

Институт информационных и вычислительных технологий
МОН РК



МАТЕРИАЛЫ

научной конференции

ИИВТ МОН РК

**«Современные проблемы информатики и
вычислительных технологий»**

29-30 июня 2017 года

Алматы 2017

УДК 004(063)
ББК 32.973
С56

Главный редактор:

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

Ответственные редакторы:

Юничева Н.Р. - ученый секретарь ИИВТ МОН РК, кандидат технических наук, доцент

Мамырбаев О.Ж. - заместитель генерального директора ИИВТ, доктор PhD

Магзом М.М. - заместитель генерального директора ИИВТ

С56 Современные проблемы информатики и вычислительных технологий:
Мат. науч. конф. (29-30 июня 2017 г). – Алматы, 2017, – 303 с.

ISBN 978-601-280-948-0

В сборнике представлены материалы конференции ИИВТ МОН РК «Современные проблемы информатики и вычислительных технологий».

В сборнике опубликованы научные материалы сотрудников института, докторантов PhD и магистрантов, а также научных работников, принимающих участие в проектах по грантовому и программно-целевому финансированию.

Рассмотрены актуальные вопросы в области информационных и вычислительных технологий, информационной безопасности, проблем распознавания образов, классификации и теории принятия решений, оптимизации и оптимального управления динамическими системами, разработки моделей методов и информационной технологии построения интеллектуальных экспертных систем прогнозирования и управления сложными объектами, математического моделирования и управления динамическими, техническими и экономическими системами, теории моделей и спецификаций информационных систем, робототехнических систем, проблем синтеза и распознавания казахской речи.

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

УДК 004(063)

ББК 32.973

ISBN 978-601-280-948-0

© Институт информационных и
вычислительных технологий
МОН РК, 2017

Программный комитет

Председатель:

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

Сопредседатели:

Мамырбаев О.Ж., доктор PhD, зам. ген. директора ИИВТ МОН РК
Магзом М.М., зам. ген. директора ИИВТ МОН РК

Ученый секретарь:

Юничева Н.Р., к.т.н., доцент, ученый секретарь ИИВТ МОН РК

Члены Программного комитета:

Амиргалиев Е.Н., д.т.н., профессор
Арсланов М.З., д.ф.-м.н., профессор
Ашимов А.А., академик НАН РК, д.т.н.
Бияшев Р.Г., д.т.н., профессор
Калижанова А.У., к.ф.-м.н., доцент
Карабеков Б.С., к.ф.-м.н., доцент
Кудайкулов А.К., д.ф.-м.н., профессор
Мазаков Т.Ж., д.ф.-м.н., профессор
Мусабаев Р.Р., к.т.н.
Мустафин С.А., к.т.н., доцент
Найзабаева Л.К., д.т.н., профессор
Нуртазин А.Т., к.т.н., доцент
Нысанбаева С.Е., д.т.н., профессор
Пак И.Т., академик РАЕН, д.т.н., профессор
Самигулина Г.А., д.т.н., профессор
Тлеубергенов М.И., д.ф.-м.н., профессор
Утепбергенов И.Т., д.т.н., профессор

Организационный комитет

Председатель:

Сахариев Б.Б., член-корр. МАИН, зав. лабораторией ИИВТ МОН РК

Члены Организационного комитета:

Абдилдаева А.А., доктор PhD
Анищенко Л.Н.
Ахметжанов М.А., доктор PhD
Калиева Г.С.
Капалова Н.А., к.т.н.
Кулемзин А.А.
Мажитов Ш.С.
Шахмаев Р.А.

СЛЕПАЯ ЭЛЕКТРОННАЯ ПОДПИСЬ НА ОСНОВЕ КРИПТОСИСТЕМЫ RSA-M

Абдикаликов К.А.
e-mail: abdikalikov@mail.ru

Актюбинский университет им.С.Баишева, Казахстан

Аннотация. В данной работе рассматривается слепая подпись на основе модификации криптосистемы RSA-M, соответствующая принципам построения схем ЭЦП- алгоритмов и протоколов.

В настоящее время электронный документооборот повсеместно используется во всех малых и больших фирмах, организациях. Ни один юридически значимый документ, представленный в электронном виде, не может существовать без такого атрибута как электронная подпись (ЭП). Существует множество модификаций ЭП, каждая из которых отвечает требованиям и задачам конкретной практической цели.

Слепая электронная подпись является (СЭП) одной из наиболее интересных и значимых модификаций. Ее основной областью применения является банковская сфера, а также сфера электронного голосования. Как известно, автоматизация процесса оплаты ведется уже давно. В то же время, при использовании средств электронных платежных систем, банк всегда имеет полную информацию о том, кто, где, когда и кому перевел денежные средства. Этот факт оказывает большое влияние на неприкосновенность личной жизни пользователей. Использование СЭП позволяет создавать такие платежные системы, которые способны обеспечить анонимность платежей, но в то же время, дать пользователям возможность при необходимости доказать факт совершения платежа, например, в случае судебных разбирательств.

Схема СЭП является безопасной, если она обладает следующими свойствами:

Неуязвимость случайных параметров - невозможность извлечения параметров маскирования из замаскированных величин.

Не подделываемость - невозможность выработки верной электронной подписи никем кроме банка.

Слепота - свойство, гарантирующее, что переменные, которые подписывающий орган получает во время протокола выработки подписи и полученная подпись являются статистически независимыми.

Анонимность - невозможность установить личность или другие данные о пользователе, который предоставлял сообщение на подпись.

Известно, что разновидность электронной цифровой подписи (ЭЦП), особенностью которой является то, что подписывающая сторона не может точно знать содержимое подписываемого документа, названная слепой подписью, была придумана Дэвидом Чаумом [1].

Суть идеи подписи “вслепую” заключается в том, что сторона A посылает документ стороне B , который B подписывает и возвращает A . Используя полученную подпись, сторона A может вычислить подпись стороны B на более важном для себя сообщении. По завершении этого протокола сторона B ничего не знает ни о сообщении, ни о подписи под этим сообщением.

Опишем реализацию данных операций с использованием технологии СЭП.

Протокол снятие наличности клиентом (A) со своего счета в банке (B) с использованием СЭП:

1. Клиент A генерирует последовательность и умножает на сгенерированного множителя M , т.е. маскирует ее;
2. Клиент A зашифровывает полученное сообщение открытым ключом и отправляет банку B ;
3. Банк B расшифровывает полученное сообщение личным секретным ключом;
4. Банк B подписывает сообщение СЭП, соответствующей номиналу монеты;
5. Банк B зашифровывает подписанное сообщение и отправляет клиенту A ;
6. Клиент A расшифровывает полученное сообщение, снимает маскирующий множитель M .

Протокол внесение наличности клиентом (A) на свой счет в банке (B) с использованием СЭП:

1. Клиент A отправляет монету, полученную от банка B , обратно в банк B , зашифровав открытым ключом;
2. Банк B расшифровывает полученное сообщение и убеждается, что данная монета не была использована;
3. Банк B заносит номер монеты в базу монет и зачисляет соответствующую сумму на счет клиента A .
4. В данном протоколе СЭП не позволяет банку B собрать информацию о клиентах. Банк B может только вести учет погашенных монет, тем самым контролируя единовременное использование каждой монеты.

Таким образом, подпись “вслепую” применяется в тех областях, где необходима анонимность и невозможность повторного использования документа.

Первая реализация слепых подписей была осуществлена Д. Чаумом с помощью криптосистемы RSA [1]:

- а) A маскирует m путем умножения на степень случайно сгенерированного числа r (закрывающего множителя):

$$m' = r^e m \bmod n.$$

- б) B подписывает m' , накладывая свою подпись:

$$s' = (m')^d = (r^e m)^d \bmod n.$$

- в) A “удаляет” закрывающий множитель, вычислив подпись для исходного m .

$$s = s' r^{-1} \bmod n.$$

Следовательно, имеющаяся в распоряжении A пара (m, s) представляет собой документ, подписанный стороной B . При этом B может проверить свою подпись, когда документ возвращается ему.

Существуют разновидности реализации СЭП:

- система Брандса, основанная на использовании двойного протокола Шнорра;
- система Фергюсона, основанная на использовании алгоритма RSA и протокола Шнорра.

В протоколе Шнорра применяется дискретное логарифмирование, благодаря чему операция выполняется быстрее, и передается меньшее количество данных. При этом,

вместо дискретного логарифмирования могут использоваться алгоритмы на основе эллиптических кривых.

Так как при реализации криптографических систем защиты информации, основанных на методах типа алгоритма RSA, основная вычислительная нагрузка приходится на выполнение арифметических операций над многоразрядными числами, то вопрос модификации алгоритмов ЭЦП с целью повышения их быстродействия остается актуальным, включая эффективную программную реализацию криптоалгоритмов.

В данной работе рассматривается вариант алгоритма на основе модификации криптосистемы RSA-M [2], соответствующий принципам построения схем ЭЦП – алгоритмов и протоколов, позволяющих построить информационное взаимодействие между участниками таким образом, чтобы факт авторства переданного сообщения, “подписанного” одним из участников, мог быть надежно подтвержден или опровергнут.

Согласно схеме криптосистемы RSA-M, для формирования ЭЦП отправитель выполняет над контрольной суммой документа те же операции, что и при шифровании, но использует не открытый ключ пользователя, а свой личный закрытый ключ, т.е. $S = m^D \bmod N$.

На приемной стороне получатель возводит S в степень E , где E – открытый ключ отправителя, и получает $S^E \bmod N = m'$.

Компьютерную технологию рассматриваемого алгоритма можно описать следующим образом:

I шаг. Открытый ключ E , секретный ключ D , сообщение M , криптограмма C и цифровая подпись принадлежат множеству $Z_N = \{0, 1, 2, \dots, N-1\}$, образующему с операциями сложения и умножения по модулю N арифметику по модулю N , где $N = p \cdot q$, а p и q – случайно выбранные простые числа, которых выбирают равными по длине и хранят в секрете.

Для нахождения произведения $p \cdot q$ можно использовать модифицированный алгоритм быстрого преобразования Фурье [3]

II шаг. Открытый ключ E выбирается случайным образом так, чтобы выполнялись условия:

$$1 \leq E \leq \varphi(N), \text{НОД}(E, \varphi(N)) = 1,$$

где $\varphi(N)$ – функция Эйлера. Вычисляет значение функции Эйлера для полученного значения модуля N , функция Эйлера для двух простых чисел, в частности для выбранных значений p и q определяется как: $\varphi(N) = (p-1) \cdot (q-1)$. Функция Эйлера указывает, сколько во множестве чисел от 1 до N есть чисел взаимно простых с N , т.е. $\text{НОД}(E, \varphi(N)) = 1$. Это определение необходимо для случайного выбора значения открытого ключа E из подмножества, определяемого численным значением функции Эйлера.

III шаг. Вычисляется секретный ключ D , такой, что

$$D < N, E \cdot D \equiv 1 \pmod{\varphi(N)}.$$

При этом используется алгоритм Евклида.

IV шаг. Сообщение M сжимается с помощью хэш-функции на основе теоретико-числовых преобразований Ферма (ТЧПФ) [4]:

$$h(M) = m.$$

V шаг. Вычисляется цифровая подпись S под электронным документом M , используя хэш-значение m и секретный ключ D :

$$S = m^D \pmod{N}.$$

Для быстрого вычисления S используется алгоритм Монтгомери [5] и бинарный метод [6].

VI шаг. Пара (M, S) передается получателю как электронный документ, подписанный цифровой подписью S . После приема пары (M, S) получатель вычисляет хэш-значение сообщения M двумя разными способами – криптографическим преобразованием подписи S и хэшированием принятого сообщения с помощью той же хэш-функции на основе ТЧПФ.

VII шаг. Сравниваются полученные хэш-значения

$$m' = S^D \pmod{N} \text{ и } m = h(M) \text{ сообщения.}$$

Если они совпадают, то получатель признает пару (M, S) подлинной.

При этом заметим, что по данной методике можно получить оценки подлинности, целостности и стойкости алгоритма, обеспечивающие его высокую эффективность и перспективные применения в различных информационных системах.

Литература

1. Шнайер Б. Прикладная криптография. 2-е издание. -М. “Триумф”, 2002;
2. Абдикаликов К.А. Алгоритмы решения задач обработки информации и информационной безопасности компьютерной технологии. –Актобе: ПринтА, 2014. - 456с.
3. Задирака В.К., Абдикаликов К.А. Быстрые ортогональные преобразования: теория и приложения. – Алматы: “Гылым”, 2003, 220с.;
4. Абдикаликова Н.И. Алгоритм хэш-функции, основанной на теоретико-числовом преобразовании Ферма. – Известия МОН, НАН РК, сер.физ.-мат., 2202, №3, с.74-78;
5. Montgomery P.L. Modular Multiplication Without Trial Division // Math..Comp. - 1985. -V.44, -№ 170. -P.519-521.
6. Кнут Д.Е. Искусство программирования для ЭВМ. Т.2. –М.: Мир, 1977. -724 с.

АЭРОФОТОСЪЕМКА ОТКРЫТЫХ ГОРНОРУДНЫХ МЕСТОРОЖДЕНИЙ С ИСПОЛЬЗОВАНИЕМ БПЛА

Айнакулов Ж.Ж.
e-mail: jaras1987@mail.ru

Казахский национальный университет имени аль-Фараби, Казахстан, г. Алматы

Аннотация. Для оценки и прогнозирования производительности открытых горнорудных месторождений очень важно получать оперативную достоверную информацию с периодичностью хотя бы в один квартал. Самым объективным источником информации является аэрофотосъемка. Однако применение больших самолетов и вертолетов для этих целей очень дорогостоящее мероприятие, поскольку размеры разработок в среднем не превышают 10 квадратных километров и не всегда аэродром расположен вблизи месторождений. Поэтому весьма целесообразным является использование малогабаритных беспилотных летательных аппаратов (БПЛА). В данной работе приведены результаты аэрофотосъемки с БПЛА открытого горнорудного месторождения и их фотограмметрической обработки.

В мировой практике с появлением гражданских беспилотников началось их использование в целях мониторинга промышленных объектов в частности в области разработок полезных ископаемых [1,2].

Казахстан обладает огромными природными богатствами и ведет активную их разработку. Например, ОАО «Корпорация Казахмыс» имеет лицензии на освоение 23 месторождений медных, полиметаллических руд, строительных материалов, угля. Разработка месторождений ведется как открытым, так и подземным способом [3].

Многие компании занимаются освоением угольных месторождений. К наиболее крупным относятся: Майкубенский буроголовый бассейн и Екибастузский в Павлодарской области, Карагандинский каменноугольный бассейн, Шубаркольское чекинское и Борлыньское месторождения в Карагандинской области, Юбилейное месторождение в Восточно-Казахстанской области [4].

Аэрофотосъемка открытого горнорудного месторождения с БПЛА производилась с целью отработки методик съемки карьеров с беспилотных аппаратов мультиторного и самолетного типа и последующей фотограмметрической обработки полученных данных для получения трехмерной модели и ортофотоплана высокого разрешения – сотые доли метра на пиксель для систематического мониторинга производимых работ и вычисления вырабатываемых объемов породы. В качестве объекта исследований было выбрано открытое горнорудное месторождение в Центральном Казахстане.

Это месторождение начало разрабатываться в 1985 году. Оно вытянуто с юга на север и в настоящее время имеет размеры порядка 2х3х0.25 км. Ориентировочно ежегодно добывается около 30 млн. тонн руды. Проектная мощность месторождения, определенная институтом «Карагандагипрошахт», составляет 20 млн. тонн руды в год. 1 тонна добытой руды соответствует 1,33 куб. метров [5].

Преимуществом съемки с БПЛА является оперативный мониторинг состояния месторождения и его бортов, 3D визуализация всего месторождения и отдельных его частей, дает объективность получаемой информации.

Аэросъемка осуществлялась в двух уровнях – самолетом (Геоскан 101) и гексакоптером (собственной сборки), фотографии приведены на рисунке 1.



Рисунок 1 - Самолет и гексакоптер

Аэрофотосъемка и с самолета и с гексакоптера выполнялась цифровым фотоаппаратом Sony Nex 5N разрешением 14 Мп. Фокусное расстояние в обоих случаях выставлялось равным 28 мм. В самолете фотоаппарат занимал фиксированное положение, а в гексакоптере устанавливался на двух осевую гиростабилизированную платформу, что обеспечивало фиксированное положение фотокамеры.

Съемка с самолета производилась с высоты 150 метров над уровнем поверхности земли у края месторождения. Было осуществлено 3 полета с запада на восток от края до края месторождения. Каждый полет содержал около 20 линий. Общее количество линий составляло 60, общее количество снимков – 2435. Кадры, выполненные во время разворотов, исключались из фотограмметрической обработки. Поскольку перекрытие кадров по линии полета составляло около 80% при теоретической необходимости 60%, кадры со смазанными изображениями также исключались из обработки (таблица 1).

Таблица 1 - Статистика полетов

	Самолет	Гексакоптер
Количество вылетов	3	8
Количество фотографий	2435	824
Рабочие фотографии	1898	807
Высота от точки старта (м)	150	100
Точка старта	Поверхность земли	Внутри месторождения

Запуск гексакоптера производился внутри месторождения с глубины примерно 200 метров от верхнего края поверхности земли. С места старта мультиротор поднимался на высоту 100 метров. Полеты производились с востока на запад. Было выполнено 8 полетов примерно по 4 линии в каждом. Количество полетов в обоих случаях определялось ресурсом LiPo аккумуляторов емкостью 10 А/ч. Схема полетов представлена на рисунке 2.

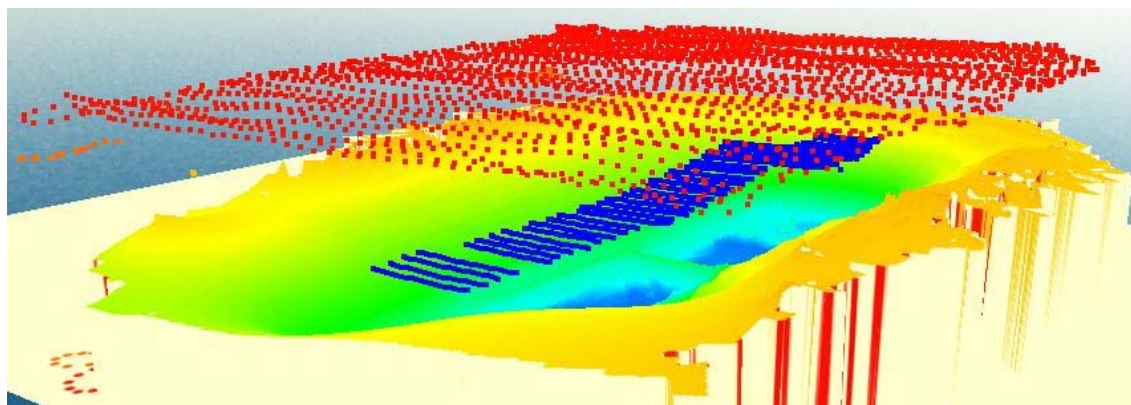


Рисунок 2 - Маршруты полетов самолета (красные точки) и гексакоптера (синие точки) над открытым горнорудным месторождением

Следует отметить, что точки старта мультиротора имели разные высоты и это обстоятельство стало небольшим затруднением при фотограмметрической обработке полученных снимков с которым мы успешно справились путем установки связующих точек на снимках, выполненных с разных высот в ручном режиме.

Расстановка опорных знаков. До выполнения аэросъемки для привязки снимков к местности равномерно по всему разрезу были расставлены и замерены координаты опорных точек, положение которых показано на рисунке 3.

В качестве опорных знаков использовались нарезанные из клеенчатого материала полосы шириной 25 см и длиной 200 см, которые перегибались по центру под углом 90 градусов.

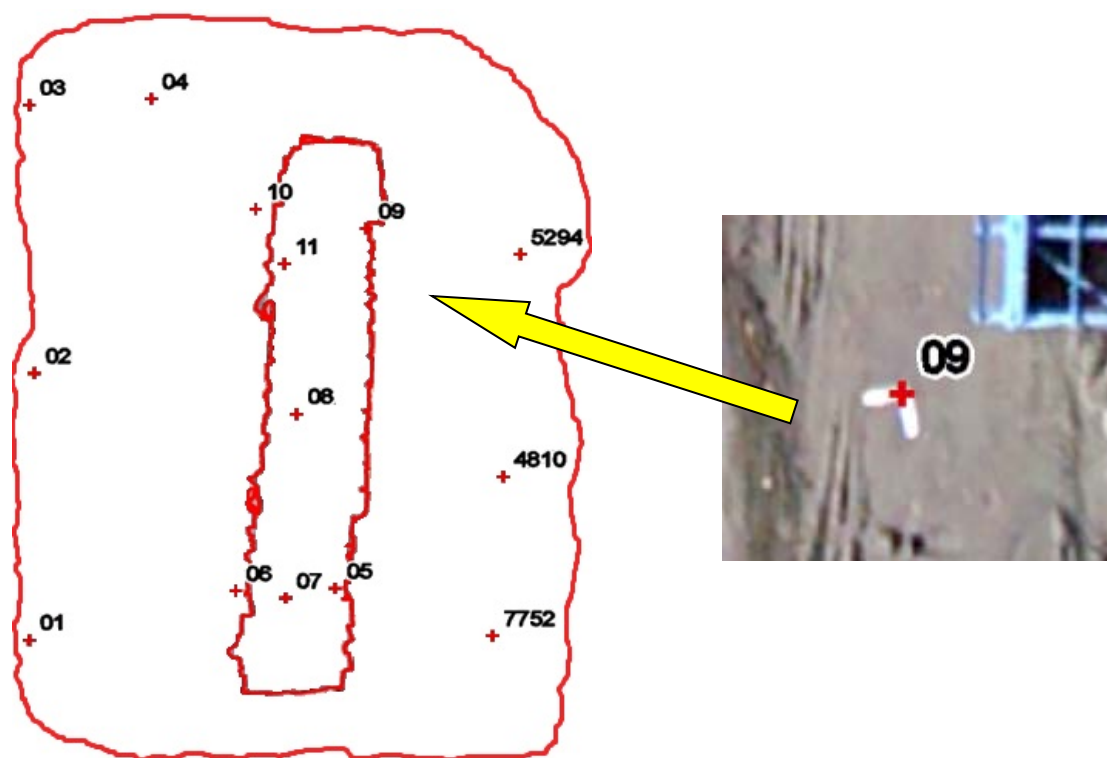


Рисунок 3 - Схема расстановки опорных точек

Ошибки по опорным точкам после уравнивания приведены в таблице 2.

Таблица 2 - Ошибки по опорным точкам после уравнивания

Имя точки	Ошибка (см)			
	X	Y	Z	Общая
03	1.42623	0.0190399	-0.629046	1.55891
02	-1.05392	1.79315	2.1179	2.96844
05	-2.19141	7.21445	-1.85466	7.76469
07	-7.40204	-3.55447	-0.388473	8.22055
08	-0.256165	0.873776	-2.55333	2.71083
09	-1.69852	-7.32364	-.0581117	7.54045
04	-6.31944	5.04837	3.02228	8.63456
06	5.36666	0.387021	-0.220922	5.38513
10	3.87104	-5.01862	0.855148	6.39553
11	0.148656	-4.05701	-2.21976	4.62696
4810	4.0133	1.82096	2.67144	5.15355
5294	3.88597	2.28367	1.58826	4.77896
7752	0.49976	0.776777	0.629407	1.11772
Суммарная	3.73021	3.90971	1.75906	5.68284

По нормативным данным средняя погрешность планового положения пунктов съемочной сети относительно ближайших пунктов опорной сети не должна превышать 0,4 мм на плане в принятом масштабе съемки и 0,2 м по высоте. (Для масштаба 1:500 0.4 мм на плане соответствует 20 см на местности) [6,7].

Фотограмметрическая обработка аэрофотоснимков проводилась в программном комплексе Agisoft PhotoScan. Поскольку объем исходных данных достаточно большой, вычисления выполнялись в режиме распределенной обработки на пяти компьютерах, самый слабый из которых работал в качестве сервера.

Было найдено 993518 связующих точек и построено плотное облако, содержащее 761872566 точек. Таким образом разрешение на местности составило 12.5 см/пикс, а плотность точек равнялась 64/м². На основе этих данных построена цифровая модель местности, показанная на рисунке 4. На этом же рисунке показаны профили поперечных сечений для двух положений – на перешейке и между перешейками.

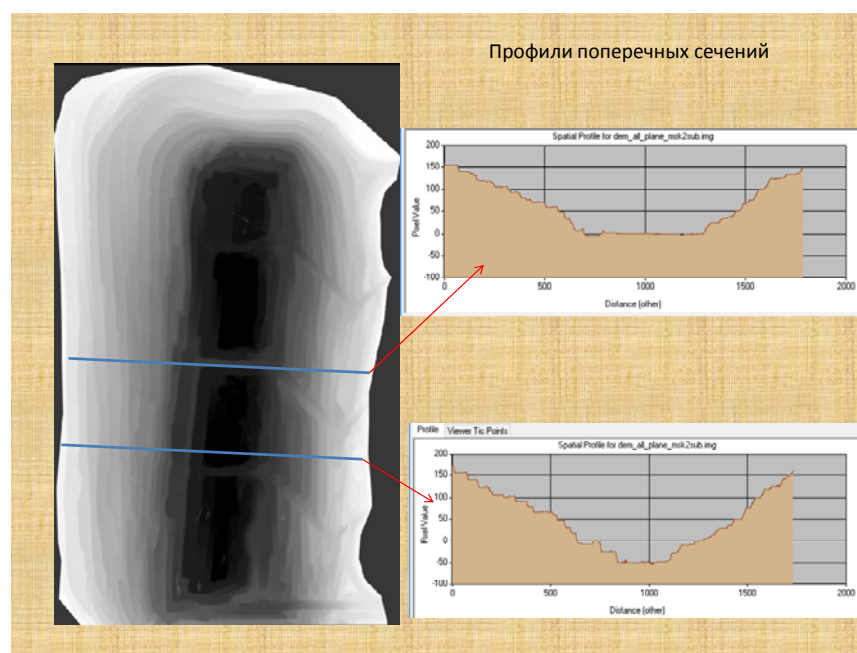


Рисунок 4 – Цифровая модель местности

Используя данные цифровой модели местности были выполнены оценки объемов вынутого из месторождения грунта в зависимости от выбора высоты расположения плоскости отсчета. Результаты оценок показана в таблице 3.

Таблица 3 – Объем вынутого грунта в зависимости от выбора начальной высоты

Площадь и объем \ Высота	150 метров	160 метров
Объем куб.м	636 926 829,20673	700 078 238,86711
Площадь поверхности 3D кв.м	8 665 442,4094792	9 261 983,9845889
Площадь основания кв.м.	6 100 294,9348178	6 540 529,0667387
Объем грунта куб.м	20 546 026,74860419	22 583 168,99571323
Объем угля куб.м	15 448 140,41248436	16 979 826,31256634

Учитывая, что выработка месторождения началась в 1985 году (2016-1985=31 год) можно оценить среднюю ежегодную производительность, что составило порядка 21 млн. куб. метров/год.

Для пересчета всего объема грунта в объем руды был использован коэффициент 1.33, хотя для каждого месторождения этот коэффициент различен.

Полученная ЦММ позволила вычислить объемы внутренних производственных насыпей, что показано на рисунках 5, 6.

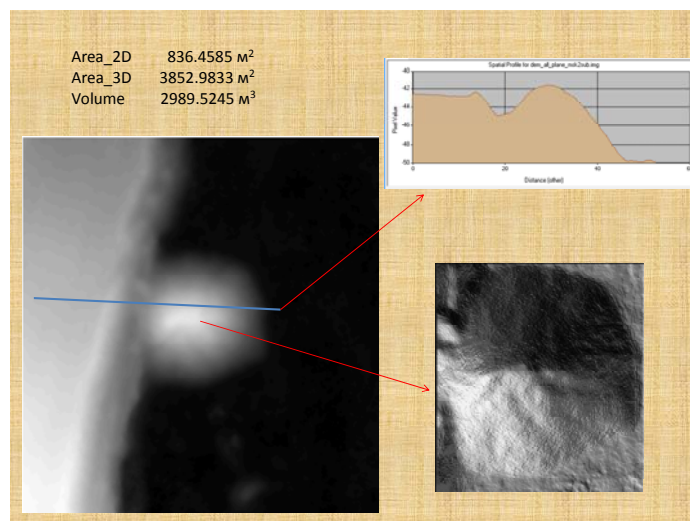


Рисунок 5 - Объем первой внутренней производственной насыпи

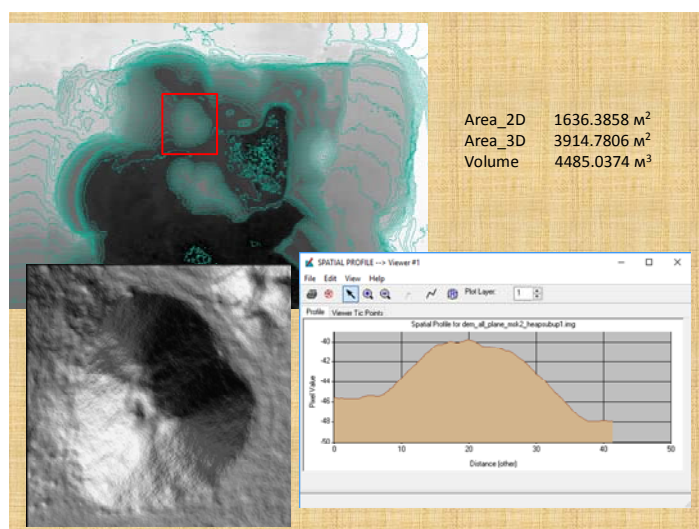


Рисунок 6 - Объем второй насыпи

В таблице 4 показаны затраты машинного времени на обработку данных с БПЛА.

Таблица 4 – Затраты на обработку данных с БПЛА

№	Операция	Компьютеры	Время
1	Загрузка фотоснимков	1	1 - 5 мин.
2	Поиск связующих точек	4	3 ч.
3	Построение плотного облака	4	37 ч. 18 мин.
4	Построение модели	1	1 ч. 37 мин.
5	Построение текстуры	1	6 ч. 55 мин.
6	Построение тайловой модели	4	8 ч. 52 мин.
7	Построение карты высот	4	14 мин
8	Создание ортофотоплана	1	55 мин
9	Построение горизонталей	1	30 мин.

Общее время съемки и обработки составило 128 часов (~ 20 рабочих дней).

В результате выполненных работ было показано, что аэросъемка открытых горнорудных разработок с использованием беспилотных летательных аппаратов является перспективным направлением для мониторинга производственных процессов.

Аэросъемку всего месторождения целесообразно производить с применением БПЛА самолетного типа, а для внутренних отвалов использовать БПЛА вертолетного типа.

Литература

1. Фирсов А.П., Злыгостев И.Н., Савлук А.В. и др. Применение беспилотных летательных аппаратов при геолого-геофизическом картировании / Материалы V Всероссийской научно-практической конференции «Геология и минерально-сырьевые ресурсы северо-востока России», 31 марта – 2 апреля, 2015. - С. 529-533.
2. <http://insideunmannedsystems.com/monitoring-mapping-measuring-drones-changing-mining-industry/> (Мониторинг, картографирование, измерение: как дроны меняют горнодобывающую промышленность. Дата обращения: 03.05.2017 год).
3. <http://www.kase.kz/news/show/97121> (Казахстанская фондовая биржа. СПРАВКА: ОАО "Корпорация Казахмыс" (Казахстан) - характеристика деятельности. Дата обращения: 03.05.2017 год).
4. <http://ibrain.kz/ekonomika-kazahstana/ugolnaya-promyshlennost> (Образовательный портал. Угольная промышленность. Дата обращения: 03.05.2017 год).
5. Физические величины: Справочник / Бабичев А.П., Бабушкина Н.А., Братковский А.М. и др.; Под ред. Григорьева И.С., Мелихова Е.З. - М.: Энергоатомиздат, 1991. – 1232 с. - ISBN 5-283-040135.
6. Маркшейдерская энциклопедия / Гл. ред. Пучков Л.А. - М.: Издательство Мир горной книги, 2006. - 605 с. ISBN 5-91003-003-5.

ЖОҒАРЫ РЕТТІ АНЫҚТАЛМАҒАН СЫЗЫҚТЫ ЕМЕС ЖҮЙЕЛЕРДІ ШЫҒЫС КОМПЕНСАТОРЫ ЖӘРДЕМІНДЕ КҮШТІ ПРАКТИКАЛЫҚ БАҚЫЛАУ

Алимхан К^{1.}, Калимолдаев М.Н.^{2.}, Тасболатұлы Н.^{3.}

e-mail: tasbolatuly@gmail.com

¹Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан

²Ақпараттық және есептеуіш технологиялар институты, Алматы, Қазақстан,

³Әл-Фараби атындағы Қазақ ұлттық университеті, Алматы, Қазақстан

Түйіндеме. Бұл жұмыста жоғары ретті анықталмаған сызықты емес жүйелерді шығыс контроллері (шығыс компенсаторы аталатын) жәрдемінде күшті практикалық бақылау мәселесі зерттелді. Қатаң емес шарт жағдайында жоғары ретті анықталмаған сызықты емес жүйелерге күшті бақылауды орындауға мүмкіндік беретін шығыс компенсаторын құру мүмкіндігі қарастырылды және бұл компенсатор

алдын белгілі контроллер-бақылаушы әдісіне сүйеніп құрылды. Жұмыстың соңында, нәтиженің тиімділігіне көз жеткізу үшін қарапайым сандық мысал келтірілді.

Түйін сөздер: басқару теориясы, сызықты емес басқару теориясы, кері байланыс, контроллер, кең ауқымды практикалық бақылау, Ляпуновтың тура әдісі, тірек сигналы, қателік сигналы, шығыс компенсаторы.

Кіріспе. Бұл жұмыста жоғары ретті анықталмаған сызықты емес жүйелерді кері байланыс шығысы жәрдеміне кең ауқымды практикалық бақылау проблемасы қарастырылады. Жоғары ретті анықталмаған сызықты емес жүйелердің жалпылама көрінісін келесі формула бойынша сипаттаймыз:

$$\begin{aligned}\dot{x}_i &= x_{i+1}^{p_i} + \phi_i(t, x, u), & i &= 1, \dots, n-1 \\ \dot{x}_n &= u + \phi_n(t, x, u) \\ y &= x_1 - y_r\end{aligned}\tag{1}$$

мұндағы, $x = (x_1, \dots, x_n)^T \in R^n$ – жүйе күйі, $u \in R$ – басқарудың кіріс сигналы, $y \in R$ – шығыс сигналы, $\phi_i(t, x, u)$, $i = 1, \dots, n$ үшін C^1 – белгісіз үздіксіз функциялар және $p_i \in R_{odd}^{\geq 1} := \left\{ \frac{p}{q} \in [0, \infty) : p \text{ және } q - \text{тақ бүтін сандар, мұнда } p \geq q \right\}$ ($i = 1, \dots, n-1$) –

жүйенің жоғары реттілігін көрсетеді, ал y_r – ізіне түсуге арналған тірек сигналы. Әдетте ізіне түсу мәселесінің қарапайым жағдайында $y_r(t)$, $t \in [0, \infty)$ тірек сигналы, сондай ақ оның туындылары белгілі, бірақ біздің қарастыратын мәселемізде x_1 шығыс мәліметі мен y_r тірек сигналы арасындағы $y = x_1 - y_r$ қателікті өлшеуге болады деп есептеледі. Сәйкесінше, тек y – ті компенсаторды жобалау кезінде қолдануға рұқсат етіледі. Алайда, біздің реттеуіміз қарапайым жағдайдан тұратындығы белгілі, өйткені y_r белгілі, x_1 – ді $x_1 = y - y_r$ арқылы алуға болады. Осыған қосымша ретінде, кейбір практикалық бақылау программаларында қателік сигналы $y = x_1 - y_r$ тек ақпарат деп саналып, міндетті түрде есептелуге жатады. Мысалы, ракетаны бағыттау жүйесінде борттық радар қозғалыстағы нысанның абсолютті позициясын, яғни y_r сигналын өлшеудің орнына ракета мен нысанның арасындағы арақашықтықты/қателікті өлшеуді жалғастыра береді [1]. Басқа жағдайда тек қателік сигналы датчик құрылымын қарапайым етеді, өйткені, контроллер жіті бақылануы тиіс сигналдан тәуелсіз деп тұжырымдалады. Осылайша, контроллер түрлі тірек сигналдарына көбірек бейімделген болып табылады [2].

Із кесуді практикалық басқару проблемасы сызықты емес басқару теориясының ең маңызды есептерінің бірі болып табылады және бұл мәселені шешу үшін соңғы онжылдықтарда қарқынды зерттеулер жүргізілуде. Кері байланыс күйі бойынша басқару мәселесіне қарағанда кері байланыс шығысы арқылы басқару теориясы баяу дамыған, өйткені, сызықты емес контроллерді жобалаудың ешқандай жалпыға ортақ және тиімді әдісі жоқ.

Сызықты емес дифференциалды теңдеулермен берілген динамикалық процесстер, объектілер басқару нысаны саналып, оларды тұрақтандыру есебіне құрылған әдістердің басым көпшілігі Ляпуновтың тура әдісіне негізделіп жасалып келеді. [3] еңбекте әр алуан топтағы сызықты емес объектілер үшін түрліше басқару жүйелерін жобалау есептері Ляпуновтың тура әдісі жәрдеміне шешіледі. Кері байланыс негізінде шығыс мәліметтерін реттеудің тиімді әдісі [4] еңбекте қарастырылып, оның нәтижесі шығыс мәліметтері бойынша күшті бақылау жүйесін құруда, сызықты емес жүйелерді кең ауқымды бақылау есептерінде қолданылуда. Салыстырмалы түрде соңғы жылдары шыққан еңбектердің бірінде [5] және монографияда [6] сызықты және сызықты емес

жүйелер үшін шығыс сигналын бақылау проблемасына қатысты басқару теориясындағы жетістіктер толық және жіті баяндалады. Сонымен қатар, осы мәселеге қатысты алғашқы еңбектердің көпшілігі тірек сигналын тұрақты немесе экзосистема арқылы алынады деп қарастырылды [7-10]. Ал тірек сигналы уақытқа байланысты өзгеріске ұшырайтын жалпылама жағдайды ең алғаш рет А. Исидори және С.И. Бирнс [6,11] қарастырды. Жоғарыда аталған еңбектердің көпшілігінде басқарылатын сызықты емес жүйелердегі Якобиан сызықтандыруы тұрақты және анықталады [6] деген талап қойылды, және осы екі қасиет сызықты емес реттегіш нәтижесін немесе күйін немесе қателікке ие кері байланыс мәселесін шешудің негізгі алғышарты болып табылды. Алайда, сызықты емес жүйедегі Якобиан сызықтануы тұрақтанбайтын және/немесе анықталмайтын жағдайында бұл мәселені шешу күрделі әрі қиын болады, және мұндай сызықты емес жүйелер үшін нәтижелі еңбектер өте аз [12,13].

Бұл зерттеумен тығыз байланысты келесі еңбектерді [14-16] қарастырайық. Бұл еңбектерде «шығыс мәліметтерін практикалық бақылау» жаңа концепциясы ұсынылды және үшбұрышты пішінді (triangular systems) жүйелер тобы үшін шығыс мәліметтерін практикалық бақылау проблемасын зерттеді және бұл бақылау мәселесін шешу үшін үздіксіз күйдегі локальды кері байланыс контроллерін алды. Үшбұрышты пішіндес жүйелер яғни, үшбұрышты (жоғарғы және төменгі) матрица коэффициенттерінен тұратын жүйелер. Әрі қарай, бір кіріс мәліметі мен бір шығыс мәліметінен тұратын келесі түрдегі сызықты емес жүйелердің арнайы тобы үшін кең ауқымды күшті практикалық бақылау проблемасы [15] зерттелді:

$$\begin{aligned} \dot{x}_i &= x_{i+1}^{p_i} + \phi_i(t, x, u), & i &= 1, \dots, n-1 \\ \dot{x}_n &= u^{p_n} + \phi_n(t, x, u), & y &= x_1 \end{aligned} \quad (2)$$

Жоғарыдағы еңбектегі тұжырым бойынша (2) жүйенің шығыс сигналдарын кең ауқымды күшті асимптотикалық бақылау тірек сигналының тұрақты жағдайында тегіс күйдегі кері байланыс арқылы шешімге ие. Алайда, осы мәселе тірек сигналы уақытқа байланысты өзгертін жағдайда кері байланыстың тегіс күйі арқылы шешу мүмкін емес. Сондықтан да, бұл жағдайды еңсеру үшін Цянь және Линь [17] шығыс мәліметтерін практикалық бақылау проблемасында (2) жүйеге қарағанда жалпылама жүйені ұсынып, қайсыбір сәйкес шарттар қою арқылы кең ауқымды күшті практикалық бақылау есебі кері байланыс күйі жәрдемінде шешімге ие болатындығын дәлелдеді.

Практикалық жағдайда мұндай контроллер құру үшін тек шығыс мәліметтерін қолданған дұрыс және (2) жүйені тұрақтандыру мәселесі шығыс мәліметтері бойынша кері байланыс жәрдемінде әлі шешімін таппаған, сәйкесінше із кесу мәселесі шешілмеген. Сондықтан да, Ян және Лин [18] (2) жүйеге қарағанда жұмсақтау жүйені ұсынды және мұндағы $p_i = p(i = 1, \dots, n-1)$ және $p_n = 1$ деп болжам жасады:

$$\begin{aligned} \dot{x}_i &= x_{i+1}^{p_i} + \phi_i(t, x, u), & i &= 1, \dots, n-1 \\ \dot{x}_n &= u + \phi_n(t, x, u), & y &= x_1 \end{aligned} \quad (3)$$

және «екі контроллер – бақылаушы және компенсатор» идеясын ұсынды. Ол бойынша (3) жүйені кең ауқымды күшті тұрақтандыру тегіс кері байланыс арқылы қол жеткізуге болатынын көрсетті.

Мәселенің қойылуы және алғышарттар. Жоғарыда келтірілген (1) түрдегі жүйені қарастырайық және $y_r(t)$ тірек сигналы $[0, \infty)$ аралығымен шектелген C^1 -функция болып табылады, $\dot{y}_r(t)$ туындысы да шектелген деп тұжырымдайық. Онда осы

жұмыста қарастырған шығыс сигналын шығыс компенсаторы арқылы күшті практикалық бақылау есебі келесі түрде анықталады: кез келген берілген $\varepsilon > 0$ үшін, компенсатор құрылымын келесі түрде аламыз

$$\begin{cases} \dot{\zeta} = \alpha(\zeta, y), \zeta \in R^m \\ u = \beta(\zeta, y) \end{cases} \quad (4)$$

мұнда, α, β – қайсыбір біртекті функциялар, m – қолайлы оң бүтін сан.

- (1), (4) тұйық жүйесінің әрбір күйі $[0, \infty)$ аралығында жақсы анықталған және ауқымды шектелген;

- практикалық ізкесуді орындау мүмкін, яғни, ε -ға және бастапқы жағдайы $x(0) \in R$ байланысты $T := T(\varepsilon, x(0)) > 0$ шекті уақыт бар және (1),(4) тұйық жүйесінің шығысы келесі шартты қанағаттандырады

$$|y(t)| = |x_1(t) - y_r(t)| < \varepsilon, \quad \forall t \geq T > 0 \quad (5)$$

Ары қарай, «интегратор дәреже көрсеткішін қосу» әдісін және «үйлескен контроллер-қадағалаушы компенсатор» идеясын қолданып, біз, (1) бойынша қолайлы болжамдардан шығысты практикалық бақылау мәселесі (4) түрдегі компенсатор жәрдемінде шешуге болатындығын көрсетеміз.

1 болжам. (1) түрдегі сызықты емес жүйе үшін $C_1 \geq 0, C_2 \geq 0$ нақты саны бар болады

$$|\phi_i(t, x, u)| \leq C_1(|x_1|^p + \dots + |x_i|^p) + C_2, \quad i = 1, \dots, n \quad (6)$$

2 болжам. y_r тірек сигналы C^1 –мен шектелген функция болып табылады, яғни $D > 0$ белгілі тұрақтысы келесіні қанағаттандырады

$$|y_r(t)| \leq D, \quad |\dot{y}_r(t)| \leq D, \quad \forall t \in [0, \infty) \quad (6)$$

Шығыс сигналын күшті практикалық бақылау мәселесі.

Теорема. (1) жүйедегі 1 және 2 болжам бойынша шығысты кең ауқымды күшті практикалық бақылау мәселесі (4) түрдегі компенсатормен шешімге ие және мұндай компенсаторды құру процедурасы берілген [12,13].

Теорема дәлелдеу контроллер-бақылаушы комбинацияланған жобалау әдісін негіз етіп алады және ол екі бөлімнен тұрады:

1. Бірінші бөлімде (1) түрден алынған $\phi_i(t, x, u) = 0, i = 1, \dots, n$ және $y_r = 0$ үшін номиналды форманы (p – нормал форманы) асимптотикалық тұрақтандыратын шығыс компенсаторын құру қарастырылады; (кері байланыс күйінің құрылымы) $x_1, x_2, \dots, x_n$ -айнымалылар күйі өлшенуге жатады және бір интегратор қуаттылығы әдісі қолданылады деп есептейміз [16,17];

2. Екінші бөлімде (1) үшін кері байланыс контроллері күйін құрамыз, ол 2-болжамды қанағаттандыратын кез келген тірек сигналы үшін шығыс сигналдарын кең ауқымды практикалық бақылауды қамтамасыз етеді.

Теореманың анықтылығын жоғарыда келтірілген екі әдіс негізінде дәлелдеуге болады, дәлелдеме Поленда және Цян [19] авторлардың еңбектері негізіне сүйенеді.

Компьютерде моделдеу. Келесі түрдегі сызықты емес жүйені қарастырайық,

$$\dot{x}_1 = x_2^3 + \frac{x_2^2}{3(1+x_2^2)},$$

$$\dot{x}_2 = x_3 + \frac{1}{4} \left(x_2^3 \sin x_1^2 + x_2^3 \right),$$

$$\dot{x}_3 = u + \frac{1}{7} x_3,$$

$$y = x_1 - y_r \quad (7)$$

мұнда, $p_1 = 3, p_2 = 1, p_3 = 1$ және $y_r(t) = (\sin(t))^3$. Басқарудың мақсаты $x_1(t)$ күйін тек $y(t)$ өлшемін пайдаланып, уақыт бойынша өзгеріп отыратын $y_r(t)$ тірек сигналының ізіне түсуін мәжбүрлеу болып табылады. Бұл ізіне түсу мәселесінде $y_r(t)$ белгілі болуы шарт емес. Мұндағы (7) сызықтандырылған жүйе $x = 0$ жағдайында тұрақтанбайды және анықталмайды. Ары қарай, анық емес функциялар келесі түрде бағаланады:

$$|\phi_1(t, x, u)| = \frac{1}{3} \left| \frac{x_2^2}{1+x_2^2} \right| \leq \frac{1}{3} |x_1|^3 + \frac{1}{3},$$

$$|\phi_2(t, x, u)| = \left| \frac{1}{4} (x_2^3 \sin x_1^2 + x_2^3) \right| \leq \frac{1}{4} \left(|x_2|^{\frac{1}{3}} x_1^2 + |x_2|^3 \right) \leq \frac{11}{20} (|x_1|^3 + |x_2|^3) + \frac{28}{45}$$

$$|\phi_3(t, x, u)| = \left| \frac{1}{7} x_3 \right| \leq \frac{1}{35} (|x_1|^5 + |x_2|^5 + |x_3|^5) + \frac{8}{35}$$

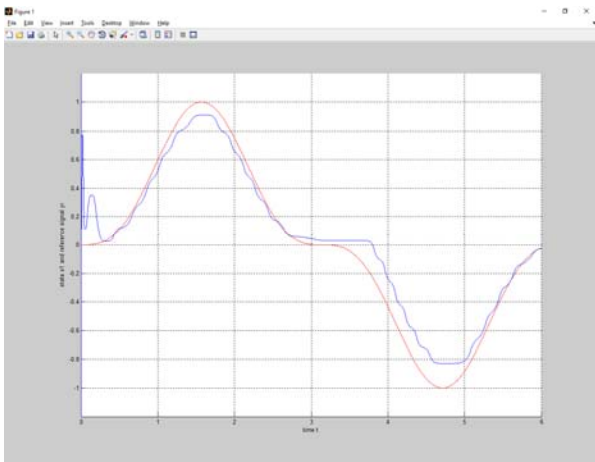
яғни, $C_1 = \frac{11}{20}$ және $C_2 = \frac{28}{45}$, *1-болжам* қанағаттанады. Ал, *2-болжам* тірек сигналын қанағаттандырады. Теореманың дәлелдемесінен шығыс компенсаторы құрылымын келесі формада аламыз:

$$\hat{\dot{x}}_2 = -ML_1(\hat{x}_2 + L_1(x_1 - y_r))^3$$

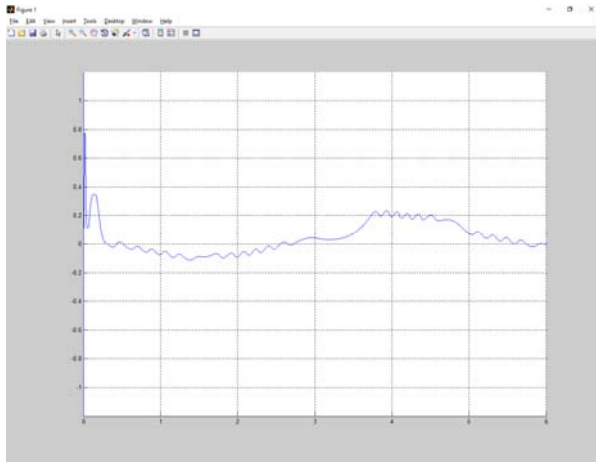
$$\hat{\dot{x}}_3 = -ML_2(\hat{x}_3 + L_2(\hat{x}_2 + L_1(x_1 - y_r)))^3$$

$$u = -M^{\frac{7}{3}} [\beta_3(\hat{x}_3 + L_2\hat{x}_2 + L_2L_1(x_1 - y_r))^5 + \beta_2(\hat{x}_2 + L_1(x_1 - y_r))^5 + \beta_1(x_1 - y_r)^5]$$

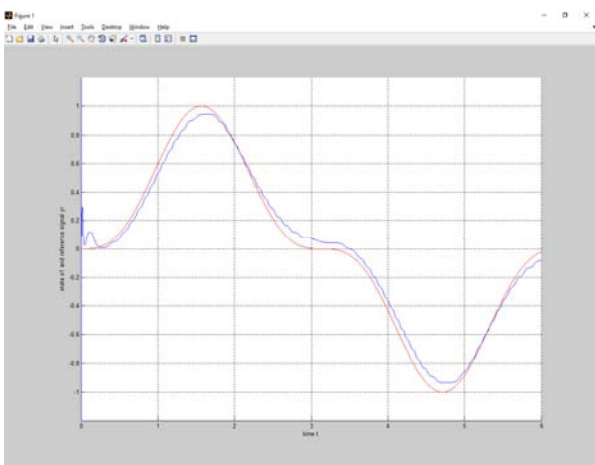
мұнда, $L_1 = 9, L_2 = 3$ және $\beta_1 = \frac{3}{20}, \beta_2 = \frac{5}{8}, \beta_3 = \frac{4}{5}$ мәндері компенсаторды құру барысында (7) номиналды формасынан алынды және компьютерде есептеу барысында $x_1(0) = -7, x_2(0) = 7, x_3(0) = 10, \hat{x}_2(0) = -10, \hat{x}_3(0) = 50$ үшін $M = 450$ мәнінде із кесу қателігі 0,2 шамасында (16-сурет), $M = 4500$ мәнінде із кесу қателігі 0,1 құрады (26-сурет).



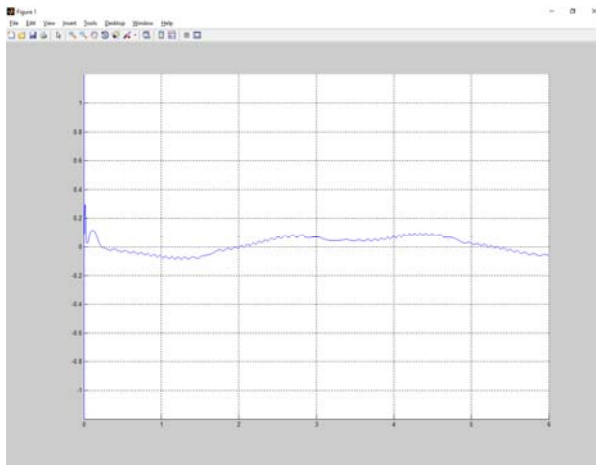
1а сурет. $M = 450$ мәніне сай $x_1(t)$ және $y_r(t) = (\sin(t))^3$ траекториясы



1б сурет. $M = 450$ мәніне сай $x_1(t)$ және $y_r(t) = (\sin(t))^3$ бойынша қателік



2а сурет. $M = 4500$ мәніне сай $x_1(t)$ және $y_r(t) = (\sin(t))^3$ траекториясы



2б сурет. $M = 4500$ мәніне сай $x_1(t)$ және $y_r(t) = (\sin(t))^3$ бойынша қателік

Қорытынды

Бұл жұмыста объект үшін тірек сигналының ізіне түсу мәселесі, сызықты емес дифференциалды теңдеулермен сипатталған динамикалық процесстер есебі қарастырылды. (1) түрдегі сызықты емес жүйелер үшін күшті практикалық ізкесуді орындау мақсатында шығыс компенсаторы құрылымы алынды. Негізгі тұжырым теоремада корсетіліп, дәлелденді. Жұмыстың соңында, нәтиженің тиімділігіне көз жеткізу үшін қарапайым сандық мысал келтіріліп, нәтижесі графикалық кескінде көрсетілді.

Қолданылған әдебиеттер тізімі

1. Q. Gong and C. Qian, C. Global practical output regulation of a class of nonlinear systems by output feedback // Proc. the 44th IEEE conference on decision and control, and the European control conference, Seville, Spain, 2005. P. 7278-7283.
2. J. Zhai and S. Fei, Global practical tracking control for a class of uncertain nonlinear systems // IET Control Theory and Applications, vol 5, Issue 11, 2011. P. 1343 – 1351.

3. H.K. Khalil, Nonlinear Systems, 3rd edition, Prentice Hall, Upper Saddle River, New Jersey, 2002.
4. C.I. Byrnes, A. Isidori, New results and examples in nonlinear feedback stabilization // Systems and control letters, 12, 1989. P. 437-442.
5. C. Byrnes, A. Isidori Output regulation for nonlinear systems: an overview // Int. J. Robust and Nonlinear Control, 10 (5), 2000. P. 323–337.
6. C.I. Byrnes, F.D. Psicoli, A. Isidori, Output Regulation of Uncertain Nonlinear Systems. Boston: Birkhäuser, 1997.
7. C. Desoer, C. Lin, Tracking and disturbance rejection of MIMO nonlinear systems with PI controller // IEEE Trans. Autom. Control, 30 (9), 1985. P. 861–867.
8. Di Benedetto, M. Synthesis of an internal model for nonlinear output regulation // Int. J. Control, 45 (3), 1987. P. 1023–1034.
9. J. Huang, W. Rugh, On a nonlinear multivariable servomechanism problem // Automatica, 1990, 26 (6), pp. 963–972.
10. J. Hepburn, W. Wonham, Error feedback and internal models on differentiable manifolds // IEEE Trans. Autom. Control, 1984, 29 (5), pp. 397–403.
11. A. Isidori, C.I. Byrnes Output regulation of nonlinear system // IEEE Transactions on Automatic Control, 35, 1990, 31-140.
12. K. Alimhan, H. Inaba, Practical output tracking by smooth output compensator for uncertain nonlinear systems with unstabilisable and undetectable linearization // International Journal of Modelling, Identification and Control, 5, 2008, 1-13.
13. K. Alimhan, H. Inaba, Robust practical output tracking by output compensator for a class of uncertain inherently nonlinear systems // International Journal of Modelling, Identification and Control, Vol.4 (2008), No.4, 304-314, 2008.
14. S. Čelikovský and J. Huang, Continuous feedback practical output regulation for a class of non-linear systems having non-stabilizable linearization // Proc.38th IEEE Conf. Decision and Control, Phoenix, AZ, pp.4796–4801.
15. W. Lin and C. Qian, Robust regulation of a chain of power integrators perturbed by a lower-triangular vector field // Int. J. Robust Non-linear Control, Vol. 10, 2000a, pp.397–421.
16. W. Lin and C. Qian, Adding one power integrator: a tool for global stabilization of high-order triangular systems // Syst. Contr. Lett., Vol. 39, 2000b, pp.339–351.
17. C. Qian, W. Lin, Practical output tracking of nonlinear systems with uncontrollable unstable linearization // IEEE Trans. Automat. Contr., Vol. 47, 2002a, pp.21–36.
18. B. Yang, W. Lin Robust output feedback stabilization of uncertain non-linear systems with uncontrollable and unobservable linearization // IEEE Trans. Automat. Contr., Vol. 50, 2005. pp.619–630.
19. J. Polendo, C. Qian, A generalized homogeneous domination approach for global stabilization of inherently non-linear systems via output feedback // Int. J. Robust Non-linear Control, Vol.17, 2007. pp. 605–629.

О ВИЗУАЛИЗАЦИИ АРХИТЕКТУРНЫХ РЕШЕНИЙ ДЛЯ БЕЗОПАСНЫХ И ЭНЕРГОЭФФЕКТИВНЫХ ЗДАНИЙ

Амиргалиев Е. Н., Калижанова А.У., Козбакова А.Х. Шамиль-уулу Ш.
e-mail: amir_ed@mail.ru, kalizhanova_aliya@mail.ru, ainur79@mail.ru

*Институт информационных и вычислительных технологий КН МОН РК,
Казахстан*

Аннотация. В данной статье рассмотрен новый уровень автоматизации проектирования, технология информационного моделирования, которая предполагает создание единой информационной модели строительного объекта и ее использование, и развитие на различных стадиях проектирования, а также на этапах строительства и эксплуатации. Статья посвящена созданию методики интеграции программных средств с использованием информационного моделирования зданий и сложных инженерных объектов с внедрением технологии BIM.

Введение. Автоматизация проектирования дает технология информационного моделирования, которая предполагает создание единой информационной модели строительного объекта и ее использование и развитие на различных стадиях проектирования, а также на этапах строительства и эксплуатации. Данное исследование посвящено созданию методики интеграции программных средств с использованием информационной модели здания и разработанных алгоритмов календарного планирования для проектирования организации строительства и учета рабочих пространств для проекта производства работ.

Внедрение BIM технологии в нашей стране огромна. При ее использовании намного уменьшаются сроки проектирования здания, увеличивается эффективность эксплуатации готового здания и многое другое.

Информационное моделирование зданий и сложных инженерных объектов, детальная визуализация фасадов и экстерьеров зданий в 3D по обычным фотографиям, централизованный контроль всех работ на каждом этапе жизненного цикла объекта – все эти возможности открываются с внедрением технологии BIM.

В нашей стране эта система почти не используется, в отличие от зарубежных стран, в которых в наше время уже не ведется строительство уникальных объектов без использования этих технологий, приведем примеры объектов, таких как One World Trade Center (Нью-Йорк, США), Концертный зал “Тулли холл” (Нью-Йорк, США), Башня “Эврика” (Мельбурн, Австралия) выполненных полностью с использованием BIM-технологий.

Система «SMART HOUSE» становится все более популярной среди жителей Казахстана, которые стремятся обеспечить комфортные условия проживания, одновременно сократив расходы потребляемых ресурсов (электроэнергия, газ, вода). Установив интеллектуальную систему, владелец дома полностью или частично освобождается от необходимости контролировать работу таких подсистем как отопление, освещение, охрана, вентиляция, кондиционирование.

При желании оборудовать «SMART HOUSE» своими руками, следует знать, что к числу наиболее важных систем, требующих контролируемого управления, относятся охранная, освещение и отопление. Принцип работы системы освещения обусловлен местом установки: внутри дома или снаружи. Управление внутренними источниками

света осуществляется через датчики движения. Они предполагают автоматическое включение света при вхождении человека в комнату и его отключение при выходе людей. Датчики освещения наружной установки реагируют на 2 типа раздражителей: движение и уровень природной освещенности.

Сегодня в мировом экспертном сообществе идут споры о понятии информационной модели, и не удивительно – ведь данная область продолжает свой бурный рост, пределы которого пока и не обозначились. «НЕОЛАНТ» выработал свою концепцию информационного моделирования и на ее основе предлагает внедрение реальных прикладных решений.

Проектирование здания при помощи построения информационной модели позволяет обеспечить согласованность процесса проектирования, быстрый обмен информацией между специалистами различных групп (технологи, архитекторы, конструкторы, инженеры), выбор оптимальных проектных и технологических решений, минимизацию рисков ошибок и конфликтов, жесткий контроль за качеством разрабатываемой документации, а также позволяет прогнозировать эксплуатационные характеристики объекта.

Есть ли в вашей организации задачи, для решения которых будет эффективно применение 3D или информационной модели? Легко проверить по представленной ниже таблице смотрите рисунок 1, в которой собраны типовые задачи предприятия и стратегии их решения за счет использования цифровых моделей.



Рисунок 1 – Типы 3D и информационных моделей

Применение информационной модели здания с самого начала проекта позволяет инженерам и проектировщикам быстрее принимать лучшие решения. Трехмерная графика зданий и систем в BIM строится на основе данных, которые легко корректировать по ходу проекта. Большинство программ типа BIM связывает интеллектуальные объекты, таким образом, при внесении изменений в один объект параметрические изменения будут вноситься во все связанные с ним объекты. К примеру, при изменении параметров расхода воздуха или при замене диффузора автоматически поменяется воздуховод, диффузор и соединительные элементы.

BIM Сервер GRAPHISOFT: Возможности и Преимущества

BIM Сервер GRAPHISOFT, являясь ответом на реальные потребности отрасли, дает возможность организовать совместную работу проектных групп над файлами больших размеров. Он позволяет работать автономно или удаленно, таким образом участники проектирования могут выполнять свою работу из любой точки мира. Любые проектные данные, доступные для импорта в ArchiCAD, могут использоваться в BIM Сервере GRAPHISOFT.

При внедрении BIM-технологий в большом масштабе, архитекторы часто сталкиваются с трудностями, связанными с доступностью модели и управлением рабочим процессом. BIM Сервер компании GRAPHISOFT – это передовое решение, предназначенное для организаций, использующих возможности Teamwork ArchiCAD в совместном проектировании на уровне моделей.

Применение Технологии Delta Server™ позволяет сократить сетевой трафик до минимума, обеспечивая мгновенный и надежный обмен данными как в пределах офиса, так и через Интернет. В Teamwork длительное ожидание синхронизации с сервером ушло в прошлое: участники проектирования могут работать над BIM-моделями в режиме реального времени, используя стандартные Интернет-соединения и находясь в любой точке мира.

Надежность системной архитектуры BIM Сервера гарантирует постоянную сохранность BIM-проектов. Любые ошибки, вызванные неисправными компонентами, моментально блокируются, что позволяет полностью сохранить целостность проекта.

Солнечные панели (коллекторы) BIPV

Солнечные коллекторы на крыше – прошлое, архитекторы ищут новые решения.

Солнечный коллектор – устройство для сбора тепловой энергии Солнца (гелиоустановка), переносимой видимым светом и ближним инфракрасным излучением. В отличие от солнечных батарей, производящих непосредственно электричество, солнечный коллектор производит нагрев материала-теплоносителя. Этот модуль может использоваться при строительстве зданий. Площадь окон занимает значительную часть здания, и ее можно использовать с выгодой. Стекло не влияет на освещенность в помещении, к тому же обладает высокими теплоизоляционными свойствами. Такое решение оптимально подойдет тем, кто не хочет устанавливать модуль на крыше или возле помещения.

Особенности.

Может заменить обычные стеклопакеты на фасадах, навесах, беседках, крышах, окнах, парапетах и др. BIPV модули добавляют эстетическую ценность зданию, а обладание высокими прочностными характеристиками позволяет выдерживать высокую ветровую нагрузку, град и другие неблагоприятные погодные условия. К тому же, они являются источником энергии, не нуждающемся в топливе и техническом обслуживании, и не имеет движущихся частей.

Основной функцией фотоэлектрических модулей (или иначе, PV — модулей) является преобразование солнечного света в электрический ток. На выходе фотоэлектрического модуля генерируется постоянный ток, который может использоваться как напрямую, так и накапливаться в аккумуляторных батареях для дальнейшего использования.

Так, наряду с обычной установкой фотоэлектрических модулей с целью получения электроэнергии, родились два новых понятия в архитектуре, описывающих два основных подхода в интеграции солнечных панелей в конструкцию зданий:

Заключение

Внедрение BIM технологии в нашей стране развиваются и становятся популярными. При ее использовании намного уменьшаются сроки проектирования здания, увеличивается эффективность эксплуатации готового здания и многое другое.

Информационное моделирование зданий и сложных инженерных объектов, детальная визуализация фасадов и экстерьеров зданий в 3D по обычным фотографиям, централизованный контроль всех работ на каждом этапе жизненного цикла объекта – все эти возможности открываются с внедрением технологии BIM.

Список использованной литературы

1. Белоконев Е.Н., Абуханов А.З., Чистяков А.А. Основы архитектуры зданий и сооружений: Учеб. пособ. - Р-н-Д, 2005.
2. Беляков, С. И. Перспективы развития производственного потенциала строительных предприятий в современных условиях / С. И. Беляков // Недвижимость. Экономика. Управление. - 2009. - № 1. - С. 54-57.
3. Бикбау, М. Я. Новые комплексные технологии строительства жилья / М. Я. Бикбау // Строительные материалы, оборудование, технологии XXI века. - 2011. - № 1. - С. 30-32; № 2. - С. 37-39.
4. Благовещенский Ф. А., Архитектурные конструкции. [учебник по специальности "Архитектура"] - 2007
5. Блэзи В., Справочник проектировщика. Строительная физика. [учебное пособие для студентов, обучающихся по направлению подготовки "Строительство". полноцветное издание] - 2012 (Мир строительства. 10, 11)
6. Бондаренко С. В., AutoCAD для архитекторов. [интерфейс и основные приемы работы в программе, создание и редактирование объектов, объектная привязка и отслеживание, слои, блоки, нанесение размеров и надписей, редактирование готовых элементов, построение различных элементов модели постройки, создание поэтажного плана, построение фасадов и крыш] - 2009
7. Инновационные компьютерные технологии по ценообразованию в строительстве // Промышленное и гражданское строительство. - 2009. - № 8. - С. 42-44.
8. Казаков Ю. Н., Строим дом быстро и дешево. [как я сам за 1 год построил коттедж всего за \$46 тыс. вместо покупки у подрядчика-риелтора за полмиллиона]- 2009 (Современный домострой)
9. Калугин, Ю. Б. Расчет календарных планов работ с вероятностными временными параметрами / Ю. Б. Калугин // Известия вузов. Строительство. - 2011. - № 10. - С. 51-59 : табл. - Библиогр.: с. 58-59.

DEVELOPING OF AN AUTOMATED SYSTEM FOR LEXICAL, SYNTAX AND SYNTAGMATIC ANALYSIS OF KAZAKH TEXTS AND ITS EMOTIONAL CLASSIFICATION

Amirgaliyev Ye.N.^{1,2}, Mussabayev R.R.¹, Tairova A.T.²,
Kozbakova A.H.², Mussabayev T.R.²
email: rmusab@gmail.com

¹ *Institute of Information and Computational Technologies SC MES RK,
Kazakhstan*

² *Uniline Group LLP, Kazakhstan*

Abstract. *In the given article considered the process of automated system development for lexical, syntax and syntagmatic analysis of Kazakh texts and its emotional classification. Development scope of this system included comprehensive research of Kazakh language features. The results of this research were later used to construct algorithms of lexical, morphological and syntax analysis processes for Kazakh texts. Linguistic analyzer system incorporates four analyzers (lexical, morphological, syntax and semantic analyzers), which handle data successively or sequentially one after another. An output thread of one analyzer is fed to the input of the following analyzer. The result analysis is the emotional (intonational) classification of the input text.*

This stage was to develop an automated system for lexical and syntax analysis of texts in Kazakh language. This system is presented in the form of a software suite and is a part of solution for the best known challenges in the field of artificial intelligence, machine-aided understanding of human language texts. Lexical and syntax (parsing) analysis modules are integrated in the framework of a own developed unified language processor LinProc v3.0. This language processor will be positioned as a separate commercial product in the future. This processor is an integral part of most systems for automated data processing in human language. The following is included among these systems which are unable to function without the use of built-in language processor:

- 1) Text-to-speech synthesis systems;
- 2) Speech recognition systems;
- 3) Information retrieval systems;
- 4) Spelling, syntax and punctuation systems.

The primary purpose of syntax analysis system is to implement automatic structuring of textual data into a variety of sentences and classify such sentences by type (narrative, exclamatory, interrogative etc.) The entire complexity of syntax analysis process is the complexity of finding sentence boundaries. For example, the full stop does not always clearly define the end of a sentence because it can be used for abbreviations, dates, decimals etc.

Development scope of this system included comprehensive research of Kazakh language features. The results of this research were later used to construct algorithms of lexical, morphological and syntax analysis processes for Kazakh texts.

Kazakh language belongs to the Turkic language family, which also includes Turkish, Uzbek, Kyrgyz, Tatar, Bashkir, Azerbaijan and other languages. Kazakh language falls into agglutinative language group. Agglutinative languages typically incorporate connection of monosemantic affixes conveying grammatical meanings to inflexible root or stem which are not lexical meaning carriers.

In particular, given Turkic or agglutinative languages in general, automatic analysis challenges should be addressed alternatively than this is being done for inflectional and inflectional - analytical languages.

In Indo-European languages, any word form is used with one or two affixes and adjustment of these word forms to dictionary aspects is not especially challenging to accomplish. With regard to Turkic languages, word forms may contain a large number of morphological indicators where each word stem can be used to create thousands of forms.

This work milestone was to develop principles and algorithms for automatic morphological analysis of Kazakh word form, build a mathematical model for the process of Kazakh text morphological analysis and then implement it in software.

The primary task within this section was to develop an analyzer for Turkic morphology which is used to construct computer-aided analysis algorithm for Kazakh text. This algorithm can be used as one of the primary modules of various computer-aided translation, indexing, annotation, referencing, etc. systems.

The work scope also included review of problems associated with software implementation of computer-aided morphology model for Turkic languages based on Kazakh language material. The proposed model allows conducting a full morphological analysis and obtaining the required grammatical characteristics for the subsequent stages of linguistic analysis.

One of the most important components of a language analyzer (LA) is the automatic morphological analysis algorithm. When building an LA algorithm, the primary objective is the optimized separation of a word form into stems and the subsequent variety of affixes. LA operates basing on comparison of textual word forms with the units linguistic data bank by the length of alphabetic chains. The results of this research revealed that this option of algorithm is the best one for agglutinative languages.

Linguistic analyzer system incorporates four analyzers (lexical, morphological, syntax and semantic analyzers), which handle data successively or sequentially one after another. An output thread of one analyzer is fed to the input of the following analyzer.

The purpose of syntax analyzer is to determine the boundaries of sentences, separate words, identifiers and punctuation marks as well as build a syntax graph of a sentence. Morphological analyzer searches for lemma (normal dictionary form) in the dictionary (separate database) and determines associated morphological parameters (for example, part of speech, gender, quantity, case etc.)

Algorithms of syntax and lexical analyzers were implemented as individual software modules (Fig. 1 and 2).

The following dictionaries were used as the source lexical materials: word stems, abbreviations, geographical names, dictionary of names and last names, phraseological dictionary. The total number of words currently includes 140 thousand words.

This processor is, above all, regarded as a proof-of-concept platform for creation of industrial syntax systems for Turkic languages group. Processing speed or throughput is determined by software support for the methodology. The available software support for the methodology may be significantly optimized for further industrial use. The quality of morphological analysis using dictionary depends on two parameters:

- The volume of dictionary - number of lexical units or lexemes included in the dictionary;
- Morphological coverage - percentage of indentified words in the dictionary while analyzing random corpus of texts.

For morphological component of LinProc project, dictionary volume includes 140 thousand lexemes (this number includes singular names, geographical names and phraseological dictionary), the coverage is 95%.

The work is currently performed to migrate morphological analyzer and morphological dictionary as a web service.

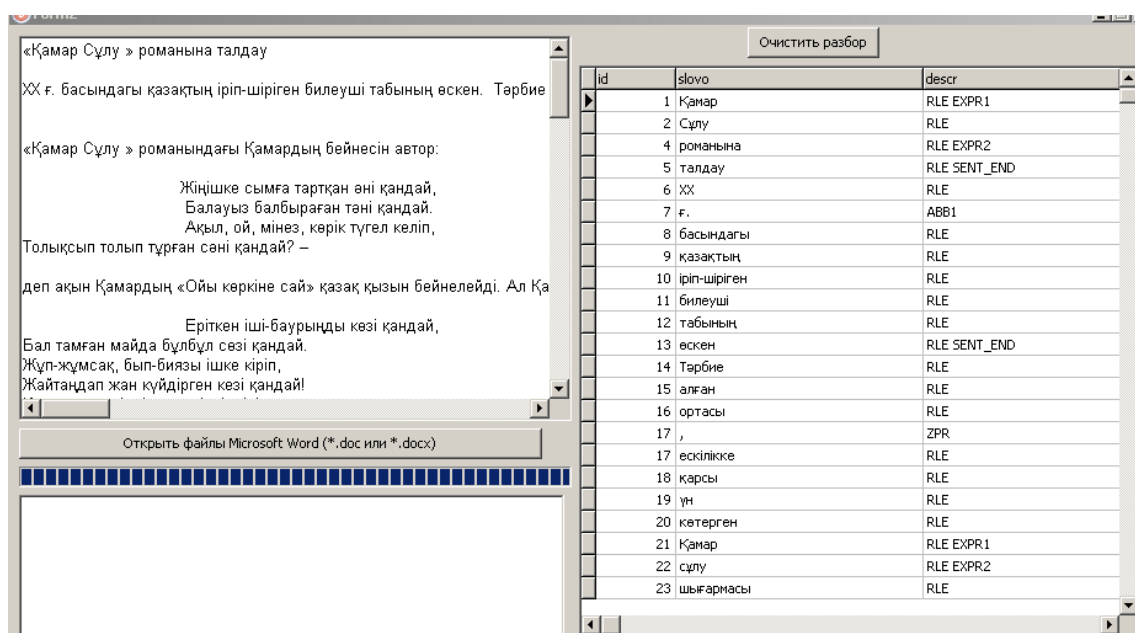


Fig. 1 - Kazakh text syntax analyzer.

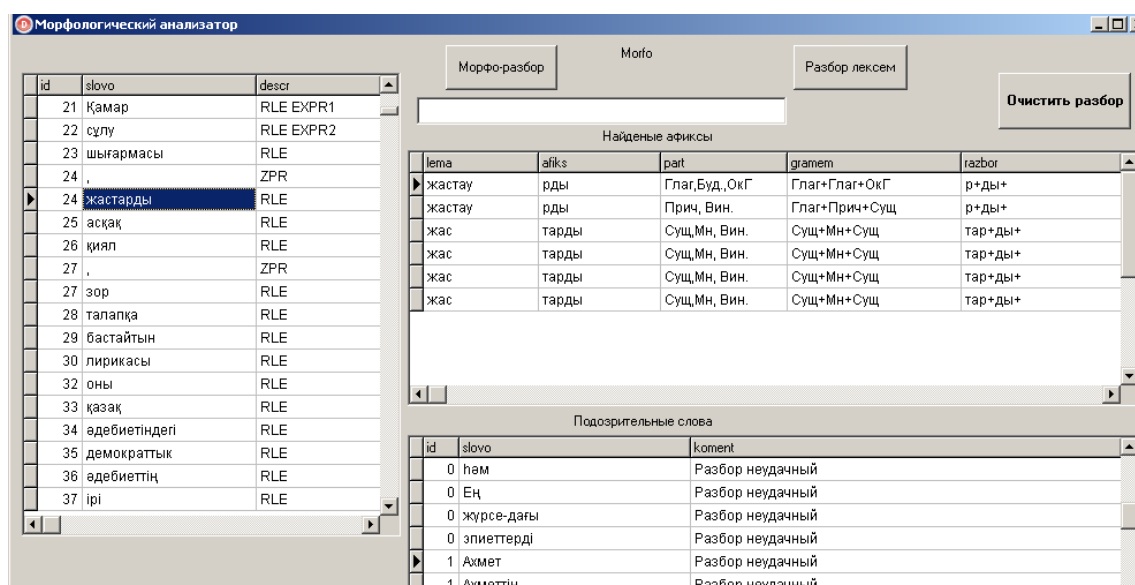


Fig. 2 Kazakh text morphological analyzer.

The next stage includes a set of works to develop an automated system for syntagmatic analysis of Kazakh language texts.

The purpose of prosodic processor is to determine the current intonation patterns, acoustic intensity, phonemic length and pause time by analyzing the identified properties of source text. Prosodic text layout results from its breakdown into syntagms, setting of syntagms by accentual units and marking of intonational types of syntagms in accordance with certain rules. In an intonational sense, the syntagm refers to an independent part of a sentence or such entire sentence. Setting of syntagm boundaries affects the reproduction of intonational features in speech synthesis as well as reproduction of semantic content. When splitting text into syntagms, it is important not to place the syntagm boundary where it can disrupt the semantic speech

perception (or reproduction of semantic content of the text), for example, between the subject and it's token / attribute [3].

One of the important intonational components is a pause. The correct pausing is needed for easy speech perception, and in many cases, for the correct understanding of sentence meaning.

Much of information on pauses in the text is reproduced using punctuation marks, however, large pieces without any marks can also be encountered that are not easy for listening recognition when the text is being read without pauses. On the other hand, the punctuation marks inside sentences do not always suggest that it is necessary or possible to make pauses. Thus, a complete text-to-speech synthesis system needs to be equipped with a special algorithm that allows splitting text into syntagms, setting pauses, an algorithm which would not have only incorporated punctuation marks, but also lexical and syntactic context [1].

The next step is to define the intonational type of a syntagm. The main intonational types of syntagms are the following: Completeness, incompleteness, question and exclamation. The number of intonational subtypes for the major intonational types may run into several tens of the same. Identifying the type of intonation contour (IC) includes the use of information on a punctuation mark, which ends with a syntagm. The information also contains certain words in syntagm structure. A total of IC types are identified (classification based on IC classification by Z.M. Bazarbayeva [1]).

Normalized text undergoes the following analysis steps through the structure of prosodic processor:

- Separation into punctuation and lexical syntagms.
- Separation into syntactic syntagms.
- Marking of intonational syntagms.

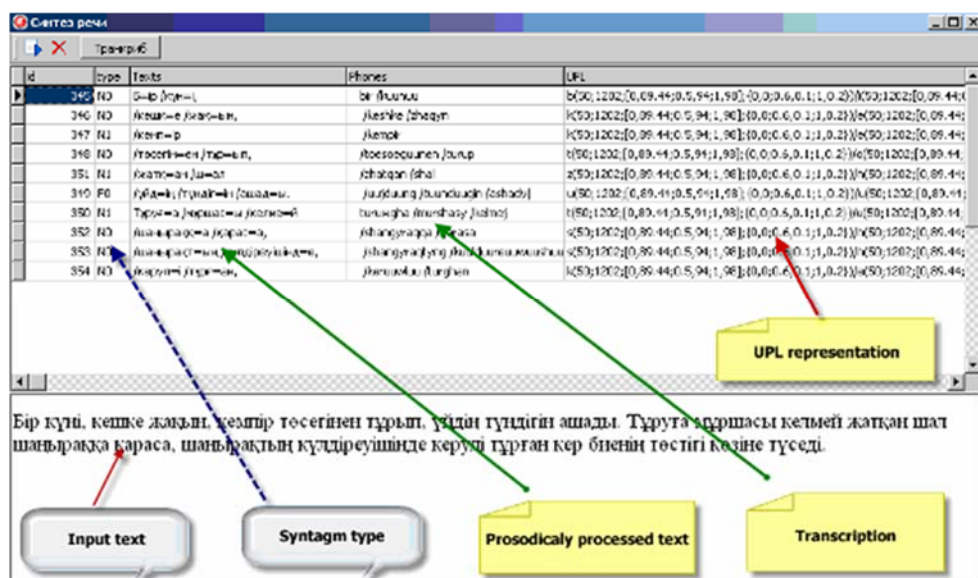


Fig. 3 User interface of the designed system for syntagmatic analysis of Kazakh language texts. Prosodic process then delivers marked-up text. Fig. 3 shows user interface of the designed system for syntagmatic analysis of Kazakh language texts.

References

1. Bazarbayevs Z. M. Kazakh intonation. – Almaty: Dayk-Press, 2008. – 284 pp.

2. Abuov Zh., Dzhunisbekov A. The phonetical writing of Kazakh text. – Alma-Ata: Science, 1991. – 83 pp.
3. Lobanov B. M., Tciryl'nik L.I. Computer synthesis Computer synthesis and cloning of speech. Minsk, «Belarus science», 2008. – 344 p.

ПРИМЕНЕНИЕ БЕСПРОВОДНЫХ СЕТЕЙ ДЛЯ ОПРЕДЕЛЕНИЯ ПОЛОЖЕНИЯ ВНУТРИ ПОМЕЩЕНИЯ – ТРИЛАТЕРАЦИЯ

Е. Амиргалиев, Р. Юнусов
e-mail: rassul.yunussov@sdu.edu.kz

*Институт информационных и вычислительных технологий МОН РК,
Казахстан*

Аннотация

В статье рассматривается способ получения положения объекта внутри помещения и проблемы определения точности расчетов с использованием беспроводных сетей передачи данных. Используется латерация, процесс определения абсолютного или относительного местоположения точек путем измерения расстояний, используя геометрию кругов, сфер или треугольников. Для плоскости данная задача получила наименование Трилатерация - так как необходимое количество известных точек равно 3-м. В трехмерном пространстве, решение возможно при наличии большего количества объектов с известными координатами и расстояниями до них. От 3-х, если они расположены на одной линии и более, когда расположение их свободно.

Ключевые слова: *навигация, трилатерация, координаты, маячок, радиосигнал, LBS, латерация, трилатерация*

Актуальность проблемы

Информация, которая может быть доступна при получении данных о внутреннем положении объектов в помещении может быть использована для решения различных актуальных задач начиная с логистики и кончая маркетингом. Одна из таких задач - эвакуация людей из опасных закрытых зон. Проблема построения оптимального маршрута для каждого участника эвакуации на основе информации о доступности прохода, о количестве кандидатов на прохождение через участок [1]. Другая задача - тактическое планирование перемещения мобильных групп при выполнении задания, где данные о текущем положении имеют большое значение.

Один из наиболее ярких примеров применения навигации внутри помещений – аудиогиды. Это автоматические системы включения звукового сопровождения в соответствии с положением объекта внутри помещения, что значительно увеличивает проходимость в музеях и снижает расходы на содержание персонала.

Суть метода трилатерации

Трилатерации состоит в определении координат пунктов, расположенных в вершинах треугольников всей сети, через измерения длин сторон между ними. Характерная схема ряда трилатерации показана на рис.1. По исходным данным известных координат смежных пунктов (А, В), расстоянию между ними (b), а также по

измеряемым длинам сторон и вычисленным горизонтальным проложениям d_1, d_2, d_3 и так далее до другой стороны (b_1) ряда между пунктами С и D получают конечный результат. Математический аппарат в виде теоремы косинусов и прямой геодезической задачи позволяет вычислить соответственно неизвестные горизонтальные углы и искомые координаты вершин треугольников.

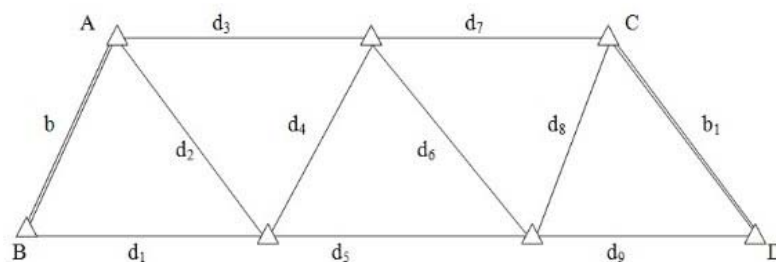


Рисунок 1 - Сеть треугольников, получаемая в геодезии для получения координат измеряемых объектов

Таким образом по горизонтальным положениям и направляющим углам (с использованием тригонометрических функций) можно найти приращения координат, через которые получают координаты геодезических пунктов.

Существующие решения

1) Навигация по Wi-Fi. Используются данные о потере мощности сигнала. Требуется предварительная работа по точному заданию координат каждого Wi-Fi роутера. Точность до 2 метров. Имеет недостатки, такие как защита устройств от рекламной слежки [5].

2) Геомагнитное позиционирование. Основано на ориентировании по магнитному полю Земли и базируется на геомагнитных аномалиях как критериях для геомагнитного позиционирования (аномалии возникают вследствие неоднородности геомагнитного поля). Заключается в фиксации геомагнитных аномалий и нанесении их на карту территории, на которой предполагается ориентироваться. В дальнейшем навигация производится по составленной карте устройством, в которое встроен магнитометр. Высокая сложность реализации и невысокая точность делают решение не масштабируемым и неэффективным в большинстве случаев [4].

3) Системы спутниковой навигации (GPS/Глонасс и т.д.) + инерциальные навигационные системы (ИНС). Используется при периодической потере открытой видимости. Удобно для коротких промежутков, вроде тоннелей. В ИНС ошибки постоянно накапливаются, и со временем данные, полученные с ИНС, становятся все более и более отличными от действительности. Поэтому на затяжных сложных участках точность резко падает [4].

4) Ориентирование по базовым станциям операторов сотовой связи (GSM). Минусы – невысокая точность (БС может быть удалена на расстоянии в 35км от пользователя + некоторые БС являются мобильными и постоянно меняют свою дислокацию) [4].

5) Использование Bluetooth-маячков Beacon – даёт достаточную точность при приемлемом уровне финансовых затрат. Именно данную технологию рассмотрим подробнее в статье.

б) Навигация, основанная на синергетическом эффекте – решает задачу определения текущего местоположения, используя все (или большинство) из перечисленных выше способов. Эффективность достигается за счёт того, что мы используем сразу несколько векторов определения координат, что способствует компенсации ошибок и повышению точности определения координат [4].

Решение задачи с использованием данных о затухании сигнала

Для нахождения расстояний используется модель распространения радиоволн, требующий калибровки некоторых параметров, зависящих от особенностей среды:

$$PL(d) = P_t - P(d) = PL(d_0) + n10 \lg \frac{d}{d_0},$$

где d — расстояние до агента, $PL(d)$ — потеря мощности сигнала на расстоянии d , P_t — мощность передатчика, $P(d)$ — мощность сигнала на приемнике на расстоянии d , d_0 — расстояние 1 метр, n — коэффициент распространения сигнала в среде. На рис. 2 изображены геометрические подходы к решению задачи позиционирования, где, r_i — расстояние до i -й точки доступа от агента.

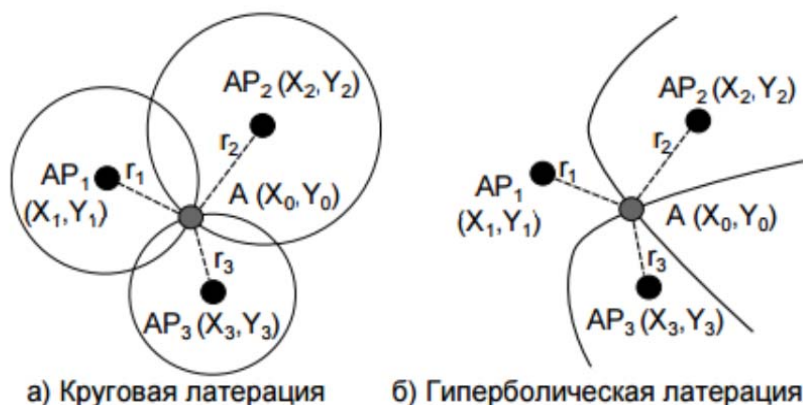


Рисунок 2 - Геометрические подходы к решению задачи позиционирования

Круговая латерация (рис. 2) основана на расстоянии между искомой точкой и точками доступа. Для вычисления координат агента, необходимо решить систему из уравнений вида:

$$r_i = \sqrt{(X_i - X_0)^2 + (Y_i - Y_0)^2}. \quad [6]$$

Гиперболическая латерация (рис. 2) основана на разнице расстояний между агентом и точками доступа. Для вычисления координат агента, необходимо решить систему из уравнений вида:

$$d_{ij} = r_i - r_j = \sqrt{(X_i - X_0)^2 + (Y_i - Y_0)^2} - \sqrt{(X_j - X_0)^2 + (Y_j - Y_0)^2}. \quad [6]$$

Достоинством алгоритма является достаточно высокая точность, при соответствующих параметрах среды. Недостатком алгоритма является необходимость

тщательного построения модели распространения сигнала в каждой конкретной среде, для каждой отдельной точки доступа, что в конечном итоге не гарантирует очень высокую точность, в результате возникновения в помещении таких эффектов как, затухание и отражение сигнала, моделирование которых является весьма проблемной задачей.

Дифференциальная латерация (Differencial lateration)

Данный алгоритм является альтернативой предыдущего и представляет собой метод аппроксимации, основанный на переборе возможных координат агента, с целью нахождения ближайшей точки к месту пересечения окружностей. Преимуществом данного алгоритма является отсутствие необходимости калибровки параметров в модели распространения сигнала. Алгоритм представлен в следующих вариантах реализации:

Вариант 1. Координаты агента вычисляются через минимизацию функционала, ядром которого является отношение затуханий сигнала от 1 и i -й точек доступа до произвольной точки с координатами (x, y) . Будем считать, что коэффициент затухания сигнала, выраженный в децибелах, соответствует формуле:

$$P(d) = P_0 - n10 \lg d,$$

где d — расстояние до агента, P_0 — значение мощности сигнала на расстоянии одного метра и n — коэффициент распространения сигнала. Значения P_0 и n неизвестны. Для того, чтобы избавиться от этих неопределенных параметров, необходимо оценить положение агента через минимизацию следующего функционала:

$$\begin{cases} (X_0, Y_0) = \operatorname{argmin}[\gamma(x, y)] \\ \gamma(x, y) = \sum_{i=2}^N \left| \frac{P_i}{P_1} - \frac{\lg[d_i(x, y)]}{\lg[d_1(x, y)]} \right|^2, \end{cases}$$

где d_1 и d_i — расстояния соответственно от 1 и i -й точки доступа до текущей точки с координатами (x, y) . [5]

Вариант 2. Координаты агента также вычисляются через минимизацию функционала, ядром которого является отношение затуханий сигнала от 1 и i -й точек доступа. Однако перед этим происходит оценка параметров в модели распространения сигнала путем минимизации среднеквадратической ошибки:

$$\begin{bmatrix} P_0 \\ n \end{bmatrix} = (M^T M)^{-1} M^T P, \quad M = \begin{bmatrix} 1 & -10 \lg d_1 \\ \vdots & \vdots \\ 1 & -10 \lg d_T \end{bmatrix}, \quad P = \begin{bmatrix} P_1 \\ \vdots \\ P_K \end{bmatrix}.$$

Тогда координаты агента могут быть оценены через минимизацию нового функционала:

$$\begin{cases} (X_0, Y_0) = \operatorname{argmin}[\gamma(x, y)] \\ \gamma(x, y) = \sum_{i=2}^N \left| \frac{P_i}{P_1} - \frac{P_0 - n10 \lg[d_i(x, y)]}{P_0 - n10 \lg[d_1(x, y)]} \right|^2. \end{cases} \quad [6]$$

Вариант 3. Координаты агента вычисляются через минимизацию функционала, ядром которого является разность затуханий сигнала от 1 и i -й точек доступа. Этот алгоритм является модификацией варианта 2. Функционал для минимизации определяется следующим выражением:

$$\begin{cases} (X_0, Y_0) = \operatorname{argmin}[\gamma(x, y)], \\ \gamma(x, y) = \sum_{i=2}^N |(P_i - P_1) - ((P_0 - n10\lg[d_i(x, y)]) - (P_0 - n10\lg[d_1(x, y)]))|^2 \end{cases}$$

Преимуществами являются простота реализации и достаточно высокая точность. Варианты алгоритма 2 и 3 демонстрируют еще более высокую точность, так как производится оценка параметров для модели распространения сигнала. К недостаткам можно отнести повышенную вычислительную сложность $O(N \cdot K)$, где K — количество точек для перебора. Для повышения качества работы алгоритма необходимо начальное приближение, что позволит уменьшить вычислительную сложность. Данный алгоритм можно отнести как к базовым, так и улучшающим, причем, не требуются предварительные измерения [6].

Использование аппаратных средств Beacons

В плане физической реализации Beacons-маячки (рисунок 3) — это Bluetooth 4.0 LE (Low Energy) устройства. Типичный Beacons-маячок имеет довольно компактные размеры, и способен проработать всего лишь от одной батарейки до двух лет. Дальность действия маячка — в среднем 10 метров (варьируется от 15-20см до 25-40м в зависимости от модели и настроек). Периодичность выдачи данных — 200мс, но можно настроить и на более частую периодичность, и на более редкую. Маячок является простым устройством, который только выдаёт всем подряд в эфир свои данные [10].

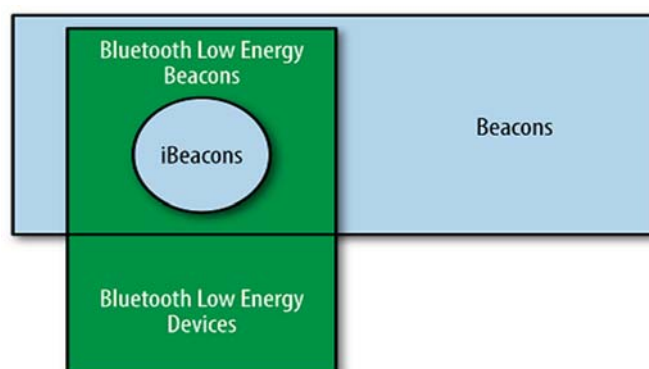


Рисунок 3 - Схема Beacons маячка

Для реализации трилатерации с использованием таких маячков - необходимо их равномерно разместить по всему периметру здания. А так же иметь метрические характеристики здания и координаты установки маячков в локальной системе. Каждый маячок передает в своем сообщении значение силы сигнала - TX Power. Это — эталонное значение мощности маячка, представляющее собой силу сигнала на расстоянии в 1 метр от маячка. Измеряется и записывается в маячок 1 раз при его производстве. Данная константа используется при определении расстояния от пользователя до маячка. Первый бит является знаковым (1 — «-», 0 — «+») [11].

Чтобы определить положение в пространстве подвижного объекта необходимо получить информацию о расстоянии до маячков. Это нам позволяет сделать параметр RSSI (Received Signal Strength Indicator), вычисляемый пользовательским Bluetooth-приёмником на основе силы принимаемого сигнала. Чем выше значение этого параметра – тем ближе объект находится к маячку. TX Power – это и есть RSSI, только эталонный, измеренный производителем маячка на расстоянии 1 метра от него. Для определения расстояния до маячка (в метрах) используется текущее значение RSSI, и эталонный TX Power для коррекции.

Сложность вычисления координат на основе получения данных о затухании радиосигнала связана с тем, что параметр RSSI не стабилен. Это происходит из-за следующих факторов:

- Ориентация и характеристика направленности излучения или приёма антенной маячка/пользовательского устройства
- Присутствие крупных экранирующих объектов (человек таковым тоже является) по направлению от маячка до устройства
- Наличие поблизости поверхностей из материалов, хорошо отражающих радиосигнал, а также большое скопление маячков Beacon на одной территории, за счёт многолучевой интерференции с основным лучём [5]

Для того, чтобы снизить разброс значений RSSI можно усреднить их путем использования буфера накопления данных и усредняя их ползущим окном.

Далее можно выбрать только три лучших по показателям усреднения RSSI маячка. И уже используя их получить координаты подвижного объекта на основе применяемой формулы трилатерации [4].

Даже если объект не движется - его вычисляемое местоположение будет с погрешностью до 3 м. Показатель можно улучшить путем дальнейшей математической обработкам полученных результатов. Для этого можно воспользоваться фильтром Калмана [12].

В фильтре имеется возможность учитывать управляющее воздействие. Например, таким управляющим воздействием может быть информация с акселерометра, что значительно улучшает результат (в таком варианте погрешность составляет уже не 3 метра в нашем случае, а 1-1.5 – тоже не мало, но связано отчасти с тем, что фильтр Калмана использует систему с заданным уравнением движения, а мы имеем дело с хаотичным движением). Т.е. схема следующая: считаем средние RSSI -> выбираем 3 маячка с лучшими RSSI -> получаем координату путём трилатерации -> подаём на вход фильтра Калмана (вместе с показаниями акселерометра в качестве управляющего воздействия).

Есть возможность уменьшения погрешности – применять сразу 2 системы – помимо основного определения положения при помощи Beacon маячков, использовать для коррекции этого положения инерциальную навигационную систему, состоящую из акселерометра, гироскопа и компаса [12].

Заключение

Поиск объектов и их координат в закрытых пространствах можно осуществлять различными способами. Как путем наружного наблюдения, так и с использованием специализированных аппаратных средств. При использовании маячков с радиосигналом можно воспользоваться методом трилатерации, который хорошо себя показывает на практике и дает относительно точное положение объектов в пространстве. В задачах эвакуации это бы помогло значительно повысить шансы людей на выживание, путем

предоставления им информации об оптимальном маршруте эвакуации, а спасательным бригадам точно применять свои усилия для спасения людей.

Следует отметить, что модель расчета и получения координат опирается на существующие алгоритмы усреднения значений и фильтры для улучшения показателей точности. В дальнейшем планируется использование нейронных сетей для улучшения качественных показателей точности определения координат в закрытом помещении.

Литература

1. Yedilkhan Amirgaliyev, Rassul Yunussov, Orken Mamyrbayev, Optimization of people evacuation plans on the basis of wireless sensor networks // Open Engineering. Volume 6, Issue 1, ISSN (Online) 2391-5439, DOI: 10.1515/eng-2016-0026, September 2016

2. Википедия (свободная энциклопедия) дала описание терминов и позволила быстро найти необходимую связанную с данными терминами информацию.

3. Google I/O 2013 — The Next Frontier: Indoor Maps данная конференция довольно точно и кратко описывает важность indoor-навигации в помещениях, а также позволяет осознать насколько разнообразны применения данного вида навигации.

4. «An evaluation of indoor location determination technologies» Kevin Curran, Eoghan Furey

Данная книга позволяет лучше понять термины, которые возникли в процессе исследования этой проблемы и предполагает новые возможности применения данной системы. Так же эта книга дает представление о самых популярных используемых на данный момент способах определения местоположения и позволяет понять, возможно ли осуществление идеи, предложенной в этой работе технически.

5. «Основы геоинформатики» Тикунов В. С. дала представление о том, что такое ГИС, позиционные и непозиционные пространственные данные, а также в ней описаны требования к БД карт, что карта является результатом обработки и визуализации данных, организованных и структурированных в виде базы географических данных.

6. Обзор алгоритмов локального позиционирования для мобильных устройств Р.М. Миниахметов, А.А. Рогов, М.Л. Цымблер. Вестник ЮУрГУ. Серия «Вычислительная математика и информатика»

7. Google Maps [Электронный ресурс] - Электр. Данные

8. Brinker, R.C. and Minnick, R. 12. Trilateration // The Surveying Handbook. — Chapman & Hall, 1995

9. Gateguru. URL: <http://gateguru.com/about.html>

10. Bluetooth Low Energy. URL: <http://developer.android.com/guide/topics/connectivity/bluetooth-le.html>

11. Статья: Применение маячков beacon и технологии bluetooth low energy для построения систем навигации в зданиях. Фальков Е.В., Романов А.Ю. URL: <http://cyberleninka.ru/article/n/primenenie-mayachkov-beacon-i-tehnologii-bluetooth-low-energy-dlya-postroeniya-sistem-navigatsii-v-zdaniyah>

12. Фильтр Калмана // URL: <https://habrahabr.ru/post/166693/>

ПОИСК КРАТЧАЙШЕГО ПУТИ В ПРЯМОУГОЛЬНОЙ СЕТИ

Арсланов М.З.
E-mail: mars@ipic.kz

*Институт информационных и вычислительных технологий МОН РК,
Алматы, Республика Казахстан,*

Статья посвящена задаче поиска кратчайшего пути в некоторой ациклической сети.

1. Основные результаты

Рассмотрим следующую задачу динамического программирования. На плоскости дана прямоугольная ациклическая сеть с узлами в целочисленных точках Z_+^2 с ребрами двух видов. Вертикальное ребро направлено из узла (x, y) в узел $(x, y + 1)$ и имеет длину $f(x)$, зависящую лишь от координаты x . Горизонтальное ребро, направленное из узла (x, y) в узел $(x + 1, y)$, имеет длину $g(y)$, зависящую лишь от координаты y . Требуется найти кратчайший путь из нулевого узла в узел (M, N) . Ясно, что любой путь из $(0, 0)$ в (M, N) содержит $M + N$ ребер, из которых M горизонтальных и N вертикальных. Без потери общности можно считать, что функции $f(x), g(y)$ неотрицательны, иначе можно прибавить к этим функциям некоторое число. Легко видеть, что при этом оптимальные маршруты сохраняются. Для поиска кратчайшего пути легко выписывается следующая задача динамического программирования:

$$F(X, Y) = \min(F(X, Y - 1) + f(X), F(X - 1, Y) + g(Y)), \quad (1)$$

где $F(X, Y)$ – длина кратчайшего пути из начала координат в узел (X, Y) , $F(0, 0) = 0$. Тогда $F(M, N)$ будет равно длине кратчайшего пути из нулевого узла в узел (M, N) .

Длинный шаг из узла (x, y) в узел $(x, y + z)$:

$$(x, y) \rightarrow (x, y + 1) \rightarrow \dots \rightarrow (x, y + z - 1) \rightarrow (x, y + z)$$

будем обозначать $(x, y) \rightarrow (x, y + z)$. Ясно, что его длина равна $zf(x)$. Аналогичный смысл имеет обозначение $(x, y) \rightarrow (x + z, y)$.

Поскольку каждый путь из нулевого узла в узел (M, N) представляет собой попеременное движение на "север" и "восток", то отсюда следует, что любой путь можно единственным образом записать в виде последовательности длинных шагов вида:

$$(0, 0) = (x_0, y_0) \rightarrow (x_0, y_1) \rightarrow (x_1, y_1) \rightarrow \dots \rightarrow (x_{k-1}, y_k) \rightarrow (x_k, y_k) = (M, N) \quad (2)$$

с условием, что $x_i \neq x_{i-1}, y_{i+1} \neq y_i, i = 1, 2, \dots, k - 1$. Возможно лишь, чтобы $y_1 = y_0, x_{k-1} = x_k$. Назовем точки $x_i, y_i, i = 0, 1, 2, \dots, k$ узловыми точками пути. Легко подсчитать, что длина L маршрута (2) равна

$$L = \sum_{i=1}^k (y_i - y_{i-1})f(x_{i-1}) + (x_i - x_{i-1})g(y_i), \quad (3)$$

то есть зависит лишь от значений функций f, g в узловых точках.

Отметим следующие свойства этой задачи.

Свойство 1 Если $f_1(x) \geq f_2(x), g_1(y) \geq g_2(y)$, то $F_1(M, N) \geq F_2(M, N)$, где $F_i(M, N)$ – длина кратчайшего пути для сети, описываемой функциями f_i, g_i .

Свойство 2 Если $f_1(x) \geq f_2(x), g_1(y) \geq g_2(y)$ и в узловых точках кратчайшего пути для второй задачи функции совпадают, то этот путь будет кратчайшим и для первой задачи.

