЛЕКТУАЛЬНЫЕ РОБОТОТЕХНИЧЕСКИЕ СИСТЕМЫ С МУЛЬТИЯЗЫЧНЫМ РАСПОЗНАВАНИЕМ ГОЛОСОВОЙ РЕЧИ И ВЕРБАЛЬНЫМ КОМАНДНЫМ УПРАВЛЕНИЕМ	325
Утепбергенов И.Т., Ахмедиярова А.Т., Касымова Д.Т.	ВНЕДРЕНИЕ ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМ НА ТРАНСПОРТЕ	332
Мамырбаев Ө.Ж., Кыдырбекова А.С., Осман М., Жумажанов Б.Ж.	БИОМЕТРИЯЛЫҚ ТЕХНОЛОГИЯЛАРДЫ ҚОЛДАНАТЫН ДАУЫСТЫ ТАНУ ҚАУІПСІЗДІК ЖҮЙЕСІН ҚҰРУ	340
Кубеков Б.С., Утегенова А.У., Науменко В.В., Ибраимкулов А.К.	ПОДГОТОВКА СПЕЦИАЛИСТОВ И АДАПТАЦИЯ IT-ОБРАЗОВАНИЯ В УСЛОВИЯХ ЦИФРОВОЙ ЭКОНОМИКИ	348

Секция 4. Информационная безопасность и защита данных. Программно-технические средства защиты информации. Математические методы обеспечения информационной безопасности сложных систем 356

Д.С. Дюсенбаев	AL01 АЛГОРИТМІНЕ ИНТЕГРАЛДЫҚ КРИПТОГРАФИЯЛЫҚ ТАЛДАУ	357
Усатова О.А., Нысанбаева С.Е., Вуйцик В.	АЛГОРИТМ АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЯ НА ОСНОВЕ ВТОРОГО ФАКТОРА В ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ СИСТЕМАХ	363
Ордабаева Г.К.	ЖЕЛІЛІК ТОПОЛОГИЯНЫҢ ҚАУІПСІЗДІК МОДЕЛІ МЕН ӘДІСТЕРІН ӘЗІРЛЕУ	367
Сақан Қ.С., Алғазы К.Т.	КРИПТОГРАФИЯЛЫҚ ХЕШ АЛГОРИТМДЕР ЖАСАУДЫҢ ӘРТҮРЛІ ЖОЛДАРЫН ҚАРАСТЫРУ	374
К. Алгазы, К. Сакан	ПРИНЦИПЫ ПОСТРОЕНИЯ БЛОЧНЫХ ШИФРОВ И ТРЕБОВАНИЯ К НИМ	378
Айтхожаева Е.Ж., Жоламан Б.Р.	РЕГЛАМЕНТАЦИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ФИНАНСОВОМ СЕКТОРЕ РК	383
Капалова Н.А., Сулейменов О.Т.	КРИПТОГРАФИЯЛЫҚ ХАТТАМАЛАРДЫҢ ЛОГИКАЛЫҚ ДҰРЫСТЫҒЫН BAN ЛОГИКАСЫ НЕГІЗІНДЕ ТАЛДАУ	389
Нысанбаева С.Е., Капалова Н.А., Варенников А.В.	СХЕМА ЭЛЬ-ГАМАЛЯ НА ОСНОВЕ НЕПОЗИЦИОННЫХ ПОЛИНОМИАЛЬНЫХ СИСТЕМ СЧИСЛЕНИЯ	394

Бегимбаева Е.Е., Бияшев Р.Г.	О РАЗРАБОТКЕ МОДЕЛИ СИСТЕМЫ КАЗАХСТАНСКОГО СЕГМЕНТА ЗАЩИЩЕННОГО ТРАНСГРАНИЧНОГО ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ	398
Ахметов С.С., Калижанова А.У., Lakhno V., Набиева Г.С.	МОДИФИЦИРОВАННЫЙ МЕТОД ДИНАМИЧЕСКОГО ПРОГРАММИРОВАНИЯ ДЛЯ ОПРЕДЕЛЕНИЯ АКТИВНОГО СОСТАВА СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ	401
Капалова Н., Хаумен А., Ержанов А.	КЛЮЧЕВОЕ РАСПИСАНИЕ АЛГОРИТМА ШИФРОВАНИЯ ДАННЫХ «ВС-2»	408
Калимолдаев М.Н., Бияшев Р.Г., Нысанбаева С.Е., Капалова Н.А.	ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И КИБЕРБЕЗОПАСНОСТЬ В КАЗАХСТАНЕ	414
Ахметов Б.С., Лахно В.А., Ыдырышбаева М.Б.	КОМПЬЮТЕРЛІК ЖҮЙЕЛЕРДЕГІ (КЖ) КИБЕРШАБУЫЛДАРДЫ АНЫҚТАУДЫҢ ЗАМАНАУИ ЖҮЙЕЛЕРІН ТАЛДАУ	418
Самрат С.М., Әлиасқар М.С.	«AL01» ШИФРЛЕУ АЛГОРИТМІНІҢ ҚАСИЕТТЕРІН ЗЕРТТЕУ	424
Содержание		428

МАТЕРИАЛЫ
V международной научно-практической конференции
"Информатика и прикладная математика",

29 сентября - 1 октября 2020, Алматы, Казахстан

Под редакцией М.Н. Калимолдаева

Компьютерная верстка
Шокишалов Ж.М.

Подписано в печать 25.09.2020 г. Формат А4
Печать цифровая. Бумага офсетная. Усл. печ. л. 70,8.
Тираж 300 экз. Заказ № 006686.
Отпечатано в ИИВТ МОН РК.
Алматы, ул. Пушкина, 125