Свойство 3 Задача о кратчайшем пути из узла (a, b) в узел (M, N) эквивалентна задаче о кратчайшем пути из начала координат в узел $(M - a, N - b)$ с соответствующим образом преобразованными функциями:

$$f'(x) = f(x - a), g'(y) = g(y - b).$$

Важность задачи (1) вытекает из задачи оптимального раскроя прямоугольного листа (A, B) на равные меньшие прямоугольники (c, d) и (d, c) . При этом критерием оптимальности является площадь остатков. В [7] показано, что эта задача эквивалентна следующей задаче динамического программирования

$\varphi(A, B) = \min(\varphi(A - c, B) + cd\{B/d\}), \varphi(A, B - c) + cd\{A/b\}$,
где $\varphi(A, B)$ – наименьшая площадь остатков, $\{\cdot\}$ – дробная часть аргумента,

$$\varphi\left(A - c\left\lfloor\frac{A}{c}\right\rfloor, B - c\left\lfloor\frac{B}{c}\right\rfloor\right) = c^2 \left\{\frac{A}{c}\right\} \left\{\frac{B}{c}\right\}.$$

Эта задача эквивалентна задаче о кратчайшем пути из узла $(0, 0)$ в (M, N) , где

$$M = \left\lfloor\frac{A}{c}\right\rfloor, N = \left\lfloor\frac{B}{c}\right\rfloor, f(x) = \left\{\frac{A - cx}{d}\right\}cd, g(y) = \left\{\frac{B - cy}{d}\right\}cd.$$

Если $F(M, N)$ – ее решение, то

$$\varphi(A, B) = F(M, N) + c^2 \left\{\frac{A}{c}\right\} \left\{\frac{B}{c}\right\}.$$

Для того, чтобы убедиться в эквивалентности обеих задач, достаточно сопоставить движению по ребру $((x, y), (x + 1, y))$ отрезание от стороны $A - cx$ прямоугольника $(A - cx, B - cy)$ полосы $(c, B - cy)$, остаток от раскроя которой на прямоугольники (c, d) равен $g(y) = \left\{\frac{B - cy}{d}\right\}cd$. Аналогично сопоставление движению по ребру $((x, y), (x, y + 1))$ отрезание от стороны $B - cy$ полосы $(A - cx, c)$, остаток от раскроя которой на прямоугольники (c, d) равен $f(x) = \left\{\frac{A - cx}{d}\right\}cd$.

Для решения задачи (1) существует стандартный алгоритм, для реализации которого достаточно памяти размера $O(\min(M, N))$ и времени порядка $O(MN)$. Коротко опишем этот алгоритм. Пусть $M \geq N$. Тогда легко видеть, что $F(0, Y) = Yf(0)$. Сохраним в памяти вектор $(F(0, 0), F(0, 1), \dots, F(0, N)) = (v_0, v_1, \dots, v_N)$.

На первой итерации по формуле (1) вычисляем вспомогательный вектор

$$u_0 := v_0 + g(0), u_0 := \min(v_1 + g(1), u_0 + f(1)), \dots, u_N := \min(v_N + g(1), u_{N-1} + f(1)) \quad (4)$$

После этого вектору v присвоим вектор u , т.е. $v := u$. На i -й итерации вычисления аналогичны:

$$u_0 := v_0 + g(0), u_1 := \min(v_1 + g(1), u_0 + f(i)), \dots,$$

$$u_N := \min(v_N + g(1), u_{N-1} + f(i)); v := u.$$

В памяти достаточно хранить $2(N + 1)$ чисел. Поскольку на каждой итерации необходимо $N + 1$ вычислений типа (4), то поскольку итераций всего $M + 1$, то получаем временную сложность алгоритма $O(MN)$.

Оказывается, что структура задачи (1) позволяет построить алгоритм с временной сложностью $O(M + N)$.

Для дальнейшего изложения нам понадобятся некоторые понятия и теоремы выпуклого анализа [2], перенесенные на функции дискретного аргумента $x \in Z$.

Определение 1 Функция $f(x)$ дискретного аргумента $x \in Z$ называется выпуклой на отрезке $[a, b] = \{a, a + 1, \dots, b - 1, b\}$, если для любых $x < y < z$ из этого интервала

$$f(y)(z - x) \leq f(x)(y - x) + f(z)(z - y).$$

В частности, линейная функция $f(x) = \alpha + \beta x$ является выпуклой на любом отрезке.

Приведем без доказательства следующее простое, но важное свойство выпуклых функций.

Свойство 4 Если функция $f(x)$ выпукла на отрезке $[a, b]$, то для некоторых точек $a = x_0 < x_1 < \dots < x_m = b$ она может быть единственным образом представлена в виде

$$f(x) = \begin{cases} \alpha_1 + \beta_1 x, & x \in [x_0, x_1] \\ \alpha_2 + \beta_2 x, & x \in [x_1, x_2] \\ \dots\dots\dots \\ \alpha_m + \beta_m x, & x \in [x_{m-1}, x_m] \end{cases} \quad (5)$$

где $\alpha_i + \beta_i x_i = \alpha_{i+1} + \beta_{i+1} x_i$ и $\beta_1 < \beta_2 < \dots < \beta_m$.

Назовем точки x_i в таком представлении крайними точками функции $f(x)$.

Ясно, что концы отрезка $[a, b]$, на котором рассматривается функция, будут всегда ее крайними точками. Отметим также, что если рассматривать график выпуклой функции, то точки плоскости

$$(a, f(a)), (a + 1, f(a + 1)), \dots, (b, f(b))$$

будут граничными точками их выпуклой оболочки, являющейся выпуклым многоугольником, а точки

$$(x_0, f(x_0)), (x_1, f(x_1)), \dots, (x_m, f(x_m))$$

будут его вершинами, откуда свойство 1 также очевидно.

Нам понадобится также следующая операция над функцией дискретного аргумента, аналогичная операции выпуклой оболочки, поэтому также назовем ее выпуклой оболочкой.

Определение 2 Наибольшую из выпуклых функций, не превышающих заданную на отрезке $[a, b]$ функцию $f(x)$ назовем ее выпуклой оболочкой и будем обозначать $f^{co}(x)$.

Отметим без доказательства следующие свойства этой операции.

Свойство 5 В крайних точках функция совпадает со своей выпуклой оболочкой, т.е. $f(x) = f^{co}(x)$, если x – крайняя точка f^{co} .

Свойство 6 Выпуклая оболочка функции на отрезке $[a, b]$ может быть вычислена за время $O(b - a)$.

Свойство 6 следует из хорошо известного алгоритма построения выпуклой оболочки простого многоугольника линейной временной сложности $O(n)$, где n – число точек в описании многоугольника [3,4]. Дело в том, что график функции представляет собой простой многоугольник, т.е. многоугольник без самопересечений.

Отметим также, что если имеется некоторая априорная информация о множестве крайних точек выпуклой оболочки, то эти оценки можно скорректировать следующим образом. Именно, пусть известно, что множество крайних точек выпуклой оболочки функции на интервале $[a, b]$ содержится в некотором подмножестве $V \subset [a, b]$, $V = \{a = v_1 < v_2 < \dots < v_{|V|} = b\}$. Тогда выпуклую оболочку можно вычислить за время $O(|V|)$ при помощи того же алгоритма [3,4]. В применении к нашему частному случаю, основная идея этого алгоритма заключается в динамически изменяющемся описании выпуклой оболочки по мере поступления каждой следующей точки v_i .

Опишем пошагово алгоритм для нашего случая. Заметим, что вектор $(y_1, \dots, y_j)$ хранит точки, являющиеся крайними для функции f на отрезке $[v_1, v_i]$.

Алгоритм Выпуклая Оболочка

Шаг 1 (предварительный). Делаем присваивания:

$$i := 2; y_1 := v_1; y_2 := v_2; j := 2;$$

Шаг 2. $i := i + 1$. Если $i = |V| + 1$, то переход на Шаг 4.

Если

$$\frac{f(v_i) - f(y_j)}{v_i - y_j} > \frac{f(y_j) - f(y_{j-1})}{y_j - y_{j-1}}$$

то делаем присваивания

$$j := j + 1; y_j := v_i;$$

и возвращаемся к началу Шага 2, иначе переходим к Шагу 3.

Шаг 3. $j := j - 1$.

Если

$$\frac{f(v_i) - f(y_j)}{v_i - y_j} > \frac{f(y_j) - f(y_{j-1})}{y_j - y_{j-1}},$$

то переходим к началу Шага 2, иначе возвращаемся к началу Шага 3.

Шаг 4. Вектор $(y_1, y_2, \dots, y_j)$ представляет собой список крайних точек функции f .

Линейность данного алгоритма обосновывается тем, что точка v_i на втором шаге включается в список крайних точек, а на шаге 3 исключается из этого списка, причем для любой точки эти события могут произойти лишь однажды.

Теперь мы готовы к дальнейшему исследованию задачи о кратчайшем пути. Предположим, что обе функции $f(x)$, $g(y)$ являются линейными функциями. Тогда структура оптимального пути проста и дается следующей леммой [1].

Лемма 1 Пусть $f(x) = \alpha_1 + \beta_1 x$, $g(y) = \alpha_2 + \beta_2 y$. Если $\beta_1 \leq \beta_2$, то маршрут $(0,0) \rightarrow (M,0) \rightarrow (M,N)$ будет кратчайшим. Иными словами, существует кратчайший путь, посещающий узел $(M,0)$.

Доказательство. Эта лемма доказана в [1]. Тем не менее, дадим для полноты доказательство индукцией по числу ребер в кратчайшем пути. Рассмотрим некоторый кратчайший путь. Пусть он впервые пересечет линию $(1,y)$ в некоторой точке $(1,y_0)$. Тогда его структура на этом начальном участке такова: $(0,0) \rightarrow (0,y_0) \rightarrow (1,y_0)$. Длина этого участка равна $f(0)y_0 + g(y_0) = \alpha_1 y_0 + \alpha_2 + \beta_2 y_0$. Длина же маршрута $(0,0) \rightarrow (1,0) \rightarrow (1,y_0)$ равна $g(0) + f(1)y_0 = \alpha_2 + y_0(\alpha_1 + \beta_1)$. Легко подсчитать, что этот маршрут не длиннее первого. Поэтому можно изменить кратчайший путь так, чтобы он посетил узел $(1,0)$. Но теперь в силе индукция. Лемма доказана.

Ясно, что если в условиях леммы $3\beta_2 < \beta_1$, то существует оптимальный маршрут, посещающий узел $(0,N)$.

Доказанная лемма позволяет определить структуру и длину кратчайшего пути для выпуклых функций $f(x)$, $g(y)$, поскольку они кусочно-линейны.

Для этого представим эти функции в виде (5):

$$f(x) = \begin{cases} \alpha_1^f + \beta_1^f x, & x \in [x_0, x_1] \\ \alpha_2^f + \beta_2^f x, & x \in [x_1, x_2] \\ \dots\dots\dots \\ \alpha_m^f + \beta_m^f x, & x \in [x_{m-1}, x_m] \end{cases}$$

$$g(y) = \begin{cases} \alpha_1^g + \beta_1^g y, & y \in [y_0, y_1] \\ \alpha_2^g + \beta_2^g y, & y \in [y_1, y_2] \\ \dots\dots\dots \\ \alpha_n^g + \beta_n^g y, & y \in [y_{n-1}, y_n] \end{cases}$$

На первом отрезке $x \in [x_0, x_1]$ $f(x) = \alpha_1^f + \beta_1^f x$ и соответственно, на отрезке $y \in [y_0, y_1]$ $g(y) = \alpha_1^g + \beta_1^g y$. Справедлива

Лемма 2 Если $\beta_1^f \geq \beta_1^g$, то существует кратчайший путь из (x_0, y_0) в (M, N) , проходящий через узел (x_0, y_1) . Аналогично, если $\beta_1^f \leq \beta_1^g$, то существует кратчайший путь из (x_0, y_0) в (M, N) , проходящий через узел (x_1, y_0) .

Доказательство. Пусть $\beta_1^f \geq \beta_1^g$. Рассмотрим некоторый оптимальный путь из (x_0, y_0) в (M, N) . Пусть он впервые пересечет линию (x, y_1) в точке (x', y_1) . Применим лемму 1 для задачи о кратчайшем пути из (x_0, y_0) в (x', y_1) для линейных соответственно на отрезках $[x_0, x']$, $[y_0, y_1]$ функций $f'(x) = \alpha_1^f + \beta_1^f x$, $g'(y) = \alpha_1^g + \beta_1^g y$. Для таких функций существует оптимальный маршрут $(x_0, y_0) \rightarrow (x_0, y_1) \rightarrow (x', y_1)$, посещающий узел (x_0, y_1) . Его длина равна $f(x_0)(y_1 - y_0) + (x' - x_0)g(y_1)$. Но такова же длина этого маршрута и для исходных функций $f(x)$, $g(y)$. В силу же условий выпуклости имеем $f'(x) \rightarrow f(x)$. Ясно также, что на отрезке $[y_0, y_1]$ имеем $g'(y) = g(y)$. Поэтому существует кратчайший путь из (x_0, y_0) в (M, N) , проходящий через узел (x_0, y_1) . Лемма доказана.

Доказанная лемма редуцирует задачу поиска кратчайшего пути из (x_0, y_0) в (M, N) в случае $\beta_1^f \geq \beta_1^g$ к поиску кратчайшего пути из (x_0, y_1) в (M, N) , а в случае $\beta_1^f \leq \beta_1^g$ к поиску кратчайшего пути из (x_1, y_0) в (M, N) . При этом суммарное количество линейных кусков функций f, g уменьшается на единицу.

Таким образом, из леммы 2 следует следующий алгоритм синтеза кратчайшего пути для выпуклых f, g .

Алгоритм А.

Шаг 1. Объединяем совокупность коэффициентов $\{\beta_i^f, \beta_j^g\}$ в одну упорядоченную последовательность $\beta_1 \leq \beta_2 \leq \dots \leq \beta_{m+n}$. Делаем присваивания: $i := 1$; $k := 1$; $l := 1$; $X := x_0$; $Y := y_0$; $F := 0$.

Шаг 2. Если $\beta_i = \beta_k^f$, то двигаемся из узла (X, Y) в узел $(X + (x_k - x_{k-1}), Y)$, т.е. делаем присваивания:

$$X := X + (x_k - x_{k-1}); F := F + (x_k - x_{k-1}) * g(Y); i := i + 1; k := k + 1.$$

Если же $\beta_i = \beta_l^g$, то двигаемся из узла (X, Y) в узел $(X, Y + (y_l - y_{l-1}))$, т.е. делаем присваивания:

$$Y := Y + (y_l - y_{l-1}); F := F + (y_l - y_{l-1}) * f(X); i := i + 1; l := l + 1.$$

Шаг 3. Если $i \leq m + n$, то возвращаемся к началу Шага 2. Иначе F равно длине кратчайшего пути.

Легко видеть, что основной Шаг 2 соответствует лемме 2. Теперь заметим, что движение в оптимальном маршруте проходит по крайним точкам выпуклых функций f, g . Это замечание позволяет использовать уже для произвольных функций f, g их выпуклые оболочки f^{co}, g^{co} . Алгоритм А строит для пары функций f^{co}, g^{co} кратчайший путь,двигающийся по их крайним точкам. Но в крайних точках эти функции как раз совпадают с исходными и кроме того, они не больше исходных. Поэтому длина этого маршрута для функций f, g будет совпадать с его длиной для функций f^{co}, g^{co} в силу свойства 2 и этот маршрут будет кратчайшим и для пары f, g .

Таким образом, следующий алгоритм решает задачу поиска кратчайшего пути.

Алгоритм В.

Шаг 1. Строим выпуклые оболочки f^{co}, g^{co} функций f, g .

Шаг 2. Алгоритмом А строим кратчайший путь для функций f^{co}, g^{co} .

Полученный путь является кратчайшим и для функций f, g .

Временная сложность Шага 1 в силу [1,2] оценивается сверху величиной $O(M + N)$. Временная сложность Шага 2, как легко видеть, равна $O(M + N)$. Таким образом, установлена следующая теорема

Теорема 1 Для задачи о кратчайшем пути (1) существует алгоритм с временной сложностью $O(M + N)$.

Более того, пусть априори известно, что множества крайних точек выпуклых оболочек функций f, g принадлежат соответственно множествам $H = \{h_1 < h_2 < \dots < h_{|H|}\}$, $V = \{v_1 < v_2 < \dots < v_{|V|}\}$, не обязательно совпадая с ними. Легко видеть, что это обстоятельство позволяет соответственно уменьшить время выполнения обоих шагов Алгоритма В. То есть справедлива.

Теорема 2 Для задачи о кратчайшем пути (1) с априорной информацией о множестве крайних точек выпуклых оболочек функций f, g существует алгоритм с временной сложностью $O(|H| + |V|)$.

Литература

- 1 Tarnowski A.G. Advanced polynomial time algorithm for guillotine generalized pallet loading problem // Decision Making Under Conditions of Uncertainty (Cutting-Packing Problems).-Ufa, 1997.-P. 93 -124.
- 2 Рокафеллар Р. Выпуклый анализ. - М.: Мир, 1973. - 469 с.
- 3 Graham R.L., Yao F. Finding the Convex Hull of a Simple Polygon // Journal of Algorithms. - 1983.- Vol 4.- P. 324-331.
- 4 Graham R.L., Yao F. Finding the Convex Hull of a Simple Polygon.- TR-81-887.- 1981 // <http://cs-tr.cs.cornell.edu:80/Dienst/VI/1.0/Display/stanford.cs/CS-TR-81-887>

ВОССТАНОВЛЕНИЕ КОЭФФИЦИЕНТОВ ФУРЬЕ-УОЛША

Баев А.Ж.¹, Нурсултанов Е.Д.², Тлеуханова Н.Т.³
 e-mail: ^[1]bayev.alen@yandex.kz, ^[2]er-nurs@yandex.ru

^[1,2] *Казахстанский филиал МГУ имени М.В.Ломоносова,*
^[3] *Евразийский национальный университет имени Л.Н.Гумилева*

Аннотация. В работе рассматривается задача восстановления коэффициентов Фурье-Уолша функции двух переменных по её значениям в заданных точках. Построен функционал восстановления коэффициентов Фурье-Уолша для класса $UW_2^\alpha[0,1]^2$.

Пусть $\alpha > 0, 1 \leq r < \infty$ и функция $f(x_1, x_2)$ – измеримая 1-периодическая функция с рядом Фурье-Уолша $\sum_{i_1=1}^{\infty} \sum_{i_2=1}^{\infty} a_{i_1 i_2} \varphi_{i_1}(x_1) \varphi_{i_2}(x_2)$. Будем говорить, что f принадлежит пространству $UW_r^\alpha[0,1]^2$, если существует функция $f^\alpha \in L_r[0,1]^2$ с рядом Фурье-Уолша:

$$\sum_{k_1=0}^{\infty} \sum_{k_2=0}^{\infty} \bar{k}_1^\alpha \bar{k}_2^\alpha a_{k_1 k_2} \varphi_{k_1}(x_1) \varphi_{k_2}(x_2),$$

где $\bar{k}_i = \max(k_i, 1)$. Норма в пространстве $UW_r^\alpha[0,1]^2$ задается следующим равенством $\|f\|_{UW_r^\alpha} = \|f^\alpha\|_{L_r}$.

Пусть $m \in \mathbb{N}$. Гиперболическим крестом порядка m назовем множество

$$G_m = \bigcup_{p_1+p_2 \leq m} \{(v_1, v_2) | v_1, v_2 \in \mathbb{Z}_+, [2^{p_i-1}] \leq v_i < 2^{p_i}, i = 1, 2\}.$$

Пусть $m \in \mathbb{N}$, $(v_1, v_2) \in G_m$ и $[2^{p_i-1}] \leq v_i < 2^{p_i}$, $i = 1, 2$. Определим функционал:

$$A_{v_1, v_2}(f) = \frac{1}{2^m} \sum_{k=p_1}^{m-p_2} (-1)^{\text{sign}(k-p_1)} \sum_{j_1=0}^{2^{k-1}-1} \sum_{j_2=0}^{2^{m-k-1}-1} f\left(\frac{j_1}{2^k}, \frac{j_2}{2^{m-k}}\right) \times \\ \times \varphi_{v_1+2^{k-1}\text{sign}(k-p_1)}\left(\frac{j_1}{2^k}\right) \varphi_{v_2}\left(\frac{j_2}{2^{m-k}}\right) \quad (1)$$

Теорема 1. Пусть $m \in \mathbb{N}$ и $(v_1, v_2) \in G_m$. Для многочлена Уолша вида

$$T_m(x_1, x_2) = \sum_{(i_1, i_2) \in G_m} a_{i_1 i_2} \varphi_{i_1}(x_1) \varphi_{i_2}(x_2)$$

верно равенство $A_{v_1 v_2}(T_m) = a_{v_1 v_2}$.

Таким образом функционал, определенный равенством (1) точно восстанавливает коэффициенты полином Уолша со спектром из соответствующего гиперболического креста. Заметим, что количество использованных узлов в определении функционала (1) совпадает с мощностью соответствующего гиперболического креста G_m .

Теорема 2. Пусть $\alpha > \frac{1}{2}$, $m \in \mathbb{Z}_+$ и $(v_1, v_2) \in G_m$. Функция $f(x_1, x_2) \in UW_2^\alpha[0,1]^2$ имеет ряд Фурье-Уолша $\sum_{i_1=1}^{\infty} \sum_{i_2=1}^{\infty} a_{i_1 i_2} \varphi_{i_1}(x_1) \varphi_{i_2}(x_2)$. Тогда имеет место оценка

$$|A_{v_1 v_2}(f) - a_{v_1 v_2}| \leq \frac{C}{2^{\alpha m}} \|f\|_{UW_2^\alpha},$$

где C не зависит от f и m .

Отметим, что подобная задача для восстановления тригонометрических коэффициентов Фурье рассмотрена в работах [1], [2].

Работа выполнена при финансовой поддержке комитета науки РК, грант 3311 / ГФ4.

Литература

1. Нурсултанов Е.Д., Тлеуханова Н.Т. Квадратурные формулы для классов функций малой гладкости / Нурсултанов Е.Д., Тлеуханова Н.Т. – Математический сборник. 2003. – Т.194, №10. – С. 133-160.
2. Нурсултанов Е.Д., Тлеуханова Н.Т. О восстановлении мультипликативных преобразований функций из анизотропных пространств / Нурсултанов Е.Д., Тлеуханова Н.Т. – Сиб. матем. журн., 2014. – Т.55, №3. – С. 592-609.

АЛГОРИТМ ФОРМИРОВАНИЯ ПОЛНЫХ КЛЮЧЕЙ ДЛЯ СИСТЕМЫ ШИФРОВАНИЯ НА БАЗЕ НЕПОЗИЦИОННЫХ ПОЛИНОМИАЛЬНЫХ СИСТЕМ СЧИСЛЕНИЯ

Бияшев Р.Г., Варенников А.В., Нысанбаева С.Е.

e-mail: brg@ipic.kz, avarennikov@gmail.com, snyssanbayeva@gmail.com

Институт информационных и вычислительных технологий КН МОН РК,
Казахстан

Аннотация. Предлагается алгоритм формирования ключей шифрования для системы криптографической защиты информации (СКЗИ) на базе непозиционных полиномиальных систем счисления (НПСС), предназначенной для использования в системах и сетях передачи и хранения информации.

Введение

Создаваемая система криптографической защиты информации является программной реализацией нетрадиционного криптографического алгоритма, разработанного на основе непозиционной полиномиальной системы счисления с двоичными коэффициентами, суть которого заключается в следующем [1].

Исходное открытое сообщение представляется в виде последовательности блоков заданной длины N (в битах). Каждый блок интерпретируется как последовательность остатков $\alpha_1(x), \alpha_2(x), \dots, \alpha_S(x)$ от деления некоторого многочлена $F(x)$ степени не выше N с двоичными коэффициентами на неприводимые многочлены (рабочие основания) $p_1(x), p_2(x), \dots, p_S(x)$:

$$F(x) = (\alpha_1(x), \alpha_2(x), \dots, \alpha_S(x)), \quad (1)$$

где $F(x) \equiv \alpha_i(x) \pmod{p_i(x)}$, $i = \overline{1, S}$, S – число выбранных рабочих оснований. В соответствии с китайской теоремой об остатках представление (1) является единственным при условии, что все основания НПСС $p_i(x)$ будут различными.

Рабочие основания выбираются из числа всех неприводимых полиномов с двоичными коэффициентами степени от m_1 до m_S , $1 \leq m_i \leq N$, из условия выполнения уравнения:

$$k_1 m_1 + k_2 m_2 + \dots + k_S m_S = N, \quad (2)$$

Здесь k_i – количество выбранных полиномов степени m_i , $0 \leq k_i \leq n_i$, n_i – общее количество всех неприводимых многочленов степени m_i , S – количество различных степеней выбранных полиномов.

Для получения криптограммы требуется выполнить наложение секретного ключа (или псевдослучайной последовательности - ПСП) $G(x)$ на каждый блок исходного сообщения $F(x)$. ПСП также интерпретируется как последовательность остатков от деления некоторого многочлена $G(x)$ степени не выше N на соответствующие рабочие основания:

$$G(x) = (\beta_1(x), \beta_2(x), \dots, \beta_S(x)), \quad G(x) \equiv \beta_i(x) \pmod{p_i(x)}, \quad i = \overline{1, S}.$$

Тогда криптограмма получается в результате выполнения некоторой функции $H(F(x), G(x))$:

$$H(x) = (\omega_1(x), \omega_2(x), \dots, \omega_S(x)), H(x) \equiv \omega_i(x) \pmod{p_i(x)}, i = \overline{1, S}.$$

Применение конкретной функции $H(F(x), G(x))$ задаёт метод шифрования на базе НПСС. В разрабатываемой криптосистеме в качестве функции $H(F(x), G(x))$ используется операция умножения модулю:

$$\alpha_i(x)\beta_i(x) \equiv \omega_i(x) \pmod{p_i(x)}, i = \overline{1, S}. \quad (3)$$

При расшифровании криптограммы $H(x)$ по известному ключу $G(x)$ для каждого значения $\beta_i(x)$ производится вычисление, как следует из (3), обратного (инверсного) многочлена $\beta_i^{-1}(x)$ из условия выполнения следующего сравнения:

$$\beta_i(x)\beta_i^{-1}(x) \equiv 1 \pmod{p_i(x)}, i = \overline{1, S}. \quad (4)$$

В результате получается многочлен

$$G^{-1}(x) = (\beta_1^{-1}(x), \beta_2^{-1}(x), \dots, \beta_S^{-1}(x)),$$

инверсный к многочлену $G(x)$. Тогда элементы последовательности вычетов (1) в соответствии с (3) и (4) восстанавливаются по сравнению:

$$\alpha_i(x) \equiv \beta_i^{-1}(x)\omega_i(x) \pmod{p_i(x)}, i = \overline{1, S}.$$

Таким образом, в рассмотренной модели системы шифрования электронного сообщения заданной длины N бит в НПСС полным ключом является выбранная система полиномиальных рабочих оснований $p_1(x), p_2(x), \dots, p_S(x)$ и секретный ключ $G(x) = (\beta_1(x), \beta_2(x), \dots, \beta_S(x))$.

Как уже упоминалось выше, шифрование осуществляется путём наложения на электронное сообщение сгенерированной ключевой последовательности также длиной N бит. Число таковых битовых последовательностей равно 2^N . Тогда один вариант выбора системы из S оснований для конкретного набора степеней $m_1, m_2, \dots, m_S$ будет задаваться формулой:

$$2^N (k_1 + k_2 + \dots + k_S)! C_{n_1}^{k_1} C_{n_2}^{k_2} \dots C_{n_S}^{k_S}$$

Общее количество ключей длины N рассчитывается по формуле:

$$2^N \times \sum_{k_1, k_2, \dots, k_S} (k_1 + k_2 + \dots + k_S)! C_{n_1}^{k_1} C_{n_2}^{k_2} \dots C_{n_S}^{k_S} \quad (5)$$

в которой суммирование распространено на всевозможные комбинации коэффициентов $k_1, k_2, \dots, k_S$, удовлетворяющих равенству (2) [1].

Для создаваемой СКЗИ были предложены два варианта выбора полного ключа шифрования [2].

Первый вариант предполагает предварительное заполнение базы данных полных ключей. В этом случае в процессе шифрования полный ключ выбирается из этой базы данных случайным образом. Достоинством данного подхода является более высокая скорость выполнения алгоритма шифрования, однако при этом необходимо учитывать количество полных ключей, вычисляемое по формуле (5), которое измеряется величинами порядка 10^{37} (для ключей длиной 64 бита) и выше, что неизбежно приводит к проблеме «больших данных» и не позволяет сохранить в базе данных весь диапазон возможных ключей.

Во втором варианте полный ключ шифрования формируется «на лету», непосредственно в процессе выполнения криптоалгоритма и хранится отдельно от других ключей. Такой подход позволяет обеспечить использование всего диапазона возможных ключей, но при этом возможно уменьшение скорости процедур шифрования. Увеличить скорость можно за счет распараллеливания вычислительных операций по всем основаниям, используемым в реализуемом криптоалгоритме, а также за счет программно-аппаратной реализации.

В данной статье предлагается эффективный алгоритм формирования ключей шифрования для СКЗИ на базе непозиционных полиномиальных систем счисления, который позволяет использовать оба эти варианта. Основная идея заключается в том, чтобы хранить в базе данных не все возможные полные ключи, а только те данные, которых достаточно для их формирования (в соответствии с уравнением (2)). К таким данным относятся:

- I_m – количество неприводимых полиномов над полем $GF(2)$ степени m ;
- b_l – минимальная допустимая степень рабочего основания из набора степеней длины l , сумма которых равна N ;
- e_l – максимальная допустимая степень рабочего основания из набора степеней длины l , сумма которых равна N ;
- q_l – количество всех возможных наборов степеней длины l , сумма которых равна N (без учета перестановок).

В таблице 1 приведено количество неприводимых полиномов над полем $GF(2)$ со степенями от 1 до 32. Формула для вычисления I_m приведена в [4].

Таблица 1. Количество неприводимых полиномов над полем $GF(2)$

m	I_m	m	I_m	m	I_m	m	I_m
1	1	9	56	17	7710	25	1342176
2	1	10	99	18	14532	26	2580795
3	2	11	186	19	27594	27	4971008
4	3	12	335	20	52377	28	9586395
5	6	13	630	21	99858	29	18512790
6	9	14	1161	22	190557	30	35790267
7	18	15	2182	23	364722	31	69273666
8	30	16	4080	24	698870	32	134215680

В таблице 2 приведены значения b_l , e_l и q_l для $N = 32$ и для всех возможных значений l , рассчитанные с использованием метода полного перебора допустимых наборов степеней рабочих оснований, сумма которых равна N (без учета перестановок).

Таблица 2. Расчетные данные для генерации 32-битовых ключей

l	b_l	e_l	q_l
1	32	32	1
2	1	31	16
3	1	29	83
4	1	26	219
5	1	23	329
6	1	19	297
7	1	15	154
8	1	11	37
9	1	6	2

Описание алгоритмов

Алгоритм генерации полного ключа:

Шаг 1. Выбрать длину ключа в битах N (задается в качестве параметра).

Шаг 2. Используя расчетные данные для заданного значения N , получить общее число $Q = \sum q_i$ возможных вариантов наборов степеней рабочих оснований, сумма которых равна N (без учета перестановок).

Шаг 3. Используя генератор случайных чисел, выбрать номер k набора степеней рабочих оснований такой, что $1 \leq k \leq Q$.

Шаг 4. Используя расчетные данные для заданного значения N , получить длину l набора степеней с номером n такую, что $\sum_{i < l} q_i < k \leq \sum_{i \leq l} q_i$

Шаг 5. Используя генератор случайных чисел, выбрать значение степени рабочего основания $b_l \leq m \leq e_l$.

Шаг 6. Если $m > N$ вернуться на шаг 5.

Шаг 7. Если текущее количество полиномов степени m в наборе степеней рабочих оснований D превышает I_m , вернуться на шаг 5.

Шаг 8. Включить m в набор степеней рабочих оснований D .

Шаг 9. Если $m < N$, перейти на шаг 1 с новым значением $N = (N - m)$.

Шаг 10. Для полученного набора степеней D , сгенерировать набор P неприводимых полиномов $p_i(x)$ выбранных степеней m_i , $i = \overline{1, l}$, используемых в качестве рабочих оснований. Алгоритм генерации неприводимых полиномов приведен ниже.

Шаг 11. Для полученного набора степеней D сгенерировать набор K ненулевых ПСП $\beta_i(x)$, $i = \overline{1, l}$ используемых в качестве секретных ключей, длина которых совпадает со степенями рабочих оснований m_i , $i = \overline{1, l}$. Алгоритм генерации ПСП описан в [3].

Шаг 12. Возвратить полный ключ $\langle P, K \rangle$.

Алгоритм генерации неприводимых полиномов:

Шаг 1. Выбрать степень неприводимого полинома N (задается в качестве параметра).

Шаг 2. Используя генератор случайных чисел, выбрать произвольное целое число n такое, что $2^N \leq n < 2^{N+1}$.

Шаг 3. Преобразовать полученное число n в битовую последовательность, представляющую полином $p(x)$ с двоичными коэффициентами.

Шаг 4. Проверить неприводимость полинома $p(x)$ с использованием вероятностного алгоритма Бен-Ора [5].

Шаг 5. Если полином $p(x)$ не является неприводимым, вернуться на шаг 2.

Шаг 6. Возвратить полином $p(x)$.

Приведенные алгоритмы реализованы на языке C++ в рамках проекта целевого финансирования «Разработка и исследование моделей алгоритма шифрования на базе модулярной арифметики» и получены следующие результаты:

Таблица 3. Время генерации 128-битовых ключей

Общее время генерации 100 ключей (в мкс)	281179
Минимальное время генерации одного ключа (в мкс)	684
Максимальное время генерации одного ключа (в мкс)	4392
Среднее время генерации одного ключа (в мкс)	2812
Среднее количество ключей (в сек.)	355

Заключение

Предложенный алгоритм позволяет эффективно решить проблему выбора ключа шифрования для системы криптографической защиты информации на базе непозиционных полиномиальных систем счисления за счёт использования предварительно рассчитанных данных, генератора случайных чисел, генератора ПСП и генератора неприводимых полиномов на основе вероятностного алгоритма Бен-Ора.

Список использованных источников

1. Нысанбаева, С. Е. Разработка и исследование криптографических систем на базе непозиционных полиномиальных систем счисления: Дис. докт. техн. наук. / С. Е. Нысанбаева. – Алматы.: 2009. – 240 с.
2. Бияшев, Р. Г. Разработка систем криптографической защиты с заданными характеристиками. / Р. Г. Бияшев, С. Е. Нысанбаева, Н. А. Капалова. // Проблемы информатики. 2013. №2. – с. 30-36.
3. Капалова, Н. А. Разработка и исследование генерации и распределения ключевых последовательностей: Дис. канд. техн. наук. / Н.А. Капалова. – Алматы.: 2008. – 131 с.
4. Arndt, J. Matters Computational. Ideas, Algorithms, Source Code. / J. Arndt. // Springer-Verlag GmbH, Berlin, 2011. – P. 843
5. Ben-Or, M. Probabilistic algorithms in finite fields. / M. Ben-Or. // In Proc. 22th IEEE Annual Symposium on Foundations of Computer Science, 1981. P. 394-398

ФИЛИАЛДАР ЖЕЛІСІН БАСҚАРУ ҮШІН ҮЛЕСТІРІЛГЕН ДЕРЕКТЕР ҚОРЫНЫҢ МОДЕЛІ МЕН КОРПОРАТИВТІК АҚПАРАТТЫҚ ЖҮЙЕСІ

¹Вальдемар Вуйчик, ²Найзабаева Л.Қ, ³Оразбеков.Ж.Н.

E-mail: ¹Waldemar.wojcik@pollub.pl, ²naizabayeva@mail.ru, ³O.Jas@mail.ru

¹Люблин технологиялық университеті (Польша)

^{2,3}ҚР БжҒМ Ақпараттық және есептеуіш технологиялар институты, Алматы,
Қазақстан

Аңдатпа. Бұл мақалада филиалдың ДҚБЖ бастапқы деректерді жазу, сақтау орнына бірігу деректерін жазу, орталықтан тираждау деректерін жазу, жергілікті басқаруды жазу, қолданушымен сұралатын деректерді оқу, біріктіру үшін деректерді оқу, орталыққа тираждау үшін деректерді оқу және жергілікті басқару үшін деректерді оқу мәселелері, сондай-ақ, үлестірілген деректер қорының моделі және оның жұмыс істеу параметрлерін есептеу секілді бірқатар мәселелер қарастырылған.

Аннотация. В статье рассматривается СУБД филиала выполняет задачи записи исходных данных, записи данных агрегирования в хранилище, записи данных тиражирования из центра, записи локального управления, чтения данных запрашиваемых пользователями, чтения данных для агрегирования, чтения данных для тиражирования в центр и чтения данных для локального управления, а также рассмотрены проектирование распределенной базы данных и расчет параметров ее функционирования.

Abstract. In the article, the branch's DBMS is used to perform the tasks of recording the original data, recording the aggregation data in the store, recording replication data from the center, local management records, reading data requested by users, reading data for aggregation, reading data for replication to the center, and reading data for local management, And also the design of a distributed database and calculation of the parameters of its functioning are considered.

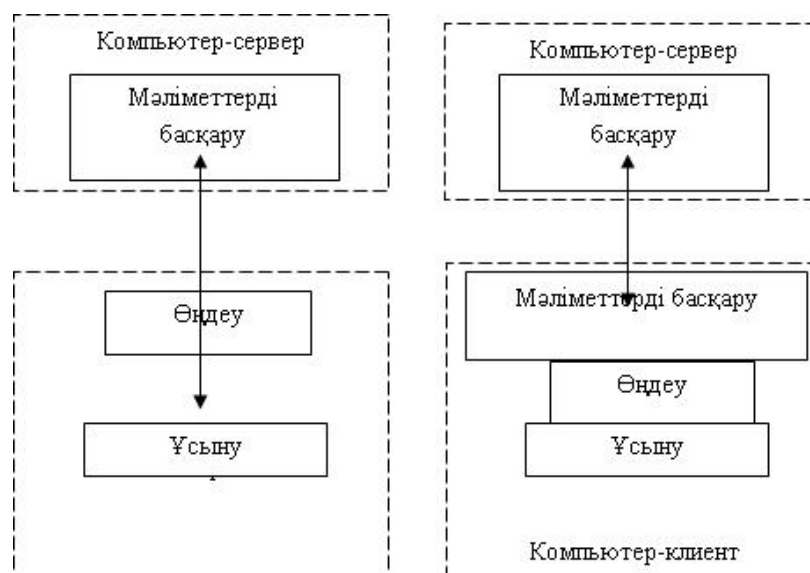
Қазіргі кездегі ұйымдар (мекемелер) көпжақты қызметтің, бөлімшелердің территориялық бөлінуінің, серіктестерімен кооперативтік байланыстардың көп болуына байланысты күрделі құрылымға ие. Корпоративтік деректер қоры (КДҚ) осындай ірі мекемелердің барлық ресурстарын және іскерлік процесстерін басқаруды автоматтандыруға бағытталған. Сонымен қатар басқарушылық процесстерді автоматтандыру ақпаратты өңдеуге кететін шығындарды азайтуға ғана емес, мекеменің жұмыс кезіндегі іскерлік процесстерін және ұйымдық құрылымын динамикалық оптимизациялауға бағытталған.[1]

Екі буындық модельдер ДҚБЖ қызметтерін желінің екі торабының арасында үлестірілуіне сәйкес келеді. Өзіндеміндетті түрде деректерді басқару қызметі болатын компьютерді (желінің торабын) компьютер-сервер деп атайық. Тұтынушыға жақын және ақпараттыкейіптеу мәселелерімен міндетті түрде айналысатын компьютерді компьютер-клиент деп атайық. [2] Компьютер-сервер мен компьютер-клиенттіңарасында қызметтерді үлестірудің аса типтік нұсқалары (1, 2-суреттер) келесілер болып табылады:

- үлестірілген түрдегі ұсыну;
- қашықтан ұсыну;
- үлестірілген қызмет;
- деректерге қашықтан қол жеткізу;
- үлестірілген ДҚ.



Сурет.1 Екі буынды сұлба.



Сурет.2 Екі буынды сұлбалар.

Клиент-сервер құрылымы бар жүйелерде қызметтерін үлестірудің аталған әдістері әр түрлі нұсқаларды көрсетеді: қуатты сервер – бұл жағдайда барлық жұмыс сонда орындалады, қуатты клиент-қызметтердің басым бөлігі жұмыс станциясында орындалады, ал сервер желі арқылы соған келіп түсіп жатқан SQL-шақыртуларды өңдеуден өткізеді.

Деректерге қашықтан қол жеткізу моделінде (Remote Data Access – RDA), ақпаратты ұсыну қызметтері мен қолданбалы өңдеудің логикасын жүзеге асыратын программалар біріктірілген компьютер-клиенте орындалады. Деректерді басқару сервисіне жүгіну ісі операторлардың көмегімен SQL тілінің операторлары арқылы немесе API (Application Programming Interface – қолданбалы программалау интерфейсы) арнайы кітапхананың қызметтерін шақырту арқылы орындалады. [3]

RDA-моделінің негізгі артықшылығы – SQL-интерфейстері бар дайын ДҚБЖ-лардың көптеп болуы және клиенттік бөлік программаларының жылдам түрде құрылуын қамтамасыз ететін аспаптық құралдардың болуы. Жасау құралдары көбінесе MS Windows-те тұтынушының графикалық интерфейсін, ODBC интерфейсінің стандартты мен кодты автоматты түрде генерациялау құралдарын қолдайды. Жасау құралдарының басым көпшілігі төртінші буынның тілдерін пайдаланады.

RDA-моделінің кемшіліктері біріншіден, барлық логика қосымшада шоғырланып, өңдеуден өткізілетін деректер қашықтағы торапта орналасқандықтан деректерді беру жүйесі жоғары дәрежеде жүктемеленгендігі болып табылады. Қосымшалардың жұмыс істеуі кезінде желі арқылы әдетте тұтастай ДҚ-лар беріледі.

Үлестірілген түрде ұсыну моделі кіші, орташа және үлкен ЭЕМ-дарда жұмыс істеген алғашқы буындағы ДҚБЖ-ларға ие болған болатын. X-терминалдар рөлінде дисплейлік станциялар мен абоненттік пунктер (жергілікті және қашықтағы) қызмет етті. Бұл жағдайда ақпаратты ұсыну қызметтерінің негізгі бөлігін ДҚБЖ-лардың өздері орындады, ал тұтынушының терминалдарында бейнелерді соңғы деңгейде құрастыру ісі шеткі құрылғыларда орындалды.[4-5]

Қызметтерді үлестірудің үш буындық моделі қосымшаның үш қызметінің әрқайсысы жекелеген компьютерде орындалатын типтік нұсқа болып табылады. Қосымшалардың қызметтерін компьютерлердің көптеген санына үлестірудің нұсқалары болуы мүмкін, алайда олар сирек қолданылатын болғандықтан, қарастырылмайды.

Біз қарастырып отырған модель қосымшалар сервері немесе AS-модель(Application Server) деп аталады және 3-суретте көрсетілген.



Сурет.3 Үшбуынды сұлба

Ақырғы тұтынушымен сұхбат жүргізуге жауап беретін үш буындық AS-моделге сәйкес, аталған процесс, әдетте, ақпаратты ұсыну қызметтерін орындайды және қосымшаның компонентімен DBS моделіндегіге ұқсас түрде әрекеттеседі. Қосымшаның компоненті жеке компьютерде орналасып өз кезегінде RDA моделіне ұқсас түрде деректерді басқару компонентімен байланысты болады.

AS-моделінің орталық буыны қосымшалар сервері болып табылады. Қосымшалар серверінде бірнеше қолданбалы қызметтер орындалады, олардың әрқайсысы оны қажет ететін программалардың барлығына қызмет көрсету қызметі ретінде рәсімделген. Қосымшалар серверлерінің бірнешеуі болуы мүмкін, олардың әрқайсысы өз қызметін ұсынады. Қосымшалар серверінен қызмет көрсетуін сұраған кез келген программа ол үшін клиент болып табылады. Клиенттерден серверлерге келіп түскен сұраныстар

кезекке тұрады, олар ол жерден қандай да бір пәнге байланысты, мысалы, басымдылықтары бойынша іріктеліп алынады. [6-7]

AS-модельдің артықшылығы – қосымшаның қызметтері өзара тәуелсіз үш бөлікке бөлінгендіктен, оның икемділігі мен әмбебаптығы болып табылады. Көптеген жағдайларда бұл модель екі буындық модельмен салыстырғанда тиімдірек болады. Модельдің негізгі кемшілігі – қосымшаның компоненттерінің арасында ақпаратпен алмасуға жұмсалатын компьютердің ресурстары екі буындық модельмен салыстырғанда көбірек жұмсалатындығы.[8]

Филиалдар желісін басқарудың желі КАЖ ҮДҚ-ның жұмыс істеуінің тиімді параметрлерін таңдау. Филиалдардың *N бір тунні* жергілікті деректер қоры және басқару орталығының бір жергілікті деректер қоры бар. Филиалдар мен орталық ADSL (Asymmetric Digital Subscriber Line — Асимметриялық санды абоненттік желі) арқылы байланысқан. Орталық анықтамасының филиалдарға тираждалуы, шын мәнінде жаһандық басқаруды жіберу. Жаһандық басқарудан басқа филиалдың жергілікті өзін-өзі басқаруы жүзеге асады.[9] Филиалдар бір-бірімен байланыспайтын жағдайды қарастырамыз.

Белгілеулер енгіземіз:

$T\Phi$ – Филиалдың жедел деректер қорының бірігу периоды

$T\Omega$ – Филиалдың сақталу орнының тираждау периоды

$K_{арг}^{\Phi}$ – Филиалдың деректер қорының бірігу коэффициенті

$V\Phi$ – Филиалдың деректер қорының бастапқы деректерінің ағынының қуаты

$v\Pi$ – Филиал қолданушыларының деректер сұранысының ағынының қуаты

$q\Pi$ – Қолданушылардың сұранысының саны

N – Филиалдар саны

$V\Omega$ – Орталық анықтамасының көлемі (жаһандық басқарудың)

T_y^{Φ} – Жергілікті басқару периоды

T_y^{Ω} – Орталықтан тираждау периоды (жаһандық басқарудың)

$T_{иу}^{\Phi}$ – Жергілікті басқаруды есептеу үшін деректердің өңделетін көлемі

V_y^{Φ} – Жергілікті басқаруды есептеп болғаннан кейінгі деректердің түзелтілетін көлемі

$S_{бд}^{\Phi}$ – Филиалдың ДҚБЖ-нің деректер бірлігін өңдеу уақыты

sn – Қолданушының жұмыс станциясының орталық процессорының деректер бірлігін өңдеу уақыты

z – Үлестірілген есептеулер параметрі

$K_{сп}^{\Phi}$ – Қосымшаның серверінен сұраныс жасаған кездегі деректердің салыстырмалы қысқартылуы

Филиалдың ДҚБЖ бастапқы деректерді жазу, сақтау орнына бірігу деректерін жазу, орталықтан тираждау деректерін жазу, жергілікті басқаруды жазу, қолданушымен сұралатын деректерді оқу, біріктіру үшін деректерді оқу, орталыққа тираждау үшін деректерді оқу және жергілікті басқару үшін деректерді оқу мәселелерін орындайды. Сонымен қатар жазудың бір амалына кфд оқудың бір амалы сәйкес келеді. [11,12]

$$K_{бд}^{\Phi} \left(V^{\Phi} + V^{\Phi} * K_{арг}^{\Phi} + \frac{V^{\Omega}}{T_y^{\Omega} + T^{\Omega} + T^{\Phi}} + \frac{V_y^{\Phi}}{T_y^{\Phi} + T^{\Phi}} \right) + V^{\Pi} + V^{\Phi} + \frac{V^{\Phi} * K_{арг}^{\Phi}}{T^{\Omega} + T^{\Phi}} + \frac{V_{иу}^{\Phi}}{T_y^{\Phi} + T^{\Phi}} < \frac{1}{S_{бд}^{\Phi}}$$

Филиалдың жергілікті желісі тікелей сұраныстар нәтижелері мен қосымша сервері арқылы жасалған сұраныс нәтижелерін жіберу мәселелерін орындайды.

$$z * V^{\Pi} + (1 - z) * K_{\text{сн}}^{\Phi} * V^{\Pi} < \frac{1}{S_{\text{сет}}^{\Phi}}$$

Жаһандық желі тираждау деректерін филиалдан орталыққа және орталықтан филиалға жіберу мәселесін орындайды. Сонымен қатар **kADSL** –дағы кіру жылдамдығы шығу жылдамдығынан үлкен.

$$N * K^{\text{ADSL}} * \frac{V^{\Pi}}{T_y^{\Pi} + T^{\Pi} + T^{\Phi}} + N * \frac{V^{\Phi} * K_{\text{арп}}^{\Phi}}{T^{\Pi} + T^{\Phi}} < \frac{1}{S_{\text{сет}}^{\text{ADSL}}}$$

$$K^{\text{ADSL}} * \frac{V^{\Phi} * K_{\text{арп}}^{\Phi}}{T^{\Pi} + T^{\Phi}} + \frac{V^{\Pi}}{T_y^{\Pi} + T^{\Pi} + T^{\Phi}} < \frac{1}{S_{\text{сет}}^{\text{ADSL}}}$$

Қолданушының жұмыс станциясының орталық процессоры(ОП) тікелей сұраныстарды өндеуді орындайды.

$$z * V^{\Pi} < \frac{1}{S^{\Pi}}$$

Филиал серверінің ОП-ы ДҚБЖ-нің жұмысын қамтамасыз етумен қатар, біріктіруді есептеу, жергілікті басқаруды есептеу және қосымша сервері арқылы сұраныс деректерін өндеу мәселелерін орындайды.

$$\begin{aligned} g_{\text{бд}}^{\Phi} * \left(K_{\text{бд}}^{\Phi} * \left(V^{\Phi} + V^{\Phi} * K_{\text{арп}}^{\Phi} + \frac{V^{\Pi}}{T_y^{\Pi} + T^{\Pi} + T^{\Phi}} + \frac{V_y^{\Phi}}{T_y^{\Phi} + T^{\Phi}} \right) + V^{\Pi} + V^{\Phi} + \frac{V^{\Phi} * K_{\text{арп}}^{\Phi}}{T^{\Pi} + T^{\Phi}} + \frac{V_{\text{йу}}^{\Phi}}{T_y^{\Phi} + T^{\Phi}} \right) \\ + g_{\text{арп}}^{\Phi} * V^{\Phi} + \frac{G_{\text{арп}}^{\Phi}}{T^{\Phi}} + \frac{G_y^{\Phi}}{T_y^{\Phi} + T^{\Phi}} + g_{\text{сн}}^{\Phi} * (1 - z) * V^{\Pi} < \frac{1}{S_{\text{обп}}^{\Phi}} \end{aligned}$$

Қолданушы сұранысын өндеудің орташа уақыты:

$$t_{\text{ср}}^{\Pi} = \frac{T}{q^{\Pi}} * \left[S_{\text{бд}}^{\Phi} * \left(K_{\text{бд}}^{\Phi} * \left(V^{\Phi} + V^{\Phi} * K_{\text{арп}}^{\Phi} + \frac{V^{\Pi}}{T_y^{\Pi} + T^{\Pi} + T^{\Phi}} + \frac{V_y^{\Phi}}{T_y^{\Phi} + T^{\Phi}} \right) + \right. \right. \\ \left. \left. + V^{\Pi} + V^{\Phi} + \frac{V^{\Phi} * K_{\text{арп}}^{\Phi}}{T^{\Pi} + T^{\Phi}} + \frac{V_{\text{йу}}^{\Phi}}{T_y^{\Phi} + T^{\Phi}} \right) + \right. \\ \left. + S^{\Pi} * z * V^{\Pi} + S_{\text{арп}}^{\Phi} * V^{\Phi} + \frac{S_{\text{арп}}^{\Phi}}{T^{\Phi}} + \frac{S_y^{\Phi}}{T_y^{\Phi} + T^{\Phi}} + S_{\text{сн}}^{\Phi} * (1 - z) * V^{\Pi} + \right. \\ \left. + S_{\text{сет}}^{\Phi} * (z * V^{\Pi} + (1 - z) * K_{\text{сн}}^{\Phi} * V^{\Pi}) \right]$$

Жаһандық желі трафикін асыра қолдануға айыппұл:

$$C^{\text{ADSL}} = \begin{cases} 0, V^{\text{ADSL}} * T < V_{\text{абон}}^{\text{ADSL}} \\ C^{\text{ADSL}} * (V^{\text{ADSL}} * T - V_{\text{абон}}^{\text{ADSL}}) \end{cases}, \text{ қайда } V^{\text{ADSL}} = N * \left(\frac{V^{\Pi}}{T_y^{\Pi} + T^{\Pi} + T^{\Phi}} + \frac{V^{\Phi} * K_{\text{арп}}^{\Phi}}{T^{\Pi} + T^{\Phi}} \right)$$

Жергілікті басқаруды кешіктіруге айыппұл

$$C_{\text{упр}}^{\Phi} = \begin{cases} 0, & T_y^{\Phi} + T^{\Phi} < T_{\text{упр}}^{\Phi} \\ C_{\text{упр}}^{\Phi} * T * \left(1 - \frac{T_{\text{упр}}^{\Phi}}{T_y^{\Phi} + T^{\Phi}}\right) \end{cases}$$

Жергілікті басқаруды кешіктіруге айыппұл:

$$C_{\text{упр}}^{\Pi} = \begin{cases} 0, & T_y^{\Pi} + T^{\Pi} + T^{\Phi} < T_{\text{упр}}^{\Pi} \\ C_{\text{ср}}^{\Pi} * T * \left(1 - \frac{T_{\text{упр}}^{\Pi}}{T_y^{\Pi} + T^{\Pi} + T^{\Phi}}\right) \end{cases}$$

Қолданушы сұранысын өңдеуді кешіктіруге айыппұл:

$$C_{\text{ср}}^{\Pi} = \begin{cases} 0, & t_{\text{ср}}^{\Pi} < T_{\text{ср}}^{\Pi} \\ C_{\text{ср}}^{\Pi} * (t_{\text{ср}}^{\Pi} - T_{\text{ср}}^{\Pi}) \end{cases}$$

Жұмыс істеу параметрлері $(T^{\Phi}, T^{\Pi}, T_y^{\Pi}, T_y^{\Phi}, z)$ айыппұл қосындысы минималды болатындай етіп таңдалуы керек.

$$C^{\text{ADSL}} + C_{\text{упр}}^{\Phi} + C_{\text{упр}}^{\Pi} + C_{\text{ср}}^{\Pi} \xrightarrow{(T^{\Phi}, T^{\Pi}, T_y^{\Pi}, T_y^{\Phi}, z)} \min$$

$$\begin{aligned} 1 &< T^{\Phi} < T \\ 1 &< T_y^{\Phi} + T^{\Phi} < T \\ 1 &< T^{\Pi} + 1 < T^{\Phi} < T \\ 1 &< T_y^{\Pi} + T^{\Pi} + T^{\Phi} < T \\ 0 &< z < 1 \end{aligned}$$

Алынған есеп сызықты шектеулері бар сызықты емес бағдарламалау есебін береді. Сандық шешімі заманауи бағдарламалық пакеттердің көмегімен табылуы мүмкін.

Қорытынды: Сонымен бұл жұмыста үлестірілген деректер қорының моделі және оның жұмыс істеу параметрлерін есептеу секілді бірқатар мәселелері, сондай-ақ, үш деңгейлі архитектураны пайдаланып үлестірілген есептеулер әдісі мен филиалдар желісін басқарудың корпоративтік ақпараттық жүйесі үшін үлестірілген деректер қоры құрылымын қолданудың қажеттілігі көрсетілген.

Әдебиеттер

1. Бугаев А.С., Петров М.В., Рекалов Д.В., Хельвас А.В., Шабунин В.М. Методы классификации объектов при создании информационных систем. М.: Открытые системы. Автоматизация проектирования, 1999, №2
2. Гари Хансен, Джеймс Хансен Базы данных: Разработка и управление. М.: Бином, 2000
3. Ананьин В.И. Корпоративные стандарты - точка опоры автоматизации. М.: Открытые системы. СУБД, 1997, №5-6
4. Андреев А.М., Березкин Д.В., Кантонистов Ю.А. Выбор СУБД для построения информационных систем корпоративного уровня на основе объектной парадигмы. М.: Открытые системы. СУБД, 1998, №4-5

5. Артемьев В.И. Обзор способов и средств построения информационных приложений. М.: Открытые системы, Системы управления базами данных, 1996, №5
6. Бритов П.А., Липчинский Е.А. Практика построения хранилищ данных: система SAS. М.: Открытые системы. СУБД. 1998, №4-5
7. Васильев Г.П. Программное обеспечение неоднородных распределенных систем. Анализ и реализация. М.: Финансы и статистика, 1986
8. Волков И., Галахов И. Архитектура современной информационной системы. М.: Открытые системы. Директор ИС, 2002, №3
9. Топорец А.Ю. Расчет оптимальных параметров функционирования РаБД КИС управления сетью филиалов. М.: СТАНКИН, 2003

МЕТОДЫ ЛОКАЛЬНОЙ МНОГОКРИТЕРИАЛЬНОЙ ОПТИМИЗАЦИИ

Калимолдаев М.Н., Голиков А.И., Евтушенко Ю.Г., Посыпкин М.А.,
Абдилдаева А.А.
e-mail: mposypkin@gmail.com

*Вычислительный центр им. А.А. Дородницына ФИЦ ИУ РАН
Институт информационных и вычислительных технологий КН МОН РК,
Казахстан*

Аннотация. Рассматривается класс локальных методов решения задач многокритериальной оптимизации, в основе которых лежит движение вдоль направления уменьшения критериев (спуска). Введено понятие множества направлений спуска для задачи локальной многокритериальной оптимизации. Сформулирована математическая задача, решением которой являются векторы этого множества. Разработаны возможные подходы к решению этой задачи.

Задача многокритериальной оптимизации условно записывается в виде:

$$\min_{x \in X} F(x), \quad (1)$$

где X – допустимое множество параметров, а вектор-функция $F: R^n \rightarrow R$ определяет векторный критерий, компоненты которого $f_1, \dots, f_m$ составляют набор из m скалярных критериев. Образ $Y = F(X)$ допустимого множества X при отображении F назовем множеством достижимых критериальных векторов. Всюду далее вектор-функция F предполагается непрерывной, а множество X – непустым компактом. При сделанных предположениях множество Y также будет непустым компактом.

Для произвольной точки $z \in R^m$ определим юго-западное $SW(z)$ и северо-восточное $NE(z)$ множества следующим образом:

$$SW(z) = \{x \in R^m : x \leq z\}, \quad NE(z) = \{x \in R^m : x \geq z\}.$$

Здесь и далее запись $x \leq z$ означает одновременное выполнение m неравенств $x_i \leq z_i, i = 1, \dots, m$

Для произвольного множества $\Omega \subseteq R^n$ определим $SW(\Omega) = \bigcup_{\omega \in \Omega} SW(\omega)$,
 $NE(\Omega) = \bigcup_{\omega \in \Omega} NE(\omega)$ и его множество Парето следующим образом:

$$P(\Omega) = \{\omega \in \Omega : SW(\omega) \cap \Omega = \omega\}.$$

Если в качестве Ω взять множество достижимых критериальных векторов Y , то данное определение совпадает со стандартным определением множества Парето, принятым в работах по многокритериальной оптимизации [1-3].

Решение задачи (1) состоит в нахождении множества $P(Y)$ и его прообраза при отображении F . Точку $x \in X$ такую, что $F(x) \in Y$ будем называть *точкой Парето*.

Далее рассмотрим случай, когда допустимое множество задано неравенствами:

$$X = \{g_i(x) \leq 0, i \in \overline{1, k}\}. \quad (2)$$

Будем считать, что ограничения $g_i(x), i \in \overline{1, k}$ и критерии $f_i(x), i \in \overline{1, m}$ являются непрерывными и дифференцируемыми функциями.

Понятие локального минимума и свойства локальной оптимальности

Точка $x \in X$ называется *локальной точкой Парето*, если существует такая окрестность $B_\varepsilon(x)$, $\varepsilon > 0$ этой точки, что $F(x) \in P(F(B_\varepsilon(x) \cap X))$.

Множество $J = \{j \in \overline{1, k} : g_j(x) = 0\}$ называется *множеством активных ограничений в точке $x \in X$* . Будем считать, что в любой допустимой точке градиенты активных ограничений образуют линейно-независимую систему векторов. Вектор $d \in R^n$ называется допустимым направлением в точке $x \in X$ если $d^T \nabla g_j(x) \leq 0$ для всех $j \in J$ [4].

Следующее утверждение дает необходимое условие того, что точка является локальной точкой Парето.

Утверждение 1. Если точка $x \in X$ является локальной точкой Парето, то не существует такого допустимого в точке $x \in X$ направления $d \in R^n$, что

$$d^T \nabla f_i(x) < 0, i \in \overline{1, m}. \quad (3)$$

Точки, для которых не существует допустимого направления, удовлетворяющего неравенствам (3), будем называть *критическими точками Парето*.

Направлением спуска в точке $x \in X$ будем называть любой вектор $d \in R^n$, $\|d\| = 1$, удовлетворяющий следующей системе неравенств:

$$\begin{aligned} d^T \nabla f_i(x) &< 0, \quad i = 1, \dots, m, \\ d^T \nabla g_j(x) &\leq 0, \quad j \in J, \quad J = \{j \in \overline{1, k} : g_j(x) = 0\}. \end{aligned}$$

Здесь и далее через $\|\cdot\|$ обозначается Евклидова норма. Из утверждения 1 следует, что если направление спуска в точке $x \in X$ существует, то она не является локальной точкой Парето.

Множество всех направлений спуска в точке $x \in X$ обозначим через $D(x)$. Из этого множества наиболее предпочтительными являются направления, максимальное уменьшающие все критерии. Математически данное требование может быть сформулировано в виде следующей многокритериальной оптимизационной задачи:

$$\begin{aligned} d^T \nabla f_i(x) &\rightarrow \min, \quad i = 1, \dots, m, \\ d^T \nabla g_j(x) &\leq 0, \quad j \in J, \quad J = \{j \in \overline{1, k} : g_j(x) = 0\}, \\ \|d\| &= 1. \end{aligned} \tag{4}$$

Заметим, что величина $\frac{\partial f}{\partial d} = d^T \nabla f_i(x)$ является производной функции $f_i(x)$ по направлению d . Поэтому в задаче (4) ищется направление, минимизирующее производные критериев по нему. Множество Парето задачи (4) будем обозначать через $D_p(x)$ и называть множеством *направлений наискорейшего спуска*.

Методы многокритериального спуска состоят в определении направления спуска и движения вдоль него по аналогии с методами градиентного спуска в задачах математического программирования. Принципиальное отличие от градиентного спуска состоит в том, что в качестве направления спуска нельзя выбрать антиградиент одного из критериев, т.к. при этом данное направление может не быть направлением убывания для другого критерия.

Численные методы нахождения направлений спуска

Определение направления спуска сводится к нахождению допустимого решения d следующей системы линейных неравенств:

$$\begin{aligned} d^T \nabla f_i(x) &< 0, \quad i = 1, \dots, m, \\ d^T \nabla g_j(x) &\leq 0, \quad j \in J, \quad J = \{j \in \overline{1, k} : g_j(x) = 0\}. \end{aligned} \tag{5}$$

Задачу (5) можно свести к следующей задаче линейного программирования относительно переменных $u, d_1, \dots, d_n$:

$$\begin{aligned} u &\rightarrow \min, \\ d^T \nabla f_i(x) &\leq u, \quad i = 1, \dots, m, \\ d^T \nabla g_j(x) &\leq 0, \quad j \in J, \quad J = \{j \in \overline{1, k} : g_j(x) = 0\}. \end{aligned} \tag{6}$$

Множество допустимых решений задачи (6) в общем случае неограниченно. Вследствие этой неограниченности возникает неограниченность целевой функции

снизу, что делает невозможным применение стандартных методов линейной оптимизации для ее решения. Для предотвращения данной проблемы добавим следующие ограничения на переменные d_i в задачу (6):

$$\begin{aligned} u &\rightarrow \min, \\ d^T \nabla f_i(x) - u &\leq 0, \quad i = 1, \dots, m, \\ d^T \nabla g_j(x) &\leq 0, \quad j \in J, \quad J = \{j \in \overline{1, k} : g_j(x) = 0\}, \\ -1 &\leq d_i \leq 1, \quad i = 1, \dots, n. \end{aligned} \quad (7)$$

Справедливо следующее утверждение.

Утверждение 2. Область допустимых решений задачи (7) ограничена.

Ограничения и целевая функция в задаче (7) являются линейными, и она может быть решена любым стандартным методом линейного программирования.

Утверждение 3. Пусть $u^*, d_1^*, \dots, d_n^*$ – оптимальное решение (7). Тогда если $u^* < 0$, то существует направление спуска. В противном случае, точка x является критической точкой Парето.

Для нахождения направления наискорейшего спуска требуется найти хотя бы одно решение задачи (4). Одним из возможных способов решения задачи (4) является метод взвешенной суммы или линейной свертки критериев [5]. Данный метод состоит в рассмотрении линейной комбинации критериев $\varphi(x) = \sum_{i=1}^m \lambda_i d^T \nabla f_i(x)$ с положительными коэффициентами $\lambda_i > 0, i = \overline{1, m}$.

$$\begin{aligned} d^T \sum_{i=1}^m \lambda_i \nabla f_i(x) &\rightarrow \min, \\ d^T \nabla g_j(x) &\leq 0, \quad j \in J, \quad J = \{j \in \overline{1, k} : g_j(x) = 0\}, \\ \|d\| &= 1. \end{aligned} \quad (8)$$

Известно [5], что если x^* оптимальное решение задачи (8), то $f(x^*) \in D_p(x)$. Заметим, что задача (8) является задачей выпуклой оптимизации и может быть решена с использованием стандартных методов решения подобных задач. В частном случае, когда множество активных функциональных ограничений пусто, задача (8) решается аналитически.

Использование направлений спуска в задаче аппроксимации границы Парето

С помощью решения задач (7) и (8) можно найти направление спуска в некоторой допустимой точке и выполняется шаг в направлении спуска. Величина шага выбирается такой, чтобы происходило уменьшение всех критериев. Приведем одну из возможных реализаций данного алгоритма:

procedure STEP

input: d /* Descent direction */

```

    S  /* Initial step */
    x  /* Initial point */
do
    x' := x + s d
    if  $F(x') \leq F(x)$  and  $F(x') \neq F(x)$  then
        x := x'
    else
        s :=  $\alpha s$ 
    endif
until  $s \geq s_{\min}$ 

```

Начиная с некоторой изначально заданной величины, смещение S вдоль направления d уменьшается на каждой итерации в случае, если прежнее значение не позволяет уменьшить хотя бы один из критериев. Уменьшение производится с коэффициентом $\alpha < 1$ до тех пор, пока величина смещения больше некоторого минимального значения $s_{\min}$.

После выполнения шага с использованием процедуры STEP вычисляется новое направление спуска. Эта последовательность действий выполняется до тех пор, пока удастся найти направление спуска, либо до тех пор, пока не выполнен другой критерий останова. Такими критериями могут быть слишком маленькая величина смещения или уменьшения критериев.

Литература

1. Ehrgott M. Multicriteria optimization. – Springer Science & Business Media, 2006.
2. Stadler W. (ed.). Multicriteria Optimization in Engineering and in the Sciences. – Springer Science & Business Media, 2013. – Т. 37.
3. Deb K., Miettinen K. Multiobjective optimization: interactive and evolutionary approaches. – Springer Science & Business Media, 2008. – Т. 52.
4. Мину М. Математическое программирование. Теория и алгоритмы. – Наука, 1990.
5. Лотов А. В., Поспелова И. И. Многокритериальные задачи принятия решений. – М. : Изд. отдел фак. ВМиК МГУ им. МВ Ломоносова, 2008.

ИСПОЛЬЗОВАНИЕ АЛГОРИТМОВ НА ГРАФАХ ДЛЯ ДОБАВЛЕНИЯ ПЕРЕСТАНОВОК В БЛОЧНЫХ ШИФРАХ ПРИ СКРЫТИИ ИНФОРМАЦИИ

Жатқанбаев А.А.
e-mail: wildlife.kz@gmail.com

*Институт информационных и вычислительных технологий КН МОН РК,
Казахстан*

Аннотация. В статье описаны процедуры шифрования информации и перестановок, которые будут использованы при разработке системы скрытия

(закрытия и раскрытия) информации. Процесс перестановки основан на выходной последовательности кратчайших путей алгоритмов на графах Беллмана-Форда и Флойда Уоршелла. Создание этой системы скрытия информации и её программная реализация является целью магистерской диссертации.

Введение

Алгоритмы на графах для нахождения кратчайших путей Беллмана-Форда и Флойда-Уоршелла используются в качестве нахождения самых коротких путей между двумя вершинами в графе. Связка результатов применения криптоалгоритмов и выходной последовательности кратчайшего пути обеспечивает дополнительную секретность информации. Если зашифрованная информация записана в режиме шифрования ECB (Electronic Code Book - Электронная Цифровая Книга), то проанализировав различные закрытые тексты, можно предположить, например, что в качестве алгоритма шифрования был использован какой-то определенный шифр. Такие уязвимости были обнаружены в симметричных алгоритмах DES, FEAL-N. Поэтому при использовании пары слабый ключ - слабый открытый текст можем получить и слабый закрытый [1].

В связи с этим предлагается технология, позволяющая на основе построенного графа в виде матрицы смежности, находить кратчайшие пути с использованием алгоритмов Беллмана-Форда и Флойда-Уоршелла. Затем эта последовательность кратчайших путей используется как дополнительная операция перестановок в закрытых текстах для блочных шифров Twofish, Blowfish, DES, 3DES. Использование дополнительных перестановок позволит защитить закрытые тексты от дифференциального криптоанализа.

Разработанная технология актуальна для таких шифров как FEAL-N, DES. Для шифров, в которых S-блоки зависят от ключа и используются операции по модулям неприводимых многочленов не подходят для использования в системах с ограниченными вычислительными ресурсами (POS терминалы, банкоматы и т.п.).

Цель работы

Цель данной работы является исследование полученной выходной последовательности алгоритмов потоков Беллмана-Форда и Флойда-Уоршелла, по которой будут выполнено перемешивание для усиления стойкости.

1. Используемые блочные симметричные алгоритмы шифрования

1.1. Алгоритм шифрования Twofish с зависящими от ключа S-блоков замен

Это алгоритм является одним из самых сложных для программной реализации и самым криптоустойчивым шифром в виду использования модулярной арифметики в раундах шифрования и при формировании раундовых ключей. Шифр Twofish является одним из немногих алгоритмов, в котором обеспечивается генерация зависимых от ключа S-блоков. Алгоритм Twofish, как и большинство блочных алгоритмов шифрования, построенных на сети Фейстеля, имеет фиксированные размеры блоков 128, 192, 256 бит (рисунок 1).

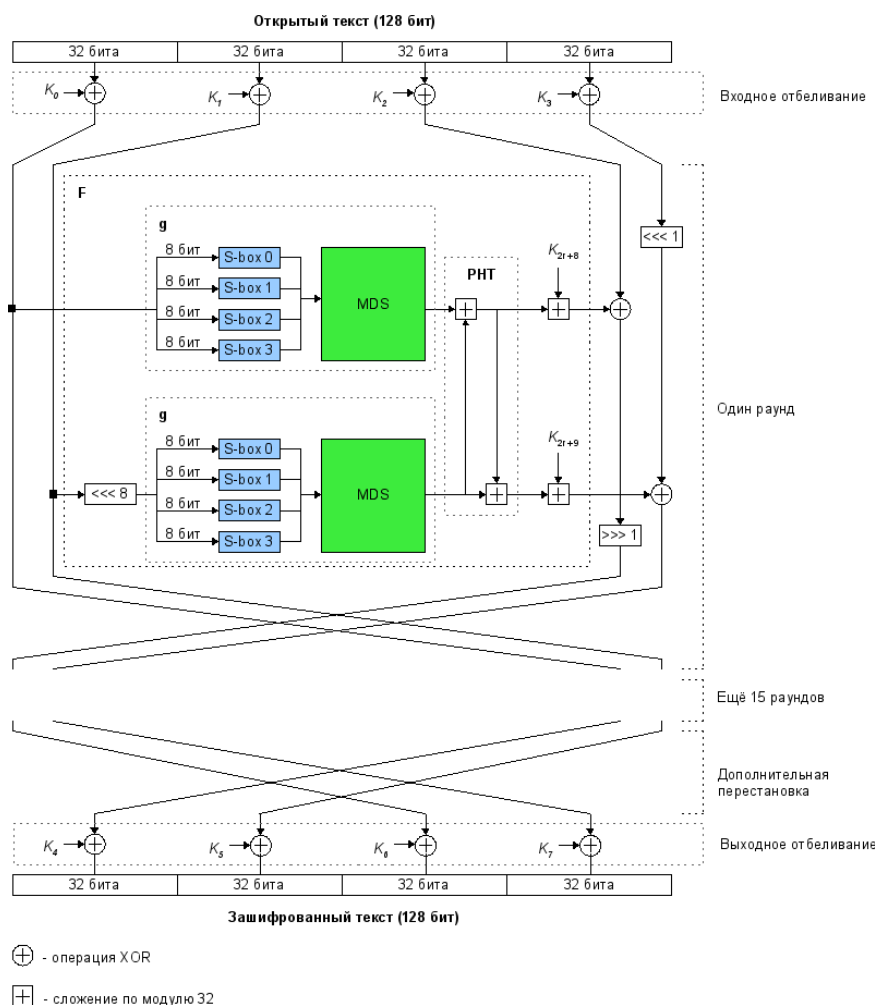


Рис. 1 Схема алгоритма Twofish-128

1.2. Алгоритм шифрования Blowfish с зависящими от ключа S-блоков замен

Шифр Blowfish является основан на сети Фейстеля и зависящих от ключа S-блоков. Он был создан после безуспешных попыток достичь баланса производительности и высокой криптостойкости таких шифров как FEAL-N, DES. Блочный симметричный шифр Blowfish имеет размер ключа в 448 бит для блочных симметричных шифров, что более присуще потоковым шифрам A5-1, RC-4. Ввиду использования быстрых унарных операции (XOR, сложение по модулю 32) и сети Фейстеля данный алгоритм имеет схожую конструкцию с IDEA, FEAL-N. Это один из немногих шифров достигших оптимального баланса между скоростью шифрования и высокой криптостойкостью. Тем самым данный алгоритм можно использовать в системах с ограниченными ресурсами или же требующих высокую скорость шифрования. Блочный симметричный шифр Blowfish также легко реализуем на множестве систем включая ПЛИС и не требует сложных криптографических расчетов как в случае с Rijndael, Twofish.

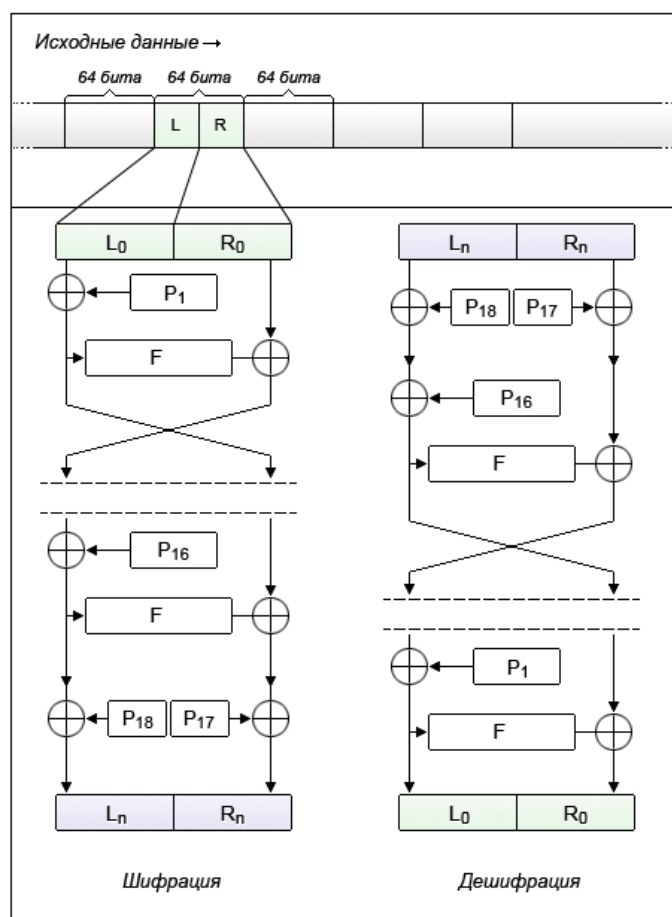


Рис. 2 Схема алгоритма Blowfish

1.3. Алгоритм шифрования DES

Официальный стандарт шифрования FIPS 46-3 1977 года. Как и многие шифры того периода DES основывался на таблице замен, фиксированных S-блоков и в своей структуре не содержал сложных криптографических функций как последующие шифры, базировавшиеся на сети Фейстеля: IDEA, FEAL-N. Уязвимой стороной DES являлось наличие слабых S блоков (не равномерное повторение значений внутри каждого S блока), что позволило быстро вычислять ключ посредством дифференциального криптоанализа. Так же с ростом вычислительных мощей ЭВМ, размер ключа в 64 бита являлся уязвимой стороной шифра, позволявшей полным перебором подобрать ключ. Так же в виду неиспользования каких-либо сложных криптографических функций, DES не полностью шифровал открытые тексты.

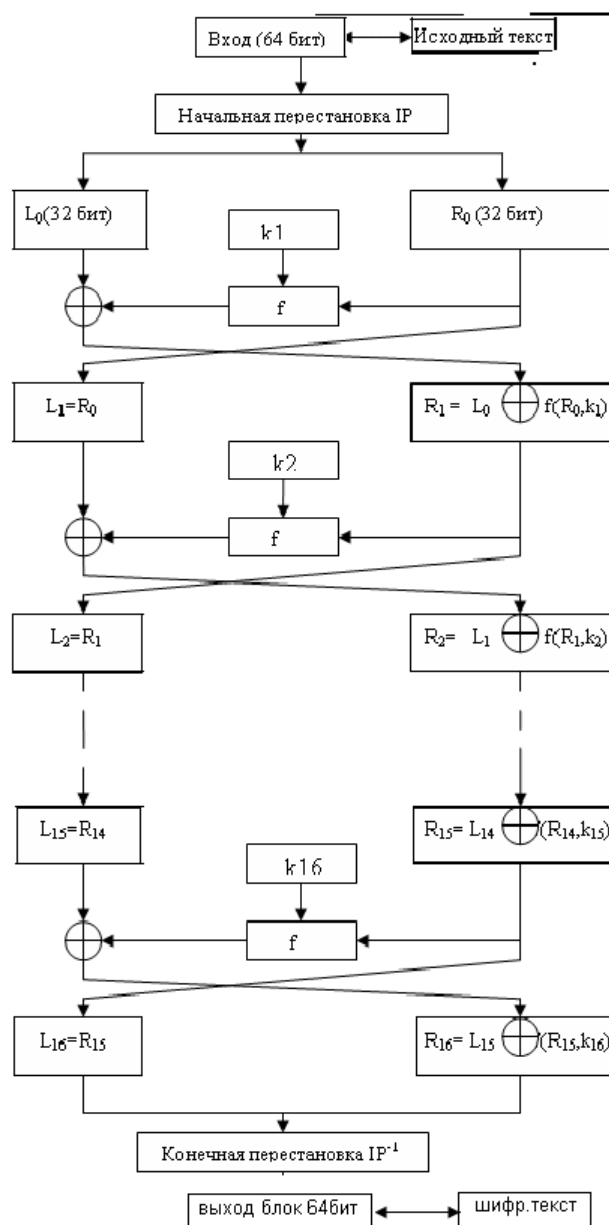


Рис. 3 Схема алгоритма DES

1.4. Алгоритм шифрования 3DES

Этот алгоритм полностью аналогичен DES, но используется 3 ключа по 64 бита. Общая длина 192 бита, это решало проблему атак, основанных на полном переборе, однако проблема с парами слабый ключа, слабый открытый текст не решалась что послужило полным отказом от данного шифра и в процессе разработок шифров больше внимания уделялось сложным криптографическим функциям, а не только лишь процессам перестановок и замен (рисунок 4).



Рис. 4 Схема алгоритма 3DES

2. Введение дополнительной перестановки на основе выходной последовательности алгоритмов Беллмана-Форда и Флойда-Уоршелла

2.1. Алгоритм Флойда-Уоршелла

Если использовать алгоритм Беллмана-Форда для обхода графа и применить полученную выходную последовательность для перемешивания байтов закрытого текста (шифртекста), то пользователь получит шифртекст открытого сообщения с шумом. Будет также получена матрица смежности графа для алгоритма Беллмана-Форда, который будет выступать в роли дополнительного ключа. В результате будет выдана некая последовательности обхода, которая является кратчайшем путем в данном графе.

Если пользователь имеет закрытый текст перед записыванием его в картинку он будет использовать выходную последовательность алгоритма Беллмана-Форда для добавления шума к закрытому тексту, т.е. перемешивает байт текста. Используя выходную последовательность, он получит измененный закрытый тест с соблюдением перестановки байтов. Также используется функция восстановления для получения начального закрытого текста.

Программная реализация алгоритма проведена в среде Microsoft Visual Studio 2013 на языке программирования C#.

2.2. Алгоритм нахождения кратчайшего пути Беллмана-Форда

Алгоритм нахождения кратчайших путей Беллмана-Форда основан на операции релаксации ребер. Изначально алгоритм не применим к графам, имеющим отрицательный цикл, в виду того, что изменять расстояние для двух узлов в таком графе можно бесконечно. Алгоритм в данном случае только найдет признак того, что имеется отрицательный цикл. Процедура релаксации между двумя ребрами - это попытка улучшения расстояния между двумя вершинами a и b вдоль некого ребра c .

Процедура псевдокода для нахождения кратчайшего пути в графе с использованием алгоритма Беллмана-Форда:

```

Function BellmanFord
{
  //Установим начальные расстояния до всех вершин V равным бесконечным, также
  для всех предков каждой вершин установим нулевое значение
  For(int i=1; i<=V; i+=1)
  {
    d[i]=inf;
    p[i]=0;
  }
  d[s]=0; //Установим начальное значение 0 от источника
  //Пройдемся по всем вершинам

```

```

For(int i=1;i<=V-1;i+=1)
{
//Для каждого исходящего ребра от вершины проверим
For each Edge e in Edges(G)
{
//Если расстояния между двумя вершинами a,b вдоль некого ребра с меньше
текущего. Это значит что мы используем ребро с уже имея текущее ребро
кратчайшего пути между a,b + некое ребро с, то значит путь можно улучшить
If(distance[e.from]+lengthof(e)< distance[e.to])
{
distance[e.to]=distance[e.from]+lengthof(e);
p[e.to]=e.from; //Запишем в массив предков новую найденную вершину
}
}
}
}

```

2.3. Алгоритм нахождения кратчайшего пути Флойда-Уоршелла

Этот алгоритм так же решает проблему нахождения кратчайшего пути между двумя вершинами в графе, но он выполняется медленнее, чем алгоритм Беллмана Форда в виду полного перебора пар вершин и ребер.

Псевдокод алгоритма:

```

Function Floyd-Warshall{
d[uv]=w//Устанавливаются начальные веса ребер графа.
For(int i=1;i<V;i+=1) //Просмотр всех вершин графа
{
For(int u=1;u<V;u+=1)//Просмотр всех ребер графа
{
For(int v=1;v<V;v+=1)
{
d[uv]=min(d[uv-1],d[ui-1]+d[iv-1])//Если расстояние можно улучшить путем
добавления промежуточной вершины (ребра), то записываем данную вершину(ребро)
}
}
}
}
}

```

3. Программная реализация алгоритмов осуществлена в среде программирования Microsoft Visual Studio 2013 на языке программирования C#

3.1. Программная реализация алгоритма Twofish

Ключ- 0x9F589F5C, 0xF6122C32, 0xB6BFEC2F, 0x2AE8C35A

Открытый текст- 0x16db91d4, 0x9ec3b1e7, 0x6b08cb86, 0x19549f78

```

Output
Show output from: Debug
CIPHERTEXT
P[0]=9989f01
P[1]=851117de
P[2]=a3c3aa8f
P[3]=c3fb20ba
PLAINTEXT
P2[0]=16db91d4
P2[1]=9ec3b1e7
P2[2]=6b08cb86
P2[3]=19549f78

```

Рис. 5 Программная реализация алгоритма Twofish

3.2. Программная реализация алгоритма Blowfish

Ключ- 0x01234567, 0x89ABCDEF, 0x01234567, 0x89ABCDEF, 0x01234567,
0x89ABCDEF,
0x01234567,0x89ABCDEF,0x01234567,0x89ABCDEF,0x01234567,0x89ABCDEF,0x
01234567,0x89ABCDEF,0x01234567,0x89ABCDEF,0x01234567,0x89ABCDEF
Открытый текст- 0x11111111 0x11111111

```

Output
Show output from: Debug
CT[0]=61f9c380
CT[1]=2281b096
PT[0]=11111111
PT[1]=11111111
The thread 0x1b88 has exited with code 0 (0x0).

```

Рис. 6 Программная реализация алгоритма Blowfish

3.3. Программная реализация алгоритма DES

Ключ- 0x40000000,0x00000000
Открытый текст- 0x00000000, 0x00000000

```

Output
Show output from: Debug
CT=eec1487dd8c26d5

Error List Output Find Symbol Results Locals Watch 1

Output
Show output from: Debug
PT=0

Error List Output Find Symbol Results Locals Watch 1

```

Рис. 7 Программная реализация алгоритма DES

3.4. Программная реализация алгоритма 3DES

Ключ- 0x2BD6459F, 0x82C5B300 0x952C4910, 0x4881FF48 0x2BD6459F,
0x82C5B300
Открытый текст- 0x8598538A, 0x8ECF117D

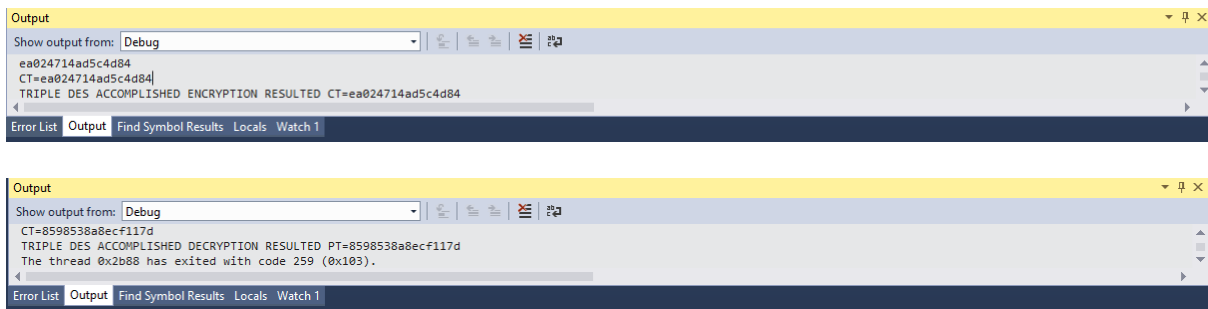


Рис. 8 Программная реализация алгоритма 3DES

3.5. Программная реализация алгоритма Флойда Уоршелла

//Представленный граф с 6-ью вершинами

```
{0,10,18,8,inf,inf},
{10,0,16,9,21,inf},
{inf,16,0,inf,inf,15},
{7,9,inf,0,inf,12},
{inf,inf,inf,inf,0,23},
{inf,inf,15,inf,23,0}
```

Ниже предоставлена выходная последовательность кратчайших путей из всех возможных вершин графов в вершины графа

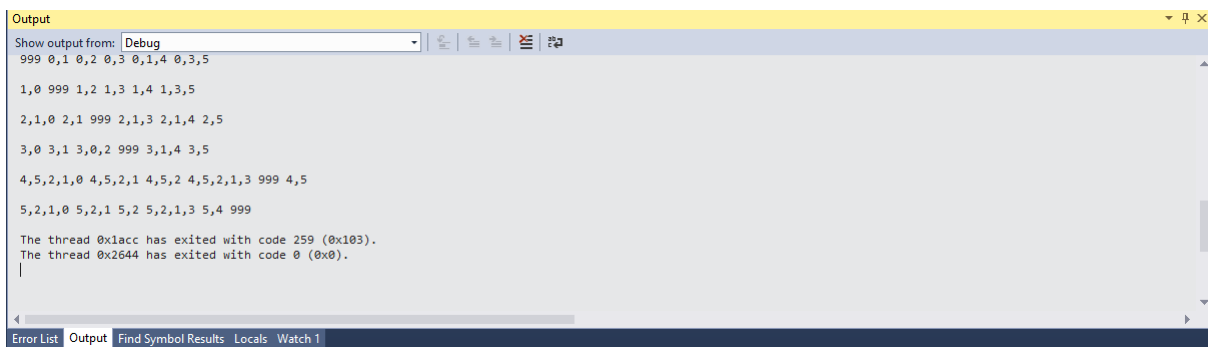


Рис. 9 Программная реализация алгоритма Флойда Уоршелла

3.6. Программная реализация алгоритма Беллмана-Форда

//Представленный граф с 6-ью вершинами

```
{0,10,18,8,inf,inf},
{10,0,16,9,21,inf},
{inf,16,0,inf,inf,15},
{7,9,inf,0,inf,12},
{inf,inf,inf,inf,0,23},
{inf,inf,15,inf,23,0},
```

Ниже предоставлена выходная последовательность кратчайших путей из всех возможных вершин графов в вершины графа.

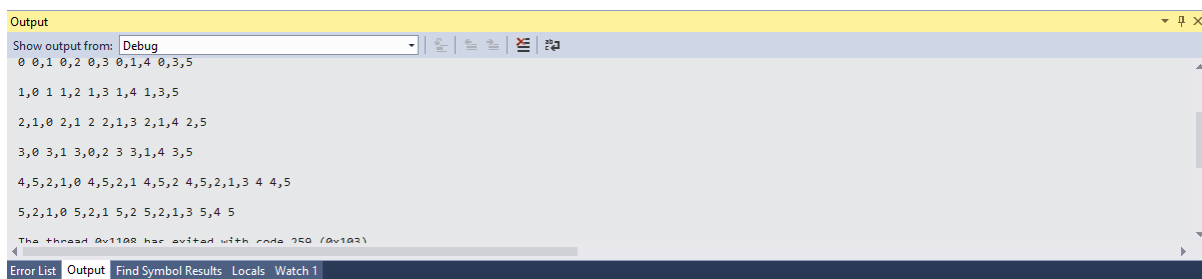


Рис. 10 Программная реализация алгоритма Беллмана-Форда

Заключение

В магистерской диссертации будет разработана система скрытия и раскрытия электронной информации. Скрытие – это процедура шифрования, перестановки, сжатия, применение алгоритмов максимального потока и запись в картинку. Следует учесть, что размерность графа не должна превышать размер электронного графического изображения.

В статье приводятся полученные результаты при разработке системы скрытия информации. Суть этой системы заключается в записи некоторой информации в графическое изображение.

Литература

1. Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, and Niels Ferguson. The Twofish Encryption Algorithm, A 128-Bit Block Cipher. Wiley, 1999.
2. Oppersmith Don. 1994. The data encryption standard (DES) and its strength against attacks. IBM Journal of Research and Development. 38(3): 243-250.
3. Henk C.A. van Tilborg, Eindhoven. 2012. Encyclopedia of Cryptography and Security. 2005, Springer Science+Business Media, Inc.
4. Alan G. Konheim. 2007. Computer security and cryptography. By John Wiley and Sons, Inc.

ИССЛЕДОВАНИЕ МОДЕЛИ ПРОГНОЗИРОВАНИЯ И УПРАВЛЕНИЯ ЭПИДОБСТАНОВКОЙ С ПРИМЕНЕНИЕМ НЕЧЕТКОГО И ИНТЕРВАЛЬНОГО АНАЛИЗА

Исимов Н., Джомартова Ш.А., Мазаков Т.Ж.

e-mail: int_nurdaulet@mail.ru

*Институт информационных и вычислительных технологий КН МОН РК,
Казахстан*

Аннотация. В статье для модели прогнозирования управления эпидемиологической обстановки на основе интервальной математики получен критерий нечеткой управляемости. На основе решения модельной задачи показана эффективность полученного критерия.

Ключевые слова: Эпидобстановка, управляемость, интервальная математика, лингвистическая переменная.

Введение

Одна из актуальных задач медицины состоит в своевременной профилактике различных эпидемических болезней с помощью медико-биологических и социально-экономических мер. Своевременность и действенность медицинских мероприятий может быть обеспечена лишь при условии хорошо разработанной службы прогнозирования, которая должна предсказывать эпидобстановку в обследуемом районе в зависимости от состояния многочисленных абиотических, биотических, социальных и других факторов [1].

Работа посвящена исследованию математической модели динамики эпидемиологических процессов на основе методов теории обыкновенных дифференциальных уравнений, математической теории управления, интервального и нечеткого анализа.

Постановка задачи

В статье исследуется управляемость нелинейной системы, описываемой обыкновенными дифференциальными уравнениями

$$\dot{x} = f(x, u, t) \quad (1)$$

где $f(x, u, t)$ – n -вектор, элементы которого являются непрерывно-дифференцируемыми функциями по своим аргументам, x – n -мерный вектор состояния системы, u – m -мерный вектор управления.

На управление даются ограничения

$$u(t) \in U = \{u(t): -L_i \leq u_i(t) \leq L_i, i = 1, m, t \in [t_0, t_1]\} \quad (2)$$

В работе [2] предложена математическая модель, характеризующая эпидемиологическую обстановку в исследуемом регионе. В предложенной математической модели используются следующие абиотические факторы:

w_1 – солнечная активность (числа Вольфа),

w_2 – температура (среднемесячная температура в исследуемом районе),

w_3 – суммарное количество осадков за месяц,

w_4 – максимальное суточное количество осадков за месяц,

w_5 – уровень подземных грунтовых вод,

w_6 – просачиваемость почвы;

биотические факторы:

x_1 – общее количество носителей эпидемии (блех),

x_2 – количество заразных носителей эпидемии,

x_3 – общее количество переносчиков эпидемии (песчанок),

x_4 – количество заразных переносчиков эпидемии.

Факторы $w_i, i = \overline{1,6}$ независимы. Значения факторов $w_i, i = \overline{1,3}$ в момент времени t определяются с помощью временных рядов. Значения факторов $w_i, i = \overline{4,6}$ определяются из геофизических данных по исследуемому району.

Динамика факторов x_i ($i = 1, 2$) в момент времени t описывается уравнениями:

$$\dot{x}_1 = f_1(w)x_1 - f_2(w)x_1 - b_1 u_1, \quad (3)$$

$$\dot{x}_2 = \mu_1 x_2 \left(1 - \frac{x_2}{x_1}\right) - c_1 x_2 \quad (4)$$

где функция f_1 определяет рождаемость популяции, функция f_2 определяет смертность популяции в зависимости от абиотических факторов среды. Коэффициент μ_1 определяет вероятность заражения одной особи в единицу времени. Коэффициент c_1 определяет темп естественного оздоровления и смертность больных носителей.

Функцию рождаемости f_1 задается следующим образом:

$$f_1(w) = \sum_{i=1}^3 f_{1i}(w_i) \quad (5)$$

$$f_{1i}(w_i) = a_i e^{-\frac{(w_i - \widehat{w}_i)^2}{\sigma_i^2}}, i = 1, 3 \quad (6)$$

Здесь $\widehat{w}_i$ определяет наиболее благоприятное для жизнедеятельности носителя значение i -го абиотического фактора, σ_i - ширину интервала с центром в точке $\widehat{w}_i$, при котором возможна жизнедеятельность носителя. Численные значения параметров $\widehat{w}_i$ и σ_i доступны из соответствующих справочников. Коэффициенты a_i определяют степень влияния i -го абиотического фактора на рождаемость носителя.

Функцию смертности f_2 выберем следующим образом:

$$f_2(w) = \sum_{i=1}^3 f_{2i}(w_i) \quad (7)$$

$$f_{2i}(w_i) = \beta_i \left(1 - \varepsilon e^{-\frac{(w_i - \widehat{w}_i)^2}{\sigma_i^2}} \right), i = 1, 2 \quad (8)$$

$$f_{23}(w) = \beta_3 (1 - \varepsilon e^{-\frac{(w_3 - \widehat{w}_3)^2}{\sigma_3^2}}) / w_4. \quad (9)$$

В формулах (8)-(9) коэффициент ε определяет естественную смертность носителя. Коэффициенты β_i определяют степень влияния i -го абиотического фактора на смертность носителя.

Для прогнозирования значения факторов x_i ($i = 3, 4$) в момент времени t предлагается модель:

$$\dot{x}_3 = f_3(W)x_3 - f_4(W)x_3 - b_2u_2, \quad (10)$$

$$\dot{x}_4 = \frac{x_2}{x_1}x_4 \left(1 - \frac{x_4}{x_3}\right) - c_2x_4,$$

где функция f_3 определяет рождаемость, функция f_4 определяет смертность переносчиков в зависимости от абиотических факторов среды. Коэффициент c_2 определяет смертность больных переносчиков. Функции рождаемости f_3 и смертности f_4 аналогичны соответственно функциям f_1 и f_2 .

В отличие от модели Вольтерра в (3) – (10) задаются управления u_1 и u_2 , определяющие противоэпидемиологические мероприятия. Коэффициенты b_1 и b_2 задают степень влияния управления на динамику численности носителей и переносчиков.

В [2] для модели (3)-(10) разработаны: алгоритмы идентификации параметров a_i , β_i , b_i ; доказано существование и решение соответствующей задачи для Коши при фиксированном управлении; экспертная система мониторинга эпидобстановки.

Как видно, модель (3)-(10) полностью погружается в более общую модель (1)-(2).

В классической теории управления обычно исследуется задача управляемости [3] (Задача 1): существует ли управление, удовлетворяющее ограничению (2) и переводящее систему (1) из начального состояния

$$x(t_0) = x_0 \quad (11)$$

в конечное заданное состояние

$$x(t_1) = x_1. \quad (12)$$

за фиксированное время $t_1 - t_0$.

Начальные значения вектора состояния x_0 в формуле (11) задаются по фактическим измерениям. В то же время, для задачи мониторинга эпидемиологической ситуации актуально не фиксированное значение x_1 в конечный момент времени t_1 в формуле (12), а перевод системы в некоторое множество, позволяющее обеспечить удобную интерпретацию.

В этой связи, на основе теории нечетких множеств введем для переменных состояния x системы (1), соответствующие лингвистические переменные следующим образом [4].

Каждой переменной состояния x_i поставим в соответствие лингвистическую переменную $x_{\text{линг}i}$, $i = \overline{1, n}$. Так как в модели (3)-(10) переменные состояния системы имеют количественный характер и большее значение их повышает степень опасности возникновения эпидемии, предложены следующие значения лингвистических переменных: TermLin[1]=«идеальный уровень», TermLin[2]=«оптимальный уровень», TermLin[3]=«комфортный уровень», TermLin[4]=«умеренный уровень», TermLin[5]=«допустимый уровень», TermLin[6]=«критический уровень» и TermLin[7]=«катастрофический уровень».

Каждому j – му значению i –й лингвистической переменной $x_{\text{линг}i,j}$ соответствует числовой интервал $(x_{\min i,j}, x_{\max i,j})$ и множество $\bigcup_{j=1}^7 (x_{\min i,j}, x_{\max i,j})$ должно охватывать

всевозможные значения переменной $(x_{\min i,j}, x_{\max i,j})$. В частности, допускается, чтобы $\bigcup_{j=1}^7 (x_{\min i,j}, x_{\max i,j}) = (-\infty, +\infty)$.

Введем множество индексов $I_{kr} \subseteq [1, \dots, n]$, определяющее перечень переменных состояния, на которые накладываются терминальные ограничения. Например, если для модели (3)-(10) терминальные ограничения накладываются только на переменную x_2 – количество заразных носителей эпидемии, то множество индексов $I_{kr} = [2]$ состоит из одного элемента.

Далее рассматривается следующая нечеткая задача управляемости (Задача 2): существует ли управление, удовлетворяющее ограничению (2) и переводящее систему (1) из начального состояния (11) в конечное состояние

$$x_{\text{кон}}(t_1) = \text{TermLin}[i_j], i \in I_{kr} \quad (13)$$

за фиксированное время $t_1 - t_0$.

В (13) индекс i_j соответствует выбранному j -му лингвистическому нечеткому значению для i -й переменной состояния.

Задача 1 является частным случаем задачи 2.

Основные результаты

В силу свойств наложенных на правую часть системы уравнений задачи Коши (1), (11) при фиксированном управлении $u(t) \in U$ выполнены условия теоремы существования и единственности решения $x(t)$, $t \in [t_0, t_1]$ [5].

Перепишем задачу Коши (1), (11) в интегральной рекуррентной форме

$$x_{k+1}(t) = x_0 + \int_{t_0}^t f(x_k(\tau), u(\tau), \tau) d\tau. \quad (14)$$

В силу свойств наложенных на правую часть уравнения (1) и ограничений на функцию $u(t)$ в работе [6] доказано, что метод последовательных приближений (5) сходится к решению абсолютно и равномерно при любом фиксированном управлении.

Тогда задача управляемости сводится к исследованию следующей задачи: существует ли хотя бы одно управление $u(t) \in U$, при котором решение интегрального уравнения (14) в момент времени t_1 удовлетворяет условию (13).

Для решения поставленной задачи применим результаты интервального анализа [7]. Обозначим через $\bar{v}$ интервал от $-L$ до L , через $\bar{f}$ интервальнозначную функцию, полученную из функции $f(x_k(t), u(t), t)$.

Подставляя в уравнение (14) вместо функции $u(t)$ интервал $\bar{v}$ получим интервальное интегральное уравнение

$$\bar{x}_{k+1}(t) = x_0 + \int_{t_0}^t \bar{f}(\bar{x}_k(\tau), \bar{v}, \tau) d\tau. \quad (15)$$

Теорема. Для того чтобы исследуемая система была управляемой необходимо и достаточно, чтобы заданный вектор для всех $i \in I_{kr}$ пересечение множества $(x_{\min i, j}, x_{\max i, j})$ с множеством $\bar{x}_{k+1, i}(t_1)$ было непустым.

На основе библиотеки процедур интервальных вычислений [8] произведены численные расчеты для модельной задачи. Легкость разработки программного обеспечения, алгоритмизируемость процедуры проверки условий теоремы показывает эффективность его применения.

Литература

1. Ревич Б.А., Авалиани С.Л., Тихонова Г.И. Экологическая эпидемиология. Москва: Издательство Академия, 2004. – 384 с.
2. Тойкенов Г.Ч., Мазаков Т.Ж. Применение математических методов в эпидемиологии // Вестник КазГУ. Матем., механ., информатика. N 4. – Алматы: КазГУ, 1996. – С.184-189.
3. Воронов А.А. Устойчивость, управляемость, наблюдаемость. – Москва: Издательство Наука, 1979. – 336 с.
4. Заде А.Л. Понятие лингвистической переменной и его применение к принятию приближенных решений. – Москва: Издательство Мир, 1976. – 166 с.
5. Понтрягин Л.С. Обыкновенные дифференциальные уравнения. – Москва: Издательство Наука, 1974. – 332 с.
6. Верлань А.Ф., Сизиков В.С. Интегральные уравнения: методы, алгоритмы, программы. – Киев: Издательство Наукова Думка, 1986. – 543 с.
7. Шокин Ю.И. Интервальный анализ. – Новосибирск: Издательство Наука, 1986. – 224 с.
8. Мазаков Т.Ж., Джомартова Ш.А., Оспанова М.К. Библиотека процедур интервальной математики // Материалы 1-й междунар. Научно-практ. конф. – Алматы: «Информатизация общества», 2004. – С.160-162.

АҚПАРАТТЫҚ МОДЕЛЬДЕРДІ ЖӘНЕ АҚПАРАТТЫҚ ЖҮЙЕНІ ЖҮЗЕГЕ АСЫРУ ӘДІСТЕРІН ҚҰРУ

Калимолдаев М.Н., Абдилдаева А.А.
e-mail: abass_81@mail.ru

*Институт информационных и вычислительных технологий КН МОН РК,
Казахстан*

Аннотация. Бұл мақалада электроэнергетикалық жүйелердің тұрақтылығы үшін ақпараттық жүйелердің құрылымы қарастырылған. Ақпараттық жүйенің жүйелік және функционалдық толығы сипатталған. Сонымен қатар, электроэнергетикалық жүйелердің моделдері көрсетілген. Қазіргі кезде мәліметтерді тарату жүйесін қолданудың негізгі салаларына релелік қорғаныс жүйесі мен

автоматиканы, электроэнергетикалық объектілерді диспетчерлік және автоматты технологиялық басқаруды, сонымен қатар, энергоресурстарды автоматты есептеу жүйелерін жатқызуға болады. Қозуды автоматты реттеу (ҚАР) синхрондық машина электр жүйесін реттеу және тұрақтылықты сақтайтын бірден -бір тиімді тәсілдердің бірі. Сонымен қатар, көптеген қолайлы параметрлер мен тұрақты жұмыс істеу тәртібінде энергиялық жүйе көптеген кедергілерге ұшырап тұрақтылықты құру барысында кедергі келтіруі мүмкін. Мұндай жағдайда ҚАР жүйесін қолдану тұрақтылықты қамтамасыз етуге жеткіліксіз болады. Сондықтан, ақпараттық жүйені құру қажеттілігі туындайды.

Кіріспе. Қазіргі таңда заманауи ЭЭЖ әртүрлі өзара әрекеттесетін, кері байланыстар мен факторлардан тұратын өте күрделі объект болып табылады. Сондықтан электр-энергетикалық объектілерді жобалау, басқару және эксплуатациялаумен байланысты кез-келген есепті шешу үшін жоғары қуатты есептеу математикасының аппараттарын, есептеу техникасының барлық түрін, байланыс жүйесін, және телекоммуникацияны қолдану керек.

Берілген есептерді шешу үшін электр-энергетикалық параметрлерді есептеу құралдары және әртүрлі электр қондырғылары мен шағын станциялардың автоматтандырылған жобалау жүйелері қолданылады. Тұрақты режимде сенімді және сапалы электр-энергиясымен қамтамасыз ету үшін, электр-энергетикалық жүйені эксплуатациялау кезінде оперативті-диспетчерлік басқару жүргізіледі. Заманауи жағдайларда бұл түрдегі басқару жинақтау жүйесі мен ақпаратты өңдеудің «үлкенді» комплексін қолдануды талап етеді. Деректерді жинау мен өңдеуді қамтамасыз ететін программалық кешендер өте көп. Бастапқы кезде олар тек деректерді жинауға және көрсетуге арналды. Қазіргі таңда олар есептеу және ақпарат анализі бойынша қосымша модульдармен жабдықтала алады.

Қазақстандық электр энергетикасында қолданылатын ақпараттық жүйелер мен автоматты басқару жүйелерінің негізгі түрлері [1]:

- телемеханика , ақпаратты жинау және тасымалдау жүйесі;
- оперативті-ақпараттық кешендер (ОАК, SCADA-жүйелер);
- өтпелі режимдердің мониторингтік жүйесі (СМПП, WAMS-жүйелер);
- ЭЭЖ-дің режимінің анализін, моделін және күйін бағалауға арналған бағдарламалық-есептеуіш кешендер;
- өлшеу функцияларын, күйді бағалау, онтайландыру және болжау SCADA/EMS жүйелері.

Ақпараттық жүйенің құрылымы.

Біздің құрған ақпараттық жүйеміз электр-энергетикалық жүйенің орнықтылығы мен тиімді басқаруын қамтамасыз етеді. Жүйенің атқаратын қызметі:

- деректерді жинақтау құрылғысынан ақпаратты қабылдау;
- математикалық модельдерді қолдану арқылы электр-энергетикалық жүйенің жұмысын (апатты жағдайда) қалпына келтіру;
- апатты жағдайды көрсету механизмін қолдану;
- ақпараттарды архивтеу (қолданушының тәуліктік, апталық іс әрекетінің архивін жүргізу);
- мәтіндік ақпаратты экранға шығару жүйесін қолдану;
- есептік құжаттарды дайындау;
- электр-энергетикалық жүйелерді автоматты басқару.

Құрылған жүйе үш деңгейлі архитектурадан тұрады:

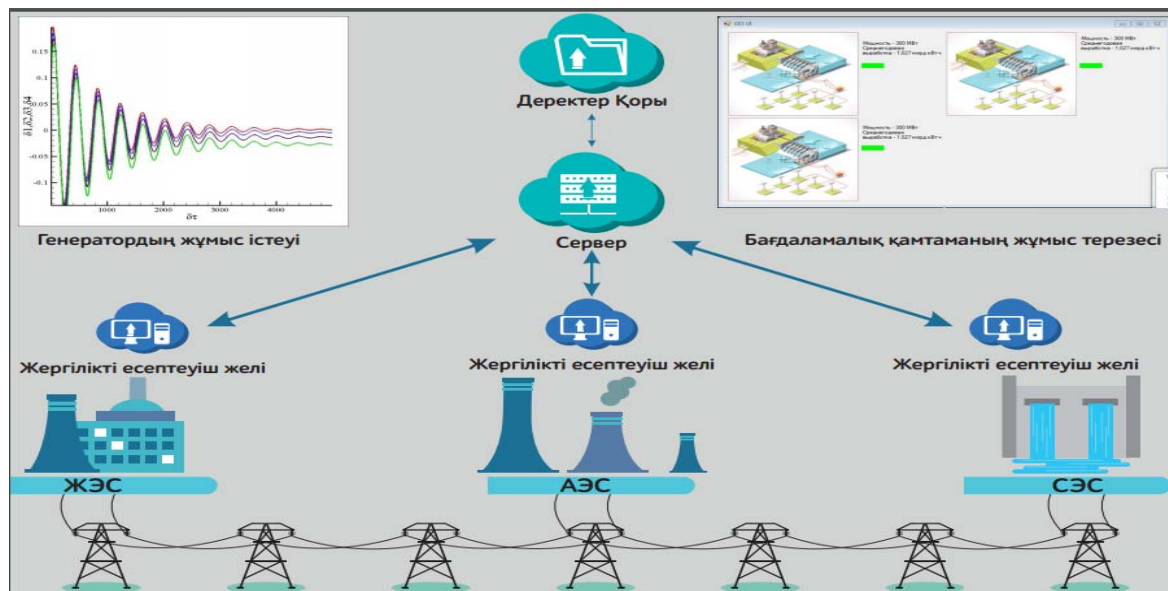
1. аппараттық деңгей - деректерді жинақтауды қамтамасыз ететін бағдарламалық техникалық құрылғы;
2. ақпараттық деңгей - жүйенің кез келген параметріне қол жеткізуді қамтамасыз ету;
3. қолданбалы деңгей - нақты мәселелерді шешу үшін деректерді ұсыну және өңдеу.



Сурет 1 - Жүйенің құрылысы

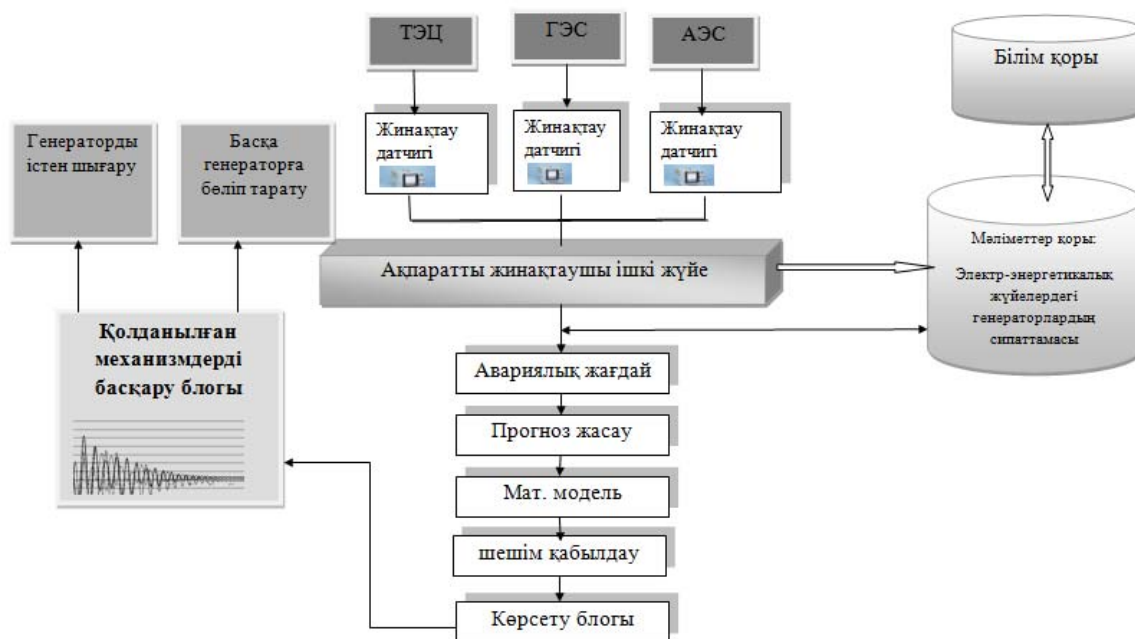
Жүйенің бұндай архитектурасы жүйенің функционалдық бөлімінен аппараттық деңгейдің тәуелсіздігін қамтамасыз етеді. Ақпараттық деңгей қолданбалы деңгейдің өзара және аппараттық деңгеймен қосымша әрекеттесуін қамтамасыз етеді. Қолданбалы деңгей жергілікті есептеуіш желі арқылы жұмыс істейді.

Жүйенің жалпы архитектурасы сурет 2 көрсетілген. Бұл жүйеде электр-энергетикалық жүйеден жергілікті есептеуіш желі арқылы генератордан алынған ақпарат деректер қорына жинақталады.



Сурет 2 - Ақпараттық жүйенің жалпы архитектурасы.

Электр-энергетикалық жүйелердің қозғалысының орнықтылығы мен тиімділігін зерттеу үшін құрылған ақпараттық жүйенің концептуалдық схемасы 3 суретте келтірілген. Схемда электр-энергетикалық жүйелерден жинақтау датчигі арқылы алынған мәлімет ақпаратты жинақтаушы ішкі жүйесі арқылы деректер қорына ақпаратты жібереді. Деректер қорында генераторлардың сипаттамасы, қолданушы жайында жалпы мәлімет сақталады. Деректер қоры білім қорымен тікелей байланысты. Білім қорында генераторда өңделетін жалпы энергия туралы мәлімет сақталады. Апаттық жағдай кезінде, ішкі жүйе арқылы ақпаратты деректер қорына сақтай отырып, математикалық модельді қолданамыз және шешім қабылдаймыз: генераторды істен шығарамыз және оның жүктемесін басқа генераторларға үлестіреміз немесе резервтегі генераторды іске қосамыз.



Сурет 3 – Электр-энергетикалық жүйенің ақпараттық жүйесінің сызбасы

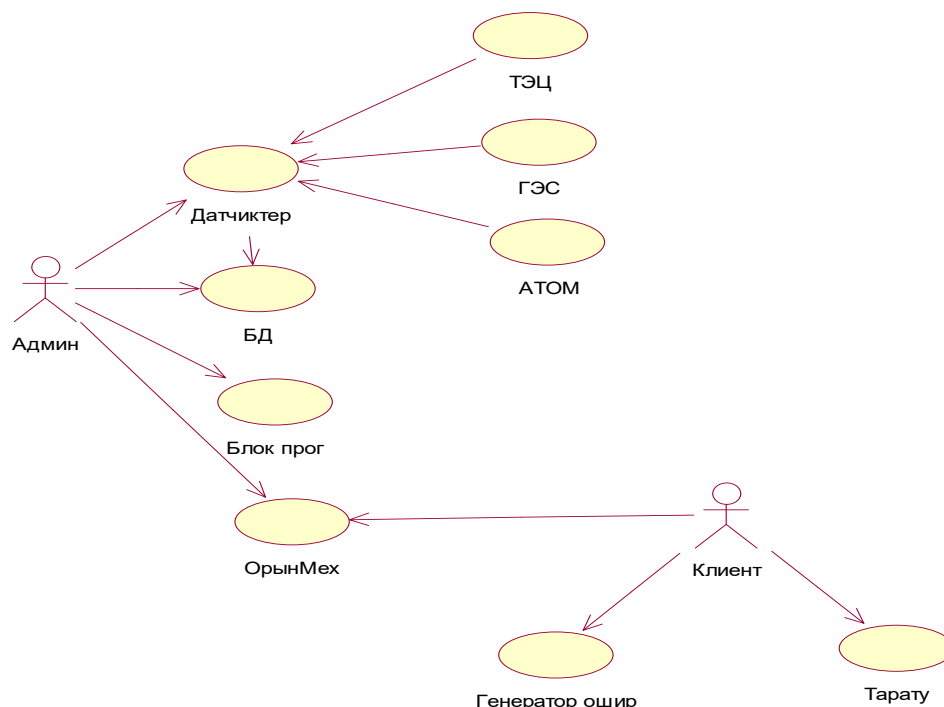
Ақпараттық жүйе процесстерді басқару үшін қажетті деректерден тұрады. Функционалдық толықтыруда ЭЭЖ орнықтылығы талданады, энергия жүйесінің жұмыс режимдері анықталады, математикалық модельдер есептері үшін тәсілдер сипатталады және ЭЭЖ электр желісі мен жүктемелері қарастырылады.

Ақпараттық жүйенің *жүйелік және функционалдық* толықтырылуы ЭЭЖ электр механикалық ауыспалы процесстерді сандық модельдеуге және талдауға арналған. Электр механикалық ауыспалы процесстерді сандық модельдеу дегеніміз есептік модельдерді құру, деректерді дайындау, модельдік тендеулерді дискреттеу, тендеулер жүйесін шешу және алынған нәтижелерді өңдеу жатады [2].

ЭЭЖ белгіленген апатқа дейінгі режимі ауыспалы үрдістің басты нүктесіндегі параметрлер мәнін береді. Орнықтылық талдауы үшін, ЭЭЖ түрлі режимдерін көрсететін апатқа дейінгі және апаттан кейінгі режимдерді қарастырамыз. Режим есебі үшін Гаусстың, Эйлердің және Рунге - Куттаның 4 ретті әдістері қолданылады.

Режимдер. Энергия жүйесінің жұмысын бұзатын апатты әрекеттерді қоса алғандағы, сонымен қатар тиімді апаттан кейінгі режимге сәйкес келетін жүйенің

орнықты жұмысындағы жаңа нүктеге динамикалық ауысуды қамтамасыз етуге бағытталған апатқа қарсы автоматика жұмысын қоса алғандағы, энергия жүйесінің элементтеріндегі ауытқуларын сипаттайды.



Сурет 4 – Электр-энергетикалық жүйе үшін ақпараттық жүйенің UML- дағы сұлбасы

Электр-энергетикалық жүйелердің UML тіліндегі сұлбасы сурет 4-те көрсетілген. Администратор мен инженердің жұмысының орындалуы туралы ақпарат берілген. Администратор электр-энергетикалық жүйелерден датчиктер арқылы келген ақпаратты деректер қорында сақтайды және бағдарламалық блок арқылы орындау механизімінде өңдейді. Инженер орындау механизімі арқылы генераторды өшіру немесе генератордағы жүктемені басқа генераторларға үлестіруді орындайды.

Талдау. ЭЭЖ орнықтылығын талдау үшін элементтер бойынша, сонымен қатар есептік сериялар бойынша ақпаратты құрылымдаудың ауқымды мүмкіндіктері бар ыңғайлы көзбен шолу блогы қажет. Бұл түрлі типті және кез келген қуатты электр станцияларды жобалау, қалыпты күйге келтіру және пайдалану кезінде олардың жұмыс режимін жылдам әрі түсінікті зерттеуге немесе болжауға мүмкіндік береді.

Программалық жасақтаманы объектілік іске асыру негізі ретінде математикалық объектілер, объектілердің есептегіш алгоритмдері және ауыспалы процесстердің модельдеу алгоритмі қарастырылады.

Математикалық объект қандай да бір математикалық санатты және есептеу объектінің құраушысын айқындайтын мәні болып табылады. Объектілер ретінде энергия жүйесінің элементтері, векторлар және матрицалар қарастырылады. Әр математикалық объектілерде математикалық белгілер жиынтығы бар, алайда олар өздігінен есептік мәселе болып табылмайды және оны шешу үшін аспапты құрал болып табылады.

Класстарды іске асыру кезінде тәсілдер деректердің әр құрылымына байланады, ал олардың виртуальдық қолданылуы дерексіз деңгейге ауысады. Бұндай жағдайда

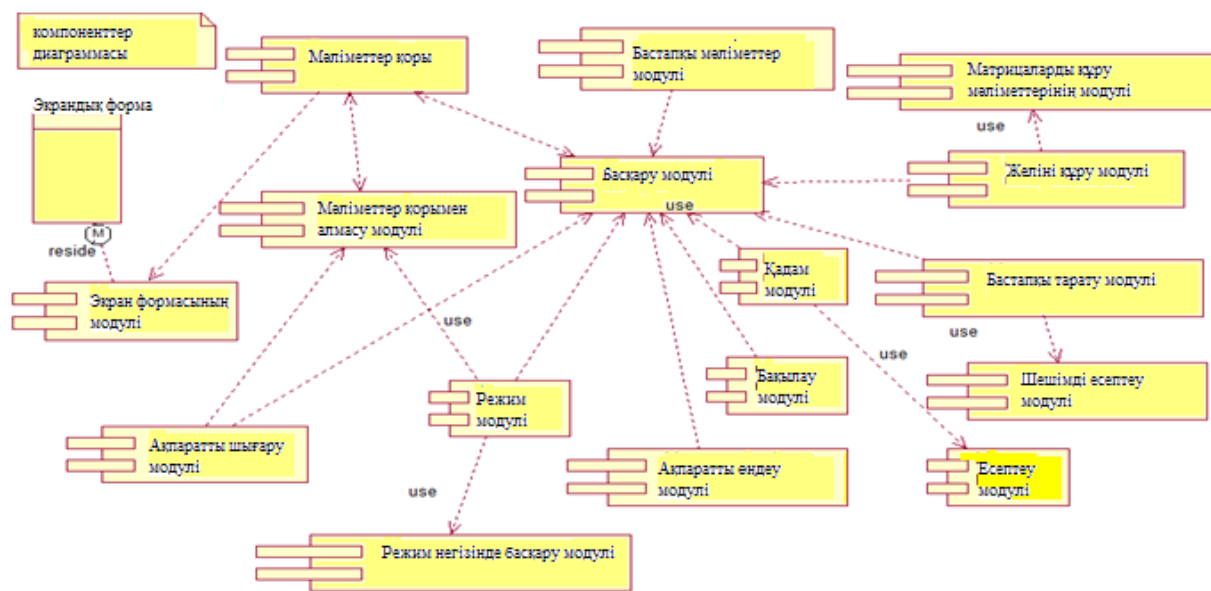
виртуалдық тәсілдердің шақыруын пайдаланып, класстық сатылықтың ең жоғарғы деңгейлерінде көрсеткіштер бойынша жүзеге асырылатын күрделі ұйымдасқан есептегіш процесстер базалық класстың объектілеріне шын мәнінде көрсететін объектілерге сол класстардың тәсілдері шақыртылады.

Объектілердің есептеу алгоритмдері деп алгоритмдік пайдаланудың шарттарын анықтайтын есептегіш математика мен көмекші ақпараттың тәсілдерін айтады. Әр алгоритм бір мәселені шешуге арналған. Ауыспалы үрдісті үлгілеу алгоритмі қарапайым жағдайда есептеу алгоритмдеріндегі тізбектелген шақырулардың сценарийі болып табылады. Алгебралық және дифференциалдық теңдеулер жүйесін шешу алгоритмінің шақыруынан тұрады, сонымен қатар, ағымдағы есептік жағдайдағы қолданылатын есептік алгоритмнің тиімділігі мен дұрыстығын қадағалайды.

Деректердің динамикалық құрылымдарымен, сонымен қатар деректердің бір өлшемді және екі өлшемді алаптарымен жұмысты орындайтын класстар сәйкес жалпыланған класстар түрінде рәсімделеді, ол оларды қолданбалы программаның пәндік үлгілерінде пайдалануға мүмкіндік береді. Векторлар мен матрицалардың класстары ЭЭЖ элементтерінің сипаттамалары туралы ақпаратты сақтау үшін арналған. Осы класстардың интерфейстері қайта жүктелетін операторлардың үлгісіндегі тәсілдер жиынтығы болып табылады. Динамикалық алаптардың классы кез келген өлшемді элементтер мәнін сақтауды жүзеге асырады және өлшемділіктің өзгеру, толтыру, сұрыптау және меңгеру тәсілдерін орындайды. Векторлар классы динамикалық алаптардың барлық қасиеттеріне ие және сызықты алгебраның операцияларын анықтайды. Екі өлшемді матрицаның классы қосымша анықтауышты есептеуді және кері матрицаны алуды орындайды.

Алгоритмдердің класстары объектілердің дұрыстығын тексеру және олардың арасындағы қажетті байланыстарды орнату, сонымен қатар, есептерді шешу қадамдарын басқару және операциялардың кезектілігін анықтау үшін арналған.

Сценарийлер ауыспалы үрдістің алгоритмдерін сәйкес класстардың виртуалдық тәсілдерін кезектеп шақырту жолымен жүзеге асырылады. Құрылымдық-функционалдық алгоритмнің сызбасы 5 суретте көрсетілген.



Сурет 5 - Құрылымдық-функционалдық алгоритмнің сызбасы

Жүйеде функционалдық тағайындалуына сәйкес үш жүйеге бөлінген: бастапқы деректерді дайындау жөніндегі жүйе, есепті басқару жөніндегі жүйе, алынған деректерді көзбен шолу және талдау жүйесі. Жүйелер 6 суретте ұсынылған келесі құраушылардан тұрады [3-5,7].

1. Деректерді дайындаудың жүйесі. Белгіленген режимдегі параметрлердің бастапқы мәндерін анықтау және энергия жүйесінің үлгілерін анықтау.

– Белгіленген режим негізінде бастапқы мәндерді беру.

– Энергия жүйесінің элементтерін олардың үлгілерімен және коэффициенттерімен беру.

– Ауыспалы үрдісті үлгілеу сценарийін беру.

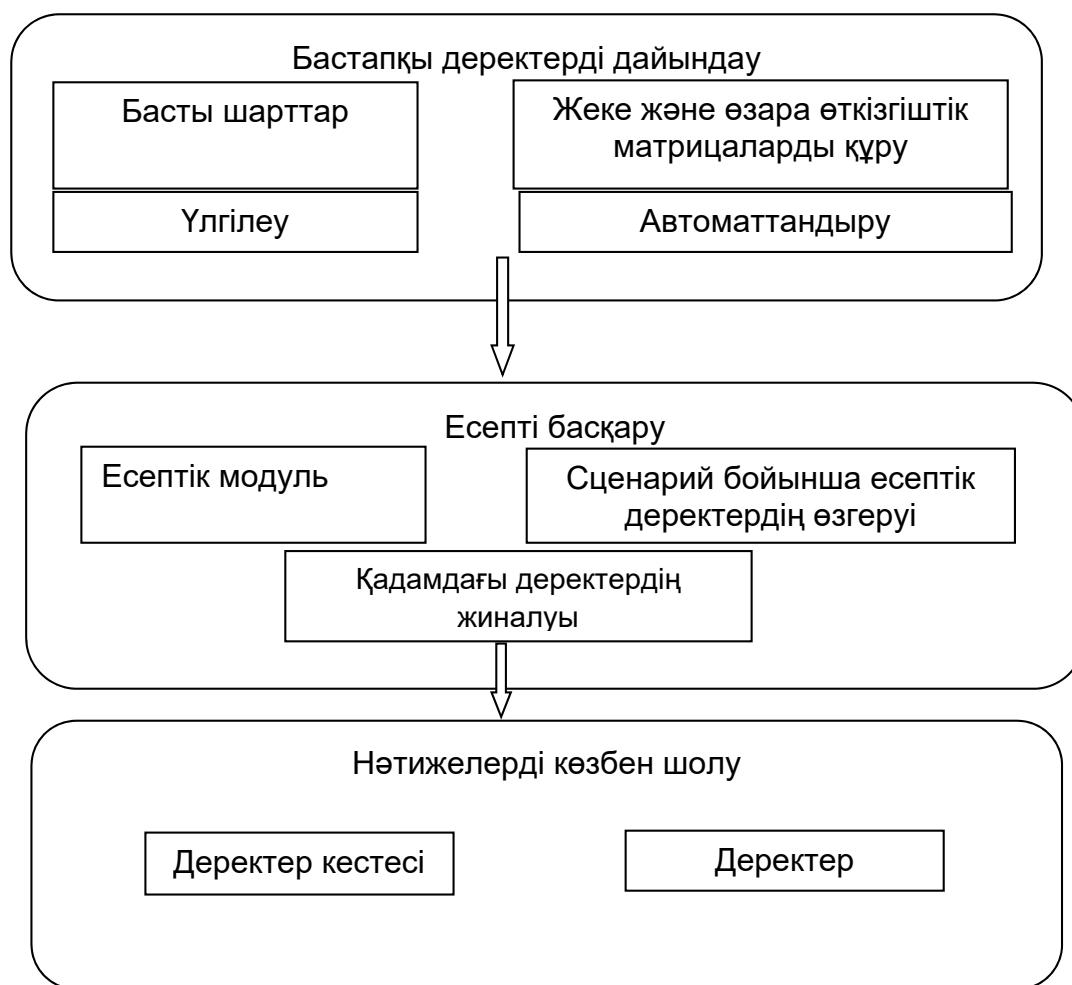
– Осы сценарийлерді іске қосу үшін апатқа қарсы автоматика мен бақыланатын параметрлер

2. Үлгілеу үрдісін басқару жүйесі.

– Берілген үлгілеу сценарийіне сәйкес интегралдау қадамындағы өзгерістерді енгізуге рұқсат беріледі.

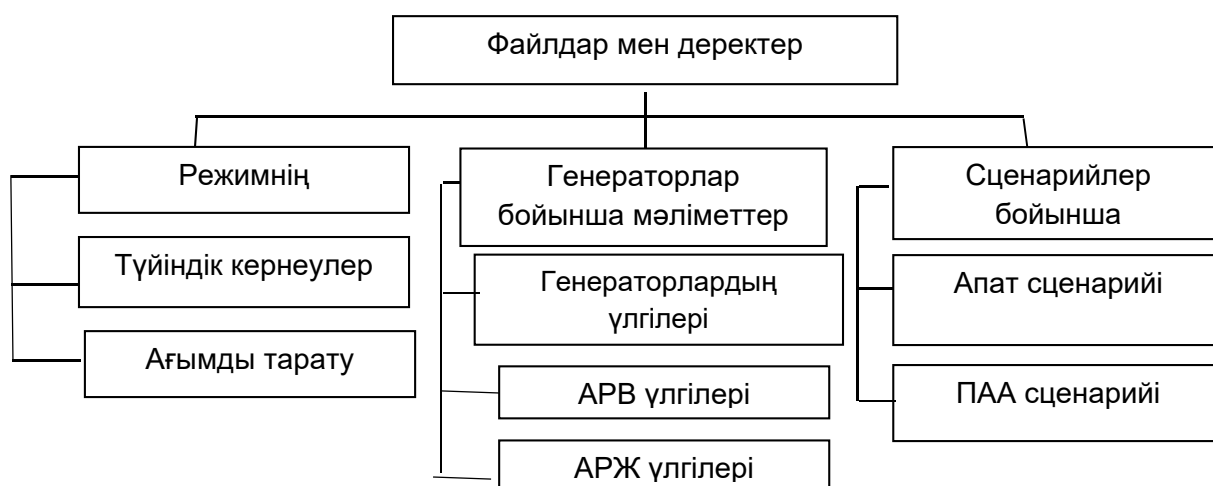
– Бақыланатын мәндердің өзгеру шарты бойынша апатқа қарсы автоматика сценарийлерін іске қосуға рұқсат беріледі.

3. Нәтижелерді көзбен шолу жүйесі. Динамикалық орнықтылықты талдау үшін таңдалған жиынтықтарды кесте және графика түрінде ұсыну[6,7].



Сурет 6 – ақпараттық жүйенің функционалдық жүйесі

Электромеханикалық ауыспалы процесстерді сандық үлгілеу үшін қажетті деректер жиынтығы 7 суретте көрсетілген. Енгізілетін және есептік деректер редакциялауға және басып шығаруға болатын SQL-сервердің деректер қорында сақталады. Деректер қорында басты қондырғылар бекітіледі: есептік сызба күйі, электр жабдықтың параметрлері, стандартты тағайындалуы, есептік шарттар, хабарламалар және т.б. бойынша. Сценарий файлы есеп үшін, соның режимдері, генераторлары, апатқа қарсы автоматика ауытқуы мен жұмысы бойынша деректер жиындарының атауларына қажетті ақпараттан тұрады [8-10].



Сурет 7 – деректерді таңдау

Қорытынды

Бұл мақалада электр энергетикалық жүйелердің тұрақтылығы үшін ақпараттық жүйелерінің модельдік құрылымын қолдану мен іс жүзінде іске асыру жолдары қарастырылған. Сонымен қатар заманауи үлгідегі ИС сипаттамасы әзірленген және ЭЭЖ тұрақтылығын зерттеу үшін бағдарламалық қамтамасыз ету жолдары көрсетілген. Осы жүйені дамыту негізінде иерархиялық механизм ұсынылып және параллель ұсынымы АЖ есеп айырысу схемасы берілген. Жұмыс істеудің модульдік құрылымы, сонымен қатар шығу, кіру мәліметтері, ақпаратты өңдеу және басқару; негізгі ЭЭЖ-нің ақпараттық ішкі жүйесі, мәліметтерді дайындаудың ішкі жүйесі, есеп айырысуды басқарудың ішкі жүйесі, алынған мәліметтерді визуализациялау немесе талдаудың ішкі жүйесі мен мәліметтер мен файлдар схемасы қарастырылып, модельдік электромеханикалық процесне ауысу барысы жөніндегі схемалар көрсетілген.

Пайдаланылған әдебиеттер

1 А.Б. Осақ, Е.Я.Бузина Анализ эффективности автоматических и автоматизированных систем управления в электроэнергетике // 5-ая Международная научно-практическая конференция "Современные направления развития систем релейной защиты и автоматики энергосистем" - Сочи. 2015.

2 Maksat N. Kalimoldayev, Assel A. Abdildayeva, Orken Zh. Mamyrbayev, and Maksat Akhmetzhanov Information system based on the mathematical model of the EPS // Open Engineering. Volume 6, Issue 1, ISSN (Online) 2391-5439, DOI: 10.1515/eng-2016-0053, 2016. P. 464–469

- 3 Калимолдаев М.Н., Абдилдаева А.А., Мамырбаев О.Ж. Элементы функционирования информационной системы для электроэнергетических систем // ВЕСТНИК КазНУ. №2 (114) – 2016. – С.132-136.
- 4 Попов Д.Б. Разработка и реализация информационно-вычислительной системы для исследования динамической устойчивости электроэнергетических систем. // Вычислительные технологии. Т.13. 2008. -С. 59-68.
- 5 М.Н. Калимолдаев, Абдилдаева А.А., О.Ж. Мамырбаев, Г.А. Амирханова Проектирование информационной системы для исследования устойчивости электроэнергетических систем // Матер. науч. конф. ИИВТ МОН РК «Современные проблемы информатики и вычислительных технологий». – Алматы, 2015. – С.67-73.
- 6 Попов Д.Б. Разработка программного обеспечения в научных подразделениях // Компьютерное моделирование – 2007: Тр. Междунар. научно-техн. конф., СПб.: Изд-во Политехн. ун-та, 2007. С. 250-258.
- 7 Маклаков С.В. BPWin и ERWin. CASE-средства разработки информационных систем. М.: ДИАЛОГ-МИФИ, 2000.
- 8 Калимолдаев М. Н., Кулпешов Б. Ш., Мамырбаев О. Ж., Абдилдаева А.А. Электр-энергетикалық комплекстің тұрақтылық жұмысының ақпараттық жүйесін құру // Международная научно-практическая конференция «Научная дискуссия: инновации в современном мире». – 2016. №4(47) Часть 2. – С.2015-212.
- 9 Калимолдаев М.Н., Абдилдаева А.А., Ахметжанов М.А., Сақыпбекова М.Ж. Электрэнергетикалық жүйесіне ақпараттық жүйе құру // Вестник КазНПУ имени Абая, серия «Физико-математические науки». №1(53). – 2016. – С.190-196
- 10 Калимолдаев М.Н., Абдилдаева А.А., Мамырбаев О.Ж., Дузбаев Т., Тойбаева Ш.Ж., Галиева Ф.М. Разработка информационной системы для электроэнергетических систем // Проблемы информатики – Новосибирск, 2016. – №4. – С.57-72.

ЭЛЕКТРОЭНЕРГЕТИКАЛЫҚ ЖҮЙЕЛЕР ҚОЗҒАЛЫСЫН ТҰРАҚТАНДЫРУ

Калимолдаев М.Н., Ахметжанов М.А., Галиева Ф.М.
maks714@mail.ru

*Институт информационных и вычислительных технологий КН МОН РК,
Казахстан*

Андатпа. Берілген жұмыста қозғалысты басқару теориясының актуалды есебі қарастырылған, атап айтқанда, фазалық жүйелер тұрақтандыру. Математикалық модельдеу негізінде тұрақтылықтың теориялық нәтижелерін алу. Компьютерлік модельдеу, яғни тұрақтылық есепін шешу және бағдарламалық іске асыру. көпөшемді фазалық жүйелердің қозғалыс заңдылықтарын тұрақтылығы мен тұрақтандыру, атап айтқанда электр энергетикалық жүйелердің тұрақтылық есебінің компьютерлік модельдеуі мен қолданылған сандық әдістер, сонымен оларды салыстырулар көрсетілген. Көп қадамды сандық әдіс негізінде Адамс-Бэшфорд және Адамс-Моултонның 4-ші ретті әдістері қолданылды. Әдістерге қысқаша сипаттама берілген.

Кіріспе. Белгілі болғандай, перспективалық бағыттардың бірі болып табылатын басқару теориясы заманауи тәжірибе мен технологиялардың сұраныстарынан пайда болды. Заманауи қоғамның индустриалды дамуы электр-энергия тұтынуының өсуіне әкеліп соғуда. Қазіргі уақытта әлемде триллиондаған киловатт-сағат электр энергиясы өндірілуде. Электр-энергетикалық жүйелер (ЭЭЖ) өндіріске, транспортқа, жарықтандыруға және ақпарат жіберуге, халықтың тұрмысына қажетті электр қуатын өндіреді.

Зерттеу өзектілігі генераторлар және көпбайланысты энергетикалық объекттерден тұратын күрделі электр-энергетикалық орнықтылығын, Т-орнықтылығын қамтамасыз ету және басқару қиындығымен анықталады.

Оң жақ бөлігі бұрыштық координатамен периодты болатын дифференциалдық теңдеумен сипатталатын көпөлшемді фазалық жүйелер моделі қозғалысының тұрақтылығы зерттелді.

Есептің қойылымы.

$Z_i^{n_i+2}(\delta_i, S_i, x_i), i = \overline{1, n}$; цилиндрлі фазалық кеңістікте динамикалық жүйені қарастырамыз, ол i -ші оқшауланған ішкі жүйе үшін $(n+2)$ -ші ретті дифференциалдық теңдеумен сипатталады

$$\frac{d\delta_i}{dt} = S_i, \frac{dS_i}{dt} = w_i - K_i S_i - f_i(\delta_i), w_i = C_i x_i, \quad (1.1)$$

$$\frac{dx_i}{dt} = A_i x_i + q_i S_i + b_i u_i + R_i(S_i, x_i), \quad (1.2)$$

$\ell = 2$ (екі синхронды генератор) кезінде электроэнергетикалық жүйелер қозғалысын тұрақтандыруды қарастырайық. Онда (1.79) және (1.80) теңдеулері жүйенің жұмысын сипаттайды, ал (1.81) және (1.82) теңдеу реттегіштің жағдайын сипаттайды.

$$\frac{d\delta_1}{dt} = S_1, \quad (1.79)$$

$$\frac{dS_1}{dt} = c_1 x_1 - K_1 S_1 - f_1(\delta_1) - P_{12},$$

$$\frac{d\delta_2}{dt} = S_2,$$

$$\frac{dS_2}{dt} = c_2 x_2 - K_2 S_2 - f_2(\delta_2) - P_{12}, \quad (1.80)$$

$$\frac{dx_1}{dt} = A_1 x_1 + u_1, \quad (1.81)$$

$$\frac{dx_2}{dt} = A_2 x_2 + u_2, \quad (1.82)$$

мұндағы x_1, x_2 – фазалық айнымалылар; C_1, C_2 – скалярлар; u_1, u_2 – басқару;

$$A_1 = A_2 = -39.81 \cdot 10^{-4};$$

$$\begin{aligned}
K_1 &= K_2 = 66.7 * 10^{-4}; \\
\Gamma_0 &= 1.513 * 10^{-4}; \\
\theta_0 &= 0.3562; \\
c_1 &= c_2 = 4.167 * 10^{-8}; \\
\theta_1 &= -0.001; \theta_2 = -0.001; \\
a_1 &= -0.001; a_2 = -0.001; \\
H_1 &= H_2 = 0.61 * 10^{-6}; \\
\Gamma_1 &= 0.06 * 10^{-4}; \\
f_1 &= \Gamma_0(\sin(\delta_1 + \theta_0) - S_1); f_2 = \Gamma_0(\sin(\delta_2 + \theta_0) - S_2); \\
P_{12} &= \Gamma_1((\delta_1 + \delta_2 + 2\theta_0) - S_2).
\end{aligned}$$

Бастапқы шарт:

$$\begin{aligned}
\delta_{10} &= 1.34; \delta_{20} = 0.84; \\
S_{10} &= 0.0; S_{20} = 0.0; \\
x_{10} &= 0.001; x_{20} = 0.001;
\end{aligned}$$

теореманың барлық шарттары тексерілген.

$$\frac{d\delta}{dt} = S, \quad \frac{dS}{dt} = w - KS - f(\delta) - \psi(\delta_*), \quad w = C^*x, \quad (1.83)$$

$$\frac{dx}{dt} = Ax + qS + bu + e\phi(\sigma), \quad \sigma = g^*x + \gamma S, \quad (1.84)$$

(1.79)-(1.82) теңдеулер жүйесін шешу үшін 4-ші ретті Рунге-Кутта әдісін және Эйлер әдістерін пайдаланымыз.

δ_1 және δ_2 бұрыштық координата үшін:

$$\begin{aligned}
\delta_{1i} &= \delta_{1i-1} + \Delta t S_{1i-1}, \\
\delta_{2i} &= \delta_{2i-1} + \Delta t S_{2i-1},
\end{aligned}$$

S_1 бұрыштық жылдамдық үшін:

$$\begin{aligned}
S_{1i} &= S_{1i-1} + \frac{1}{6}(m_1 + 2m_2 + 2m_3 + m_4), \\
m_1 &= \Delta t F(S_{1i-1}), \\
m_2 &= \Delta t F(S_{1i-1} + \frac{1}{2}m_1), \\
m_3 &= \Delta t F(S_{1i-1} + \frac{1}{2}m_2), \\
m_4 &= \Delta t F(S_{1i-1} + m_3),
\end{aligned}$$

мұндағы

$$F(S_{1i-1}) = c_1 x_{1i-1} - K_1 S_{1i-1} - f_1(\delta_{1i-1}) - P_{12},$$

$$f_1(\delta_{l_{i-1}}) = \Gamma_0(\sin(\delta_{l_{i-1}} + \theta_0) - S_{l_{i-1}});$$

S_2 бұрыштық жылдамдық үшін:

$$S_{2_i} = S_{2_{i-1}} + \frac{1}{6}(l_1 + 2l_2 + 2l_3 + l_4),$$

$$l_1 = \Delta t F(S_{2_{i-1}}),$$

$$l_2 = \Delta t F(S_{2_{i-1}} + \frac{1}{2}l_1),$$

$$l_3 = \Delta t F(S_{2_{i-1}} + \frac{1}{2}l_2),$$

$$l_4 = \Delta t F(S_{2_{i-1}} + l_3),$$

мұндағы

$$F(S_{2_{i-1}}) = c_2 x_{2_{i-1}} - K_2 S_{2_{i-1}} - f_2(\delta_{2_{i-1}}) - P_{12},$$

$$f_2(\delta_{2_{i-1}}) = \Gamma_0(\sin(\delta_{2_{i-1}} + \theta_0) - S_{2_{i-1}});$$

x_1 үшін:

$$x_{1_i} = x_{1_{i-1}} + \frac{1}{6}(k_1 + 2k_2 + 2k_3 + k_4),$$

$$k_1 = \Delta t F(x_{1_{i-1}}),$$

$$k_2 = \Delta t F(x_{1_{i-1}} + \frac{1}{2}k_1),$$

$$k_3 = \Delta t F(x_{1_{i-1}} + \frac{1}{2}k_2),$$

$$k_4 = \Delta t F(x_{1_{i-1}} + k_3),$$

мұндағы $F(x_{1_{i-1}}) = A_1 x_{1_{i-1}} + u_{1_{i-1}},$

x_2 үшін:

$$x_{2_i} = x_{2_{i-1}} + \frac{1}{6}(n_1 + 2n_2 + 2n_3 + n_4),$$

$$n_1 = \Delta t F(x_{2_{i-1}}),$$

$$n_2 = \Delta t F(x_{2_{i-1}} + \frac{1}{2}n_1),$$

$$n_3 = \Delta t F(x_{2_{i-1}} + \frac{1}{2}n_2),$$

$$n_4 = \Delta t F(x_{2_{i-1}} + n_3),$$

мұндағы $F(x_{2_{i-1}}) = A_2 x_{2_{i-1}} + u_{2_{i-1}}, \Delta t - t$ бойынша қадам.

Көпқадамды әдістер Рунге-Кутта және де Эйлер әдістеріне қарағанда әлдеқайда нақты мәндерді алуға мүмкіндік береді. Эйлер әдісі шешімнің дұрыстығын тексеруге мүмкіндік береді.

Адамс-Башфорд әдісі бірінші ретті қарапайым дифференциалдық теңдеулерді сандық интегралдаудың шекті көпқадамды әдісі болып табылады. Рунге-Кутта әдісіне қарағанда алдыңғы нүктелерде есептелген шешімнің бір емес бірнеше шекті мәндерін есептеу үшін қолданылады.

Кесте 1 – Әр түрлі реттегі Адамс-Бешфорд формулалары

Реті	Формуласы	Қателік реті
1	$y_{n+1} = y_n + hf_n$	$\frac{h^2}{2} y''(\eta)$
2	$y_{n+2} = y_{n+1} + \frac{h}{2}[3f_{n+1} - f_n]$	$\frac{5h^3}{12} y'''(\eta)$
3	$y_{n+3} = y_{n+2} + \frac{h}{12}[23f_{n+2} - 16f_{n+1} + 5f_n]$	$\frac{3h^4}{8} y^{(4)}(\eta)$
4	$y_{n+4} = y_{n+3} + \frac{h}{24}[55f_{n+3} - 59f_{n+2} + 37f_{n+1} - 9f_n]$	$\frac{25h^5}{720} y^{(5)}(\eta)$
5	$y_{n+5} = y_{n+4} + \frac{h}{720}[190f_{n+4} - 277f_{n+3} + 261f_{n+2} - 127f_{n+1} + 25f_n]$	$\frac{95h^6}{2880} y^{(6)}(\eta)$

Кесте 2 – Әр түрлі реттегі Адамс-Моултон формулалары

Реті	Формуласы	Қателік реті
1	$y_{n+1} = y_n + hf_{n+1}$	$-\frac{h^2}{2} y''(\eta)$
2	$y_{n+2} = y_{n+1} + \frac{h}{2}[f_{n+2} - f_{n+1}]$	$-\frac{h^3}{12} y'''(\eta)$
3	$y_{n+3} = y_{n+2} + \frac{h}{12}[5f_{n+3} + 8f_{n+2} - f_{n+1}]$	$-\frac{h^4}{24} y^{(4)}(\eta)$
4	$y_{n+4} = y_{n+3} + \frac{h}{24}[9f_{n+4} + 19f_{n+3} - 5f_{n+2} + f_{n+1}]$	$-\frac{19h^5}{720} y^{(5)}(\eta)$
5	$y_{n+5} = y_{n+4} + \frac{h}{720}[25f_{n+5} + 64f_{n+4} - 26f_{n+3} + 10f_{n+2} - 19f_{n+1}]$	$-\frac{3h^6}{160} y^{(6)}(\eta)$

Бұдан да нақтырақ нәтижелерді алу үшін 1 және 2 кестелеріндегі 4-ші ретті Адамс-Башфорд, Адамс-Моултон әдістерін қолданамыз.

Адамс-Башфорд әдісі:

$$y_{n+4} = y_{n+3} + \frac{h}{24}(55f(t_{n+3}, y_{n+3}) - 59f(t_{n+2}, y_{n+2}) + 37f(t_{n+1}, y_{n+1}) - 9f(t_n, y_n)), \quad \frac{251}{720} h^5(\eta)$$

Адамс-Моултон әдісі:

$$y_{n+4} = y_{n+3} + \frac{h}{24}(9f(t_{n+4}, y_{n+4}) + 19f(t_{n+3}, y_{n+3}) - 5f(t_{n+2}, y_{n+2}) + f(t_{n+1}, y_{n+1})), \quad -\frac{19}{720} h^5(\eta).$$

және де 4-ші ретті Рунге-Кутта әдісін қолданамыз:

$$y_{n+1} = y_n + \frac{h}{6}(k_1 + 2k_2 + 2k_3 + k_4),$$

мұндағы

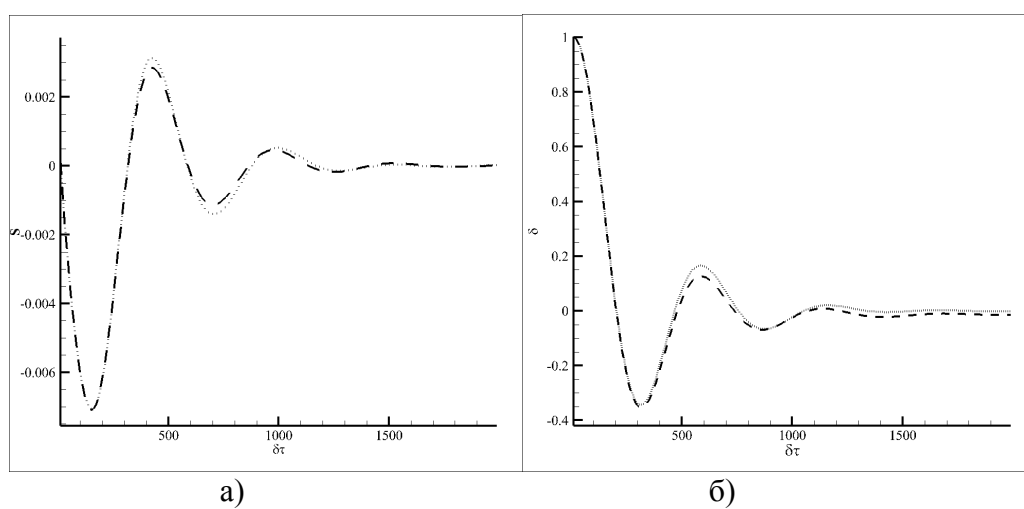
$$k_1 = f(t, y),$$

$$k_2 = f\left(t + \frac{h}{2}, y + \frac{hk_1}{2}\right),$$

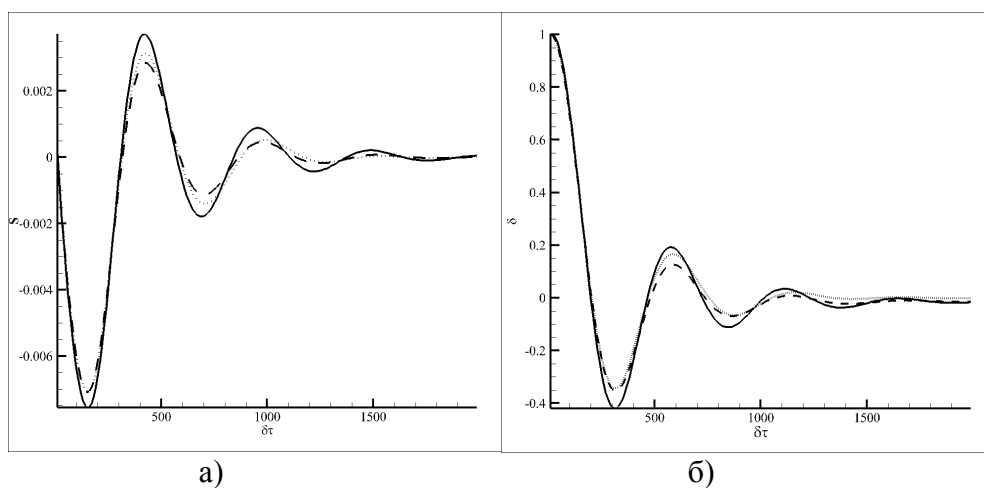
$$k_3 = f\left(t + \frac{h}{2}, y + \frac{hk_2}{2}\right),$$

$$k_4 = f(t + h, y + hk_3).$$

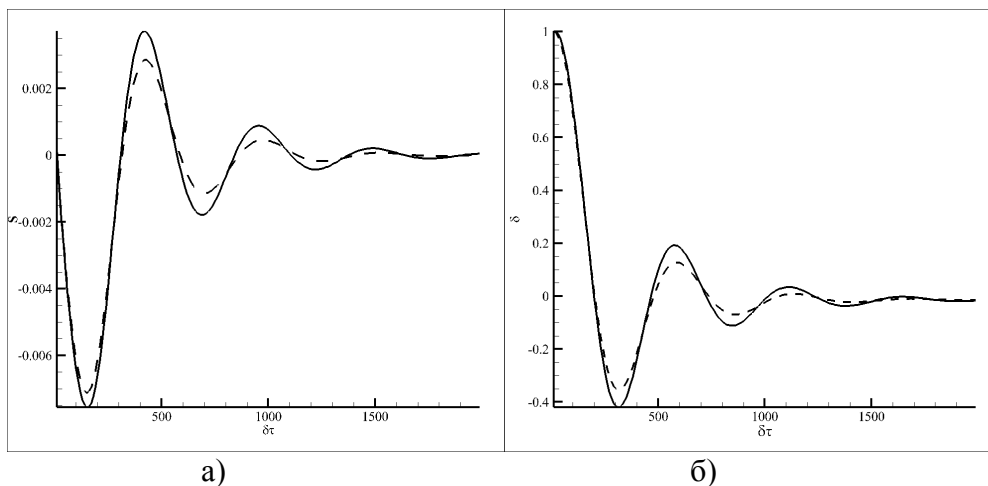
Қолданылған әдістерді салыстыру нәтижелерін төмендегі суреттерден көруге болады:



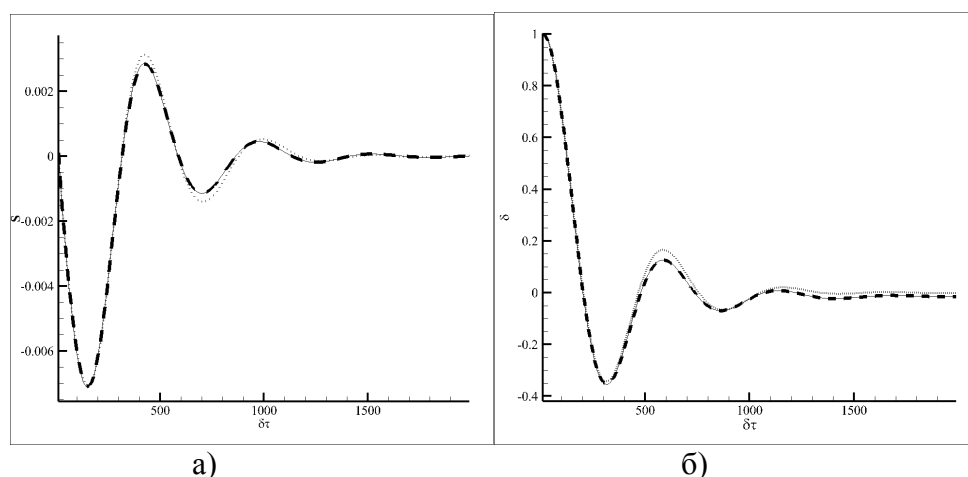
Сурет 1- а) S -н уақыт бойынша өзгеруі; б) δ -н уақыт бойынша өзгеруі
4-ші ретті А-Б (- - -сызығы), А-М ($\cdots$ сызығы) әдістері



Сурет 2 - а) S -н уақыт бойынша өзгеруі; б) δ -н уақыт бойынша өзгеруі
4-ші ретті А-Б (- - -сызығы), А-М ($\cdots$ сызығы) және Эйлер (-сызығы) әдістері



Сурет 3 - а) S -н уақыт бойынша өзгеруі; б) δ -н уақыт бойынша өзгеруі
Р-К (- - -сызығы) және Эйлер (- сызығы) әдістері



Сурет 4 - а) S -н уақыт бойынша өзгеруі; б) δ -н уақыт бойынша өзгеруі
4-ші ретті А-Б (- - -сызығы), А-М ($\cdots$ сызығы) және Р-К (-сызығы) әдістері

Қорытынды. Алынған нәтижелерден график сызығы барлық суретте де нольге ұмтылатындықтан 4-ші реттен жоғары ретін қарастырудың қажет еместігін көруге болады. Берілген есеп үшін Адамс-Башфорд және Рунге-Кутта әдістерінде Адамс-Моултон әдісіне қарағанда нольге жылдамырақ ұмтылады. Бұл апаттық жағдайды анықтау процесін жиламдатуға және уақытысын азайтуға мүмкіндік береді. Адамс-Моултон әдісі айқын емес әдіс болып табылады және «тарихи» мәндерді анықтауды талап етеді.

Пайдаланылған әдебиеттер

1. Kalimoldayev M.N., Abdildayeva A.A., Mamyrbayev O.Zh., Akhmetzhanov M.A. Information system based on the mathematical model of the EPS // Open Engineering, ISSN (Online) 2391-5439, DOI: 10.1515/eng-2016-0053. – 2016. – Vol. 6, issue 1. – P. 464–469.

2. Калимолдаев М.Н., Дженалиев М.Т., Абдилдаева А.А., Ахметжанов М.А. Об устойчивости фазовых систем при постоянно действующих возмущениях // Вестник КазНУ. – 2016. – №2 (114). – С. 413.

3. Калимолдаев М.Н., Сақыпбекова М.Т., Абдилдаева А.А., Ахметжанов М.А. Электр энергетикалық жүйесіне ақпараттық жүйе құру // Вестник КазНУ. – 2016. – №1(53). – С. 190.

4. Калимолдаев М.Н., Абдилдаева А.А., Мамырбаев О.Ж., Ахметжанов М.А. Информационная система на основе математической модели ЭЭС // Матер. Межд. науч. конф. ИИВТ МОН РК «Современные проблемы информатики и вычислительных технологий». – Алматы, 2016. – С.142-153.

ОСНОВЫ АРХИТЕКТУРЫ ПРОГРАММНЫХ СИСТЕМ ДЛЯ ОСУЩЕСТВЛЕНИЯ ТИПИЗИРОВАННОГО АТРИБУТНОГО РАЗГРАНИЧЕНИЯ ДОСТУПА

Калимолдаев М.Н., Бияшев Р.Г., Рог О.А.
e-mail: mnk@ipic.kz, brg@ipic.kz, olga@ipic.kz

*Институт информационных и вычислительных технологий КН МОН РК,
Казахстан*

Аннотация. *Определены понятия и предложены принципы конструирования архитектуры программных систем для осуществления разграничения доступа привилегированных субъектов к защищаемым объектам на основе оценки их атрибутов безопасности. Обработка атрибутов производится в соответствии с концепцией типизированного атрибутного разграничения доступа и его многоуровневой модели, для которой получены формальные языковые представления в виде алгебраической и логической систем на мета и объектном уровнях. В зависимости от уровня определения, данные формальные языки служат для описания архитектуры программных систем, а также являются языками спецификации различных политик типизированного атрибутного разграничения доступа. Дано определение программной системы, способной одновременно реализовать ряд моделей разграничения доступа, как программы на этих языках. Определен состав, принципы конструирования и стадии функционирования системы, перечислены функции составляющих ее модулей.*

1. Введение

В современном мире, где огромное количество информации хранится в разнообразных источниках, имеет место тенденция к объединению вычислительных устройств и их сетей в вычислительные среды – интегрированные распределенные компьютерные системы для решения задач в различных проблемных областях. Вычислительные среды могут состоять из традиционных локальных и региональных сетей, быть организованными на основе веб-сервисов, содержать зоны для специализированных устройств. Эта смешанная вычислительная среда требует применения различных политик разграничения доступа к различным классам объектов данных, решая при этом проблему авторизации для большого числа субъектов и

объектов, обладающих многочисленными признаками, которые необходимо учитывать при организации защиты.

Как правило, существующие политики безопасности обеспечивают разграничение доступа по одному критерию, будучи к тому же привязанными к определенным системам. Например, широко применяемая в настоящее время модель DAC (дискреционного разграничения доступа) управляет доступом на основе идентификаторов сущностей, модель MAC (мандатного разграничения доступа) основывается на уровнях конфиденциальности субъекта и объекта, а модель RBAC (ролевого разграничения доступа) предоставляет доступ в соответствии с группами привилегий пользователей.

Использование одной политики, которая не в состоянии учесть разнообразные параметры сущностей, приводит к избыточности прав доступа, возможности утечки привилегий к неавторизованным пользователям, способствует снижению уровня безопасности информационных систем.

Для преодоления существующих недостатков, исследователи ведут интенсивную работу по созданию новых методов разграничения доступа, решая при этом следующие задачи:

1. разработки новых моделей разграничения доступа, учитывающих сразу несколько признаков субъекта и объекта при принятии решения о доступе в соответствии с данной политикой безопасности;
2. решения вопросов о возможности применения ряда политик в рамках одной системы в целях одновременного учета нескольких критериев разграничения доступа;
3. создания средств динамического создания новых политик;
4. конструирования настраиваемых программных систем, объединяющих и применяющих одновременно ряд моделей разграничения доступа.

Для решения первой задачи в последнее время интенсивно разрабатываются атрибутно-ориентированные модели разграничения доступа (Attribute-based Access Control - ABAC), которые основаны на представлении сущностей – субъектов, объектов, операций и вычислительной среды – наборами их атрибутов [1-3].

Атрибуты выражают свойства сущностей, необходимые для организации процесса разграничения доступа, такие как идентификаторы в модели DAC, уровни конфиденциальности в модели MAC, роли (RBAC), а также многие другие признаки – организационная и тематическая принадлежность, расположение, должность, дата, квалификация и т.д.

Доступ субъекта к объекту предоставляется на основе **политики атрибутного разграничения доступа**, представленной набором правил вычисления и оценки значений атрибутов. Хотя ABAC обладает возможностью гибкого конфигурирования разнообразных политик разграничения доступа, включая традиционные, обеспечивая при этом однозначную идентификацию сущностей их атрибутами, его основным недостатком является сложность администрирования и вычисления значений разнородных атрибутов. При этом отмечается необходимость создания формальных моделей и языков описания политик атрибутного разграничения доступа, в том числе моделей с настраиваемыми характеристиками.

Решению задач 2-4 посвящены такие работы как [3-6] и др. Они содержат описания разработок различных языков спецификации политик разграничения доступа и создания соответствующих моделей, пытаясь так или иначе решить проблему сложности вычисления атрибутов сущностей. Описываются фреймворки, создаваемые как инструменты для формирования моделей и языков.

В данной статье описываются принципы конструирования систем разграничения доступа на основе подхода, предлагаемого авторами к решению вышеперечисленных задач [7-13].

Дано определение типизированного атрибутного разграничения доступа (ТАРД), которое отличается от АВАС тем, что атрибуты безопасности сущностей принадлежат определенным типам. Тип атрибута задается в виде математического объекта – частично упорядоченного множества с набором определенных на нем операций. Решение о возможности доступа принимается на основе обработки однотипных атрибутов пары субъект-объект. Типизация дает разные виды структуризации пространства атрибутов, предоставляя возможность реализовывать различные политики безопасности.

Построена модель ТАРД, основанная на понятии типа атрибута, которая служит механизмом разграничения доступа. Задачей модели является типизация сущностей. Она заключается в присвоении им значений атрибутов, образующих их метки безопасности, и манипулировании значениями однотипных атрибутов с целью определения возможности доступа субъектов к объектам.

ТАРД, наряду с гибкостью формулирования политик безопасности, допускает групповую обработку атрибутов, дает ускорение и упрощение вычисления, облегчает процесс администрирования систем, осуществляющих типизированное атрибутное разграничение доступа.

Разработана многоуровневая модель ТАРД. На мета-уровне она представляет собой абстрактный тип T атрибутов, выполняющий роль фреймворка для конструирования конкретных моделей разграничения доступа объектного уровня. Одновременное использование полученных моделей в рамках одной системы обеспечивает разграничение доступа по ряду критериев.

С целью построения программных систем, осуществляющих типизированное атрибутное разграничение доступа, разработано двойное представление модели как типа атрибутов T . Алгебраическое представление в виде домена типа и операций, определенных на нем, порождает денотационную семантику модели. Представление типа в виде логической системы, имеющей в своем составе дедуктивный аппарат, служит средством вычисления семантических значений и позволяет управлять безопасностью процесса разграничения доступа, используя средства логического вывода.

На основе вышеперечисленных положений, предложено многоуровневое определение системы типизированного атрибутного разграничения доступа (СТАРД) как программы на языке T . При этом метаязык служит языком описания ее архитектуры, а объектные языки являются спецификациями политик ТАРД, получаемых в результате интерпретации метаязыка. Описана архитектура программной системы, реализующей СТАРД – ее состав и назначение ее модулей, а также выполняемые ими функции.

2. Теоретические основы построения систем типизированного атрибутного разграничения доступа

Определим предметную область разграничения доступа, или ее субъектно-объектную модель, как фиксированную совокупность сущностей, состоящую из множеств субъектов и объектов, их свойств и взаимосвязей между ними, имеющих отношение к организации защищенного доступа к информации.

Суть вышеупомянутого атрибутно-ориентированного метода разграничения доступа АВАС заключается в управлении процессом разграничения доступа на основании конечных множеств свойств, или атрибутов его участников. Проблема идентификации субъектов и объектов их свойствами заключается в том, чтобы, с одной стороны, свойств было достаточно для обеспечения различимости сущностей системой

разграничения доступа. С другой стороны, увеличение количества свойств значительно повышает сложность и время их обработки.

Впервые подход к решению вопроса о вычислимости большого числа атрибутов, заключающийся в использовании множества атрибутов с алгебраическими операциями в качестве структур данных для спецификации политик атрибутного разграничения доступа, был предложен в [3].

Развивая этот подход, с целью структуризации пространства признаков и упорядочения вычисления их значений, авторы вводят понятие типа T атрибутов, определение которого дается в виде математического объекта – языка, который является моделью типизированного атрибутного разграничения доступа. Тип T может быть представлен двояко – в виде алгебраической T^{AS} и в виде логической T^{LS} систем.

Основной задачей типизированного атрибутного разграничения доступа является ограничение круга операций, выполняющихся над атрибутами определенных типов, операциями, определенными и разрешенными для этого типа.

Модель типизированного атрибутного разграничения доступа T в виде алгебраической системы [12], задается следующим образом:

$$T = T^{AS} = (D, \sigma),$$

где

$D = (A, \sqsubseteq)$ – домен всевозможных значений атрибутов A , структурированный в виде полной решетки, упорядоченной отношением частичного порядка $\sqsubseteq$;

$\sigma = \{SL, SL1, Acc\}$ – многосортная сигнатура набора операций и предикатов. $Sort = \{D, B\}$ – множество сортов (типов) аргументов и значений этих операций. Среди них $B = \{true, false\}$ – булев тип.

Обозначим множество сущностей субъектно-объектной модели ТАРД как $E = \{e\}$, $E = SUO$, где $S = \{s\}$ – субъекты, а $O = \{o\}$ – объекты разграничения доступа.

Политика типизированного атрибутного разграничения доступа выражается формально с помощью операций σ :

Операция типизации $SL: D \rightarrow D$ присваивает сущности метку безопасности в виде атрибута $a \in A$ типа T .

Операция типизации $SL1: D \rightarrow P(D)$ присваивает сущности метку безопасности в виде подмножества атрибутов $SL1(a) = \{a_i \mid a_i \sqsubseteq a, a_i \in A\}$ типа T .

Операция сравнения атрибутов $Acc: (D \rightarrow D) \rightarrow B$ осуществляет сравнение однотипных меток безопасности, разрешая/отвергая возможность доступа субъекта к объекту:

$$Acc(SL(s), SL(o)) = true/false \text{ или } Acc(SL1(s), SL1(o)) = true/false.$$

Модель типизированного атрибутного разграничения доступа, представленная как логическая система [13], имеет вид:

$$T = T^{LS} = (L, Ax, Inf),$$

где

$L = (D, G)$ – язык с алфавитом, представленным доменом D и правилами грамматики $G = \{SL(e), SL1(e), Acc(s, o)\}$, которые порождают цепочки – метки безопасности субъектов и объектов в виде элементов домена D или его структурированных подмножеств.

$Ax - \{SL, SL1\}$ - схема аксиом в виде множества значений функций типизации, $Inf = \{Acc\}$ – набор правил вывода для получения теорем.

L задает синтаксис, а дедуктивный аппарат (Ax, Inf) – порождает семантику языка, представляемого логической системой.

Каждый из языков T^{AS} и T^{LS} определяются на мета и объектных уровнях:

$$T_{META} \rightarrow T_{OBJ} \rightarrow AM.$$

T_{META} – определение типа T на метауровне, T_{OBJ} - определение T на объектном уровне, получаемое из T_{META} . В свою очередь, язык T_{OBJ} порождает всевозможные значения меток безопасности сущностей данного типа, образующие матрицу доступа AM .

В работах [11-13] было показано, что, в силу своего определения, структуры решетки домена D алгебры T^{AS} и алфавита D логики T^{LS} представляющих модель ТАРД, позволяют выделить следующие подструктуры: S - в виде скалярного множества, Li – линейно упорядоченного множества и Tr – в виде дерева.

В соответствии с этим, метамодель T_{META} порождает объектные модели $T_{OBJ}(I)$, которые являются конкретными моделями разграничения доступа разных видов. Индекс структуризации принимает значения $I \in \{S, Li, Tr\}$. $I=S$ служит для создания моделей типа MAC , $I=Li$ – моделей MAC , а $I=Tr$ моделей $RBAC$.

При этом

$$\begin{aligned} T_{META}^{AS} &= T^{AS} = (D, \sigma), \\ T_{META}^{LS} &= T^{LS} = (L, Ax, Inf), \\ T_{OBJ}^{AS}(I) &= (D^I, \sigma^I), \\ T_{OBJ}^{LS}(I) &= (L^I, Ax^I, Inf^I). \end{aligned}$$

Модель ТАРД, представленная в виде пары (T^{AS}, T^{LS}) :

- служит основой для построения систем, в которых возможно одновременное применение различных моделей безопасности, объединяемых единообразной обработкой типизированных атрибутов разграничения доступа;
- дает возможность управления процессом их построения и функционирования;
- обеспечивает формальное доказательство безопасного доступа субъектов к объектам путем логического вывода теорем;
- непосредственно реализуема на языках логического и функционального программирования.

Программную систему для реализации модели типизированного атрибутного разграничения доступа можно определить формально как программу P на языке T , которая представляет собой функцию, устанавливающую отношение между синтаксическими конструкциями языка T и их денотатом:

$$P(T): SynD \rightarrow SemD,$$

где $SynD$ – синтаксический, а $SemD$ – семантический домены.

Программная система $P(T)$, основанная на определенном типе атрибутов, производит разграничение доступа по одному критерию, задаваемому этим типом. Система, содержащая K независимых типов $T_1, T_2, \dots, T_K$,

$$P(T_1, T_2, \dots, T_K),$$

обеспечивает многокритериальное разграничение доступа.

3. Архитектура и функции систем ТАРД

Согласно мета- и объектному уровням определения модели Т, выделены основные модули – модуль настройки и модуль выполнения, составляющие архитектуру систем типизированного атрибутного разграничения доступа (СТАРД). Они соответствуют стадиям настройки и выполнения в процессе функционирования системы (Рис. 1).

В соответствии с разработанными теоретическими принципами, алгебраическая система T^{AS} составляет основу архитектуры СТАРД, а логика T^{LS} используется для управления процессом функционирования ее модулей.



Рис.1. Модульный состав СТАРД

Функционирование системы предполагает наличие выделенного пользователя – администратора, который управляет ее конфигурацией и присваивает пользователям и информационным объектам привилегии доступа в виде их меток безопасности.

Модуль настройки осуществляет конфигурирование системы путем задания типов атрибутов $T_k, k=\overline{1, K}$, которые, являясь конкретными вариантами моделей безопасности, осуществляют разграничение доступа по определенным критериям. На этой стадии система выполняет функцию администрирования, в процессе которого задаются структуры и значения элементов доменов, образующих типы T_k .

В функции модуля выполнения входит администрирование, когда администратор присваивает пользователям и информационным объектам их атрибуты безопасности в рамках определенных для системы типов T_k . Второй функцией, реализуемой модулем, является собственно контроль доступа пользователей к ресурсам.

Рассматривая T^{LS} как функцию с аргументом T^{AS} , можно представить работу модуля настройки СТАРД на стадии ее конфигурирования следующим образом:

$$T_{META}^{LS}(T_{META}^{AS}) \rightarrow T_{OBJ}^{AS},$$

где аргументом функции является метамодель ТАРД, а значением (денотатом) – интенциональное представление типа Т атрибутов в виде конкретной модели разграничения доступа T_{OBJ}^{AS} .

Далее, на стадии выполнения, работа СТАРД описывается в виде:

$$T_{OBJ}^{LS}(T_{OBJ}^{AS}) \rightarrow (T_{OBJ}^{AS})_t.$$

При этом аргументом функции является объектная модель ТАРД, а значением – экстенциональное представление типа Т атрибутов в виде конкретной матрицы доступа, состоящей из структурированного множества меток безопасности сущностей, представляющих матрицу доступа в моменты времени t .

Заключение

Для разрабатываемой концепции типизированного атрибутного разграничения доступа дано формальное определение типа атрибутов субъектов и объектов – участников процесса доступа к защищаемой информации.

Приведены многоуровневые представления типа атрибутов безопасности в виде алгебраической и логической систем. Показана возможность создания из них различных моделей разграничения доступа. На основе данных теоретических разработок предложены принципы конструирования архитектуры и функций программных систем, осуществляющих типизированное атрибутивное разграничение доступа в соответствии с критериями защиты, обеспечиваемой составляющими их моделями.

Литература

1. Hu V.-C., Ferraiolo D., Kuhn R., Schnitzer A., Sandlin K., Miller R., Scarfone K. NIST Special Publication 800-162. Guide to Attribute Based Access Control (ABAC). Definition and Considerations // NIST National Institute of Standards and Technology – <http://dx.doi.org/10.6028/NIST.SP.800-162>. – Jan 2014.
2. Khalid Bijon, Ram Krishnan and Ravi Sandhu, Constraints Specification in Attribute Based Access Control, *IEEE/ASE Science Journal*, Vol 2, No. 3, 2013, P. 131-144.
3. Wang L., Wijesekera D., Jajodia S. 2004. A logic-based framework for attribute based access control. In *Proceedings of the 2004 ACM workshop on Formal methods in security engineering (FMSE '04)*. ACM, New York, NY, USA, 45-55. DOI=<http://dx.doi.org/10.1145/1029133.1029140>
4. Jajodia S., Samarati P., Sapino M.L., Subrahmanian V.S. 2001. Flexible support for multiple access control policies. *ACM Trans. Database Syst.* 26, 2 (June 2001), 214-260. DOI=<http://dx.doi.org/10.1145/383891.383894>
5. Jajodia S., Samarati P., Subrahmanian V. S., "A logical language for expressing authorizations," *Proceedings. 1997 IEEE Symposium on Security and Privacy (Cat. No.97CB36097)*, Oakland, CA, 1997, pp. 31-42. doi: 10.1109/SECPRI.1997.601312
6. Bertino E., Catania B., Ferrari E., Perlasca P. 2003. A logical framework for reasoning about access control models. *ACM Trans. Inf. Syst. Secur.* 6, 1 (February 2003), 71-127. DOI=<http://dx.doi.org/10.1145/605434.605437>
7. Калимолдаев М.Н., Бияшев Р.Г., Рог О.А. Формальное представление функциональной модели многокритериальной системы разграничения и контроля доступа к информационным ресурсам // Проблемы информатики. – 2014. – № 1(22). – С. 43-55.
8. Rog O.A. Polymorphic typing of entities in the multi-criteria system of access control and a task of constructing types // Information Technologies, Management and Society. The 12 th International Scientific Conference Information Technologies and Management. 2014 April 16 – 17. Riga, 2014. - с. 66.
9. Бияшев Р.Г., Калимолдаев М.Н., Рог О.А. Полиморфная типизация сущностей и задача конструирования механизма многокритериального разграничения доступа. // Известия НАН РК. Серия физико-математическая. – 2014. – № 5. – С. 33-41.
10. Бияшев Р.Г., Калимолдаев М.Н., Рог О.А. Логический подход к организации многокритериального атрибутивного разграничения доступа. // Совместный выпуск по материалам международной научной конференции «Вычислительные и информационные технологии в науке, технике и образовании» (CITech-2015) (24-27 сентября 2015 г.) Вычислительные технологии т.20, Вестник КазНУ им. Аль-Фараби, серия математика, механика и информатика №3(86) Часть 1. - С.275-278.
11. Бияшев Р.Г., Калимолдаев М.Н., Рог О.А. Представление ограничений моделей атрибутивного разграничения доступа // Известия НАН РК. Серия физико-математическая. – 2016. – № 1. – С. 58-65.

12. Бияшев Р.Г., Калимолдаев М.Н., Рог О.А. Моделирование семантики типизированного атрибутивного разграничения доступа // журнал Проблемы информатики, 2017, № 1. С. 25-37.

13. Калимолдаев М.Н., Бияшев Р.Г., Рог О.А. Применение логики для построения моделей разграничения доступа к информации // принята к печати в журнал «Доклады НАН РК» 13.04.2017

ЧИСЛЕННОЕ РЕШЕНИЕ ЗАДАЧИ СТАБИЛИЗАЦИИ СИСТЕМЫ «СИНХРОННЫЙ ГЕНЕРАТОР – ПАРОВАЯ ТУРБИНА»

Калимолдаев М.Н., Дузбаев Т.Т., Ахметжанов М.А., Галиева Ф.М.
e-mail: mnk@ipic.kz, talgat.duzbayev@gmail.com, galyeva.fariza@gmail.com,
maks714@mail.ru

*Институт информационных и вычислительных технологий КН МОН РК,
Казахстан*

Аннотация. В данной работе рассматривается стабилизация системы «синхронный генератор – паровая турбина», а также проводится исследование устойчивости системы с помощью метода функции Ляпунова. В результате численного вычисления получено оптимальное решение приведенных параметров.

Упрощенная модель системы «синхронный генератор – паровая турбина», описывается уравнениями вида:

$$\begin{aligned} \frac{d\delta_i}{dt} &= S_i, \\ T_{ji} \frac{dS}{dt} &= P_{Ti} - D_i S_i - \left[\frac{E_i^2}{z_{11i}} \sin \alpha_{11i} + \frac{E_i U}{z_{12i}} \sin(\delta_i - \alpha_{12i}) \right], \\ T_{Pi} \frac{dP_{Ti}}{dt} &= -P_{Ti} - \rho_0 P_{0i} - \frac{P_{0i}}{\sigma_{0i}} S_i + u_i, \end{aligned} \quad (1)$$

Здесь, δ_i – угол ЭДС генератора; S_i – скольжение генератора; T_{ji} – постоянная инерции вращающихся масс; P_{Ti} – мощность паровой турбины; T_{Pi} – постоянная времени тракта регулирования паровой турбины; $D_i > 0$ – коэффициент демпфирования; E_i – расчетная ЭДС генератора; U_i – напряжения на шинах бесконечной мощности, z_{11i} – собственное сопротивление генератора; z_{12i} – взаимное сопротивление между генератором и шинами; α_{11i} – дополнительный угол собственного сопротивления; α_{12i} – дополнительный угол взаимного сопротивления; ρ_0, P_{0i} – заданные постоянные величины (ρ_{0i} – начальное открытие окон золотника, P_{0i} – номинальная мощность

турбины); σ_{0i} – статизм АРЧВ (автоматического регулятора частоты вращения); u_i – управляющее воздействие МУТ (механизма управления турбиной).

Пусть заданы следующие параметры системы регулирования паровой турбины: $T_{Pi}=2512$, $\rho_{0i}=0.994$, $P_{0i}=1126$, $\sigma_{0i}=0.06$.

Осуществляя перенос начала координат в положение равновесия $(\delta_i, S_i, P_{Ti}) = (0.686, 0, 1035.748)$, перейдем к системе уравнений возмущенного движения:

$$\begin{aligned}\frac{d\delta_i}{dt} &= S_i, \\ \frac{dS_i}{dt} &= c_i P_{Ti} - D_i S_i - f_i(\delta_i), \\ \frac{dP_{Ti}}{dt} &= A_i P_{Ti} + u_i,\end{aligned}\quad (2)$$

где $D_i = 50.5 \cdot 10^{-4}$, $f_i(\delta_i) = f_{oi}[\sin(\delta_i + \theta_{0i}) - \sin \theta_{0i}]$, $f_{oi} = 1.513 \cdot 10^{-4}$, $\theta_{0i} = 0.3562$, $c_i = 4.167 \cdot 10^{-8}$, $A_i = -39.81 \cdot 10^{-4}$. В системе (2) предполагается, что сигнал от АРЧВ, пропорциональный скольжению, адаптивно входит в управление u_i . Для упрощения расчетов рассматривается линейная модель паровой турбины.

Для исследования устойчивости «в большом» системы (2) функция Ляпунова имеет вид:

$$\tilde{v}_{0i}(\delta_i, S_i, P_{Ti}) = \frac{1}{2} H_i P_{Ti}^2 + 2\nu_{0i}(\delta_i, S_i), \quad (3)$$

определенную в фазовом пространстве $R_i^3(\delta_i, S_i, P_{Ti})$ в полосе $G_{0i} = \{(\delta_i, S_i, P_{Ti}) / \delta_{-li} < \delta_i < \delta_{0i}, S_i \in R_i^1, P_{Ti} \in R_i^1\}$. Найдём область притяжения начала координат в полосе G_{0i} при управлении вида:

$$u_i = a_i P_{Ti} + \alpha_{1i} S_i + \alpha_{2i} \delta_i, \quad a_i = 0, \quad \alpha_{1i} = -\frac{P_{0i}}{\sigma_{0i} T_{Pi}} = -747.3.$$

Имеем $\tilde{A}_i = A_i$, $\tilde{q}_i = \alpha_{1i}$, $l_{1i} = \alpha_{2i}$, $l_{2i} = 0$, $B_i = (\alpha_{1i}, \alpha_{2i}, 0)$,

$$\xi_i = \begin{pmatrix} S_i \\ \delta_i \\ f_i(\delta_i) \end{pmatrix}, \quad g_i = \begin{pmatrix} c_i \\ \alpha_i c_i \\ 0 \end{pmatrix}, \quad 0 < \alpha_i < D_i, \quad Y_i(P_{Ti}, \xi_i) = -\text{Re} \xi_i^* g_i P_{Ti},$$

$$\Pi_i(j\omega) = \text{Re} g_i (\tilde{A}_i - j\omega)^{-1} B_i = \frac{A_i c_i}{A_i^2 + \omega^2} \begin{pmatrix} \alpha_{1i}, & \alpha_{2i}, & 0 \\ \alpha_i \alpha_{1i}, & \alpha_i \alpha_{2i}, & 0 \\ 0, & 0, & 0 \end{pmatrix}.$$

Для выполнения частотного неравенства $\Pi_i(j\omega) \geq 0 \quad (\forall \omega \in R_i^1)$, достаточно, $\alpha_{1i} < 0$, так как $c_i > 0$, $A_i < 0$. Величину $H_i > 0$ определяем из условия:

$$2H_i A_i < 0, \quad H_i(\alpha_{1i}, \alpha_{2i} 0) + (c_i, \alpha_i \cdot c_i, 0) = 0,$$

для которой

$$H_i = -\frac{c_i}{\alpha_{1i}} = -\frac{\alpha_i c_i}{\alpha_{2i}} = 44.22 \cdot 10^{-12}, \quad \alpha_{2i} = -4.435.$$

Область притяжения начала координат в полосе G_{0i} можно оценить, таким образом: $\tilde{v}_{0i}(\delta_i, S_i, P_{Ti}) < \tilde{C}_i$, где параметры функции Ляпунова $v_{0i}(\delta_i, S_i, P_{Ti})$ и критериальное значение $\tilde{C}_i = 3.671 \cdot 10^{-4}$.

При указанных выше значениях параметров область притяжения координат, задаваемая в полосе G_{0i} неравенством $\tilde{v}_{0i}(\delta_i, S_i, P_{Ti}) < \tilde{C}_i$, имеет вид, представленной на рисунке 4. Сечение этой области плоскостями $\delta_i = \text{const}$ (т.е. $\delta_i = \delta_{-li} + 0$, $\delta_i = 0$, $\delta_i = \delta_{0i} - 0$) являются эллипсами. Начальные условия: $\delta_i = 0$, $S_i = 2.5 \cdot 10^{-2}$, $P_{Ti} = 0$.

Для численного решения рассматриваемой задачи был создан программный модуль написанный на языке программирования C# использующий интерфейс создания приложения Windows Forms. В программе для численного интегрирования системы (2) используются двухшаговый метод Адамса-Башфорта. Формула данного метода имеет следующий вид:

$$y_{i+1} = y_i + h \cdot \left(\frac{3}{2}(f(x_i, y_i)) - \frac{2}{1}(f(x_{i-1}, y_{i-1})) \right). \quad (3)$$

Используя формулу (3) перепишем систему (2) в виде:

$$\begin{aligned} \delta_{i+1} &= \delta_i + h \cdot \left(\frac{3}{2}S_i - \frac{1}{2}S_{i-1} \right); \\ S_{i+1} &= S_i + h \cdot \left(\frac{3}{2}(cP_{Ti} - DS_i - f(\delta_i)) - \frac{1}{2}(cP_{Ti-1} - DS_{i-1} - f(\delta_{i-1})) \right); \\ P_{Ti+1} &= P_{Ti} + h \cdot \left(\frac{3}{2}(AP_{Ti} + u) - \frac{1}{2}(AP_{Ti-1} + u) \right). \end{aligned} \quad (4)$$

Результаты численного дифференцирования системы (4) приведены ниже:

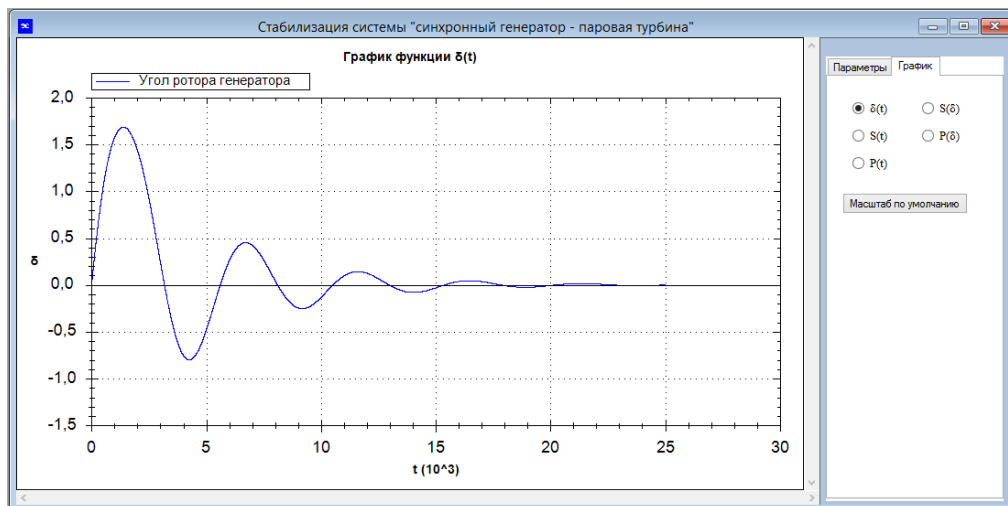


Рис. 1 График параметра δ

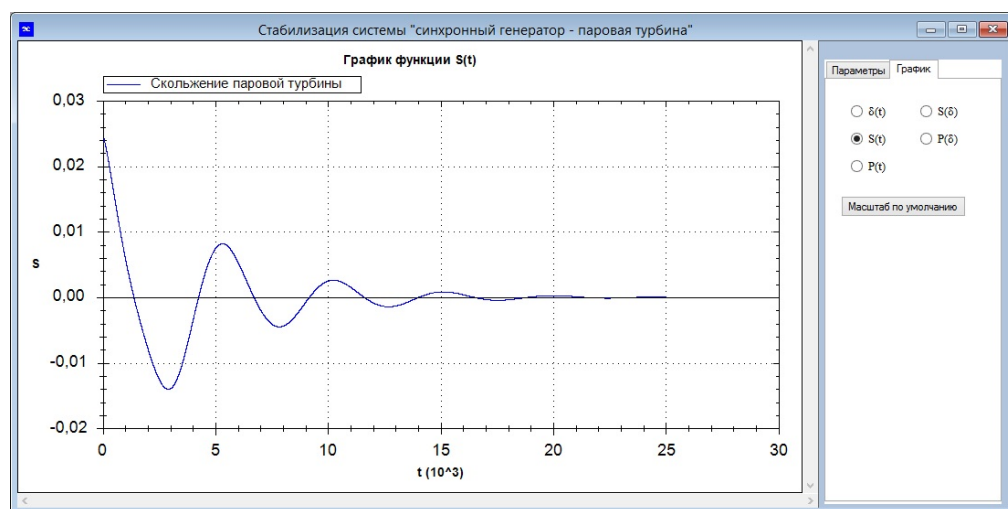


Рис. 2 График параметра S

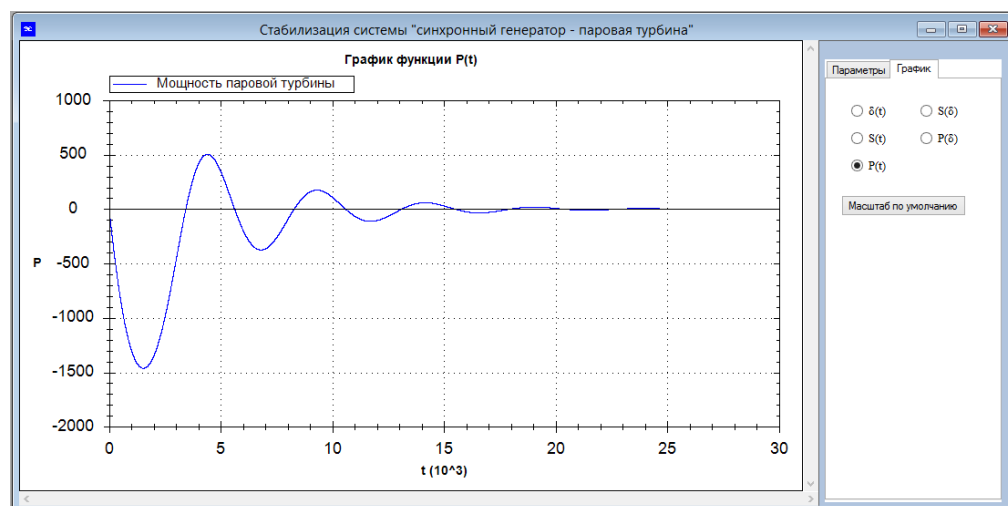


Рис. 3 График параметра P

Области притяжения скольжения и мощности находим из формулы (3).
Полученные результаты приведены на рисунках 4-5.

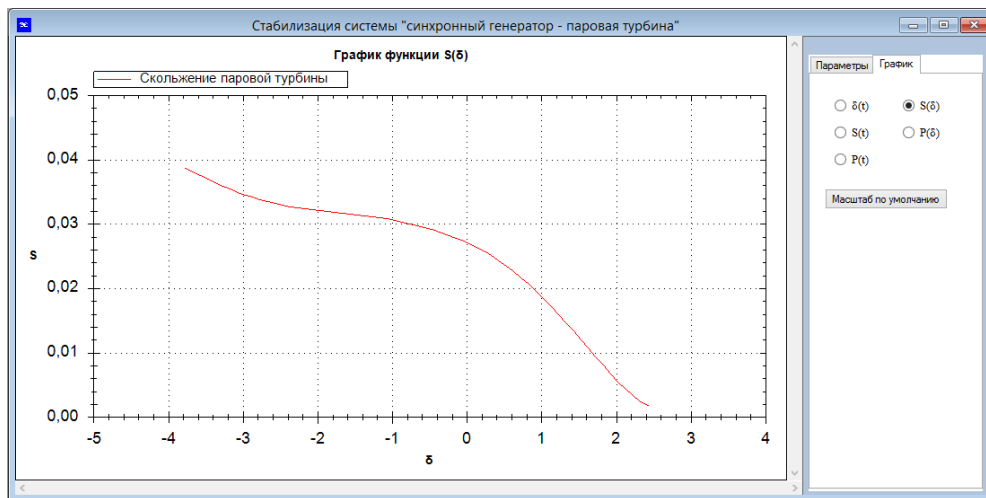


Рис. 4 Область притяжения скольжения

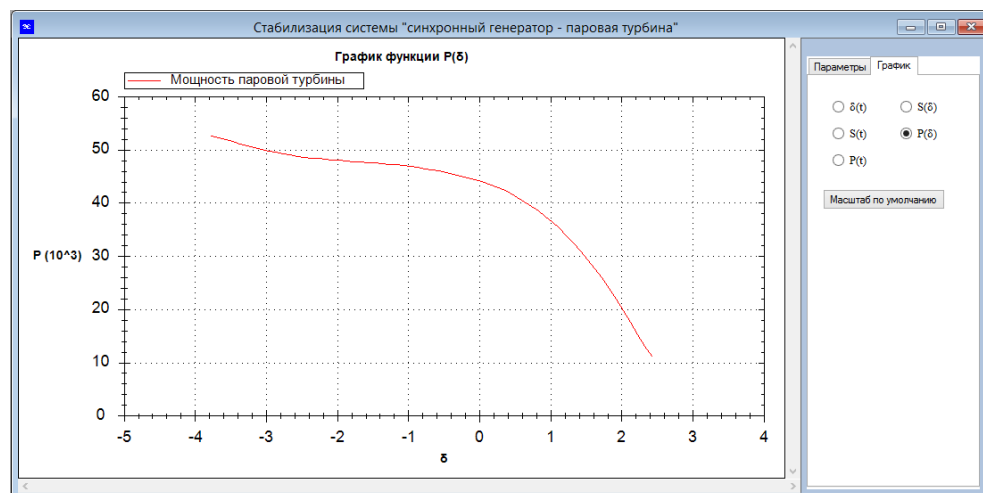


Рис. 5 Область притяжения мощности

Литература:

1. Ляпунов А.М. Общая задача об устойчивости движения -М.: Л.: Гостехиздат, 1950, -475 с.
2. Барбашин Е.А. Введение в теорию устойчивости. -М.: Наука, 1967. -224 с.
3. Калимолданов М.Н. Докторская диссертация на тему «Устойчивость и математическое моделирование нелинейных многомерных фазовых систем» по специальности 05.13.16 – применение вычислительной техники, математического моделирования и математических методов в научных исследованиях. 2000 г.
4. Метод Эйлера. –https://ru.wikipedia.org/wiki/Метод_Эйлера

МОДЕЛИРОВАНИЕ СБОРА И АНАЛИЗА ДАННЫХ ДЛЯ ПРОГРАММНОГО КОМПЛЕКСА СТАБИЛИЗАЦИИ И УПРАВЛЕНИЯ МНОГОСВЯЗНЫМИ ФАЗОВЫМИ СИСТЕМАМИ

Калимолдаев М.Н., Қосынбай Е.Б.
e-mail: conprefor@gmail.com

*Институт информационных и вычислительных технологий КН МОН РК,
Казахстан*

Аннотация. В статье описана предложенная модель, сбора и предварительной обработки данных для хранения, а также модель анализа и подготовки исходных данных для программного комплекса стабилизации и управления многосвязными фазовыми системами предложенная в работе на соискание степени доктора Ph.D. Ахметжанова М.А.

Введение

Комплекс предложенный в работе [1] Ахметжанова М.А. включает 6 моделей стабилизации и управления многосвязными фазовыми процессами, отмеченными на рисунке 1, такими как:

1. Стабилизации движения электроэнергетической системы при $l=2$;
2. Устойчивость движения синхронного генератора;
3. Оптимальное управление движением двухмашинной системы;
4. Система «синхронный генератор – паровая турбина»;
 - а. Система «синхронный генератор – паровая турбина»;
 - б. Стабилизация системы «синхронный генератор – паровая турбина»;
5. Математическая модель Парка-Горева синхронного генератора;
6. Стабилизация генератора;

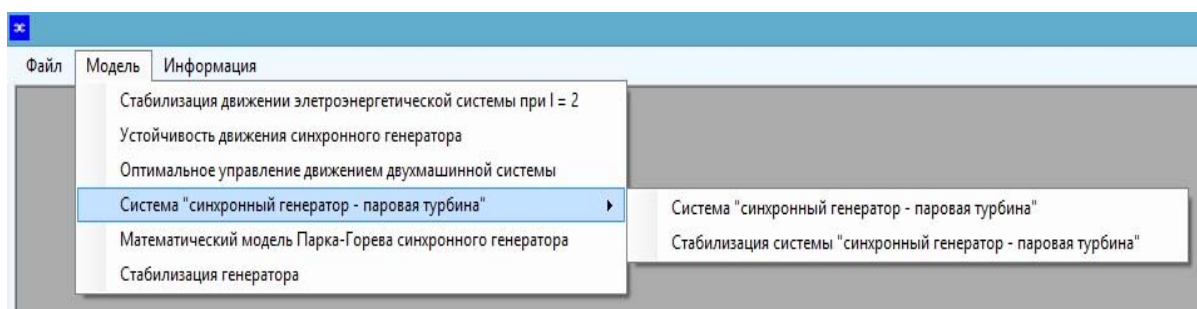


Рисунок 1 – Модели программного комплекса [1]

Входные данные указанного комплекса имеют числовой формат и называются параметрами, а выходными данными является графическое представление численного решения управления процессом стабилизации многосвязными фазовыми системами согласно исследованным моделям, в случаях разбалансировки системы. Интерфейс входных и выходных данных программного комплекса представлен на рисунке 2.

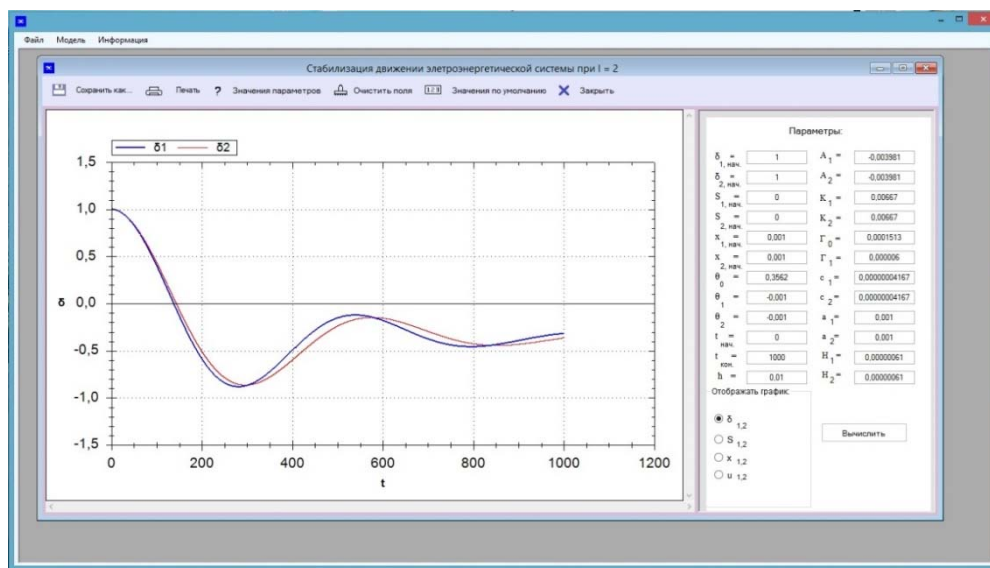


Рисунок 2 – Входных и выходных данных программного комплекса [1].

Описание проблемы

В Республике Казахстан на 2017 г. 18 ГЭС, 59 ТЭЦ, 6 солнечных и ветряных электростанций. По данным KEGOC [2] - системного оператора единой электроэнергетической системы Казахстана — производство электрической энергии в стране осуществляют 119 электростанций различной формы собственности. Фактическая установленная мощность на конец 2012 года — 19,4 ГВт, на конец 2013 года — 19,6 ГВт, на конец 2014 г. — 20,8 ГВт, на конец 2015 г. — 21,3 ГВт. Располагаемая мощность на 18 % ниже — всего 17,5 ГВт.

KEGOC подразделяет электрические станции на электростанции национального значения, электростанции в составе промышленных комплексов и электростанции регионального значения.

В списке [3] перечисляются электростанции Казахстана, включённые в фактический баланс мощности ЕЭС Казахстана. Список сгруппирован по видам электростанций. Установленная мощность и структура собственности электростанций приводится в соответствии с официальными годовыми отчётами генерирующих компаний Казахстана. В качестве собственника электростанций АО «АлЭС» (Алматинские ТЭЦ-1, ТЭЦ-2 и ТЭЦ-3, Капчагайская ГЭС и Алматинский каскад ГЭС) указывается Самрук-Энерго, так как 100 % акций АО «АлЭС» принадлежит Самрук-Энерго.

В последнее время все больше и больше интеллектуальных систем моделируются и разрабатываются с применением технологий [4], называемыми большие данные, в том числе и в области энергетики.

Исходя из вышеописанного, отмеченный комплекс управления и стабилизации может быть частично автоматизирован за счет оптимизации процесса сбора, обработки и ввода/передачи входных данных за счет применения технологии больших данных.

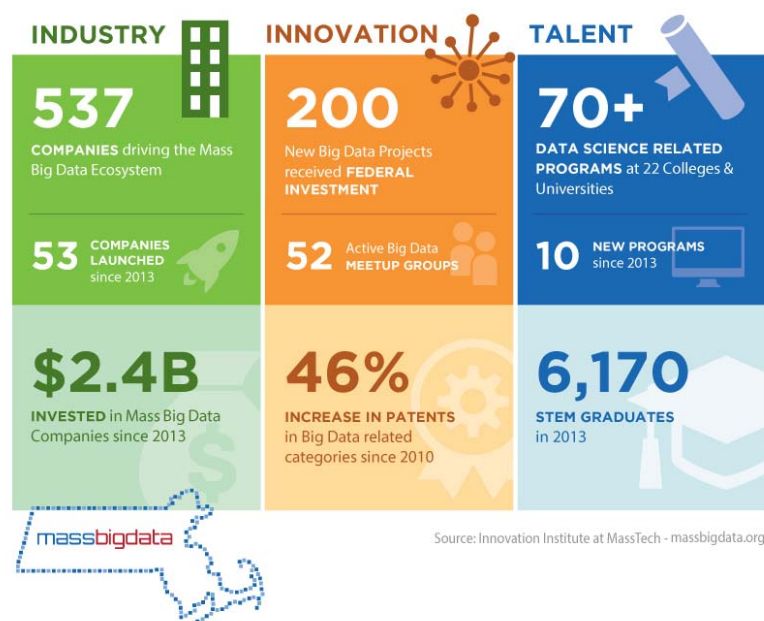


Рисунок 3 – Экосистема больших данных по версии MIT [4]

Типы задач энергетики, решаемые большими данными

Первый тип – NP-полные задачи.

Второй тип задач, где обработка выборок заменяется знаменитой формулой BIG DATA ($N=BCE$), связан с обработкой всех имеющихся однотипных данных, например, с целью прогнозирования.

Третий тип задач представляет особый интерес. Это тотальный анализ слабоструктурированных данных. Простейшим вариантом такой слабой структурированности может служить фрагментарная структурированность.

Постановка задачи и построение модели обработки входных данных комплекса

Термин "Большие данные" скрывает огромный набор информации. Причем объем ее столь велик, что обработка больших объемов данных стандартными программными и аппаратными средствами представляется крайне сложной. Другими словами, Big Data – это огромный класс задач хранения и обработки гигантских объемов данных. Классическая концепция Big data базируется на принципах четырех «V» [5], что означает Volume – объем данных, Velocity – скорость обработки или появления данных, Variety – многообразие и структурированность данных, Veracity – ценность данных, а также стоимость обработки.

При построении модели прежде всего надо определиться с тем, что будет являться стандартом или эталоном для входных данных, а также критериями для их обработки. Существенным будет являться выбор инструментов для моделирования, определение граничных условий для выборки данных или порций данных (равномерное распределение, неравномерное распределение данных), также среды моделирования.

В данной задаче самым логичным выбором является: подход больших данных для итеративного анализа поступающих входных данных потоком. Можно было бы рассматривать энергосистему более подробно и брать за узлы источники параметров, например, различные датчики на каждом возможном роторе генератора с учетом типа

генерируемых данных, но в данной задаче не принципиален вид энергосистемы внутри предприятий и страны в целом, т.к. необходим общий тип входных данных вне зависимости от типа электростанции и энергопотребителя.

Критерии для обработки входных параметров Big data в электроэнергетике

В связи с вышеизложенными сведениями и моделям в электроэнергетике можно сформировать следующие критерии:

Критерий 1. Информация в электроэнергетике может быть как структурирована, так и не структурирована и представлять из себя различные форматы данных, сводимых в выборку. Авторами проводится исследование в области формирования критериев для источников данных по энергетике,

Критерий 2. Выборка данных определяется как нечеткое множество неструктурированных данных согласно выборочному запросу.

Критерий 3. Геолокационные данные играют важную косвенную роль при корреляции параметров обработки данных.

Критерий 4. Высокая доступность данных с учетом политики безопасности и защиты данных.

Критерий 5. Датификация энергетических данных/данных многофазных электростанций может быть определена через беспроводные и мобильные сети, мобильные устройства и операторов.

Критерий 6. Сходимость корреляции при датификации в режиме реального времени

Критерий 7. Сходимость на устойчивость корреляции по датификации в режиме реального времени дает в среднем от 78-99% точности прогноза данных.

Критерий 8. Актуальность и периодичность хранения запросов данных энергетике/электростанции, хранение истории запросов, логов программного комплекса.

Критерий 9. Ценность энергетических данных, их криптобезопасность и права принадлежности должны определяться в соответствии со стандартами информационной и национальной безопасности страны.

Критерий 10. Оценка и прогнозирование энергетических данных позволят мониторить текущее состояние энергопотребления по регионам, а также учитывать и планировать рост/развития энергетики по регионам.

Выбор инструментов для моделирования обработки больших данных

Широкое развитие альтернативной энергетики привело к принципиальному изменению целостной системы генерации, доставки и потребления электроэнергии, а также прогнозу потребления электроэнергетики с использованием больших данных. Появилась терминология интеллектуальных энергетических сетей (Smart Grid – [6-8]). Многие ученые сравнивают текущее состояние исследований, разработок и внедрения новых методов управления в энергетике с началом развития Internet, введя в оборот термин Enernet – энергетический Интернет с огромным неструктурированным потоком данных (Big Data) [9]. Доход от интеллектуальных систем управления энергетическими сетями оцениваются в миллиарды долларов.

Одной из популярных технологий больших данных является Hadoop. Особенностью и преимуществом Hadoop, относительно текущей задачи, является следующее:

Hadoop следует использовать, если:

- вычисления должны быть компонуемыми, другими словами, вы должны иметь возможность запустить вычисления на подмножестве данных, а затем слить результаты.
- вы планируете обрабатывать большой объем неструктурированных данных - больше, чем можно уместить на одной машине (> нескольких терабайт данных). Плюс здесь будет возможность использовать commodity hardware для кластера в случае Hadoop.

Hadoop не следует использовать:

- Для некомпонуемых задач - например, для задач рекуррентных.
- Если весь объем данных умещается на одной машине. Существенно сэкономите время и ресурсы.
- Hadoop в целом -система для пакетной обработки и не подходит для анализа в режиме реального времени (для данного существуют более эффективные инструменты, например Storm).

Если большие данные поступают в виде высокоскоростных потоков и реагирование системы должно происходить с малой задержкой, то вместо пакетной аналитики применяется аналитика реального времени. Касательно чего в мире еще не существует общепринятых стандартных подходов. Однако, отталкиваясь от групповых свойств входных данных, рекомендуется обратить внимание на смешанный подход, когда сбор и прием производится в реальном времени, а анализ данных производится по последним актуальным данным.

Подробнее о Hadoop, в составе четыре функциональных части [10]:

- Hadoop Common;
- Hadoop HDFS;
- Hadoop MapReduce;
- Hadoop YARN;

Hadoop Common – это набор библиотек и утилит, необходимых для нормального функционирования технологии. В его состав входит специализированный упрощенный интерпретатор командной строки.

HDFS (Hadoop Distributed File System) – это распределенная файловая система для хранения данных на множестве машин в больших объемах. Проектировалась так, чтобы обеспечивать:

- Надежное хранение данных на дешевом
- ненадежном оборудовании;
- Высокую пропускную способность чтения-записи;
- Поточковый доступ к данным;
- Упрощенную модель согласованности;
- Архитектуру аналогичную Google File System.

Модель обработки входных данных

Обработка данных в Hadoop осуществляется с помощью технологии MapReduce, данная технология была разработана компанией Google (Джеффри Дин и Санджай Гемават) в 2004 году, которая заключается в следующем -решение для обработки больших объемов «сырых» данных (индексированных документов, логов запросов и т.п.): огромный массив информации делится на части, и обработка каждой из этих частей поручается отдельному серверу. Как правило, данные обрабатываются на тех же серверах, где они и хранятся, что позволяет ускорить процесс обработки и избежать лишних перемещений данных между серверами. После этого полученные результаты

объединяются в единое целое. Архитектура MapReduce построена по принципу «главный — подчиненные» (master — workers). В качестве главного выступает сервер (называемые node) JobTracker, раздающий задания подчиненным узлам (также называемыми node) DataNode кластера и контролирующий их выполнение TaskTracker.

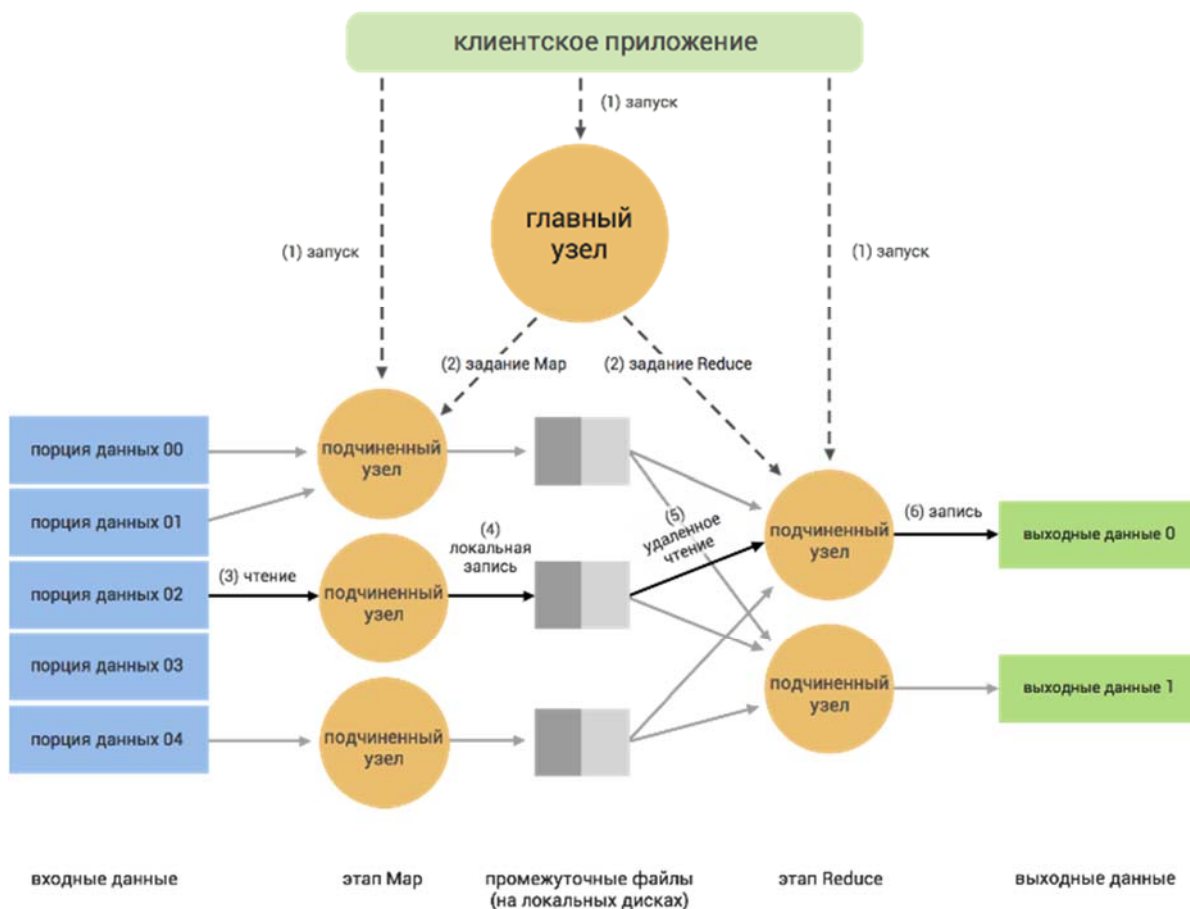


Рисунок 4 - Архитектура MapReduce [11]

Обработка данных подразделяется на следующие этапы:

Запуск приложения: передача кода приложения на главный (master) и подчиненные узлы (workers);

1. Мастер назначает конкретные задачи (Map или Reduce) и распределяет части входных данных по вычислительным узлам (workers);

2. Map-узлы читают назначенные им входные данные и начинают их обработку;

3. Map-узлы локально сохраняют промежуточные результаты: каждый узел сохраняет полученный результат на локальные диски;

4. Reduce-узлы читают промежуточные данные с Map-узлов и выполняют Reduce обработку данных;

5. Reduce-узлы сохраняют итоговые результаты в выходные файлы, обычно в HDFS.

Создание приложений для MapReduce — дело достаточно трудоемкое. Написание всех функций, компилирование и упаковка занимают много времени. Чтобы облегчить работу компания Yahoo! разработала специализированный инструмент под названием Pig, повышающий уровень абстракции при обработке данных.

Основываясь на парадигмах Hadoop и MapReduce, а также учитывая агентный подход [12] для создания программных сервисов, предлагается модель, согласно которой, каждый функциональный блок будет разделен в отдельные модули:

- Сборщик - прием и сбор данных (pull - push модели), сохранение данных или ключевых мета-данных о принятой информации в базе данных, совместимой с Hadoop (например, Hbase), а также по пакетно дублировать данные в распределенную файловую систему HDFS. Фактически данный модуль можно рассматривать как интерфейс входных данных системы.

- Анализатор – предполагается, будет состоять из двух комплексов: быстрый анализ для фиксации критических пиков разбалансировки системы [1], а также продолжительный анализ для фиксации закономерной разбалансировки системы. Также предполагается данный модуль будет производить подготовку входных данных программного комплекса стабилизации и управления многосвязными фазовыми системами.

В результате работы модулей должно будет производиться запуск программы стабилизации для поиска решения балансировки системы с передачей обработанных и структурированных входных данных.

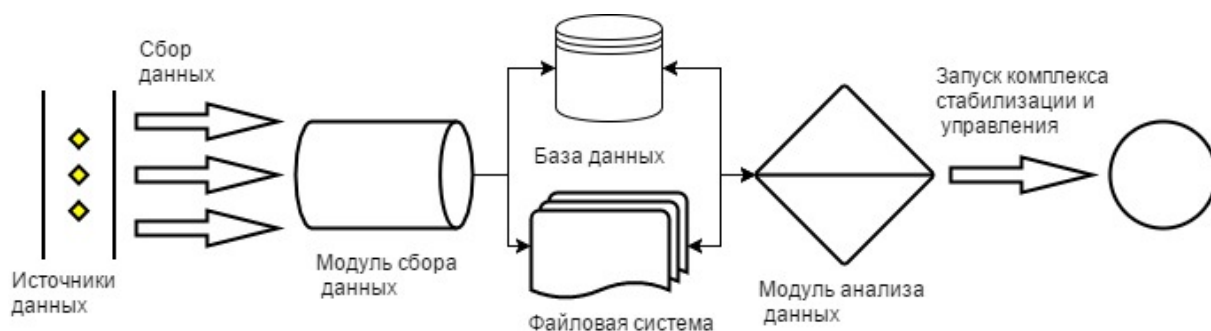


Рисунок 5 – Модель подготовки данных для программного комплекса стабилизации и управления многосвязными фазовыми системами

Выводы

Авторами изучено текущее состояние проблемы Энергетической отрасли в Республике Казахстан и существующие системы и программные комплексы для обработки данных с электростанций (Huawei SCADA, SmartGrid, GE Energy Products, Schneider Electric, ABB и др.).

Авторами выделены основные критерии для обработки входных параметров данных энергетических систем, а также выбран подход для обработки больших данных на основе Hadoop в предлагаемой модели сбора и анализа данных для подготовки запуска программного комплекса стабилизации и управления многосвязными фазовыми системами.

Литература

1. Ахметжанов М.А., Көп байланысты фазалық жүйелерді басқару және тұрақтандыру // дисс. на соискание степени доктора Ph.D. – КазНУ им.аль-Фараби, Алматы 2016. – 107 с.
2. Годовой отчет 2015 год. АО «KEGOC». - http://www.kegoc.kz/sites/default/files/content-manager/godovoy_otchet_2015g_na_sayt_rus_0.pdf (05.06.2017).

3. Список электростанций Казахстана. Википедия свободная энциклопедия. - https://ru.wikipedia.org/wiki/Список_электростанций_Казахстана#cite_note-kegoc_yr_2015-1 (05.06.2017).
4. Massachusetts Big Data project. Massachusetts Big Data Indicators 2015 research report published in March 2016. - <http://www.massbigdata.org/index.php/2015-report/> (06.06.2017).
5. Doug Laney. 3D Data Management: Controlling Data Volume, Velocity, and Variety. Gartner Blog. - <http://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf> (11.03.2017).
6. Иванов В.С., Рыжов А.П. Моделирование энергетических систем в рамках многоагентного подхода. - МГУ им. М.В. Ломоносова.
7. European technology platform for the electricity networks of the future. Smart Grids. - <http://www.smartgrids.eu> (09.06.2017).
8. Ледин С. Интеллектуальные сети Smart Grid — будущее российской энергетики. - Автоматизация и ИТ в энергетике. № 11 (16), 2010. - <http://www.sicon.ru/about/articles/?base=&news=16> (28.05.2017).
9. Bob Metcalfe. ENERNET. Internet Lessons for Solving Energy. Stanford University Computer Systems Colloquium May 20, 2009. <http://web.stanford.edu/class/ee380/Abstracts/090520slides.pdf> (03.06.2017).
10. Documentation of Apache Hadoop 2.6.0. The Apache Software Foundation. - <https://hadoop.apache.org/docs/r2.6.0/hadoop-project-dist/hadoop-hdfs/HdfsDesign.html> (30.04.2017).
11. Hadoop, часть 3: Pig, обработка данных. Блог компании Селектел. - <https://habrahabr.ru/company/selectel/blog/215307/> (17.05.2017).
12. А.В. Борщев. Практическое агентное моделирование и его место в арсенале аналитика 7. - www.anylogic.ru (10.06.2017).
13. В.Н. Сидоренко Системно-динамическое моделирование в среде powersim.
14. Dr. Enrique Kremers, Competence Cluster Intelligent Energy Systems EIFER, EDF R&D & KIT Modelling and simulation of intelligent energy systems: approach and case studies. Anylogic User Conference 2017 Paris 13.04.2017. - https://classic.anylogic.com/upload/presentations/anylogic_paris_seminar_presentations/simulating_intelligent_energy_systems_with_anylogic.pdf
15. Torres, S., O. Barambones, J. M. G. de Durana, F. Marzabal, E. Kremers and J. Wirges (2015). Agent-based modelling of electric vehicle driving and charging behavior. Control and Automation (MED), 2015 23th Mediterranean Conference.
16. Kremers, E., J. M. González de Durana, O. Barambones and A. Koch (2013). "Towards Complex System Design and Management in the Engineering Domain- the Smart Grid Challenge." Emergence: Complexity & Organization 15 (2, Complexity and the Smart Energy Grid): 14-22 C.
17. Kremers, E. A. (2013). Modelling and Simulation of Electrical Energy Systems through a Complex Systems Approach using Agent-Based Models. Karlsruhe, KIT Scientific Publishing. <http://dx.doi.org/10.5445/KSP/1000031133>

КРИПТОАЛГОРИТМДЕРДІҢ СТАТИСТИКАЛЫҚ ҚАУІПСІЗДІГІН ЗЕРТТЕУ

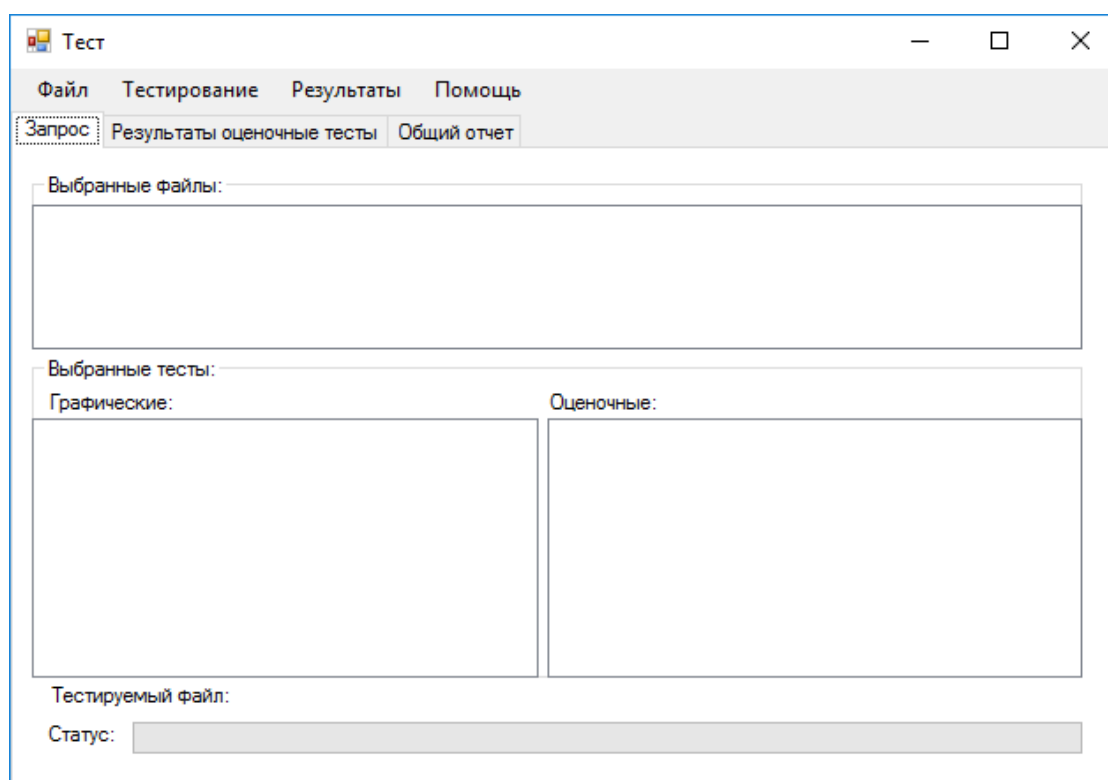
Капалова Н.А., Алгазы К.Т., Самрат С.М.
e-mail: nkapalova@mail.ru, kunbolat@mail.ru, sancho_samrat@mail.ru

ҚР БҒМ ҒК «Ақпараттық және есептеуіш технологиялар институты»

Аннотация. Бұл мақалада статистикалық тесттер жинағын қолдана отырып криптографиялық алгоритмдердің статистикалық қауіпсіздігін зерттеу, талдау және сапасын бағалау қарастырылған. Позициялы емес полиномды санау жүйесі негізінде құрылған шифрлеу алгоритмдерінің қасиеттері зерттеліп, өзара салытырылды.

Бүгінгі таңда жүргізіліп жатқан зерттеу жұмыстарының негізгі мақсаты әзірленген криптоалгоритмдердің статистикалық қауіпсіздігін бағалау. Ұсынылатын криптоалгоритмдерге қойылатын талаптардың бірі, оларды псевдокездейсоқ тізбек генераторы ретінде пайдалану жарамдылығы болып табылады. Ол үшін шифрмәтіндерді (алынған тізбектерді) статистикалық тесттерден өткізіп, нәтижелерін талдау керек.

Криптоалгоритмнің 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 әзірленді [1].



1-сурет. «Д.Кнуттың статистикалық тесттерді және графикалық тесттерді таңдаудың автоматтандырылған жүйесі» бағдарламасының басты терезесі

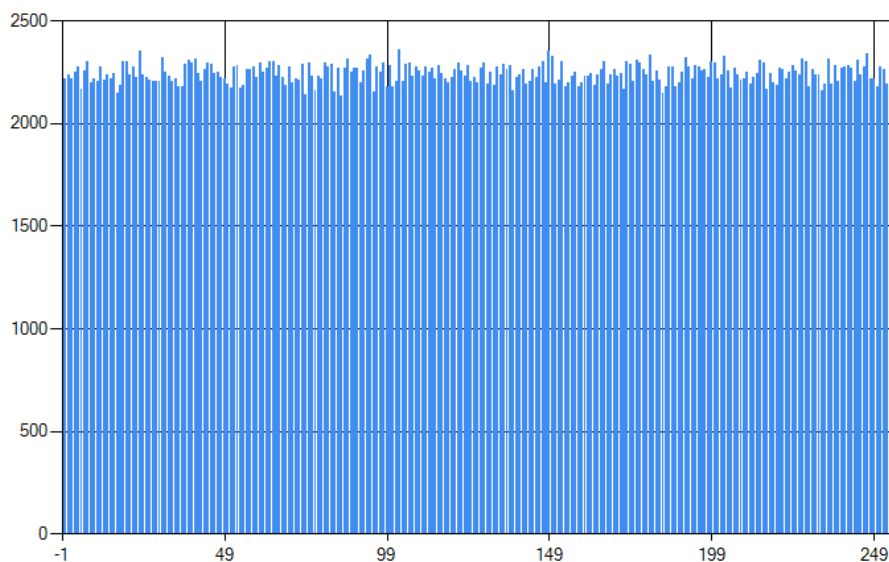
Псевдокездейсоқ тізбекті зерттеу үшін, екі тест тобы қолданылады [2].

- **Графикалық тесттер.** Тізбектің статистикалық қасиеттері графикалық тәуелдік түрінде көрсетіледі. Графикке қарап зерттелетін тізбек қасиеттеріне қорытынды жасалады.
- **Бағалау тесттері.** Тізбектің статистикалық қасиеттері сандық сипаттамалармен анықталады. Бағалау критерийлер негізінде талданатын және шын мәнінде кездейсоқ тізбек қасиеттерінің жақындық дәрежесіне қорытынды жасалады.

Графикалық тесттерге: тізбек элементтерін үлестіру гистограммасы; жазықтықта үлестіру; серияларды тексеру; монотондылыққа тексеру; автокорреляциялық функция (АКФ) және графикалық спектрлік тест жатады.

Тізбек элементтерін үлестіру гистограммасы. Бұл тест зерттелетін тізбектегі символдардың біркелкі таралғанын бағалауға және нақты символдың пайда болу жиілігін анықтауға мүмкіндік береді.

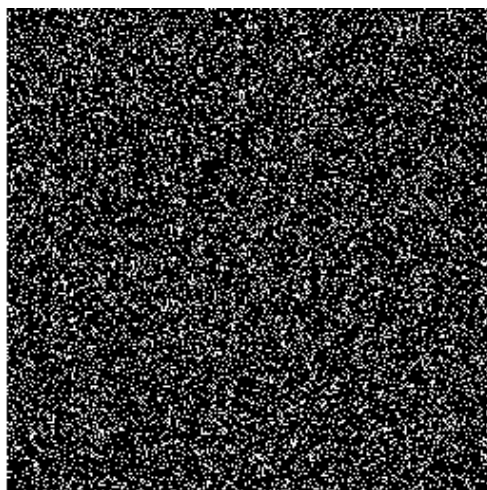
Гистограмманың құрылуы келесідей: зерттелетін тізбекте әрбір элементтің қанша рет кездескені есептеліп, кездесетін элементтердің санының сандық ұсынысқа (ASCII-байт мәні) тәуелді график құрылады.



2-сурет. Тізбек элементтерін үлестіру гистограммасы

Жазықтықта үлестіру. Бұл тест зерттелетін тізбектегі элементтердің арасындағы тәуелділікті анықтауға арналған.

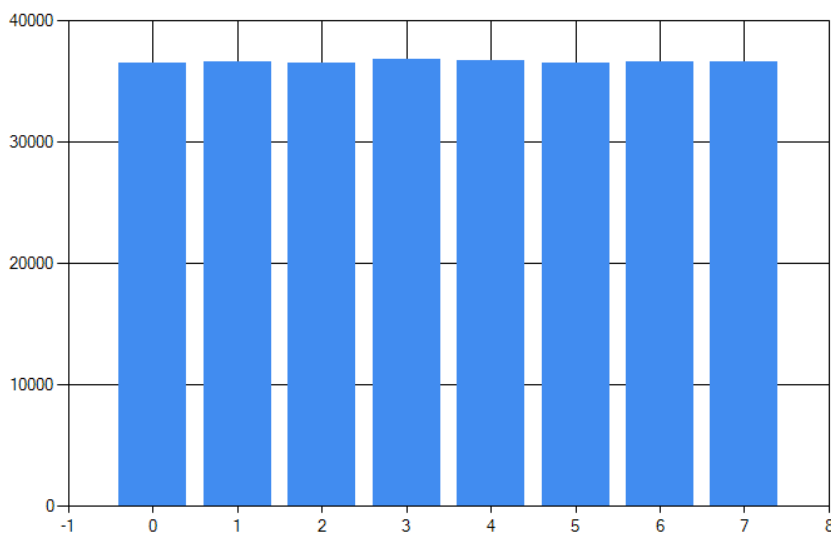
Жазықтықта үлестіру келесідей құрылады: $(2^R - 1) \times (2^R - 1)$ (R - зерттелетін тізбек сандарының разрядтылығы) өлшемді өріске координаталары $(\varepsilon_i; \varepsilon_{i+1})$ болатын нүктелер түсіріледі, мұндағы ε_i - зерттелетін тізбек элементтері, $i = 1, (n - 1), n$ - тізбек ұзындығы. Егер зерттелетін тізбектегі элементтердің арасындағы тәуелділік болмаса нүктелер ретсіз орналасады. Егер өрісте өрнектер көрінсе, тізбек кездейсоқ емес болады.



3-сурет. Жазықтықта үлестіру

Серияларды тексеру. Бұл тест зерттелетін тізбектегі символдардың арасындағы тәуелділікті нөл және бірлердің пайда болу жиілігі, k биттен тұратын серияларды талдау негізінде анықтауға мүмкіндік береді.

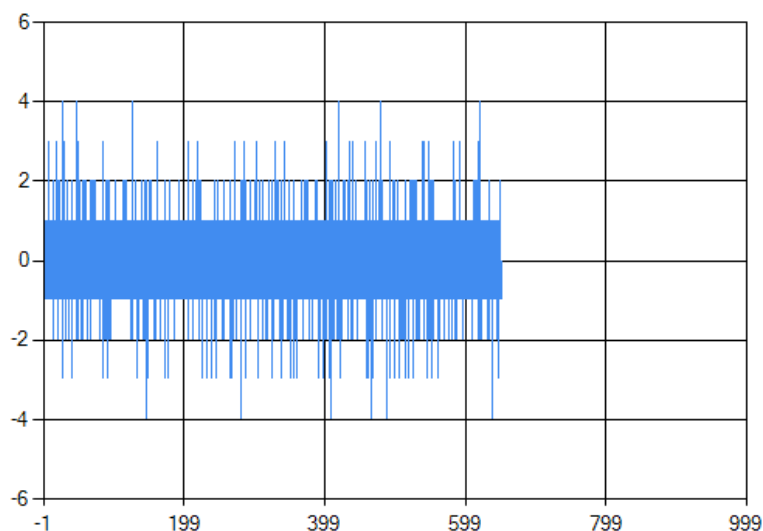
Нөл және бірлердің, екілік-серия (00, 01, 10, 11), үштік-серия (000, 001, 010, 011, 100, 101, 110, 111) және т.б. қанша екені саналады. Алынған нәтижелер график түрінде көрсетіледі.



4-сурет. Серияларды тексеру

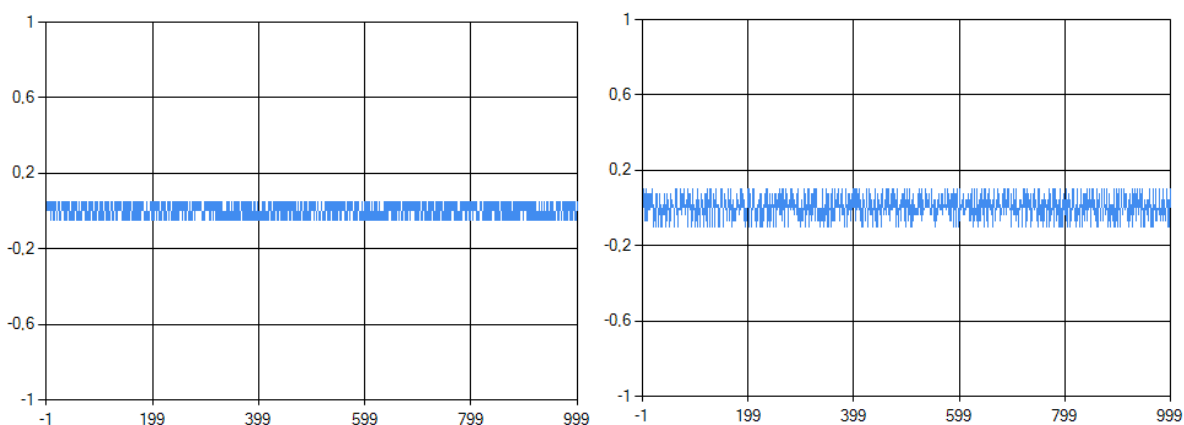
Монотондылыққа тексеру. Бұл тест зерттелетін тізбектегі символдардың арасындағы тәуелділікті тізбек элементтерінің өспейтін және кемімейтін аралықтарының ұзындықтарын талдау негізінде анықтауға мүмкіндік береді.

Тізбек элементтерінің жүйелі түрде қиылыспайтын өспейтін және кемімейтін аралықтары нәтижелер график түрінде көрсетіледі.



5-сурет. Монотондылыққа тексеру

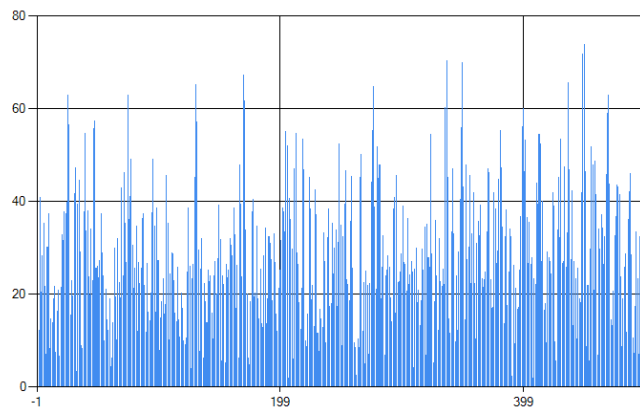
Автокорреляциялық функция (АКФ). Бұл тест зерттелетін тізбектің ығысқан көшірмелерінің арасындағы корреляцияны бағалауға арналған. Талданатын тізбектің тізбекшелерінің арасындағы тәуелділікті анықтай алады. Биттік және символдық АКФ болып бөлінеді.



6-сурет. Биттік және символдық автокорреляциялық функция

Графикалық спектрлік тест. Бұл тест Фурье түрлендіруінде шығарылу биіктігін талдау негізінде зерттелетін тізбекте 0 және 1 біркелкі үлестірілгенін тексереді.

$\varepsilon = \varepsilon_1 \varepsilon_2 \dots \varepsilon_n$ – ұзындығы n екілік тізбек болсын. Оны $x = x_1 x_2 \dots x_n$ (мұндағы $x_i = 2\varepsilon_i - 1$) тізбегіне түрлендіреміз ($1 \rightarrow 1, 0 \rightarrow -1$). x -ке дискретті Фурье түрлендіруін қолданып, гармоник тізбегін аламыз: $S = DFT(x)$. Алғашқы $n/2$ гармоникті графикте көрсетеміз. Шын мәнінде кездейсоқ тізбекте гармониктің орташа ұзындығынан едәуір асатын гармониктер саны нөлге ұмтылу керек. Кері жағдайда тізбек кездейсоқ емес болады.



7-сурет. Графикалық спектрлік тест

Бағалау тесттері беретін сандық сипаттама арқылы тесттің өткенін немесе өтпегенін нақты айтуға болады. Көп қолданылатын Д.Кнут және НИСТ тесттер жинағы.

Байланыссыз серияларды тексеру. Тест мақсаты — ұзындығы әртүрлі байланыссыз сериялардың ұзындықтарын талдау арқылы тізбекті кездейсоқтыққа тексеру.

Интервалдарды тексеру. Бұл тест барлық элементтері белгілі бір сандық интервалда болатын тізбекшелердің ұзындықтарын талдау арқылы зерттелетін тізбек символдарының біркелкі үлестірілгенін тексереді.

Комбинацияларды тексеру. Бұл тест тізбекшелердегі сандардың әртүрлі комбинацияларын талдау арқылы зерттелетін тізбек символдарының біркелкі үлестірілгенін тексереді.

Орын ауыстыруларды тексеру. Бұл тест тізбекшелердегі сандардың өзара орналасуын талдау арқылы зерттелетін тізбек символдарының біркелкі үлестірілгенін тексереді.

Монотондылыққа тексеру. Бұл тест тізбек элементтерінің өспейтін және кемімейтін аралықтарын талдау арқылы зерттелетін тізбек символдарының біркелкі үлестірілгенін тексереді.

Корреляцияны тексеру. Бұл тест тізбек элементтерінің өзара тәуелсіздігін тексереді.

Ақпараттық қауіпсіздік зертханасы криптоалгоритмнің төрт моделін әзірледі. Статистикалық қасиеттерін тексеру үшін барлық ұсынылған позициялы емес шифрлеу жүйесінің (ПШЖ) моделдеріне компьютерлік эксперименттер жүргізілді. Осы модификацияларды M1, M2, M3, M4 деп белгілейміз:

1. M1 – американдық DES стандарттың «Шифртекст бойынша блоктар тіркемі» шифрлеу режимін пайдаланатын ПШЖ модификациясы.

2. M2 – ресейлік ГОСТ 28147-89 стандарттың «Кері байланыспен гаммалау» шифрлеу режимін пайдаланатын ПШЖ модификациясы.

3. M3 – гаммалау процедурасын және алмастыру кестелерін пайдаланатын ПШЖ модификациясы.

4. M4 – шифрленетін деректер блогын алдыңғы және одан кейінгі өңдеу ретінде Фейстел желісін пайдаланатын ПШЖ модификациясы.

Бұл моделдерді компьютерлік зерттеу үшін қолданылған файлдар:

– өлшем мен кеңейтілімімен ерекшеленетін 12 файл;

– жұмыс негіздерінің саны бойынша ерекшеленетін K1, K2, K3, K4, K5 бес толық кілт;

Әр модель 12 түрлі файлды бес кілтпен шифрледі. Алынған 440 шифрленген мәтінді «Д.Кнуттың статистикалық тесттерді және графикалық тесттерді тандаудың автоматтандырылған жүйесі» бағдарламасының көмегімен статистикалық нәтижелерін алып, талдау жүргіздік.

Ұсынылған модельдер үшін графикалық тесттерді зерттеу келесілерді көрсетті:

– болашақ зерттеулерде талданатын шифртексттер ұзындығы 2^{20} биттен кем емес болуы керек.

– болашақ зерттеулерде талданатын шифртексттер саны әр моделге 1000-нан кем емес болуы керек.

Графикалық және бағалау тесттері бойынша зерттелетін шифртексттердің сапасын бағалаудан М3 және М4 моделдерінен алынған шифрленген файлдардың статистикалық қауіпсіздігі ең жоғары екенін көреміз. Сонымен қатар, әрбір қарастырылған модель тесттерде кілт пен файл типіне байланысты әр түрлі нәтижелер көрсететіні анықталды.

Пайдаланылған әдебиеттер тізімі:

1. Бияшев Р.Г., Нысанбаева С.Е., Капалова Н.А., Дюсенбаев Д.С. и др. / Отчет по НИР «Разработка и исследование моделей национального алгоритма шифрования на базе модулярной арифметики» ПЦФ О.0678, № госрегистрации 0115РК01304. Инвентарный номер 0215РК01452.

2. Иванов М.А., Чугунков И.В. Теория, применение и оценка качества генераторов псевдослучайных последовательностей. – М.: КУДИЦ-ОБРАЗ, 2003. – 240 с.

3. В. Столлингс Криптография и защита сетей: принципы и практика. 2-е изд. / Пер. С англ. – М.: Вильямс, 2001.

АЛГОРИТМ ШИФРОВАНИЯ НА SP-СЕТИ

Капалова Н.А., Хаумен А.

e-mail: kapalova@ipic.kz, haumen.armanbek@gmail.com

Институт информационных и вычислительных технологий КН МОН РК

Аннотация. В данной статье рассматриваются структуры и свойства алгоритма криптографической защиты информации, основанного на НПСС, сконструированного на SP-сети. Главной задачей работы является повышение стойкости алгоритма. В работе подробно описаны преобразования, благодаря которым достигается улучшение криптостойкости алгоритма. Рассматриваемый алгоритм основан на SP-сети. Причины использования SP-сети в данной модели, лежат в свойствах преобразований, используемых в этих сетях. В процессе шифрования используются преобразования, основанные на S-блоках и P-блоках. Известно, что эти преобразования могут противостоять криптоанализу. Помимо этого, в рассматриваемом алгоритме использованы преобразования, удовлетворяющие требования “лавиного эффекта”. В результате данной работы была разработана компьютерная программа, реализующая алгоритм шифрования, основанный на SP-сети.

В лаборатории информационной безопасности Института информационных и вычислительных технологий разработан симметричный блочный алгоритм шифрования данных на основе непозиционных полиномиальных систем счисления (НПСС), используя особенности модулярной арифметики [1-3].

В данной статье речь идет об одном варианте этого блочного алгоритма, названного «KazCrypt».

Шифр «KazCrypt» представляет собой симметричный алгоритм блочного шифрования с размером блока 128 бит и длиной ключа 128 бит.

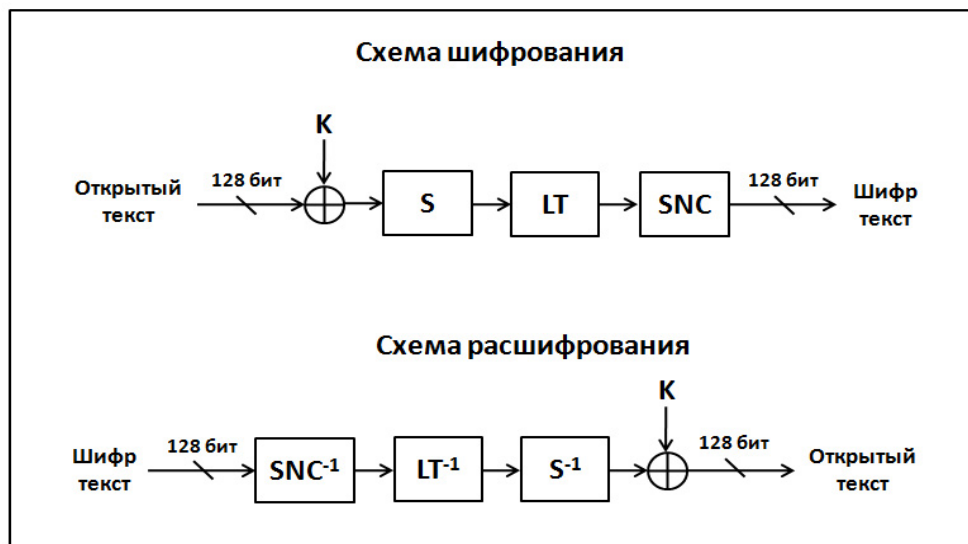


Рис. 1 – Схема алгоритма «KazCrypt»

Структура шифра является вариантом подстановочно-перестановочной сети (SP-сети), который состоит из наложения ключа с помощью операции побитового сложения (*xor*), нелинейной подстановки (*S*-блоков замен), линейного перемешивания *LT* и процедуры систем непозиционного шифрования (*CHШ*). Поэтому шифр принадлежит к классу *LSX*-шифров: его базовое преобразование (функция шифрования блока) представляется последовательными преобразованиями *LT* (линейное преобразование), *S* (подстановка) и *X* (смешивание с ключом). Отличие от подобных *LSX*-шифров, как *AES*, «Кузнечик», состоит в использовании процедур *CHШ* [4-5].

Алгебраически шифртекст *C* зависит от открытого текста *A* следующим образом:

$$C = SNC(LSX(A)).$$

Первой выполняется операция наложения ключа на блок открытого текста с помощью побитового сложения (*xor*). Как и в алгоритмах *AES*, «Кузнечик» нелинейное преобразование алгоритма «KazCrypt» использует операции с байтами, представляя их как элементы поля Галуа $F=GF(2^8)$.

Входной 128-битовый блок *A* алгоритма шифрования представляется в виде последовательности 16 байтов, которые нумеруются справа налево, начиная с 0: $A = a_{15} || a_{14} || a_{13} || \dots || a_1 || a_0$, где знаком $||$ обозначена операция конкатенации строк.

К каждому байту применяется нелинейная, биективная подстановка, задаваемая одномерным массивом, состоящих из 256 элементов.

$S(256) = (37, 127, 46, 108, 23, 56, 96, 51, 141, 33, 120, 84, 75, 5, 103, 69, 151, 9, 111, 185, 137, 146, 15, 171, 115, 191, 41, 181, 123, 132, 62, 6, 85, 101, 174, 27, 73, 226, 65, 211, 20, 149, 223, 36, 95, 113, 188, 39, 32, 164, 77, 202, 121, 144, 161, 91, 155, 60, 126, 153, 175, 24, 167, 0, 117, 180, 218, 43, 183, 12, 233, 204, 30, 213, 178, 52, 136, 162, 99, 159, 70, 195, 22, 237, 81, 220, 48, 107, 229, 87, 2, 109, 255, 68, 200, 17, 173, 40, 187, 55, 114, 245, 130, 241, 94, 209, 234, 193, 57, 197, 47, 147, 90, 232, 214, 243, 217, 61, 236, 1, 166, 35, 134, 216, 3, 118, 143, 72, 157, 7, 59, 206, 247, 254, 64, 252, 170, 199, 239, 14, 222, 190, 88, 179, 76, 168, 249, 160, 13, 251, 230, 242, 253, 71, 250, 246, 102, 19, 224, 129, 208, 26, 145, 98, 248, 44, 227, 125, 11, 156, 92, 231, 58, 212, 139, 78, 140, 54, 198, 221, 244, 201, 215, 240, 219, 238, 53, 203, 186, 110, 31, 172, 18, 225, 165, 86, 34, 235, 104, 29, 176, 112, 228, 8, 131, 207, 194, 25, 133, 189, 49, 124, 192, 119, 210, 205, 63, 82, 182, 38, 150, 42, 163, 122, 105, 4, 177, 184, 66, 196, 16, 154, 93, 106, 74, 142, 135, 158, 97, 10, 67, 148, 89, 28, 152, 80, 138, 100, 50, 169, 21, 128, 83, 45, 116, 79).$

Для выходного блока в целом нелинейная *подстановка* может быть определена как

$$S(A) = S(a_{15} || \dots || a_0) = S(a_{15}) || \dots || S(a_0).$$

Линейное перемешивание *LT* шифра «*KazCrypt*» проводится на два этапа. Байты блока размещаются в двумерный массив с размером 4×4 .

$$A = \begin{pmatrix} a_0 & a_1 & a_2 & a_3 \\ a_4 & a_5 & a_6 & a_7 \\ a_8 & a_9 & a_{10} & a_{11} \\ a_{12} & a_{13} & a_{14} & a_{15} \end{pmatrix}$$

Сначала байты в строке массива складываются между собой по модулю 256,

$$L(c_{ij}) = \sum_{i=0}^3 a_{ij} \bmod 256, j = \overline{0..3}$$

и полученный новый байт размещается вместо левого крайнего байта. А остальные байты сдвигаются вправо на одно место. Эта операция повторяется 4 раза для этой строки. В итоге мы получаем новых 4 байта. И так далее операция производится для каждой строки массива.

На следующем этапе выше изложенная операция производится по столбцам массива. Полученные новые байты в этом случае размещаются сверху вниз. После проведения преобразований *LT* байты в массиве получают новые значения.

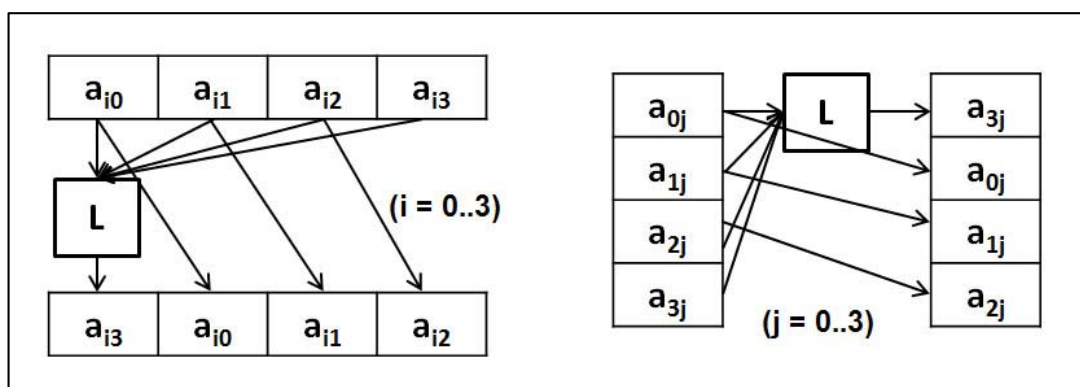


Рис. 2 – Схема преобразования LT

Главной целью использования преобразований LT , является обеспечение требования «лавинного эффекта» (*the avalanche effect*). «Лавинный эффект» – важное криптографическое свойство для шифрования, которое означает, что изменение значения малого количества битов во входном тексте или в ключе ведет к «лавинному» изменению значений выходных битов шифртекста. Другими словами, это зависимость всех выходных битов от каждого входного бита.

После этого преобразования полученные битовые последовательности отправляются на процедуру СНШ. Эта процедура шифрует блок битов на основе НПСС.

Опишем процедуру системы непозиционного шифрования [].

Вначале производится формирование НПСС: для этого выбираются рабочие основания, которыми являются неприводимые многочлены $p_1(x), p_2(x), \dots, p_S(x)$ над полем $GF(2)$ степени $m_1, m_2, \dots, m_S$ соответственно. Эти полиномы с учетом порядка их расположения образуют одну систему оснований. Все основания должны быть различными и в том случае, если они имеют одну степень. Рабочий диапазон НПСС

определяется многочленом (модулем) $P(x) = (p_1(x), p_2(x), \dots, p_S(x))$ степени $m = \sum_{i=1}^S m_i$

. Процедура выбора системы рабочих оснований (1) - это нахождению всевозможных решений алгебраического уравнения

$$k_1 m_1 + k_2 m_2 + \dots + k_S m_S = N, \quad (1)$$

где $0 \leq k_i \leq n_i$ - неизвестные коэффициенты, любой конкретный набор которых является одним из решений (1) и задает одну систему рабочих оснований; n_i - количество всех неприводимых многочленов степени m_i , $1 \leq m_i \leq N$, k_i - число выбранных неприводимых многочленов степени m_i , $S = k_1 + k_2 + \dots + k_S$ - число выбранных оснований.

Тогда сообщение (или его блок) длины N бит можно интерпретировать как последовательность остатков $\alpha_1(x), \alpha_2(x), \dots, \alpha_S(x)$ от деления некоторого многочлена $F(x)$ на рабочие основания $p_1(x), p_2(x), \dots, p_S(x)$ соответственно:

$$F(x) = (\alpha_1(x), \alpha_2(x), \dots, \alpha_S(x)). \quad (2)$$

Для шифрования используется ключевая последовательность длины N бит, которая также интерпретируется как последовательность остатков $\beta_1(x), \beta_2(x), \dots, \beta_S(x)$, но от деления некоторого другого многочлена $G(x)$ по тем же рабочим основаниям системы:

$$G(x) = (\beta_1(x), \beta_2(x), \dots, \beta_S(x)), \quad (3)$$

где $G(x) \equiv \beta_i(x) \pmod{p_i(x)}, i = \overline{1, S}$.

Для получения криптограммы $H(x) = (\omega_1(x), \omega_2(x), \dots, \omega_S(x))$ используется операция умножения многочленов (2) и (3). Тогда элементы последовательности вычетов $\omega_1(x), \omega_2(x), \dots, \omega_S(x)$ являются остатками от деления произведений $\alpha_i(x) \beta_i(x)$ на соответственные основания $p_i(x)$:

$$\alpha_i(x) \beta_i(x) \equiv \omega_i(x) \pmod{p_i(x)}, i = \overline{1, S}. \quad (4)$$

При расшифровании криптограммы $H(x)$ по известному ключу $G(x)$ для каждого значения $\beta_i(x)$ производится вычисление обратного (или инверсного) многочлена $\beta_i^{-1}(x)$ из условия выполнения следующего сравнения:

$$\beta_i(x) \times \beta_i^{-1}(x) = 1 \pmod{p_i(x)}, i = \overline{1, S} \quad (5)$$

В результате получается многочлен $G^{-1}(x) = (\beta_1^{-1}(x), \beta_2^{-1}(x), \dots, \beta_S^{-1}(x))$, инверсный к многочлену $G(x)$. Тогда исходное сообщение в соответствии с (4) и (5) восстанавливается через вычеты по следующим сравнениям:

$$\alpha_i(x) = \beta_i^{-1}(x) \omega_i(x) \pmod{p_i(x)}, i = \overline{1, S} \quad (6)$$

Таким образом, в рассмотренном алгоритме шифрования сообщения заданной длины N бит в НПСС полным ключом является выбранная система полиномиальных оснований $p_1(x), p_2(x), \dots, p_S(x)$, полученный при генерации псевдослучайных последовательности ключ $G(x) = (\beta_1(x), \beta_2(x), \dots, \beta_S(x))$ и инверсный к нему ключ $G^{-1}(x) = (\beta_1^{-1}(x), \beta_2^{-1}(x), \dots, \beta_S^{-1}(x))$, который вычисляется в соответствии с выражением (5).

Для реализации алгоритма шифрования на базе НПСС была разработана компьютерная программа «KazCrypt v2.2.0». Целью этой программной реализации является исследование статистических свойств алгоритма шифрования. Ключи для зашифрования и расшифрования хранятся в отдельном файле. Для исследования криптограмм на статистическую безопасность применялись графические и оценочные тесты. Для проверки статистических свойств зашифрованных файлов применялся разработанный программный комплекс «Автоматизированная система подборки статистических тестов Д.Кнута и графических тестов». Проведенное тестирование показало, что шифртексты обладают лучшими статистическими характеристиками по сравнению с исходным алгоритмом шифрования на базе НПСС. Но скорость выполнения процесса зашифрования снизилась, т.к. ключевая гамма генерируется для каждого блока отдельно.



Рис. 3 Главное окно программы «KazCrypt»

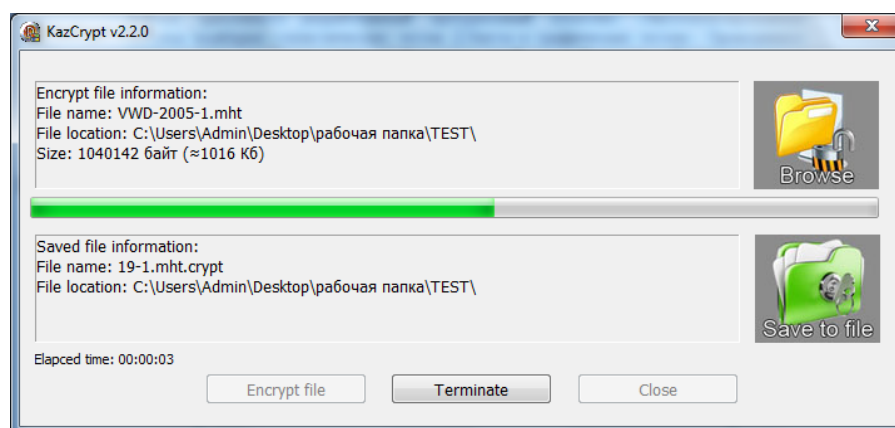


Рис. 4 Окно для шифрования файла

Литература

1. Бияшев Р. Г. Разработка и исследование методов сквозного повышения достоверности в системах обмена данными распределенных АСУ: дисс. докт. тех. наук: 05.13.06: защищена 09.10.1985: утв. 28.03.1986. - М., 1985.
2. Biyashev R., Kapalova N., Nyssanbayeva S., Haumen A., Construction and analysis of models of increasing reliability for modular encryption algorithm // Proceedings of the 10th International Conference on Computer Engineering and Applications (CEA '16). – Barcelona, Spain, 2016. –P. 161-165.
3. R. Biyashev, S. Nyssanbayeva, N. Kapalova , A. Haumen, Modified symmetric block encryption-decryption algorithm based on modular arithmetic // Proceedings of the International Conference on Wireless Communications, Network Security and Signal Processing (WCNSSP2016). –Chiang Mai, Thailand,2016. –P. 263-265. (Web of Science, Thomson Reuters)
4. Капалова Н.А., Хаумен А., Исследование модели алгоритма шифрования на базе непозиционных полиномиальных систем счисления // Сборник докладов 12-ой Международной Азиатской школы-семинар «Проблемы оптимизации сложных систем». – Новосибирск, 2016. – С. 264-268.
5. Капалова Н.А., Хаумен А. Позициялық емес полиномдық санау жүйесіне негізделген шифрлеу алгоритмінің SP-желі бойынша құрастырылған моделі // Вестник КазНУ, Физико-математические науки. – Алматы, 2017. – №3. С. 445-449.

ОДИН ЯЗЫК ДЛЯ СПЕЦИФИКАЦИИ ОНТОЛОГИЙ

Карабеков Б.С.¹⁾, Машеров Д.Е.²⁾, Плесневич Г.С.²⁾

e-mail: bskarabekov@mail.ru, salve777@mail.ru

1) *Институт информационных и вычислительных технологий КН МОН РК,
Казахстан,*

2) *Национальный исследовательский университет МЭИ, Москва, Россия*

Аннотация. Предложен язык для спецификации онтологий, синтаксис которого позволяет создавать описание моделируемой предметной области в форме предложений со структурой, приближенной к структуре фраз естественного языка. Представлен метод вывода для онтологий в предложенном языке, а также метод трансляции основного фрагмента этого языка в язык OWL.

1. Введение

Онтологии являются средством для представления знаний в информационных системах, разрабатываемых на основе методов инженерии знаний [1]. Онтологии служат существенным компонентом многих приложений, ориентированных на задачи, возникающие в Семантическом вебе (основанный на семантике доступ к Интернету), в бизнес-информатике, в медицинской и био-информатике, в роботике и т.п.

В различных областях применения онтологий предъявляются различные требования к языкам для спецификации онтологий. Стандартными языками онтологий, используемыми, в частности, в Семантическом вебе, являются RDF(S) и OWL (в различных диалектах) [2].

В настоящее время для OWL часто используется так называемый «Манчестерский синтаксис», который был создан для тех экспертов в прикладных областях, которые не привыкли к математической нотации (с логическими символами) [3]. Записанные в OWL 2 онтологии относят к классу «легковесных» (lightweight) онтологий, которые получают формализацией знания, не требующего сложных логических связей. OWL-онтологии основаны на дескриптивной логики, которая является узким фрагментом логики первого порядка [4].

Язык OWL адекватен для многих задач (например, в бизнес-информатике). Но для задач во многих областях (например, в роботике) нужны «весомые» (heavyweight) онтологии, для записи которых уже требуется логика, более сильная, чем дескриптивная. Михаил Кифер предложил фреймовую логику (F-logic) для представления знаний, которую он положил в основу языка для спецификации весомих онтологий [5]. Однако этот язык имеет нотацию, затруднительную для пользователей, не имеющих опыта работы с логическими языками.

Мы опишем язык онтологий, имеющий синтаксис, подобный Манчестерскому для OWL. Этот синтаксис удобен для экспертов и пользователей, так как дает им возможность описывать предметную область в виде предложений, имеющих структуру, приближенную к структуре фраз естественного языка. Этот язык (названный ЯЛС-2) разрабатывался в 2017 г. на этапах I и II выполнения проекта № 0115 RK 00532 МОН Казахстана.

2. Язык ЯЛС-2

Сначала рассмотрим пример составления онтологий в языке ЯЛС-2 для известной задачи Стимроллер (Steamroller – паровой каток). Эту задачу предложил Леонард Шуберт как просто формулируемую задачу, которая при формализации ее в языке дизъюнктов требует для решения очень большого числа резольвент. (Отсюда название «паровой каток».)

2.1 Задача «Стимроллер»

(а) Волки, лисы, птицы, гусеницы и улитки – животные.

(б) Классы «Волк», «Лиса», «Птица», «Гусеница» и «Улитка» – не пусты.

(в) Зерновые – растения.

(г) Класс «Зерновые» – не пуст.

(д) Каждое животное либо ест все растения, либо ест всех тех животных, которые его меньше и которые едят некоторые из растений.

(е) Гусеницы и улитки меньше птиц, а птицы меньше лис, которые, в свою очередь, меньше волков.

(ж) Волки не едят ни лис, ни зерновые, а птицы едят гусениц, но не едят улиток.

(з) Гусеницы и улитки едят некоторые из зерновых.

Задача состоит в доказательстве утверждения

(и) Существует животное, которое ест тех животных, питающихся зерновыми.

Составляя онтологию в языке ЯЛС-2 для задачи Стимроллер, введем имена Животное, Растение, Волк, Лиса, Птица, Гусеница, Улитка и Зерно для классов, а также имена Ест и Меньше для бинарных отношений.

Утверждения (а) – (и) запишем в языке ЯЛС-2 в виде следующих предложений:

(а):

Волк ISA Животное (2.1)

Лиса ISA Животное (2.2)

Птица ISA Животное (2.3)

Гусеница ISA Животное (2.4)

Улитка ISA Животное (2.5)

(б):

EXIST Волк (2.6)

EXIST Лиса (2.7)

EXIST Птица (2.8)

EXIST Гусеница (2.9)

EXIST Улитка (2.10)

(в):

Зерно ISA Растение (2.11)

(г):

EXIST Зерно (2.12)

(д):

EACH Животное:X Ест SOME Растение OR Ест EACH Животное THAT Меньше X AND Ест SOME Зерно (2.13)

(е):

EACH Гусеница Меньше EACH Птица (2.14)

EACH Птица Меньше EACH Лиса (2.15)

EACH Лиса Меньше EACH Волк (2.16)

(ж):

EACH Волк NOT Ест EACH (Гусеница OR Растение) (2.17)

EACH Птица Ест EACH Гусеница AND NOT Ест EACH Улитка (2.18)

(з):

EACH Птица Ест EACH Гусеница AND NOT Ест EACH Улитка (2.19)

(и):

EXIST Животное THAT Ест SOME Животное THAT Ест EACH Зерно (2.20)

В предложении (2.13) переменная *S* указывает на тождество примеров понятия. Таким образом, *S* играет роль местоимения.

Мы рассматриваем множество предложений $O = \{(2.1), (2.2), \dots, (2.19)\}$ как пример онтологии, записанной в языке ЯЛС-2. Решение задачи «Стироллер» состоит в автоматическом доказательстве, что предложение (2.20) логически следует из онтологии *O*. Это эквивалентно тому, что множество предложений $\{(2.1), (2.2), \dots, (2.19), \sim(2.20)\}$ невыполнимо, где $\sim(2.20)$ обозначает отрицание предложения (2.20). Отрицание предложения (2.20) в языке ЯЛС-2 записывается как

NULL Животное THAT Ест SOME Животное THAT Ест EACH Зерно (2.21)

2.2 Синтаксис и семантика языка ЯЛС-2

В языке ЯЛС-2 имеется три типа термов: С-термы, L-термы и Р-термы. С-термы обозначают классы объектов. Они интерпретируются как подмножества множества *Surr* суррогатов (идентификаторов объектов). Вот примеры С-термов:

Волк, Животное, NOT Волк, Волк OR Лиса,
Животное THAT Ест SOME Растение.

L-термы обозначают бинарные отношения. Они интерпретируются как подмножества множества *Surr* × *Surr*. Вот примеры L-термов:

Меньше, Ест, NOT Ест, Меньше AND NOT Ест.

P-термы обозначают одноместные предикаты, заданные на множестве *Surr* × *Surr*. Если *P* – P-терм и *X* – переменная, то $(X P)$ обозначает применение *P* к *X*. Одно и то же имя может обозначать класс или предикат. Вот примеры P-термов и их применений:

Волк, (X Волк), (объект21 Волк), Меньше EACH Волк,
(X Меньше EACH Волк)б

Here are the examples of P-terms:

Smaller, Smaller EACH (Wolf Fox),
LikesToEat SOME Plant.

Describing syntax and semantics of the language LSL-1, we will use the following syntactic classes:

- *c* for individual objects;
- *N* for concept names;
- *C, D, C_i* for C-terms (*i* = 1, 2, 3, ...);
- *L, M, L_i* for L-terms;
- *P, Q, P_i* for P-terms;
- *S, T* for sentences;
- *I* for sameness indicators *S, S1, S2, ...*

By “ α ” denote the value of an expression α of LSL-1 under an arbitrary fixed interpretation “ $_$ ”.

SYNTAX of C-terms:

$C_1 ::= \text{NOT } C_1 \mid (C_1 \text{ AND } C_1) \mid (C_1 \text{ OR } C_1) \mid N$;

$C ::= C_1 \mid C_1 \text{ THAT } P \mid \text{THOSE } P \mid C_1 : I$

SEMANTICS of C-terms:

“ C ” $\subseteq \text{Surr}$, “NOT C ” = $\text{Surr} \setminus “C”$, “ $C : I$ ” = “ C ”,

“ $C \text{ AND } D$ ” = “ C ” $\cap$ “ D ”, “ $C \text{ OR } D$ ” = “ C ” $\cup$ “ D ”,

“ $C \text{ THAT } P$ ” = $\{x \in “C” \mid “P”(x)\}$, “ $\text{THOSE } P$ ” = $\{x \mid “P”(x)\}$.

SYNTAX of L-terms:

$L_1 ::= \text{NOT } L_1 \mid L_1 \text{ AND } L_1 \mid L_1 \text{ OR } L_1 \mid N$;

$L ::= L_1 \mid \text{INV}(L_1)$;

SEMANTICS of L-terms:

“ L ” $\subseteq \text{Surr} \times \text{Surr}$, “NOT L ” = $\text{Surr} \times \text{Surr} \setminus “L”$,

“ $L \text{ AND } M$ ” = “ L ” $\cap$ “ M ”, “ $C \text{ OR } D$ ” = “ C ” $\cup$ “ D ”,

“ $\text{INV}(M)$ ” = $\{(x, y) \mid (y, x) \in “M”\}$.

SYNTAX of P-terms:

$P_1 ::= \text{NOT } P_1 \mid (P_1 \text{ AND } P_1) \mid P_1 \text{ OR } P_1 \mid N$

$P ::= P_1 \mid L \text{ SOME } C \mid L \text{ EACH } C \mid L \text{ ONLY } C \mid (L \mid) \mid (L \mid c)$.

SEMANTIC of P-terms:

“ $(x \mid P)$ ” $\Leftrightarrow “P”(x)$, “ $(x \text{ NOT } Q)$ ” $\Leftrightarrow \neg “Q”(x)$,

“ $(x \mid P \text{ AND } Q)$ ” $\Leftrightarrow “P”(x) \wedge “Q”(x)$,

“ $(x \mid P \text{ OR } Q)$ ” $\Leftrightarrow “P”(x) \vee “Q”(x)$,

“ $(x \mid L \text{ SOME } C)$ ” $\Leftrightarrow (\exists y \in “C”) (x, y) \in “L”$

“ $(x \mid L \text{ EACH } C)$ ” $\Leftrightarrow (\forall y \in “C”) (x, y) \in “L”$,

“ $(x \mid L \text{ ONLY } C)$ ” $\Leftrightarrow \forall y [(x, y) \in “L” \rightarrow y \in “C”]$,

“ $(x \mid (L \mid V))$ ” $\Leftrightarrow (x, “I”) \in “L”$,

“ $(x \mid (L \mid c))$ ” $\Leftrightarrow (x, “c”) \in “L”$.

SYNTAX of statements:

$S, T ::= \text{NOT } T \mid S \text{ AND } T \mid S \text{ OR } T \mid S \text{ IMP } T \mid$

$S = T \mid \text{EXIST } C \mid \text{EXIST } L \mid \text{NULL } C \mid$

$\text{NULL } L \mid C \text{ ISA } D \mid L \text{ ISA } M \mid C = D \mid$

$L = M \mid C = \text{NOT } D \mid L = \text{NOT } M \mid$

$\text{EACH } C \mid \text{SOME } C \mid$

SEMANTICS of statements:

“NOT T ” $\Leftrightarrow \neg “T”$, “ $S \text{ AND } T$ ” $\Leftrightarrow “S” \wedge “T”$,

“ $S \text{ OR } T$ ” $\Leftrightarrow “S” \vee “T”$, “ $S \text{ IMP } T$ ” $\Leftrightarrow “S” \rightarrow “T”$,

“ $S = T$ ” $\Leftrightarrow “S” \Leftrightarrow “T”$, “EXIST C ” $\Leftrightarrow “C” \neq \emptyset$,

P-terms denote unary predicates defined on the set Surr . Here are the examples of P-terms:

Smaller, Smaller EACH (Wolf Fox),

LikesToEat SOME Plant.

Describing syntax and semantics of the language LSL-1, we will use the following syntactic classes:

- c for individual objects;
- N for concept names;
- C, D, C_i for C-terms ($i = 1, 2, 3, \dots$);
- L, M, L_i for L-terms;
- P, Q, P_i for P-terms;
- S, T for sentences;
- I for sameness indicators $S, S_1, S_2, \dots$.

By “ α ” denote the value of an expression α of LSL-1 under an arbitrary fixed interpretation “ $_$ ”.

SYNTAX of C-terms:

$C_1 ::= \text{NOT } C_1 \mid (C_1 \text{ AND } C_1) \mid (C_1 \text{ OR } C_1) \mid N;$

$C ::= C_1 \mid C_1 \text{ THAT } P \mid \text{THOSE } P \mid C_1: I$

SEMANTICS of C-terms:

“ C ” $\subseteq \text{Surr}$, “NOT C ” = $\text{Surr} \setminus “C”$, “ $C:V$ ” = “ C ”,

“ $C \text{ AND } D$ ” = “ C ” $\cap$ “ D ”, “ $C \text{ OR } D$ ” = “ C ” $\cup$ “ D ”,

В предложении (2.13) переменная X указывает на тождество примеров понятия. Таким образом, X играет роль местоимения.

Мы рассматриваем множество предложений $O = \{(2.1), (2.2), \dots, (2.19)\}$ как пример онтологии, We introduce three types of terms in LLS-1: C-terms, L-terms and P-terms.

C-terms denote classes of objects. They are interpreted as subsets of the set Surr of surrogates. The examples of C-terms are

Wolf, Animal, Animal:S, NOT Wolf, Wolf OR Fox,

Animal THAT LikesToEat SOME Plant.

L-terms denote binary relations (links). They are interpreted as subsets of $\text{Surr} \times \text{Surr}$. The examples of L-terms are

MuchSmaller, LikesToEat, NOT LikesToEat,

MuchSmaller AND NOT LikesToEat.

P-terms denote unary predicates defined on the set Surr . Here are the examples of P-terms:

Smaller, Smaller EACH (Wolf Fox),

LikesToEat SOME Plant.

Describing syntax and semantics of the language LSL-1, we will use the following syntactic classes:

- c for individual objects;
- N for concept names;
- C, D, C_i for C-terms ($i = 1, 2, 3, \dots$);
- L, M, L_i for L-terms;
- P, Q, P_i for P-terms;
- S, T for sentences;
- I for sameness indicators $S, S_1, S_2, \dots$.

By “ α ” denote the value of an expression α of LSL-1 under an arbitrary fixed interpretation “ $_$ ”.

SYNTAX of C-terms:

$C_1 ::= \text{NOT } C_1 \mid (C_1 \text{ AND } C_1) \mid (C_1 \text{ OR } C_1) \mid N;$

$C ::= C_1 \mid C_1 \text{ THAT } P \mid \text{THOSE } P \mid C_1: I$

SEMANTICS of C-terms:

“ C ” $\subseteq \text{Surr}$, “NOT C ” = $\text{Surr} \setminus “C”$, “ $C:V$ ” = “ C ”,

“ $C \text{ AND } D$ ” = “ C ” $\cap$ “ D ”, “ $C \text{ OR } D$ ” = “ C ” $\cup$ “ D ”,

Существуют несколько подходов к записи информации в наноструктуры, один из них основывается на использовании тех или иных разновидностей процессов самоорганизации [4]. Однако применение таких методов в интересах молекулярного программирования сталкивается с серьезными затруднениями, прежде всего, связанными с тем, что процессы самоорганизации не позволяют адресно записывать последовательности логических переменных в заданные ячейки памяти.

В данной работе показано, что можно предложить несколько алгоритмов, которые обеспечивали бы запись информации в микро- и наномасштабные структуры при помощи макроскопических воздействий. Конечной задачей разработки такого рода алгоритмов является запись информации в молекулярные структуры за счет изменения

по заданному закону термодинамических переменных (температуры среды, ее кислотности и т.д.).

Один из таких алгоритмов основывается на использовании совокупности ячеек памяти, различающихся по порогу срабатывания. Следует подчеркнуть, что молекулярные системы, являющиеся аналогом триггера, т.е. способные находиться в двух различных устойчивых состояниях, известны. К ним относятся, например, любая макромолекула термочувствительного полимера (или ее фрагмент), обладающая гистерезисными свойствами [5].

Радиотехническим аналогом такой системы является совокупность бистабильных элементов (рис.1), на все входы которых одновременно подается один и тот же сигнал по общей шине данных. Задача состоит в том, чтобы обеспечить адекватную адресацию, т.е. запись строго определенной последовательности логических символов именно используя **общую** шину данных, что является аналогом изменения термодинамических переменных, которое также протекает **одновременно** для всех элементов системы.

Будем считать, что изменение состояния элемента (точнее, инверсия логической переменной, характеризующей состояние выхода) имеет место, если сигнал, поступающий на его вход, превышает порог срабатывания (по амплитуде). Будем также считать, что порог срабатывания элемента с номером $n+1$ рассматриваемой совокупности отличается на дискретную величину от порога срабатывания элемента с номером n :

$$U_{n+1} = U_n + \delta U \quad (1)$$

Реакцию системы в целом на входной импульс определенной амплитуды иллюстрирует рис.1. Рисунок подчеркивает, что если амплитуда импульса превышает порог срабатывания для элементов с номером 1 по номер n включительно, то логическая переменная, характеризующая состояние выхода каждого из этих элементов, будет инвертирована.

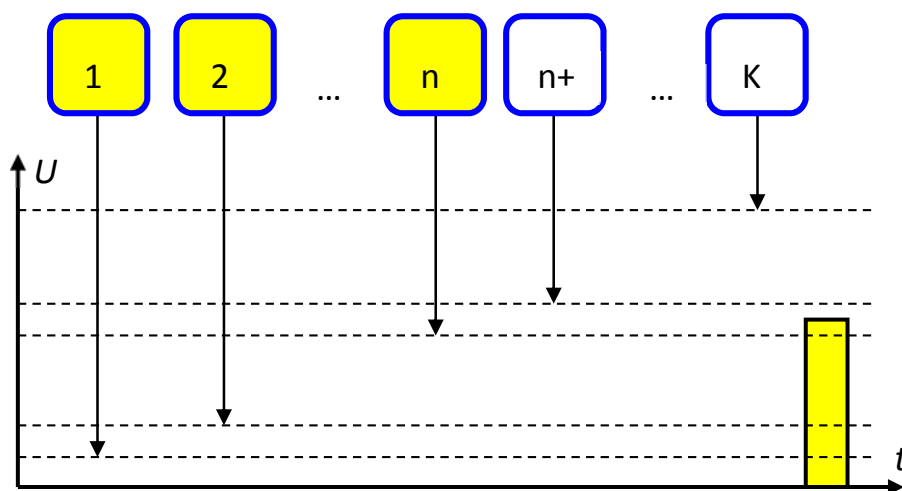


Рис.1. Реакция совокупности бистабильных элементов с дискретно отличающимися порогами срабатывания на внешний импульс

Покажем, что существует простой алгоритм записи произвольной последовательности логических переменных в такую систему ячеек.

Предположим, что требуется осуществить запись следующей последовательности

$$s_1, s_2, s_3, \dots, s_K \quad (2)$$

где s_i – логические переменные

Будем использовать следующие обозначения для последовательности импульсов, обеспечивающих запись информации в рассматриваемую систему ячеек.

- A_i есть логическая переменная, отражающая наличие импульса с амплитудой, обеспечивающей инверсию состояния ячеек с номерами с первого по i -тый включительно, в последовательности сигналов, обеспечивающих запись информации;

- $A_1, A_2, A_3, \dots, A_K$ есть последовательность, описывающая профиль сигнала, обеспечивающего запись информации в рассматриваемую совокупность ячеек; рис. 2 иллюстрирует характер описания профиля сигнала при помощи данной последовательности;

- L_i есть оператор, описывающий изменение состояния ячеек, составляющих рассматриваемую систему, при воздействии на нее импульса, отвечающего логической переменной A_i .

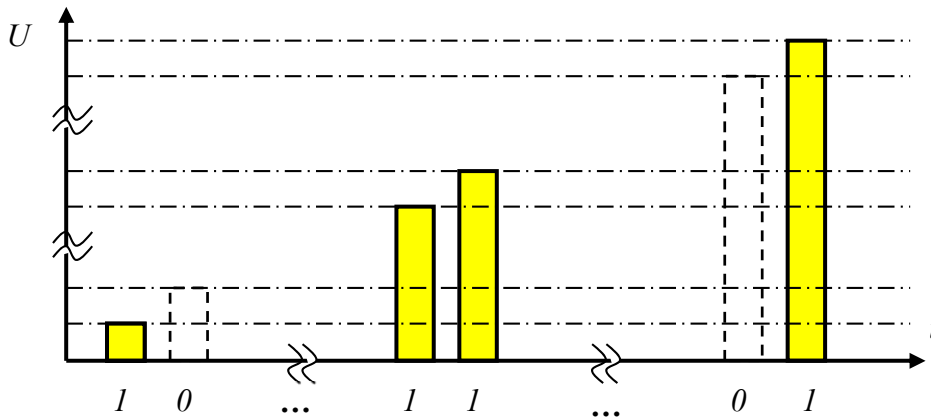


Рис.2. Соответствие профиля управляющего сигнала и последовательности логических переменных A_i

Тогда, воздействие импульса, отвечающего логической переменной A_i , на состояние системы в целом описывается следующим выражением

$$L_i(s_1, s_2, \dots, s_i, s_{i+1}, \dots, s_K) = (A_i + s_1, A_i + s_2, \dots, A_i + s_i, s_{i+1}, \dots, s_K) \quad (3)$$

где произведения логических переменных, стоящих под знаком скобки, подчиняются обычным правилам оперирования с логическими переменными

$$\begin{cases} 1 + s_n = 1, & s_n = 0 \\ 1 + s_n = 0, & s_n = 1 \end{cases} \quad (4)$$

для случая, когда $A_i = 1$; если $A_i = 0$, значения логических переменных s_n остаются неизменными.

Запись (4) подчеркивает также, что при ненулевом значении переменной A_i имеет место инверсия состояния ячеек с номером $n \leq i$.

Инвертируем последовательность (2)

$$s_K, s_{K-1}, s_{K-2}, \dots, s_1 \quad (5)$$

Это заведомо можно сделать, так как воздействие управляющих импульсов на все ячейки системы происходит одновременно.

Воздействие последовательности импульсов различной амплитуды на рассматриваемую систему описывается следующим произведением.

$$(A_K L_K, A_{K-1} L_{K-1}, \dots, A_1 L_1)(s_K, s_{K-1}, \dots, s_1) \quad (6)$$

Примем, что в исходном состоянии все ячейки находятся в состоянии, отвечающему логическому нулю. Тогда, задача о записи заданной последовательности логических переменных $(s_K, s_{K-1}, \dots, s_1)$ сводится к отысканию последовательности $(A_K, A_{K-1}, \dots, A_1)$ такой, что

$$(A_K L_K, A_{K-1} L_{K-1}, \dots, A_1 L_1)(0, 0, \dots, 0) = (s_K, s_{K-1}, \dots, s_1) \quad (7)$$

Будем решать задачу (7) пошагово. На состояние ячейки с номером K может повлиять только импульс максимальной амплитуды. В соответствии с записью (7) этот импульс поступает на входы ячеек последним.

Обозначим через

$$(s_K^{K-1}, s_{K-1}^{K-1}, \dots, s_1^{K-1}) \quad (8)$$

последовательность импульсов, которая формируется на такте с номером $K - 1$. Поскольку изначально предполагается, что все ячейки находятся в состоянии $s_n = 0$, то выражение (8) можно переписать в форме

$$(0, s_{K-1}^{K-1}, \dots, s_1^{K-1}), \quad (9)$$

так как все предыдущие импульсы не могут изменить состояние ячейки с максимальным значением порога срабатывания.

Следовательно, на основании соотношения (7) можно записать следующее уравнение на логические переменные, составляющие последовательность (9)

$$A_K L_K(0, s_{K-1}^{K-1}, \dots, s_1^{K-1}) = (s_K, s_{K-1}, \dots, s_1) \quad (10)$$

Из соотношения (10) немедленно следует, во-первых, что

$$A_K = s_K \quad (11)$$

а, во-вторых, что

$$s_n^{K-1} + A_K = s_n \quad (12)$$

или

$$s_n^{K-1} = s_n + A_K \quad (13)$$

где принято во внимание, что при любом значении логической переменной A_i имеет место

$$A_i + A_i = 0 \quad (14)$$

Таким образом, на следующем шаге решения уравнения (7) можно рассматривать последовательность, фактически содержащую число элементов на единицу меньше

$$A_{K-1}L_{K-1}(0, s_{K-2}^{K-2}, \dots, s_1^{K-2}) = (s_{K-1} + A_K, s_{K-2} + A_K, \dots, s_1 + A_K) \quad (15)$$

В соотношении (15) принимается во внимание, что до прихода импульса с амплитудой, отвечающей оператору L_{K-1} , состояние элемента с номером $K - 1$ заведомо отвечает условию $s_{K-1} = 0$, так как на вход каких-либо элементов системы еще не поступал импульсов, способных изменить его состояние (все они обладали недостаточной амплитудой). Следовательно,

$$A_{K-1} = s_{K-1} + A_K \quad (16)$$

$$s_n^{K-2} + A_{K-1} = s_n + A_K, \quad n \leq K - 2 \quad (17)$$

или

$$A_{K-1} = s_{K-1} + s_K \quad (18)$$

$$s_n^{K-2} = s_n + A_K + A_{K-1}, \quad n \leq K - 2 \quad (19)$$

Используя соотношения (11) и (18), выражение (19) можно переписать в виде

$$s_n^{K-2} = s_n + s_{K-1}, \quad n \leq K - 2 \quad (20)$$

где также принимается во внимание, что

$$s_i + s_i = 0 \quad (21)$$

Действуя далее по индукции, можно видеть, что искомые коэффициенты, описывающие последовательность импульсов, обеспечивающих запись информации в рассматриваемую систему ячеек, выражаются формулой

$$A_{m-1} = s_{m-1} + s_m \quad (22)$$

Формулы (11) и (22) представляют собой решение уравнения (7), т.е. составляют алгоритм, позволяющий осуществить запись произвольной последовательности логических переменных в совокупность бинарных ячеек рассматриваемого типа.

Таким образом, существует возможность реализовать запись информации с адресацией за счет одновременного воздействия на все без исключения ячейки памяти системы. Это создает необходимые предпосылки для реализации систем молекулярного программирования, в которых запись заданной программы в наноструктуры обеспечивается за счет изменения термодинамических переменных по заданному закону.

Литература

1. Staab S., Studer R. (Eds), Handbook on Ontologies in Information Systems, Springer 2003.
2. Allemang D., Hendler J. Semantic Web for the Working Ontologist (Effective Modeling in RDFS and OWL). Elsevier, 2011.
3. OWL 2 Web Ontology Language Manchester Syntax – <http://www.w3.org/TR/2012/NOTE-owl2-manchester-syntax-20121211/>.
4. Baader F., McGuinness D., Nardi D., Patel-Schneider P. (Eds.) The Description Logic Handbook (theory, implementation, and applications), Cambridge University Press, 2010.
5. Kifer M. Rules and Ontologies in F-logic // Reasoning Web, LNCS 3564, Springer, 2005.
6. 2003 Сулейменов, И. Э. Молекулярное программирование: аналогия с радиотехническими системами / И. Э. Сулейменов, С. В. Панченко, М. А. Ердаулетова // Известия НТО «Кахак», 2015, № 4(51). – С.77-84.
7. Барышников, А. Ю. Наноструктурированные липосомальные системы как средство доставки противоопухолевых препаратов / А. Ю. Барышников // Вестник Российской академии медицинских наук. – 2012. – Т. 67. – №. 3.
8. Иванов, Р. В., Балакин К. В., Шоболов Д. Л., Федотов Ю. А., Калмыков Ю. М. Разработка систем доставки лекарственных средств с применением микро- и наночастиц – <http://cyberleninka.ru/article/n/razrabotka-sistem-dostavki-lekarstvennyh-sredstv-s-primeneniem-mikro-i-nanochastits> (дата обращения: 03.06.2017).
9. Ергожин, Е. Е. Гидрофильные полимеры в нанотехнологии и наноэлектронике (монография) / Е. Е. Ергожин, А. Б. Зезин, И. Э. Сулейменов, Г.А. Мун // Алматы-Москва: Издательство LEM, Библиотека нанотехнологии, 2008. – 214 с.

РАЗРАБОТКА ФИЗИКО-МАТЕМАТИЧЕСКОЙ МОДЕЛИ ТЕПЛОФИЗИЧЕСКОГО СОСТОЯНИЯ ТЕЛ С УЧЕТОМ ОДНОВРЕМЕННОГО НАЛИЧИЯ ЛОКАЛЬНЫХ ТЕПЛОИЗОЛЯЦИЙ, ТЕМПЕРАТУР, ТЕПЛООБМЕНОВ И ТЕПЛОВЫХ ПОТОКОВ И ИХ РЕАЛИЗАЦИЯ НА ПК

Кудайкулов А.К., Ташев А.А., Аскарова А.
e-mail: kudaykulov2006@mail.ru

*Институт информационных и вычислительных технологий КН МОН РК,
Казахстан*

Аннотация. Разработана физико-математическая модель неустановившегося теплофизического состояния тел с учетом одновременного наличия локальных теплоизоляций, температур, теплообменов и тепловых потоков и их реализация на ПК.

Рассматривается горизонтальный стержень длиной l [см] (рисунок 1) изготовленного из жаропрочного материала, площадью поперечного сечения которого есть $F [см^2] = const$. Горизонтальная ось OX направлен слева на право и совпадает с осью

исследуемого стержня. Через правый торец стержня происходит теплообмен с окружающей средой. Температура окружающей среды $T_{oc} (^{\circ}C) = \text{const}$, коэффициент теплообмена $h\left(\frac{Bm}{cm^2 \cdot ^{\circ}C}\right) = \text{const}$. На площади поперечных сечений правого конца

стержня подведен тепловой поток с интенсивностью $q\left(\frac{Bm}{cm^2}\right) = \text{const}$.

Оценивалось не установившееся теплофизическое состояние следующих характеристик стержня по времени [1-2]:

- 1) Удлинение стержня $\Delta\ell$ в зависимости от $T(x)$, которая определяется как: для линейного случая:

$$\Delta\ell = \int_0^{\ell} \alpha T(x) dx = \frac{\alpha\ell}{2} (T_i + T_j)$$

для квадратичного случая:

$$\Delta\ell = \int_0^{\ell} \alpha T(x) dx = \frac{\alpha\ell}{2} (T_i + 4T_j + T_k)$$

- 2) Осевое термическое усилие R :

$$R = -\frac{\Delta\ell EF}{\ell}.$$

- 3) Термо-упругое напряжение σ :

$$\sigma = \frac{R}{F} = -\frac{\Delta\ell E}{\ell}.$$

- 4) Термо-упругая деформация ε :

$$\varepsilon = \frac{\sigma}{E} = -\frac{\Delta\ell}{\ell}.$$

- 5) Температурная деформация $\varepsilon_T(x)$:

$$\varepsilon_T(x) = -\alpha T(x).$$

- 6) Температурное напряжение $\sigma_T(x)$:

$$\sigma_T(x) = E \varepsilon_T(x).$$

- 7) Упругая деформация $\varepsilon_x(x)$:

$$\varepsilon_x(x) = \varepsilon - \varepsilon_T(x).$$

Для апробаций разработанной физико-математической модели были использованы следующие исходные данные:

$$L = 7,5 \text{ см}; \quad q = -150 \frac{Bm}{cm^2}; \quad k_{xx} = 75 \frac{Bm}{cm \cdot ^{\circ}C}; \quad h = 10 \frac{Bm}{cm^2 \cdot ^{\circ}C}; \quad T_{oc} = 40^{\circ}C; \quad r = 1 \text{ см};$$

$$F = \pi r^2 = \pi cm^2; \quad P = 2\pi r = 2\pi \text{ см}; \quad \alpha = 0,0000125 \frac{1}{^{\circ}C}.$$

Задача заключалась в определении не установившегося состояния температур, и всех составляющих деформации, напряжения, а также величин удлинения стержня и возникающего осевого усилия.

Нестационарная часть установления температуры на концах и в середине стержня по времени представлен на рисунке 1

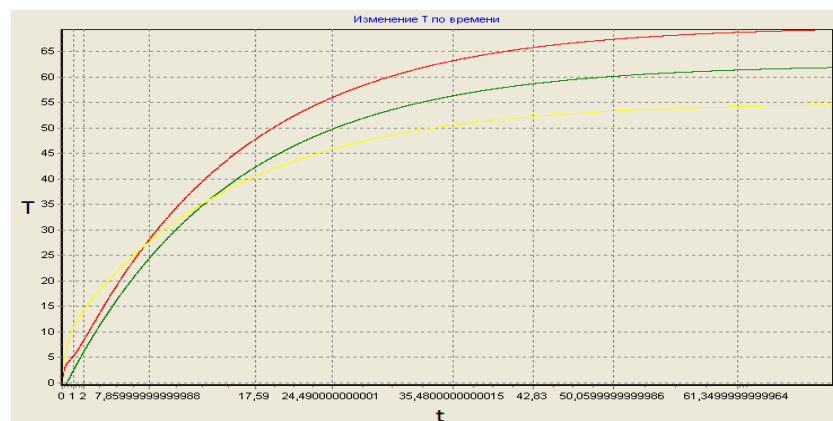


Рис. 1. Изменение температуры по времени

Все составляющие деформации, напряжения, а также величин удлинения стержня и возникающее осевое усилие вычислены на основе изменения температуры по времени.

Изменение удлинения по времени показана на рисунке 2

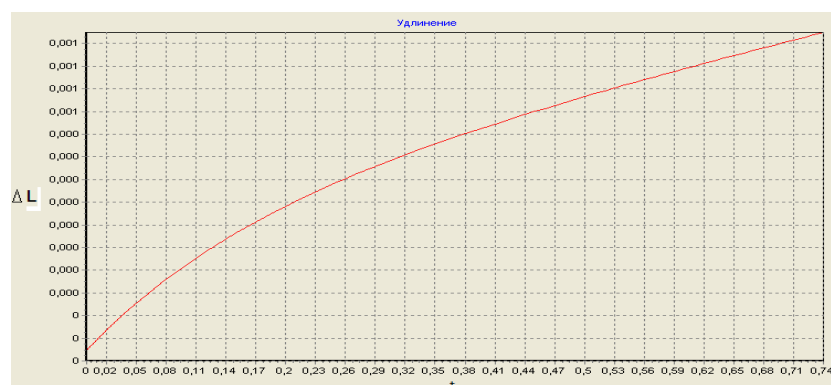


Рис. 2. Изменение удлинения по времени

Изменение осевого термического усилия по времени показана на рисунке 3.

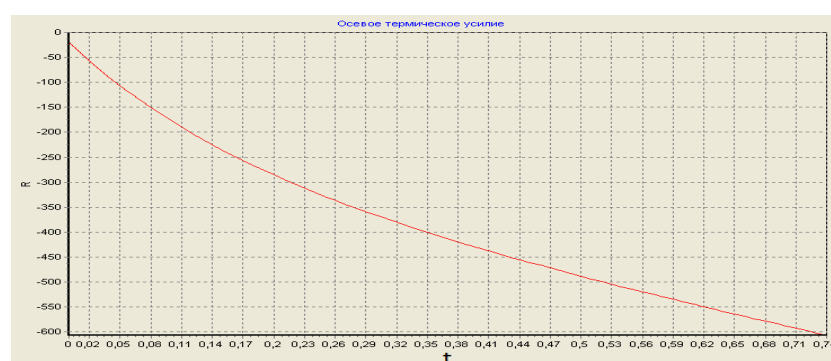


Рис. 3. Изменение осевого термического усилия по времени

Изменение термоупругого напряжения по времени показана на рисунке 4.

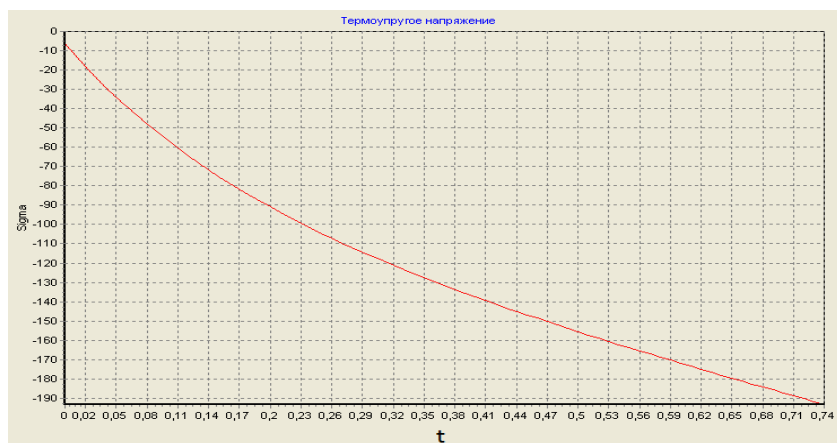


Рис. 4. Изменение термоупругого напряжения по времени

Изменение термоупругой деформации по времени показана на рисунке 5.

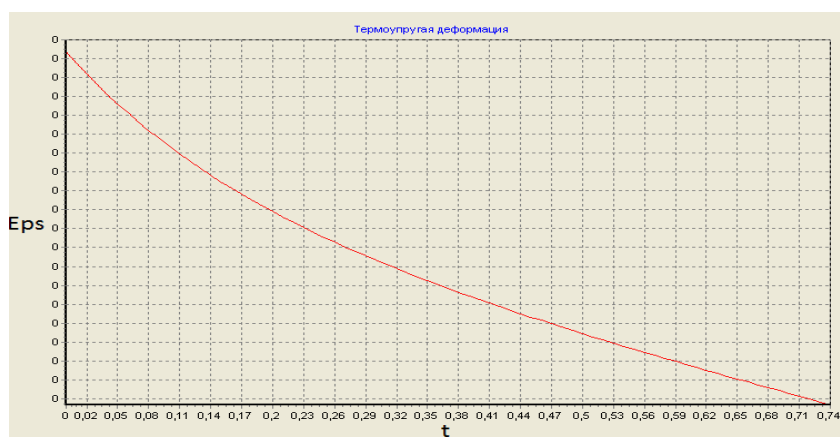


Рис. 5. Изменение термоупругой деформации по времени

Изменение температурного напряжения по времени показана на рисунке 6.

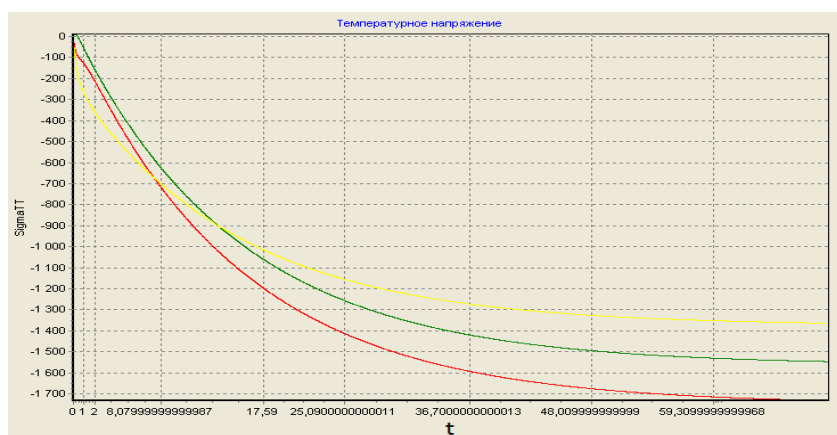


Рис. 6. Изменение температурного напряжения по времени

Изменение упругой деформации по времени показано на рисунке 7.

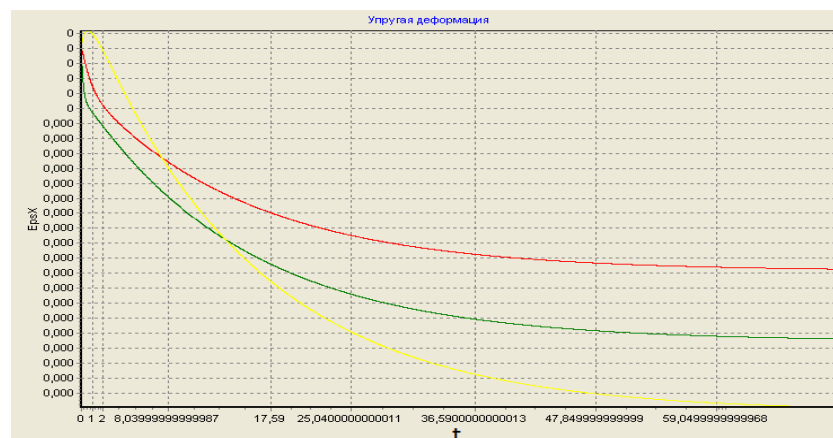


Рис. 7. Изменение упругой деформации по времени

Изменение упругого напряжения по времени на рисунке 8.

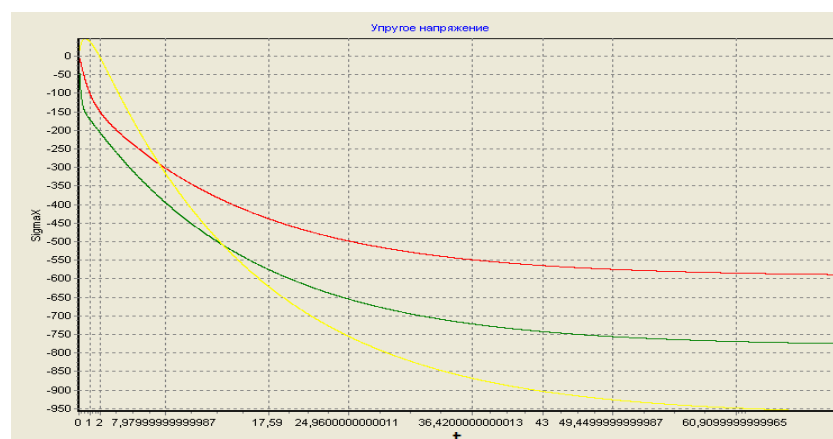


Рис. 8. Изменение упругого напряжения по времени

Далее, рассматривается физико-математическая модель теплофизического состояния тел установившегося процесса с учетом одновременного наличия внутренних точечных источников тепла и других наружных источников тепла.

Рассматривается горизонтальный стержень, описанный на рисунке 1.

Разработана физико-математическая модель теплофизического состояния тел изготовленного из жаропрочного материала с использованием вариационного подхода [3].

Для апробаций разработанного алгоритма и метода были использованы следующие исходные данные:

$$L = 100 \text{ см}; \quad q = -500 \frac{\text{Вт}}{\text{см}^2}; \quad k_{xx} = 100 \frac{\text{Вт}}{\text{см} \cdot ^\circ\text{C}}; \quad h = 10 \frac{\text{Вт}}{\text{см}^2 \cdot ^\circ\text{C}}; \quad T_{oc} = 40^\circ\text{C}; \quad r = 1 \text{ см};$$

$$F = \pi r^2 = \pi \text{ см}^2; \quad P = 2\pi r = 2\pi \text{ см}; \quad \alpha = 0,0000125 \frac{1}{^\circ\text{C}}.$$

На рисунке 9 приводится закон распределения температуры по длине стержня.

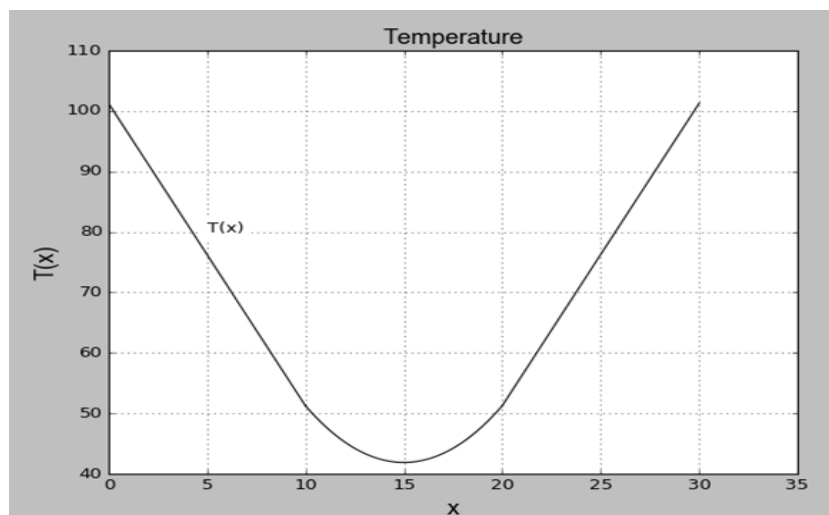


Рис. 9. Закон распределения температуры по длине стержня

Закон распределения всех составляющих деформации по длине стержня показан на рисунке 10.

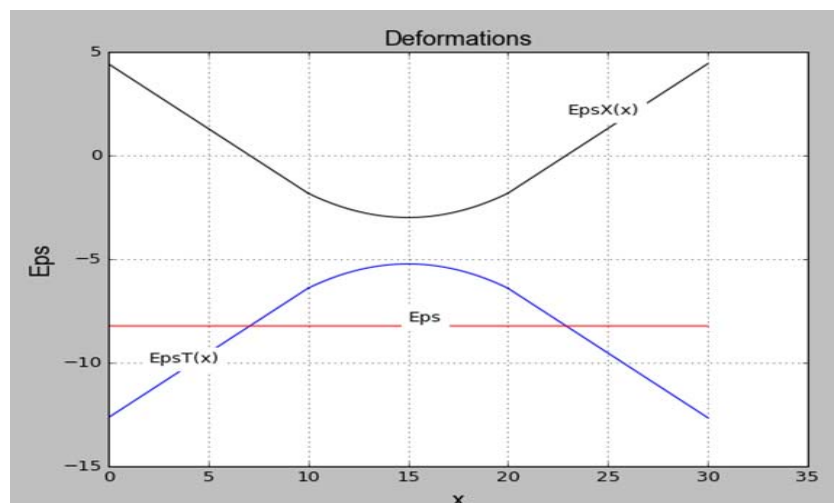


Рис. 10. Закон распределения всех составляющих деформации по длине стержня

Из рисунка 10 видно, что значение термоупругой составляющей деформации постоянно по всей длине стержня ($\epsilon = \text{const}$), что означает их сжимающий характер. А закон распределения температурной составляющей имеет симметричный вогнутый характер. По всей длине стержня $\epsilon_T(x) < 0$, и имеет сжимающий характер. При этом наибольшее значение соответствует к участкам стержня ближе к заземленным концам. Наименьшее значение приходится к середине стержня, где происходит теплообмен с окружающей средой. Закон распределения упругой составляющей $\epsilon_x(x)$ имеет выпуклый квадратичный характер, а на участках с заземленными концами $\epsilon_x(x) > 0$, т.е. имеет растягивающий характер. В средних сечениях $\epsilon_x(x) < 0$, т.е. имеет сжимающий характер.

Законы распределения всех составляющих напряжений по длине стержня приводится на рисунке 11.

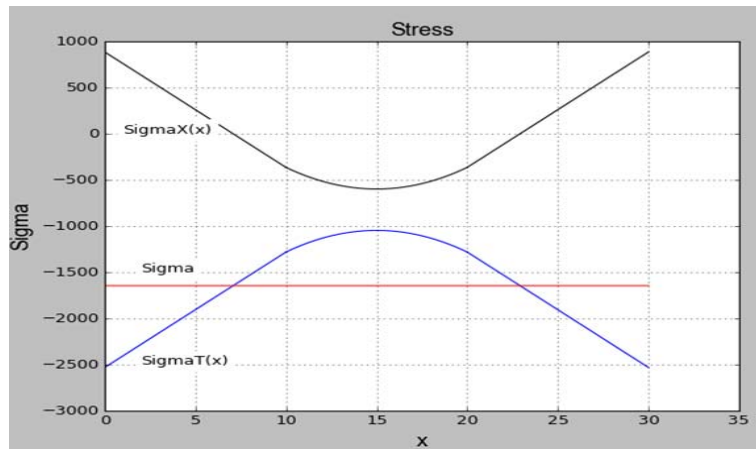


Рис. 11. Закон распределения всех составляющих напряжения по длине стержня

Из-за пропорциональности, характер составляющих напряжения такие же, как в случае деформации.

Закон распределения перемещения сечений по длине стержня приведены на рисунке 12.

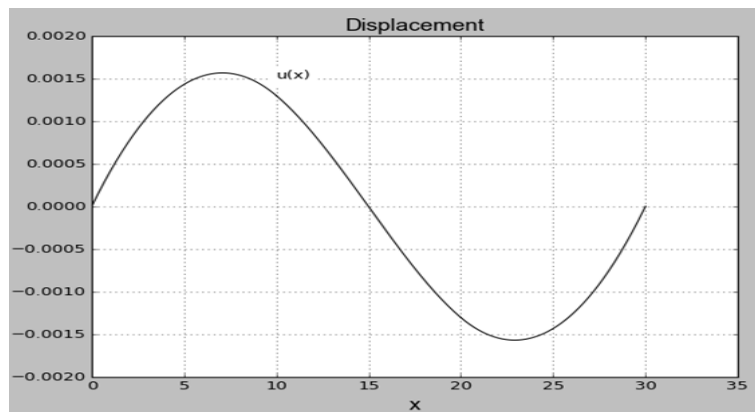


Рис. 12. Закон распределения перемещения по длине стержня

Как видно из рисунка перемещения сечений двух зашеченных концов и середины сечения равны нулю. На участке $0 \leq x \leq \frac{L}{2}$ сечения перемещаются слева направо, а на участке $\frac{l}{2} \leq x \leq L$ - справа налево. Это обусловлена наличием симметричных источников тепла, подведенных на концах стержня. Амплитуда перемещения середины первого и второго участков стержня равны по модулю. Эта объясняется симметричностью исследуемого процесса.

Результаты применения предложенного подхода, основанной на фундаментальном законе сохранения энергии, для решения конкретного примера показывают, что его можно использовать при решении актуальных инженерных задач разной сложности. Эти решения характеризуются повышенной точностью и адекватностью позволяет решать практически любые задачи, связанные с определением термомеханического состояния стержня.

Литература

- 1 Meyers G.E. Analytical Methods in Conduction Heat Transfer, McGraw-Hill, N.Y., 1971
- 2 Timoshenko S.P., Goodier J.N., Theory of Elasticity, McGraw-Hill, N.Y., 1970
Larry J. Segerlind. Applied Finite Element Analysis, 2nd Edition. 448 pages, February 1985, ©1984

MODELLING SERVICES INFRASTRUCTURE IN THE INTEGRATED SYSTEM OF CROSS-BORDER INFORMATION EXCHANGE

Magzom M.M., Begimbayeva Ye.Ye., Biyashev R.G., Nyssanbayeva S.E.
e-mail: magzomxzn@gmail.com

*Institute of Information and Computational Technologies of MES RK Almaty, 050010,
Republic of Kazakhstan*

Abstract. *Information exchange between interacting sides in the informational space of CIS and EAEU countries is provided by the creation and use of the national segments and an integration gateway. This paper describes the structural scheme of a national segment of the cross-border information exchange. These segments are a complex of secured systems of data transmission, which included to each interacting side's nodes.*

Keywords: cross-border information exchange, integrated system, digital signatures.

Introduction

The development and research of the models and methods of protected cross-border information exchange are based on the following initial package of legal documents:

- agreement on establishment, operation and development of the integrated information system of foreign and mutual trade in the Customs Union;
- agreement on application of information technologies in the exchange of electronic documents in foreign and mutual trade within the common customs territory of the Customs Union;
- «The Model and Methodology on formation of transboundary trust space in the Internet Network».

These documents define objectives, functions and procedures for the creation of international information systems.

Cross-border interaction is the interaction of subjects of different legal fields. Consequently, the unresolved complex of organizational, technological and legal issues of the legal significance of electronic information in the integrated system is one of the major problem in cross-border information interaction.

The main problems of ensuring information interaction is to develop an effective and reliable rights management mechanism of subject and provide each side of this interaction its own information security and protection of their informational independence.

One of key directions of work on the creation and implementation of integrated information system of the Eurasian Economic Union (EAEU or EEU) are solving problems of reliable and effective integration of geographically distributed state information resources and information systems of the member countries, ensuring interaction of authorities of the Member

States in electronic form, including opportunities of legally valid electronic documents exchange [1].

Electronic data exchange between interacting sides in the integrated system is provided by creation and use of the national segments and integration gateway.

Model of national segment's structure

Functional nodes in a national segment can be formed on the base on different services: a digital signature service, key generation service, timestamp service, notary service, location service, a trusted storage service and etc.

Each service can have several options of implementation, whereas their description approach can be based on the concepts of centralization/decentralization and mono/multi-jurisdiction.

Depending on the requirements of interacting parties, only particular services can be chosen to operate with. To provide a flexible integration of selected services so called microservices architecture is applied [2].

This architectural style suggests that a unified information system built as a small set of services, each of which runs on its own hardware and software platform and communicates within the system through a variety of protocols.

These microservices developed around the specific requirements of the parties. They can be written in different programming languages and can use different technologies for data processing and storage. They can be developed and integrated into the trusted information environment by different organizations and developers that have the appropriate authority.

Client applications of interacting parties communicate with the particular instances of microservices, depending on the purpose and stages of communication: receiving an encryption key, to obtain the certificate, signature confirmation, receipt of the timestamp, etc.

Communication between the system nodes must be cryptographically protected. Each country uses their own cryptographical systems in their national segment. These systems must implement the means of providing symmetrical and asymmetrical encryption, key exchange mechanism, digital signature verification, etc.

For the national segment of Kazakhstan several models of cryptographic systems were developed [3,4].

Model of cryptographic systems in the national segment

In the cross-border exchange of information, each of the communicating parties develops their national cryptographic means. Proposed algorithms are developed on the base of nonpositional polynomial notation systems (NPNs) or a polynomial residual notation system (RNS). Classical modular arithmetic is based on the Chinese remainder theorem, which states that any number can be represented by their remainders (residues) from its division by the base numbers (moduli) systems, which are formed pairwise prime numbers [5]. In polynomial RNS moduli are represented by irreducible polynomials with coefficients over the GF(2). The usage of NPNs allows improving durability and efficiency of nonpositional cryptographic algorithms without increasing the length of secret key.

Improved efficiency is provided by the rules of NPNs in which all arithmetic operations can be performed in parallel to the base module NPNs. In nonpositional cryptosystems the cryptostrength is characterized by a complete secret key. Cryptostrength in this case depends not only on the length of a key sequence, but also on choice of a system of polynomial bases. With the growth of the order of irreducible polynomials with binary coefficients, their number also grows rapidly. The greater the length of the input block, the more choices of working

systems bases are possible. Therefore, the cryptostrength of the proposed encryption algorithm against brute-force attack significantly increases with the length of the electronic message.

As a symmetric encryption algorithm, different models, based on Feistel network and block cipher modes, were proposed [4,6]. The application of Feistel scheme is considered as a pre- and postprocessing of data block.

Unlike traditional Feistel network where the input data is a plain text message, the input of the modified postprocessing Feistel scheme is supplied by the bit sequence of ciphertext, obtained from the unconventional encryption algorithm.

In the model with preprocessing, the input block of plain data first is encrypted by classical Feistel scheme, then is transformed by the unconventional encryption algorithm.

Additionally, the model was developed, which repeats the structure of classical Feistel scheme, but the round function of which encrypts the subblock of data by the unconventional encryption algorithm. The round function might depend not only on round key, but also on selected system of bases. In this case the round function is called heterogeneous. The use of heterogeneous networks can significantly improve the characteristics of the cipher as uneven changes in internal properties of the network makes the study of statistical characteristics of encrypted data rather difficult task.

To implement the system of digital signature the developed model of public-key based NPNs is considered. The structural scheme of the model for the implementation of the non-traditional algorithm of digital signature is shown in Figure 1. This scheme shows the structure of the main stages of the algorithm of digital signature formation and its software implementation.

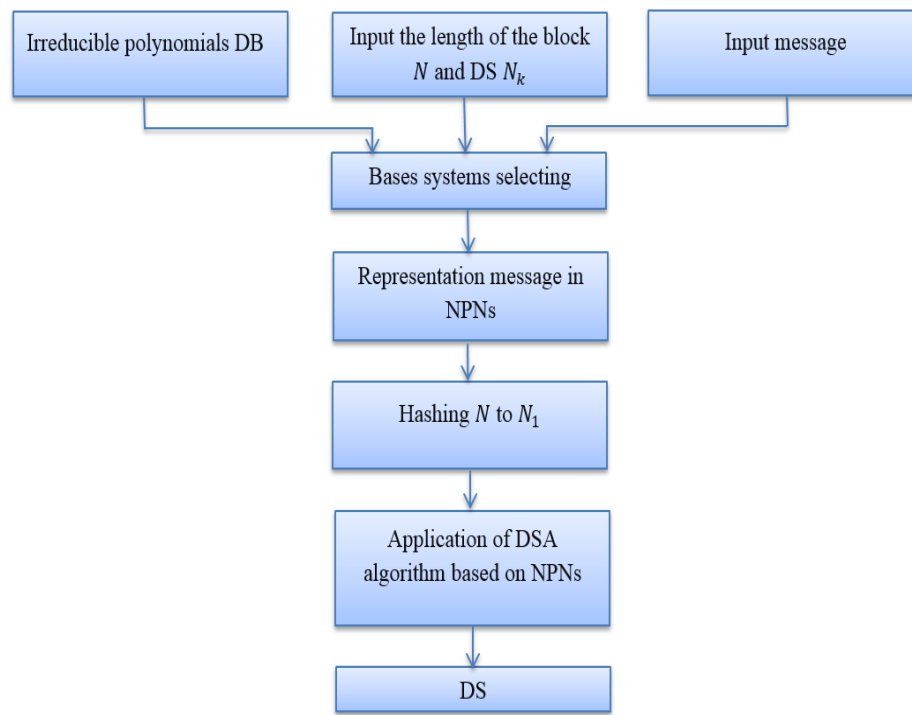


Figure 1 - Structural scheme the implementation of the DS model

Selecting of working and redundant bases systems is produced from the database of irreducible polynomials with binary coefficients. To find the irreducible polynomials with binary coefficients and database creation the program «Polinom» was developed.

Sieve of Eratosthenes was used in finding the irreducible polynomials. The found irreducible polynomials are represented in binary, octal and decimal systems. On completion of the calculations program displays a message about it.

The text of the program laid down parameters of searching, which indicated the values of the degree to which you need to find irreducible polynomials. The found irreducible polynomials are stored in a separate file or database accessed by the service for creation of full keys as needed.

Next is the hashing (compression) of the electronic message from a given length N bits to bits N_k . Digital signature is calculated according to the modified algorithm DSA based NPNs [7].

As the use of cryptographic protection means of public key has an extremely low speed, the use of NPNs increase the speed of creation and verification of signature by parallelizing computational operations that laid down in the signature formation algorithm, that is, by selected working bases.

Conclusions

In the solving the tasks in ensuring the protected cross-border information exchange should be taken into account both organizational and technological features of such interaction and the legal issues of ensuring the legal significance of electronic information in integrated system.

Today there is no common model of technology of the cross-border information exchange. The developed model of the technology of protected cross-border information exchange will contribute to the creation of the national segment and development of the domestic means of information security ensuring.

References

1. Biyashev R., Nyssanbayeva S., Begimbayeva Y. Development of the model of protected cross-border information interaction // Open Engineering – 2016. – №6. PP. 199-205.
2. Lewis J., Fowler M., Microservices: a definition of this new architectural term // <http://www.martinfowler.com/articles/microservices.html>
3. Biyashev R., Nyssanbayeva S., Kapalova N. The Key Exchange Algorithm on Basis of Modular Arithmetic // 2013 International Conference on Electrical, Control and Automation, 2013, PP.501-505.
4. Biyashev R., Nyssanbayeva S., Begimbayeva Y., Magzom M. Modification of the Cryptographic Algorithms, Developed on the Basis of Nonpositional Polynomial Notations // Proceedings of the International Conference on Circuits, Systems, Signal Processing, Communications and Computers (CSSCC 2015), Vienna, Austria, 2015, PP.170-176.
5. D. Schinianakis, T. Stouraitis. Residue Number Systems in Cryptography: Design, Challenges, Robustness // Secure System Design and Trustable Computing, Springer, 2016
6. Kalimoldayev M., Nyssanbayeva S., Magzom M. Model of nonconventional encryption algorithm based on nested Feistel network // Open Engineering – 2016. – №6. PP. 225-227.
7. Bijashev, R.G. and Nyssanbayeva, S.E.: Algorithm for Creation a Digital Signature with Error Detection and Correction //Cybernetics and Systems Analysis. №4, 2012, PP. 489-497.

ЖЕКЕ ТҮЛҒАНЫ ДАУЫСЫ АРҚЫЛЫ ТАНУ ЖҮЙЕСІН ЖОБАЛАУ МЕН ҚҰРУ ӘДІСІНЕ СИПАТТАМА

Ө.Ж. Мамырбаев, А.Е. Ибраимкулов*, Абдилда Б.Г.
e-mail: orkenj@mail.ru, aibek_ibraimkulov@mail.ru

Алматы қ., ҚР БҒМ Ақпараттық және есептеуіш технологиялар институты
*-магистрант

Аңдатпа. Табиғи тілде сөйлеулерді автоматты түрде тану үрдісі жасанды интеллект дамуының негізгі бағыты болып табылады. Бұл бағыттағы нәтижелер адам мен компьютер арасындағы тиімді қарым-қатынас орнату жабдықтарын жасау мәселесін шешуге мүмкіндік береді. Сөйлеу технологияларының өндірістің кез-келген саласына енгізілуі зерттеу орталықтары мен өндіруші фирмалардың сөйлеуді танумен байланысты мәселелерге қызығушылығын арттырды. Бұл мақалада жеке тұлғаны дауысы арқылы тануды зерттеудегі әдістер мен алгоритмдер, бағдарламалық ресурстардың түрлері жалпылама қарастырылған және талданылған.

Түйін сөздер: сөйлеу, сөйлеулерді тану, сөйлеуді автоматты түрде тану, сөйлеу технологиялары, Гаусс қоспа моделі.

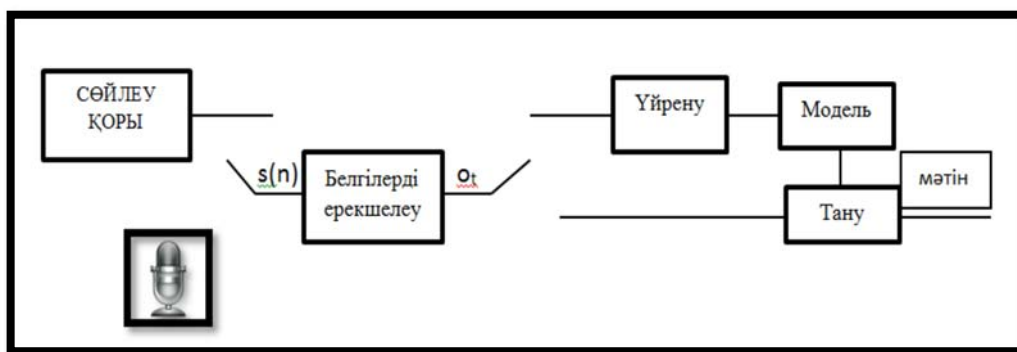
Кіріспе. Сөйлеулерді автоматты түрде тану заманауи өмірдегі адамдардың әдеттенерлік атрибуты болып саналуда. Алайда, атақты мамандардың көптеген жоспарларына қарамастан күнделікті өмірде сөйлеулерді тану мен сәйкестендіру технологиясын кеңінен қолдану әзірше бақыланбай отыр. Осындай салдардың негізгі себебі ретінде сөйлеулерді тану әдісінің жетіспеушілігі болып табылады. Мұндай кезде, байланыс арнасының сипаттамасын жоғары деңгейде өзгерту кезіндегі сөйлеулерді тану жүйесінің қасиетін сақтау саналады. Сөйлеулерді танудың заманауи әдістерінде сөйлеулердің ағынын модельдеу сөйлеу кезіндегі дыбыстардың акустикалық инвентарилері мен сөздерді дыбыстап транскрипциялау көмегімен жүзеге асады. Дыбыс моделі параметрін бағалау үйренуші таңдалым – мәліметтердің сөйлеулер корпусында іске асырылады. Тұрақты қосылып тұратын дыбыс қабылдағыштан енген сөйлеулерді тану жүйесіндегі сөздіктерге кірмейтін сигнал шулардан тұруы мүмкін, өзге адамның сөздері, сөйлеу ағынының әртүрлі өзгерістері (күлкі, жөтел, дыбыстық ғырылдар) кездесуі мүмкін. Мұндай факторлар тану кезінде әртүрлі қателіктерге орын береді [1].

Сөйлеулерді тану жүйесі адамның кейбір қолданбалы жүйемен байланысын орнықтыру үшін қызмет атқарады. Мұндай жағдайда хабарламаның мәтін санына емес, оның мағынасына қарап сенімділігін қамтамасыз ету керек. Сондықтан да сөйлеулерді тану нәтижесін логикалық безендіру сенімділік тұрғысынан мәтінді дыбыстаудың бірнеше ықтималдары арқылы ұсынылады. Мысалы, әрбір ұсынылатын сөз танудың сенімділігін сандық тұрғыда бағалау арқылы іске асады.

Сөйлеуді автоматты түрде тану жүйесі үш этаптан тұрады: белгілерді анықтау, үйрену және тану.

Бірінші этапта бастапқы сигналдан – ақпаратты тану үшін сығылған дауыс сигналдары кездесетін вектор белгілерін алады. Бұл үшін жиілік аумақта жұмыс жасайтын әдістер (мел-кепстральды коэффициенттер, сызықты болжау коэффициенті) қолданылады [2]. Т ұзындық белгісі бар векторлар кезектесі акустикалық немесе кезектескен қадағашылық $O=(o_1, o_2, \dots, o_T)$ деп аталады. Осындай реттілікпен $W=(w_1, w_2, \dots, w_N)$ сөздер тізбегін таратады. 1-суретте көрсетіліп тұрғындай сөйлеулерді

тану тапсырмасы келесі түрде орын алады: W тізбектелген сөзді тану керек, яғни акустикалық реттілікпен сәйкес келу керек.



1 - сурет. Сөйлеулерді автоматты түрде танудың жалпылама сызбасы

Үйрену кезеңінде осындай тапсырмаларды шешу үшін λ моделі құрылады, O кезектескен барлық мүмкіндікке сәйкес келе алатын барлық W мүмкіндікке ие болуы шарт. (W, λ) функциясы (1) тек W –ға берілген барлық мүмкін болған O -ны қайтарса. Сонда танылатын сөздер W^* тізбегіндей болуы керек:

$$W^* = \text{ArgMin}_{w \in W} d(h(W, \lambda), O) \quad (1)$$

мұндағы, $d(O, O)$ - O , мен O арасындағы айырмашылық.

Осы орайда, W сөздер тізбегін тексеріп шығу керек. Осындай тапсырманы оңтайландыру үшін белгілі бір сөздерді іріктеп алып, тану тілдің грамматикасы көмегімен тану үдерісін іске қосу қажет.

Тұлға дауысын тану үдерісінде орын алатын кедергілер. Шулар, кедергілер, құбылулар. Сөйлеушіні тану жүйесін құру жолында көп кездесетін кедергілердің бірі сөйлеу сигналының өзгергіштігі. Ең алдымен бұл өзгергіштік диктордың өзіндік сөздерді дыбыстаулардағы құбылмалылыққа тікелей байланысты. Қолданушыны түпнұсқаландыру мен тіркеуге жазу кезіндегі негізгі қиындықтар ретінде байланыс арнасындағы құбылулар мен шулар жатады.

Телефон каналдарымен жұмыс кезінде тиімді қабылдаудың жолақтық сүзгісі 400-3500 Гц болады. Осындай ретпен тестіленген және эталонды жазбалар әртүрлі телефонды трактта айырмашылық деңгейде теңдей көрінеді. Басқа қабылдаулар RASTA-сүзгі деп аталатын тұрақты немесе аздап-өзгергіш сипатта арналардың өзгеру құбылысы қолданылады [3].

Орташа спектрмен есептеумен байланысты басқада қабылдаулар кездеседі. Сөйлеулерді жіберу арнасы сызықты болып табылған соң, уақытында өзгеріске ұшырамайды. Алайда мұндай нормализациялау әдісі жарамды емес, егерде құпия сөз фонетикалық теңдей болмаса және жалғасын таппаса. Мұндай жағдайда сөйлеушіні идентификациялау жұмысы төмендейді. Сол себепті идентификациялау барысында әртүрлі кедергілерді жою күрделі талап етеді.

Дыбысты тану жүйесінің құрылымы зерттелетін тапсырманың күрделілігіне негізделіп таңдалынады. Жүйенің әртүрлі деңгейіне байланысты шешімдердің техникалық көптірлілігін таңдау күрделенеді. Жүйе құрылымын таңдау тапсырмасын жеңілдету үшін «шаблон» негізінде сәйкес келетін жиынтықтардың белгілерін жіктелуін алдын ала қамтамасыз ету керек. Белгі ретінде мыналар көрсетіледі: жүйемен танылған

дыбыс типі; диктор дауысын танудан жүйенің тәуелділігі; эталондар детализацияларының деңгейлері; танылған сөздердің саны. Осы жүйеге сөздіктің толықтылық түсінігі енгізіледі содан кейін кілттік сөзді іздестіру тапсырмасы интерпретацияланады, яғни толық емес сөздіктен тану үдерісін жетілдіре отырып іске асады. Одан әрі жіктелген белгілер көрсетіледі: жүйені тағайындау, жұмыс істеу механизмі және тұтыну қасиеті [4].

Сөйлеген сөздерінің типі бөлектелген сөздер мен командаларды тану жүйесі болып бөлінеді. Бірінші жағдайда сөздерді арнайы дыбыстауды талап етеді, онда сөздер арасындағы кідіртулер сөзішілік кідіртуді айтарлықтай жоғарылатады. Әдетте, мұндай кідіртулер жартысекунд шамасындағы уақытты қамтиды. Бөлектелген сөздерді тану кезінде қолданушы ешқандай кідіріссіз сөздерді дыбыстауы мүмкін. Тану жүйесінің тағыда бір нұсқасы сөздердің дыбысталуы кідірістерге байланыссыз дыбыстық ағын ретінде тануды жатқызамыз. Дыбыстық ағын ретінде тану нұсқасында қолданушы жүйеге енгізген сөздерінің арасындағы дыбысталудың кідіртіп дыбысталуына тәуелсіз жұмыс атқарады. Тану жүйесінің осындай түрі кілттік сөздерді іздеу режимі деп аталады.

Диктор дауысын тану жүйесінің тәуелділігіне байланысты дикторға тәуелді және дикторға тәуелсіз жүйе болып бөлінеді. Бірінші жүйе қолданушысы үшін алдын-ала дауысқа үйренуді оқытуды талап етеді, екіншісі – жүйеге орнатылғаннан кейін бірден жұмыс істеуге дайын. Дикторғатәуелді жүйе басқа қолданушылардан қарағанда, негізгі қолданушы дауысын тануды жоғары деңгейде қамтамасыз етеді. Яғни, жүйені тұрақты қолданып жүрген қолданушыны өте аз уақытта оның жүйеге енуге деген мүмкіндігін қысқа уақыт аралығында жүзеге асырады деген сөз.

Гаусс қоспа моделі. Гаусс қоспа әдісі сөйлеушіні тану аумағында кеңінен қолданылатын модель түрі. Мұндай модель Гауссиан өлшенген суммасынан (2) тұрады:

$$p(x|\lambda) = \sum_{i=1}^M w_i p_i(x) \quad (2)$$

мұндағы λ – диктор моделі, M – модельдің компоненттінің саны, w_i – компонент салмағы (3), яғни:

$$\sum_{i=1}^M w_i \quad (3)$$

Әрбір компоненттің тегіс ықтималдылық функциясы келесі формуламен беріледі (4):

$$p_i(x) = 1/(2\pi)^{D/2} |\Sigma_i|^{-1/2} \exp(-1/2(x - \mu_i)^T \Sigma_i^{-1} (x - \mu_i)), \quad (4)$$

мұндағы, D – белгілер кеңістігіндегі өлшем, μ_i – математикалық күту векторы, Σ – ковариация матрицасы. Осындай модельді орындайтын жүйеде көбінесе диагональды ковариация матрицасы қолданылады. диктор моделінің барлық компоненті үшін бір ковариация матрицасын қолдануы мүмкін немесе барлық модель үшін бір матрицаны қолдану мүмкін [5].

Сол себептен, диктор моделін құру үшін орташа векторды, ковариация матрицасын және компонент салмағын анықтап алу қажет. Мұндай міндеттерді ЕМ-алгоритмі көмегімен шешуге болады.

Кіріске $X=\{x_1, \dots, x_t\}$ үйренуші кезектескен векторлар кіреді. Модельдер параметрлері бастапқы мәнге инициализацияланады да алгоритмнің әрбір қадамында параметрлерді қайта бағалау орын алады.

Бастапқы параметрлерді анықтау үшін әдетте К-орташа алгоритмі секілді кластеризация алгоритмдері қолданылады. М кластерлерге үйренуші векторлар жиынын бөлуді құрғанда, модельдер параметрлері келесі үлгіде инициализациялануы мүмкін. $\square_i$ бастапқы мәні кластерлердің ортасына сәйкес келеді, ковариация матрицасы векторлардың кластеріне түсу негізінде есептелінеді, компоненттер салмағы үйренуші векторлардың жалпы саны арасындағы сол кластер векторының үлесімен анықталады [6].

Параметрлерді қайта бағалау келесі формула түрінде жүзеге асады:

- апостериорлы ықтималдылықты (5) есептеу (Estimation-step)

$$p(i|x_t, \lambda) = w_i p_i(x_t) / \sum_{k=1}^M w_k p_k(x_t); \quad (5)$$

- модельдің жаңа параметрлерін есептеу (6) (Maximization-step)

$$w_i = 1 / T \sum_{t=1}^T p(i|x_t, \lambda); \quad (6)$$

$$\mu_i = \sum_{t=1}^T p(i|x_t, \lambda) x_t / \sum_{t=1}^T p(i|x_t, \lambda); \quad (7)$$

$$\Sigma_i = \sum_{t=1}^T p(i|x_t, \lambda) (x_t - \mu_i)^T / \sum_{t=1}^T p(i|x_t, \lambda) \quad (8)$$

Мұндай кезең параметрлердің ұқсастығына дейін қайталанады.

Тану тапсырмасы үшін модельдер классификациясы тәсілдерінің бірнешеуі кездеседі. Әдебиеттерде көбіне модельге генеративті немесе дискриминативті негізде сілтеме береді. Генеративті деп аталатын модель негізі оқыту үшін құрылған мәліметтер модельдеуінен тұрады, яғни ықтималдылықтың тығыздық функциясының бағасы көмегі жатады. Мысал ретінде, жоғарыда сипатталған Гаусс моделі жатады. Ал дискриминативті модель класстар арасында шектеулер қою негізі жатады, мысалы, тірек векторлар әдісінде жүзеге асқанды жатқызуға болады.

Қорытынды. Дауыс арқылы сәйкестендіру құрылғысын құрудың ең бастысы – дауыстың өзіндік қасиетін сипаттайтын параметрлерді таңдау. Осы сигналдың параметрі өзгеше белгі деп аталады. Осындай белгілер, дауыстың ерекшелігенде өзге қасиеттерден тұруы тиіс.

Бүгінгі таңдағы сөйлеуді автоматты тану жүйелері соңғы ондаған жылдарда үлкен қарқынмен алға қадам басты. Олардың ішінде қарапайым дикторға тәуелді қосымшалардан бастап жаналықтарды, телефонмен сөйлесулерді, дәрістерді т.б. автоматты мәтінге айналдыратын дикторға тәуелсіз жүйелер бар.

Пайдаланылған әдебиеттер тізімі

- 1 Ландэ Д.В. Фурашев В.Н. О цифровой идентификация личности. //Открытые информационные и компьютерные интегрированные технологии. – Харьков: НАКУ, 2007. - №34. –С. 127-135.
- 2 Матвеев Ю.Н. Технологии биометрической идентификации личности по голосу и другим модальностям,. ISSN 0236-3933. Вестник МГТУ им. Н.Э. Баумана. Сер. “Приборостроение”, 2012.
- 3 Малинин П. В., Программа идентификации личности по голосу. Алтайский государственный университет г. Барнаул// <http://elibr.altstu.ru>
- 4 Яковлев Ф.И. Лингвистические аспекты идентификации личности по голосу. – Москва: 2003. – 190 с.

5 Агапиев А. Н., Милашенко В. И. Идентификация пользователей по голосу. [Электронный ресурс]. Военный институт правительственной связи (ФАПСИ)// <http://www.speech-soft.ru>

6 Сорокин В.Н., Вьюгин В.В., Тананыкин А.А. Распознавание личности по голосу: Аналитический обзор, Институт проблем передачи информации, Российская академия наук, Москва, 2012.

СӨЙЛЕУЛЕРГЕ СПЕКТРЛІК ТАЛДАУ ЖАСАУҒА АРНАЛҒАН АЛГОРИТМ

Мамырбаев О.Ж., Нурлан К.Е.
e-mail: morkenj@mail.ru, nurkam_89@mail.ru

*Институт информационных и вычислительных технологий КН МОН РК,
Казахстан*

Аңдатпа. Бұл мақалада негізгі сөйлеулерге спектрлік талдау жасауға арналған алгоритм қарастырылды және олардың артықшылықтары мен ерекшеліктері сипатталды. Сөйлеулерге спектрлік талдау жасайтын математикалық модель ұсынылып, соған сәйкес алгоритмі құрылды.

Соңғы уақыттық ретпен дискретті нақты сигналды $x(nT)$ -ны $x(n)$ деп жазамыз, мұнда $n = 0, \overline{N-1}$, N – есеп саны, T – дискреттеу мерзімі.

N – нүктелік дискретті Фурье түрлендірілуі (ДФТ) келесідей формуламен беріледі:

$$X(k) = \sum_{n=0}^{N-1} x(n) \cdot W_N^{nk}, k = \overline{0, N-1}, \quad (1)$$

Мұнда $X(k)$ – k -шы жиілік есебі немесе или k -шы спектральдық сигналды құраушы (шығыс жиілігінің жүйелігін анықтайды, сигналдың спектрін),

$W_n = e^{-j\frac{2\pi}{N}} = \cos\frac{2\pi}{N} - i \cdot \sin\frac{2\pi}{N}$ комплексті экспонента, $W_N^{nk} = e^{-j\frac{2\pi}{N} \cdot nk}$ түрлендіру яросы.

$n \cdot k$ мәні N еселі ұзындығына өзгеру барысында W ядросы өзгермейді (косинус және синус мерзімділігінде). Демек, ядро жоғарғы индексі бойынша N периоды бар периодты функция болып табылады. Сондықтан, $n \cdot k$ көбейтіндісінің орнына оның N -ға бөлінген қалдығын қалдыруға болады, яғни $(n \cdot k) \bmod N$ (немесе $\langle n \cdot k \rangle_N$). Спектральды функция $X(k)$ k аргументі бойынша N периодқа ие.

Нақты сигналдың (1) комплекс ядросында көбейту саны N^2 -қа тең, ал комплекс сандардың қосулар саны – $(N-1)N$. Бұл операциялардың саны N артуымен күрт артады және бұл тым көп уақыт түрлендіруіне алып әкеледі.

ДФТ жылдам алгоритмдерді ойлап тапқаннан кейін кеңінен қолданыла бастады. Олардың бірі (классикалық болып үлгерген) Фурье жылдам түрлендіру деп аталады. Бұл алгоритм, егер N 2 санының дәрежесі болып табылса, демек $N = 2^\nu$, мұнда ν -бүтін сан, $\nu \geq 0$.

Біз тоқталатын түрлендірудің негізгі формулалары, екі қосындыға (1) қосындысын бөлу арқылы алынады және жұп, тақ нөмірлері бар [1].

$$X(k) = \sum_{n=0}^{N/2-1} x(2n) \cdot W_N^{2nk} + \sum_{n=0}^{N/2-1} x(2n+1) \cdot W_N^{(2n+1)k}, k = \overline{0, N-1} \quad (2)$$

Негізінде бұл операция қосындының ретін өзгерту болып табылады (қосылғышты қайта топтастыру), бірақ бұдан қосынды өзгермейді.

Былай жазуға болады:

$$W_N^{2nk} = W_{N/2}^{nk}, W_N^{(2n+1)k} = W_N^k \cdot W_{N/2}^{nk}$$

Осыдан кейін (2) келесідей түрге ие болады:

$$X(k) = \sum_{n=0}^{N/2-1} x(2n) \cdot W_{N/2}^{nk} + W_N^k \cdot \sum_{n=0}^{N/2-1} x(2n+1) \cdot W_{N/2}^{nk}, k = \overline{0, N-1} \quad (3)$$

Байқасақ, (2.3) қосынды $N/2$ - бірінші қосындыдағы нүктелік ДФТ уақыттық жұп нөмірлер және екінші қосындыда тақ нөмірлер болып табылады. (3) шыққанды келесідей белгілейміз,

$X(k) = X_\nu(k)$ – ДФТ, барлық $N = 2^\nu$ кіріс дискретті сигналының,

$X_{\nu-1,0}(k) = \sum_{n=0}^{N/2-1} x(2n) \cdot W_{N/2}^{nk}$ – ДФТ $N/2 = 2^{\nu-1}$ жұп нөмірлі кіріс есептеулері (төмегі индекстегі бірінші сан $\nu-1$ тең, екіншісі жұп санға (нөлге) тең),

$X_{\nu-1,1}(k) = \sum_{n=0}^{N/2-1} x(2n+1) \cdot W_{N/2}^{nk}$ – ДФТ $N/2 = 2^{\nu-1}$ тақ нөмірлі кіріс есептеулері (төмегі индекстегі екінші сан тақ санға (бірге) тең).

Енгізілген мәндерден (3) қысқаша формасын аламыз:

$$X_\nu(k) = X_{\nu-1,0}(k) + W_N^k \cdot X_{\nu-1,1}(k), \quad k = \overline{0, N-1} \quad (4)$$

$X_{\nu-1,0}(k)$ және $X_{\nu-1,1}(k)$ спектрлары $N/2$ периоды бар периодты функциялар болып табылады (түрлендіру ядросында N орнында $N/2$ болады). Көлемі $W_N^k = e^{-i\frac{2\pi}{N}k}$ – бұрылыс көбейткіші деп және келесідей қасиетке ие $W_N^{k+N/2} = e^{-i\frac{2\pi}{N}(k+N/2)} = e^{-i\frac{2\pi}{N}k} \cdot e^{-i\pi} = W_N^k$. Бұл қасиет W_N^k есептеу барысында K нөмірлі $N/2$ бастап $(N-1)$ дейін алдын ала есептелген W_N^k сәйкес мәндері 0-ден бастап $(N/2 - 1)$ көрсетеді (тек белгіні ауыстыру керек).

Әдетте (4) формуланы жоғарыда көрсетілген нөмірлер үшін екі ара қатынасқа бөледі және Фурье түрлендіруінің негізгі формуласын мына түрде алады:

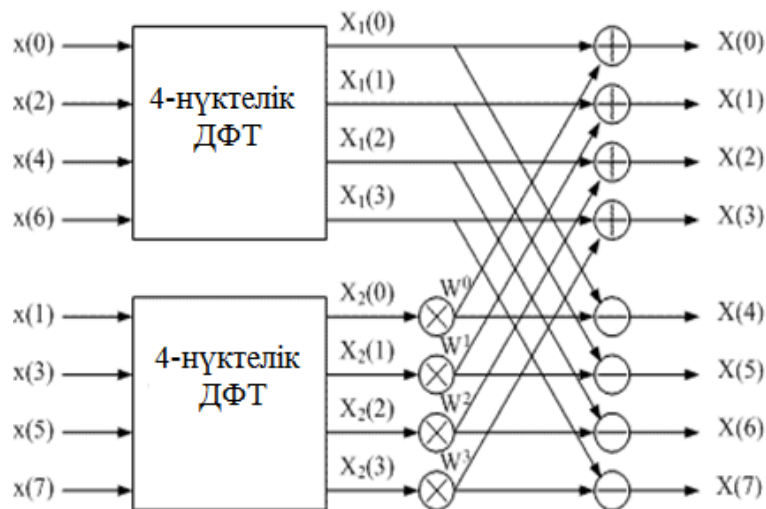
$$X_v(k) = \begin{cases} X_v(k) = X_{v-1,0}(k) + W_N^k \cdot X_{v-1,0}(k) \\ X_v(k + N/2) = X_{v-1,0}(k) - W_N^k \cdot X_{v-1,0}(k), k = \overline{0, N/2-1} \end{cases} \quad (5)$$

$$k = \overline{0, N-1}$$

Базалық арақатынасты Фурье жылдам түрлендірілуі (ФЖТ) деп атауға болады, себебі операциялар саны азайды. Комплексі ядроғағы сигналдың заттық көбейтіндісінің санына тең $\left(\frac{N}{2}\right)^2 \cdot 2 = \frac{N}{2}$. Бұған комплексі сандардың көбейтіндісін $\frac{N}{2}$ қосу керек. Қосындылар саны мынаған тең:

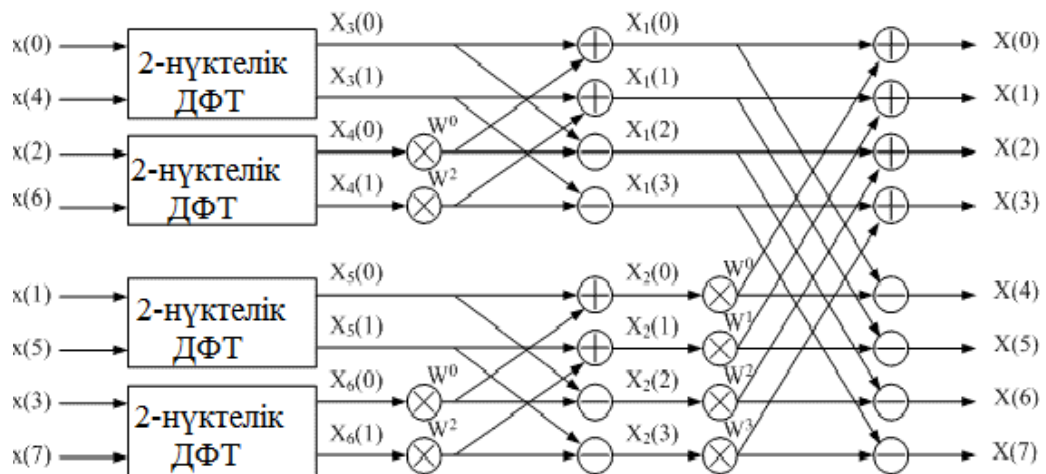
$$\left(\frac{N}{2} - 1\right) \frac{N}{2} \cdot 2 + 2 \cdot \frac{N}{2} = \frac{N^2}{2}.$$

Базалық арақатынас схемасы бойынша бөлу процесін Фурье түрлендіруінің бірлік санауларына келгенге дейін жалғастыра береміз (өздерінің санауларымен сәйкес келгенше). Операцияларды қажетті саны, содан кейін әлдеқайда аз болады [1]. Осы түрде бұл ФЖТ уақыт бойынша сиретуі деп аталады. Фурье жылдам түрлендіруінің уақыттық ситетуі бойынша есептеу графы 1 суретте көрсетілген.



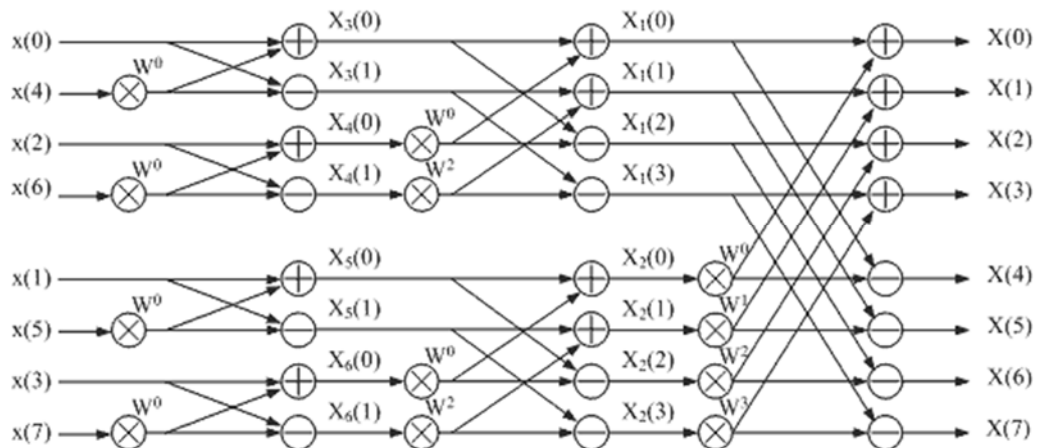
1 – сурет. Фурье жылдам түрлендіруін есептеу графы

Егер (нүктелер) санауларының саны алғашқы ДФТ саны тағы да жұп санболса, онда оларды жұп және тақ реттерімен уақыттық санауларға бөлуге болады. Бұл тағы да комплексі көбейту операция санының азаюына мүмкіндік береді. Бұл ретте Фурье жылдам түрлендіруінің графы 2 суреттегі түрге ие.



2-сурет. Фурье жылдам түрлендірілуін есептеудің жақсартылған графы

Соңғы алгоритм үшін, 8 нүктелік Фурье жылдам түрлендіруінің уақыттық сиретуі бойынша графы 3 суретте көрсетілгендей бейнеленеді [2].

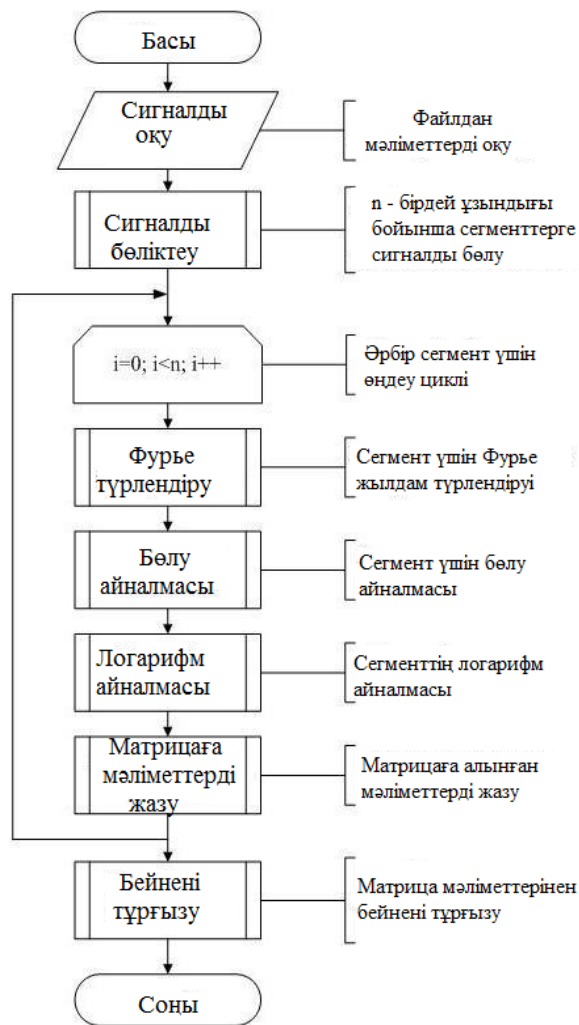


3 – сурет. Фурье жылдам түрлендіруін есептеудің соңғы графы

Енді Фурье жылдам түрлендіруінің алгоритмінің уақыттық сиретуі бойынша алынған ұтысын бағалаймыз. Көбірек ұтысты $N = 2^k$ уақыттық жүйелігінің ұзындығы алынады, бұл ретте яғни екі жүйелікке бөлу процессін 2 нүктелік Фурье түрлендіруіне дейін жеткізуге болады. Бұл ретте әрбір этапта төменгі қатардағы екі ФЖТ біріктіру үшін $N/2$ көбейту операциясы қажет болады. ФЖТ есептеу үшін қажет жалпы комплексті көбейту операцияларының саны:

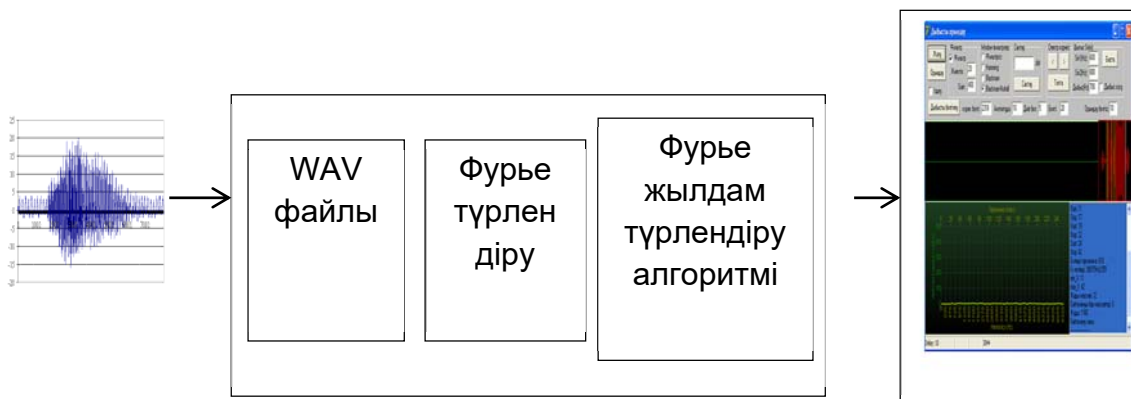
$$N_{\text{оп}} = N/2 \times \log_2 N$$

4 – суретте көрсетілген Фурье жылдам түрлендіру алгоритмінің блок – схемасы ұсынылған. Мұнда алгоритмнің жұмыс істеу механизмі сипатталған. Нәтижесінде алынған сөйлеулерге спектрлік талдау жасайтын ақпараттық жүйе 5-суретте көрсетілген.



4 – сурет. Фурье жылдам түрлендірудің блок – схемасы.

Сөйлеулерге спектрлік талдау жасайтын АЖ



5 – сурет. Ақпараттық жүйе құрылымы

Қорытынды. Қазіргі уақытта Фурье жылдам түрлендіруі әдетте сигналды процессірлерде орындайды, ал оларда адрестеудің ерекше түрі- екілік инверсті адрес қарастырылған. Бұл ретте үлкен және кіші адрес биттері орындары аппарат бойынша

ауысады, ал шынайы ауыстырулар жүргізілмейді. Бұл кіріс сигналының спектрді есептеудің уақытын мейлінше азайтуға мүмкіндік береді.

Пайдаланылған әдебиеттер

1. Гольденберг Л. М., Матюшкин Б.Д., Поляк М.Н. Цифровая обработка сигналов. Справочник. –М.: Радио и связь, 1985.
2. Кнут Д. Э. Искусство программирования. Том 1. – Москва, Санкт-Петербург, Киев: Вильямс, 2000.

SENSOR-DRIVEN ADAPTER FOR CAR DIAGNOSTICS

Muratkhanova T.A.
muratkhanovat@mail.ru

Institute of information and computational technologies KN MES RK, Kazakhstan

Summary. *More recently, such service as computer diagnostics of a vehicle was available only at specialized service stations, which have specialized equipment (complex devices like self-contained scanners). Today, computer diagnostics of cars can be done without high-level specialists. Diagnostic programs for cars are used for maintenance and repair using a PC in almost all conditions. The program reads the information from the electronic control unit (ECU) of the car through the adapter and allows visualizing the received data, both graphically and digitally. At the present time USB adapters are in great demand. These devices support the standard OBD-II. Depending on the functionality, the program can display real-time data, control the executive mechanisms, receive error data, and do much more.*

Key words: *OBD II adapter, sensor, diagnostic scanner, dashboard, DTC Codes.*

Introduction. Computer diagnostics of the car is a very important procedure for troubleshooting. Scanning various car systems using a laptop or a PC will provide a quick identification and at the same time a quick elimination of the defect and guarantees further safety on the roads.

Buying equipment for car service it is necessary to remember that a full-fledged auto repair shop can never do without high-quality diagnostic equipment. That is why they are becoming more and more popular due to the ability of promptly and accurately determining the presence of various malfunctions in the car system, which will contribute to their qualitative correction.

Now diagnosing a car using a PC or a laptop is in demand, among both car services and private motorists. Various equipment for car service includes special devices for car diagnostics (stand-alone scanners, adapters, accessories and so on).

In general, car scanning is basically done in two ways - using a standalone scanner, either by using a laptop or a PC, using a car diagnostic adapter that connects to the electronic control unit (ECU) using an adapter and cables [1, 2]. For a good reading of all data coming from the car, a special adapter is used, as well as a car diagnostic cable that connects the adapter to the car and to the PC.

Depending on the brands of the car and the set of existing functions, an adapter is used to diagnose different types of cars. The most common are USB KL line adapters that translate

OBD II data into information that is available for later analysis on a PC. Most often, such K-line adapter is called OBD II adapter [2]. Depending on the destination, the OBD II adapter usually has variations and many additional functions. For example, the ability to connect this device to the diagnostic socket via a universal cable completely eliminated the need.

Returning to the origins. In 1996, the EPA (Environmental Protection Agency), issued a decree that all vehicles sold in the United States must comply with uniform diagnostic standards. This meant that repair shops now were not required to buy half a dozen diagnostic scanners for each brand, but could work on universal equipment [3].

The standard was named OBD II (On-Board Diagnostics, version II). One or more computers control the ignition system, fuel injection and automatic transmission on most modern cars with fuel injection. The state of monitoring the engine and other systems of auto-sensors, "permeate" the whole car. Computers give commands to injectors and ignition coils to ignite the combustible mixture in the engine cylinders.

They use the data of all the sensors in order to configure the combustion process with the exact amount of fuel supplied, the optimal ignition timing to ensure efficient combustion of the fuel-air mixture with the necessary power "kickback ", economy and environmental friendliness [4]. Dozens of sensors that measure the opening level of the throttle, the speed of the crankshaft, the temperature of the air and coolant, the position of the crankshaft and the camshaft, the speed and much more send their data to computers (Figure 1).

This is a complex, high-speed system with a self-diagnosis function that keeps the car running for a long period. Mechanically, the engine tuning is somewhat obsolete, since for each revolution of the crankshaft, the computer system adjusts the amount and timing of the fuel injection, as well as the ignition parameters.



Figure 1- On-Board Diagnostics, version II

All this functions perfectly work as long as the Check Engine indicator does not light up on the instrument panel. The OBD II standard implies a MIL (malfunction indicator lamp) below it [6].

Its "Preoccupation" is expressed in the MIL indicator, which informs about the need to replace the sensor or diagnose a malfunction in the system. Despite this, the car will still move well, although it will be possible to notice slightly increased fuel consumption and some loss in power.

Moreover, PMM will store the DTC «Dynamic troubleshooting code» and the diagnostician will have a hint where to look for the problem. The scanners used to identify these codes were formerly expensive and focused on one manufacturer, that is a scanner for VW cars could not be used to diagnose, say, Chrysler. Now these tools are relatively inexpensive, even

for car owners [5]. Prices range from \$ 20 for a simple trouble-code reader, to full-featured machines, for \$ 400, with an updated software and a package of languages for users around the world. In addition, it is possible to borrow a diagnostic scanner in the car service for an hour or two, though it's unlikely.

Code verification. To start the diagnostics, it is necessary to connect the scanner to the connector of OBD II on the car (most often under the dashboard). The ignition key must be turned to the "ON" position, but the engine must not be started.

The scanner will request a lot of information, such as the VIN number, model of the vehicle, and the type of engine. It should be noted that most scanners are created on a user-friendly interface that is understandable to a typical user of electronic devices, so the user just has to follow the instructions that appear on the screen.

In the diagnostics menu the user will get a set of various functions, among which will be the verification of fault codes. Advanced versions of scanners can even give a transcript of these scanners. Some give it in an application, on a CD or in hard copy. Before resetting the MIL indicator, it is necessary to write these codes.

Inspection and maintenance (I/M) will be another option in the advanced scanner menu. If the "errors" were "dropped", it is necessary to drive out the car in order to make sure of it for PMM. Any diagnostic tool worth up to \$ 50 can erase errors, remove the MIL indicator and read out the DTCs.

The next menu option is to view the system parameters in real time. This tool allows delving deep into the problem [7]. For example, the user will get access to information about the indicators taken by the above sensors, the performance of oxygen sensors (lambda probe) and many other parameters of the system (Figure 2). There is even a function of a kind of stop frame, which allows capturing the parameters of the system during its failure on the road. This function is very important, and it is that which most often helps the mechanic or a car owner to find out the cause of the malfunction.

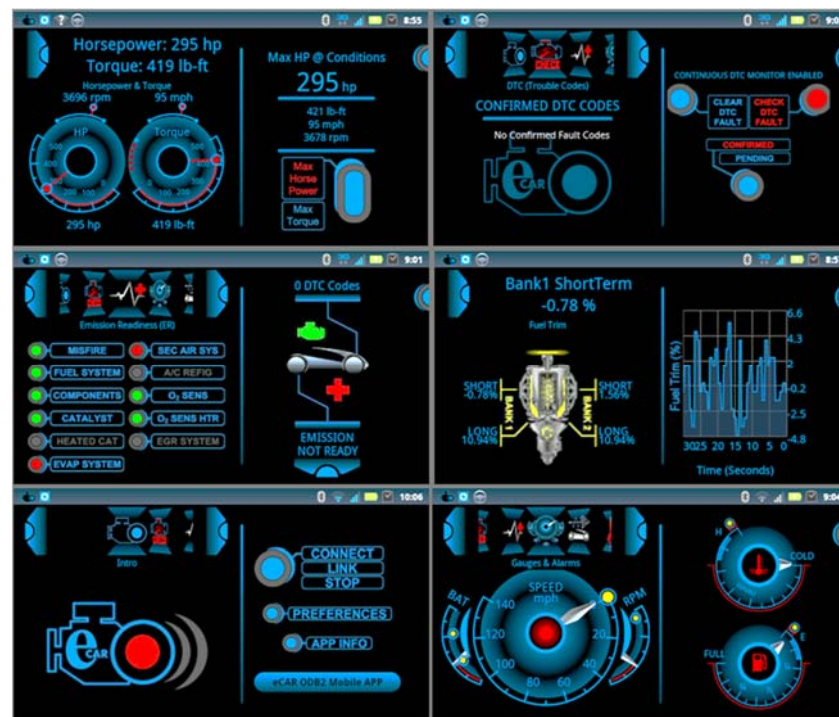


Figure 2- OBD2 Car Diagnostic

Professional-level scanners have graphical functions that allow registering in online mode the operation of all car systems when the engine is started.

Conclusion. To sum up, professional-level scanners are designed to receive and display diagnostic information about engine operation via OBD-II interface.

For connection, it is necessary to have an OBD-II Bluetooth adapter.

The scanner itself knows how to get all the information on the OBD II interface.

There are 7 customizable screens. It is possible to display information in the form of graphs, digital values, and a dial. There are several predefined widgets, that the user can create his own.

The program is able to display the current parameters of the engine, display and decode the error codes, erase errors from the vehicle's control unit (to extinguish the check engine on the dashboard). The user can configure alarms for different sensor values, for example, the fluid is cooling the temperature, engine speed, and speed.

The program can automatically send logs of sensor values to the web server and afterwards the user can see the route and the values of the sensors at different times.

In general, such tool is very convenient and functional. To add more, there is a set of convenient plug-ins and widgets - diagnostics are always at hand.

References

[1] "Escape PHEV TechInfo - PIDs". Electric Auto Association - Hybrid Electric Vehicle. - 11 December 2013. - P.28-30.

[2] "Frequently Asked Questions (FAQ) About On-Board Diagnostic II (OBD II) Systems". *Arb.ca.gov*. Retrieved 4 April 2017.

[3] "Diagnostics on Controller Area Networks – Requirements for emissions-related systems". - *ISO 15765-4: Road vehicles*. - 2005. – P.120-124.

[4] "Catalogue for Newly-released Environmental Regulations and Standards". *English.mep.gov.cn*. Retrieved 4 November 2016.

[5] *Peter Gargano*. "Reading GM's 160 baud ALDL Data Stream with a Standard PC Serial Port". *Techedge.com.au*. Retrieved 16 February 2017.

[6] "Prado 90 OBDI vs OBDII TDCL vs MOBD". *Pradopoint.com*. Retrieved 16 February 2017.

[7] "Emission Standards: USA: On-Board Diagnostics". - *Dieselnets.com*. Retrieved 16 February 2017.

РАЗРАБОТКА ИНФОРМАЦИОННОЙ СИСТЕМЫ ДЛЯ ФОРМИРОВАНИЯ ЦИФРОВОГО ГОЛОСОВОГО ПОРТРЕТА ЛИЧНОСТИ

Мусабаев Р.Р.
email: rmusab@gmail.com

¹ *Институт информационных и вычислительных технологий КН МОН РК,
Казахстан*

² *ТОО "Uniline Group"*

***Аннотация.** В данной статье рассмотрены вопросы разработки информационной системы для формирования цифрового голосового портрета личности. Разработанная система осуществляет предварительную обработку сигнала, их полосовую фильтрацию, осуществляет поиск локальных экстремумов, параметризацию, сегментацию и кластеризацию полученных сегментов.*

1 Введение

Важное теоретическое и прикладное значение имеет получение знаний о низкоуровневой субфонемной структуре речевого сигнала конкретного человека, являющейся важной составной частью цифрового голосового портрета личности (ЦГПЛ).

Под низкоуровневой структурой речевого сигнала понимается получение сведений о составе элементарных речевых единиц субфонемного алфавита, из которых формируется фонетический уровень речевого сигнала как динамический процесс их группирования и чередования во времени.

Для автоматизации данного процесса могут быть разработаны соответствующие алгоритмы. В частности, в данной статье даётся описание методологии и разработанного на её основе инструментария для автоматического членения речевого сигнала на субфонемные атомарные единицы с последующей их группировкой по критерию близости признаков с целью идентификации используемого субфонемного алфавита и формирования ЦГПЛ. По результатам данной процедуры получается описание речевого сигнала в виде последовательности состоящей из идентификаторов субфонемных единиц.

На вход данного алгоритма подаётся речевой сигнал в виде последовательности выборок, а на выходе получается числовая последовательность, состоящая из идентификаторов субфонемных единиц. Изначальное представление речевого сигнала в виде последовательности выборок импульсно-кодовой модуляции имеет некоторую избыточность, так как одна секунда речевого сигнала может кодироваться в среднем от 8000 до 44100 выборками. Используя же алгоритм идентификации субфонемных речевых единиц мы можем получить более компактное и информативное представление речевого сигнала, где одна секунда сигнала задаётся уже не тысячами, а десятком субфонемных идентификаторов. Таким образом, получается не только на порядок более сжатое и информативное представление речевого сигнала, но и поддающееся прямой интерпретации, что очень удобно использовать при последующем алгоритмическом анализе.

2 Запись и транскрибирование исходного речевого сигнала

Для рассмотрения предложенного алгоритма на конкретном примере необходимо произвести запись исходного речевого сигнала. Для того чтобы данный речевой сигнал в дальнейшем удобно было отображать на графиках, выберем одно короткое слово. Желательно чтобы оно содержало несколько реализаций одной и той же фонемы, что позволит нам проанализировать схожесть и различие признаков в разрезе различных аллофоновых реализаций одной фонемы. Для этих целей было выбрано английское слово «computer». На Рис. 1 представлен график двухканальной записи соответствующего речевого сигнала. Вверху расположен график микрофонного сигнала, а внизу его ларингофонный аналог. Произнесённое слово «computer» в соответствии со стандартом ARPAbet произнесено в следующей транскрипции: K AX M P Y UH T AX. В соответствии со стандартом IPA данная транскрипция будет иметь следующий вид:

[kəm`pjʊ:tə]. Здесь мы имеем шесть фонем в одиночной реализации и одну фонему с двойным повторением.

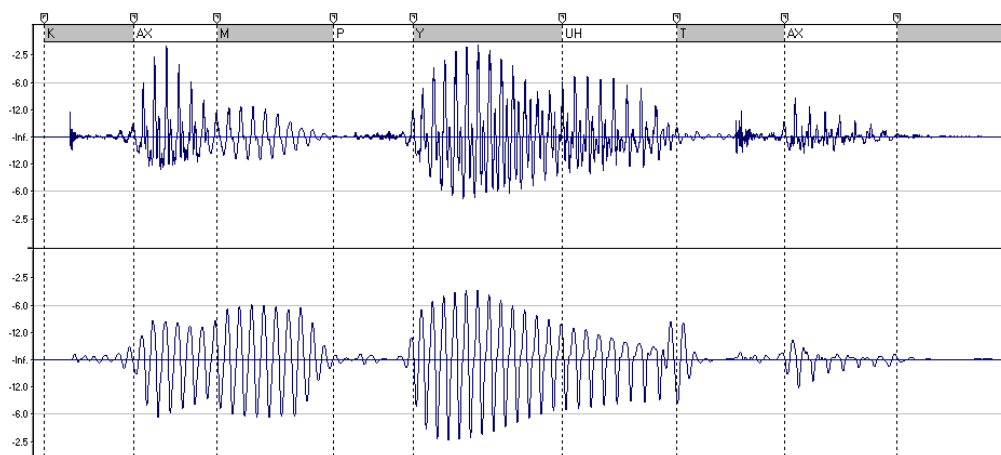


Рис. 1 Двухканальная запись речевого сигнала в момент произношения на английском языке слова «Computer». Вверху расположен микрофонный сигнал, а внизу его ларингофонный аналог. Пунктирной линией вручную экспертом помечены границы отдельных фонем

На приведённом графике сигнала можно выделить относительные границы отдельных фонем. Они на графике вручную помечены экспертом пунктирной линией. Также в соответствующих регионах помещены символьные обозначения отдельных фонем. В дальнейшем это поможет нам оценить правильность результатов автоматической идентификации субфонемного алфавита в речевом сигнале.

3 Общее описание алгоритма идентификации субфонемного алфавита в речевом сигнале

Для решения задачи идентификации субфонемного алфавита в речевом сигнале был разработан соответствующий алгоритм. Данный алгоритм включает в себя следующие основные стадии:

- 1) Предварительная обработка двухканального речевого сигнала с целью разделения его на отдельные каналы (модальности);
- 2) Полосовая фильтрация ларингофонного сигнала;
- 3) Полосовая фильтрация микрофонного сигнала;
- 4) Поиск локальных экстремумов в фильтрованном ларингофонном сигнале;
- 5) Параметризация речевого сигнала;
- 6) Сегментация речевого сигнала;
- 7) Кластеризация полученных сегментов.

В дальнейшем мы дадим более подробное описание каждого шага данного алгоритма в отдельности. Данный алгоритм программно реализован в виде специализированного инструментария, представленного в виде самостоятельной информационной системы, позволяющей в автоматическом режиме по заданным пользователем параметрам осуществить идентификацию субфонемного алфавита в анализируемом речевом сигнале. Главное меню пользователя данной информационной системы представлено на Рис.2.

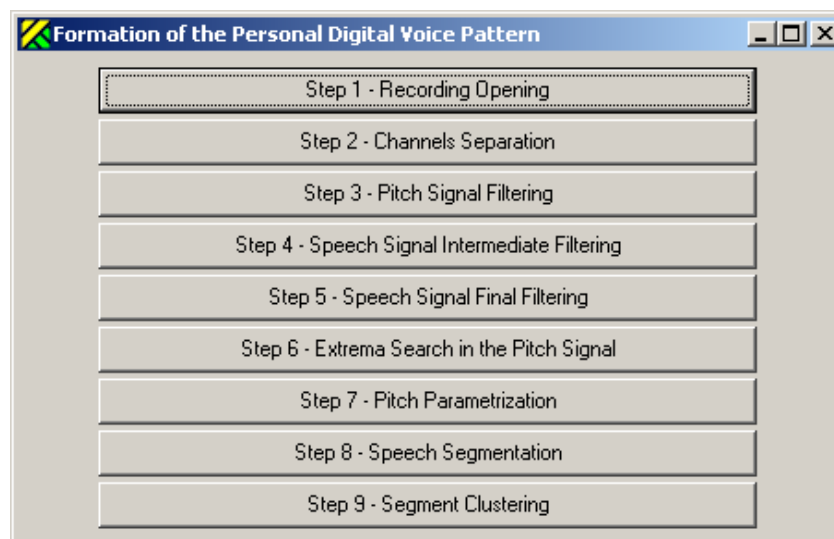


Рис. 2 Главное меню пользователя информационной системы автоматической идентификации субфонемного алфавита в речевом сигнале

На первом шаге алгоритма осуществляется выбор и открытие звукового файла предназначенного для последующего анализа. Анализируемый звуковой файл должен соответствовать следующим требованиям:

- формат файла: Microsoft WAVE;
- расширение файла: wav;
- количество каналов: 2;
- левый канал: микрофонный сигнал;
- правый канал: ларингофонный сигнал;
- разрядность оцифровки: 16 бит;
- частота дискретизации сигнала: 44100 Гц.

Для удобства дальнейшей обработки на втором этапе осуществляется разделение одной двухканальной записи на два отдельных файла. В один файл извлекается микрофонный сигнал, а в другой – ларингофонный. Разделение на отдельные файлы обусловлено тем, что на дальнейших этапах необходимо обрабатывать каждый из этих файлов отдельно.

4 Нормализация сигналов на основе полосовой фильтрации

Последующие три этапа предназначены для осуществления процедуры нормализации сигналов с применением метода полосовой фильтрации на основе фильтров с конечной импульсной характеристикой (КИХ-фильтр). Необходимость фильтрации ларингофонного сигнала обусловлена тем, что ларингофонный сигнал изначально имеет более широкий диапазон частот, который для нас является избыточным. Если внимательно посмотреть на ларингофонный сигнал представленный на Рис.1, то можно заметить, что помимо непосредственно колебаний голосовых связок в нём присутствуют незначительные низкочастотная и высокочастотная составляющие, которые создают паразитные локальные экстремумы. Соответственно зная интересующий нас диапазон частот, и применив к сигналу полосовой фильтр, мы можем увеличить точность идентификации локальных экстремумов на последующем этапе.

Фильтр с конечной импульсной характеристикой описывается следующим разностным уравнением отображающем связь между входным и выходным сигналами фильтра [1]:

$$y(n) = \sum_{i=0}^P b_i x(n-i),$$

где $x(n)$ – входной сигнал, $y(n)$ – выходной сигнал, P – порядок фильтра, b_i – коэффициенты фильтра. Требуемые для данной полосы частот коэффициенты фильтра вычисляются с использованием окна Кайзера [1].

Для синтеза соответствующего фильтра работающего в требуемой полосы частот пользователю предлагается указать следующие параметры: нижнюю частоту и верхнюю частоту диапазона, порядок фильтра, минимальный уровень затухания в полосе фильтрации.

По результатам фильтрации мы получаем нормализованные по требуемому диапазону частот микрофонный и ларингофонный сигналы. На Рис. 3 показан результат фильтрации ларингофонного сигнала (для сравнения исходный сигнал до фильтра показан на Рис.1).

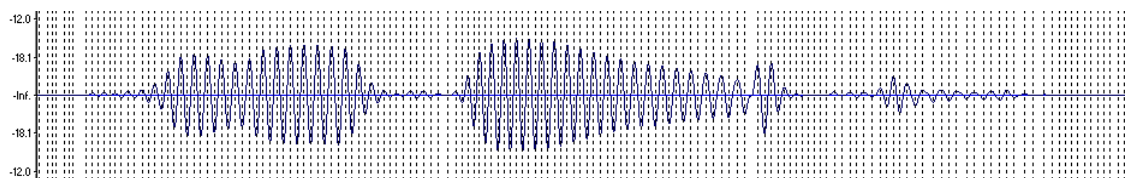


Рис. 3 Результат фильтрации ларингофонного сигнала и поиска в нём локальных экстремумов

5 Поиск локальных экстремумов в ларингофоне сигнале и их использование для вычисления частоты основного тона

Следующим этапом является процедура поиска локальных экстремумов в фильтрованном ларингофоне сигнале. Идентифицировав точки расположения локальных экстремумов имеется возможность в дальнейшем определить месторасположения отдельных периодов колебаний голосовых связок. Весь дальнейший анализ речевого сигнала осуществляется методом его разбиения на отдельные кратковременные окна. При этом анализируемые окна могут иметь фиксированную длительность и шаг смещения, а могут быть привязаны к периоду колебания голосовых связок, что в некоторых ситуациях некоторые преимущества, связанные с эффектом хорошего соответствия фазовых характеристик близлежащих сегментов.

Месторасположения локальных экстремумов определяется поисковым методом путём последовательного перебора отдельных выборок сигнала и сравнения их значений с близлежащими выборками. Выборка помечается как локальный максимум, в случае если её значение больше значений выборок, расположенных слева и справа. Если же значение выборки меньше левой и правой примыкающих к ней выборок, то она помечается как локальный минимум.

6 Параметризация анализируемого речевого сигнала

На следующем этапе осуществляется параметризация анализируемых микрофонных и ларингофонных речевых сигналов. Необходимость осуществления процесса параметризации речевого сигнала обусловлена тем, что по своей природе речевой сигнал несёт довольно много избыточной информации. Среди этого большого объёма информации необходимо выделить наиболее информативную составляющую пригодную для решения поставленной задачи. Фактически на данном этапе необходимо осуществить сжатие имеющегося речевого сигнала так чтобы на выходе получить набор параметров имеющих определённую физическую интерпретацию и позволяющих описывать различные свойства речевого сигнала и используя их принимать решения по его опознаванию или классификации.

Приведём перечень параметров и алгоритмов параметризации включённых в состав данной библиотеки:

- 1) Гармонический анализ [10];
- 2) Быстрое преобразование Фурье (БПФ) [2];
- 3) Мел-частотные кепстральные коэффициенты (MFCC) [3];
- 4) Коэффициенты линейного предсказания (LPC) [4];
- 5) Отражённые коэффициенты линейного предсказания (LPREFC) [5];
- 6) Кепстральные коэффициенты линейного предсказания (LPCEPSTRA) [6];
- 7) Линейные выходы банка фильтров с использованием мел-шкалы (FBANK) [7];
- 8) Перцепционные кепстральные коэффициенты линейного предсказания (PLP) [8];
- 9) Спектральный вариационный контур (SVC) [9];
- 10) Энергетические контуры [11];
- 11) Частота перехода через нулевой уровень [12];
- 12) Частота основного тона [13];

Также в рамках данной работы впервые были предложены и исследованы следующие новые информативные признаки:

- 1) Гортанно-речевые корреляционные коэффициенты;
- 2) Коэффициент симметрии сегмента;
- 3) Энергия полосы частот;
- 4) Вариационный контур во временной области;
- 5) Спрямлённая длина локального речевого сегмента;
- 6) Плотность речевого сигнала;
- 7) Относительный уровень всплеска высоких частот;
- 8) Гармоническая энергия;
- 9) Сглаженный вариационный контур амплитудного спектра;
- 10) Сглаженный вариационный контур фазового спектра;

Итого в общей сложности в системе имеется возможность осуществить параметризацию речевого сигнала используя 22 различных алгоритмов для вычисления информативных параметров. При этом для каждого из полученного параметрического набора имеется возможность дополнительно вычислить первую производную. На Рис. 4 представлено диалоговое окно для выбора пользователем перечня параметров, вычисляемых в процессе параметризации.

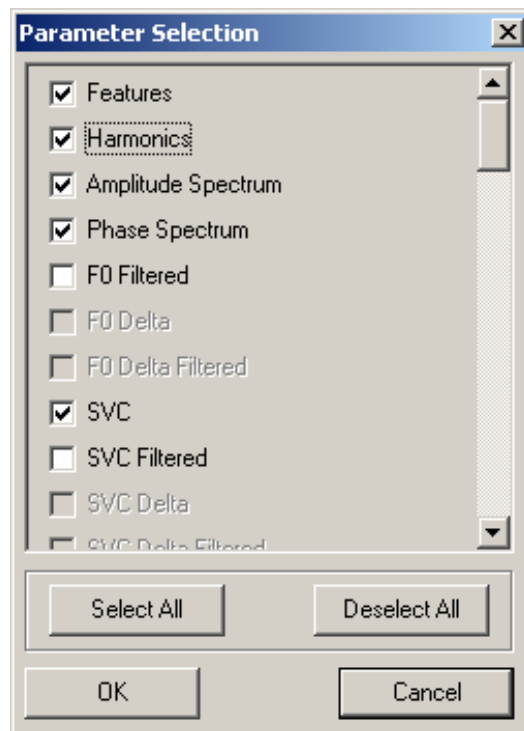


Рис. 4 Диалоговое окно для выбора пользователем перечня параметров, вычисляемых в процессе параметризации

Некоторые из предлагаемых к выбору параметров имеют собственные настройки, которые пользователь также может изменять. Поэтому после выбора расширенного перечня используемых параметров пользователю предлагается задать детальные настройки процесса параметризации (Рис.5). По умолчанию в окне настроек уже произведена установка значений по умолчанию

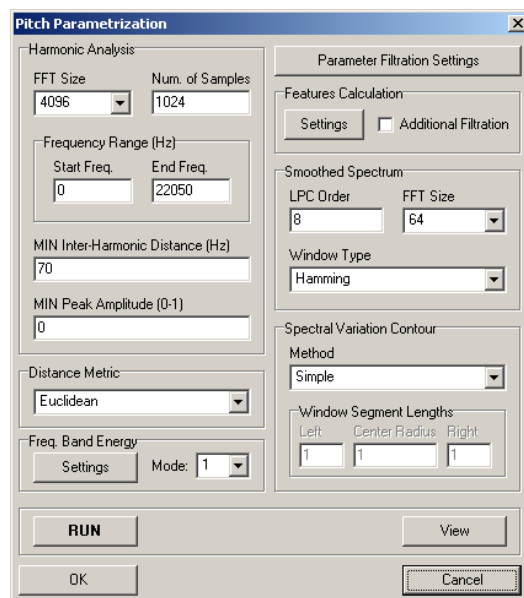


Рис. 5 - После выбора расширенного перечня используемых параметров пользователю предлагается задать детальные настройки процесса параметризации

В частности, для процесса гармонического анализа можно задать размерность быстрого преобразования Фурье, количество анализируемых выборок, анализируемый частотный диапазон, минимальное расстояние между соседними гармониками, минимальная амплитуда гармонических пиков, подлежащих анализу. При вычислении некоторых из параметров используется метрика близости между двумя векторами признаков, которую можно задать, выбрав требуемую метрику из списка. Выбрать можно евклидову либо корреляционную метрику.

В случае если выбрана опция фильтрации параметров, то можно указать параметры используемого фильтра (Parameter Filtration Settings). Также в окне задания настроек параметризации можно осуществить настройку процесса вычисления сглаженного спектра (Smoothed Spectrum). Для этого можно установить требуемое количество коэффициентов линейного предсказания, размерность БПФ, тип используемой оконной функции (Хэмминга или прямоугольная). Отдельные настройки можно задать для алгоритма вычисления спектрального вариационного контура: используемый метод и длины оконных сегментов.

Все те параметры, которые можно выбрать с помощью диалогового окна, представленного на Рис.4 являются опционными. Однако в данной системе введено такое понятие как базовый набор параметров. То есть это тот набор параметров, который вычисляется для любого речевого сигнала. При нажатии на кнопку «Settings» в области «Features Calculation» открывается отдельное окно, предназначенное для задания состава базового набора параметров (Рис. 6).

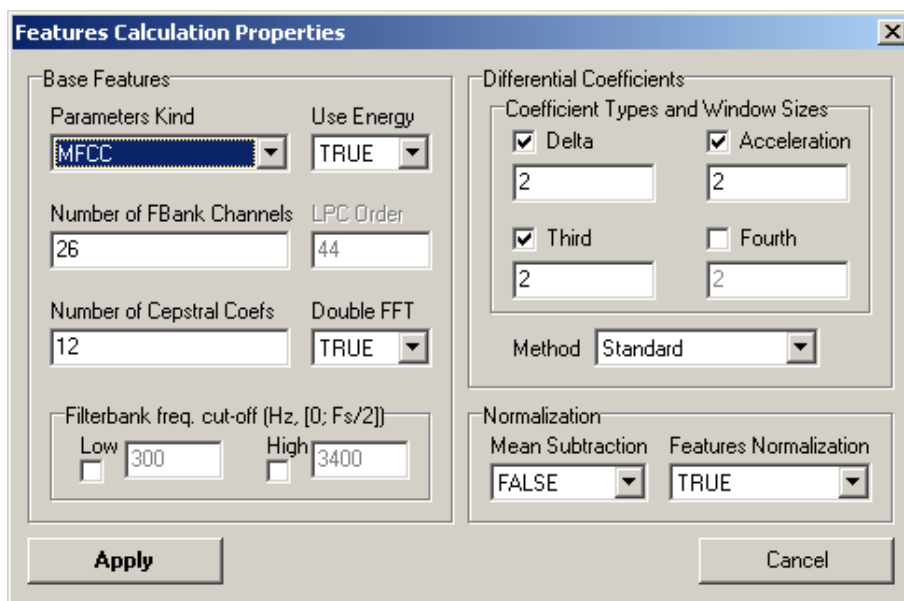


Рис. 6 - Задание состава базового набора параметров

В качестве базового может быть выбран один из следующих наборов признаков: LPC, LPREFC, LPCEPSTRA, MELSPEC, FBANK, MFCC, PLP. При использовании мел-кепстральных коэффициентов можно задать необходимость включения нулевого коэффициента, отражающего энергетический уровень (опция Use Energy). Для базового набора указывается количество используемых коэффициентов и другие настройки, регулирующие способ их вычисления. Помимо непосредственно базового набора можно также задать необходимость вычисления производных (от первой до четвёртой). Настройка состава и количества параметров для которых вычисляются производные

указываются в области «Differential Coefficients». Для вычисленного базового набора признаков может быть выполнена процедура нормализации. Нормализация выполняется при задании соответствующих настроек в секции «Normalization».

После завершения процесса параметризации сигнала у пользователя имеется возможность просмотреть динамику изменения каждого из параметров. Для этого ему необходимо нажать на кнопку «View». Нажатие на данную кнопку приводит к открытию отдельного окна в котором в виде графиков можно просмотреть динамику изменений значения по любому из выбранных параметров. Также имеется возможность просмотра результатов гармонического анализа в виде спектра. Чем больше интенсивность определённой гармоникой, тем больше её цветовая насыщенность.



Рис. 7 Детальный гармонический спектр отдельного участка сигнала

Для любого из кратковременных речевых сегментов можно отобразить детальные результаты гармонического анализа (Рис.7). На графиках Рис. 7 показан набор гармоник, составляющих анализируемый речевой сегмент. Гармоники отображаются в виде двух спектров: спектр амплитуд и спектр фаз. Каждая отдельная гармоника отмечена линией. Серой линией на графике показан сглаженный спектр, вычисленный на основе коэффициентов линейного предсказания.

7 Сегментация речевого сигнала

Следующим важным этапом в процессе построения цифрового голосового портрета личности является сегментация речевого сигнала на отдельные сегменты, которые формируют своего рода базовый акустический алфавит и являются атомарными речевыми единицами. Фактически программа позволяет осуществить сегментацию по любому из имеющихся параметров. Однако имеет смысл производить сегментацию, используя параметры, имеющие отношение к спектральному вариационному контуру. Именно они дают наилучшие физически интерпретируемые результаты сегментации. В качестве таковых могут быть использованы следующие параметры:

- SVC – Spectral Variation Contour (Спектральный вариационный контур)
- SPSVC - Smoothed Phase Spectrum Variation Contour (сглаженный вариационный контур фазового спектра);
- SASVC - Smoothed Amplitude Spectrum Variation Contour (сглаженный вариационный контур амплитудного спектра);
- TDVC Delta - Time Domain Variation Contour Delta (производная от вариационного контура во временной области).

Сегментация осуществляется следующим образом: анализируется динамика изменения выбранного параметра, находятся его экстремальные точки, в качестве отдельного сегмента помечается участок речевого сигнала, находящийся между двумя соседними экстремумами. Тип экстремума (максимум/минимум), а также его минимальная амплитуда также могут быть заданы пользователем до начала процесса сегментации.

Также сегментация может быть осуществлена синхронно с частотой основного тона речевого сигнала.

После завершения процесса сегментации его результаты могут быть просмотрены в виде отдельной диаграммы либо экспортированы в отдельный звуковой файл с пометкой отдельных сегментов регионами. Для просмотра полученных сегментов на диаграмме необходимо нажать кнопку «View».

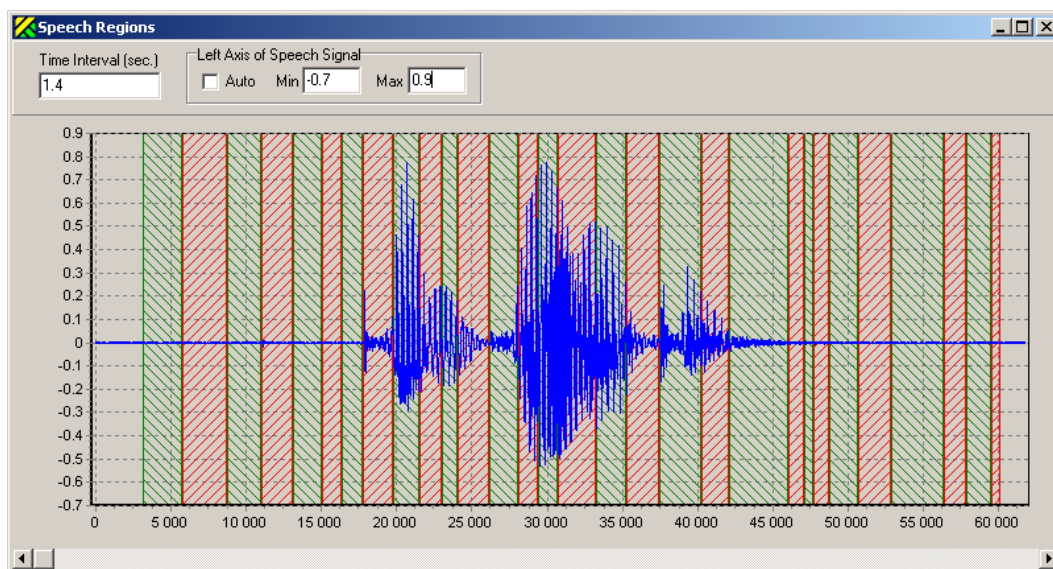


Рис. 8 – Окно для просмотра результатов автоматического сегментирования

На Рис.8 показан результат автоматического сегментирования

8 Кластеризация полученного множества речевых сегментов

Одним из финальных этапов в процессе формирования цифрового голосового портрета личности является кластеризация всего полученного множества речевых сегментов с целью их распределения на относительно небольшое количество их групп (кластеров). Все сегменты, объединённые в рамках одного кластера, должны обладать общностью своих свойств.

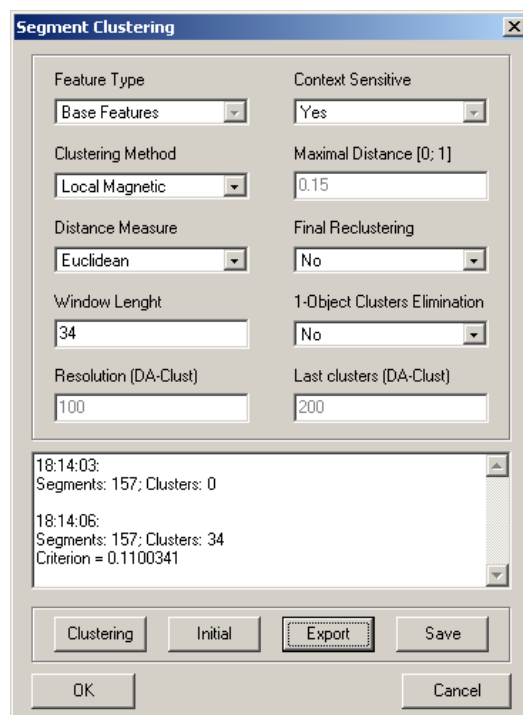


Рис. 9 Интерфейс для задания параметров кластеризации

На Рис.9 приведён интерфейс пользователя, с помощью которого осуществляется задание настроек процесса кластеризации. Сначала пользователю необходимо выбрать тип информативных признаков, которыми будут заданы объекты в процессе кластеризации. Имеется возможность выбора базового набора признаков, расширенного набора (базовые признаки, дополненные производными) и сглаженного спектра. Кластеризация может быть выполнена с использованием нескольких методов. Каждый из этих обладает своими преимуществами и недостатками. Некоторые методы показывают хорошие точностные характеристики при кластеризации большого количества объектов, другие показывают наименьшее время кластеризации.

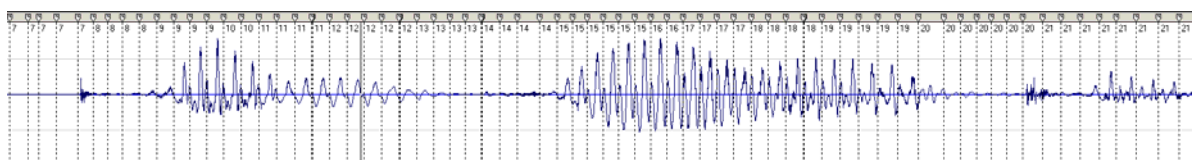


Рис. 10 Результат кластеризации фрагмента речевого сигнала с использованием метода «Local Magnetic»

Важно отметить, что все разработанные и включённые в библиотеку методы кластеризации не требуют изначального задания количества кластеров. Данное количество определяется самим алгоритмом по результатам кластеризации. В инструментарии кластеризации имеется возможность использовать шесть различных алгоритмов.

Для примера на Рис. 10 показан результат кластеризации фрагмента речевого сигнала с использованием метода «Local Magnetic». Данный алгоритм специально разработан в рамках реализации данного проекта. В нём учитываются априорные знания

о структуре речевого сигнала, а именно то, что близкие по признакам объекты синхронизированные с частотой основного тона имеют тенденцию располагаться компактно по временной шкале. Анализируя «силу притяжения» между текущим объектом и его правым и левым соседями принимается решение о его присоединении к одному из них. Данная процедура выполняется итеративно и в итоге получается распределение объектов по компактным локальным группам. На втором этапе уже сами локальные компактные группы выступают в качестве агрегированных объектов, над которыми также выполняется процедура кластеризации, результат которой является итоговым.

Одним из основных параметров в разработанных алгоритмах является допустимое максимальное расстояние любыми двумя объектами, включёнными в один кластер (Maximal Distance). Значение данного параметра оказывает существенное влияние на полученное итоговое количество кластеров.

Общее количество полученных кластеров характеризует размерность используемого субфонемного алфавита. В каждом полученном кластере выявляется центральный экземпляр (центроид), который является эталоном всего кластера. По результатам кластеризации формируется компактный инвентарь сегментных эталонов, который включается в состав цифрового голосового портрета личности. Результаты кластеризации сохраняются системой в отдельный файл и могут быть проинспектированы графически в том виде как показано на Рис.10, где над каждым сегментом указан номер того кластера, в который он вошел по итогам кластеризации.

Список источников

- 1 Kaiser, James F. "Nonrecursive Digital Filter Design Using the I0-sinh Window Function." Proceedings of the 1974 IEEE International Symposium on Circuits and Systems. 1974, pp. 20–23.
- 2 Bou-Ghazale S.E., Hansen Jh, L. A comparative study of traditional and newly proposed features for recognition of speech under stress // IEEE transactions on speech and audio processing. -2000. -4(8). -C.429-442.
- 3 Murty K.R., Yegnanarayana B. Combining evidence from residual phase and MFCC features for speaker recognition // IEEE signal processing letters. -№1(13). -2006. -C. 52-55.
- 4 Polur P.D., Miller G.E. Experiments with fast Fourier transform, linear predictive and cepstral coefficients in dysarthric speech recognition algorithms using hidden Markov model // IEEE transactions on neural systems and rehabilitation engineering. -2005. -№4(13). -C. 558-561.
- 5 Marzetta T.L. Two-dimensional linear prediction - auto-correlation arrays, minimum-phase prediction error filters, and reflection coefficient arrays // IEEE transactions on acoustics speech and signal processing. -1980. -№6(28). C. 725-733.
- 6 Arai T., Pavel M., Hermansky H. Syllable intelligibility for temporally filtered LPC cepstral trajectories // Journal of the acoustical society of America. -1999. -№5(105). -C. 2783-2791.
- 7 Sahidullah M., Saha G. Design, analysis and experimental evaluation of block based transformation in MFCC computation for speaker recognition // Speech communication. -2012. -№4(54). -C.543-565.
- 8 Shah N.J., Vachhani B.B., Sailor H. Beffectiveness of plp-based phonetic segmentation for speech synthesis // IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). -Florence, ITALY. -2014. -C.432-445.

- 9 Zhao Y.X. Self-learning speaker and channel adaptation based on spectral variation source decomposition // Speech communication. -1996. -№1(18). -C. 65-77.
- 10 Quatieri T.F., McAulay R.J. Speech transformations based on a sinusoidal representation // IEEE transactions on acoustics speech and signal processing. -1986. -№6(34). -C. 1449-1464.
- 11 Evangelopoulos G., Maragos P. Multiband modulation energy tracking for noisy speech detection // IEEE transactions on audio speech and language processing. -2006. -№6(14). -C. 2024-2038.
- 12 Shenoy R.R., Seelamantula C.S. A Zero-Crossing Rate Property of Power Complementary Analysis Filterbank Outputs // IEEE signal processing letters. -2015. -№12(22). -C. 2354-2358.
- 13 Leemann A., Mixdorff H., O'Reilly M. Speaker-individuality in Fujisaki model f0 features: implications for forensic voice comparison // International journal of speech language and the law. -2014. -№2(24). -C. 343-370.

DEVELOPMENT OF SPEAKER-INDEPENDENT LIMITED-VOCABULARY KAZAKH SPEECH RECOGNITION SYSTEM

Mussabayev R.R.¹, Amirgaliyev Ye.N.¹, Tairova A.T.², Kozbakova A.H.²
email: rmusab@gmail.com

¹ *Institute of Information and Computational Technologies SC MES RK,
Kazakhstan*

² *Uniline Group LLP, Kazakhstan*

Abstract. *In the given article considered the process of speaker-independent limited-vocabulary Kazakh speech recognition system development. System is based on the hidden Markov models, i.e. possibilities of observable symbols are set up by the continuous function of distribution while the transition probabilities from one status to another is kept as discontinuous. The process of recognition is based on the applying of Viterbi algorithm. For the limited vocabulary the recognition accuracy of 90% was archived.*

At the present moment active investigations to create software module of Speaker-independent limited-vocabulary (200-300 words) Kazakh speech recognition system are conducted. Design system is proposed to be used for desk computers and mobile devices (smartphones, tablet computers) for voice search in Google maps.

It was decided that the system had to be based on the hidden Markov models, i.e. possibilities of observable symbols are set up by the continuous function of distribution while the transition probabilities from one status to another is kept as discontinuous. The process of recognition is based on the Viterbi algorithm usage [1]. System testing was performed with the dictionary of 200 words, which were pronounced by different speakers who didn't participate in system setting process. System development consisted of the following stages: dictionary making, initial speech processes and feature selection, construction of code book, setting of hidden Markov models, recognition system testing.

1 Dictionary making

For Dictionary making the detailed map of Almaty (up to building number) with was taken. Example: Алматы Абай даңғылы екінші үй. Program module (developed by the creators) will use interface API which is presented on Google web site. As interface API understands only Russian words, it is necessary to perform translation of words from Kazakh to Russian language. Avenues and streets of Almaty center as well as numerals (Table 1) were included into the list of words. In Future this list will be updated with information of the rest of city Almaty districts.

Table 1. List of words

Алматы	Фурманов
Астана	Достық
Даңғылы	Бірінші
Көшесі	Екінші
үй	үшінші
Абай	төртінші
Панфилов	Бесінші
Пушкин ...	Алтыншы

There are 300 words in the dictionary.

2 Initial speech processing and feature selection

The speaker pronounces the certain phrase which is made as word sequence $W = w_1, \dots, w_N$. The task of the system is to recognize this word sequence. However, during recognition there can be mistakes, so the result will differ from W .

On the first stage of speech signal recognition it is necessary to pass the signal through low-frequency filter for the purpose of decreasing noise impact on the comparand words which will be used later for speech recognition. It is necessary to «cut» obtained sequence of digital read-outs on segments with the duration of 10-30 msec. Usually the segments are selected in such a way that they are covered in half or in 2/3. The covering is used for prevention of loss of the information about the signal on the border (Fig. 1) [1].

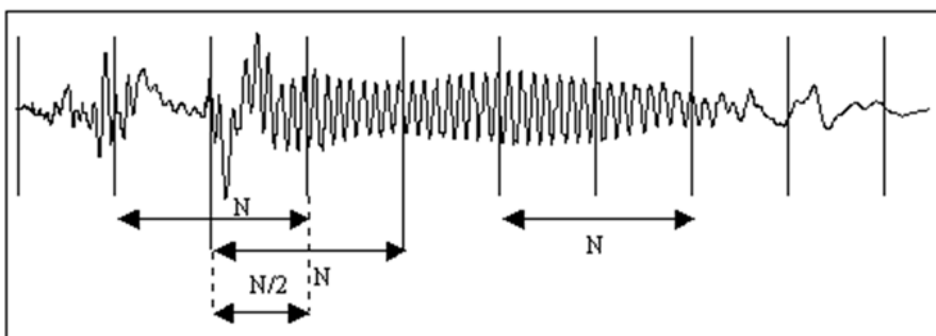


Fig. 1 Dividing of the speech signal on covering signals

For suppression of the unwanted boundary effects it is customary to multiply the signal on Hamming window function, which is given by the following formula:

$$w(n) = \begin{cases} 0.54 - 0.46 \cos\left(\frac{2\pi n}{N-1}\right), & 0 \leq n \leq N \\ 0, & \text{else} \end{cases}$$

The graph of the Hamming window function is presented below (Figure 2):

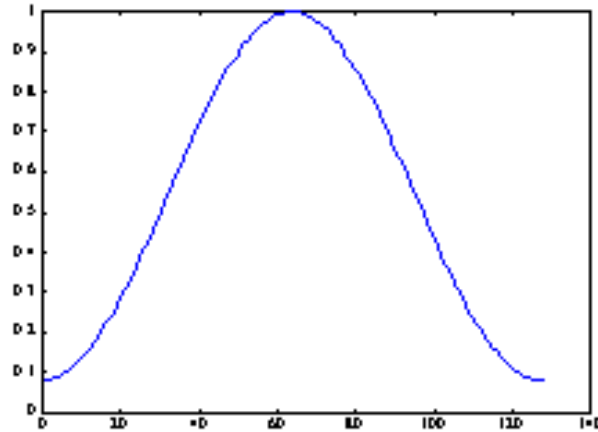


Fig. 2 The graph of the Hamming window function

The superposition of the Hamming window slightly reduces the specter's contrast, but it allows taking away side lobes of cracked frequencies, however speech harmonic composition is especially become apparent.

In developing system from the speech signal output the following distinguished element are extracted: mel- frequency coefficient (MFCC); E – energy level of signal indicated in window, where P is determined energy threshold (Fig. 3).

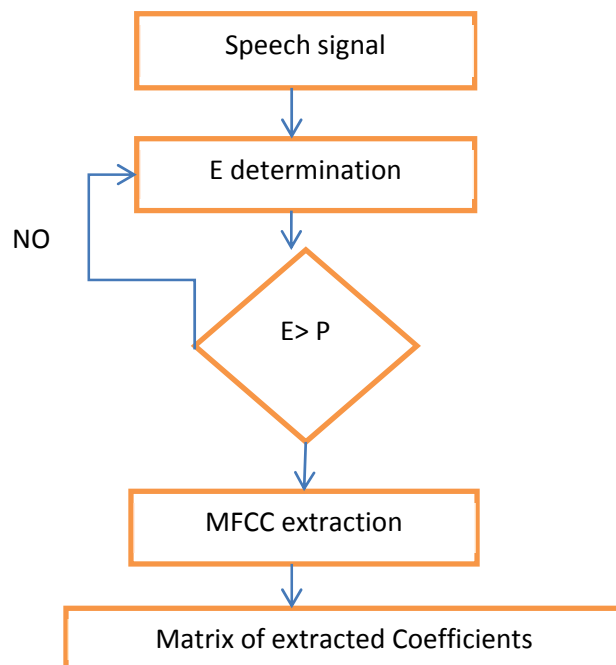


Fig. 3 – The scheme of voice processing

At present time there is a wide pattern of signal parameter representation on the basis of auto-correlation analysis, instrumental bandpass filtering, spectrum analysis methods, linear prediction coefficients [1,2]. The signal spectrum analysis with calculation of its cepstral characteristics is the most common approach to the speech parameterization [3].

Cepstral coefficients technically can be calculated in the following way:

$$\check{C} = \hat{H}(\log(|H(\check{Y})|)),$$

where H и $\hat{H}$ – direct and indirect inverse Fourier transformation respectively, $\check{Y}$ - original signal. There is an effective method of cepstrum calculation – directly from coefficients of linear prediction a_i :

$$c_k = a_k + \frac{1}{k} \sum_{i=1}^{k-1} i c_i a_{k-i}, \quad \text{где } k = 1, \dots, p$$

$$c_k = \frac{1}{k} \sum i c_i a_{k-i}, \quad \text{где } k > p$$

Coefficient c_0 is determined from the formula:

$$c_0 = \ln \delta^2, \quad \text{where } \delta^2 = \frac{E^{(0)}}{E^{(F)}} - \text{is a magnification coefficient, which can be}$$

determined in the process of algorithm Levinson-Durbin usage.

«Dynamic» effects of the specific characteristics can be improved by the addition of “cepstrum derivatives” of order K , which are determined from the formula:

$$\Delta c_k = \mu \sum_{i=-K}^K i c_{k-i},$$

where μ - normalization factor, K - order of derivative.

Received feature vector later will be used for code book construction, for practice in hidden Markov models, as well as for speech recognition.

3 Construction of code book

The final target of our work is the development of speaker-independent recognition system. It means that the system has to be of low sensitive to the pronunciation of different people. It's not possible to store all kinds of pronunciation specialties, as we have hardware restrictions of memory space for recognizer and for system response time. That is why the code book is usually used– i.e. the list of limited number of «sample» characteristics (code book's words) is used. The number of code words has to be large enough for simple speech encoding of any man. At the same time the volume of the code book has to be as compact as possible for recognition time cutting. This results in task of optimal choice of code book size. The speech $S(t)$ is convert into the set of characteristic features $\{X_1, \dots, X_N\}$, for those features the most closest analogous of sample features is selected from code book $\{C_1, \dots, C_N\}$. For Code book

construction the clustering of initial speech signals was performed; initials speech signals of large number of speakers were recorded with the help of modified K-average algorithm [4].

At first it is necessary to select the number of clusters N and to perform initialization of centroids $y_1, y_2, \dots, y_N$. Initialization can be performed in a random way or in a way of simple fragmentation equally, as well as in a way with definite more simple algorithms for clustering. After that the classification of input value is performed with using of calculated centroids:

$$d(x, y_i) = \min_j d(x, y_j) \Rightarrow Q(x) = y_i, \quad j = 1, 2, \dots, N$$

The assessment of the distance between two feature vectors is calculated with the help of Euclidean metric. As the result the local distance between vector X of the signal 1 and vector Y of the signal 2 calculated by formula:

$$d(x, y) = \sqrt{\sum_i (x_i - y_i)^2}$$

On the next step each centroid is changed with mean value of objects related to match cluster.

$$y_i = \frac{\sum_{k=1}^{K_i} x_k}{K_i}, \quad Q(x_k) = y_i, \quad i = 1, 2, \dots, N.$$

One of two criteria is chosen as stopping criterion:

1. The absence of conversion of the object from cluster to cluster.
2. Minimum change of mean square root error.

4 Speech recognition model

At the present time hidden Markov models (HMM) are the most effective methods of speech recognition [1]. When constructing the model, the main characteristics are chosen: model type (ergodic, Backs model, left-right model etc.), model size (number of states), type of observable parameters (discrete or continuous frequency distribution of observation vector). As our dictionary is not large, the number of distance for each word is equal to number of phonemes in the word (Fig. 4).

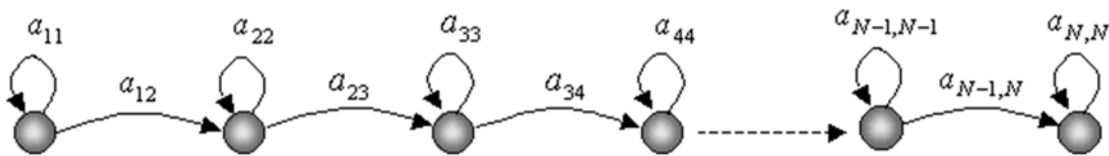


Fig. 4 Left-right model

Its own set of parameter vectors corresponds to each state.

Markov word model $\lambda = (A, B, \pi)$ set by the following parameters [5]:

- 1) $A = \{a_{ij}\}$ - stochastic distribution of state transitions.
- 2) $B = \{b_j(k)\}$ - stochastic distribution of appearance of observation symbols in state j.
- 3) probability distribution of initial states $\pi = \{\pi_i\}$ of the model.

At the stage of automatic speech recognition all possible state transitions HMM are built and with the help of Viterbi algorithm the probability of final state is calculated. The algorithm consists of forward and backward passes [5]. As the first step it is necessary to introduce the following variable:

$$\delta_t(i) = \max P[q_1 q_2 \dots q_{t-1} q_t = S_i, o_1 o_2 \dots o_t | \lambda]$$

as a maximum probability as what the sequence of states will be completed in time t of the state S_i at given observations till the time t. Also the variable $\omega_e(j)$ is to be introduced for conservation of arguments, maximum $\delta_t(j)$. The algorithm consists of 4 steps:

- 1) Initialization

$$\begin{aligned} \delta_1(j) &= \pi_j b_j(o_1), 1 \leq j \leq N \\ \omega_1(j) &= 0 \end{aligned}$$

- 2) Inductive transition

$$\delta_t(j) = \max_{1 \leq i \leq N} [\delta_{t-1}(i) a_{ij}] b_j(o_t), 1 \leq j \leq N, 2 \leq t \leq T$$

$$\omega_t(j) = \arg \max_{1 \leq i \leq N} [\delta_{t-1}(i) a_{ij}]$$

- 3) Stopping

$$P = \max_{1 \leq i \leq N} [\delta_T(i)]$$

During the third step the maximum probability of observation in sequence of observations is determined $O_1 O_2 \dots O_T$.

- 4) Repair of the best sequence of states (backward pass):

$$q_t = \arg \max_{1 \leq i \leq N} [\delta_t(i)], t = T-1, T-2, \dots, 1$$

Maximum appearance probability of recognized sequence of observations of specified hidden Markov word model is the result of algorithm output.

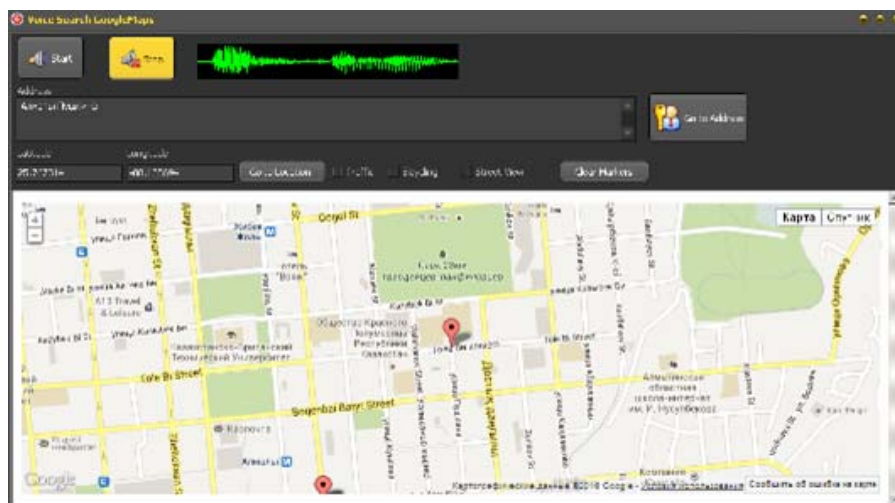


Fig. 5 The system of voice search by maps in Kazakh language

5 Recognition system testing

The graphical user interface of the developed system is shown in the Fig. 5. For recognition system checking the dictionary with 300 words was used. For hidden Markov model settings speech data of 8 speakers was used: 4 males and 4 females, in total 2000 words. For test performance the speech data of 4 speakers was used: 2 males and 2 females (with normal and high pitched voices), in total 1000 words. According to results of testing the recognition accuracy of 90% was archived.

References

1. Rabiner L.R. Fundamentals of Speech Recognition / L. Rabiner, B. Juang – New Jersey: Prentice – Hall, Englewood Cliffs, USA, 1993.
2. Markel, D.D Speech linear prediction / D.D. Marckel, A.H. Grey; M: Svyaz, 1980. – 308 p.
3. Kosarev U.A. True form of computerized dialog / U.A. Kosarev – JL.: Mashinostroyeniye, 1989. – 143 p.
4. P. Hedelin. Vector Quantization for Speech Transmission / P. Hedelin, P. Knagenhjelm, M. Skoglund. – Speech Coding and Synthesis. – 1995. – pp. 311 – 346.
5. Rabiner L.R. A tutorial on Hidden Markov Model and Selected Applications in Speech Recognition / L.R Rabiner // Proceeding of the IEEE, vol, 77. No.2, 1989, pp. 257-284.

DETERMINATION OF THE OPTIMAL PHONETIC SET OF THE KAZAKH LANGUAGE

Mussabayev R.R.¹, Amirgaliyev Ye.N.¹, Tairova A.T.², Kozbakova A.H.²
email: rmusab@gmail.com

¹ *Institute of Information and Computational Technologies SC MES RK,
Kazakhstan*

² *Uniline Group LLP, Kazakhstan*

Abstract. *In the process of the Kazakh speech recognition system realization, the complex of works was carried out for the determination of the optimal phonetic set of the Kazakh language. The optimality is defined by the compromise between the reduction of redundancy of phonetic structure and the completeness of reflection of all available sounds.*

The majority of the speech recognition systems are developed on the basis of the phonetic representation of the speech. This is the main level, and its realization quality impacts on the whole system. The speech recognition systems are the language depending systems. In its turn any natural language has its own phonetic set [1] and the specifics of intonation pronunciation [2]. The degree of the phonetic set similarity is higher for kindred languages.

In the process of the Kazakh speech recognition system realization, the complex of works was carried out for the determination of the optimal phonetic set of the Kazakh language. First of all the optimality is defined by the compromise between the reduction of redundancy of phonetic structure and the completeness of reflection of all available sounds. On the one hand, if we use the big amount of phonemes on the phonetic level, then we can obtain potentially much more qualitative signal in the output of recognizer. On the other hand, due to the increase of the amount of phonemes, the complexity of processing and formation of databases of speech segments increases. The sounding of each phoneme in the main degree depends on its phonetic neighborhood. For the providing of qualitative recognition it is necessary to take into consideration all possible combination variants whose amount increases with the increase of the phonetic set of the language. If the phonetic set of the Kazakh language consists of 35 phonemes, then in the ideal variant for providing of the best recognition quality it is necessary to extract $35^2 = 1225$ sounding variants for each phoneme. In this case all the possible variants of phonetic combinations will be considered.

In accordance with the methodic proposed in [3], the basic phonetic set of the Kazakh language is represented by the following set of 28 phonemes: A, AE, E, I, O, OE, U, UU, Y, B, D, G, GG, J, K, L, M, N, NN, P, Q, R, S, SH, SW, T, Z, ZH.

For the providing of possibility of synthesis of numerous Russian, English, Arabian and Persian loanwords the 7 more additional phonemes are added: CH, F, C, V, EH, H, X.

Thus, as the general phonetic structure of the Kazakh language it is offered to use 35 phonemes. The given phonetic set has been as much as possible minimized. The following complex phonemes which can be recognized of the listed above elementary components: IJ, JA, JAE, JUU, JU, JO, UJ, UUU, YJ, DZH - have not entered this set.

For the recognition purposes it is necessary to use also a phoneme which describes a speech pause - PAU.

At the process of the development of the speech recognition system it is important to make the analysis and classification of the phonetic structure of the Kazakh language by the sound wave forms. During the conduction of the analysis of the sound wave forms the main types of classes are determined which are used for acoustic classification.

During the conducting of the analysis of existing sound wave forms, several main acoustic classes were determined for the Kazakh language.

All phonemes, where the dominant frequency is the frequency of the fundamental tone, were referred to the first class. These are all the vowels (A, AE, E, I, O, OE, U, UU, Y, EH) and the part of the consonants which have the vocalized dominant (B, D, G, GG, J, L, M, N, NN, V, Z, ZH) [4]. On the Fig. 1 the typical forms of sound waves are shown.

This class also includes the consonants of the Kazakh language which have the strong domination of low frequency component in the form of fundamental frequency: B, D, G, GG, J, L, M, N, NN, V, Z, ZH. These sounds are mainly formed by resonance processes in the vocal tract during the low work of vocal fold.

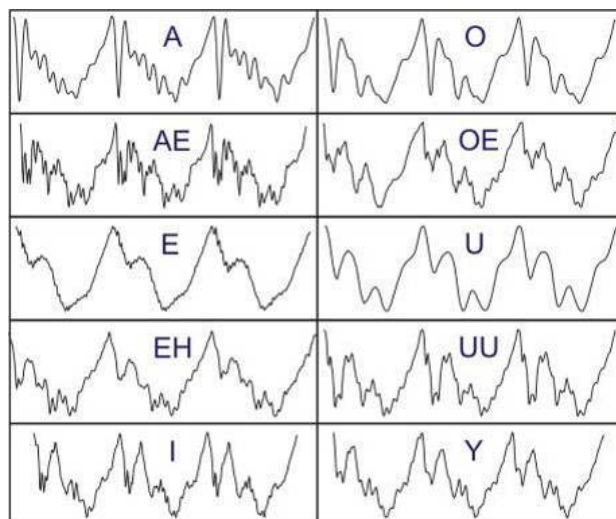


Fig.1 The typical wave forms of vowel sounds

In the Fig. 2 the typical wave forms for each of the Kazakh vocalized consonant phonemes are depicted.

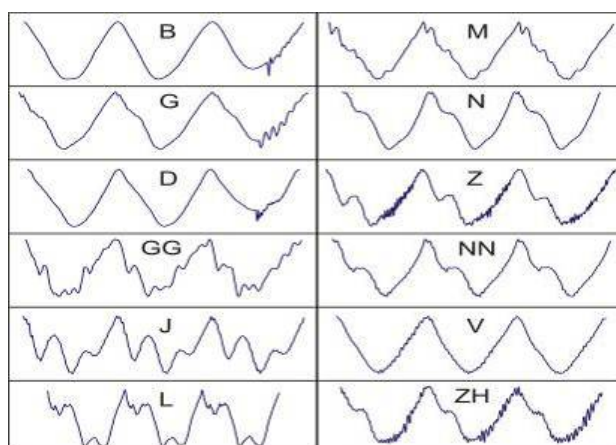


Fig. 2 The typical wave forms for each of the Kazakh vocalized consonant phonemes

From the showed above figure it is seen that the part of vocalized consonants also has the high frequency component: V, Z, ZH, GG.

The noise consonant phonemes with the dominant high frequency component: F, H, S, SH, SW, X – were referred to the second class. The vocalized component is fully absent in this class of phonemes. The noise sound is produced by collision of outgoing air with some obstacle. On the Fig. 3 the form of the sound wave of noise consonant between two vowel sounds is shown.

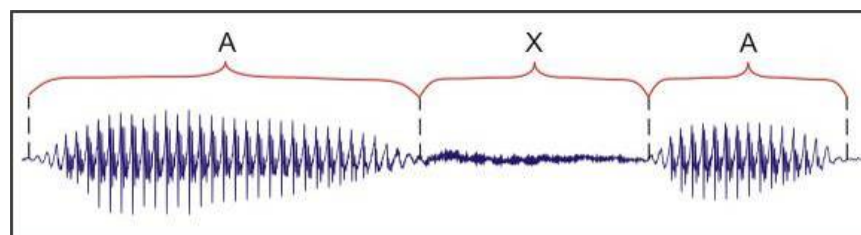


Fig. 3 The form of the sound wave of noise consonant between two vowel sounds

In the Fig. 3 it is seen that noise consonants in comparison with vocalized sounds have much lower amplitude of fluctuations, but their fluctuation frequency is higher.

In the Fig. 4 the forms of sound waves for all noise consonants of the Kazakh language are depicted.

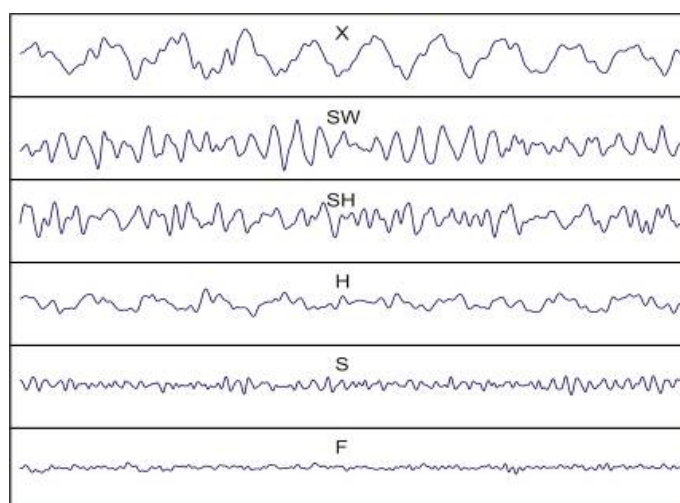


Fig. 4 The forms of sound waves for all noise consonants of the Kazakh language with duration of 10 ms

The Kazakh language consonants which also have the noise source of excitation are referred to the third class: CH, K, P, Q, T, C. They are formed with the preceding area of aspiration expressed in the form of a short pause (PAU) with the subsequent sharp short-term explosion with smooth transformation to the subsequent noise. In the Fig. 5 the example of the transitions in the sound wave with plosive consonant between two vowels: A-PAU-K-A is shown.

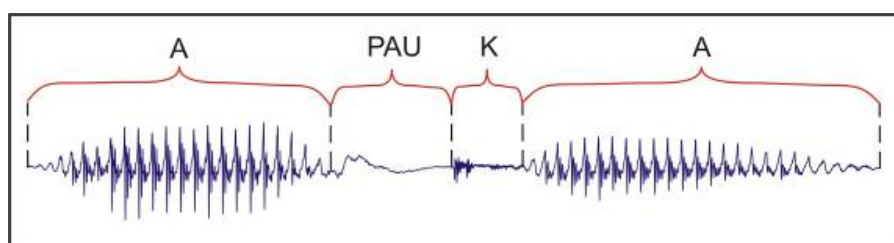


Fig. 5 The example of the transitions in the sound wave with plosive consonant between two vowels: A-PAU-K-A

In Fig. 6 the typical forms of the sound wave for each plosive phoneme are shown.

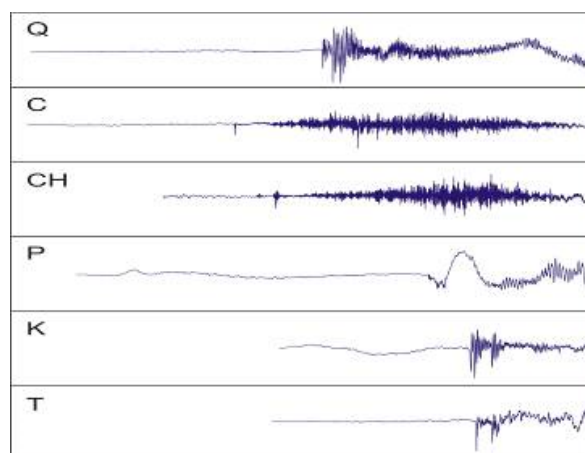


Fig. 6 The typical forms of the sound wave for each plosive phoneme

It is seen from the figure that these types of sounds have different durations of noise field and also have the different durations of previous pauses.

Within the process of the analysis of the phoneme structure of the Kazakh language, the allophone analysis also was carried out. In particular during the allophone analysis the possible transitions from one acoustic class to another in the set of allophones of one phoneme in the various phonetic environment were revealed. The special phoneme type is the phoneme R whose allophones can be classified by three set of classes: with dominant fundamental frequency, clear noise and mixed noise-vocalized (Fig.7).

Thus, in the process of classification of the Kazakh language phonetic structure the following phonetic-acoustic classes were revealed:

1. Vowels and consonants with dominant fundamental frequency (low frequency component).
2. Consonant phonemes with dominant high frequency component.
3. Consonant phonemes consisting both low frequency and high frequency components.
4. Consonant phonemes with the preceding pause and the following explosion which transforms to the high frequency noise.

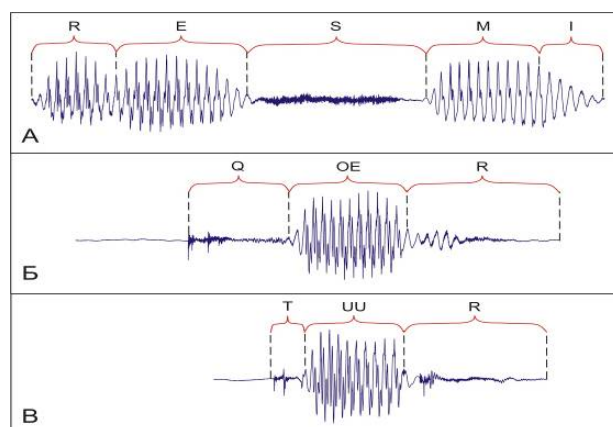


Fig.7 The allophones of phoneme R with different acoustic classifications (A – fundamental frequency; B - fundamental frequency + noise component; B – only noise component)

In the process of classification of the phonetic structure of the Kazakh language it is necessary to specify both the set of the objective physical features which characterize the phonemes and set of subjective (perceptive) properties which appear during the auditory perception of the phonemes. If the objective features of a phoneme can be physically measured, then the subjective properties are evaluated by empirical methods.

The objective physical characteristics of the Kazakh phonemes are:

1. Duration;
2. Sound wave form;
3. Amplitude envelope form;

The empirical ones:

1. Intonation;
2. Pitch of sound;
3. Loudness;
4. Softness/Hardness
5. Labial/Non labial.

In the Table 1 the complex classification of the investigated phoneme structure of Kazakh language is given.

The listed above table is the base system of the phonetic classification of the Kazakh language. In its turn, this classification is the base for various algorithms for the realization of the speech recognition processes. Both the consistence of all phonetic system and the final quality of the recognition results depend on the correctness of this classification formation.

The division into vowels and consonants is caused by the degree of participation of vocal chords in the formation of a corresponding sound. In case of dominating of vocal fold participation in the formation of a concrete sound it has the obvious voice-frequency periodic structure at the level of fundamental frequency in the range of 80-150 Hz (a man's voice) and is classified as a vowel. In the Kazakh language it is possible to determine the following set consisting of 10 vowel sounds: A, AE, E, I, O, OE, U, UU, Y, EH. They are characterized by a wide range of change of duration: can be both short and long.

Table 1. The phonetic structure of the Kazakh language

Transcription	Example	Alphabetic correspondence	Noise / Tone / Plosive	Labial vowel	Soft /Hard vowel	Vowel /Consonant	Original / Adopted	Phoneme	ID
10	9	8	7	6	5	4	3	2	1
								PAU	0
B A L A	бала	a	T		T	V	O	A	1
ZH A E N E	және	ə	T		M	V	O	AE	2
M E N	мен	e	T		M	V	O	E	3
ZH I G I T	жігіт	i	T		M	V	O	I	4
B O L	бол	o	T	O	T	V	O	O	5
S O E Z	сөз	ə	T	O	M	V	O	OE	6

7	U	O	V	T	O	T	ұ	бұл	B U L
8	UU	O	V	M	O	T	ү	түс	T U U S
9	Y	O	V	T		T	ы	қызыл	Q Y Z Y L
10	EH	A	V	M		T	э	экран	E H K R A N
11	B	O	C			T	б	еңбек	E N N B E K
12	CH	A	C			NP	ч	матч	M A T C H
13	D	O	C			T	д	қайда	Q A J D A
14	F	A	C			N	ф	флот	F L O T
15	G	O	C			T	г	деген	D E G E N
16	GG	O	C			NT	ғ	маған	M A G G A N
17	H	A	C			N	h	қаһар	Q A H A R
18	J	O	C			T	й	айт	A J T
19	K	O	C			NP	к	екен	E K E N
20	L	O	C			T	л	ала	A L A
21	M	O	C			T	м	аман	A M A N
22	N	O	C			T	н	ойна	O J N A
23	NN	O	C			T	ң	жаңа	Z H A N N A
24	P	O	C			NP	п	аспан	A S P A N
25	Q	O	C			NP	қ	ақыл	A Q Y L
26	R	O	C			T/N/NT	р	қара	Q A R A
27	S	O	C			N	с	кісі	K I S I
28	SH	O	C			N	ш	қамшы	Q A M S H Y
29	SW	O	C			N	щ	тұщы	T U S W Y
30	T	O	C			NP	т	мата	M A T A
31	C	A	C			NP	ц	матрац	M A T R A C
32	V	A	C			NT	в	аванс	A V A N S
33	X	A	C			N	х	хат	X A T
34	Z	O	C			NT	з	қызыл	Q Y Z Y L
35	ZH	O	C			NT	ж	олжа	O L Z H A

Also one of the distinctive features of vowel sounds is their raised peak level concerning the general peak level of consonants. Consonants have more diverse structure and as consequence more various properties. In the process of recognition the set consisting of 25 consonants has been used: B, CH, D, F, G, GG, H, J, K, L, M, N, NN, P, Q, R, S, SH, SW, T, C, V, X, Z, ZH. The part of the given set consisting of 12 sounds also has the strongly pronounced low frequency tonal structure: B, D, G, GG, J, L, M, N, NN, V, Z, ZH. The sounds like V, Z, ZH, GG besides the low frequency tonal component also have the high frequency noise component. In the sounds F, H, S, SH, SW, X only the high frequency noise component dominates. There are also the mixed types of consonant sounds when the noise component is preceded by the pause, and the subsequent plosive component is smoothly transformed to the noise one: CH, K, P, Q, T, C. All the listed vowel and consonant phonemes keep the stable structure, that is their allophones have the fixed structure on classification « Noise / Tone / Explosion » within the limits of one phoneme. The special phoneme is the phoneme R. It changes the structure depending on the phoneme environment and the position relatively to PAU. So, if R is situated in the beginning or in the middle of a word, then it has the tonal structure. On the last position in a word before a pause or in a soft variant, the given phoneme can have both the pure noise structure and the tonal one. Differentiation on hardness and softness of vowels is used at the realization of the algorithm of the phonetic transcription of the pronounced speech. According to the law of vowel harmony within the limits of a word all

vowels should be hard or soft. Some vowels are paired on the basis of softness-hardness: AE - A, OE - O, UU - U. The attribute of vowel labiality also is used at the phonetic transcription in the process of speech recognition. There is a tendency in the Kazakh language: if within the limits of one word at least one labial vowel is available, then the other vowels are also pronounced in the labial form.

References

1. Kenesbayev S. K., Aralbayev Zh. A. The questions of Kazakh phonetics and phonology.-Alma-Ata: Science, 1979. – 249 pp.
2. Bazarbayevs Z. M. Kazakh intonation. – Almaty: Dayk-Press, 2008.–284 pp.
3. Abuov Zh., Dzhunisbekov A. The phonetical writing of Kazakh text. – Alma-Ata: Science, 1991. – 83 pp.
4. Aralbayev Zh. A. Vocalizm of Kazakh language (the notes on the phonetics and phonology). – Alma-Ata: Science, 1970. – 179 pp.

МЕТОД ОЦЕНКИ ОДНОРОДНОСТИ СМЕСИ СЫПУЧИХ МАТЕРИАЛОВ

Мустафин С.А.
e-mail: sam@ipic.kz

*Институт информационных и вычислительных технологий КН МОН РК,
Казахстан*

Аннотация. Оценка однородности смеси из трудноразделимых материалов, имеет большую предысторию и является одной из операций анализа качества смеси. Важной является задача контроля качества смеси, предполагающая выбор критерия, дающего количественную оценку качества смеси, а также эффективную по времени и точности методику. Цель работы разработка оценки качества однородности смеси.

Задача оценки однородности смеси, состоящей из трудноразделимых материалов, имеет большую предысторию и является одной из трудоемких операций анализа качества смеси в строительной индустрии. При этом важной является задача контроля качества смеси, предполагающая выбор критерия, дающего количественную оценку качества смеси, а также эффективную методику для его экспериментального определения.

Трудность оценки однородности смеси возникает при одинаковых размерах, плотности и форм составляющих элементов смеси, когда традиционные способы разделения невозможны или трудоемки.

Целью данной работы является разработка методики оценки качества однородности получаемой смеси.

Одним из перспективных путей решения оценки смеси на однородность является применение методов анализа с использованием методов обработки изображений для быстрого и качественного анализа экспериментальных данных с извлечением информации о состоянии смеси по получаемым изображениям проб.

В работе рассмотрен метод оценки однородности смеси сыпучих материалов. Для решения предлагается использовать методы автоматической классификации. Существующие методы оценки, как правило, трудоемки.

Трудности, возникающие при оценке качества смеси, вызвали рост работ по разработке методов оценки, основанных на методах обработки изображений, что позволяет производить оценку без механического разделения смеси на составляющие ее элементы. Эти методы основаны на обработке изображения, имеющего определенную цветовую мозаику цветов [1,2].

В основе предлагаемого решения обозначенной проблемы лежит общее положение теории распознавания образов, исходящее из чисто практической установки – несмотря на отсутствие у модели механизма решения проблемы человеком, и, несмотря на отсутствие адекватной математической модели реальной ситуации, попытаться построить правила, реализующие нужный процесс преобразования информации. Другими словами, предлагается расширить (восстановить) описание объекта по его частичным описаниям. Суть анализа заключается в получении информации о геометрических свойствах трехмерных объектов по их представлениям на плоскости.

При определении однородности смеси выделяют следующие этапы (операции):

1. Отбор проб;
2. Равномерное распределение проб на плоскости;
3. Получение фотографий проб - изображение;
4. Обработка изображений.

Не останавливаясь на деталях этапов, рассмотрим подробнее последние два этапа.

Результатом третьего этапа является, по сути, матрица, каждый элемент которой несет информацию о цвете. После считывания информации в память ЭВМ генерируется растровое изображение, под которым понимается матрица, состоящая из большого числа упорядоченных дискретных элементов, каждый из которых может иметь при одинаковых размерах, отличное от других элементов значение оптических характеристик (цвет, плотность и др.). Такие элементы, являющиеся минимальными фрагментами цифрового изображения, называются пикселями.

Используя информацию о цветовой природе изображения можно получать выводы об однородности смеси в целом.

Таким образом, имея матрицу, каждый элемент которой имеет одинаковый набор признаков, требуется произвести проход с одного ребра изображения на противоположное ребро, сохраняя близость необходимых характеристик в локальном окне прохода.

Предлагаемый нами способ позволяет оптимизировать процесс получения оценки однородности - существенно уменьшить трудоемкость операций, повысить точность и, по крайней мере, в несколько раз сократить время процесса по определению однородности.

Предлагаемый метод основан на развитии идеи хорошо зарекомендовавшего себя алгоритма автоматической классификации. Он не относится ни к одному из известных алгоритмов, является примером алгоритма не итерационного типа, который не использует понятия контурных точек, а производит обход изображения в автоматически определяемом им самим направлении.

Данный подход можно применять для быстрого и более точного определения однородности строительных смесей.

Для решения предложенной задачи был построен алгоритм классификации объектов на изображении и создана программа для количественного анализа изображений.

Близкий по идее трассировочный алгоритм выделения осевой линии на изображении был использован нами для горно-геологической задачи - проектирование вскрышных работ, когда требуется определить направление проведения горных работ по выемке минерального сырья и максимально приблизиться к требуемым условиям по содержанию минералосодержащих компонент.

Многие методы распознавания, предложенные для решения научно-технических задач, с той или иной степенью адаптации применимы к задачам, далеким от рассматриваемых задач. Например, методика работы с картографическими материалами может быть трансформирована для понимания изображений, связанных с кровеносными сосудами, сетью нервных волокон, дерматоглификой, сетью дорог по фотографиям, полученным с большой высоты и т.п. Определение скелетов и контуров объектов изображений находит успешное применение при решении различных практических задач - анализ структуры кровеносных сосудов глаза, обработка картографической информации и космических снимков, разделение перекрывающихся частей объекта, анализ формы объекта, нахождение серединной линии в отпечатках пальцев, задачи сегментации изображения, распознавание рукописных знаков, архивация данных изображения.

Работа выполнена в рамках грантового финансирования КН МОН РК.

Литература

1. Экспресс - метод оценки однородности сыпучих материалов / Петров А.А. и др. // Изв. ВУЗов. Химия и химическая технология. - 2012. - вып. 8. - С. 88-90.
2. Богомягих В.А. К определению условного диаметра реальной частицы дискретного сыпучего тела // Инженерный вестник Дона, 2014, №3
3. Мустафин, С.А. Метод построения скелетов бинарного изображения / Мустафин, С.А. // Новости науки Казахстана. – 2001. - № 1. - С. 24-26

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ КИНЕТИКИ РОСТА РАСТЕНИЙ В УСЛОВИЯХ ЗАГРЯЗНЕНИЯ ПОЧВЫ ТЯЖЕЛЫМИ МЕТАЛЛАМИ

Найзабаева Л.К., Нуржанов Ч.А., Мукимбеков М., Сатымбеков М.Н.
e-mail: DarkEremite@yandex.kz

*Институт информационных и вычислительных технологий КН МОН РК,
Казахстан.*

Аннотация

*В статье предложена математическая модель изменения линейных размеров нового биоэнергетического фиторемедианта *Miscanthus x giganteus*, произрастающих на загрязненной почве в зависимости от концентрации тяжелых металлов, с помощью метода наименьших квадратов для дифференциального уравнения.*

Ключевые слова: математическое моделирование, кинетика роста.

Математических моделей роста и развития растений, с учетом процессов протекающие в антропогенно нарушенных почвах, в связи с ростом уровня загрязнения

почвы различными ксенобиотиками незначительны. Техногенное воздействие на растения изучаются в основном на биологическом уровне. В основном модели направлены для решения прикладных задач, таких, например, как диагностика агрометеорологических условий формирования урожая и оценка влияния наблюдаемых и ожидаемых изменений климата на продуктивность сельскохозяйственных культур [1]. Для создания таких моделей предлагаются различные аппроксимирующие зависимости такие, как экспоненциальная, линейная, параболическая и другие [2, 3]. При этом не учитывают внутренние биологические процессы, обуславливающие рост растений, и внешние воздействия, такие как дополнительное питание, температурные изменения, антропогенное воздействие [4].

Цель исследования: создать алгоритмы для моделирования роста и развития растений в условиях загрязнения почвы ксенобиотиками в зависимости от концентрации тяжелых металлов в почве.

В данной работе предлагается математическая модель роста и развития нового фиторемедианта *Miscanthus x giganteus* в условиях загрязнения почвы тяжелыми металлами в двух концентрациях (геохимический показатель загрязнения почвы Zс 165,4±17,1 мг/кг и Zс 20,0±3,1 мг/кг). Для обоснования структуры математической модели при исследовании закономерностей роста растений использовали экспериментальные данные ИББР МОН РК [5].

Все экспериментальные данные по кинетике роста близки к логистической зависимости. Параметры кривой роста определяли с помощью метода наименьших квадратов (МНК), сумма квадратов отклонений рассчитывается по модели значений $\hat{y}_t$ от фактических y_t уровней временного ряда наименьшей:

$$\sum_{t=1}^n (y_t - \hat{y}_t)^2 = \sum_{t=1}^n e_t^2 \rightarrow \min \quad 1$$

$$e_t = y_t - \hat{y}_t \quad 2$$

где, остаток - расхождение фактических и модельных значений показателя Y.

При оценке параметров полиномиальных кривых использовали следующую формулу;

$$y_t = a_0 + a_1 t + a_2 t^2 + \dots + a_q t^q \quad 3$$

В результате минимизации получили систему нормальных уравнений. Система состоит из $(q + 1)$ линейных уравнений, содержащих в качестве известных величин $\sum y_t, \sum y_t t, \sum y_t t^2, \sum y_t t^q$ и $(q + 1)$ неизвестных коэффициентов a_j .

Решение этой системы относительно $a_0, a_1, a_2, \dots, a_q$ позволяет вычислить искомые оценки параметров.

$$\sum_{t=1}^n y_t = a_0 n + a_1 \sum_{t=1}^n t + a_2 \sum_{t=1}^n t^2 + \dots + a_q \sum_{t=1}^n t^q \quad 4$$

$$\sum_{t=1}^n y_t t = a_0 \sum_{t=1}^n t + a_1 \sum_{t=1}^n t^2 + a_2 \sum_{t=1}^n t^3 \dots + a_q \sum_{t=1}^n t^{q+1} \quad 5$$

$$\sum_{t=1}^n y_t t^{q-1} = a_0 \sum_{t=1}^n t^{q-1} + a_1 \sum_{t=1}^n t^q + a_2 \sum_{t=1}^n t^{q+1} \dots + a_q \sum_{t=1}^n t^{2q-1} \quad 6$$

$$\sum_{t=1}^n y_t t^q = a_0 \sum_{t=1}^n t^q + a_1 \sum_{t=1}^n t^{q+1} + a_2 \sum_{t=1}^n t^{q+2} \dots + a_q \sum_{t=1}^n t^{2q} \quad 7$$

На основании анализа экспериментальных данных создали структуру модели роста растений на незагрязненной и загрязненной почве, с помощью метода наименьших квадратов (МНК) и получили эмпирическое уравнение регрессии (рис.1):

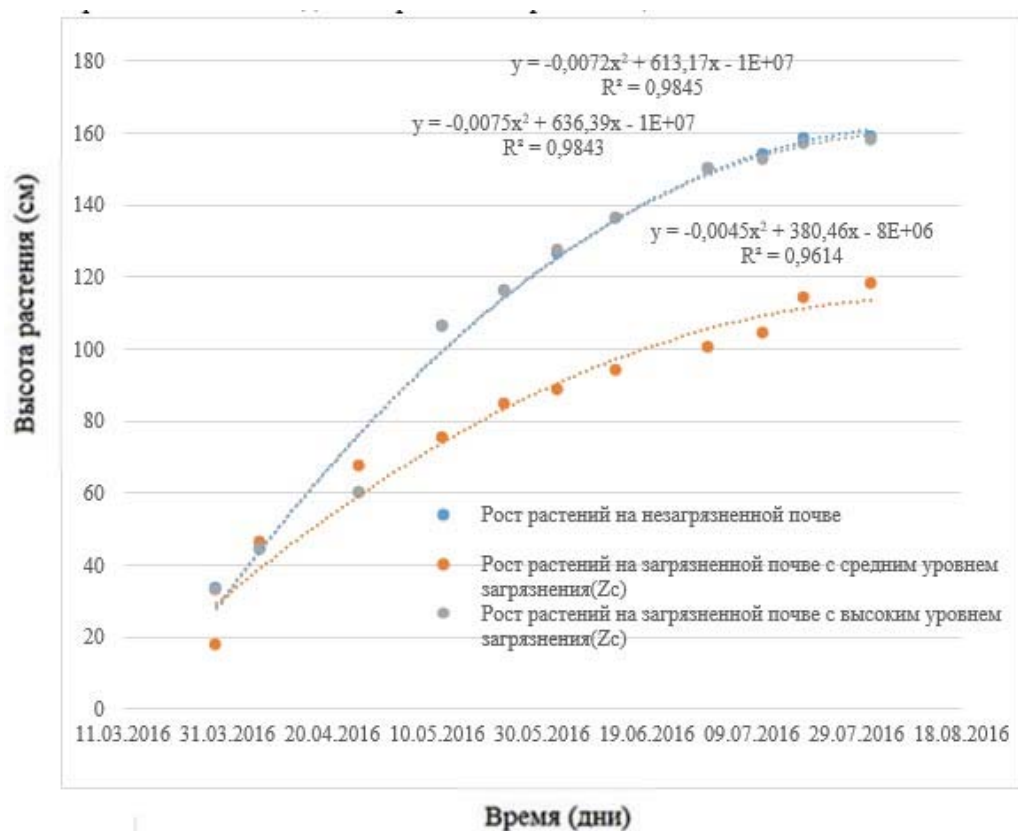


Рис. 1 – Зависимость высоты растений *Miscanthus x giganteus* от времени произрастания с учетом концентрации тяжелых металлов в почве

Эмпирическое уравнение регрессии роста растений на незагрязненной почве:

$$y = -0.0072x^2 + 613.17x - 1E + 07 \quad 8$$

При этом величина достоверности аппроксимации составляет: $R^2 = 0.9843$

Эмпирическое уравнение регрессии роста растений на загрязненной почве со средним уровнем загрязнения ($Z_c 20,0 \pm 3,1$ мг/кг)

$$y = -0.0075x^2 + 636.39x - 1E + 07 \quad 9$$

При этом величина достоверности аппроксимации составляет: $R^2 = 0.9845$

Эмпирическое уравнение регрессии роста растений на загрязненной почве с высоким уровнем загрязнения ($Z_c 165,4 \pm 17,1$ мг/кг).

$$y = -0.0045x^2 + 380.46x - 8E + 06 \quad 10$$

При этом величина достоверности аппроксимации составляет: $R^2 = 0.9845$

Для описания динамики роста растений использовали следующее уравнение [2, 6]:

$$\frac{dl}{dt} = \mu l \left(1 - \frac{l}{l_{max}}\right) \quad 11$$

где t – время (дни), l – текущая высота растения (см), l_{max} – теоретическая максимальная высота (см), которую может достигнуть растение по окончании роста, μ – константа (удельная скорость роста, размерность – 1/день).

Решением данного уравнения была функция (l_0 – начальная высота растения):

$$l(t) = l_{max} \frac{l_0 e^{\mu t}}{l_{max} - l_0 + l_0 e^{\mu t}} \quad 12$$

На основании данных уравнения (12) получили эмпирическое уравнение теоретической кривой роста растений на незагрязненной почве и загрязненной почве (рис.2).

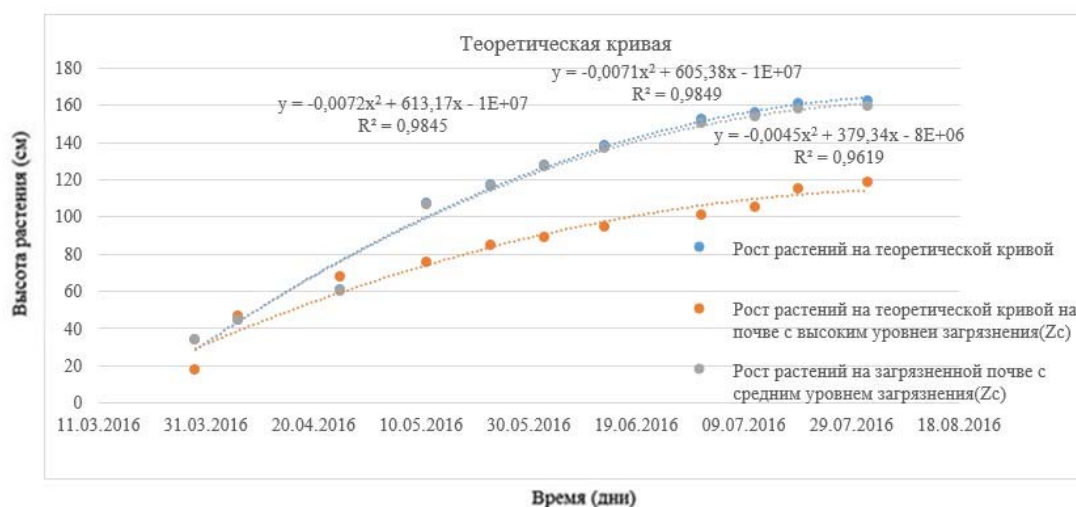


Рис. 2 – Теоретическая кривая роста *Miscanthus x giganteus* от времени произрастания с учетом концентрации тяжелых металлов в почве

Эмпирическое уравнение теоретической кривой динамики роста на незагрязненной почве:

$$y = -0.0071x^2 + 605.38x - 1E + 07 \quad 13$$

При этом величина достоверности аппроксимации составляет: $R^2 = 0.9849$

Эмпирическое уравнение теоретической кривой динамики роста растений на загрязненной почве со средним уровнем загрязнения ($Z_c 20,0 \pm 3,1$ мг/кг)

$$y = -0.0072x^2 + 613.17x - 1E + 07 \quad 14$$

При этом величина достоверности аппроксимации составляет: $R^2 = 0.9845$

Эмпирическое уравнение теоретической кривой динамики роста на загрязненной почве с высоким уровнем загрязнения ($Z_c 165,4 \pm 17,1$ мг/кг).

$$y = -0.0045x^2 + 380.45x - 8E + 06 \quad 15$$

При этом величина достоверности аппроксимации составляет: $R^2 = 0.9614$

Таким образом, получено уравнение кинетики роста и создана теоретическая кривая динамики развития нового фиторемедианта *Miscanthus x giganteus* с учетом концентрации тяжелых металлов в почве.

Литература

- 1 Водопьянов В.В. Математическое моделирование динамики роста грибных пропагул в почве, загрязненной нефтью // Вестник УГАТУ – 2007. – Т. 9. № 7 (25). – С. 79-82.
- 2 Кузнецов В.И., Козлов Н.И., Хомяков П.М. Математическое моделирование эволюции леса для целей управления лесным хозяйством – М.: Ленад. 2005. 232 с.
- 3 Urban H.J. Modeling growth of different developmental stages in bivalves // Mar. Ecol. Prog. Ser. – 2002. – Vol. 238. – P. 109-114.
- 4 Колпак Е.П., Столбовая М.В. Математическая модель кинетики роста растений // Журнал научных публикаций аспирантов и докторантов. Математика. – 2013. – № 12. – Р. 29-32.
- 5 Отчет проекта 0451/ГФ4 «Разработка технологии улучшения загрязненных тяжелыми металлами и пестицидами земель с использованием растения мискантуса гигантского (*miscanthus x giganteus*) – нового высокоэффективного фиторемедианта». 2016. – 85 с.
- 6 Горбунова Е.А., Колпак Е.П. Математические модели одиночной популяции // Вест. С.-Петерб. ун-та. Прикладная математика, информатика и процессы управления. – 2012. – Вып. 4, Сер. 10 – С.18-30.

ПРИМЕР КОМПАНИОН-ТЕОРИИ С ДВУМЯ НЕ ЭЛЕМЕНТАРНО ЭКВИВАЛЕНТНЫМИ ЭКЗИСТЕНЦИАЛЬНО ЗАМКНУТЫМИ СЧЁТНЫМИ МОДЕЛЯМИ

Нуртазин А.Т.

e-mail: abyznurtazin@mail.ru

Институт информационных и вычислительных технологий КН МОН РК,
Казахстан

Аннотация. Строится компаньон-теория T^c , имеющая в точности две счётные не элементарно эквивалентные экзистенциально замкнутые модели.

В теории экзистенциальной замкнутости значительную роль играют результаты о числе попарно не элементарно эквивалентных экзистенциально замкнутых моделей в ряде классических теорий. В [5] найдены условия, когда данный компаньон-класс содержит лишь одну счётную экзистенциально замкнутую структуру. Там же найдены компаньон-классы, содержащие любое конечное или счётное число попарно неизоморфных элементарно эквивалентных счётных экзистенциально замкнутых моделей. В связи с этим для дальнейшего развития теории важным представляется вопрос о возможном числе попарно не элементарно эквивалентных экзистенциально замкнутых моделей произвольных компаньон-теорий. В этой статье будет построена компаньон-теория T^c , имеющая в точности две не элементарно эквивалентные счётные экзистенциально замкнутые модели.

Для задания требуемой теории мы вначале построим её простую и минимальную модель. Здесь достаточно неожиданным явился тот факт, что построенная нами структура M оказалась простой и минимальной в своём компаньон-классе $C(M)$. Обычно выделение экзистенциально замкнутых структур сопровождается преодолением больших трудностей. Но рассматриваемом нами случае эти вопросы решаются достаточно легко.

Структура.

$$M = (M; \Sigma) = (M; E^{(1)}, W^{(1)}, P_1^{(1)}, \dots, P_m^{(1)}, \dots, L^{(3)}, =).$$

Основное множество.

$$M = A \cup B, \quad A \cap B = \emptyset, \quad |A| = |B| = \omega.$$

При этом A называем множеством элементов, а B -- множеством свидетелей.

В свою очередь множества элементов и свидетелей разбиваются в объединения конечных подмножеств:

$$A = A_1 \cup \dots \cup A_m \cup \dots, \quad B = B_1 \cup \dots \cup B_m \cup \dots$$

Где для любого натурального $m > 0$

$$A_m = \{a_0^m, \dots, a_{m-1}^m\} \quad \text{и} \quad B_m = \{b_{00}^m, \dots, b_{m-1 \ m-1}^m\}$$

Базисные отношения.

$$E(M) = A, \quad W(M) = B;$$

Для любого $m > 0$

$$P_m(M) = A_m \cup B_m = M_m;$$

$$L(M) = \{(a_i^m, a_j^m, b_{ij}^m) : i \leq j < m, m \in \omega\}.$$

Этим структура M задана полностью.

Для кортежа a из произвольной реляционной структуры $A = (A; \Sigma)$ и конечной подсигнатуры $\sigma \subset \Sigma$ для кортежа переменных x той же длины, что и a ,

формула $D_a^\sigma(x)$ является конъюнкцией всех атомных и отрицаний атомных σ -формул от x , выполняющихся на a , и называется σ -диаграммой a . Основным и хорошо известным свойством диаграмм является то, что $B \models D_a^\sigma(b)$ эквивалентно тому, что покоординатное отображение из a в b является σ -изоморфизмом.

В структуре M на множестве A формула $x \leq y \equiv \exists z E(x, y, z)$ задаёт частичный порядок, состоящий из непересекающихся цепей: $a_0^1, a_0^2 < a_1^2, \dots, a_0^m < \dots < a_{m-1}^m, \dots$ соответственно длин $1, 2, \dots, m, \dots$. Для простоты дальнейших рассуждений

для каждого натурального $m > 0$ введём следующие обозначения: $a^m = (a_0^m, \dots, a_{m-1}^m)$ и $b^m = (b_{00}^m, b_{01}^m, \dots, b_{m-1m-1}^m)$. Тогда $c = a^1 b^1 \dots a^m b^m$. Также положим $\sigma = (E, W, P_0, \dots, P_m, L, =)$. В структуре M выполняется экзистенциальное предложение $\exists z Dc^\sigma(z)$. С другой стороны, если бы для $f = d^1 e^1 \dots d^m e^m$ выполнялось бы $M \models Dc^\sigma(f)$, то в M элементы d_0^1 и e_{00}^1 удовлетворяли бы предикату P_1 и выполнялось бы $L(d_0^1, d_0^1, e_{00}^1)$. Но в структуре M этим соотношениям удовлетворяют только элементы a_0^1 и b_{00}^1 . Далее, для любого $n \leq m$ элементы $d_0^n, \dots, d_{n-1}^n$ и $e_{00}^n, e_{01}^n, \dots, e_{n-1n-1}^n$ различны и удовлетворяют предикату P_n . И выполнялись бы соотношения $L(d_0^n, d_0^n, e_{00}^n), L(d_0^n, d_1^n, e_{01}^n), \dots, L(d_{n-2}^n, d_{n-1}^n, e_{n-2n-1}^n), L(d_{n-1}^n, d_{n-1}^n, e_{n-1n-1}^n)$. Но в структуре M такими свойствами обладают лишь кортежи a^m и b^m . Этим доказано, что

1°. В структуре M вместе с экзистенциальным $\exists z Dc^\sigma(z)$ выполняется универсальное предложение $\forall z z^1 [Dc^\sigma(z) \& Dc^\sigma(z^1) \rightarrow z = z^1]$

Теперь мы можем доказать и исследовать вложимость структуры M в любой её компаньон M' . Так как в M должны выполняться экзистенциальное и универсальное предложения из 1°, то существует единственное вложение f_m структуры $M \mid M_1 \cup \dots \cup M_m \mid \sigma$ в структуру M' . При этом при $m < n$ вложение f_n является единственным расширением вложения f_m . Но тогда объединение $f_m = \cup \{f_m : m \sqsubseteq \omega\}$ является единственным изоморфным вложением структуры M в M' . Таким образом можно считать, что выполняется включение $M < M'$. Если c^0 кортеж из M и b' кортеж из $M' - M$ и выполняется $M' \models \varphi(c^0; d')$, то для некоторого m c^0 является подкортежом $c = c^m$ и формула $\varphi(z; t')$ является σ -формулой. Тогда из определения компаньон-структуры следует, что формула $Dc^\sigma(z; t)$ выполняется на некотором кортеже вида $c^0 d$ для d из M . Но формула $Dc^\sigma(z)$ является логическим следствием формулы $Dc^\sigma(z; t)$ и из $M \models Dc^\sigma(c^0; d)$ следует $c^0 = c^m$. В свою очередь формула $\varphi(z; t)$ также является логическим следствием формулы $Dc^\sigma(z; t)$ и, следовательно, выполняется $M \models \varphi(c^0; d)$. То-есть структура M экзистенциально замкнута в расширении M' . Таким образом, нами доказано, что

2°. Структура M проста, минимальна и экзистенциально замкнута в своём компаньон-классе $C(M)$.

Теперь поймём как должно выглядеть собственное счётное экзистенциально замкнутое расширение N структуры M . Пусть d произвольный элемент из $N - M$. В N так же, как и в её компаньоне M , должно выполняться предложение $\forall t [E(t) \vee W(t)]$. То есть d должен оказаться либо элементом, либо свидетелем.

Пусть d свидетель. Тогда, ввиду экзистенциальной замкнутости, в структуре N должно выполняться истинное в M $\forall \exists$ -предложение $\forall t \exists x y [W(t) \rightarrow L(x, y, t)]$. То-есть в N найдутся a и b такие, что $M \models E(a, b, d)$. Заметим, что если бы хотя бы один из них a оказался бы в M , то для некоторого m выполнялось бы $M \models P_m(a)$ и, ввиду $M \models \forall x y t [P_m(x) \& E(x, y, t) \rightarrow P_m(y) \& P_m(t)]$, оказалось бы $d \in M$. Таким образом, нами доказано, что в любом случае в $N - M$ имеется хотя бы один элемент a . Теперь покажем, что формула $x \leq y$, как и в M , определяет частичный порядок на элементах из $E(N)$. Действительно в $(E(M); \leq)$ выполняются аксиомы частичного порядка, которые в M задаются Σ - $\forall \exists$ -предложениями $\forall x \exists y L(x, x, y), \forall x y \exists z z' [L(x, y, z) \& L(y, x, z') \rightarrow x = y \& z = z']$ и $\forall x y z u v \exists w [L(x, y, u) \& L(y, z, v) \rightarrow L(x, z, w)]$. Обозначим (a) подмножество элементов из $E(N)$, сравнимых

с a . Во первых покажем, что (a) линейно упорядочено. Если выполняется $b \leq a$ и $a \leq c$, то, ввиду транзитивности $\leq$, выполняется $b \leq c$. Теперь предположим, что в N выполняется $a \leq b$ и $a \leq c$. Тогда в (a) найдутся d и e с $N \models L(a,b,d) \& L(a,c,e)$. Но в M для любых a, b и c выполняется $a \leq b \& a \leq c \rightarrow [b \leq c \vee c \leq b]$. То-есть в M и, следовательно, в N выполняется $\forall \exists$ -предложение $\forall x y z u v \exists w [L(x,y,u) \& L(x,z,v) \rightarrow [L(y,z,w) \vee L(z,y,w)]]$. Следовательно в N выполняется $b \leq c$ или $c \leq b$. Случай $b \leq a$ и $c \leq a$ симметричен предыдущему и рассматривается аналогичным способом. Итак, нами доказано, что (a) линейно упорядочено формульным отношением $\leq$.

Теперь методом от противного покажем, что (a) не имеет наибольшего элемента. При этом без ограничения общности можно считать, что сам элемент a является наибольшим в (a) . В этом случае расширим N до N' элементом b , большим a . Одновременно также расширим и множество свидетелей $W(N)$, добавив к нему для каждого c из $(a) \cup \{b\}$ свидетеля d_c с $N' \models L(c, b, d_c)$. Тогда выполняется $N' \models \exists yz [L(a, y, z) \& y \leq a]$ и не выполняется $N' \models \exists yz [L(a, y, z) \& y \leq a]$. Что противоречит предположению об экзистенциальной замкнутости структуры N . Аналогично доказывается и то, что (a) не содержит наименьшего элемента.

Наконец проверим, что порядок $\leq$ на (a) плотен. Действительно, пусть в (a) нашлась пара элементов a_0 и c с условием $a_0 \leq c$. Тогда не выполнялось бы $N \models \exists yuv [L(a_0, y, u) \& L(y, c, v) \& a \leq y \& y \leq c]$. Теперь построим компаньон-расширение N' структуры N , в котором выполняется $\exists yuv [L(a_0, y, u) \& L(y, c, v) \& a \leq y \& y \leq c]$. Для этого для $b \notin N$ положим $E(N') = E(N) \cup \{b\}$, $W(N') = W(N) \cup \{bd : d \leq a_0\} \cup \{bb\} \cup \{be : c \leq e\}$ и $L(N') = L(N) \cup \{(d, b, bd) : d \leq a_0\} \cup \{(b, b, bb)\} \cup \{(b, e, be) : c \leq e\}$. Тогда непосредственно из определения предиката L следует, что в компаньон-расширении N' выполняется формула $\exists yuv [L(a_0, y, u) \& L(y, c, v) \& a \leq y \& y \leq c]$, ложная в N . То-есть наше предположение об экзистенциальной замкнутости N неверно.

Итак к настоящему моменту нами доказано, что в собственном счётном экзистенциально замкнутом компаньон-расширении N структуры M подмножество элементов помимо конечных цепей, выделенных предикатами P_m , $m \in \omega$, должен содержать бесконечные, плотные линейные порядки без концевых элементов вида $(a) ; \leq$. Покажем, что в N число таких бесконечных плотных линейных порядков равно единице. Действительно, предположим, что в N имеются несравнимые друг с другом элементы a и b , для которых плотные бесконечные линейные порядки $(a) ; \leq$ и $(b) ; \leq$ не пересекаются. Тогда в структуре N не выполняется экзистенциальная формула $\exists z L(a, b, z)$. Построим компаньон-расширение N' структуры N , положив для $e \notin N$ $E(N') = E(N)$, $W(N') = W(N) \cup \{ecd : c \sqsubseteq (a), d \sqsubseteq (b)\}$ и $L(N') = L(N) \cup \{(c, d, ecd) : c \sqsubseteq (a)\}$. Тогда в компаньон-расширении N' структуры N в частности выполняется экзистенциальная формула $\exists z L(a, b, z)$, не выполняющаяся в N . Это противоречит предположению об экзистенциальной замкнутости структуры N и доказывает, что

3°. Структура M и её расширение N , в котором содержится в точности одно счётное плотно и линейно упорядоченное подмножество элементов вида (a) , составляют весь подкласс счётных экзистенциально замкнутых структур в компаньон-классе $S(M)$.

Литература

1. Cohen P.J., Set Theory and the Continuum Hypothesis, N.-Y., Benjamin, 1966.
2. Fraisse R., Sur quelques classifications des systemes de relations, Publ. scient. De l'univ. d'Algers, 1955, A1, 35-182.
3. Macintyre A., On algebraically closed groups, Ann. Math., 1972, 96, 53 - 97.
4. Macintyre A., Omitting quantifier-free types in generic structures, Journ. of Symbolic Logic, 1972, 37, 512 - 520.
5. Nurtazin A.T., Countable infinite existentially closed models of universally axiomatizable theories, Siberian Advances in Mathematics, 2016, 26, 99-125.
6. Robinson A., On the Metamathematics of Algebra, Amsterdam: North -- Holland, 1951.
7. Robinson A., Infinite forcing in model theory, Proceedings of the second Scandinavian Logic Symposium, Amsterdam: North -- Holland, 1971, 317 - 340.

АВТОМАТИЗАЦИЯ ПРЕДСТАВЛЕНИЯ ТЕКСТА В ВИДЕ ПРАВИЛ ЛОГИЧЕСКОГО ПРОГРАММИРОВАНИЯ

Нуртазин А.Т., Хисамиев З.Г.
AbyzNurtazin@mail.ru, KhisamievZ@mail.ru

*Институт информационных и вычислительных технологий КН МОН РК,
Казахстан*

Аннотация. Целью исследования является развитие алгоритма автоматического представления текста естественного языка в виде теории логического программирования, для последующего автоматического извлечения как обоснованных ответов на вопросы по этому тексту, так и извлечения логических следствий из текста и сопутствующей области знаний, к которой относится текст. В настоящей работе алгоритм, представленный в предыдущих работах авторов, усовершенствован автоматизацией введения переменных в правила логического программирования представляющих текст. Так как наличие переменных – необходимая часть построения теории логического программирования. Работа алгоритма проиллюстрирована примерами из текста Конституции Республики Казахстан.

1. Тексты и преобразование П

Рассматриваются тексты определенного вида. Предложение τ текста $\mathcal{T}$ имеет один из следующих типов: 1. Предложение τ выражает одно действие или конъюнкцию действий, разделенных знаками препинаний или союзами, которое можно рассматривать как одно сложное действие δ . Действие, выраженное явно или неявно сказуемым или сказуемыми, имеет агента т.е. исполнителя действия, или конъюнкцию агентов, впрочем, конъюнкция агентов с одним конъюнктивным членом означает единственного агента, этой экономией слов мы будем иногда пользоваться. Агент выражается явно или неявно подлежащим. Обозначим агента предложения τ через α . Далее, в τ имеется результат действия или конъюнкция результатов, обозначим его ρ . Результат может выражаться дополнениями, определениями или

дополнительным предложением τ' которое также считается предложением из $\mathcal{T}$ и имеет тип 1. Агент α' такого τ' называется *объектом* τ , более подробно можно сказать, что α' объект на которое направлено действие τ , при этом α является действующим агентом в τ' .

Определим

$\Pi(\tau) = [\text{действие}([\delta]), \text{агент}([\alpha]), \text{результат}([\rho]), \text{время}([v]), \text{каталог}([\mu])]$, последние два аргумента введены для указания времени действия и каталогизации предложений, эти аргументы технические и будут опущены в алгоритме и примере ; 2. Предложение τ является конъюнкцией предложений типа 1; 3. Предложение τ является условным предложением с одним заключением (консеквентом) имеющим тип 1 и посылкой (антецедентом), которая является конъюнкцией предложений типа 1, напомним что конъюнкция может иметь только один конъюнктивный член.

Предложение текста $\mathcal{T}$, может состоять из нескольких обычных предложения, связанных анафорическими местоимениями или общим агентом или общим действием как одно предложение. Например, для текста $\mathcal{T}$ Конституции Республики Казахстан, отдельный пункт статьи рассматриваем как одно предложение типа 1 или 2 или 3.

2 Алгоритм создания $\mathfrak{F}$ -теории текста $\mathcal{T}$

Рассматриваемый алгоритм является развитием подхода изложенного в [1,2,3].

В сигнатуре имеется единственный одноместный предикат Φ .

Пусть $\tau \in \mathcal{T}$ и имеет тип 1.

1. Отнесем $\Phi(\Pi(\tau))$ к $\mathfrak{F}$ -теории текста $\mathcal{T}$ которую обозначаем $\mathfrak{F}(\mathcal{T})$.

Формулу $\Phi(\Pi(\tau))$ называем $\mathfrak{F}$ -правилом текста $\mathcal{T}$;

2. Введение переменных. Пусть

$\Phi([\text{действие}([\delta]), \text{агент}([\alpha]), \text{результат}([\rho])]) \in \mathfrak{F}'_0(\mathcal{T})$ и агент α содержит имя κ некоторого класса и нет переменной расположенной непосредственно за κ в α .

Отнесем $\mathfrak{F}$ -правило $\Phi([\text{действие}([\delta]), \text{агент}([\dots \kappa X \dots]), \text{результат}([\rho])])$ к $\mathfrak{F}(\mathcal{T})$, где $[\alpha] = [\dots \kappa \dots]$ и X – любая переменная не входящая в $\Phi([\text{действие}([\delta]), \text{агент}([\dots \kappa X \dots]), \text{результат}([\rho])])$.

Аналогично, когда класс κ входит в ρ , относим соответствующие $\mathfrak{F}$ -правило с переменной к $\mathfrak{F}(\mathcal{T})$.

3. Пусть $\Phi([\text{действие}([\delta]), \text{агент}([\alpha]), \text{результат}([\rho])]) \in \mathfrak{F}'_0(\mathcal{T})$ и α есть конъюнкция агентов $\alpha_1, \dots, \alpha_n$ тогда, для некоторых из действий таких как «есть», «является», «обладает» и т.д., но не действий которые указывают на совместное выполнение результата ρ . Отнесем к $\mathfrak{F}(\mathcal{T})$ следующее $\mathfrak{F}$ -правило

$$\Phi([\text{действие}([\delta]), \text{агент}([\alpha]), \text{результат}([\rho])]) \leftarrow \bigwedge_i \Phi([\text{действие}([\delta]), \text{агент}([\alpha_i]), \text{результат}([\rho])]).$$

4. Пусть $\Phi([\text{действие}([\delta]), \text{агент}([\alpha]), \text{результат}([\rho])]) \in \mathfrak{F}'_0(\mathcal{T})$ и ρ есть конъюнкция результатов $\rho_1, \dots, \rho_n$. Отнесем к $\mathfrak{F}(\mathcal{T})$ следующее $\mathfrak{F}$ -правило

$$\Phi([\text{действие}([\delta]), \text{агент}([\alpha]), \text{результат}([\rho])) \leftarrow \\ \&_{\substack{i \\ \Phi([\text{действие}([\delta]), \text{агент}([\alpha]), \text{результат}([\rho_i])])}}.$$

5. Пусть $\Phi([\text{действие}([\delta]), \text{агент}([\alpha]), \text{результат}([\rho])) \in \mathfrak{P}'_0(\mathfrak{T})$ и в ρ имеется агент α' . Отнесем к $\mathfrak{P}_0(\mathfrak{T})$ следующее $\mathfrak{P}$ -правило

$$\Phi([\text{действие}([\delta]), \text{агент}([\alpha]), \text{результат}([\dots\alpha'\dots])) \leftarrow \\ \Phi([\text{действие}([\delta]), \text{агент}([\alpha]), \text{результат}([\dots\text{объект}([\alpha'])\dots])).$$

6. Пусть $\tau \in \mathfrak{T}$ и имеет тип 2, т.е. τ есть конъюнкция предложений $\tau_1, \dots, \tau_n$ типа 1. Отнесем к $\mathfrak{P}_0(\mathfrak{T})$ следующие $\mathfrak{P}$ -правила $\Phi(\Pi(\tau)), \Phi(\Pi(\tau)) \leftarrow \&_{\substack{i \\ \Phi(\Pi(\tau_i))}}$.

7. Пусть $\tau \in \mathfrak{T}$ и имеет тип 3, т.е. τ есть условное предложение с консеквентом τ_0 конъюнкцией антецедентов $\tau_1, \dots, \tau_n$ типа 1. Отнесем к $\mathfrak{P}_0(\mathfrak{T})$ следующие $\mathfrak{P}$ -правила $\Phi(\Pi(\tau)), \Phi(\Pi(\tau)) \leftarrow \&_{\substack{i \\ \Phi(\Pi(\tau_i))}}$.

8. Введение переменных в условные $\mathfrak{P}$ -правила. Новая переменная для класса κ вводится $\mathfrak{P}$ -правило как в пункте 2 этого алгоритма если κ входит в консеквент этого правила. Полученное $\mathfrak{P}$ -правило относится к $\mathfrak{P}'_0(\mathfrak{T})$.

3. Пример работы алгоритма

3.1 $\mathfrak{P}$ -теория Конституции РК

Рассмотрим применение алгоритма к тексту $\mathfrak{T}$ Конституции Республики Казахстан [4].

Статья КРК.1.1.1. «Республика Казахстан утверждает себя демократическим, светским, правовым и социальным государством, высшими ценностями которого являются человек, его жизнь, права и свободы».

В результате преобразования Π и применения пункта 1 алгоритма получается $\mathfrak{P}$ -правило $\Phi(\Pi(\text{КРК.1.1.1}))$

$$\Phi([\text{[[действие ([утверждает]), агент ([«РК»]),} \\ \text{результат ([объект([себя]), демократическим«}, \\ \text{светским «}, \\ \text{правовым и} \\ \text{социальным государством «}, \\ \text{высшими ценностями которого являются человек «}, \\ \text{права и свободы»]],} \\ \text{время ([начало, «30.8.1995», действующая, «17.02.2017»]),} \\ \text{каталог ([«КРК.1.1.1»])}]]).$$

В этом $\mathfrak{P}$ -правиле, результат есть конъюнкция 5 результатов, поэтому автоматически, по пункту 3 преобразования Π , строится конъюнкция $\Phi(\Pi(\text{КРК.1.1.1})) \leftarrow A_1 \& A_2 \& A_3 \& A_4 \& A_5$ 5 антецедентов которых – A_1, A_2, A_3, A_4, A_5 приведены ниже. Автоматически анафорическое местоимения «себя» и «которого» заменены на их значение «РК». Напомним, что аргумент «время» необходим для отражения временных интервалов в которых законы являются действительными.

Аргумент «каталог» нужен для объяснения обоснования выводов следствий из текста. Эти два вида важных аргумента носят технический характер и в дальнейших описаниях $\mathfrak{F}$ -правил они опускаются.

- $\Phi([\text{действие}([\text{утверждает}]), \text{агент} ([\langle \text{РК} \rangle]), \text{результат} ([\text{объект}([\langle \text{РК} \rangle]), \text{демократическим государством}])]) ;$ (A₁)
 $\Phi([\text{действие}([\text{утверждает}]), \text{агент} ([\langle \text{РК} \rangle]), \text{результат} ([\text{объект}([\langle \text{РК} \rangle]), \text{светским государством}])]) ;$ (A₂)
 $\Phi([\text{действие}([\text{утверждает}]), \text{агент} ([\langle \text{РК} \rangle]), \text{результат} ([\text{объект}([\langle \text{РК} \rangle]), \text{правовым государством}])]) ;$ (A₃)
 $\Phi([\text{действие}([\text{утверждает}]), \text{агент} ([\langle \text{РК} \rangle]), \text{результат} ([\text{объект}([\langle \text{РК} \rangle]), \text{социальным государством}])]) ;$ (A₄)
 $\Phi([\text{действие}([\text{утверждает}]), \text{агент} ([\langle \text{РК} \rangle]), \text{результат} ([\text{объект}([\text{человек} \langle , \rangle \text{его жизнь права и свободы}]), \text{являются высшими ценностями} \langle \text{РК} \rangle))]) ;$ (A₅)

Правила A₁, A₂, A₃, A₄ являются $\mathfrak{F}$ -правилами без объекта, а A₅ содержит в структуре результат – объект действия. Рассмотрим применения алгоритма для построения $\mathfrak{F}$ -правил необходимых для семантико-синтаксического представлений структур A₄.

По пункту 7 преобразования алгоритма добавляется $\mathfrak{F}$ -правило

$$\Phi(\Pi(K.1.1.1)) \leftarrow A_1 \& A_2 \& A_3 \& A_4 \& A_5.$$

Мы строим систему $\mathfrak{F}$ -правил являющихся естественным логическим представлением текста $\mathfrak{T}$, поэтому для логического вывода в этой системе $\Phi(\Pi(K.1.1.1))$ достаточно вывести A_i, i=1,...,5.

Приведем автоматизированное построение набора $\mathfrak{F}$ -правил, раскрывающих семантико-синтаксическое и дедуктивное значение $\mathfrak{F}$ -правила A₄. В [1,2,3], такого рода построение рассмотрено для A₁, A₂ и A₃.

3.2 $\mathfrak{F}'$ -правила семантико-синтаксического представления A₄

Обратимся к $\mathfrak{F}'$ -правилу A₄ : [*действие*([*утверждает*]), *агент* ([*РК*]), *результат* ([*социальное государство* *РК*])]. В тексте $\mathfrak{T}$ нет определения социального государства, но в области знаний «юриспруденция», к которой относится текст, есть следующие определение (Википедия). *Социальное государство* - государство, политика которого направлена на перераспределение материальных благ в соответствии с принципом социальной справедливости ради достижения каждым гражданином достойного уровня жизни, сглаживания социальных различий и помощи нуждающимся. Представим это определение социального государства в виде $\mathfrak{F}'$ -правила (S).
 $\Phi([\text{действие}([\text{является}]), \text{агент} ([\text{государство X}], \text{результат} ([\text{социальным государством X}])])$ (S)

←

$\Phi([\text{действие}([направлена \text{ на}]), \text{агент} ([\text{политика которого(государства X)]),$
(S_1)

результат (перераспределение материальных благ в соответствии с принципом социальной справедливости ради достижения каждым гражданином достойного уровня жизни в государстве X)])

&

$\Phi([\text{действие}([направлена \text{ на}]), \text{агент} ([\text{политика которого(государства X)]),$
(S_2)

результат (перераспределение материальных благ в соответствии с принципом социальной справедливости ради сглаживания социальных различий в государстве X)])

&

$\Phi([\text{действие}([направлена \text{ на}]), \text{агент}([\text{политика которого (государства X)]),$ (S_3)
 результат (перераспределение материальных благ в соответствии с принципом социальной справедливости ради помощи нуждающимся в государстве X)])

Результат является конъюнкцией результатов поэтому после преобразования результата определения (S) в антецеденте три конъюнктивных члена. В правиле важна переменная X , так как это правило будет использоваться для вывода о социальном государстве «Казахстан» и не важна переменная и связывающий ее квантор для выражения «каждый гражданин», в первом конъюнктивном члене, так как имена граждан не будут использоваться в выводах о социальности государства. По той же причине во втором и третьем конъюнктивных членах не вводятся переменные для подразумеваемых граждан в выражениях «сглаживания социальных различий в государстве X » и «помощи нуждающимся в государстве X » .

Для вывода утверждения о том что «Казахстан» является социальным государством, следует указать все статьи на которые опираются $\mathfrak{P}_0'$ –правила (S_{1X}^{PK}), (S_{2X}^{PK}), (S_{3X}^{PK}), где S_{iX}^{PK} – результат подстановки в (S_i) вместо переменной X константы «РК». В рамках Конституции $\mathfrak{P}_0'$ –правила этих статей и будут антецедентами каждого из правил в которых консеквентами являются (S_{1X}^{PK}), (S_{2X}^{PK}), (S_{3X}^{PK}). Статьи Конституции поддерживающие утверждение о направленности деятельности государства на «перераспределение материальных благ в соответствии с принципом социальной справедливости ради достижения каждым гражданином достойного уровня жизни в государстве «РК» служат основаниями для антецедента следующего правила с консеквентом (S_1).

$\Phi([\text{действие}([направлена \text{ на}]), \text{агент} ([\text{политика которого(государства «РК»)]),$
(S_1) результат (перераспределение материальных благ в соответствии с принципом социальной справедливости ради достижения каждым гражданином достойного уровня жизни в государстве «РК»)])

←

$\Phi([\text{действие}([поддерживают]),$
 $\text{агент} ([\text{Статьи К.2.24.2, К.2.24.4 , К.2.25.1, К.2.25.2, К.2.27.2, К.2.28.1, К.2.29.1, К.2.29.2, К.2.30.1, К.2.30.2, К.2.31.1, К.2.31.2 «РК»}],$
 результат (утверждение о «перераспределение материальных благ в соответствии с принципом социальной справедливости ради достижения каждым гражданином достойного уровня жизни в государстве «РК» »)])

Сказуемое «поддерживают» позволяет выполнить преобразование этого правила в эквивалентное правило импликацию с 12 конъюнкциям в антеценденте.

Литература

1 Нуртазин А.Т., Хисамиев З.Г. Синтаксическое и семантическое представление текстов // Труды XI междунар. школы-семинара «Проблемы оптимизации сложных систем». – Чолпон-Ата, 2015. – Ч. II. – С.494-497.

2 Nurtazin A., Khisamiev Z. Automatic extraction of corollaries from semantic structure of text // Open engineering: Special Issue on “Mathematical modeling in applied sciences”. – 2016.

3 Нуртазин А.Т., Хисамиев З.Г. Автоматическое извлечение следствий из семантической структуры текста // Матер. междунар. науч. конф. «Информатика и математика», посв. 25-летию Независимости Республики Казахстан и 25-летию Института информационных и вычислительных технологий. – Алматы, 2016. – Ч. II. – С.75 – 83.

4 Конституция Республики Казахстан
//[http://www.akorda.kz/ru/official_documents/ constitution](http://www.akorda.kz/ru/official_documents/constitution) : 14.10.2016.

АЛГОРИТМ ШИФРОВАНИЯ НА БАЗЕ КИТАЙСКОЙ ТЕОРЕМЫ ОБ ОСТАТКАХ

Нысанбаева С.Е., Капалова Н.А., Дюсенбаев Д.С., Дузбаев Т.Т.

e-mail: sultasha1@mail.ru, kapalova@ipic.kz, dimash_dds@mail.ru,
talgat.duzbaev@mail.ru

*Институт информационных и вычислительных технологий КН МОН РК,
Казахстан*

Аннотация. В данной работе рассматривается алгоритм шифрования, разработанный на основе китайской теоремы об остатках и непозиционной полиномиальной системе счисления (НПСС). В этом алгоритме блок открытого текста длины N бит в процессе преобразования в НПСС не интерпретируется как последовательность остатков, а представляется в виде остатков от деления на рабочие основания НПСС.

Пусть $p_1(x), p_2(x), \dots, p_s(x)$ – неприводимые многочлены с двоичными коэффициентами, используемые в качестве рабочего диапазона, т.е. они являются рабочими основаниями НПСС. Это означает, что многочлен $P(x) = p_1(x) \cdot p_2(x) \cdots p_s(x)$ степени $m = \sum_{i=1}^s m_i$ определяет основной рабочий диапазон НПСС. В НПСС любой многочлен степени меньше m может быть единственным образом представлен в виде его вычетов по модулям рабочих оснований $p_1(x), p_2(x), \dots, p_s(x)$ соответственно [1-4].

Описание алгоритма шифрования. Блок открытого сообщения длины N бит представляется в НПСС как некоторый многочлен $T(x)$ с двоичными коэффициентами.

Тогда в НПСС этот многочлен $T(x)$ может быть представлен в непозиционном виде, т.е. в виде последовательности остатков или вычетов, которые получаются при делении этого многочлена $T(x)$ на рабочие основания $p_1(x), p_2(x), \dots, p_s(x)$. По правилам системы счисления в остаточных классах получение вычетов осуществляется следующим образом:

$$T(x) \equiv \alpha_i(x) \pmod{p_i(x)}, \text{ где } i=1, 2, \dots, S. \quad (1)$$

Тогда, $T(x)$ в непозиционном виде записывается как $T(x) = (\alpha_1(x), \alpha_2(x), \dots, \alpha_s(x))$.

Восстановление многочлена (1) в позиционном виде производится по следующей формуле:

$$F(x) = \sum_{i=1}^S \alpha_i(x) B_i(x), \text{ где } B_i(x) = \frac{p_s(x)}{p_i(x)} M_i(x) \equiv 1 \pmod{p_i(x)}. \quad (2)$$

Для проведения этих вычислений необходимо определить базисы $B_i(x)$ в НПСС по формуле (2). Для этого нужно вычислить многочлены:

$$\delta_i(x) \equiv \frac{p_s(x)}{p_i(x)} \pmod{p_i(x)} \quad (3)$$

и инверсные к ним полиномы: $\delta_i^{-1}(x)$: $\delta_i^{-1}(x) \delta_i(x) \equiv 1 \pmod{p_i(x)}$.

Тогда базисы находятся по формуле:

$$B_i(x) = \delta_i^{-1}(x) \frac{p_s(x)}{p_i(x)}, \quad (4)$$

которые также являются секретными параметрами алгоритма.

Используемая ключевая последовательность длины N бит в НПСС интерпретируется как последовательность остатков $(\beta_1(x), \beta_2(x), \dots, \beta_s(x))$, полученных при делении некоторого многочлена $G(x)$ на рабочие основания $p_1(x), p_2(x), \dots, p_s(x)$:

$$G(x) = (\beta_1(x), \beta_2(x), \dots, \beta_s(x)),$$

где $G(x) \equiv \beta_i(x) \pmod{p_i(x)}, i = \overline{1, S}$. Остатки $(\beta_1(x), \beta_2(x), \dots, \beta_s(x))$ выбираются таким образом, что первым l_1 битам ключа ставятся в соответствие двоичные коэффициенты остатка $\beta_1(x)$, следующим l_2 битам – двоичные коэффициенты остатка $\beta_2(x)$ и так далее, последним l_s двоичным разрядам ставятся в соответствие двоичные коэффициенты вычета $\beta_s(x)$.

По известному ключу $G(x)$ для каждого значения $\beta_i(x)$ производится вычисление обратного (или инверсного) многочлена $\beta_i^{-1}(x)$ из условия выполнения следующего сравнения:

$$\beta_i(x) \times \beta_i^{-1}(x) \equiv 1 \pmod{p_i(x)}, i = \overline{1, S}.$$

В результате получается многочлен $G^{-1}(x) = (\beta_1^{-1}(x), \beta_2^{-1}(x), \dots, \beta_s^{-1}(x))$, инверсный к многочлену $G(x)$.

Далее производится зашифрование блока открытого текста. Шифртекст $H(x)$ получается в результате выполнения некоторой функции $H(x) = (F(x), G(x), P(x))$:

$$H(x) \equiv \omega_i(x)(\text{mod } p_i(x)), \text{ где } i=1,2,\dots,S$$

или

$$H(x) = (\omega_1(x), \omega_2(x), \dots, \omega_S(x)).$$

Шифрование производится по следующей формуле:

$$\alpha_i(x)\beta_i(x) \equiv \omega_i(x)(\text{mod } p_i(x))$$

или

$$T(x) \otimes G(x) \equiv H(x)(\text{mod } P(x)),$$

где $T(x) = (\alpha_1(x), \alpha_2(x), \dots, \alpha_S(x))$ - открытый текст, $G(x) = (\beta_1(x), \beta_2(x), \dots, \beta_S(x))$ - ключ, $P(x) = (p_1(x), p_2(x), \dots, p_S(x))$ - рабочие основания.

Перевод шифртекста $H(x)$ в позиционный вид производится по формуле:

$$H(x) = \sum_{i=1}^S \omega_i(x) B_i(x)(\text{mod } P(x)). \quad (5)$$

Расшифрование шифртекста осуществляется по следующему выражению:

$$\omega_i(x)\beta_1^{-1}(x) \equiv \alpha_i(x)(\text{mod } p_i(x)) \quad ; \quad (6)$$

$$H(x) \otimes G^{-1}(x) \equiv F(x)(\text{mod } P(x)) \quad ; \quad (7)$$

где $F(x) = (\alpha_1(x), \alpha_2(x), \dots, \alpha_S(x))$,
 $G^{-1}(x) = (\beta_1^{-1}(x), \beta_2^{-1}(x), \dots, \beta_S^{-1}(x))$ - инверсный ключ,
 $P(x) = (p_1(x), p_2(x), \dots, p_S(x))$ - рабочий основания,
 $H(x) = (\omega_1(x), \omega_2(x), \dots, \omega_S(x))$ - шифртекст.

Представление результата расшифрования в позиционном виде производится по формуле:

$$T(x) = \sum_{i=1}^S \alpha_i(x) B_i(x)(\text{mod } P(x)), \quad (8)$$

где $T(x)$ - расшифрованный (открытый) текст.

Программная реализация рассмотренного алгоритма выполнена на языке программирования C# с использованием интерфейса программирования в приложении Windows Forms (рисунок 1).

При выполнении алгоритмов шифрования/дешифрования файл считывается с диалогового окна программы. При нажатии кнопки «Шифрование»/«Дешифрование» начинается процесс шифрования или дешифрования соответственно. При шифровании для записи полученного шифртекста создаётся файл с названием шифруемого файла, но с расширением «.сургт» в том каталоге, который был выбран пользователем. Если же файл уже существует, то он заменяется текущим шифртекстом по умолчанию в той же папке, где хранится и сама программа. Принципиальная схема работы программной реализации приведена на рисунке 2.

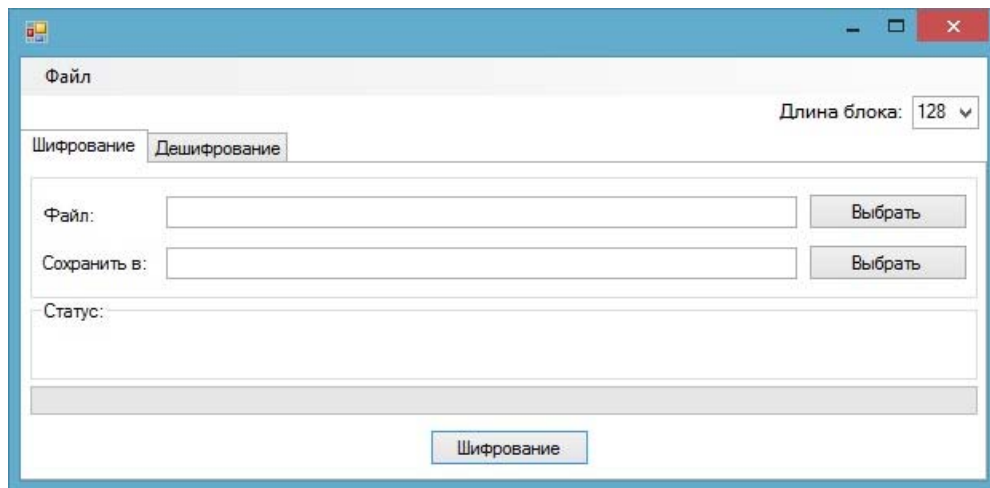


Рис. 1 - Пользовательский интерфейс программы

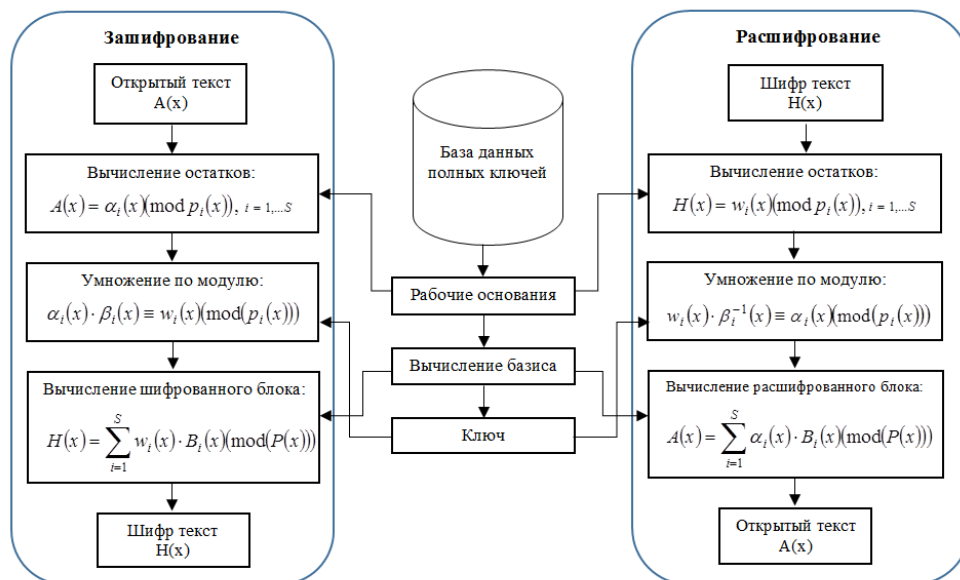


Рис. 2 – Принципиальная схема алгоритма шифрования на базе китайской теоремы об остатках

Рассмотрим примеры шифрования для одного блока открытого файла, демонстрирующие проявление «лавинного эффекта» у рассмотренного алгоритма.

Пример 1. При изменении одного бита в конце открытого текста при одном и том же ключе шифртексты, полученные для исходного и измененного открытого блока, полностью отличаются друг от друга.

Набор ключей:

100100000100101 110011110000110 11110101101110 1010101001100 100110110111001
101010011100000 10110100010100 10111100

Открытый текст:

50726f6772616d6d6572637368617270
50726f6772616d6d6572637368617271



Шифртекст:

D31FDA7909205AC93813A4D9EDB3E54E
951748E6E9CC911DE27A3F07F45DD6FE

Пример 2. При изменении одного бита в середине открытого текста при одном и том же ключе шифртексты, полученные для исходного и измененного открытого блока, полностью отличаются друг от друга.

Открытый текст:

50726f6772616d6d6572637368617270
50726f6772616d6c6572637368617270



Шифртекст:

D31FDA7909205AC93813A4D9EDB3E54E
E4CCABF3DDDC39ADA6E7C4EBA1A89192

Пример 3. При изменении одного бита в конце открытого текста и ключа шифртексты, полученные для исходного и измененного открытого блока, полностью отличаются друг от друга.

Набор ключей:

100100000100101 110011110000110 11110101101110 1010101001100 100110110111001
101010011100000 10110100010100 10111000



Открытый текст:

50726f6772616d6d6572637368617270
50726f6772616d6d6572637368617271



Шифртекст:

1B80ACE699830754C5DBD7E90B5EC57F
493C69376852233AC93A0D43950AF586

Заключение

Предлагаемый алгоритм шифрования при сравнении с разработанным ранее алгоритмом шифрования на базе НПСС [3] имеет следующие преимущества: алгоритм удовлетворяет требованиям по «лавинному эффекту» или статистическому криптоанализу.

Вместе с тем имеются и недостатки. В процессе шифрования и дешифрования при выполнении операции деления полиномов снижается производительность (эффективность) работы программы. Так как в самом алгоритме изначально заложено возможность распараллеливания по рабочим основаниям НПСС, то это позволяет избавиться от этого недостатка. Это и будет являться предметом дальнейших исследований по надежности и эффективности рассмотренного алгоритма шифрования на основе китайской теоремы об остатках.

Литература

1. Бияшев Р. Г. Разработка и исследование методов сквозного повышения достоверности в системах обмена данными распределенных АСУ: дисс. докт. тех. наук: 05.13.06: защищена 09.10.1985: утв. 28.03.1986. - М., 1985.
2. Амербаев В.М., Бияшев, Р.Г., Нысанбаева С.Е. Применение непозиционных систем счисления при криптографической защите // Изв. Нац. акад. наук Республики Казахстан.– Сер. физ.-мат.– Алматы:Гылым, 2005. - № 3. – С. 84-89.
3. R. Biyashev, M. Kalimoldayev, S. Nyssanbayeva, N. Kapalova, R. Khakimov. Program Modeling of the Cryptography Algorithms on Basis of Polynomial Modular Arithmetic / The 5th International Conference on Society and Information Technologies (ICSIT 2014, march 4-7, 2014- Orlando, Florida, USE) – IIIS. pp. 49-54
4. Бияшев Р.Г., Нысанбаева С. Е., Капалова Н.А. Секретные ключи для непозиционных криптосистем. Разработка, исследование и применение. – LAB LAMBERT Academic Publishing, 2014, с. 126.

РЕАЛИЗАЦИЯ АЛГОРИТМА КРИПТОГРАФИЧЕСКОГО ПРЕОБРАЗОВАНИЯ

Нысанбаева С. Е., Кабылханов А. Б.
e-mail: sultasha1@mail.ru, faircisco@gmail.ru

*Институт информационных и вычислительных технологий КН МОН РК,
Казахстан*

Аннотация. В данной работе приводится описание разработанной компьютерной программы для криптографического алгоритма, разработанного на основе режима стандарта шифрования США «Режим сцепления блоков по шифртексту», сети Фейстеля и системы шифрования на базе НПСС. Данная программа является реализацией ранее полученных теоретических результатов при разработке указанного выше криптоалгоритма.

В Институте информационных и вычислительных технологий (ИИВТ) Министерства образования и науки Республики Казахстан выполняются работы по созданию, исследованию и реализации криптографических алгоритмов защиты хранимой и передаваемой информации. Эти алгоритмы разрабатываются с использованием непозиционных полиномиальных систем счисления (НПСС).

Одним из основных примеров при разработке блочных алгоритмов криптографического преобразования является многократная, состоящая из нескольких циклов (раундов), обработка одного блока открытого текста. На каждом цикле данные подвергаются специальному преобразованию при участии вспомогательного ключа, полученного из заданного секретного ключа. Примером такого криптографического преобразования является сеть Фейстеля [1]. Выбор числа циклов определяется требованиями по криптостойкости и эффективности реализации блочного шифра. Как правило, чем больше циклов, тем выше криптостойкость, но ниже эффективность реализации блочного шифра [1].

В данной статье приведены результаты, полученные при создании компьютерной программы для криптографического алгоритма, разработанного с использованием трех криптографических преобразований: режима стандарта шифрования США «Режим сцепления блоков по шифртексту», сети Фейстеля и системы шифрования на базе НПСС (далее будем называть этот алгоритм как разработанный криптоалгоритм) [2].

Реализация алгоритма шифрования. В настоящее время существуют различные языки программирования, наиболее популярными из которых являются такие, как C++, Java, Python, Delphi и другие [3]. Средой программирования для некоторых из них является среда разработки Microsoft Visual Studio. Он прост и удобен в использовании, при этом он очень функционален, а интерфейс приложений, выполненных на этом языке, удобен для пользователя. Дизайн и интерфейс программы разработаны при помощи встроенного редактора Visual Studio, что позволило сделать ее наиболее удобной и функциональной.

Разработанный программный продукт не требует установки на персональном компьютере. Запуск программы для разработанного криптоалгоритма производится двумя кликами левой кнопки мыши по исполняемому файлу «lib17.exe» (рис. 1).

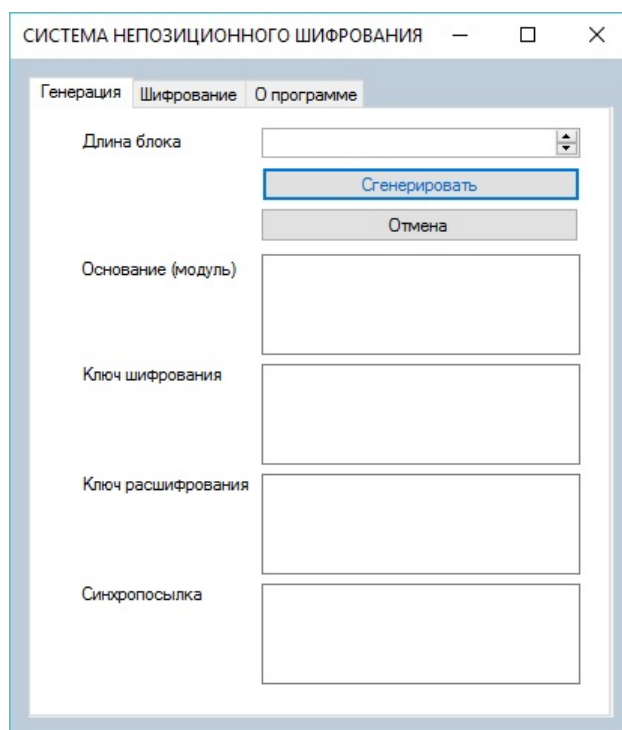


Рис. 1. Главное окно программы

Интерфейс программы. Рабочее окно программы разделено на 3 вкладки (или логические части), в каждой из которой выполняются функции, необходимые для выполнения, разработанного криптоалгоритма.

Первая вкладка «Генерация» служит для управления входными данными. Эта часть включает в себя клавиши «Сгенерировать» и «Отмена», а также поля входных параметров для работы алгоритма шифрования:

- Длина блока;
- Основание (модуль);
- Ключ шифрования;

- Ключ расшифрования;
- Синхропосылка (вектор инициализации).

Перед генерацией входных параметров нужно задать длину блока шифруемых данных, размер блока по умолчанию 64 бита. Генерация осуществляется автоматически по заданной длине блока. Для этого нажимаем на клавишу «Сгенерировать» и программа реализует следующие функции (рис. 2):

- Выбор основания (модуля) из массива данных;
- Генерацию ключей шифрования и расшифрования: псевдослучайная последовательность генерируется функцией «rand»;
- Генерацию синхропосылки: используется также функция «rand».

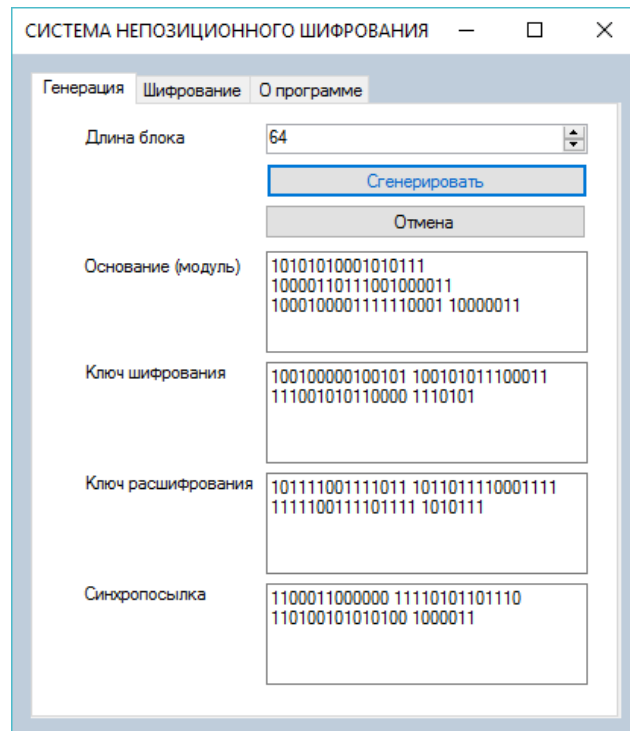


Рис. 2. Генерация входных данных

Вторая вкладка «Шифрование» - это диалоговое окно для работы с файлами различного формата. Она состоит из клавиш «Зашифровать» и «Расшифровать», также включает поля для вывода, открытого и зашифрованного файлов в двоичном виде (рис. 3 и 5).

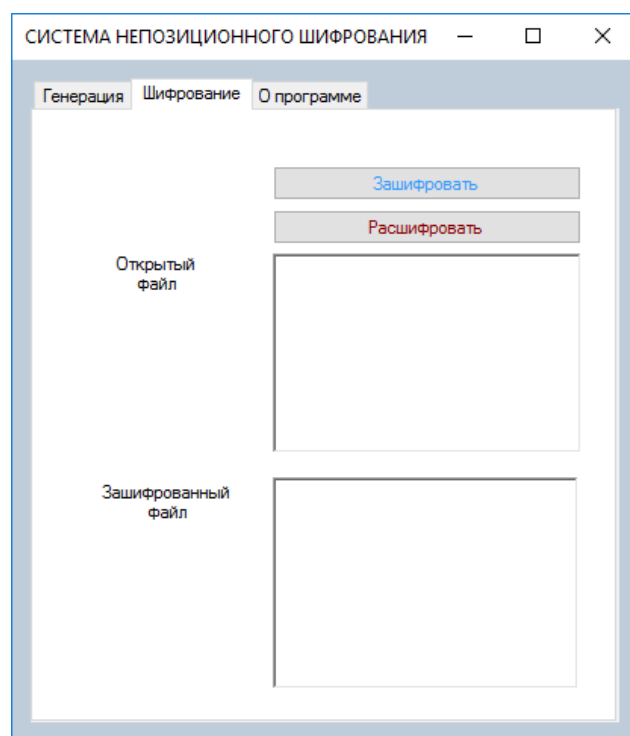


Рис. 3. Шифрование файлов

При нажатии на клавишу «Зашифровать», открывается рабочее окно для загрузки открытого файла и последующего сохранения зашифрованного файла (рис. 4).

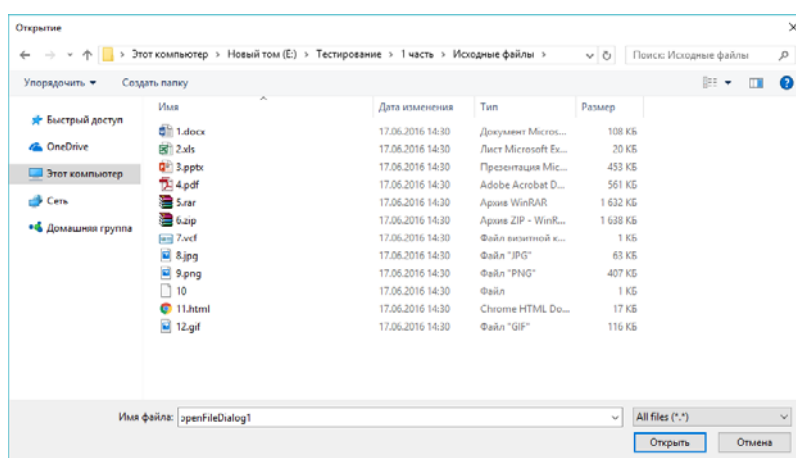


Рис. 4. Загрузка открытого файла и сохранение зашифрованного файла

Процесс работы программы можно разделить на 2 этапа: зашифрование файла и его расшифрование, открытый файл и шифртекст открываются в соответствующих полях (рис. 5).

Третья вкладка «О программе» содержит такие данные, как информацию об авторе, используемом программном обеспечении и краткое описание алгоритма шифрования (рис. 6).

Разработка и исследование алгоритма криптографического преобразования необходима для улучшения статистических характеристик системы шифрования [4].

Для улучшения статистических характеристик данного алгоритма шифрования проводится тщательный анализ следующих параметров:

- вектор инициализации;
- количество раундов;
- размер входных данных.

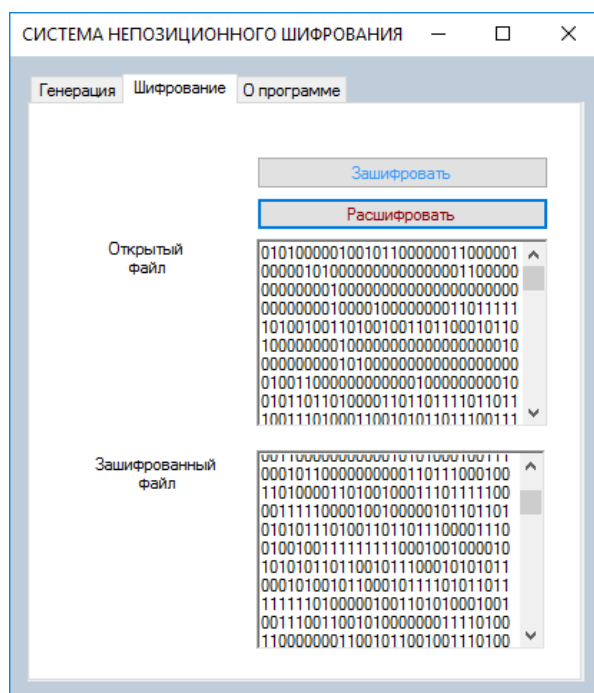


Рис. 5. Процедуры шифрования и расшифрования криптограмм

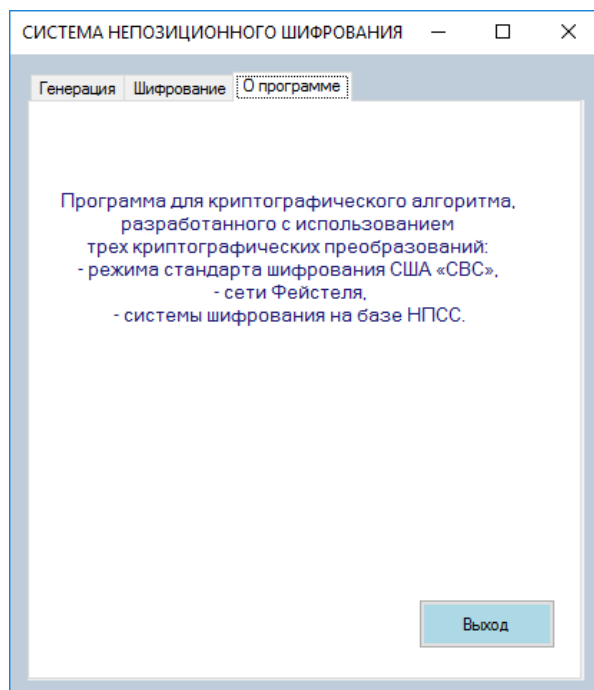


Рис. 6. О программе

Для проверки функционирования разработанного криптоалгоритма в качестве примера работы был использован файл .txt, содержащий набор произвольных цифр «1 2 3 4 5 6 7 8 10 11 12 13 14 15 16 17», размер шифруемого блока равен 64 бита.

Ниже приведен результат зашифрования одного открытого блока - блока криптограммы. Он получен при использовании режима стандарта шифрования США «Режим сцепления блоков по шифртексту», сети Фейстеля и системы шифрования на базе НПСС (табл. 1).

Таблица 1. Структура одного блока криптограммы

Исходный файл с расширением .txt (в двоичном виде)	00110001 00110010 00110011 00110100 00110101 00110110 00110111 00111000 11100010 11101111 01010110 01011101 11110001 01110111 10101011 00101110 11111000	
Деление на блоки: работа с 1-м блоком (64 бит)	00110001 00110010 00110011 00110100 00110101 00110110 00110111 00111000	
Деление на подблоки для сети Фейстеля (32 бит)	L ₀	00110001 00110010 00110011 00110100
	R ₀	00110101 00110110 00110111 00111000
Вектор инициализации (32 бит)	00110011 00110101 00110100 00110110	
Работа с первым блоком		
Левый подблок L ₀		Правый подблок R ₀
00110001 00110010 00110011 00110100		00110101 00110110 00110111 00111000
R ₁ = L ₀ ⊕ IV		
00000010 00000111 00000111 00000010		
Шифрование на базе НПСС E ₀ = F(L ₀ ⊕ IV, k)		
01010011 11100000 00101010 10000001		
		L ₁ = R ₀ ⊕ E ₀
		01100110 11010110 00011101 10111001
1 раунд		
R ₂ = L ₁		R ₁
01100110 11010110 00011101 10111001		00000010 00000111 00000111 00000010
E ₁ = F(L ₁ , k)		
10110101 00101100 11110011 00100000		
		L ₂ = R ₁ ⊕ E ₁
		10110111 00101011 11110100 00100010
2 раунд		
R ₃ = L ₂		R ₂
10110111 00101011 11110100 00100010		01100110 11010110 00011101 10111001
E ₂ = F(L ₂ , k)		
01011001 00001011 00111101 01011001		
		L ₃ = R ₂ ⊕ E ₂
		00111111 11011101 00100000 11100000

3 раунд	
$L_4 = L_3$	R_3
00111111 11011101 00100000 11100000	10110111 00101011 11110100 00100010
$E_3 = F(L_3, k)$	
11110111 01110000 11010111 10110100	
	$R_4 = R_3 \oplus E_3$
	01000000 01011011 00100000 10010110
4 раунд	
L_4	R_4
00111111 11011101 00100000 11100000	01000000 01011011 00100000 10010110

Заклучение. На основе разработанной программы будет исследовано влияние каждого из использованных криптографических преобразований (режим стандарта шифрования США «Режим сцепления блоков по шифртексту», сеть Фейстеля и система шифрования на базе НПСС) на надежность разработанного криптоалгоритма и проведен анализ статистических свойств получаемых криптограмм.

В данной статье описаны:

1. программная реализация разработанного криптоалгоритма, построенного на основе режима стандарта шифрования США «Режим сцепления блоков по шифртексту», сети Фейстеля и системы шифрования на базе НПСС;
2. пример выполнения программы для конкретного открытого файла длины 64 бита.

Литература

1. Баричев С. Г., Гончаров В. В., Серов Р. Е. Основы современной криптографии - 3-е изд. - М.: Диалог-МИФИ, 2011. - 176 с.
2. Калимолдаев М. Н., Кабылханов А. Б., Магзом М. М., Нысанбаева С. Е. Построение модели для системы шифрования, разработанной на базе модулярной арифметики // Вестник КазНУ. Серия математика, механика, информатика - Алматы, 2016. №3/1(90). - С. 30-40.
3. *Язык программирования.* - https://ru.wikipedia.org/wiki/Язык_программирования (30.05.2017 г.).
4. М. А. Иванов, И. В. Чугунков. Теория, применение и оценка качества генераторов псевдослучайных последовательностей. - М.: КУДИЦ-ОБРАЗ, 2003. - С. 60-136.

РАЗРАБОТКА ИТЕРАЦИОННОГО МЕТОДА РАСЧЕТА НЕТОЧНЫХ ТЕПЛОФИЗИЧЕСКИХ ПАРАМЕТРОВ МЕТАСТАБИЛЬНЫХ ГОРНЫХ СИСТЕМ

Рысбайулы Б., Юничева Н. Р.
b.rysbauly@mail.ru, naduni@mail.ru

Аннотация. В связи с развитием науки и техники интерес к анализу интервально-заданных объектов и вопросам двусторонних оценок в последнее время нарастает. Анализ интервально-заданных объектов появился сравнительно недавно как метод

автоматического контроля ошибок округления на ЭВМ. Впоследствии он превратился в один из разделов вычислительной математики, учитывающий также ошибки дискретизации численных методов, ошибки в начальных данных. Ценность интервальных решений заключается в том, что они содержат точные решения исходных задач.

Процесс передвижения тепла в горной породе описывается хорошо проверенная на практике уравнением теплопроводности. В работе ставятся начально-граничные условия, максимально точно описывающие физику переноса тепла в горной системе. В силу различных факторов точно задавать входные данные не всегда возможно, поэтому в настоящей работе разрабатывается приближенный метод расчета температуры грунта на недоступной границе области с интервально - заданными исходными данными.

1. Постановка задачи

В работе изучается начально-граничная задача в области $Q=(0,H) \times (0,t_{\max})$:

$$C_p \frac{\partial T}{\partial t} = \frac{\partial}{\partial z} \left(\lambda \frac{\partial T}{\partial z} \right), \quad (1)$$

$$T|_{z=0} = T_1(t), \quad \lambda \frac{\partial T}{\partial z} \Big|_{z=H} = -\alpha(T - T_a(t))|_{z=H}, \quad T|_{t=0} = T_0(z), \quad 0 < z < H. \quad (2)$$

Здесь $T(z,t)$ – температура грунта в области Q . C_p, λ – соответственно объемный коэффициент теплоемкости и коэффициент теплопроводности грунта. $T_a(t)$ – температура окружающей среды; H – толщина грунта. $t_{\max}$ – продолжительность времени наблюдения; t – время; z – фазовая координата; $T_1(t)$ – неизвестная температура грунта на нижней границе области. $T_0(t)$ – начальные распределения температуры грунта.

В прикладных задачах уравнений математической физики возникла необходимость решения начально-краевых задач с неточными данными. В результате чего в 1991 году группа авторов разработали методы интервального анализа [1]. Идею этого метода подхватили другие ученые и вышла в свет работы [2-5]. Эти работы посвящены различным проблемам интервального анализа. В последующем методы интервального анализа стали применять при решении начально-краевых корректно поставленных задач уравнений математической функции [6, 7].

Однако, применение методов интервального анализа к решению обратнo-некорректно поставленных задач мало изучено. Поэтому, настоящая работа посвящена к разработке метода решения задачи продолжения для системы (1) – (2).

Дело в том, что $T_a(t)$ измеряется с использованием определенного типа приборов. Каждый прибор характеризуется точностью измерения. Обычно в технической характеристике прибора указываются пределы допустимой ошибки данного прибора. Это говорит о том, что задачи (1) – (2) следует решать, когда:

$$T_a(t) \in [\underline{T_a(t)}, \overline{T_a(t)}],$$

где, $T_a(t)$ и $\overline{T_a(t)}$ - нижние и верхние пределы измерений величины $T_a(t)$. Аналогичным образом допускаем

$$T_0(t) \in [T_0(t), \overline{T_0(t)}].$$

На доступной границе $z = H$ становится измерения температуры грунта на поверхности земли

$$T_g(t), 0 < t < t_{\max}.$$

Полагаем, что граница $z = 0$ не доступна. В дальнейшем будем заниматься разработкой метода нахождения величины $T_1(t)$.

Проведенные нами измерения [8] показывают, что $T_g(t)$ медленно меняется в зависимости от времени. Исходя из этого в дальнейшем принимается зависимость:

$$T_1(t) = At + B.$$

Будем искать величин A и B .

2 Дискретные задачи

Отрезок $(0, H)$ разбиваем на N равных частей с шагом $\Delta z = \frac{H}{N}$, а отрезки $(0, t_{\max})$ на

m равных частей с шагом $\Delta t = \frac{t_{\max}}{m}$. В полученной дискретной области

$$\omega = \{(z_i, t_j), z_i = i \cdot \Delta z, t_j = j \cdot \Delta t, i = 0, 1, \dots, N; j = 0, 1, \dots, m\}$$

изучается задача

$$C_p \frac{Y_i^{j+1} - Y_i^j}{\Delta t} = \frac{1}{\Delta z} \left(\lambda_{i+1/2} \frac{Y_{i+1}^{j+1} - Y_i^{j+1}}{\Delta z} - \lambda_{i+1/2} \frac{Y_i^{j+1} - Y_{i-1}^{j+1}}{\Delta z} \right), \quad (3)$$

$$i = 1, 2, \dots, N-1; \quad j = 0, 1, \dots, m-1.$$

$$Y_0^{j+1} = T_1(t_{j+1}), \quad \lambda_{N-1/2} \frac{Y_N^{j+1} - Y_{N-1}^{j+1}}{\Delta z} + \alpha Y_N^{j+1} = \alpha T_a(t_{j+1}), \quad j = 0, 1, \dots, m-1, \quad (4)$$

$$Y_i^0 = T_0(z_i), \quad i = 0, 1, \dots, N-1. \quad (5)$$

Коэффициенты A и B определяются итеративно. Сначала задаются начальные приближения $A(n)$ и $B(n)$, $n = 0$; где n – номер итераций. Следующие приближения $A(n+1)$ и $B(n+1)$ определяются из монотонности функционала

$$J(A, B) = \sum_{j=0}^{m-1} (Y_N^{j+1} - T_g(t_{j+1}))^2 \Delta t.$$

Действуя так же как в работе [8] после некоторых вычислений получаем сопряженную разностную задачу

$$C_p U_{i,\bar{t}}^{j+1} + \left(\lambda_{i-1/2} U_{i,\bar{z}}^j \right), \quad i = 1, 2, \dots, N-1; \quad j = m-1, m-2, \dots, 0, \quad (6)$$

$$\alpha U_N^j + \lambda_{N-1/2} U_{N,\bar{z}}^j = 2 \left(Y_N^{j+1} - T_g(t_{j+1}) \right), \quad j = m-1, m-2, \dots, 0, \quad (7)$$

$$U_i^j = 0, \quad j = 0, 1, \dots, N, \quad U_i^m = 0, \quad i = 0, 1, \dots, N. \quad (8)$$

Кроме этого выводится равенство

$$2 \sum_{j=0}^{m-1} \Delta Y_N^{j+1} \cdot \left(Y_N^{j+1} - T_g(t_{j+1}) \right) \Delta t = \sum_{j=0}^{m-1} \lambda_{1/2} U_{1,\bar{z}}^j \left(\Delta A \cdot t_{j+1} + \Delta B \right) \Delta t. \quad (9)$$

Предполагаем, что C_p , λ и α задаются точно. По предположению $T_a(t)$, $T_0(z)$ и $T_g(t)$ задано интервально. Поэтому точно вычисляется ширина этих интервалов

$$\omega(T_a) = \overline{T_a}(t) - \underline{T_a}(t), \quad \omega(T_g) = \overline{T_g}(t) - \underline{T_g}(t), \quad \omega(T_0) = \overline{T_0}(z) - \underline{T_0}(z).$$

3. Решение задачи продолжения

Так как A и B являются функцией от номера итераций n , то можно вести следующее обозначение

$$J(A(n), B(n)) = J_n(A, B).$$

В силу введенного обозначения и используя определение функционала $J(A, B)$ выводится формула

$$J_{n+1}(A, B) - J_n(A, B) = 2 \sum_{j=0}^{m-1} \Delta Y_N^{j+1} \cdot \left(Y_N^{j+1} - T_g(t_{j+1}) \right) \Delta t + \sum_{j=0}^{m-1} \left(\Delta Y_N^{j+1} \right)^2 \Delta t.$$

С учетом (9) последняя формула записывается в виде

$$J_{n+1}(A, B) - J_n(A, B) = \sum_{j=0}^{m-1} \lambda_{1/2} U_{1,\bar{z}}^j \left(\Delta A \cdot t_{j+1} + \Delta B \right) \Delta t + \sum_{j=0}^{m-1} \left(\Delta Y_N^{j+1} \right)^2 \Delta t.$$

Интуиция подсказывает, что первые два выражения, стоящие в правой части знака равенства сильно влияют на ΔJ в отличие от третьей суммы, стоящей в правой части знака равенства. Поэтому записывается следующее равенство:

$$A_{n+1} = A_n + \xi_n \sum_{j=0}^{m-1} \lambda_{1/2} U_{1,\bar{z}}^j t_{j+1} \Delta t, \quad B_{n+1} = B_n + \zeta_n \sum_{j=0}^{m-1} \lambda_{1/2} U_{1,\bar{z}}^j t_{j+1} \Delta t. \quad (10)$$

Здесь достаточно малые положительные функций ξ_n и ζ_n играют очень важный роль при численном решении поставленной задачи. А именно этими параметрами управляют весь вычислительный процесс.

4. Вычислительная устойчивость метода прогонки

Систему (3) – (5) записываем в виде:

$$A_i Y_{i+1}^{j+1} - B_i Y_i^{j+1} + C_i Y_{i-1}^{j+1} + F_i^j = 0, \quad i = 1, 2, \dots, N-1, \quad j = 0, 1, \dots, m-1, \quad (11)$$

$$Y_N^{j+1} = \frac{1}{1+E} Y_{N-1}^{j+1} + \frac{E}{1+E} T_a^{j+1}. \quad (12)$$

Здесь

$$A_i = \frac{\Delta t \lambda_{i+1/2}}{(\Delta z)^2 C_p}, \quad C_i = \frac{\Delta t \lambda_{i-1/2}}{(\Delta z)^2 C_p}, \quad B_i = A_i + C_i + 1, \quad F_i^j = Y_i^j, \quad E = \frac{\alpha \Delta z}{\lambda_{N-1/2}}. \quad (13)$$

Функций метода прогонки для системы (11) - (13) записываются в виде

$$\alpha_{i+1} = \frac{A_i}{B_i - C_i \alpha_i}, \quad \beta_{i+1} = \frac{C_i \beta_i + F_i^j}{B_i - C_i \alpha_i}. \quad (15)$$

В работе доказана

Теорема 1. Если коэффициенты трехточечной разностной схемы определяются по формуле (15) и $A_i \leq q < 0.5$, то имеют место неравенства:

$$|\alpha_i| < \frac{1}{2}, \quad i = 0, 1, \dots, N-1.$$

Особый интерес для приложения представляет оценка свободного члена метода прогонки. Мы провели оценки такого характера результат исследований записывается в виде следующей теоремы.

Теорема 2. Если для коэффициентов трехточечной разностной задачи (11) имеет место условие Куранта с константой $q < 1$, то из второй формулы системы (15) следует оценка:

$$|\beta_{N-i}| \leq \left(\frac{q}{1+q_0} \right)^{i-1} \frac{E}{1+E} T_a^{j+1} + \frac{1}{1-q+q_0} \left[1 - \left(\frac{q}{1+q_0} \right)^{i-1} \right] M^j,$$

где $i = 2, 3, \dots, N$; $M^j = \max_i |Y_i^j|$. В нашем случае условий Куранта записывается в виде:

$$0 < q_0 \leq C_i \leq q < 1, \quad i = 1, 2, \dots, N-1.$$

6. Оценки

Для решения прямой разностной задачи получена оценка

$$Y_{N-i}^{j+1} \leq Y_N^{j+1} \left(\frac{q}{1+q} \right)^{i-1} + \beta_0^{j+1} \frac{1}{1 - \left(\frac{q}{1+q} \right)^{N-i+1}} + M^j (1+q), \quad i = 1, 2, \dots, N. \quad (16)$$

Из оценки (16) видно, что при начальных значениях i наблюдается существенное влияние Y_N^{j+1} на решения разностной задачи. Обращая внимание на формулу (16) заключаем, что при этих значениях i на решение Y_i^{j+1} наблюдается влияние функций T_a и Y_i^j - значение сеточной функции в предыдущем временном слое.

Аналогичная оценка получена для решения сопряженной задачи:

$$\left| N^{m-j} \right| \leq q \sum_{k=1}^j \left| \frac{(1+E-\alpha_N)(1+E)\tilde{\beta}_N + 2[\beta_N + E \cdot T_a^{k+1} - (1+E-\alpha_N)T_g^{k+1}]}{(1+E-\alpha_N)^2} \right|.$$

$$N^{j+1} = \max_i |U_i^{j+1}|.$$

Оценка ширины интервала решений прямой задачи. Выше нами было показано, что коэффициенты α_i вычисляются точно. Но коэффициенты β_i являются интервальными величинами. Поэтому нас интересует ширина этих интервалов.

Рассмотрим случай, когда принимается гипотеза $Y_{i-1}^{j+1} = \alpha_i Y_i^{j+1} + \beta_i$. Сначала берем функцию ширину ω от обе части знака равенства (15):

$$\omega(\beta_{i+1}^{j+1}) = \frac{C_i}{B_i - C_i \alpha_i} \omega(\beta_i^{j+1}) + \frac{1}{B_i - C_i \alpha_i} \omega(Y_i^j).$$

Отсюда следует оценка

$$\omega(Y_{N-i}^{j+1}) \leq q^i \frac{\omega(\beta_N)}{1+E-\alpha_N} + q^i \frac{E}{1+E-\alpha_N} \omega(T_a^{j+1}) + \frac{1}{1-q} \omega(M^j).$$

Оценка ширины интервала решений сопряженной задачи. Чтобы оценить $\omega(\tilde{\beta}_i)$ мы должны пользоваться формулой:

$$\tilde{\beta}_{i+1} = \frac{C_i \tilde{\beta}_i + F_i}{B_i - C_i \cdot \alpha_i}.$$

После некоторых рассуждений выводится оценка:

$$\omega(U_N^j) \leq \frac{2}{E} (\omega(Y_N^{j+1}) - \omega(T_a^{j+1})).$$

В окончательном виде получаем оценку

$$\max_i \omega(Y_i^{j+1}) \leq \omega(T_a^{j+1}), \quad \max_i \omega(U_i^j) \leq \frac{2}{E} |\omega(T_a^{j+1}) - \omega(T_g^{j+1})| \quad (17)$$

Теорема 3. Ширина интервалов решения прямой задачи $\omega(Y_i^{j+1})$ оценивается через ширину $\omega(T_a^{j+1})$, а ширина решения сопряженной задачи $\omega(U_i^j)$ оценивается через ширину $\omega(T_a^{j+1})$ и $\omega(T_g^{j+1})$ в явном виде и выражаются формулой (17).

Оценка итерационных формул обратной задачи. В работе получены оценки

$$|A(n)| \leq \sum_{j=0}^{m-1} C_1(T_{j+1}) |T_a^{j+1} - T_g^{j+1}| \Delta t,$$

$$|\omega(A(n))| \leq \sum_{j=0}^{m-1} C_1(T_{j+1}) |\omega(T_a^{j+1}) - \omega(T_g^{j+1})| \Delta t.$$

Отсюда незамедлительно следует устойчивость вычислительной схемы. С другой стороны получили управляемость ширины интервала $A(n)$ в процессе вычислительных операций.

Таким образом, можно заключить следующее:

1) Объектом изучения является математическая модель процесса распространения тепла в метастабильном горном массиве.

2) Построена математическая модель переноса тепла в горном массиве. На основе дискретной модели исходной задачи с неточными данными выводится сопряженная разностная задача.

3) Разработана итерационная формула расчета температуры горного массива на недоступной границе рассматриваемой области.

4) Температура горного массива на недоступной границе находится через решения прямой и сопряженной разностной задачи итерационным способом. Все вычисления проводятся с использованием интервальной арифметики. Сходимость вычислительного процесса, а также монотонность минимизируемого функционала достигается параметрами управления ξ_n и ζ_n .

5) Прямая и сопряженная разностная задача решается методом прогонки, и выводятся условия вычислительной устойчивости метода прогонки для прямой задачи $|\alpha_i| < 1$, $i = N - 1, N - 2, \dots, 0$, а также условий вычислительной устойчивости метода прогонки для сопряженной задачи $|\tilde{\alpha}_i| < 1$, $i = N - 1, N - 2, \dots, 0$.

6) Оцениваются функции β_i и $\tilde{\beta}_i$, $i = N - 1, N - 2, \dots, 0$ через входные данные исходной задачи.

7) Получены интервальные оценки для ширины функций α_i и $\tilde{\alpha}_i$ и доказываются, что ширина коэффициентов прогонки α_i и $\tilde{\alpha}_i$ управляются через Δz и Δt .

8) Получены интервальные оценки для решения прямой разностной задачи Y_i^{j+1} и для решения сопряженной разностной задачи U_i^j .

9) Получены интервальные оценки для решения прямой разностной задачи Y_i^{j+1} и для решения сопряженной разностной задачи U_i^j .

10) Получены интервальные оценки для ширины разностных функций $\omega(Y_i^{j+1})$ и $\omega(U_i^j)$. Доказано непрерывная зависимость ширины разностных функций $\omega(Y_i^{j+1})$ и $\omega(U_i^j)$ от ширины входных данных исходной задачи.

11) Получены интервальные оценки для суммы $\sum_j^{m-1} t_{j+1} \lambda_{1/2} U_{1,z}^j \Delta t$ и $\sum_j^{m-1} t_{j+1} \lambda_{1/2} U_{1,z}^j \Delta t$.

12) Получены интервальные оценки для ширины $\omega(\Delta A)$ и $\omega(\Delta B)$. Доказано непрерывная зависимость ширины $\omega(\Delta A)$ и $\omega(\Delta B)$ от ширины входных данных исходной задачи.

13) Проведены численные расчеты.

Литература

1. Жолен Л. Кифер М. и др. Прикладной интервальный анализ. 2007, 468 с.
2. Joulin L etc. Applied Interval Analysis. – Springer, 2001. – 307 p.
3. Hongli Li etc. Analysis and Synthesis for Interval Type-2 Fuzzy – Model – Based Systems. – Springer, 2016. – 347 p.
4. Wei G. Interval Finite Element Analysis using Interval Factor Method // Computational Mechanics. – 2007. – Vol. 39, № 6. – P. 709-717.
5. Rui Yao etc. Accuracy analysis of Stewart platform based on interval analysis method // Chinese formal of Mechanical Engineering. – 2013. – Vol. 26, № 1. – P. 29-34.
6. Tepoyan L., Zschorn S. Degenerate nonselfadjoint high-order ordinary differential equations on an infinite interval // Journal of Contemporary Mathematical Analysis. – 2015. – Vol. 50, № 3. – P. 114–118.
7. Thandapani E. Interval oscillation criteria for second-order forced impulsive delay differential equations with damping term. – Springerplus. 2016. – P. 3- 4.
8. Rysbaiyly B., Yunicheva N., The computational stability of finding method the coefficient of thermal conductivity of earthmaterial with inexact data, Proceedings of International Conference «ICECCO - 2015» (27-28 September 2015, Almaty), 2015, p. 46–54
9. Samarski A.A. The theory of difference schemes. Printed in the united states of America, 2001, Pp.788.

КОМПЬЮТЕРНЫЙ МОЛЕКУЛЯРНЫЙ ДИЗАЙН ЛЕКАРСТВЕННЫХ ПРЕПАРАТОВ НА ОСНОВЕ АЛГОРИТМОВ РОЕВОГО ИНТЕЛЛЕКТА И ИММУННОСЕТЕВОГО МОДЕЛИРОВАНИЯ

Самигулина Г.А., Масимканова Ж.А.
e-mail: galinasamigulina@mail.ru

*Институт информационных и вычислительных технологий КН МОН РК,
Казахстан*

Аннотация. При разработке интеллектуальной информационной системы ведения научных исследований и прогнозирования зависимости структура-свойство/активность новых лекарственных препаратов применение алгоритмов роевого интеллекта для построения оптимальной иммунносетевой модели является актуальной и перспективной задачей. Интеллектуальная иммунносетевая технология прогнозирования зависимости структура-свойство/активность позволяет анализировать скрытые взаимодействия между дескрипторами, сократить время обучения иммунной сети и исключить малоинформативные дескрипторы. В работе решается задача отбора информативных дескрипторов сульфаниламидов для построения оптимальной иммунносетевой модели и дальнейшего иммунносетевого моделирования новых лекарственных препаратов в соответствии с концепцией мультиалгоритмического подхода. Использование алгоритмов роевого интеллекта позволяет решать сложные оптимизационные задачи на основе применения коллективного интеллекта и мультиагентных систем. Наиболее распространёнными из них являются методы муравьиной и пчелиной колонии, а также алгоритм роя частиц.

Бурное развитие техники и технологий способствует широкому применению современных подходов биоинформатики и искусственного интеллекта для обработки и анализа накопленных химических данных. Применение этих методов актуально для построения баз данных лекарственных соединений при прогнозировании физических, химических и биологических свойств веществ. Одним из важных этапов процесса прогнозирования зависимости структура-свойство/активность является выделение информативных дескрипторов для уменьшения размерности дескрипторного пространства [1]. В настоящее время применение новых инновационных интеллектуальных методов для решения задачи прогнозирования новых химических соединений с заданными свойствами является актуальной задачей. Поэтому методы искусственного интеллекта такие, как нейронные сети, эволюционные алгоритмы, искусственные иммунные системы, алгоритмы роевого интеллекта [2] нашли применение в решении задачи отбора информативных дескрипторов.

В работе [3] разработана иммунносетевая технология прогнозирования зависимости структура-свойство/активность химических соединений, состоящая из следующих задач: выбора химических соединений; описания структуры соединений на основе дескрипторов; отбора информативных дескрипторов и построения оптимального набора дескрипторов для дальнейшего иммунносетевого моделирования; классификации и обучения искусственной иммунной системы; распознавания образов; оценки энергетических ошибок; отбора кандидатов лекарственных соединений с заданными свойствами для дальнейших исследований. Выделение информативных дескрипторов выполняется на основе алгоритмов роевого интеллекта согласно концепций мультиалгоритмического подхода [4]. Отбор информативных дескрипторов позволяет находить оптимальное количество дескрипторов, при котором после иммунносетевого моделирования и прогнозирования свойств новых химических соединений ошибка обобщения будет минимальной [5].

Постановка задачи формулируется следующим образом: необходимо решить задачу выделения информативных дескрипторов на основе алгоритма муравьиной колонии и метода роя частиц для дальнейшего иммунносетевого моделирования лекарственных препаратов сульфаниламидной группы с заданными свойствами.

Алгоритмы роевого интеллекта основаны на моделировании поведения общественных живых существ и широко применяются для решения оптимизационных

задач [6]. Для поведения роя характерны автономность, распределение функций и самоорганизация. Эффективность алгоритмов роевого интеллекта зависит от ряда параметров, таких как: количества частиц, коэффициентов ускорения, веса инерции, типа и размера соседнего окружения, количества итераций и свободных параметров [7]. В алгоритмах агенты меняют свое положение основываясь на знании текущего положения, предыдущего состояния и предыдущих состояний соседей.

Разработана структурная схема интеллектуальной информационной системы (Рисунок 1), которая состоит из модулей предварительной обработки, распознавания образов, оценки энергетической ошибки и прогноза сульфаниламидов с заданными свойствами. Модуль предварительной обработки включает в себя отбор информативных дескрипторов на основе алгоритма муравьиной колонии и метода роя частиц.



Рис.1 Структурная схема интеллектуальной иммунносетевой технологии

Алгоритм муравьиной колонии представляет собой итеративный метод случайного поиска, основанный на моделировании поведения муравьев. В решении задачи выбора информативных дескрипторов набор дескрипторов представлен в виде графа, узлы которого являются дескрипторами [8]. Сначала задается количество дескрипторов, и затем каждый муравей из колонии устанавливается в какую-то начальную точку. Следующий дескриптор выбирается в зависимости от качества феромона на ребре. На каждом шаге происходит испарение феромона и при каждой итерации выбирается набор дескрипторов с минимальной ошибкой. Алгоритм завершается только тогда, когда пройдено требуемое количество итераций. В данном подходе предполагается, что

существует какой-то оптимальный набор дескрипторов, на котором классификаторы дают минимальный процент ошибки и подграф, на гранях которого будет максимальное количество феромона, а на гранях, соединяющих неинформативные дескрипторы феромона должно быть минимальное количество. Затем агент составляет набор дескрипторов, который предлагается использовать для построения модели [9, 10].

Разработка модуля предварительной обработки химических соединений «SIIM» (Swarm Intelligence for Immune network Modeling)

При разработке модуля предварительной обработки данных «SIIM» был использован язык программирования Python 3.6 с использованием PyQt.

Разработан следующий алгоритм функционирования системы «SIIM».

Алгоритм:

Шаг 1. Подключение базы данных.

Шаг 2. Выбор метода роевого интеллекта (муравьиного алгоритма, метода роя частиц).

Шаг 3. Ввод коэффициентов (количество популяций, количество итераций, вес, скорость)

Шаг 4. Обработка данных и выделение информативных дескрипторов.

Шаг 5. Построение оптимального набора дескрипторов. Критерием оптимальности является сохранение максимальной информативности дескрипторов при минимальном их количестве. Избыточность и малоинформативность дескрипторов снижает качество прогноза, поэтому при отборе новых химических соединений в кандидаты лекарственных препаратов важно учитывать информативность дескриптора.

Шаг 6. Вывод результата работы алгоритма.

Интеллектуальная технология иммунносетевого моделирования включает в себя работу с базами данных дескрипторов химических соединений. В качестве базы данных для поиска новых лекарственных соединений используются сульфаниламиды, которые относятся к лекарственным средствам широкого антибактериального действия. База данных сульфаниламидов создана [11] на основе спецификации химических веществ SMILES (Simplified Molecular Input Line Entry Specification), которая используется для поиска структурного сходства соединений. В качестве примера были использованы 15 химических соединений сульфаниламидов и 1500 дескрипторов разных уровней. В таблице 1 представлен фрагмент базы данных сульфаниламидов.

Таблица 1. Фрагмент базы данных сульфаниламидов

Class	Number of atoms	Relative number of C atoms	Relative number of H atoms	Relative number of O atoms	Relative number of N atoms	Number of single bonds	Molecular weight	...	Gravitation index (all pairs)
1	2	3	4	5	6	7	8	9	10
short_acting	27,00	0,37	0,37	0,07	0,15	16,00	250,28	...	3794,10
short_acting	33,00	0,36	0,42	0,06	0,12	24,00	278,33	...	4085,10
short_acting	31,00	0,35	0,42	0,10	0,10	26,00	267,30	...	3758,20
short_acting	27,00	0,33	0,37	0,07	0,15	23,00	270,32	...	4067,40

short_acting	46,00	0,33	0,54	0,04	0,07	39,00	311,44	...	4740,90
short_acting	33,00	0,36	0,42	0,06	0,12	24,00	278,33	...	4085,10
short_acting	46,00	0,33	0,54	0,04	0,07	39,00	311,44	...	4740,90
medium_acting	24,00	0,33	0,42	0,13	0,08	20,00	214,24	...	2919,40
medium_acting	35,00	0,34	0,40	0,11	0,11	25,00	310,33	...	4879,20
medium_acting	28,00	0,36	0,39	0,11	0,11	18,00	253,28	...	3666,80
medium_acting	31,00	0,35	0,42	0,10	0,10	22,00	267,30	...	4220,30
long_acting	35,00	0,34	0,40	0,11	0,11	25,00	310,33	...	4879,20
long_acting	36,00	0,42	0,39	0,06	0,11	22,00	314,36	...	4893,80
long_acting	31,00	0,35	0,39	0,10	0,13	26,00	280,30	...	4159,30
long_acting	30,00	0,37	0,40	0,07	0,13	22,00	264,30	...	3711,20

Химические соединения были классифицированы на сульфаниламиды короткого действия, средней длительности действия, длительного действия. Рассмотрены такие дескрипторы, как: количество атомов, количество атомов водорода, молекулярный вес, количество связей, гравитационный индекс и др.

В разработанной интеллектуальной информационной системе «SIIM» (Рисунок 2) с помощью кнопки «Data connection» выбирается база данных и отображается в первом окне. Затем осуществляется выбор алгоритма (алгоритма муравьиной колонии или метода роя частиц) и ввод коэффициентов. После запуска результаты моделирования отображаются во втором окне.

Результаты моделирования сульфаниламидов

На рисунке 2 показаны результаты моделирования сульфаниламидов на основе муравьиного алгоритма. При моделировании размер популяции равен 100, количество итераций равно 50, c_1 (количество феромона) = 1, c_2 (испарение феромона) = 2, частота отчета = 50. В результате из 1500 дескрипторов были выбраны 25 информативных дескрипторов. Аналогично интеллектуальная система работает с методом роя частиц. Выбирается тот алгоритм, который после иммунносетевого моделирования показывает наилучшие прогностические результаты.

Intellectual information system "SIIM"

Ant Colony Optimization

Population size100Number of generations50C11C22Report frequency50

Database connection

	Class	Number of atoms	ve number of C a	ve number of H a	ve number of O a	ve number of N a	ive num
1	short_acting	27.00	0.37	0.37	0.07	0.15	0.04
2	short_acting	33.00	0.36	0.42	0.06	0.12	0.03
3	short_acting	31.00	0.35	0.42	0.10	0.10	0.03
4	short_acting	27.00	0.33	0.37	0.07	0.15	0.07
5	short_acting	46.00	0.33	0.54	0.04	0.07	0.02
6	short_acting	33.00	0.36	0.42	0.06	0.12	0.03
7	short_acting	46.00	0.33	0.54	0.04	0.07	0.02
8	medium_acting	24.00	0.33	0.42	0.13	0.08	0.04
9	medium_acting	35.00	0.34	0.40	0.11	0.11	0.03
10	medium_acting	28.00	0.36	0.39	0.11	0.11	0.04
11	medium_acting	31.00	0.35	0.42	0.10	0.10	0.03
12	Long_acting	35.00	0.34	0.40	0.11	0.11	0.03
13	Long_acting	36.00	0.42	0.39	0.06	0.11	0.03
14	Long_acting	31.00	0.35	0.39	0.10	0.13	0.03
15	Long_acting	30.00	0.37	0.40	0.07	0.13	0.03

<

Particle Swarm Optimization

Report frequency50

Run

	n d8 (atomic var	elation d7 (atomic	orrelation d7 (ato	Wiener W index	d1 (atomic Sande	elation d8 (atomic	orrelation
1	1.24	-0.38	-0.19	522.00	0.00	0.35	-0.07
2	0.22	-0.06	-0.23	839.00	-0.14	0.77	-0.02
3	1.51	0.37	-0.06	720.00	-0.25	-0.20	-0.03
4	2.59	-0.36	0.03	502.00	-0.29	-0.29	0.15
5	0.09	-0.30	0.08	1040.00	0.08	0.57	-0.07
6	0.22	-0.06	-0.23	839.00	-0.14	0.77	-0.02
7	0.09	-0.30	0.08	1040.00	0.08	0.57	-0.07
8	2.47	0.48	0.06	321.00	-0.16	-0.53	-0.14
9	0.45	-0.23	0.02	1050.00	-0.03	0.54	0.00
10	0.90	-0.57	-0.05	584.00	0.05	0.52	-0.17
11	0.05	0.00	0.14	625.00	-0.02	0.39	-0.14
12	0.45	-0.23	0.02	1050.00	-0.03	0.54	0.00
13	1.11	0.28	-0.25	1289.00	-0.04	-0.04	0.09
14	0.69	0.21	-0.11	817.00	-0.11	0.11	-0.05
15	1.47	0.04	-0.27	668.00	-0.23	-0.21	0.05

<

Visualization

Clear Screen

HELP

Exit

Рис. 2 Результаты моделирования сульфаниламидов на основе муравьиного алгоритма

Заключение

В работе решается задача выделения информативных дескрипторов сульфаниламидной группы для построения оптимальной иммунносетевой модели и дальнейшего иммунносетевого моделирования новых лекарственных препаратов на основе алгоритмов роевого интеллекта. В настоящее время не существует универсальных методов для обработки данных, которые бы не зависели от качества и размера данных, наличия независимых дескрипторов и т.д., поэтому при построении оптимальной иммунносетевой модели применяется мультиалгоритмический подход. Достоинством этого метода является возможность выбора алгоритма с наилучшими прогностическими свойствами после иммунносетевого моделирования. Разработанная интеллектуальная информационная система позволяет сократить время на обучение иммунной сети с помощью построения оптимальной иммунносетевой модели и исключить малоинформативные дескрипторы.

Работа выполнена по гранту №ГР 0115РК00549 МОН РК по теме: Компьютерный молекулярный дизайн лекарственных препаратов на основе иммунносетевого моделирования (2015-2017 гг.).

Литература

1. Kokurkina G.V., Dutov M.D., Shevelev S.A., Popkov S.V., Zakharov A.V., Poroikov V.V. Synthesis, antifungal activity and QSAR study of 2-arylhydroxynitroindoles // Eur. Med. Chem. – 2011. – №46 (9). – P. 4374-4382.
2. Hinchey M.G., Sterritt R., Rouff C. Swarms and Swarm Intelligence // Computer Society «From Ants to People: an Instinct to Swarm». – IEEE, 2007. – №40. – P. 111-113.

3. Samigulina G.A., Samigulina Z.I. Immune Network Technology on the basis of random forest algorithm for computer-aided drug design // Bioinformatics and biomedical engineering. – 2017. – P. 50-61.
4. Samigulina G.A. Immune network modeling technology for complex objects intellectual control and forecasting systems. – Yelm, WA, USA: Science and Publishing House, 2015. – 172 p.
5. Samigulina G.A., Samigulina Z.I. Computational Molecular Design of Antiseptic Drugs based on Immune Network Modeling // Proceedings of the 12-th International Conference on Electronics Computer and Computation "ICECCO 2015". – IEEE: Suleyman Demirel University, 2015. – P.47-51.
6. Morteza A., Kobra Z., Azam B. Ant colony optimization as a descriptor selection in QSPR modeling: Estimation of the k-max of anthraquinones-based dyes // Journal of Saudi Chemical Society. – 2013. – P. 2-5.
7. Liu F., Zhou Z. A new data classification method based on chaotic particle swarm optimization and least square-support vector machine // Chemometrics and intelligent laboratory systems. – 2015. – P.147-156.
8. Олейник Ан.А., Олейник Ал.А., Субботин С.А. Агентные технологии для отбора информативных признаков // Кибернетика и системный анализ. – 2012. – № 2. – С. 113-125.
9. Самигулина Г.А., Масимканова Ж.А. Обзор современных методов роевого интеллекта для решения задачи выделения информативных признаков при создании новых лекарственных препаратов // Проблемы информатики. – Новосибирск, 2016. – №2. – С. 50-61.
10. Самигулина, Г.А., Масимканова Ж.А. Выделение информативных признаков на основе муравьиных алгоритмов для иммуносетевого моделирования новых лекарственных препаратов // Труды XVIII Всесибирского семинара "Моделирование неравновесных систем (MNS-15)". – Красноярск, 2015. – С. 89-93.
11. Samigulina G.A., Samigulina Z.I. Drug Design of sulfanilamide based on Immune Network Modeling and Ontological approach // Proc. of the 10th IEEE Int. Conf. on Application of Information and Communication Technologies AICT2016. – Baku, 2016.

СПЕЦИАЛИЗИРОВАННАЯ МУЛЬТИАГЕНТНАЯ SMART-СИСТЕМА ДИСТАНЦИОННОГО ОБУЧЕНИЯ ЛЮДЕЙ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗРЕНИЯ

Самигулина Г. А., Нюсупов А.Т., Шаяхметова А.С.
galinasamigulina@mail.ru, moniumverse@outlook.com,
asemshayakhmetova@mail.ru

*Институт информационных и вычислительных технологий КН МОН РК,
Казахстан*

***Аннотация.** В статье рассматривается разработка специализированной мультиагентной smart-системы дистанционного обучения (ДО) для людей с ограниченными возможностями зрения (ЛОВЗ). Проанализированы практические приложения в ДО на основе интеллектуальных мультиагентных систем (МАС).*

Предложено комплексное решение для получения качественного инженерного образования ЛОВЗ в лабораториях коллективного пользования (ЛКП) на основе когнитивного, онтологического, статистического и интеллектуального подходов. Представлена структурная схема функционирования smart-системы ДО ЛОВЗ с использованием различных агентов, которые реализованы на основе системного подхода и мультиагентной платформы Java Agent Development Framework (JADE).

В настоящее время дистанционное обучение является одной из важных форм образования, которое в процессе становления объединило в себе все самое лучшее из педагогического и образовательного опыта [1]. В связи с бурным развитием вычислительной техники и искусственного интеллекта активно разрабатываются современные инновационные технологии ДО для улучшения качества и повышения эффективности обучения. Внедрение современных подходов и технологий улучшает качество обучения и повышает его эффективность. Перспективным являются ДО на основе интеллектуальных систем и smart-технологий, которые обладают широкими возможностями для обеспечения высокого уровня обучения. Такие smart-системы ДО предоставляют эффективную среду обучения на основе искусственных нейронных сетей [2], эволюционных алгоритмов, искусственных иммунных систем и используются для прогнозирования результатов обучения, анализа многомерных данных, выделения информативных признаков, статистической обработки данных [3, 4] и т.д.

В современном ДО актуальной является необходимость получения качественного инженерного образования с использованием современного оборудования в ЛКП для людей с различными ограниченными возможностями [5, 6]. Данная категория людей сталкивается с трудностями обучения в традиционных системах ДО и нуждается в создании специализированных систем [7]. Особенно важной задачей является организация специальной доступной среды ДО для людей с нарушениями зрения, так как данный вид обучения подразумевает длительную работу с компьютером, что сильно повышает нагрузку на зрительный аппарат и снижает уровень осознания учебной информации.

При разработке современных smart-систем ДО широко применяются мультиагентные системы, которые успешно решают задачи, связанные с обработкой больших данных и оптимальным распределением вычислительных ресурсов при организации ДО. При разработке мультиагентных smart-систем ДО создаётся совокупность агентов с необходимыми функциями. Ряд публикаций посвящён разработке мультиагентных систем ДО. В работе [8] предложена интеллектуальная система обучения на основе APLe (Agents for Personalized Learning), которая позволяет проводить обучение с учетом предпочтений обучающегося. Чтобы обеспечить построение индивидуальной траектории обучения с учетом интеллектуальных и психофизических особенностей обучающихся в ДО, применяются МАС на основе когнитивных и онтологических подходов [9, 10]. В статье [11] описаны агенты, созданные на основе онтологического подхода, которые выступают в качестве ассистентов по выбору изучаемого материала. Мультиагентная система помогает студенту подобрать необходимый для него материал для обучения на основе сбора и обработки информации с использованием онтологических моделей. В работе [12] описывается интеллектуальная система (CELTS, Conscious-Emotional-Learning-Tutoring-System) с использованием когнитивного агента. Применение когнитивного обучающего агента основывается на использовании соответствующих эмоциональных шаблонов для взаимодействия с обучаемым. В статье [13] предложена архитектура мультиагентной

онтологической системы дистанционного обучения, которая базируется на трех агентах: персональном агенте, агенте-координаторе и агенте обучающих ресурсов.

Агентно-ориентированный подход также применяется в информационных системах университетов и для связи с государственными учреждениями. В работе [14] описывается объединённая мультиагентная информационная система университета IABUIS (Integrated Agent-based University Information System), которая включает в себя четыре модуля: систему управления администрированием студента (SAMS, Student Administration Management System), систему информационной библиотеки (LIS, Library Information System), систему дистанционного обучения (DLS, Distance Learning System) и систему информационного управления университетом (UMIS, University Management Information System). Все системы функционируют взаимосвязано, обеспечивая слаженную работу всех процессов образовательной среды.

Для построения мультиагентной среды ДО используются различные агентные платформы (АП). Наиболее известными платформами являются: JADE (Java Agent Development Framework), Jack Intelligent Agents, MadKIT (Multi-Agent Development Kit), AgentBuilder, Cougaar (Cognitive Agent Architecture), MASON (Multi-Agent Simulator Of Neighborhoods), CogniTAO, Adaptive Modeler и др. Одной из широко распространенных программных сред для разработки МАС является JADE, написанная на языке Java [15]. Основой данной системы является программная среда, без которой невозможно существование агентов. Внутри среды формируются контейнеры, в которых функционируют агенты. После запуска каждый агент должен передать данные о себе в один из контейнеров, чтобы зарегистрироваться в системе. Далее программная среда будет наблюдать за работой всей системы и при необходимости производить требуемые управляющие воздействия на отдельных агентов. Между собой агенты обмениваются при помощи сообщений на языке ACL, который поддерживает современные стандарты передачи данных. Сообщения могут носить разный характер: запрос, информирование, передача данных и т.д.

Разработано большое количество МАС на основе платформы JADE. В статье [16] показана мультиагентная модель приложения, которая применяется для индексации поиска и подачи рекомендательных учебных материалов, хранящихся на различных серверах. Данная модель разрабатывается с помощью агентной платформы JADE и стандарта метаданных LOM (Learning Object Metadata), которая имеет иерархическую структуру и обеспечивает быстрый доступ к заложенной информации. Технология мультиагентов повышает точность и релевантность поиска. В статье [17] показана система моделирования информационных процессов с использованием JADE. Используется библиотека, которая интегрируется в JADE и позволяет осуществлять правильное распределение ресурсов. В результате сравнительных тестов было доказано, что в практической реализации данное моделирование на основе агентов показывает наилучшие результаты.

Постановка задачи формулируется следующим образом: необходимо реализовать мультиагентную smart-систему на основе платформы JADE (Java Agent Development Framework) для дистанционного обучения людей с ограниченными возможностями зрения, с целью получения качественного инженерного образования в лабораториях коллективного пользования.

Введем следующее определение: в качестве лабораторий коллективного пользования рассматриваются любые лаборатории, имеющие полную инфраструктуру (современное оборудование, техническое и программное обеспечение) для

осуществления дистанционного обучения и получения качественного инженерного образования людьми с ограниченными возможностями зрения.

При разработке мультиагентной smart-системы ДО актуально использование различных агентов на основе применения когнитивного, онтологического, статистического и интеллектуального подходов.

При проектировании мультиагентной системы ДО ЛОВЗ созданы следующие агенты: персональный, когнитивный, онтологический, статистический, интеллектуальный, агент помощи, менеджер, здоровья, ЛКП и государственный агент. Структурная схема мультиагентной smart-системы ДО ЛОВЗ, которая состоит из созданных агентов приведена на рисунке 1.

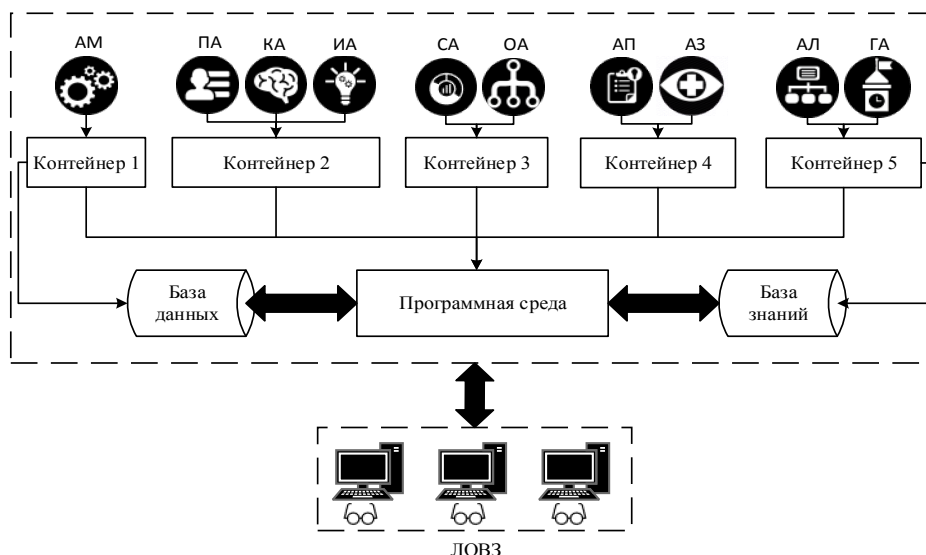


Рис.1 Структурная схема мультиагентной smart-системы ДО ЛОВЗ в JADE

Каждый агент в smart-системе ДО выполняет определенную функцию. Персональный агент (ПА) регистрирует персональные данные, собирает индивидуальные характеристики (признаки) ЛОВЗ и выбирает траекторию обучения ЛОВЗ с учетом дефектов зрения, а также подбирает нужный учебный материал. Менеджер агент (МА) следит за потоками сообщений от других агентов, чтобы осуществлять правильную взаимосвязь между ними. Онтологический агент (ОА) выполняет построение OWL модели ЛОВЗ, а также структурирует входные и выходные данные системы. Когнитивный агент (КА) предназначен для выявления уровня восприятия информации ЛОВЗ при миопии, гиперметропии, с глубокими и умеренными нарушениями зрения, а также реализации когнитивных методик обучения. Статистический агент (СА) учитывает динамику ДО пользователей, производит запись логов событий, системных ошибок и осуществляет выделение информативных признаков ЛОВЗ на основе факторного анализа. Интеллектуальный агент (ИА) определяет уровень обучения на основе нечеткой логики и прогнозирует результаты обучения ЛОВЗ с помощью нейро-нечеткой логики. Агент лаборатории коллективного пользования (АЛ) осуществляет подключение ЛОВЗ к ЛКП и доступ к современному оборудованию. Агент здоровья (АЗ) предоставляет комплекс лечебной гимнастики для глаз и предлагает индивидуальный режим работы на компьютере с учетом особенностей зрения. Агент помощник (АП) посредством подсказок и уведомлений помогает студентам в выборе материалов обучения. Государственный агент (ГА) осуществляет

взаимодействие с государственными учреждениями, предоставляет юридическую информацию пользователям и доступ к нормативно-правовой базе. агенты функционируют в программной среде, которая постоянно изменяется под воздействием деятельности ЛОВЗ в системе. Для программирования конфигурации созданных агентов используется среда, включающая в себя классы и библиотеки платформы JADE. Созданы 5 контейнеров в которых помещены соответствующие агенты: контейнер 1 (АМ), контейнер 2 (ПА, КА, ИА), контейнер 3 (СА, ОА), контейнер 4 (АП, АЗ), контейнер 5 (АЛ, ГА).

Далее в таблице 1 приведено описание созданных агентов.

Таблица 1. Описание агентов МАС ДО ЛОВЗ

Название агента	Описание
1	2
Персональный агент	1 Регистрация либо авторизация пользователя в smart-системе ДО ЛОВЗ. 2 Загрузка профиля с траекторией обучения текущего пользователя. 3 Построение траектории обучения пользователя. 4 Формирование интерфейса обучения. 5 Загрузка обработанной информации в базу данных и базу знаний. 6 Активизация контейнера 2. 7 Функционирование в программной среде.
Менеджер агент	1 Установка связи с агентами. 2 Выполнение асинхронной передачи сообщений от других агентов. 3 Осуществление организации режима подачи информации. 4 Координация работы агентов. 5 Активизация контейнера 1. 6 Функционирование в программной среде.
Онтологический агент	1 Формирование ОМ ЛОВЗ. 2 Формирование ОМ обучения. 3 Формирование ОМ ЛКП. 4 Активизация контейнера №2. 5 Выбор класса обучения. 6 Активизация контейнера №5. 7 Выбор курса. 8 Интерактивные элементы курса. 9 Активизация контейнера №3. 10 Функционирование в программной среде.

Когнитивный агент	1 Выделение психофизиологических признаков ЛОВЗ на основе анкетирования: - тест Айзенка; - тест Амтхауэра; - специальные таблицы для определения остроты и дефектов зрения. 2 Формирование среды восприятия информации. 3 Подача учебной информации с экрана монитора: - режим миопии; - гиперметропии; - при глубоком и умеренном нарушениях зрения; - режим нормального зрения. 4 Выбор цвето-схем: - выбор фона бледно-желтого, бледно-зеленого цвета для режима миопии; - выбор фона ярко-желтого, ярко-оранжевого цвета для режима гиперметропии; - выбор фона белый текст и черный фон для режима при глубоком и умеренном нарушениях зрения; - режим нормального зрения.
	5 Расположение учебной информации: - в левой верхней части экрана при миопии; - в правой нижней части экрана при гиперметропии. 6 Озвучивание. 7 Предпочтительное время суток для лучшего усвоения информации. 8 Активизация контейнера №2. 9 Загрузка обработанной информации в базу данных. 10 Функционирование в программной среде.
Статистический агент	1 Обработка многомерных данных. 2 Выделение информативных признаков ЛОВЗ и факторный анализ данных. 3 Сбор статистических данных о просмотренных материалах обучения за определённый промежуток времени. 4 Сведения о системных ошибках. 5 Загрузка полученной информации в базу данных и знаний. 6 Активизация контейнера 3. 7 Функционирование в программной среде.
Интеллектуальный агент	1 Определение уровня знаний ЛОВЗ. 2 Прогнозирование данных на основе нейро-нечеткой логики. 3 Выдача ЛОВЗ сертификата о прохождении курса либо перенаправление его на повторное обучение. 4 Загрузка полученной информации в базу данных и базу знаний. 6 Активизация контейнера 2. 7 Функционирование в программной среде.

Агент лаборатории коллективного пользования	1 Обеспечение доступа в ЛКП. 2 Современное оборудование: - вычислительный кластер; - лаборатория с промышленным оборудованием. 3 Создание виртуальной машины. 4 Установка программного обеспечения (ПО) и получение заданий. 5 Выполнение вычислений. 6 Программирование логических контроллеров. 7 Проверка и отладка созданного ПО ЛОВЗ с учителем и без учителя. 8 Получение результатов моделирования. 9 Доступ и работа с реальным оборудованием. 10 Активизация контейнера №5. 11 Загрузка полученной информации в базу данных. 12 Функционирование в программной среде.
Агент здоровья	1 Определение режима обучения по времени для различных заболеваний. 2 Выбор комплекса упражнений при миопии. 3 Выбор комплекса упражнений при гиперметропии. 4 Выбор комплекса упражнений при глубоком и умеренном нарушениях зрения. 5 Активация контейнера №4. 6 Функционирование в программной среде.
Агент помощник	1 Определение текущей страницы обучения. 2 Формирование подсказок на странице обучения и выдача подсказок по запросу. 3 Активизация контейнера 4. 4 Функционирование в программной среде.
Государственный агент	1 Организация доступа в базу знаний ВУЗов: - эл. библиотеки; - каталоги; - интеллектуальные элементы курса. 2 Организация доступа в юридическую базу данных: - законы; - акты; - нормативные документы. 3 Организация доступа на сайты гос.учреждений: - сайт МОН РК; - сайт ККСОН МОН РК; - сайт эл. правительства РК. 4 Активизация контейнера №5. 5 Функционирование в программной среде.

Таким образом, к основным достоинствам применения разработанной специализированной Smart-системы ДО для ЛОВЗ на основе многофункциональных агентов является гибкость функционирования, оперативное взаимодействие между агентами, построение индивидуальной траектории обучения с учетом психофизиологического и интеллектуального уровня обучающихся, возможность не

случайно выбирать стратегию поведения агентов, а учитывать опыт предыдущего взаимодействия с обучающей средой, возможность автономной работы агентов, оптимальное распределение вычислительных ресурсов, адаптация обучающихся в условиях динамической среды, возможность самообучаться и решать узконаправленные и глобальные задачи в обучении, а также высокая самоорганизованность и многофункциональность.

Работа выполнена по гранту КН МОН РК №ГР0115РК00536 по теме: «Разработка интеллектуальных технологий, алгоритмов и программно-аппаратного обеспечения для интеллектуальных систем управления сложными объектами в условиях параметрической неопределенности» (2015-2017 г.г.).

Литература

1. O. Zawacki-Richter. Distance Education // Encyclopedia of Educational Philosophy and Theory. – Singapore: Springer Science, 2015. – P. 1-7.
2. G. Samigulina, Z. Samigulina. Intelligent System of Distance Education of Engineers based on Modern innovative Technologies // Proceedings of the II International Conference on Higher Education Advances, HEAd'16. J. Social and Behavioral Sciences. - Valencia, Spain: Elsevier, 2016. - № 228. - P. 229–236.
3. V. Tikhomirov, N. Dneprovskaya, E. Yankovskaya. Three Dimensions of Smart Education // Smart Education and Smart e-Learning. – Switzerland: Springer International Publishing, 2015. – P. 47-56.
4. V. Štuikys. Smart Education in CS: A Case Study // Smart Learning Objects for Smart Education in Computer Science. – Switzerland: Springer International Publishing, 2015. – P. 287-310.
5. J.P. Bakken, V.L. Uskov, A. Penumatsa, A. Doddapaneni. Smart Universities, Smart Classrooms and Students with Disabilities // Smart Universities, Smart Classrooms and Students with Disabilities. – Switzerland: Springer International Publishing, 2016. – P. 15-27.
6. N. Nikashina. Particular of development people with confined eyesight // Vector of science, 2012. -Vol. 2 (9). - P. 223 –226.
7. Samigulina G. A., Shayakhmetova A. S. The information system of distance learning for people with impaired vision on the basis of artificial intelligence approaches // Proceedings of the II International conference on Smart Education and E-learning. – Italy, Sorrento: Springer, 2015. – P. 255-265.
8. Stamatis P., Panagiotopoulos I., Goumopoulos C., Kameas A. APLe: Agents for Personalized Learning in Distance Learning // Computer Supported Education. – Switzerland: Springer International Publishing, 2016. – P. 37-56.
9. Roger A., Jason H., Gregory T., Melissa D., Reza F., François B., Ronald L. Using Trace Data to Examine the Complex Roles of Cognitive, Metacognitive, and Emotional Self-Regulatory Processes During Learning with Multi-agent Systems // International Handbook of Metacognition and Learning Technologies. – New York: Springer Science, 2013. – P. 427-449.
10. Samigulina G. A., Shayakhmetova A. S. Development of the Smart - system of distance learning visually impaired people on the basis of the combined OWL model // Proceeding of the 3rd International KES Conference on Smart Education and E-learning (KES-SEEL-16). - Puerto de la Cruz, Tenerife, Spain:Springer, 2016. – P. 109-118.
11. Paula R., Néstor D., Demetrio A. Ovalle Multi-agent System for Knowledge-Based Recommendation of Learning Objects Using Metadata Clustering // Highlights of Practical Applications of Agents, Multi-Agent Systems and Sustainability. - The PAAMS Collection. – Switzerland: Springer International Publishing, 2015. – P. 356-364.

12. Chatzara K., Karagiannidis C., Stamatis D. Cognitive support embedded in self-regulated e-learning systems for students with special learning needs // Education and Information Technologies. – New York: Springer Science, 2014. – P. 283–299.
13. J.Clerk Maxwel. A Treatise on Electricity and Magnetism / 3rd ed., Vol. 2. - Oxford: Clarendon. - P.68-73.
14. Shuhua H., Xuemei S. The Study on University Library Information Service for Regional Characterized Economy Construction Based on Integrated Agent // Computer Supported Education. – Berlin: Springer – Verlag, 2013. – P. 289-294.
15. JADE Architecture Overview. <http://www.jade.tilab.com/>
16. R.L. RochaCampos, R.L. Comarella, R.A. Silveira. Multiagent Based Recommendation System Model for Indexing and Retrieving Learning Objects // Highlights on Practical Applications of Agents and Multi-Agent Systems. – Berlin: Springer - Verlag, 2012. – P. 328-339.
17. H.L. Cardoso. SAJaS: Enabling JADE-Based Simulations // Transactions on Computational Collective Intelligence XX. – Berlin: Springer - Heidelberg, 2013. – P. 387-398.

РАЗРАБОТКА ГРАФИЧЕСКИХ МОДЕЛЕЙ ДЛЯ ИНТЕЛЛЕКТУАЛЬНОГО АНАЛИЗА ДЕСКРИПТОРОВ СУЛЬФАНИЛАМИДОВ ПРИ СИНТЕЗЕ НОВЫХ ЛЕКАРСТВЕННЫХ ПРЕПАРАТОВ

Самигулина Г.А., Самигулина З.И.
e-mail: galinasamigulina@mail.ru, zarinasamigulina@mail.ru

*Институт информационных и вычислительных технологий КН МОН РК,
Казахстан*

Аннотация. В настоящее время открыто огромное количество структур химических соединений, обработка которых для синтеза новых лекарственных препаратов является трудоемкой задачей. В связи с этим актуально применение методов искусственного интеллекта и современного программного обеспечения. В статье представлена SDL диаграмма для интеллектуального анализа баз данных химической информации. Разработана графическая модель предварительной обработки дескрипторов сульфаниламидов в пакете прикладных программ Rapid Miner. Эксперименты проводились на основе химической информации ресурсов Mol-Instincts и PubChem. Получены результаты моделирования в 2D форме.

В связи с последними достижениями в области биоинформатики, хемоинформатики, химии, фармакологии и биомедицины в настоящее время открыто огромное количество структур химических соединений. По результатам только одной базы данных PubChem по состоянию на 2017 год, открыто 9 157 6624 компонентов, протестированных 2 395 818 компонентов, биоактивных соединений 233 481 319. Таким образом, мировые тенденции в области исследования структур химических соединений заключаются в применении методов искусственного интеллекта и статистического

анализа данных, а также специализированных интеллектуальных сред для работы с большими данными.

Широко применяются такие методы как: нейронные сети [1], генетические алгоритмы [2], искусственные иммунные системы [3], метод опорных векторов [4], метод «ближайшего соседа» [5] и т.д. Большинство алгоритмов, решающих задачи классификации во многом зависят от исходного набора данных. Чем лучше данные, тем точнее результаты классификации. В связи с этим актуальна предварительная обработка баз данных химической информации. Для решения данной проблемы хорошо зарекомендовали себя алгоритм на основе ансамбля деревьев решений [6,7], метод главных компонент, метод на основе сингулярного разложения и т.д. Поскольку в настоящее время не существует универсальных методов для интеллектуального анализа химической информации, целесообразно применение комплексного подхода при синтезе новых лекарственных препаратов.

Постановка задачи исследования формируется следующим образом: необходимо разработать графическую модель в среде Rapid Miner для реализации комплексного подхода при исследовании больших баз данных химической информации с применением различных алгоритмов предварительной обработки данных и решения задачи классификации.

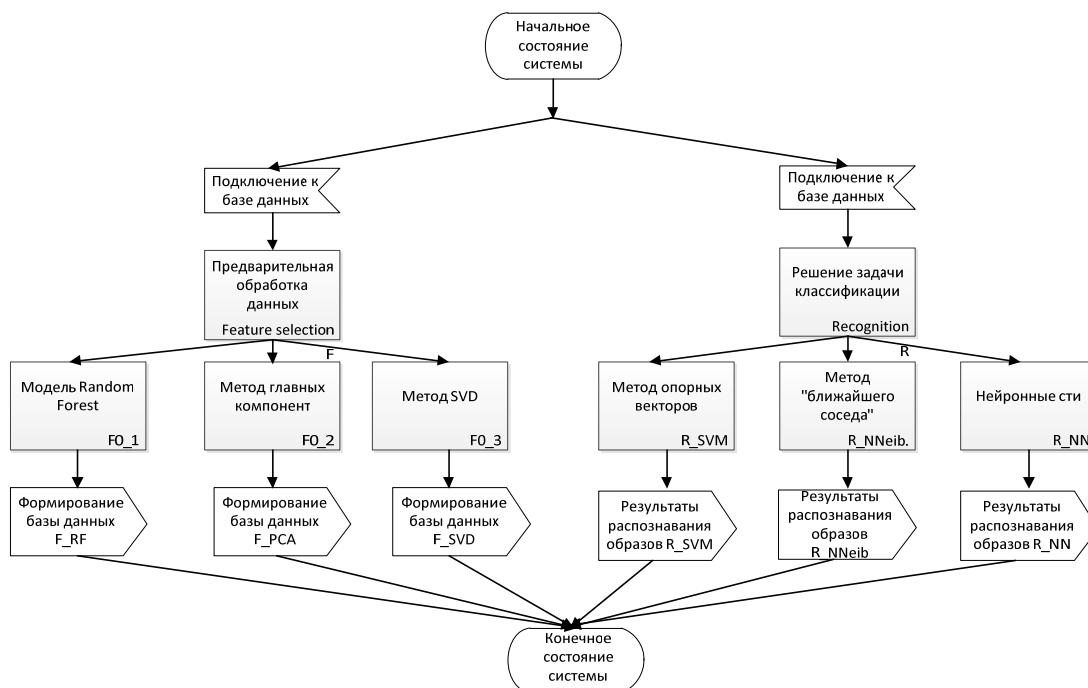


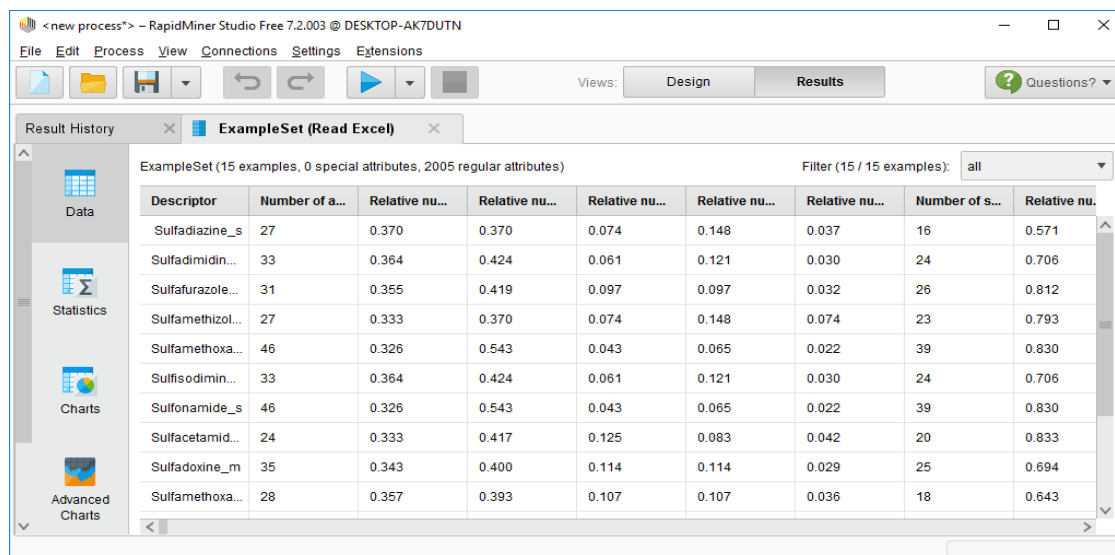
Рис. 1 SDL диаграмма интеллектуального анализа химической информации при синтезе новых лекарственных препаратов

Для решения поставленной задачи на рисунке 1 представлена SDL (Specification and Description Language) диаграмма описания спецификаций параллельных процессов, которые состоят из двух основных этапов: предварительной обработки данных и решения задачи классификации. На этапе предварительной обработки данных формируются три базы данных: F_RF, F_PCA, F_SVD, которые содержат сокращенные наборы данных химической информации после обработки методами на основе

алгоритма Random Forest, метода главных компонент и сингулярного разложения матриц. Далее полученные базы данных поэтапно исследуются с помощью: метода опорных векторов (R_SVM), метода «ближайшего соседа» (R_NNeib) и нейронных сетей (R_NN). В результате осуществляется оценка эффективности применения данных алгоритмов на сформированных базах данных химической информации F_RF, F_PCA, F_SVD. В результате для дальнейших исследований выбирается алгоритм, показавший наилучшие результаты. Стратегия на основе применения сравнительного анализа позволяет подбирать траекторию исследований с учетом исходного характера базы данных химической информации.

В качестве программного обеспечения для разработки графических моделей выбрана программная платформа для научных исследований Rapid Miner, рассчитанная на работу с большими данными. В 2017 году Gartner Research разместила Rapid Miner в лидерах рейтинга «Magic Quadrant» среди платформ для ведения научных исследований. Особенностью программного обеспечения является единый пользовательский интерфейс, который поддерживает полностью аналитический процесс от подготовки данных до развертывания и текущего управления построенными моделями. Rapid Miner является средой визуального программирования, что позволяет увеличить производительность и повысить уровень интеллектуальной аналитики.

Рассмотрим работу фрагмента разработанной графической модели для предварительной обработки данных химической информации в среде Rapid Miner. В качестве базы данных, использовалась разработанная на основе ресурсов Mol-Instincts и PubChem база данных (БД) дескрипторов сульфаниламидов. Фрагмент загруженной БД представлен на рисунке 2. На рисунке 3 показан фрагмент разработанной графической модели для предварительной обработки базы данных химической информации, включающий в себя операторы чтения данных, заполнения пропущенных данных, алгоритмов предварительной обработки и специального оператора для оценки параметра weight (веса дескриптора). Чем больше вес дескриптора, тем более ценным он является для дальнейших исследований.



Descriptor	Number of a...	Relative nu...	Relative nu...	Relative nu...	Relative nu...	Relative nu...	Number of s...	Relative nu...
Sulfadiazine_s	27	0.370	0.370	0.074	0.148	0.037	16	0.571
Sulfadimidin...	33	0.364	0.424	0.061	0.121	0.030	24	0.706
Sulfafurazole...	31	0.355	0.419	0.097	0.097	0.032	26	0.812
Sulfamethizol...	27	0.333	0.370	0.074	0.148	0.074	23	0.793
Sulfamethoxa...	46	0.326	0.543	0.043	0.065	0.022	39	0.830
Sulfisodimin...	33	0.364	0.424	0.061	0.121	0.030	24	0.706
Sulfonamide_s	46	0.326	0.543	0.043	0.065	0.022	39	0.830
Sulfacetamid...	24	0.333	0.417	0.125	0.083	0.042	20	0.833
Sulfadoxine_m	35	0.343	0.400	0.114	0.114	0.029	25	0.694
Sulfamethoxa...	28	0.357	0.393	0.107	0.107	0.036	18	0.643

Рис.2 Фрагмент БД дескрипторов сульфаниламидов в среде Rapid Miner

С помощью специальной функции Rapid Miner можно отследить структуру потока данных в графической модели (рис. 4.).

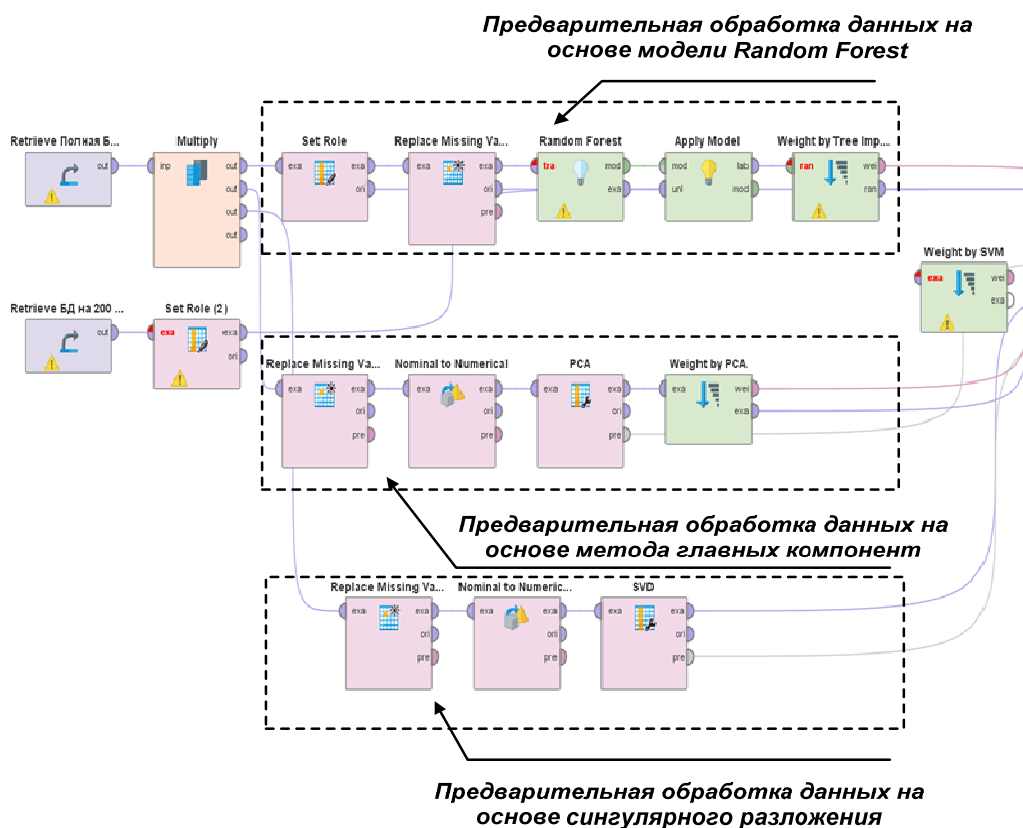


Рис. 3 Фрагмент графической модели для предварительной обработки данных БД дескрипторов сульфаниламидов

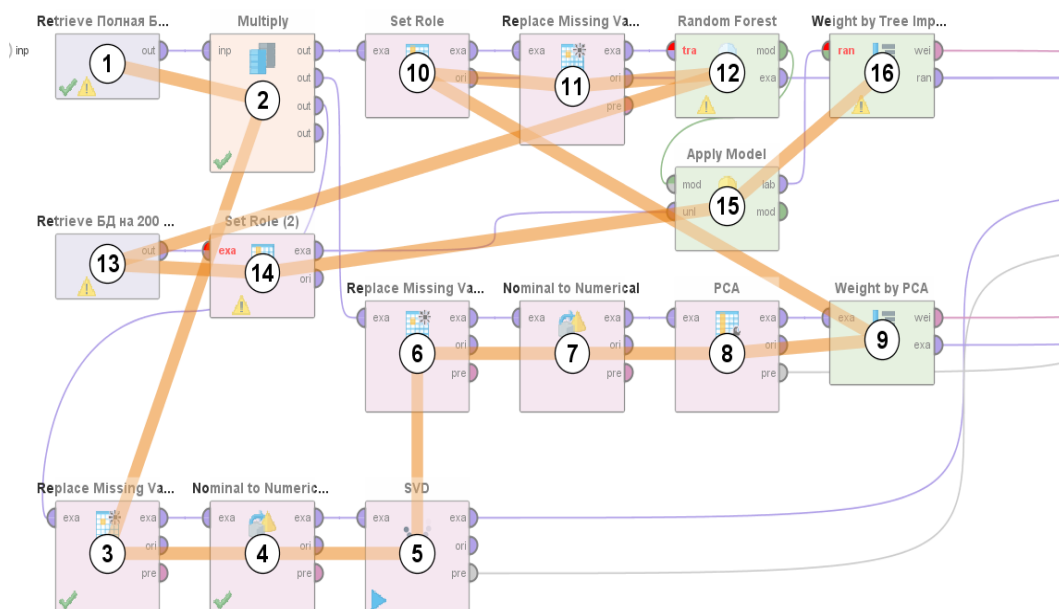


Рис. 4 Структура потока данных в графической модели в среде Rapid Miner

Далее по результатам моделирования фрагмента графической модели с предварительной обработкой данных и оценки работы каждого алгоритма с помощью оператора «Performance» наиболее эффективной себя показала модель Random Forest (рисунок 5). В представленном фрагменте дескрипторы (Gravitation index, mean electro topological state, c root of Gravitation index, Number of atomic bonds) имеют наибольший вес (weight) и являются наиболее информативными.

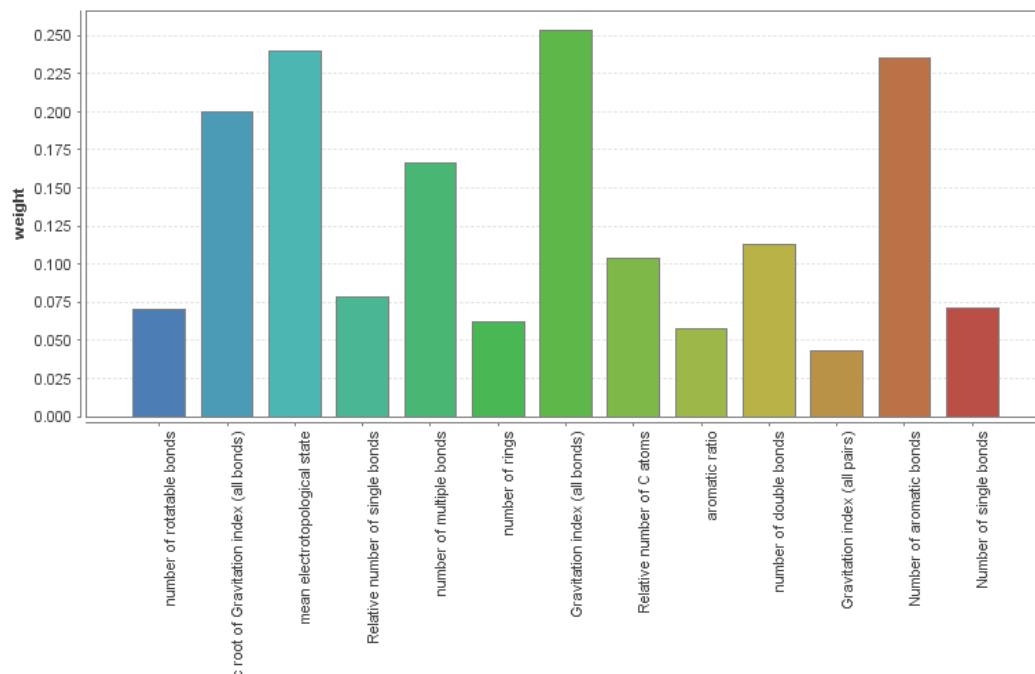


Рис. 5 Ранжирование переменных по степени значимости на основе алгоритма Random Forest при исследовании графической модели Rapid Miner

Аналогичным образом осуществляется разработка графической модели для решения задачи классификации на основе метода опорных векторов, нейронных сетей и метода «ближайшего соседа». Полученные результаты предварительной обработки данных используются для дальнейших исследований предложенными методами.

Таким образом, применение графических моделей для синтеза новых лекарственных препаратов позволяет проводить комплексные исследования и обрабатывать огромные массивы баз данных химической информации на базе платформы ведения научных исследований Rapid Miner. Особенностью разработанных графических моделей и программного обеспечения Rapid Miner является возможность работы с реальными данными.

Работа выполнена по гранту №ГР 0115РК00549 МОН РК по теме: Компьютерный молекулярный дизайн лекарственных препаратов на основе иммуносетевого моделирования (2015-2017 гг.).

Литература

1. Montañez-Godínez N., Martínez-Olguín A.C., Deeb O., Garduño-Juárez R., Ramírez-Galicia G. QSAR/QSPR as an Application of Artificial Neural Networks // Artificial Neural Networks. – Springer, 2014. – Vol. 1260. – P.319-333.

2. Fernandez M., Caballero J., Fernandez L., Sarai A. Genetic algorithm optimization in drug design QSAR: Bayesian-regularized genetic neural networks (BRGNN) and genetic algorithm-optimized support vectors machines (GA-SVM) // Molecular Diversity. – Springer, 2011. – Vol.15, №1. – P. 269-289.
3. Ivanciuc O. Artificial immune system classification of drug-induced torsade de pointes with AIRS (artificial immune recognition system) // Internet Electron. J. Mol. Des. – 2006. – № 5. – P. 488–502.
4. Liu F., Zhou Z. A new data classification method based on chaotic particle swarm optimization and least square-support vector machine // Chemometrics and intelligent laboratory systems. – 2015. – P.147-156.
5. Chikh M.A., Saidi M. Diagnosis of Diabetes Diseases Using an Artificial Immune Recognition System2 (AIRS2) with Fuzzy K-nearest Neighbor // Journal of Medical Systems. – 2012. – Vol. 36, №5. – P. 2721-2729.
6. Hapfelmeier A., Ulm K. Variable selection by Random Forests using data with missing values // Computational Statistics & Data Analysis. – Elsevier, 2014. – Vol.80. – P. 129-139.
7. Samigulina G.A., Samigulina Z.I. Immune Network Technology on the Basis of Random Forest Algorithm for Computer-Aided Drug Design // Proceedings of the 5th International Work-Conference, IWBBIO 2017, Bioinformatics and Biomedical Engineering. - Granada, Spain, 2017. – Vol. 10208. – P. 50-61.

КЛЕТОЧНЫЕ АВТОМАТЫ

Сатымбеков М.Н., Нуржанов Ч.А.
e-mail: m_satymbekov@mail.ru

*Институт информационных и вычислительных технологий КН МОН РК,
Казахстан*

***Аннотация.** Один из крупнейших специалистов в области информатики — Марвин Минский [1] считает, что самым важным при этом, видимо, является изучение различных путей возникновения сложного поведения при использовании простых устройств, действий, описаний или концепций. Нам кажется, что не существует ничего более подходящего для этой цели, чем клеточные автоматы.*

В последние десятилетия проводился ряд исследований, посвященных анализу динамических систем. К этой области, в частности, относится теория самовоспроизводящихся структур [2]. Однако использование в ней формализма, основанного на решении рекуррентных нелинейных уравнений и связанного с применением теории функций комплексных переменных, является нетривиальным подходом. Был предложен другой способ построения самовоспроизводящихся структур, основанный на применении рекурсивных процедур при написании программ, не упрощающий, однако, понимания процессов вычислений [3].

Клеточные автоматы

Клеточные автоматы были предложены в работе фон Неймана [6]. Большой интерес к ним вызван тем, что такие автоматы являются универсальной моделью параллельных вычислений подобно тому, как машины Тьюринга являются универсальной моделью для последовательных вычислений [7].

Клеточный автомат — дискретная динамическая система, представляющая собой совокупность одинаковых клеток, одинаково соединенных между собой. Все клетки образуют так называемую решетку клеточного автомата. Эти решетки могут быть разных типов и отличаться как по размерности, так и по форме клеток. В настоящей работе каждая клетка — это конечный автомат, состояние которого определяется состояниями соседних клеток и, возможно, ее собственным. В клеточных автоматах, как в моделях вычислений, не рассматриваются входные и выходные воздействия. При аппаратной реализации клеточные автоматы обычно называют однородными структурами [8]. В общем случае клеточные автоматы обладают следующими свойствами.

- **Изменения значений всех клеток происходят одновременно** после вычисления нового состояния каждой клетки решетки.
- **Решетка однородна** - невозможно различить какие-либо две области решетки по ландшафту.
- **Взаимодействия локальны.** Лишь клетки окрестности (как правило, соседние) способны повлиять на данную клетку.
- **Множество состояний клетки конечно.**

Клеточные автоматы можно реализовать разными способами. В данной работе применен такой подход.

Вводятся два массива для хранения состояний клеток: первый из них содержит текущее состояние каждой клетки, второй предназначен для хранения нового ее состояния.

Определяется функция переходов клетки решетки. Для выявления следующего ее состояния в качестве параметров в функцию переходов передаются текущие значения состояний клеток окрестности, возможно, включая ее саму. Эта функция будет задана в виде булевой формулы.

На нулевом шаге решетка (первый массив) заполняется начальными данными, что полностью определяет поведение системы для выбранных решетки и функции переходов клетки.

Вычисления новых состояний вводится цикл. На каждой итерации для любой клетки, используя в качестве переменных элементы первого массива, определяется ее новое состояние, помещаемое во второй массив. Значения аргументов функции переходов берутся из первого массива.

По завершении итерации значения из всех элементов второго массива переносятся в первый, что обеспечивает синхронное изменение значений состояний всех клеток решетки.

Визуализируется содержимое решетки. В зависимости от ее размерности (одномерная или двумерная) отображение решетки производится по-разному.

Двумерные клеточные автоматы

В двумерном (плоскостном) клеточном автомате решетка реализуется двумерным массивом. В ней каждая клетка имеет восемь соседей. Для устранения краевых эффектов

решетка так же, как и в предыдущем случае, «заворачивается» в тор. Это позволяет использовать для всех клеток автомата соотношение:

$$y'[i][j] = f(y[i][j], y[i-1][j], y[i-1][j+1], y[i][j+1], y[i+1][j+1], y[i+1][j], y[i+1][j-1], y[i][j-1], y[i-1][j-1]).$$

Пример 1. Наиболее известным из двумерных клеточных автоматов является автомат, моделирующий игру «Жизнь» [9]. В нем, как и во всех рассмотренных выше, клетки могут находиться в двух состояниях. Функция переходов клеток реализует следующие условия:

- если данная клетка мертва (находится в состоянии "ноль"), то она оживет (перейдет в состояние "единица") при условии, что у нее имеются три живых соседа;
- если данная клетка жива, то она останется живой только при условии, что у нее есть два или три живых соседа, в противном же случае она умрет.

В этой игре интересно наблюдать за развитием популяции клеток при различных начальных условиях. В качестве примера самовоспроизведения рассмотрим клеточный автомат, функционирующий по правилу:

$$y'[i][j] = y[i][j] \wedge y[i-1][j] \wedge y[i-1][j+1] \wedge y[i][j+1] \wedge y[i+1][j+1] \wedge y[i+1][j] \wedge y[i+1][j-1] \wedge y[i][j-1] \wedge y[i-1][j-1].$$

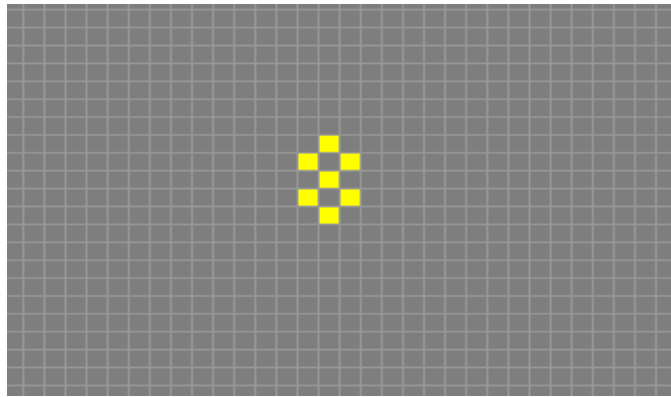


Рис. 1. Начальная конфигурация

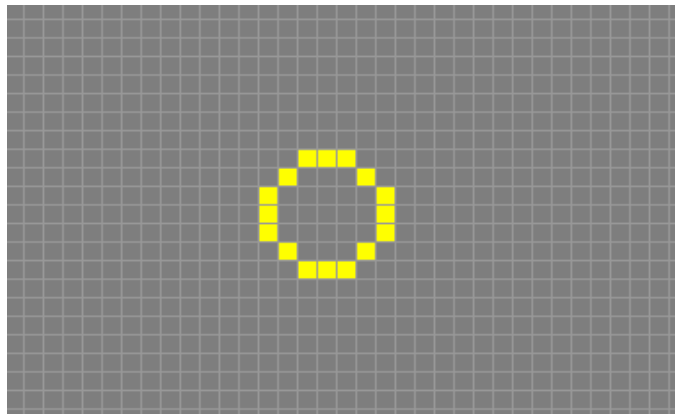


Рис. 2. Конфигурация через 6 итераций

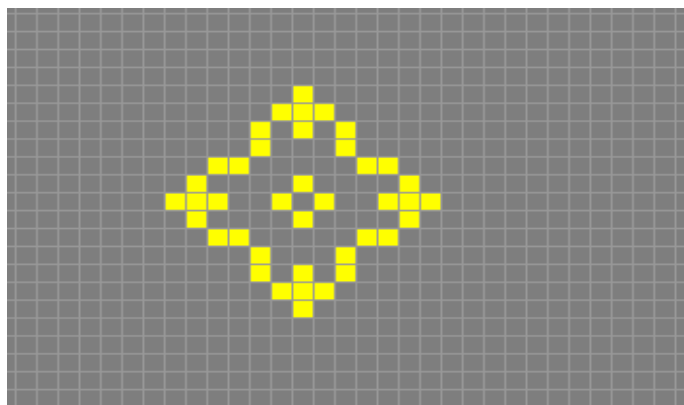


Рис. 3. Конфигурация через 11 итераций

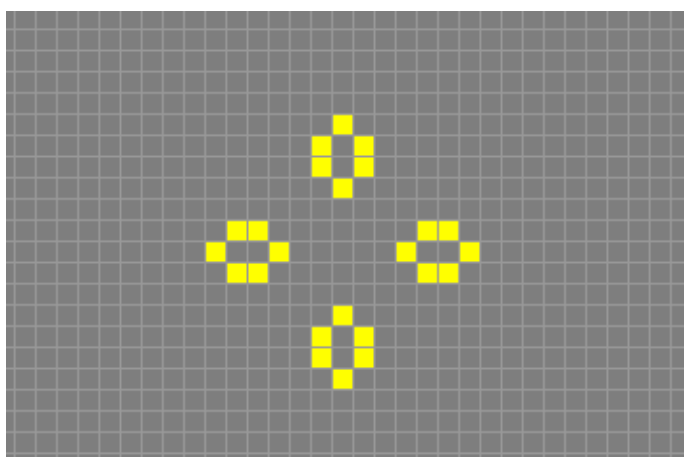


Рис. 4. Конфигурация через 28 итераций

На рис. 1 приведена начальная конфигурация решетки, а на рис. 2 — результат ее самовоспроизведения через шесть шагов.

Необходимо отметить, что вследствие свойств функции «сумма по модулю два» самовоспроизведение имеет место после любого числа шагов, являющегося степенью двух, начиная со значения, определяемого соотношением:

$$T = 2^{\lceil \log_2(\max(a;b)) \rceil},$$

где a и b — ширина и высота «зародыша» соответственно.

Для начальной конфигурации, изображенной на рис. 5, $a = 3$, $b = 5$. Поэтому $T = 8$, и, следовательно, самовоспроизведение имеет место через 8, 16, 32, 64 и т. д. шагов.

Литература

1. Минский М. Вычисления и автоматы. М.: Мир, 1971.
2. Пайтген Х.О., Рихтер П.Х. Красота фракталов. Образы комплексных динамических систем. М.: Мир, 1993.
3. Вирт Н. Алгоритмы и структуры данных. СПб.: Невский диалект, 2001.
4. Пригожин И., Стенгерс И. Порядок из хаоса. Новый диалог человека с природой. М.: Эдиториал УРСС, 2000.
5. Пайс А. Гении науки. М.: Институт компьютерных исследований, 2002.

6. Мигдал А.Б. Красота в науке. М.: Молодая гвардия, 1979.
7. Тоффли Т., Марголус Н. Машины клеточных автоматов. М.: Мир, 1991.
8. фон Нейман Дж. Теория самовоспроизводящихся автоматов. М.: Мир, 1971.

НЕКОТОРЫЕ ФИЛОСОФСКИЕ АСПЕКТЫ ИСЧИСЛЕНИЯ ПОНЯТИЙ

И.Э. Сулейменов^{1,2}
E-mail: esenych@ya.ru

¹Институт вычислительных и информационных технологий МОН РК

²Алматинский университет энергетики и связи

***Аннотация.** Обсуждаются философские аспекты попыток создать логический формализм (исчисление понятий), приближающийся по характеру к рассуждениям, осуществляемым человеческим сознанием. Показано, что для создания такой разновидности исчисления понятий, необходимо учитывать сетевые свойства естественных и искусственных языков, которые в философской литературе ранее трактовались через категорию «внетекстовых структур», понимаемых в духе Ю.М. Лотмана и У. Эко. Корректное истолкование существования внетекстовых структур дается на основе предложенной ранее трактовки сложной системы любой природы как формирующей новое качество, природа которого может быть истолкована на основании аналогии с нейронной сетью. С этой точки зрения любой язык также обладает коммуникационной оболочкой, представляющей собой аналог нейронной сети.*

Вопрос о базовых концепциях логики как самостоятельной научной дисциплины в настоящее время приобретает неожиданное звучание в связи с появлением целого ряда научных направлений, которые используют построения, во многом отличающиеся от тех, что положены в основу классической логики. К ним, в частности, относится аппарат нечеткой логики [1,2], многочисленные попытки построить исчисление высказываний, оперирующее категориями модальности [3-5] и т.д. Следуя идеям М. Клайна [6], допустимо утверждать, что логик, как и математик в настоящее время существует достаточно много и они отличаются между собой не только используемой аксиоматикой или базовыми положениями, но и базовыми схемами, в соответствии с которыми строятся рассуждения. Разработка логик, отличающихся от классической, представляет не только академический, но и сугубо прикладной интерес, в частности, для разработки прогностических систем и систем управления, обеспечения машинного перевода и решения иных лингвистических задач [2,7-9].

С максимально общих позиций, логику, соответственно, допустимо рассматривать как результат формализации того или иного способа рассуждений, который может строиться по различным схемам. Уместно подчеркнуть, что используемые схемы рассуждений не обязательно должны включать в себя критерий истинности в качестве единственного средства, позволяющего судить об их адекватности. Так, способ рассуждений, приводящий к построению любой научной гипотезы (шире – приводящий к формированию любого предположения) очень редко оперирует понятием доказательности. По крайней мере, это относится к начальному этапу, на которой

собственно гипотеза и формируется. Верификация гипотезы, как правило, представляет собой отдельную задачу, которая решается на конечном этапе.

Лучшей иллюстрацией к сказанному является классической схема построения геометрии, дошедшей до нас со времен античности. Логика – понимаемая в том смысле, который ей придавал Аристотель – используется для доказательства теорем, т.е. для верификации конкретных высказываний, но данная схема ничего не говорит о способе рассуждений, благодаря которому появляется на свет собственно формулировка доказываемой теоремы. Этот способ остается за рамками изложения; по умолчанию предполагается, что формулировка теоремы представляет собой некий акт творчества теоретика, механизм которого классическая логика не раскрывает и раскрыть не берется.

Разумеется, формализация процесса творчества вряд ли возможна, точнее такая формализация фактически будет означать создание предпосылок для появления искусственного сознания, что на данном этапе исследований вряд ли можно считать актуальной задачей, хотя вопрос о создании искусственного интеллекта у. Однако, приведенный выше краткий обзор существующих научных направлений показывает, связанных, в том числе, с разработкой аппарата нечеткой логики [7-9], показывает, что актуальным является разработка альтернатив (логик, построенных на иных основаниях, нежели логика Аристотеля), которые будут все в большей степени приближаться к тому способу рассуждений, которое реально используется любым человеком в процессе его мыслительной деятельности. Разработка таких логик, ожидаемо, требует и философского осмысления схем, по которым строятся рассуждения [10].

Показательными в этом отношении являются работы К. Льюиса [11] и его последователей [12-14], разрабатывавших аппарат логики, оперирующей категориями модальности. В данных работах, в частности, предпринимались попытки приблизить понятие импликации к тому, что существует в обыденном языке.

В обыденном языке импликация « $p \supset q$ » трактовалась и трактуется как «если p , то q » или « p влечет за собой q ». Однако было бы некорректно говорить, что импликация, понимаемая в духе Рассела и Уайтхеда (наиболее распространённая трактовка, отраженная в многочисленных учебниках по математической логике), выражает именно это. Одним из первых, кто выступил с такой точкой зрения, был К. Льюис. Он утверждал, что « p имплицитует q » должно пониматься как « q дедуцируется (выводится) из p », но операция « $\supset$ », используемая Расселом и Уайтхедом, слишком слаба для описания выводимости одного высказывания из другого [11,14].

К. Льюис разработал исчисление высказываний, содержащее более сильную форму импликации – «строгую импликацию». Им было предложено несколько версий использования данной операции, каждая из которых соответствовала своей логической системе (от $S1$ до $S5$ в терминологии К. Льюиса).

Детали здесь не столь существенны, важно подчеркнуть, что, желая приблизить формальное понятие импликации к тому, что выражает и обыденный язык, и к тому, что математики и физики столетиями использовали на практике, К. Льюис был вынужден вводить целый ряд новых понятий. Строгую импликацию он описал через понятие возможности, которому не было места в построениях Рассела и Уайтхеда. По Льюису, « p строго имплицитует q » означает «конъюнкция p и не q невозможна». Неудивительно, что использование модального оператора «возможно» сразу же вызвало шквал критики, причем небезосновательной. А именно, модальные операторы не являются истинностно-функциональными. Не существует прямой (точнее, функциональной) связи между истинностью высказываний, и истинностью конструкции, которая из них строится при помощи модальных операторов.

Попытки усовершенствовать исчисление высказываний, содержащее модельные операторы, предпринимались неоднократно, в этом контексте часто упоминается имя Я.Лукасевича [12]. Известность получили работы Р.Карнапа, в которых использовались представления о «множественности миров». На этой основе высказывание «А возможно» трактуется как «А истинно хотя бы в одном описании состояния (возможном мире)», а высказывание «А необходимо» как «А истинно во всех описаниях состояния (возможных мирах)».

Исследования в области модальной логики активно ведутся и в наши дни [13,14]. Общим для них является расширение классической логики высказываний и классической логики предикатов, когда язык логики пополняется модальными операторами необходимости и возможности, действующими на предложениях языка.

В упрощенной форме, положение дел можно выразить следующим образом. Логика Аристотеля – это тот способ рассуждений, который наиболее прост для формализации, тот способ, который в значительной степени уже передан вычислительным машинам, только потому, что инструменты формализации уже хорошо проработаны и освоены. Более того, на данный момент только логика Аристотеля имеет завершенную (если не сказать – каноническую) форму и поэтому именно она явно или неявно рассматривается как некий эталон, по которому на протяжении столетий строилась любая система рассуждений, призванная обеспечить верификацию выводов. Свидетельством этому является схема построения понятийного аппарата, применяемого в любой из научных дисциплин. Данная схема основывается на построении системы определений (дефиниций), позволяющих редуцировать используемую систему понятий к базовым.

Развитие теории нейронных сетей [9] привело к появлению противопоставления «последовательные вычисления – параллельные вычисления»; логика, одним из основных инструментов которой является построение новых истинных высказываний как следствий из уже существующих, заведомо ассоциируется именно с последовательными вычислениями. Теория нейронных сетей, становление которой изначально было связано с попытками раскрыть механизмы функционирования человеческого сознания, однозначно трактует мозг человека как систему, осуществляющую именно параллельные вычисления.

С этой точки зрения, в частности, представляет интерес проанализировать существующие подходы к построению аксиоматики в любой научной дисциплине. Классическая схема построения аксиоматики подразумевает существование базовых понятий, через которые выражаются все остальные (точнее, существует определенная иерархия понятий, которая позволяет последовательно сводить одну группу понятий к другой). Такую схему допустимо поставить в соответствие той логике, на основе которой строятся последовательные вычисления.

Однако, такой подход обладает вполне определенным недостатком. А именно, он не позволяет дать определение (в классическом смысле) базовым понятиям. Примером в этом отношении являются трудности, связанные с истолкованием понятия «информация» [15,16]. Как отмечается в [15], такие определения информации как используемые в современных учебниках по теории информации и связи (информация есть содержание сообщений [17] и им подобные) не являются конструктивными; по существу, они представляют собой тавтологию.

Как известно, объективная диалектика находит выход из этого положения, определяя базовые понятия через противопоставление. Именно так определяются парные категории объективной диалектики «содержание – форма», «количество – качество» и т.д. В [16] были представлены аргументы, доказывающие, что понятие

информации также следует определять через противопоставление, рассматривая эту категорию как парную к категории материи.

Апеллируя к противопоставлению «последовательные вычисления – параллельные вычисления», можно утверждать, что поход, используемый объективной диалектикой, допускает вполне определенное обобщение. Действительно, противопоставление можно рассматривать как частный случай связи между понятиями. Соответственно, можно утверждать, что базовые понятия допустимо определять через систему связей между ними, причем противопоставление рассматривается не более, чем частный случай взаимосвязи, устанавливаемой между понятиями. Иначе говоря, понятия, образующие базис, формируют некую сетевую структуру, что делает правомочным сопоставление с параллельными вычислениями, осуществляемыми нейронными сетями. Несколько утрируя, можно сказать, что вполне конкретная нейронная сеть – человеческий мозг – для отражения окружающего мира также использует сетевую понятийную структуру, в которой понятия определяются через связи друг с другом.

Подчеркнем, что такой подход, в известном смысле, противоречит основаниям классической логики. А именно, использование системы понятий, замыкаемой саму на себя, можно интерпретировать как «порочный логический круг». Это, однако, не может рассматриваться как препятствие по следующим причинам. Во-первых, как подчеркивалось выше, вопрос об основаниях логики отнюдь не закрыт. Во-вторых, рассматриваемый подход во многом гораздо ближе к обыденному мышлению, нежели классическая формальная логика.

Проследить это можно на примере того, как осуществляется обучение любому искусственному языку, скажем языку программирования. На первых этапах студент (или школьник) усваивает конкретные операнды, чаще все механически заучивая соответствующие правила. Иначе и не может быть – любой язык программирования представляет собой понятийную структуру, замкнутую саму на себя. Это вытекает из того, что смысл операндов, команд и т.д. окончательно раскрывается только в их взаимосвязи с остальными элементами данного языка, что и отвечает завершающему этапу его освоения, на котором студент начинает воспринимать язык программирования как некое единое целое.

Есть основания полагать, что обучение другим конструктам, составляющим в совокупности, скажем, курс высшей математики, также идет по аналогичной схеме, в которой целесообразно выделять, как минимум, два этапа. На первом этапе протекает формальное накопление сведений, целесообразность изучения которых остается для студента неочевидной или, как минимум, ненаглядной. На втором возникает понимание – на уровне возможности применять полученные знания, иногда даже получая от этого удовольствие. Этот этап не может обойтись без уяснения связей между используемыми понятиями, относящимся к новому для студента конструкту, и представления о нем как о едином целом. Упрощая, для освоения интегрального исчисления мало выучить соответствующие определения и правила, нужно что-то еще, что и обеспечивает именно понимание, неотделимое от формирования в сознании студента некоей целостности.

Следовательно, можно сформулировать следующую задачу. Имеется некий язык, сформированный определенной совокупностью понятий и отношениями между ними. Очевидно, что не все понятия в данном языке являются базовыми, во всяком случае, именно это отвечает общему случаю «языка».

Спрашивается, существуют ли формализованные инструменты, обеспечивающие выделение базовой совокупности понятий, формирующих сетевую структуру, которая задает их через взаимосвязи. Отчасти задачи подобного рода решает современная математическая лингвистика. Например, неоднократно обсуждалась задача об

определении словарного минимума, необходимого для того, чтобы объясняться на иностранном языке; ставится вопрос о разработке различных вариантов «алгебры понятий» или «исчисления понятий» [18-20]. Однако, методы решения такого рода задач далеки от завершенной формализации потому, что пока не существует методов, обеспечивающих последовательную формализацию любого из естественных языков.

Приведенные выше рассуждения позволяют сделать вывод о том, что вопрос о создании исчисления понятий (термин предполагает очевидные аллюзии с трактовкой математической логики как исчисления высказываний) содержателен. Определенные шаги в данном направлении, как отмечалось выше, уже сделаны [18-20], но эта деятельность еще весьма далека от завершения. А именно, пока не создана алгебраическая структура (алгебра понятий), которая, в частности, позволяла бы вычленять понятийное ядро конкретного языка средствами формализованного аппарата.

Вопрос о создании алгебры понятий (будем использовать этот термин, апеллируя, главным образом к аналогиям с известными алгебраическими структурами, для которых хорошо отработаны методы поиска того, что в теории алгебр именуется ядром или базисом) имеет еще одно измерение, которое заставляет рассматривать его именно в философском ключе.

А именно, любая система, перешедшая определенный критический порог сложности, например, нейронная сеть, порождает иное качество, несводимое к свойствам совокупности составляющих элементов. Наиболее значимым примером является человеческое сознание – новое качество, которое появляется в системе связанных друг с другом нервных клеток, только потому, что они способны обмениваться сигналами, имеющими электрическую природу.

Следовательно, есть основания полагать, что базисная структура достаточно сложного языка, т.е. языка, обеспечивающего формирование содержательных суждений, также должна формировать некое иное качество, не сводимое к отдельным понятиям или их совокупностям. В этом отношении уместно подчеркнуть, что применительно к естественному языку вопрос о внетекстовых структурах, о смыслах, которые нельзя редуцировать непосредственно к тексту, обсуждается уже достаточно давно [21]. Как отмечал М.К Мамардашвили, говоря о предмете философии, «почувствовать те живые вещи, которые стоят за текстом и из-за которых, собственно, он и возникает. Эти вещи обычно умирают в тексте, плохо через него проглядывают, но тем не менее они есть.»

Гораздо менее очевидно, что внетекстовые структуры в равной степени присущи и искусственным языкам, например, языкам программирования. Упрощая, внетекстовая структура языка программирования есть его внутренняя логика, замысел автора, который позволил трансформировать исходную идею в конкретную алгоритмическую структуру. Это обстоятельство позволяет говорить о том, что системы понятий, порождающие новое качество, конструируемы в той же мере, в которой конструируемы алгебраические структуры.

Представления о внетекстовых структурах как о новом качестве, которое формирует система слов языка (система его понятий) соотносятся с представлениями о новом качестве, которое порождает нейронная сеть следующим образом. В обоих случаях речь идет о появлении нового качества, которое представляет собой сугубо системный эффект. Можно сказать, что нечто иное, появляющееся в сложных системах благодаря обмену информации между элементами (скажем, благодаря обмену сигналами между нейронами головного мозга), не может иметь иного отражения, кроме сходного по информационным свойствам. Конкретно, здесь речь идет о том новом качестве, которое порождает связь между понятиями того или иного языка, не суть важно является ли он искусственным или же естественным.

Упрощая, если говорить о создании логики, в той или иной степени приближающейся к тому способу рассуждений, который на самом деле используется человеческим разумом, то придется поставить вопрос о построении методологии, способной отражать системные свойства информационных продуктов головного мозга, который не оперирует понятиями и связями между ними, существующими вне вполне определенной системы. Новое качество, появляющееся в этой системе, способна отразить только система, оперирующая, как минимум на том же уровне сложности (точнее, обладающая столь же выраженными системными эффектами). Приведенные выше соображения позволяют заключить, что естественные языки, эволюция которых неотделима от эволюции человеческого сознания, вполне удовлетворяют данному условию.

С практической точки зрения, данный вопрос (точнее, ответ на него) можно рассматривать, в том числе, как методологическую основу для создания е-существа, точнее, технических средств, которые бы обеспечили перенос индивидуального сознания на небиологические носители информации. (Вопросу о создании е-существа периодически обсуждается в печати [22]), но до самого последнего времени реалистичный путь решения этой сверхзадачи даже не был намечен.

Вместе с тем представляется очевидным, что перенос индивидуального сознания на небиологический носитель информации предполагает существование некоего алгоритма, способного обеспечить переход от совокупности сведений, зафиксированных в памяти устройства, к иному качеству, которое и именуется сознанием.

Разумеется, ставить соответствующую задачу сразу, пытаясь эмулировать сознание как таковое, во всех его проявлениях, преждевременно. Однако видение именно такой перспективы заставляет сосредоточить внимание на тех разновидностях логики (понимаемой как способ рассуждений, допускающей алгоритмизацию, предполагающую последующее воплощение в технических устройствах), которые максимально приближаются к тем, что использует – прямо или косвенно – человеческое сознание.

Такая постановка вопроса, прежде всего, позволяет исключить из рассмотрения все вопросы физиологического характера. Упрощая, реальный мозг поддерживает функционирование более чем сложной системы – человеческого организма, т.е. термодинамически открытой системы, одной из базовых функций которой является усвоение энергии, черпаемой из природных источников. Если говорить о переносе сознания на биологический носитель, данные функции являются избыточными, коль скоро предполагается, что данная система питается от искусственных источников энергии. Говоря несколько утрированно, «конструкцию» мозга можно существенно упростить, но для этого нужно иметь представление о соответствующих алгоритмах, чтобы ни понималось под этим термином.

Таким образом, и с практической, и с академической точек зрения актуален вопрос о создании логики, приближающейся к той, что используется человеческим разумом. Решить такую задачу абстрактно, т.е., не имея объекта сравнения, как минимум, сложно. Не менее сложно использовать в качестве объекта собственно человеческий мозг в виду большого числа выполняемых им «избыточных» функций, физиологические механизмы которых, равно как влияние процессов, отвечающих за управление физиологической активностью, на процессы, отвечающие за мыслительную деятельность, остаются ясными далеко не до конца.

Современная философия подсказывает выход из этой ситуации. Мышление можно рассматривать и как нечто, присущее индивиду, и как нечто, появляющееся в результате коллективной деятельности [23]. В частности, как отмечается в цитированной

монографии (стр.17) со ссылкой на [24] именно межличностная коммуникация оказывается таким местом, где возможно иное, т.е. до этого не случившееся мышление.

Суждения такого рода верны даже на уровне рассмотрения естественного языка как инструмента, обеспечивающего существование мышления как коллективного творчества. Язык заведомо не мог ни возникнуть, ни существовать как нечто, присущее отдельно взятому индивиду, поскольку он является продуктом межличностных коммуникаций, в чем убеждает пример детей, оказавшихся вне социума.

Следовательно, как объекты сравнения, пригодные для построения «сетевой» логики, т.е. логики автоматически обеспечивающей отражение системных свойств объектов, к которым данная логика прилагается, скажем, как основа инструментов для их описания и изучения, можно использовать объекты, возникающие в результате коллективной деятельности.

Наиболее значимым из таких объектов является ноосфера, понимаемая в смысле [25]. В цитированной монографии ноосфера трактовалась как некий аналог нейронной сети, причем аналогами отдельных нейронов являются индивиды, связанные системой межличностных коммуникаций, которые и формируют сеть. Такой подход в настоящее время приобретает сугубо прикладное значение, так как с позиции теории нейронных сетей можно трактовать и процессы, протекающих в социальных средах, образованных при помощи телекоммуникационных технологий (в первую очередь, к ним относятся т.н. социальные он-лайн сети). Именно социальные он-лайн сети, становятся, как известно, значимым инструментом ведения информационной войны и, шире, инструментом достижения геополитических целей.

Рассмотрение таких объектов позволило выработать следующую трактовку категории сложного (*отчетные материалы по проекту «Разработка научных основ нейросетевой теории эволюции сложных систем» Института вычислительных и информационных технологий МОН РК за 2017 г.*). Систему следует рассматривать как сложную тогда, когда существует комплементарный ей аналог нейронной сети. Иначе говоря, любая сложная система обладает собственной коммуникационной оболочкой, процессы в которой влияют на ее поведение. Рассмотрение коммуникационных оболочек сложных систем, в свою очередь, позволяет предложить механизм их эволюции, альтернативный тому, что восходит к теории происхождения видов Ч. Дарвина. А именно, в соответствии с предложенной точкой зрения эволюция сложных систем протекает в два этапа. На первом этапе имеют место трансформации структуры связей между элементами системы, что интерпретируется как эволюция ее коммуникационной оболочки, обладающей относительно самостоятельным поведением. На этом этапе не происходит изменения свойств отдельных элементов. На следующем этапе эволюции система в целом конвертируется в некий аналог фильтра, создающего благоприятные условия для появления элементов, свойства которых в большей степени отвечают новому состоянию системы. Такой подход позволяет преодолеть многие противоречия, присущие эволюционным теориям, базирующимся на дарвинистской точке зрения [26].

В соответствии с такой трактовкой категории сложного язык также можно рассматривать как «сложную систему», которая также должна обладать собственной коммуникационной оболочкой, образованной тем, что можно назвать метапонятиями. Такие представления позволяют корректно говорить о «внетекстовых структурах», т.е. об объекте, который ранее изучался только средствами гуманитарных наук. Метапонятия невыразимы в языке непосредственно, но именно их существование и задает его логику. Следовательно, построение любого исчисления понятий, в той или иной степени приближающегося к рассуждениям, ведущимся на естественном языке, должно учитывать существование метапонятий.

Таким образом, разработка исчисления понятий, изначально ориентированного на сетевые структуры («сетевую логику»), на возможность проследить за «внетекстовыми структурами», понимаемыми в духе Ю.М. Лотмана и У. Эко, представляет как академический, так и практический интерес. Философской основой для построения такой разновидности исчисления понятий является предложенная нами ранее интерпретация категории «сложного» в соответствии с которой система является «сложной» тогда, когда существует комплементарный ей аналог нейронной сети.

Литература

1. Батыршин И.З. Общий взгляд на основные черты и направления развития нечеткой логики Л. Заде //Новости искусственного интеллекта. – 2001. – №. 2-3. – С. 25-27.
2. Гриняев С. Нечеткая логика в системах управления //Компьютерра. – 2001. – №. 38. – С. 39-45.
3. Фейс Р. Модальная логика. - Главная редакция физ.-мат. литературы изд-ва «Наука», М.: 1974.
4. Вейль Г. Призрак модальности //Вейль Г. Избр. труды: Математика. Теоретическая физика. - М.: Наука. – 1984. – С. 256-274.
5. Веретенников А.А. Философия модальности: аналитическая философия и логика // История философии. 2008. №13. URL: <http://cyberleninka.ru/article/n/filosofiya-modalnosti-analiticheskaya-filosofiya-i-logika>.
6. Клайн М. Математика: утрата определенности. М.: Мир, 1984, 446 с.
7. Valdez, F., Melin, P., & Castillo, O. (2011). An improved evolutionary method with fuzzy logic for combining particle swarm optimization and genetic algorithms. *Applied Soft Computing*, 11(2), 2625-2632.
8. Lootsma, F. A. (2013). *Fuzzy logic for planning and decision making* (Vol. 8). Springer Science & Business Media.
9. Круглов В. В., Дли М. И., Голунов Р. Ю. Нечеткая логика и искусственные нейронные сети. – М.: Физматлит, 2001.
10. McCarthy J., Hayes P. J. Some philosophical problems from the standpoint of artificial intelligence //Readings in nonmonotonic reasoning. – Morgan Kaufmann Publishers Inc., 1987. – С. 26-45.
11. Lewis C.I. A Pragmatic Conception of the A Priori // The Journal of Philosophy. 1923. Vol. 20, No. 7, P. 169–177
12. Ивин А.А. Модальные теории Яна Лукасевича. – Directmedia, 2015.
13. Ивин А.А. Импликации и модальности. - М., 2004. – 126 с.
14. Веретенников А.А. Философия модальности: аналитическая философия и логика // История философии. 2008. №13. URL: <http://cyberleninka.ru/article/n/filosofiya-modalnosti-analiticheskaya-filosofiya-i-logika> (дата обращения: 31.03.2017).
15. Чернявский Д. С. Синергетика и информация. Динамическая теория информации //С. Чернявский. – М.: Наука. – 2001.
16. Диалектика информации / О. Габриелян, Г. Мун, С. Панченко, И. Сулейменов // Ученые записки Крымского федерального университета имени В. И. Вернадского. — 2015. — Т. 1(67), No 2. — С. 137—148.
17. Панфилов И.П., Дырда В.Е. Теория электрической связи. М. Радио и связь. 1991, 344 с.
18. Quine W. V. Toward a calculus of concepts //The Journal of Symbolic Logic. – 1936. – Т. 1. – №. 01. – С. 2-25.

19. Mönnich U. Toward a Calculus of Concepts as a Semantical Metalanguage //Meaning, Use, and Interpretation of Language, Walter de Gruyter, New York. – 1983. – С. 1-35.
20. Wang Y. On concept algebra: A denotational mathematical structure for knowledge and software modeling //International Journal of Cognitive Informatics and Natural Intelligence (IJCINI). – 2008. – Т. 2. – №. 2. – С. 1-19.
21. Лотман Ю.М. Текст и внетекстовые художественные структуры //СПб.: Питер. – 1994.
22. Корчмарюк Я. И. Сеттлеретика—новая междисциплинарная наука о" переселении" личности? //Новые информационные технологии. Матер. науч.–практ. семина. НИТ–98. Моск. гос. ин–т электроники и математики. – 1998. – С. 130-149.
23. Девятинин П. Страна на вырост (заочный диалог Н.Ф. Феорова и М.К. Мамардашвили об отечественной антропологической ситуации) – СПб.: Terra Fantastica, 2012. – 384 с.
24. Пятигорский А.М. Непрерывающийся разговор. СПб.: Азбука – классика, 2004, 432 с.
25. Сулейменов И.Э., Григорьев П.Е. Физические основы ноосферологии. Алматы – Симферополь, 2008, 245 с.
26. Suleimenov I. E. et al. Advanced Applications of Evolution processes in in Solutions of Interacting Polymers //Вестник КазНУ Серия Физическая. – 2015. – Т. 55. – №. 4. – С. 114-120.

РАЗРАБОТКА МЕТОДИКИ НЕПРЯМОЙ ОЦЕНКИ УРОВНЯ КОРРУПЦИИ В ВЫСШИХ УЧЕБНЫХ ЗАВЕДЕНИЯХ НА ОСНОВЕ ТЕОРИИ СЛОЖНЫХ СИСТЕМ

И.Э. Сулейменов^{1,2}, И.Т. Пак¹, Э.Е. Копишев³, З.С. Тасбулатова²
E-mail: esenych@ya.ru

¹Институт вычислительных и информационных технологий МОН РК

²Алматинский университет энергетики и связи

³Евразийский национальный университет им. Л.Н. Гумилева

Аннотация. На основе аналогии с аппаратом статистической физики развита методика, позволяющая получить аналог распределения Больцмана для распределения студентов по уровням компетенции, получаемой в ходе обучения. Такое распределение характеризуется ограниченным набором параметров, один из которых представляет собой аналог термодинамической температуры. Сравнение распределения экзаменационных оценок студентов и аналога распределения Больцмана позволяет судить об интегральном уровне коррупции, одновременно учитывающим ее криминальные и некриминальные формы.

Коррупция в высших учебных заведениях является одним из основных факторов, приводящих к существенному снижению качества образования в постсоветских

государствах [1-6]. Установка на становление экономики знаний, о которой неоднократно говорилось в выступлениях высших руководителей ЕАЭС [7], требует максимально возможного устранения всех факторов, препятствующих развитию высшей школы, включая коррупционные проявления. Следует также учитывать, что повышение качества образования в технических университетах для Казахстана в настоящее время становится жизненно важным, в том числе, с точки зрения обеспечения технологической безопасности государства.

В то же время борьба с коррупционными проявлениями, ориентированная только на использование прямых мер административного и юридического характера, не может рассматриваться как достаточная [8, 9], в частности, потому, что существуют формы коррупции некриминального характера [10, 11]. (К некриминальной коррупции относятся те ее формы, которые не предусматривают уголовную или административную ответственность в соответствии с действующим законодательством.)

Комплексная борьба с коррупцией должна включать в себя разнообразные методы, в том числе, связанные с исчислением рейтинга университетов. Одним из ключевых вопросов здесь является разработка методов косвенной оценки уровня коррупции на основе данных, доступных для статистического анализа независимыми организациями.

В настоящей работе показано, что существует возможность оценить уровень коррупции в заданном университете на основе информации, касающейся только лишь статистики оценок, официально выставляемых за успеваемость.

Подчеркнем, что разрабатываемая методика нацелена на оценку интегрального уровня коррупции, вклад в который вносят как криминальные, так и некриминальные ее формы и применима преимущественно в условиях постсоветских государств, где уровень коррупции заведомо является весьма высоким.

К криминальным формам коррупции, по определению, относятся все те деяния, ответственность за которые предусматривается действующим законодательством; перечислять их здесь нет необходимости.

К некриминальным формам коррупции относятся, в частности, следующие деяния [12, 13]:

- неоправданное завышение оценок конкретным преподавателем в целях минимизации собственных усилий (преподаватели, некачественно читающие тот или иной курс лекций, часто побуждают студентов не принимать соответствующих мер, выставя им незаслуженно завышенные оценки);

- меры, предпринимаемые руководством университетов для искусственного улучшения отчетности, например, в форме негласного запрета на неудовлетворительные оценки;

- неоправданно лояльное отношение к откровенно слабым дипломным работам и магистерским диссертациям

- неадекватный подбор и профессорско-преподавательского состава, в том числе, выражающийся в неспособности оценить реальный уровень знаний студентов т.д.

Некриминальные формы коррупции практически не поддаются прямому выявлению, но отрицательно сказываются на качестве обучения в не меньшей, а возможно, и в большей степени, нежели криминальные. В частности, вред, наносимый перечисленными выше формами некриминальной коррупции, обусловлен следующими факторами:

- подавлением состязательности между студентами за получение высоких оценок и связанных с ними преференций [14-16];

- снижением мотивации к получению реальных знаний [14-16];

- девальвацией высоких оценок, содержащихся в документах выпускника, равно как девальвацией документов о получении высшего образования в целом [14-16].

Эти факторы также являются весьма существенными и именно поэтому оценка коррупции в университетах должна носить комплексный характер [17-19].

Основная идея предлагаемого подхода состоит в следующем. В статистической физике широко применяется распределение Больцмана, которое, в частности, позволяет определить заселенность каждого уровня равновесной системы на основе ограниченного числа параметров (общее число частиц в системе и ее температура) [20]. Как будет ясно из дальнейшего, современные методы теории сложных систем позволяют отыскать аналог формулы Больцмана, позволяющий отыскивать распределение студентов по компетенциям, если известны управляющие параметры (полное число студентов в университете и аналог температуры, рассматриваемый как интегральный показатель эффективности обучения).

Распределение Больцмана носит фундаментальный характер и может быть использовано, в том числе, для оценки достоверности любых измерений, относящихся к равновесным системам [21-23]. А именно, температура системы может быть любой, но вид распределения Больцмана должен сохраняться независимо от природы исследуемой системы.

Сходным образом, если известен аналог распределения Больцмана для учреждений высшего образования, то возникает возможность сравнить его вид с распределением оценок, которые теоретически должны отражать распределение студентов по компетенциям. Точно так же, как если измерения заселенности уровней равновесной системы говорят о том, что она либо не является равновесной, либо измерения проведены некорректно, так и отклонения распределения оценок от аналога распределения Больцмана показывают, что они проставляются некорректно. Следовательно, степень отклонения вида распределения оценок от того, что задается аналогом распределения Больцмана, позволяет оценить интегральный уровень коррупции. Несколько упрощая основную идею разрабатываемой методики можно сформулировать так. Если в конкретном университете подавляющее большинство студентов получает оценки «отлично», то это означает, что реализуется один из следующих вариантов:

- руководство университета обеспечивает завышенные отчетные показатели средствами некриминальной коррупции;

- учебные программы настолько ослаблены, что для их успешного освоения не требуется существенных усилий и способностей;

- преподаватели избегают затруднений, выставляя завышенные оценки, в частности, не желая демонстрировать собственную некомпетентность (в случае неоправданной высокой оценки студент не будет вступать в дискуссию, в случае неоправданно заниженной – наоборот).

Реализация любого из этих вариантов (или их комбинации) отрицательно сказывается на качестве образования, поэтому, если говорить о мерах, направленных на повышение его качества, то, строго говоря, не столь существенно выяснить, какой именно из них реализуется на практике. Важно, что в этом случае университет не выполняет своих базовых функций должным образом. В известном смысле, предлагаемая методика основывается на количественной теории, обосновывающий тезис, который уже неоднократно был озвучен передовыми представителями педагогического сообщества: необходимо вернуть оценке «отлично» ее исходный смысл, содержащийся в самом этом термине. «Отлично» - это значит лучше, чем другие,

и если отличники – все, то университет либо не выполняет своих базовых функций, либо в нем процветает коррупция.

Покажем, что аналог распределения Больцмана, описывающий распределение студентов по компетенциям, действительно можно получить решая задачу в общем виде.

Будем рассматривать модель университета как системы, обеспечивающей последовательный переход студентов с одного уровня компетенции на другой. Предполагается, что переход осуществляется за счет внешнего информационного воздействия (обучение); предполагается также, что в системе имеется $K+1$ уровней (от нулевого, соответствующего исходному уровню компетенции студентов, поступающих на первый курс, до K -того). Для дискретного описания (основанного на использовании переходов именно между дискретными уровнями) рассматриваемой задачи имеются следующие основания. Компетенция есть определенная системная совокупность знаний. Так, невозможно освоить программирование, выучив только некоторые операции; в сознании обучающегося должна сформироваться определенная целостность, которая собственно и формирует язык программирования.

Переходы между выделенными уровнями в рамках предлагаемой модели описываются статистически, т.е. предполагается, что число «частиц», т.е. студентов в системе достаточно велико, чтобы можно было пользоваться энтропийными методами, основанными на аналогии с аппаратом статистической термодинамики [24-27].

Следуя основной идее, на основании которой строится методология статистической физики, поставим задачу следующим образом.

Применительно к равновесным системам базовым является понятие «состояние», скажем, состояние в котором данная система обладает определенной энергией. Методология статистической физики исходит из предположения, что на практике будет реализовано то состояние, которое обладает максимальной кратностью вырождения, т.е. может реализоваться максимальным числом способов. Именно это состояние в формализме Гиббса трактуется как равновесное.

Применительно к системам, не являющимся равновесными, но отвечающим условию стационарности (характеристики системы остаются неизменными во времени), допустимо говорить о потоковом состоянии [28, 29]. Потоки (в данном случае – потоки, отвечающие переходу студентов с одного уровня на другой) также могут реализовываться различным числом способов. За потоковое состояние, которое имеет место на практике, принимается то, которое реализуется максимальным числом способов, т.е. обладает максимальной кратностью вырождения по отношению к потоковым микросостояниям.

Пусть число «частиц» в системе рассматриваемого типа на уровне 0 составляет N_0 . Рассмотрим промежуток времени Δt , полагая, что за это время уровень 1 будет перенесено n_0 частиц. (Аналогично, за это время с уровня k , на котором имеется N_i частиц, на уровень $k+1$ будет перенесено n_i частиц).

Подсчитаем, следуя основной идее энтропийных методов, число способов, которыми может реализовываться такое событие. Очевидно, что число таких способов с хорошей точностью совпадает с числом способов, которыми из совокупности N_i элементов можно выбрать n_i частиц. Это число, очевидно, дается биномиальным коэффициентом $C_{N_i}^{n_i}$

$$C_{N_i}^{n_i} = \frac{N_i!}{n_i!(N_i - n_i)!}, \quad (1)$$

Применение энтропийных методов оправдано только в том случае, когда система содержит сравнительно большое количество частиц. В этом случае допустимо использовать формулу Стирлинга.

$$N! \approx \left(\frac{N}{e}\right)^N \sqrt{2\pi N}, \quad (2)$$

где e – основание натуральных логарифмов.

Имеем

$$C_{N_i}^{n_i} \approx \frac{(N_i)^{N_i}}{(n_i)^{n_i} (N_i - n_i)^{N_i - n_i}} \frac{\sqrt{N_i}}{\sqrt{2\pi n_i (N_i - n_i)}}, \quad (3)$$

В системе в целом за рассматриваемый промежуток времени развивается набор потоков, связанных с переносом частиц с предыдущего уровня на последующий.

Число способов (кратность вырождения объемлющей системы G), которыми может реализовываться такая совокупность потоков, дается произведением

$$G \approx \prod_{i=0}^{i=K-1} \frac{(N_i)^{N_i}}{(n_i)^{n_i} (N_i - n_i)^{N_i - n_i}} \frac{\sqrt{N_i}}{\sqrt{2\pi n_i (N_i - n_i)}}, \quad (4)$$

где K – число уровней (уровней компетенции в рассматриваемой системе), суммирование идет до $K-1$, так как число потоков в системе на единицу меньше числа уровней.

Формула (4) учитывает, что каждым из возможных способов реализации потока с одного из уровней системы на последующий может сочетаться любой из возможных способов реализации всех остальных потоков. В силу этого общее число реализаций всей совокупности потоков дается произведением числа способов реализаций каждого из потоков, связывающих близлежащие уровни

$$G(\{N_i\}_{i=0}^{i=K}) = \prod_{i=0}^{i=K-1} G(n_i), \quad (5)$$

что и выражает формула (4).

Следуя логике статистической термодинамики и в силу того, что логарифм является строго монотонной функцией, вместо кратности вырождения G можно использовать ее логарифм, трактуемый как энтропия системы (или ее аналог).

Кроме того, для любой системы рассматриваемого типа можно считать справедливым следующее неравенство

$$N_i \gg n_i \quad (6)$$

Оно выражает тот факт, что в течение малого промежутка времени только небольшая часть элементов системы может быть перемещена с одного уровня на другой. (Для корректности следует говорить о физически бесконечно малых интервалах; это

подразумевает, что за соответствующий интервал времени перемещается достаточно много элементов системы, но с величиной Δt можно обращаться как с дифференциалом.)

Логарифмируя (4), получаем

$$\ln G(\{N_i\}_{i=0}^{i=K-1}) \approx \sum_{i=0}^{i=K-1} N_i \ln N_i - (N_i - n_i) \ln(N_i - n_i), \quad (7)$$

В выражениях, стоящих под знаком суммы в формуле (7) отброшены слагаемые, пропорциональные n_i , что можно сделать в силу (6).

Снова примем во внимание (6). Можно записать

$$\ln(N_i - n_i) = \ln N_i \left(1 - \frac{n_i}{N_i}\right) = \ln N_i + \ln\left(1 - \frac{n_i}{N_i}\right) \approx \ln N_i - \frac{n_i}{N_i}, \quad (8)$$

Подставляя (8) в (7), имеем

$$\ln G(\{N_i\}_{i=0}^{i=K-1}) \approx \sum_{i=0}^{i=K-1} n_i (\ln N_i + 1), \quad (9)$$

Переходя к интервалу времени Δt , и предполагая, что рассматривается ситуация, в которой число переходов между уровнями сравнительно невелико, соотношение (9) можно переписать в форме

$$\ln G(\{N_i\}_{i=0}^{i=K-1}) \approx \Delta t \sum_{i=0}^{i=K-1} \beta_i N_i \ln N_i, \quad (10)$$

где снова отброшены слагаемые более высоких порядков малости и предполагается, что существует коэффициент β_i , связывающий поток с i -того уровня на уровень $i+1$ и заселённость N_i уровня i .

$$\frac{dn_i}{dt} = \beta_i N_i \quad (11)$$

Полученный результат, переписанный в форме

$$\frac{d \ln G}{dt} = \sum_{i=0}^{i=K-1} \beta_i N_i \ln N_i, \quad (12)$$

следуя [28, 30], допустимо трактовать как производство энтропии в рассматриваемой системе. Данная величина, очевидно, имеет размерность частоты.

По форме соотношение (12) весьма напоминает выражение для энтропии равновесной системы, но оно имеет другой смысл. Прежде всего, оно содержит динамические характеристики системы, находящейся в стационарном состоянии, но не являющейся равновесной. Подчеркнем, что производство энтропии в отдельной части объемлющей системы тем больше, чем выше частота перехода (в рассматриваемом примере – вероятности приобретения дополнительного «кванта компетенции»).

Покажем, что соотношение (12) содержательно, а именно, покажем, что оно позволяет решить сформулированную выше задачу – отыскание распределения студентов (или обобщенных «частиц») по уровням компетенций. Данная задача сводится к отысканию максимума производства энтропии, даваемой соотношением (12).

Можно предположить, что эта формула носит достаточно общий характер, но она не учитывает характера совокупности потоков в конкретной системе. Точнее, величины, фигурирующие в (12), не являются независимыми, но связь между ними можно указать, только принимая во внимание структуру потоков.

В частности, применительно к рассматриваемой задаче имеет место

$$\frac{dN_i}{dt} = \beta_{i-1}N_{i-1} - \beta_i N_i - \frac{N_i}{\tau}, \quad (13)$$

где τ - время обучения в университете (время жизни «частицы»).

Соотношение (13) выражает баланс потоков по отношению к i -тому уровню. На данный уровень поступают студенты с уровня $i-1$, получившие дополнительный «квант компетенции» (первое слагаемое в правой части), с него уходят студенты, получившие еще один «квант компетенции» (второе слагаемое в правой части) и уходят студенты, чье время обучения в университете завершено (третье слагаемое).

Для уровня с индексом «0» (низший уровень компетенции) аналог уравнения (13) записывается в форме

$$\frac{dN_0}{dt} = Q - \beta_0 N_0 - \frac{N_0}{\tau}, \quad (14)$$

где Q есть приток обучающихся в университет, численно равный отношению числа студентов, поступающих на первый курс к продолжительности обучения.

Отталкиваясь от соотношений (13), нетрудно показать, что в стационарном состоянии имеет место

$$Q - \beta_i N_i - \frac{1}{\tau} \sum_{j=0}^i N_j = 0, \quad (15)$$

Данное соотношение можно получить, в том числе, рассматривая совокупность уровней с нулевого по i -тый включительно. Соотношение (15) выражает баланс потоков по отношению к такой системе: общее число студентов, поступающих в данную систему, есть Q ;

Комбинируя соотношения (11) и (15), получаем следующее выражение для производства энтропии в рассматриваемой системе.

$$\frac{d \ln G}{dt} = \sum_{i=0}^{i=K-1} \left(Q - \frac{1}{\tau} \sum_{j=0}^i N_j \right) \ln N_i = Q \sum_{i=0}^{i=K-1} \ln N_i - \frac{1}{\tau} \sum_{i=0}^{i=K-1} \sum_{j=0}^i N_j \ln N_i, \quad (16)$$

Суммирование идет до значения $K-1$, так как рассматривается кратность вырождения «потоков», а не «состояний»; в частности, число слагаемых в формуле (16) равно числу потоков между состояниями, а не числу уровней. Это позволяет найти заселенности уровней с нулевого по $(K-1)$ -ый на основании решения системы $K-1$ уравнений

$$\frac{\partial}{\partial N_i} \left(\frac{d \ln G}{dt} + \lambda F(\{N_i\}_{i=0}^{K-1}) \right) \quad (16)$$

в которые входит также слагаемое, содержащее неопределенный множитель Лагранжа λ . Запись (16) позволяет найти наиболее вероятное распределение с учетом наложенного ограничения. Применительно к рассматриваемой задаче такое ограничение выражается формулой

$$F(\{N_i\}_{i=0}^{K-1}) = \sum_{i=1}^{K-1} \beta_i N_i = B = \text{const}, \quad (17)$$

Соотношение (17) предполагает, что число «квантов компетенции», усвоенных студентами, обучающимися в отдельном университете, является постоянным. По существу, данная величина представляет собой меру эффективности обучения. На этом основании величину λ можно трактовать как характеристику, связанную с аналогом термодинамической температуры, точнее с потоковой температурой.

Система уравнений (16) и (17), содержащая $K+2$ неизвестных величин (заселенности $K+1$ уровней, считая нулевой и неопределенный множитель Лагранжа λ), становится замкнутой, если дополнить ее условием баланса полного числа частиц в системе:

$$Q - \frac{1}{\tau} \sum_{i=0}^{K-1} N_i = 0, \quad (18)$$

Данное соотношение имеет простой смысл, оно, в частности, означает, что полное число студентов равно амплитуде потока на первый курс, умноженной на продолжительность обучения

$$\sum_{i=0}^{K-1} N_i = Q\tau, \quad (19)$$

Таким образом, использование энтропийных методов (а точнее, использование аналогии с аппаратом статистической физики, конкретно, формализмом Гиббса) позволяет получить аналог распределения Больцмана для распределения студентов по уровням компетентности. Тем самым, существует возможность получить эталон сравнения, отклонения от которого позволяют оценить интегральный уровень коррупции в конкретном университете.

Литература

1. Heyneman S.P., Anderson K.H., Nuraliyeva N. The Cost of Corruption in Higher Education // *Comparative Education Review*. 2008. Vol. 52, № 1. P. 1–25.
2. Round J., Rodgers P. The Problems of Corruption in Post-Soviet Ukraine's Higher Education Sector // *International Journal of Sociology*. 2009. Vol. 39, № 2. P. 80–95.
3. Osipian A.L. Corruption hierarchies in higher education in the former Soviet Bloc // *International Journal of Educational Development*. 2009. Vol. 29, № 3. P. 321–330.
4. Osipian A.L. Education corruption, reform, and growth: Case of Post-Soviet Russia // *Journal of Eurasian Studies*. 2012. Vol. 3, № 1. P. 20–29.
5. Shlapentokh V. Corruption, the power of state and big business in Soviet and post-Soviet regimes // *Communist and Post-Communist Studies*. 2013. Vol. 46, № 1. P. 147–158.

6. Habibov N., Cheung A. The impact of unofficial out-of-pocket payments on satisfaction with education in Post-Soviet countries // *International Journal of Educational Development*. 2016. Vol. 49. P. 70–79.
7. Nikitova A., Zhilenko N. Integration in innovation sphere of Eurasian Economic Union: legal aspect // 3rd International Multidisciplinary Scientific Conference on Social Sciences and Arts SGEM 2016, Book 2. 2016. Vol. 2, № SGEM2016 Conference Proceedings, ISBN 978-619-7105-73-5 / ISSN 2367-5659. P. 647–652.
8. Punch M. Police Corruption and its Prevention. // *European Journal on Criminal Policy & Research*. 2000. Vol. 8, № 3. P. 301–324.
9. Edition S. Controlling corruption // *Journal of Criminal Justice*. 1990. Vol. 18, № 6. P. 561–562.
10. Mauro P. Corruption and Growth // *The Quarterly Journal of Economics*. 1995. Vol. 110, № 3. P. 681–712.
11. Kaufmann D., Vicente P.C. Legal corruption // *Economics and Politics*. 2011. Vol. 23, № 2. P. 195–219.
12. Vargas-Hernández J.G. The Multiple Faces of Corruption: Typology, Forms and Levels // *Contemporary Legal and Economic Issues*. 2011. Vol. 3. P. 269–290.
13. Moran J. Democratic transitions and forms of corruption // *Crime, Law and Social Change*. 2001. Vol. 36, № 4. P. 379–393.
14. Obukhova P. V et al. Influence of Mass Consciousness on Quality of the Higher Education in Kazakhstan // *Procedia - Social and Behavioral Sciences*. 2015. Vol. 185. P. 172–178.
15. Suleimenova K.I. et al. Post-Transition Period and Quality of Higher Education: Ways to Overcome the Crisis Phenomena // *International Letters of Social and Humanistic Sciences*. 2013. Vol. 8. P. 49–56.
16. Suleimenov I.E. et al. Higher education and science: Portrait against the background of global crisis // *World Applied Sciences Journal*. 2011. Vol. 15, № 9. P. 1199–1205.
17. Heyneman S.P. Education and corruption // *International Journal of Educational Development*. 2004. Vol. 24, № 6. P. 637–648.
18. Feoktistova Y. Corruption in Higher Education and Government Measures for its Prevention // *Procedia - Social and Behavioral Sciences*. 2014. Vol. 112. P. 167–172.
19. Mohamedbhai G. The Scourge of Fraud and Corruption in Higher Education // *International Higher Education*. 2016. Vol. 84, № 84. P. 12–14.
20. Huang K. Maxwell-Boltzmann Distribution // *Lectures on Statistical Physics and Protein Folding*. 2005. P. 11–16.
21. De Vladar H.P., Barton N.H. The contribution of statistical physics to evolutionary biology // *Trends in Ecology and Evolution*. 2011. Vol. 26, № 8. P. 424–432.
22. Shao L., Ma B.Q. The significant digit law in statistical physics // *Physica A: Statistical Mechanics and its Applications*. 2010. Vol. 389, № 16. P. 3109–3116.
23. Yakovenko V.M., Rosser J.B. Colloquium: Statistical mechanics of money, wealth, and income // *Reviews of Modern Physics*. 2009. Vol. 81, № 4. P. 1703–1725.
24. Kittel C. Thermal Physics // *American Journal of Physics*. 1999. Vol. 67, № 12. P. 1285.
25. S. N. Singh and S. B. Tiwari. An Application of Generalized Entropy in Queueing Theory. *Journal of Applied Science and Engineering*, Vol. 16, No. 1, pp. 99E103 (2013)
26. Guiasu, S. Maximum Entropy Condition in Queueing Theory. *The Journal of the Operational Research Society*. Vol. 37, No. 3 (Mar., 1986), pp. 293–301

27. Jaynes E.T. Information theory and statistical mechanics // Physical Review. 1957. Vol. 106, № 4. P. 620–630.
28. Baigabulova Zh., Suleimenova K., Bekmagambetova J., Suleimenov I. The ecological and economic methods of analysis of the urban transport system (2008), The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences. Vol. XXXVII. Part B8. Beijing, p. 83-88
29. Сулейменов И. Байгабулова Ж., Сулейменова К., Дьяченко Е. Основы физики мегаполиса. Алматы. 2007. 167 с.
30. Wilson A.G. Inter-regional Commodity Flows: Entropy Maximizing Approaches // Geographical Analysis. 2010. Vol. 2, № 3. P. 255–282.

МАКРОСКОПИЧЕСКАЯ ЗАПИСЬ ИНФОРМАЦИИ В РАСПРЕДЕЛЕННЫЕ СИСТЕМЫ КАК ОСНОВА ДЛЯ НАНОПРОГРАММИРУЕМЫХ СИСТЕМ

Сулейменов^{1,2} И.Э., Пак² И.Т., Шалтыкова^{1,2} Д.Б., Байпакбаева¹ С.Т.

E-mail: esenych@ya.ru, pak.it@mail.ru, dina_65@mail.ru,
saltanat.baipalbayeva@gmail.com

¹Институт вычислительных и информационных технологий МОН РК

²Алматинский университет энергетики и связи

Аннотация. Предложена новая методика записи информации в распределенные среды, в том числе, неупорядоченные. Отличительной особенностью предложенной методики является макроскопическое (одновременное) воздействие на все элементы системы, однако предложенный алгоритм обеспечивает запись каждого бита в строго определенную ячейку. Методика является, в том числе, основой для записи информации в наномасштабные структуры, хаотически перемещающиеся друг относительно друга. Реализация алгоритма обеспечивается за счет использования ячеек, изменяющих логическое состояние при внешнем воздействии. Природа управляющего воздействия может быть любой, что в перспективе позволяет записывать информацию в молекулярные и надмолекулярные структуры с помощью вариаций термодинамических переменных заданного вида.

Концепция молекулярного программирования, впервые предложенная в работе [1], представляет, как прикладной, так и академический интерес. С практической точки зрения методы молекулярного программирования могут, в частности, использоваться для совершенствования средств контролируемой доставки лекарственных препаратов в организм (такие средства рассматриваются как одни из наиболее перспективных для современной фармацевтики [2,3]). С академической точки зрения, реализация систем молекулярного программирования нацелена на экспериментальное доказательство сценария пребиологической эволюции, альтернативного тем, что так или иначе используют дарвинистскую точку зрения.

Рис.1. Реакция совокупности бистабильных элементов с дискретно отличающимися порогами срабатывания на внешний импульс

Покажем, что существует простой алгоритм записи произвольной последовательности логических переменных в такую систему ячеек.

Предположим, что требуется осуществить запись следующей последовательности

$$s_1, s_2, s_3, \dots, s_K \quad (2)$$

где s_i – логические переменные

Будем использовать следующие обозначения для последовательности импульсов, обеспечивающих запись информации в рассматриваемую систему ячеек.

- A_i есть логическая переменная, отражающая наличие импульса с амплитудой, обеспечивающей инверсию состояния ячеек с номерами с первого по i -тый включительно, в последовательности сигналов, обеспечивающих запись информации;

- $A_1, A_2, A_3, \dots, A_K$ есть последовательность, описывающая профиль сигнала, обеспечивающего запись информации в рассматриваемую совокупность ячеек; рис. 2 иллюстрирует характер описания профиля сигнала при помощи данной последовательности;

- L_i есть оператор, описывающий изменение состояния ячеек, составляющих рассматриваемую систему, при воздействии на нее импульса, отвечающего логической переменной A_i .

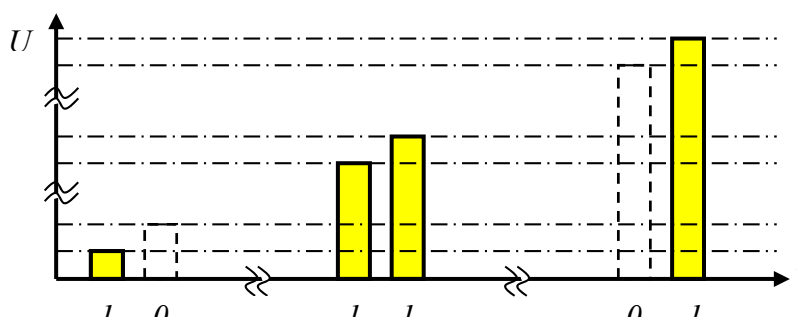


Рис.2. Соответствие профиля управляющего сигнала и последовательности логических переменных A_i

Тогда, воздействие импульса, отвечающего логической переменной A_i , на состояние системы в целом описывается следующим выражением

$$L_i(s_1, s_2, \dots, s_i, s_{i+1}, \dots, s_K) = (A_i + s_1, A_i + s_2, \dots, A_i + s_i, s_{i+1}, \dots, s_K) \quad (3)$$

где произведения логических переменных, стоящих под знаком скобки, подчиняются обычным правилам оперирования с логическими переменными

$$\begin{cases} 1 + s_n = 1, & s_n = 0 \\ 1 + s_n = 0, & s_n = 1 \end{cases} \quad (4)$$

для случая, когда $A_i = 1$; если $A_i = 0$, значения логических переменных s_n остаются неизменными.

Запись (4) подчеркивает также, что при ненулевом значении переменной A_i имеет место инверсия состояния ячеек с номером $n \leq i$.

Инвертируем последовательность (2)

$$s_K, s_{K-1}, s_{K-2}, \dots, s_1 \quad (5)$$

Это заведомо можно сделать, так как воздействие управляющих импульсов на все ячейки системы происходит одновременно.

Воздействие последовательности импульсов различной амплитуды на рассматриваемую систему описывается следующим произведением.

$$(A_K L_K, A_{K-1} L_{K-1}, \dots, A_1 L_1)(s_K, s_{K-1}, \dots, s_1) \quad (6)$$

Примем, что в исходном состоянии все ячейки находятся в состоянии, отвечающему логическому нулю. Тогда, задача о записи заданной последовательности логических переменных $(s_K, s_{K-1}, \dots, s_1)$ сводится к отысканию последовательности $(A_K, A_{K-1}, \dots, A_1)$ такой, что

$$(A_K L_K, A_{K-1} L_{K-1}, \dots, A_1 L_1)(0, 0, \dots, 0) = (s_K, s_{K-1}, \dots, s_1) \quad (7)$$

Будем решать задачу (7) пошагово. На состояние ячейки с номером K может повлиять только импульс максимальной амплитуды. В соответствии с записью (7) этот импульс поступает на входы ячеек последним.

Обозначим через

$$(s_K^{K-1}, s_{K-1}^{K-1}, \dots, s_1^{K-1}) \quad (8)$$

последовательность импульсов, которая формируется на такте с номером $K - 1$. Поскольку изначально предполагается, что все ячейки находятся в состоянии $s_n = 0$, то выражение (8) можно переписать в форме

$$(0, s_{K-1}^{K-1}, \dots, s_1^{K-1}), \quad (9)$$

так как все предыдущие импульсы не могут изменить состояние ячейки с максимальным значением порога срабатывания.

Следовательно, на основании соотношения (7) можно записать следующее уравнение на логические переменные, составляющие последовательность (9)

$$A_K L_K(0, s_{K-1}^{K-1}, \dots, s_1^{K-1}) = (s_K, s_{K-1}, \dots, s_1) \quad (10)$$

Из соотношения (10) немедленно следует, во-первых, что

$$A_K = s_K \quad (11)$$

а, во-вторых, что

$$s_n^{K-1} + A_K = s_n \quad (12)$$

или

$$s_n^{K-1} = s_n + A_K \quad (13)$$

где принято во внимание, что при любом значении логической переменной A_i имеет место

$$A_i + A_i = 0 \quad (14)$$

Таким образом, на следующем шаге решения уравнения (7) можно рассматривать последовательность, фактически содержащую число элементов на единицу меньше

$$A_{K-1} L_{K-1}(0, s_{K-2}^{K-2}, \dots, s_1^{K-2}) = (s_{K-1} + A_K, s_{K-2} + A_K, \dots, s_1 + A_K) \quad (15)$$

В соотношении (15) принимается во внимание, что до прихода импульса с амплитудой, отвечающей оператору L_{K-1} , состояние элемента с номером $K - 1$ заведомо отвечает условию $s_{K-1} = 0$, так как на вход каких-либо элементов системы еще не поступал импульсов, способных изменить его состояние (все они обладали недостаточной амплитудой). Следовательно,

$$A_{K-1} = s_{K-1} + A_K \quad (16)$$

$$s_n^{K-2} + A_{K-1} = s_n + A_K, \quad n \leq K - 2 \quad (17)$$

или

$$A_{K-1} = s_{K-1} + s_K \quad (18)$$

$$s_n^{K-2} = s_n + A_K + A_{K-1}, \quad n \leq K - 2 \quad (19)$$

Используя соотношения (11) и (18), выражение (19) можно переписать в виде

$$s_n^{K-2} = s_n + s_{K-1}, \quad n \leq K - 2 \quad (20)$$

где также принимается во внимание, что

$$s_i + s_i = 0 \quad (21)$$

Действуя далее по индукции, можно видеть, что искомые коэффициенты, описывающие последовательность импульсов, обеспечивающих запись информации в рассматриваемую систему ячеек, выражаются формулой

$$A_{m-1} = s_{m-1} + s_m \quad (22)$$

Формулы (11) и (22) представляют собой решение уравнения (7), т.е. составляют алгоритм, позволяющий осуществить запись произвольной последовательности логических переменных в совокупность бинарных ячеек рассматриваемого типа.

Таким образом, существует возможность реализовать запись информации с адресацией за счет одновременного воздействия на все без исключения ячейки памяти системы. Это создает необходимые предпосылки для реализации систем молекулярного программирования, в которых запись заданной программы в наноструктуры обеспечивается за счет изменения термодинамических переменных по заданному закону.

Литература

10. Сулейменов, И. Э. Молекулярное программирование: аналогия с радиотехническими системами / И. Э. Сулейменов, С. В. Панченко, М. А. Ердаулетова // Известия НТО «Кахак», 2015, № 4(51). – С.77-84.
11. Барышников, А. Ю. Наноструктурированные липосомальные системы как средство доставки противоопухолевых препаратов / А. Ю. Барышников // Вестник Российской академии медицинских наук. – 2012. – Т. 67. – №. 3.
12. Иванов, Р. В., Балакин К. В., Шоболов Д. Л., Федотов Ю. А., Калмыков Ю. М. Разработка систем доставки лекарственных средств с применением микро- и наночастиц – <http://cyberleninka.ru/article/n/razrabotka-sistem-dostavki-lekarstvennyh-sredstv-s-primeneniem-mikro-i-nanochastits> (дата обращения: 03.06.2017).
13. Ергожин, Е. Е. Гидрофильные полимеры в нанотехнологии и наноэлектронике (монография) / Е. Е. Ергожин, А. Б. Зезин, И. Э. Сулейменов, Г.А. Мун // Алматы-Москва: Издательство LEM, Библиотека нанотехнологии, 2008. – 214 с.

РАЗРАБОТКА И АНАЛИЗ БИОНИЧЕСКОЙ РУКИ

Сундетов Т.Р., Жакупбеков Т.Е.
e-mail: sundetovtalgat@gmail.com , 3536006@mail.ru

*Институт информационных и вычислительных технологий КН МОН РК,
Казахстан*

Аннотация. Целью данной статьи является представление дешевой роботизированной руки, которая может воспроизводить способности и движения человеческой руки, чтобы выполнить задачу занавеса, такую как захват захвата и т. Д. Роботизированная рука была разработана, чтобы помочь инвалиду, который может Способный управлять роботизированной рукой с ограниченным физическим движением. Роботизированная рука, которую мы разработали, находится в полуавтономной машине, для этой руки требуются команды от пользователя. Мы использовали датчики

fler для получения данных от руки человека, чтобы воспроизвести движение в нашей роботизированной руке. В этой системе команды от датчика, который воспринимает фактическое движение человеческого пальца и соответствующим образом посылает сигнал роботизированной руке. Чтобы достичь этой цели, мы рассмотрели три аспекта: во-первых, как разработать экзо-скелет роботизированной руки, чтобы манипулировать объектами, такими как люди. Во-вторых, было исследование правильных сигналов, которые можно использовать для перемещения роботизированного пальца. Наконец, как запрограммировать роботизированную руку для пульсирования, различают человеческие задачи. В этом документе представлены детали аппаратного обеспечения и программного обеспечения для ручного управления. Результаты экспериментальной работы для разных объектов перечислены. Ссылаясь на это, теперь мы строим недорогие роботизированные перчатки для рук, которые преодолеют физическую слабость у старых людей.

Ключевые слова: роботизированная рука, обработка контрольных материалов. Датчик Fler.

I. Введение

Роботы могут сыграть большую роль в нашем мире. Вместо людей роботы могут назначать задачи а, чтобы избежать человеческих потерь. Однако использование роботов растет, чтобы взаимодействовать с объектами в опасной среде. Люди физически взаимодействуют с окружающей средой, используя свои руки. Роботизированные ручные системы могут использоваться в надежных средах, таких как те, которые встречаются в ядерной, военной, химической и большей части для космических применений.

До сих пор сообщалось о количестве исследователей по антропоморфной мульти-роботизированной руке [1,2,3]. Рука MIT, разработанная Jacobsen, управляется приводами, которые расположены в удаленном месте от роботизированной рамы и прикреплены сухожильными кабелями [4]. Разработанные DLR-Hand, которые встроили исполнительные механизмы вручную. Каждый палец руки робота прикреплен к двигателю, 6-му датчику силы вращения пальца руки и встроеной электронике вместе с контроллером. В этой статье мы попытались создать роботизированную руку, которая является копией человеческой руки. Движения пальцев человека имеют смысл с помощью гибкого датчика. Кроме того, мы использовали Atmega 328P, который является одним из предварительных 8-битных контроллеров в семействе AVR. Программа и макет или внешний вид фрейма на ПК, выполненный с помощью Codevision Avr 1.25.8 и Proteus 7.6 SP4. В разделе II этой статьи обсуждались аппаратные средства и дизайн. В следующем разделе е обсуждался алгоритм, используемый в этой статье. Алгоритм хорошо объясняется с помощью блок-схемы. В разделе IV проиллюстрирована реализация аппаратного обеспечения. Затем следует эксперимент и результат, о котором мы говорили. Целью было воспроизвести движение пальца человека, которое выполняется, чтобы получить после того, как проект удерживается и захватить объект как человеческую руку. Также вынудите роботизированную руку в соответствии с движением человека.

II. Описание оборудование и дизайн

Для проекта используется роботизированная рука из ПВХ. Сигнал от датчиков гибки передается на схему делителя напряжения, и соответствующие сигналы

посылаются роботизированной руке. Устройство выполнено таким образом, что двигатель постоянного тока может правильно входить в механический узел. Для перемещения пальцев используются механические сервомоторы. Валы двигателей закреплены с готовой частью ПВХ, которая поможет удерживать положение пальца. Используемые детали показаны на Рис 1.

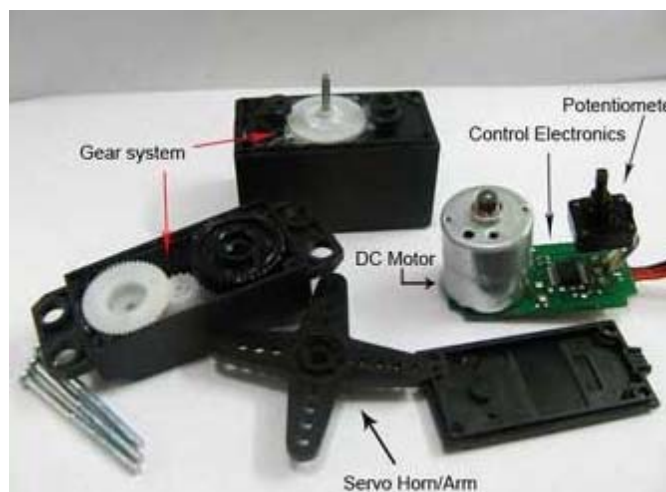


Рис. 1 Отображается внутренняя сборка сервомотора

На Рис 2. рисунке показан Flex датчик гибкости. Он дает изменение сопротивления, поскольку изогнутый датчик изогнут. Это изменение сопротивления подается на цепь делителя напряжения. Таким образом, изменение сопротивления происходит при изменении напряжения. Это напряжение является аналоговым по своей природе, так как используется для преобразования его в цифровой АЦП, присутствующий в контроллере.



Рис. 2 Flex датчик гибкости

III. Осуществление

Встроенная компьютерная роботизированная рука с пятью пальцами, разработанная и разработанная с простой и минимальной стратегией управления. Подход основан на антропоморфном дизайне с четырьмя пальцами и противоположным пальцем. На Рис 3 показана схема роботизированной руки. Порты 1, 2, 15, 16, 17 контроллера подключены к пяти серводвигателям. Порты 24, 25, 26, 27, 28 подключены к датчикам гибкости. Штырь 1,17,18,19 используется для программирования микроконтроллера. Мощность для роботизированной руки обеспечивается портативной батареей. Поставка, которую мы использовали, была стандартной батареей. При реализации проекта мы столкнулись с проблемой энергопотребления. Как там мы использовали датчик двигателя и flex для каждого из пальцев. Поэтому мы выбрали такой микроконтроллер, который выполнит это требование.

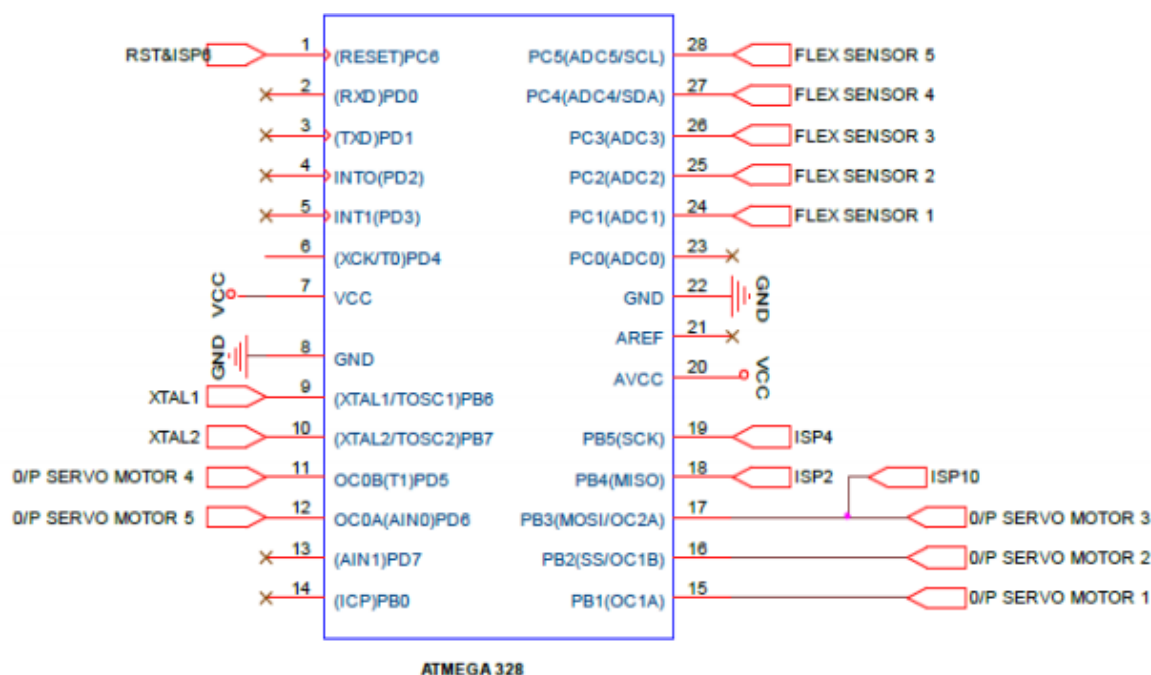


Рис. 3 Схема роботизированной руки

IV. Экспериментальный результат

Перед установкой компонентов каждый измерительный датчик испытывается с помощью отдельных серводвигателей. Поскольку каждый рис имеет различное пороговое значение. Цифровые значения на каждом рисунке наблюдаются и отображаются в реальном времени с использованием программного обеспечения Codevision AVR. Мы обнаружили разные пороговые значения для каждого пальца. Итак, при написании кода в Embedded C мы выше важного наблюдения. Положение каждого Рис наблюдается через каждые 50 мс. Для этого мы использовали программу задержки. Мы программируем микроконтроллер для того, чтобы использовать пять паре контактов АЦП и ШИМ. Для сброса кода мы используем внутреннюю память 8-битного AVR. После тестирования двигателей мы перешли на конструкцию печатной платы и установили компоненты, снова тестировали плату и проводили эксперимент.



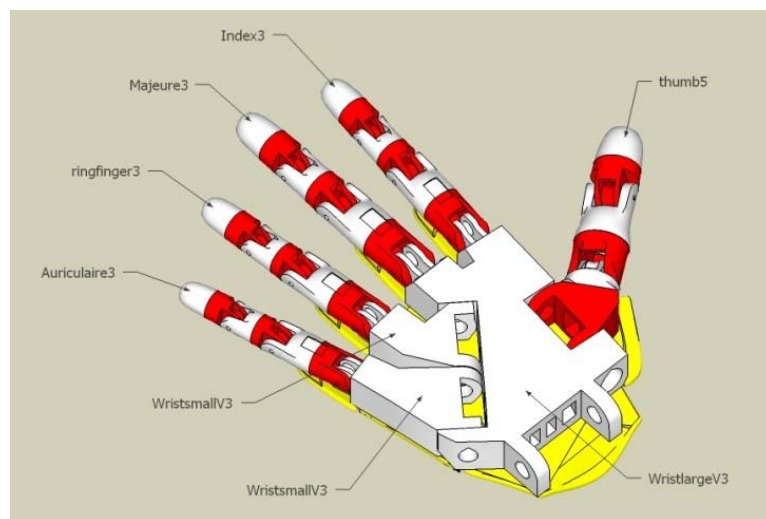


Рис. 3 Экспериментальные результаты

V. Заключение

Роботизированная рука спроектирована, построена и протестирована полностью. Испытаны операции механического перемещения пальцев по всем суставам и обнаружению объектов, захвату и выпуску различных типов объектов. Наблюдается хорошая повторяемость для каждой выполняемой задачи. Движение пальцев произвольно и проверено одинаково. Чтобы проверить ограничения по размеру объектов, эксперименты выполняются при захвате сферических объектов. Максимальный диаметр сферы составляет 90 мм, а минимальный диаметр сферы - 30 мм, наблюдается для любого объекта. Интересным аспектом этой конструкции является то, что диапазоны веса могут быть увеличены за счет добавления более мощных двигателей и кабелей с более высокой прочностью на растяжение. Это позволяет настроить руку для приложения путем выбора соответствующих двигателей. Было продемонстрировано, что эта рука может захватывать различные объекты с различными поверхностными характеристиками и формами без необходимости реконструировать поверхностное описание объекта. Мы попытались сделать точное копирование движения пальца человека. Концепция может быть использована при изготовлении механического узла, который можно носить в качестве перчаток.

Литература

1. Nicholas Thayer and S. Priya. 2011, "Design and implementation of a dexterous anthropomorphic robotic typing (DART) hand", Smart Mater. Struct.20(2011) 035010(12pp), doi:10.1088/0964-1726/20/3/035010.
2. Cipriani, C., Zaccone, F., Stellin, G., Beccai, L., Cappiello, G., Carrozza, M.C., and Dario, P., 2006, "Closed-loop Controller for a Bio-inspired Multi-fingered Under actuated Prosthesis", Proc. of the 2006 IEEE Int. Conf. on Robotics and Automation, Orlando, FL, USA, May pp. 2111-2116.
3. Hoshino, K., and Kawabuchi, I., 2006, "Dexterous robot hand with pinching function at fingertips", Proc. of the 1st IEEE/RAS Int.Conf. on Biomedical Robotics and Biomechatronics, BioRob 06, Pisa, Italy, February 20-22.

4. R. Borjas and W.Flores, "Developing a Human Prosthesis using a 3D printer in Honduras," in IEEE Thirty Fifth Central American and Panama Convention (CONCAPAN XXX), Tegucigalpa, 2015.

5. J.T. Belter, J.L.Segil, A.M.Dollar and W.F.Richard, "Mechanical design and performance specifications of anthropomorphis prosthetic hands: A review, "Journal of Rehabilitation Research & Development, vol. 50, no. 5, pp. 599-618, 2016.

О ПОСТРОЕНИИ УРАВНЕНИЙ ДВИЖЕНИЯ КОСМИЧЕСКОГО АППАРАТА ПРИ НАЛИЧИИ АЭРОДИНАМИЧЕСКИХ СИЛ

Тлеубергенов М.И., Ибраева Г.Т., Ажымбаев Д.Т.

e-mail: marat207@mail.ru, gulmira_ibraeva@mail.ru, darkhan70@gmail.com

*Институт математики и математического моделирования КН МОН РК,
Казахстан*

Аннотация. Построены уравнения вращательных движений гиростата переменной массы по заданному интегральному многообразию при наличии аэродинамических сил. Определены управляющие моменты, создаваемых активными гироскопами и обеспечивающих заданное вращательное движение гиростата переменной массы относительно центра масс, при наличии аэродинамических сил.

1. Построение уравнений вращательных движений КА

Предположим, что центр масс гиростата (твердое тело переменной массы с тремя активными гироскопами) движется в окрестности Земли по эллиптической орбите по известному закону [1-3]. В работе [1] определяются моменты, создаваемые гироскопами и управляющие движением гиростата около центра масс так, чтобы одна из главных осей эллипсоида инерции гиростата сохраняла направление на заданную точку, движущуюся по поверхности Земли и вращение вокруг этой оси происходило по заданному закону.

Предполагается также, что управляемое тело КА состоит из двух частей: неизменной и изменяющейся, и частица изменяющейся массы, движущейся по известному закону по отношению к неизменной части. При этом центр масс гиростата не перемещается относительно управляемого тела, а главные оси инерции тела относительно центра масс гиростата неподвижны по отношению к первоначальным геометрическим очертаниям тела.

При дополнительном предположении, что на внутренние рамки гироскопов действуют случайные возмущающие силы типа "белого шума"[4] в обозначениях [1-3] с учетом «белого шума» строится следующая система уравнений вращательных движений КА как твердого тела переменной массы с тремя активными гироскопами

$$\begin{cases} \dot{\alpha} = G(\alpha)p \\ \dot{p} = P(\alpha, \beta, \gamma, p) \\ \dot{\beta} = \gamma \\ \dot{\gamma} = B(\alpha, \beta, \gamma, p) + u + \sigma(\alpha, \beta, \gamma, p)\dot{\xi}, \end{cases} \quad (1)$$

по заданному интегральному многообразию

$$\Lambda(t) : \lambda(\alpha, t) = 0, \quad (2)$$

$$\lambda_1 \equiv \alpha_1 - \alpha_1^0(t) = 0$$

где

$$\lambda_2 \equiv b_{21}(\alpha)l_1(t) + b_{22}(\alpha)l_2(t) + b_{23}(\alpha)l_3(t) = 0$$

$$\lambda_3 \equiv b_{31}(\alpha)l_1(t) + b_{32}(\alpha)l_2(t) + b_{33}(\alpha)l_3(t) = 0,$$

при наличии аэродинамических сил, которые при моделировании вращательных движений КА входят, следуя [5], в правую часть системы уравнений (1) в виде функции $\varphi = \sigma(\alpha, \beta, \gamma, p)\xi$.

2. Определение управляющих моментов, обеспечивающих заданное вращательное движение КА

Предположим, что центр масс КА (твердое тело переменной массы с тремя активными гироскопами) движется в окрестности Земли по эллиптической орбите по известному закону [6]. Требуется определить моменты, создаваемые гироскопами и управляющие движением гиростата около центра масс так, чтобы одна из главных осей эллипсоида инерции гиростата сохраняла направление на заданную точку, движущуюся по поверхности Земли и вращение вокруг этой оси происходило по заданному закону.

Определяются управляющие моменты КА, обеспечивающие ему заданное программное (вращательное) движение. Пусть управление угловыми движениями КА осуществляется тремя активными гироскопами, оси внешних рамок которых направлены по главным осям эллипсоида инерции тела.

Предварительно определяются необходимые кинематические соотношения.

Пусть P_1, P_2, P_3 – проекции мгновенной угловой скорости КА (гиростата с тремя активными гироскопами) на оси Cx, Cy, Cz , $\dot{\alpha}_1, \dot{\alpha}_2, \dot{\alpha}_3$ – составляющие вектора мгновенной угловой скорости соответственно по осям Cx, Cy', Cz , где для определения вращательных движений КА вокруг центра масс C введены прямоугольные декартовы системы координат:

1. $Cx_1y_1z_1$, где Cx_1, Cy_1, Cz_1 соответственно параллельны Ox_1, Oy_1, Oz_1 .

2. $Cxyz$, оси Cx, Cy, Cz направлены по главным осям эллипсоида инерции тела.

3. Вспомогательная система координат $Cx'y'z'$ совпадает с осями Резаля.

При этом положении системы $Cxyz$ относительно $Cx_1y_1z_1$ определяется углами $\alpha_1, \alpha_2, \alpha_3$ вращений соответственно вокруг осей Cx, Cy', Cz .

Тогда

$$p = \Omega(\alpha)\dot{\alpha}, \quad \Omega(\alpha) = (\Omega_{ij}), \quad i, j = 1, 2, 3.$$

$$p = (P_1, P_2, P_3)^T, \quad \dot{\alpha} = (\dot{\alpha}_1, \dot{\alpha}_2, \dot{\alpha}_3)^T,$$

$$\Omega_{11} = \cos\alpha_2 \cos\alpha_3, \quad \Omega_{12} = \sin\alpha_3, \quad \Omega_{21} = -\cos\alpha_2 \sin\alpha_3, \quad \Omega_{22} = \cos\alpha_3,$$

$$\Omega_{31} = \sin\alpha_2, \quad \Omega_{32} = 1, \quad \Omega_{13} = \Omega_{23} = \Omega_{33} = 0,$$

$$\dot{\alpha} = G(\alpha)p, \quad G(\alpha) = \Omega^{-1} = (g_{ij}), \quad i, j = 1, 2, 3;$$

$$g_{11} = \sec\alpha_2 \cos\alpha_3, \quad g_{12} = -\sec\alpha_2 \sin\alpha_3, \quad g_{13} = g_{23} = 0,$$

$$g_{21} = \sin\alpha_3, \quad g_{22} = \cos\alpha_3, \quad g_{31} = -\tan\alpha_2 \cos\alpha_3, \quad g_{32} = \tan\alpha_2 \sin\alpha_3, \quad g_{33} = 1.$$

Далее рассмотрена задача определения управляющих моментов, создаваемых активными гироскопами.

В предположении, что

1) геометрия масс гиростата в процессе движения остается неизменной и

2) управление угловыми движениями КА осуществляется тремя активными гироскопами, оси внешних рамок которых направлены по главным осям эллипсоида инерции тела,

уравнения движения такого КА запишется (без учета случайных возмущений), следуя [1], в виде

$$\dot{p} = P(p, \beta, \dot{\beta}, M),$$

$$\ddot{\beta} = B(p, \beta, \dot{\beta}, M) + u,$$

где

$$P_1 = A_1^{-1} [M_1 + (A_2 - A_3)p_2 p_3 - H_2 \cos\beta_2 (\dot{\beta}_2 + p_2) + H_3 \sin\beta_3 (\dot{\beta}_3 + p_3)],$$

$$B_1 = -P_1 + J_1^{-1} H_2 (p_2 \sin\beta_1 - p_3 \cos\beta_1) - J_1^{-1} b_1 \dot{\beta}_1,$$

P_2, P_3, B_2, B_3 получаются соответственно из P_1, B_1 циклической перестановкой индексов. Здесь $\beta = (\beta_1, \beta_2, \beta_3)^T$ – вектор углов поворота внутренних рамок гироскопа вокруг главных осей; $M = (M_1, M_2, M_3)^T$ – вектор внешних моментов, действующих по осям Cx, Cy, Cz ; $u = (u_1, u_2, u_3)^T$ – вектор управляющих моментов, создаваемых двигателями; $A_1(t), A_2(t), A_3(t)$ – главные моменты инерции КА; H_1, H_2, H_3 – кинетические моменты гироскопов; b_1, b_2, b_3 – коэффициенты демпфирования.

А с учетом случайных возмущающих сил уравнения движения рассматриваемой системы строятся в виде (1), которые допускают заданное программное (вращательное) движение (2).

Далее, следуя работе [1], составляются необходимые и достаточные условия для осуществления программного движения (интегральности многообразия) (2). С этой целью последовательно вычисляются $\dot{\lambda}, \ddot{\lambda}, \ddot{\lambda}$ и составляется уравнение возмущенного движения относительно $\Lambda(t)$ (2)

$$\ddot{\lambda} = \Phi(\ddot{\lambda}, \dot{\lambda}, \lambda, \alpha, p, \beta, \gamma, t) + \sigma'(\ddot{\lambda}, \dot{\lambda}, \lambda, \alpha, \beta, \gamma, p)\dot{\xi}, \quad (3)$$

и при всех $t \geq t_0$ и любых α в области допустимых значений углов поворота КА требуется выполнения условия $\Phi(0,0,0, \alpha, p, \beta, \gamma, t) \equiv 0$, $\sigma'(0,0,0, \alpha, \beta, \gamma, p) \equiv 0$.

Литература

1. Галиуллин А.С., Мухарлямов Р.Г., Волков С.В. Программное управление угловыми движениями гиростата // Численные методы решения задач математической физики и теории систем. – М., 1979. – С. 118-131.
2. Киргизбаев Ж.К., Мухарлямов Р.Г. Управление угловыми движениями тела переменной массы с помощью гироскопов // Дифференциальные уравнения и обратные задачи динамики. – М., 1983. – С. 7-15.
3. Мухарлямов Р.Г., Киргизбаев Ж.К. Управление программным движением и обратные задачи динамики систем с переменной массой. – Шымкент: Нурлы бейне, 2008. – 180 с.
4. Хасьминский Р.З. Устойчивость систем дифференциальных уравнений при случайных возмущениях их параметров. – М.: Наука, 1969. – 368 с.
5. Сагиров П. Стохастические методы в динамике спутников // Механика. Периодический сборник переводов иностранных статей. – М., 1974. – № 5(147). – С. 28-47.
6. Белецкий В.В. Движение искусственного спутника относительно центра масс. – М.: Наука, 1965. – 416 с.

Публикации в 1-2 кв. 2017 года

по теме «Построение уравнений программного движения космического аппарата при наличии случайных возмущающих сил»

Статьи:

1. Василина Г.К., Тлеубергенов М.И. Об оптимальной стабилизации интегрального многообразия // Нелинейные колебания. – Киев, 2017. – Т. 20, № 1. – С. 53-65. (Scopus)
2. Тлеубергенов М.И., Ажымбаев Д.Т. О построении силовой функции по заданному интегральному многообразию // Вестник Актюбинского регионального государственного университета им. К. Жубанова. – Актюбе, 2017, № 1. – С.16-21.
3. Zhumatov S.S. On an instability of the indirect control systems in the neighborhood of program manifold // Математический журнал. - Алматы, 2017.-Т.17, № 1. – С.91-97.

Сданы в печать:

1. Tleubergenov M.I., Ibraeva G.T. On the Problem of Closure under Random Perturbation // International Journal of Pure and Applied Mathematics, Sofia, Bulgaria, 2017. Объем – 9 стр. (Scopus)
2. Tleubergenov M.I., Ibraeva G.T. On the Construction of Stochastic Closing Equations by Given Properties of Motion // Open Engineering, 2017. Объем – 5 стр. (Scopus)

Тезисы докладов и материалы научных конференций:

1. Василина Г.К. Об оптимальном управлении стохастическими системами с квадратичным критерием качества // Дифференциальные операторы и моделирование

сложных систем: тез. докл. ежегодной. науч. апрельской конф. ИМММ, посв. 70-летию юбилею проф. М.Т. Дженалиева. – Алматы, 2017. – С. 56.

2 Zhumatov S.S. Absolute instability of a program manifold of basic control system //Тезисы докладов ежегодной научной апрельской конференции Института математики и математического моделирования, посвященной дню науки и научного семинара «Дифференциальные операторы и моделирование сложных систем» (DOMCS-2017), посв. 70-летию проф. Дженалиева М.Т. Алматы-2017. С.141-143.

3 Tleubergenov M.I., Ibraeva G.T. On the problem of closure under random perturbation // Дифференциальные операторы и моделирование сложных систем: тез. докл. ежегодной. науч. апрельской конф. ИМММ, посв. 70-летию юбилею проф. М.Т. Дженалиева. – Алматы, 2017. – С. 171-173.

4 Zhumatov S.S., Onaybaev K. On auto-oscillation of control systems with break nonlinearity in the neighborhood of program manifold // Труды международной научно-практической конференции «Математические методы и информационные технологии макроэкономического анализа и экономической политики», посв. 80-летнего юбилея академика НАН РК А. А. Ашимова, 11-12 апреля 2017 года, г. Алматы. С. 292-297.

5 Zhumatov S.S. Instability of a program manifold of controllable systems // Тезисы докладов международной научной конференции «Весовые оценки дифференциальных и интегральных операторов и их приложения», посв. 70-летию члена-корр. НАН РК, проф. Р. Ойнарова. Астана: ЕНУ им. Л.Н. Гумилева, 2017. С. 268-271.

6 Тлеубергенов М.И., Ажымбаев Д.Т. Об обратной стохастической задаче построения силовой функции // Тезисы докладов международной научной конференции «Весовые оценки дифференциальных и интегральных операторов и их приложения», посв. 70-летию члена-корр. НАН РК, проф. Р. Ойнарова. Астана: ЕНУ им. Л.Н. Гумилева, 2017. С. 254-257.

РАЗРАБОТКА И РЕАЛИЗАЦИЯ АППАРАТНОГО УМНОЖИТЕЛЯ В НЕПОЗИЦИОННОЙ СИСТЕМЕ СЧИСЛЕНИЯ

Тынымбаев С.Т., Капалова Н.А., Магзом М.М.
e-mail: magzomxzn@gmail.com

*Институт информационных и вычислительных технологий КН МОН РК,
Казахстан*

Аннотация. В данной статье описывается разработка и реализация аппаратного умножителя полиномов по модулю неприводимых полиномов с двоичными коэффициентами. Данный умножитель является основным вычислительным устройством при аппаратной реализации разработанных алгоритмов шифрования на базе непозиционной полиномиальной системы счисления.

Введение

Аппаратное шифрование имеет ряд существенных преимуществ перед программным шифрованием [1, 2]. Аппаратные средства шифрования обладают большей скоростью. Кроме этого схемы, выполняющие процедуры шифрования, могут

быть установлены в качестве криптографических сопроцессоров в состав других устройств.

Как было показано в [3,4], основные преимущества применения модулярной арифметики заключается в отсутствии переноса разрядов в операциях сложения и умножения, и, следовательно, в возможности параллельного выполнения операций по каждому из оснований системы. Процессоры общего назначения не способны эффективно выполнять вычисления в непозиционной системе счисления. Для наиболее эффективной реализации вычислительных устройств на основе системы остаточных классов требуется создание специализированных схем, архитектура которых позволяет выполнять вычисления в данной непозиционной системе счисления.

Основным устройством для выполнения рутинных вычислений при программно-аппаратной реализации разработанных алгоритмов шифрования на базе НПСС [5,6] является умножитель полиномов по модулю неприводимых полиномов с коэффициентами из поля GF (2).

В данной статье рассматривается подход к реализации такого умножителя. Подход заключается в выполнении традиционных шагов, где на первом этапе вычисляется произведение двух полиномов, а на втором этапе полученное произведение приводится по модулю неприводимых полиномов.

Общая структура разработанного умножителя

Рассмотрим схему умножителя, где произведение полиномов с двоичными коэффициентами вычисляется путем суммирования строк матриц частичного произведения на многоуровневых сумматорах по модулю два (СМ), а приведение по модулю неприводимого полинома выполняется на формирователях частичных остатков (ФЧО). Опишем организацию схемы умножителя на примере умножения двух полиномов с бинарными коэффициентами A и B :

$$A = \{a_{n-1}a_{n-2} \dots a_1a_0\}, \quad B = \{b_{n-1}b_{n-2} \dots b_1b_0\}.$$

Матрица частичных произведений полиномов с разрядностью n приведена на рисунке 1. При суммировании каждого столбца этой матрицы по модулю два получается двоичное представление полинома C :

$$AxB = C\{c_{2n-1}c_{2n-2} \dots c_1c_0\}$$

Здесь произведение полиномов вычисляется путем суммирования строк матрицы частичного произведения на многоуровневых сумматорах по модулю два.

Суммирование строк матрицы частичных произведений выполняется через попарную группировку частичных произведений строк матрицы. После чего каждая пара суммируются параллельно на сумматорах по модулю два, образуя группу сумматоров первого уровня. Далее результаты сложения, полученные на первом уровне так же попарно группируются и суммируются на сумматорах по модулю два, образуя сумматоры второго уровня. Такое суммирование производится до тех пор, пока не сформируется $2n-1$ разрядный сумматор последнего уровня, то есть пока не получится окончательный результат. Таким образом, выполнение произведения двух полиномов происходит на дереве сумматоров, которое имеет несколько уровней. Число уровней и сумматоров на каждом уровне зависит от разрядности умножаемых полиномов. В таблице 1 приведены параметры умножителя полиномов в зависимости от числа разрядов полиномов.

Таблица 1 – Параметры умножителей полиномов для различных n

Разрядность Полиномов n	Распределение числа сумматоров по уровням					Всего сумматоров N	Число уровней L
	1	2	3	4	5		
32	16	8	4	2	1	31	5
28	14	7	3	2	1	27	5
23	11	6	3	1	1	22	5
18	9	4	2	1	1	17	5
10	5	2	1	1		9	4
6	3	1	1			5	3

По числу уровней можно определить время задержки сигналов на дереве сумматоров по модулю 2.

Для примера на приведем схему умножителя 6-ти разрядных полиномов A и B на основе дерева сумматоров. Данная схема отражена на рисунке 1. Как видно из схемы, матрица частичного произведения состоит из шести строк и в каждой строке имеются шесть конъюнкторов (элементов «И»), реализующих операцию «логическое умножение». Данные конъюнкторы и формируют частичные произведения. Разрядность результата произведения полиномов $C=A \times B$ определяется числом столбцов матрицы, которое составляет $2n-1$. Для получения произведения достаточно сложить по модулю два результаты каждого столбца матрицы. Для этого строки матрицы 1-6 группируются по два 1-2, 3-4, 5-6. Каждая пара суммируется в отдельном сумматоре по модулю 2 на соответствующих уровнях. Далее рассмотрим подробно сложение частичных произведений.

Биты результатов логического умножения 1-ой и 2-ой строк матрицы суммируются на сумматоре СМ1. Отметим, что при этом из 1-ой и 2-ой строк матрицы бит логического умножения a_0b_0 в сложении не участвует и формирует разряд c_0 результата C . А бит логического умножения a_5b_1 подается на вход СМ4 второго уровня.

Биты 3-4 строк матрицы суммируются на сумматоре СМ2, за исключением бита логического умножения a_0b_2 который подается на вход СМ4 второго уровня, а бит результатов логического умножения a_5b_3 подается на вход СМ5.

Биты строк 5 и 6 матрицы суммируются на сумматоре СМ3, за исключением бита логического умножения a_0b_4 , который подается на вход сумматора СМ5, а результат умножения битов a_5b_5 формирует бит C_{10} произведения C .

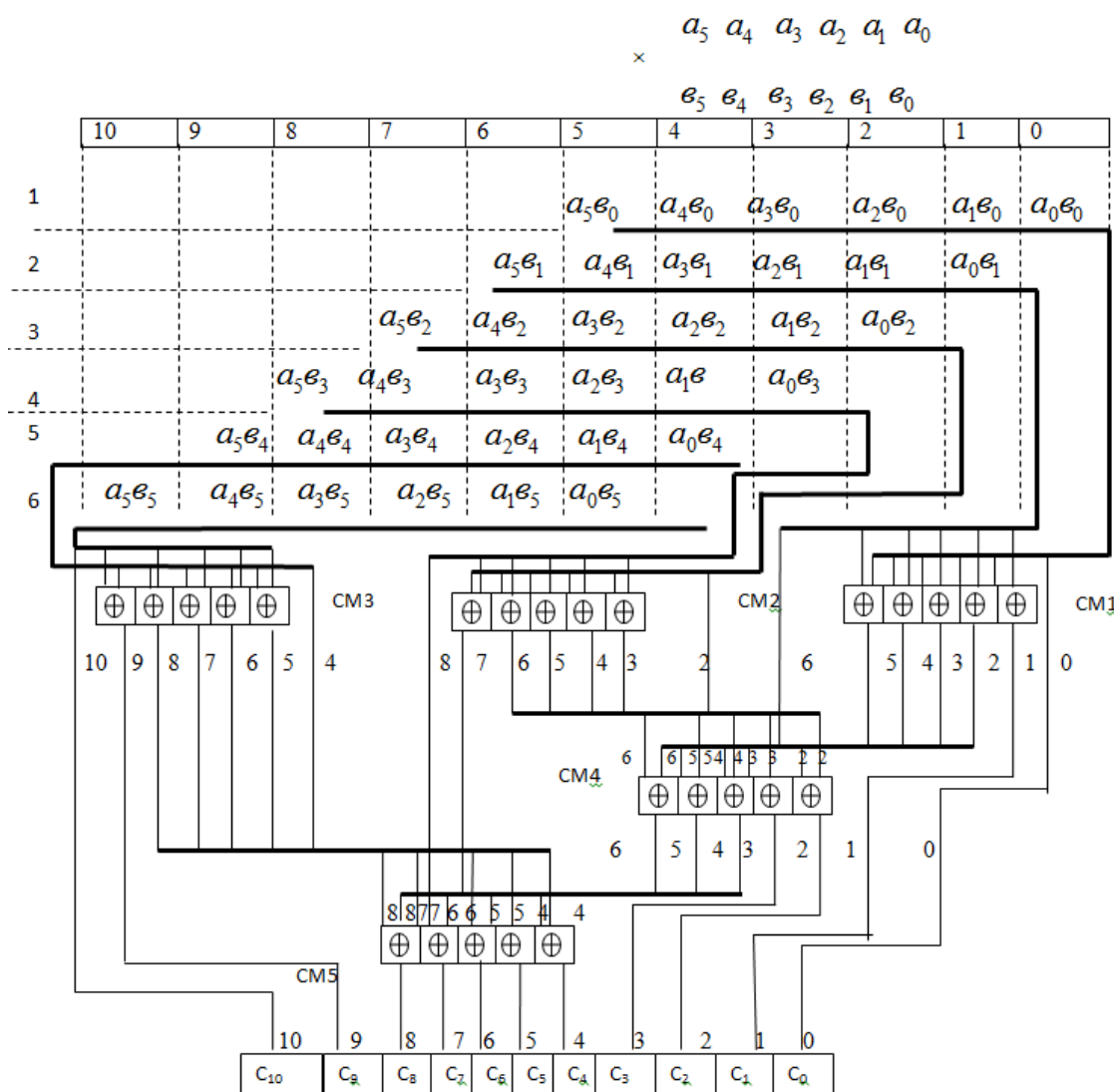


Рисунок 1 – Схема умножения 6-разрядных полиномов А и В на дереве сумматоров

Рассмотрим структуру формирователя частичного остатка (ФЧО). На рисунке 2 приведена структура ФЧО, который состоит из сумматора по модулю два (СМmod2), логического блока (ЛБ) и мультиплексора (MS). Удвоенное значения предыдущего остатка $2r_{i-1}$ подается на первый вход СМmod2 и на вход мультиплексора. На второй вход сумматора подаются коэффициенты модуля неприводимого полинома P . Логический блок (ЛБ) управляет выдачей на выход MS $2r_{i-1}$, если $2r_{i-1} < P$, либо результата сложения по модулю два $2r_{i-1} \oplus P$ с выхода СМmod2.

Теперь на базе схемы умножителя полиномов и формирователей частичных остатков можно построить матричную схему умножителя по модулю неприводимых полиномов. На рисунке 3 приведена схема матричного умножителя по модулю неприводимого полинома для $n=6$.

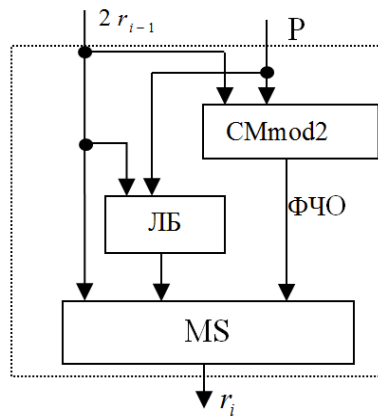


Рисунок 2 – Структура ФЧО

Матричная схема состоит из регистров (входов для умножителя) для хранения бинарного представления полиномов A , B и P . Выходы регистров PrA и PrB связаны с входами конъюнкторов частичного произведения в дереве сумматоров, которые расположены на входах сумматоров $CM1$, $CM2$, $CM3$ первого уровня. Состав дерева сумматоров по модулю два определяются числом строк матрицы частичных произведений. В приведенном примере число таких сумматоров – 5. Из них на первом уровне располагается три, на втором уровне два и на третьем уровне имеется один сумматор. На выходах умножителя формируются разряды произведения $C=c_{10}, c_9, \dots, c_1, c_0$.

Отметим, что при передаче частичных остатков из i -го ФЧО в $i+1$, они сдвигаются на один разряд влево и на место младшего разряда сдвинутого частичного остатка присоединяется следующий старший разряд произведения, подлежащего к обработке.

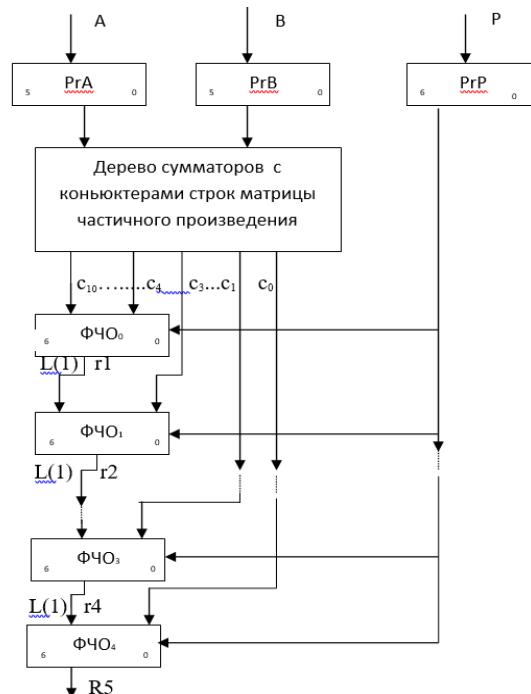


Рисунок 3 – Матричная схема умножителя полиномов по модулю неприводимых полиномов для $n=6$

Расчёт аппаратных затрат и времени задержек в схеме

Подсчитаем количество логических элементов, затрачиваемых на реализацию схемы умножителя полиномов. Аппаратная затрата складывается из числа элементов «И» матрицы частичных умножителей N_{II} , сумматоров по модулю два N и числом разрядов каждого сумматора, которые определяется числом $n-1$, тогда:

$$N_{умн}^6 = N_{II} + (n-1 * N) * 4_{л.э} = 36 + (5 * 5)4 = 36_{л.э} + 25 * 4 = 136_{л.э}.$$

Подсчитаем время, затрачиваемое на умножение двух полиномов $T_{умн}$. Общее время умножения формируется из суммы времени задержек сигналов на схемах «И» матрицы частичных умножителей τ_{II} , временем задержки на элементах однозарядного сумматора по модулю два τ_{M2} и от числа уровней сумматоров L .

Необходимо заметить, что однозарядные сумматоры строятся на четырех трехуровневых схемах И-НЕ [7] и время задержки сигнала на однозарядном сумматоре $\tau_{nr} = 3\tau_{л.э}$.

Тогда $T_{умн}^6 = \tau_{II} + L \cdot 3\tau_{л.э}$ для нашего умножителя $L=3$, тогда $T_{умн}^6 = 1\tau_{л.э} + 3(3\tau_{л.э}) = 10\tau_{л.э}$

В таблице 2 показаны расчёты $N_{лэ}$ и $T_{умн}$ для умножителей полиномов различной разрядности n .

Таблица 2 – Количество элементов и время задержек для различных n

n	$N_{лэ}$	$T_{умн}$
32	4868	$16 \tau_{л.э}$
28	3700	$16 \tau_{л.э}$
23	2465	$16 \tau_{л.э}$
18	1480	$16 \tau_{л.э}$
10	424	$13 \tau_{л.э}$
6	136	$10 \tau_{л.э}$

При подсчете количества логических элементов схемы приведения по модулю $N_{пм}$ необходимо учесть число логических элементов для построения n разрядного сумматора ФЧО, их количество, а также, как было показано выше, четырех логических схем для построения одноразрядного сумматора по модулю два. Кроме того, необходимо учитывать количество логических элементов для построения мультиплексоров N_{ms} , количество которых определяется числом ФЧО и разрядностью сумматора. Время выполнения операций приведения по модулю определяется задержкой сигналов на сумматоре по модулю два, мультиплексоров, которое составляет $3\tau_{лэ} + 2\tau_{лэ} = 5\tau_{лэ}$ и числом ФЧО, которое зависит от разрядности модуля неприводимого полинома.

В таблице 3 приведено количество логических элементов для построения умножителя $N_{\text{умод}}$ время умножения $T_{\text{умн}}$ при различных n .

Таблица 3 – Значения $N_{\text{умод}}$ и $T_{\text{умн}}$ при различных n

Разрядность умножителя [n]	Количество логических элементов для умножить		Время задержки		$N_{\text{умод}}$ [лэ]	$T_{\text{умн}}$ [лэ]
	$N_{\text{умн}}$	$N_{\text{ПМ}}$	$\tau_{\text{умн}}$	$\tau_{\text{ПМ}}$		
6	136	230	16	25	336	41
10	424	666	16	45	1090	61
18	1480	2210	16	85	3690	101
23	1465	3300	16	110	5765	126
28	3700	5400	13	135	9100	148
32	4868	6944	10	155	11812	165

Заключение

В данной статье описана разработка и реализация аппаратного умножителя полиномов по модулю неприводимых полиномов. Реализация операций в непозиционной полиномиальной системе позволяет использовать преимущества модулярной арифметики, а именно отсутствие переноса при сложении, что даёт возможность параллельного выполнения операций.

Разработанная схема была реализована в аппаратном виде на базе схемы программируемой логики технологии FPGA[8]. Данная технология позволяет реализовывать собственные архитектуры вычислительных устройств, и даёт широкие возможности для проведения экспериментов. FPGA обеспечивают аппаратную скорость и надежность, при этом не требуют больших затрат на разработку как при разработке специализированной ASIC-схемы [9].

Схему данного множителя планируется использовать в дальнейшем для программно-аппаратной реализации разработанных алгоритмов шифрования на базе НПСС.

Список использованной литературы

1. Acosta, A. J., Addabbo, T., and Tena-Sánchez, E. (2017) Embedded electronic circuits for cryptography, hardware security and true random number generation: an overview. Int. J. Circ. Theor. Appl., 45: 145–169.
2. Айтхожаева Е.Ж., Тынымбаев С.Т. Аспекты аппаратного приведение по модулю в ассиметричной криптографии Вестник НАН РК. №5. (2014). - Алматы: Наука, 2014. - С.88-99
3. Бияшев Р.Г. Разработка и исследование методов сквозного повышения достоверности в системах обмена данными распределенных АСУ: дисс. докт. тех. наук: 05.13.06: защищена 09.10. 1985: утв. 28.03.1986. - М., 1985. - 328 с.].
4. Бияшев Р.Г., Нысанбаева С.Е. Алгоритм формирования электронной цифровой подписи с возможностью обнаружения и исправления ошибки // Кибернетика и системный анализ. – 2012 г. – Т. 48, № 4. – С. 14-23.
5. Бияшев Р.Г., Нысанбаева С.Е., Бегимбаева Е.Е., Магзом М.М. Разработка модулярных симметричных и ассиметричных криптосистем. Одиннадцатая

Международная Азиатская Школа-семинар "Проблемы оптимизации сложных систем"
27 июля -7 августа 2015 г

6. R.G. Biyashev, S.E. Nyssanbayeva, Ye.Ye.Begimbayeva, M.M.Magzom. Building modified modular cryptographic systems. International Journal of Applied Mathematics and Informatics, Volume 9 2015, P103-109.

7. Орлов С.А., Цилькер Б.Я. Организация ЭВМ и систем. –СПТ.: Питер, 2014,- 688 с.:ИЛ.

8. U. Meyer-Baese, Digital Signal Processing with Field Programmable Gate Arrays, Signals and Communication Technology, Springer, 2007

9. D. Harris, S. Harris. Digital Design and Computer Architecture, 2nd Edition, Morgan Kaufmann, 2012

НЕЧЕТКАЯ МОДЕЛЬ МЕНЕДЖМЕНТА КАЧЕСТВА ТЕХНОЛОГИЧЕСКИХ ПРОЦЕССОВ ПИЩЕВОГО ПРОИЗВОДСТВА

Утепбергенов И.Т., Хисамиев З.Г., Тойбаева Ш. Д., Исабекова Л.С.,
Муслимова А.К.

e-mail: i.utepbergenov@gmail.com, shara_t@mail.ru, lyazzka07@mail.ru,
almira_muslimova@mail.ru

*Институт информационных и вычислительных технологий КН МОН РК,
Казахстан*

Аннотация

В статье описан полученная модель нечеткого управления качеством хлебопекарни для дальнейшего использования и интеграции в модель автоматизированного интеллектуального управления менеджментом качества технологических процессов хлебопекарного производства. В качестве алгоритма нечеткого вывода использован алгоритм Мамдани. Модель состоит из двух уровней, где выход первого уровня является одним из входов для второго уровня. В первом уровне создана база правил для системы определения функционирования процесса, который содержит два входа и один выход. Во втором уровне четыре входа и один выход, где выход из первого уровня "Process", является входом для второго уровня. При тестировании модели оценки определено, что все отклонения вызваны разницей функций принадлежности терм-множеств, и полученные значения относительной погрешности доказывают адекватность представленной модели.

Ключевые слова: *СМК, технологические процессы, база правил модели, алгоритм нечеткого вывода, база оценок экспертов*

Введение

Система менеджмента качества (СМК) для пищевой промышленности – важнейшее условие обеспечения безопасности продовольственной продукции. Ведь безопасность и качество продуктов являются теми необходимыми характеристиками, которые необходимо постоянно контролировать, для чего создаются специальные

службы и разрабатываются системы менеджмента (СМК). В пищевой промышленности безопасность является основным требованием, которое предъявляется потребителями. Очевидно, что употребление в пищу любой пищевой продукции не должно повлечь за собой пищевое отравление, а в составе самих продуктов не должно быть абсолютно никаких вредных ингредиентов. Следовательно, проблема разработки и внедрения на предприятиях пищевой промышленности СМК является как никогда актуальной. Для эффективного решения проблем необходимо использовать потенциал менеджмента путём внедрения систем качества и международных стандартов. Ключевым стандартом для построения процедур в организациях и для подтверждения соответствия, в случае необходимости, является стандарт СТ РК ИСО 9001 Системы менеджмента качества. Требования. Он устанавливает, что «организация должна разработать, задокументировать, внедрить, поддерживать в рабочем состоянии систему менеджмента качества и постоянно улучшать её результативность» [1]. Система менеджмента качества - это также средство для достижения определённых результатов на рынке. В то же время нужно отметить, что внедрение СМК – дело добровольное и отражает состояние процессов производства, дает определенную информацию о предприятии [2-5].

Бизнес-процессы определяются объемом информации, которые передаются между структурами хлебопекарни, их количество зависит от размера пищевого производства и уровней управления [6]. Если процессов верхнего уровня в средней пекарне около 9, то каждый процесс разделяется на 6 подпроцессов, а те, в свою очередь, еще на 5 подпроцессов. Самые важные и критичные подпроцессы описываются в виде процедур как поток определенных действий (операций). Каждая процедура имеет 10 действий. Таким образом, получаем: $9 \cdot 6 \cdot 5 = 270$ подпроцессов, описанных на $1 + 9 + 5 \cdot 6 = 40$ диаграммами, и около 30 диаграмм процедур, которые дают вместе $30 \cdot 5 = 150$ действий. Для каждого процесса (действия) определяются входы и выходы, в среднем, по 5 для процесса, а также набор параметров, описывающих процесс: исполнители, владелец, требования к срокам выполнения и т. д. Очевидно, что информация о деятельности пищевой компании, описывающая бизнес-процессы, объемна. Управление огромным числом взаимосвязей процессов между собой при оптимизации и внесении изменений будет проблематичным для команды специалистов СМК.

1 Выбор математического аппарата

Математический аппарат, используемый в традиционных методах автоматического управления, не всегда в полной мере может удовлетворить нуждам современного производства. Поэтому в условиях неопределенности используются такие информационные технологии, как экспертные системы, нейронные сети, нечеткие системы, генетические алгоритмы и ряд других [7]. В их основе лежит попытка некоторой формализации деятельности головного мозга человека и функционирования живых организмов.

Для обработки процессов СМК пищевого производства характерна работа в условиях неопределенности, поэтому актуальной является задача нахождения эффективного метода управления и построения оптимальной модели управления.

При автоматизации управления технологическими процессами пищевого производства автоматизированная система управления должна основываться на экспертных знаниях, что возможно только с использованием интеллектуальных технологий управления.

Проекты по разработке СМК (и деятельность по дальнейшему поддержанию ее в рабочем состоянии) отличаются от многих других большим объемом анализируемой и вырабатываемой информации. В этом заключается особенность таких проектов, которая

обязательно должна учитываться при планировании их методического и технического обеспечения.

Наиболее перспективными являются математический аппарат нейронных сетей и системы с нечетким выводом. Преимуществом систем с нечётким выводом является то, что анализ осуществляется в том случае, если оценка исходных экспериментальных данных носит субъективный характер и не может быть представлена в явной числовой форме. Особенно ярко преимущества проявляются при проектировании многокомпонентных пищевых продуктов, качество которых оценивается по результатам сенсорного анализа.

2 Предлагаемая модель

На первом уровне модели в качестве входных данных используем правильность описания разработанных процессов (вместо полноты разработанности документации, так как нет смысла создавать СМК ради бумаг) и несоответствия, возникшие в работе процесса или найденные в результате проведения аудита. Данные входные переменные будут определять правильность функционирования процессов.

Второй уровень рассматривает данные по выполнению целей, процессов (выходной параметр первого уровня), удовлетворенности потребителей и реализации КД/ПД, который включит в себя информацию по выполнению решений предыдущих анализов. Параметр «предложения по изменениям» в качестве входной переменной рассматриваться не будет, так как все предложения будут определяться после анализа и определения наиболее критичных параметров управления.

Двухкаскадная модель предполагает создание двух систем нечеткого вывода, причем выход первого уровня является одним из входов второго. Поэтому сначала создана база правил для системы определения функционирования процесса (таблица 1), содержащая два входа (правильность описания – Description, несоответствия – Nesootvet) и один выход (правильность функционирования процессов – Process).

Таблица 1 – База нечетких правил модели 1 уровня

x_1	x_2			
		DN	DA	DB
	NN	PB	PB	-
	NA	PA	PA	PN
	NB	PA	PN	PN

При решении задачи приходится оперировать лишь приближенными значениями входных параметров задачи. Для решения задачи логично использован аппарат теории нечетких множеств и нечеткой логики [8-11].

Для создания базы правил необходимы экспертные оценки, которые можно представить множеством пар

$$(x_1(i), x_2(i), d(i)), \quad i = 1, 2, \dots \quad (1)$$

где $x_1(i)$, $x_2(i)$ - входные переменные модуля нечеткой системы, а $d(i)$ - ожидаемая оценка функционирования процесса.

Пространство входных и выходных переменных разделено на области (терм-множества). Для этого заданы их максимальные и минимальные значения. Каждый интервал разделяется на $2N + 1$ терм-множеств:

– для переменной “Nesootvet” рассматривается 3 области ($N = 1$): NN (Количество несоответствий Малое), NA (Среднее), NB (Большое);

– для переменной “Description” рассматривается 3 области ($N = 1$): DN (Ошибок описания Мало), DA (Средне), DB (Много);

– для переменной “Process” рассматривается 3 области ($N = 1$): PN (Процессный подход функционирует плохо) PA (Средне), PB (Хорошо);
и определяется его интервал и функция принадлежности (ФП).

Для упрощения нечеткой арифметики, т.е. сложных вычислений, в качестве функции принадлежности терм-множества NA используется функция плоского нечеткого числа типа L-P

$$L(x) = P(x) = \frac{1}{1 + |x|^p}, p > 0 \quad (2)$$

с функцией принадлежности

$$\mu(x) = \begin{cases} L\left(\frac{m_1 - x}{\alpha}\right) & , x \leq m_1 \\ 1 & m_1 \leq x \leq m_2 \\ P\left(\frac{x - m_2}{\beta}\right) & , x \geq m_2 \end{cases} \quad (3)$$

где m - действительное число, называемое средним значением нечеткого числа $A(\mu_A(m) = 1)$, α - положительное действительное число или левосторонний разброс, β - правосторонний разброс. Увеличение разброса приводит к более нечеткому числу A . Нечеткое число типа L-P записывается в виде

$$A = (m_1, m_2, \alpha_A, \beta_A)_{LP} = (4, 6, 5, 5)_{LP} \quad (4)$$

В среде моделирования Matlab общий вид функции принадлежности типа L-P носит название gbellmf – обобщенная колоколообразная ФП (рисунок 1, область 2) [9].

$$\mu(x) = \frac{1}{1 + \left(\frac{x - c}{a}\right)^{2b}}, (a = 2, b = 2, c = 5) \quad (5)$$

Для терм-множества NN используется z – подобная ФП zmf

$$\mu(x) = \begin{cases} 1, & x \leq a = 0.4 \\ \text{нелинейная аппроксимация}, & a < x < b \\ 0, & x \geq b = 3.6 \end{cases} \quad (6)$$

Smf – s – подобная ФП описывает терм-множество NB

$$\mu(x) = \begin{cases} 0, & x \leq a = 6.4 \\ \text{нелинейная аппроксимация}, & a < x < b \\ 1, & x \geq b = 9.6 \end{cases} \quad (7)$$

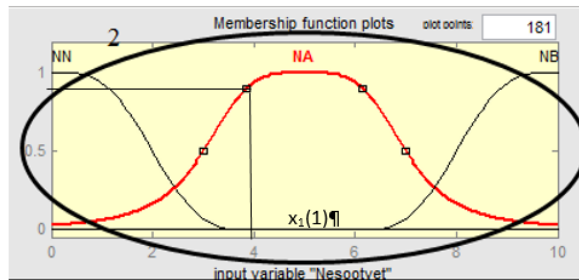


Рисунок 1 – Терм-множества входной переменной “Nesootvet”

Разделение переменной “Description” на области аналогично первой переменной (рисунок 2).

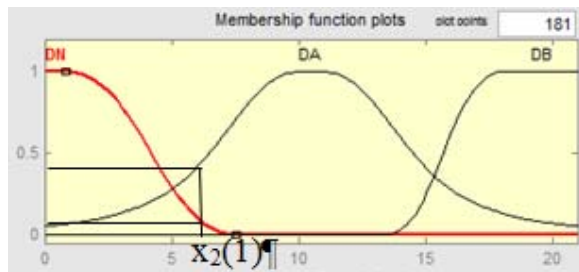


Рисунок 2 – Терм-множества входной переменной “Description”

Выход модели “Process” использует трапецевидную форму принадлежности trapezf (рисунок 3) для терм-множеств PN и PB

$$\mu(x) = \begin{cases} 0, & x \leq a \\ \frac{x-a}{b-a}, & a \leq x \leq b \\ 1, & b \leq x \leq c \\ \frac{d-x}{d-c}, & c \leq x \leq d \\ 0, & d \leq x \end{cases} \quad (8)$$

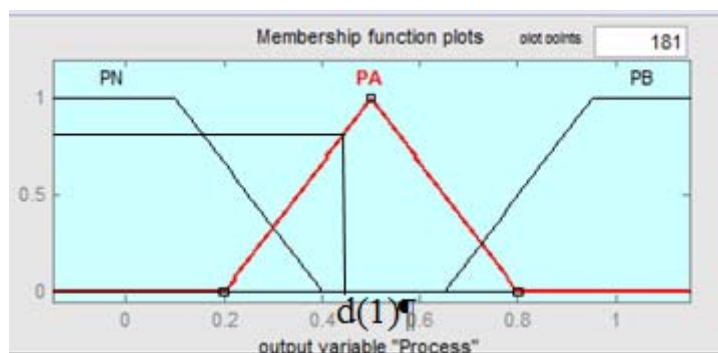


Рисунок 3 – Терм-множества выходной переменной “Process” и треугольную ФП trimpf для терм-множества PA

$$\mu(x) = \begin{cases} 0, & x \leq a \\ \frac{x-a}{b-a}, & a \leq x \leq b \\ \frac{c-x}{c-b}, & b \leq x \leq c \\ 0, & c \leq x \end{cases} \quad (9)$$

Для построения базы правил на основе оценок экспертов необходимо определить степень принадлежности экспертных данных $(x_1(i), x_2(i), d(i))$ к каждому терм-множеству. На рисунке 1 степень принадлежности $x_1(1)$ к терм-множеству NA равна 0.9, к остальным областям – 0. Аналогично для $x_2(1)$ (рисунок 2) степень принадлежности к DN=0.1, к DA=0.4, к DB=0, для $d(1)$ (рисунок 3) степень принадлежности к PA=0.8, PN=PB=0. Сопоставив экспертные данные $x_1(i), x_2(i), d(i)$ терм-множествам, в которых они имеют максимальные степени принадлежности, записываются следующее правило [10].

$$\begin{aligned} & (x_1(1), x_2(1), d(1)) \Rightarrow \\ & \{x_1(1)[\max: 0.9 \text{ в } NA], x_2(1)[\max: 0.4 \text{ в } DA], d(1)[\max: 0.8 \text{ в } PA]\} \Rightarrow \quad (10) \\ & PP^1 : \text{Если}(x_1 \text{ это } NA \text{ И } x_2 \text{ это } DA), \text{ то } d \text{ это } PA \end{aligned}$$

Так как количество экспертных оценок велико, по каждой оценке можно сформулировать одно правило, некоторые из которых могут быть противоречивыми, либо повторяться. Поэтому чтобы разрешить данную проблему и уменьшить количество правил, каждому правилу приписывается степень истинности (вес правила) и из противоречащих правил выбирается то у которого степень истинности выше. Для правила вида (10) степень истинности равна:

$$СИ(PP^1) = \mu_{NA}(x_1) \cdot \mu_{DA}(x_2) \cdot \mu_{PA}(d) = 0.9 \cdot 0.4 \cdot 0.8 = 0.288 \quad (11)$$

База правил записывается в таблицу 1, затем заносится в Matlab (рисунок 4).

1. If (Nesootvet is NB) and (Description is DB) then (Process is PN) (1)
2. If (Nesootvet is NA) and (Description is DA) then (Process is PA) (1)
3. If (Nesootvet is NN) and (Description is DN) then (Process is PB) (1)
4. If (Nesootvet is NB) and (Description is DN) then (Process is PA) (1)
5. If (Nesootvet is NB) and (Description is DA) then (Process is PN) (1)
6. If (Nesootvet is NN) and (Description is DA) then (Process is PB) (1)
7. If (Nesootvet is NA) and (Description is DN) then (Process is PA) (1)
8. If (Nesootvet is NA) and (Description is DB) then (Process is PN) (1)

Рисунок 4 – Создание базы правил в Matlab

Степень адекватности созданной модели с помощью оценки влияния входных переменных на выход можно увидеть в программе просмотра поверхности нечеткого вывода (рисунок 5).

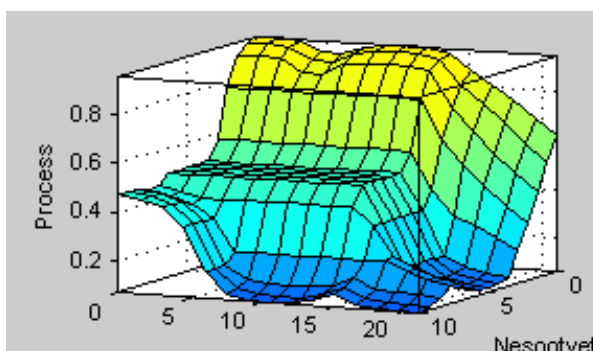


Рисунок 5 – Поверхность нечеткой системы определения функционирования процесса

Дефазификация. Методом дефазификации выбран метод центра тяжести

$$y = \frac{\int_{\min}^{\max} x \cdot \mu(x) dx}{\int_{\min}^{\max} \mu(x) dx} \quad (12)$$

Проверка на адекватность созданной модели проводится также и в системе просмотра правил (рисунок 6). Результаты анализа системы приведены в таблице 2, т.к. относительная погрешность системы не превышает 5% по отношению к экспертным данным, то считаем разработанную модель адекватной.

Таблица 2 – Результаты проверки созданной модели нечеткого вывода

№	Nesootvet	Description	Process	$\delta, \%$
1	1	1	0.844	4,09
2	5	10.5	0.5	0,00
3	9	20	0.0901	0,14
4	2	19	0.409	5,00
5	8	2	0.437	2,89

6	7	7	0.451	1,96
7	4	15	0.354	1,67
8	3	14	0.527	1,35

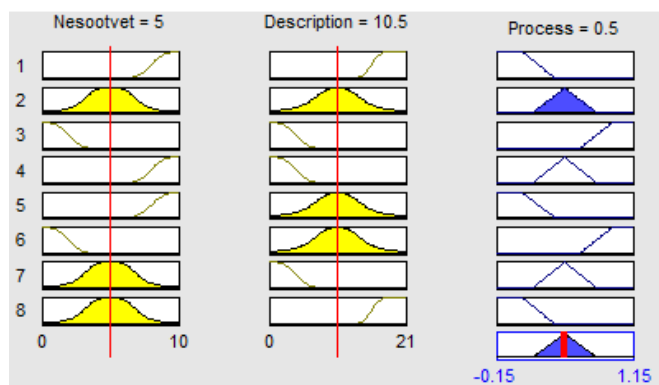


Рисунок 6– Просмотр правил нечеткого вывода при значениях $x_1(i) = 5$, $x_2(i) = 10.5$

Создание 2 уровня модели оценки функционирования СМК аналогично созданию 1 уровня:

1) Входные переменные:

- степень достижения целей – Goal (min=0, max=100);
- правильность функционирования процессов – Process (min=0, max=1);
- степень удовлетворенности потребителей – Custom (min=0, max=1);
- степень реализации КД/ПД – KD/PD (min=0, max=100).

Выход модели – оценка работоспособности СМК – Mark (0-100).

Разделение на области (терм-множества) и задание функций принадлежности:

- Goal: NG (Цели не достигнуты – плохо), NA (хорошо), NB (отлично) (Рисунок 7);

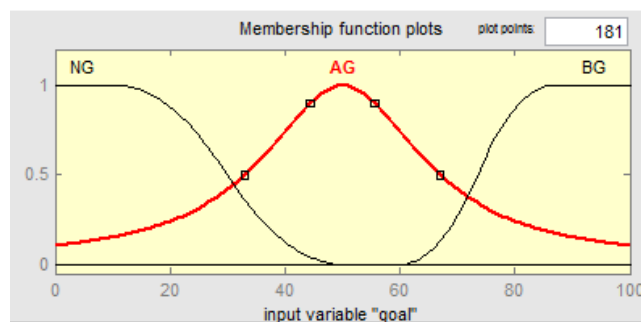


Рисунок 7– Терм-множества входной переменной “Goal”

- для Process все данные аналогичны 1-му уровню модели;
- Custom: CN (не удовлетворен), CA (средне удовлетворен), CB (удовлетворен) (Рисунок 8);

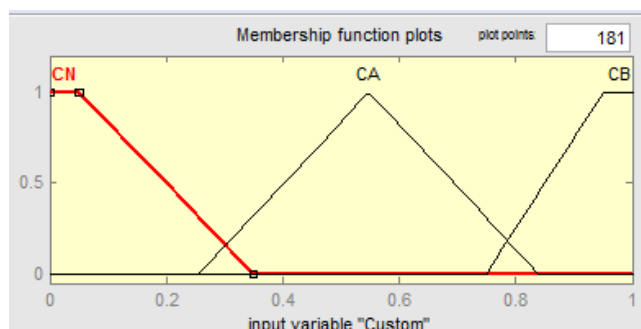


Рисунок 8 – Терм-множества входной переменной “Custom”

– KD/PD: NKD (плохо), AKD (хорошо), BKD (отлично) (Рисунок 9);

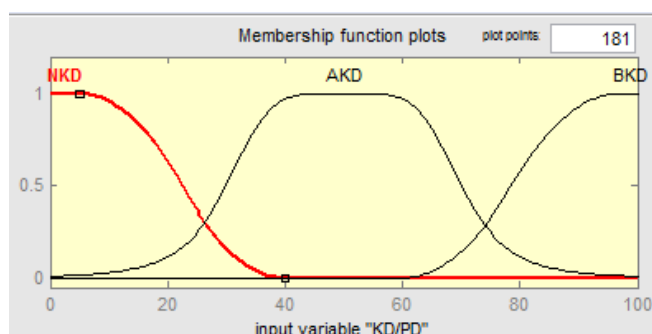


Рисунок 9 – Терм-множества входной переменной “KD/PD”

– Mark: 1, 2, 3, 4, 5 (рисунок 10).

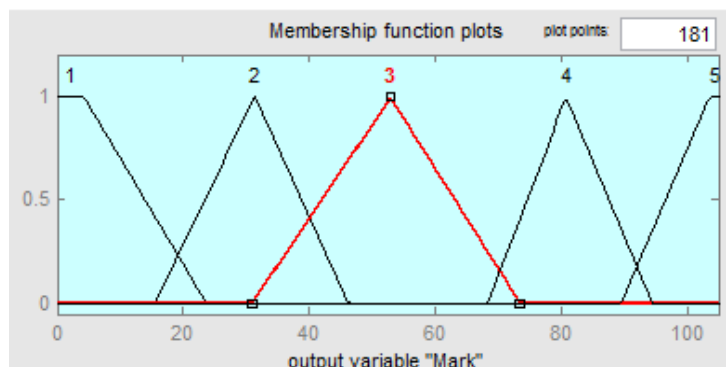


Рисунок 10 – Терм-множества входной переменной “Mark”

Так как переменные “Goal” и “KD/PD” являются чисто числовыми данными, то функции принадлежности этих переменных выбраны по формулам (9, 10, 11), которые приводят их к нечеткости. Для переменных “Custom” и “Mark” функции принадлежности определяются по формуле (12).

База правил модели, созданная по экспертным оценкам, а также оптимизированная за счет степеней истинности правил (общее количество правил $T^{ex/пер} = 3^4 = 81$, после оптимизации 30) показана в таблице 3.

Таблица 3 – База правил 2 уровня модели

№	Goal	Process	Custom	KD/PD	Mark	№	Goal	Process	Custom	KD/PD	Mark
1	NG	PN	CN	NKD	1	16	NG	PN	CA	NKD	1
2	AG	PN	CN	NKD	1	17	NG	PN	CB	NKD	1
3	BG	PN	CN	NKD	2	18	AG	PA	CN	AKD	3
4	NG	PA	CA	AKD	2	19	AG	PA	CB	AKD	4
5	AG	PA	CA	AKD	3	20	BG	PB	CN	BKD	4
6	BG	PA	CA	AKD	4	21	BG	PB	CA	BKD	5
7	NG	PB	CB	BKD	3	22	NG	PN	CN	AKD	1
8	AG	PB	CB	BKD	5	23	NG	PN	CN	BKD	1
9	BG	PB	CB	BKD	5	24	AG	PA	CA	NKD	3
10	NG	PA	CN	NKD	1	25	AG	PA	CA	BKD	4
11	NG	PB	CN	NKD	2	26	BG	PB	CB	NKD	4
12	AG	PN	CA	AKD	2	27	BG	PB	CB	AKD	5
13	AG	PB	CA	AKD	4	28	NG	PB	CN	BKD	2
14	BG	PN	CB	BKD	3	29	NG	PB	CA	BKD	2
15	BG	PA	CB	BKD	5	30	NG	PB	CB	AKD	3

Проверка на адекватность созданной базы правил на основе анализа поверхности дала положительные результаты. Результаты тестирования модели указаны в таблице 4.

Таблица 4 – Тестирование созданной модели

№	Goal	Process	Custom	KD	Mark	$\delta, \%$	№	Goal	Process	Custom	KD	Mark	$\delta, \%$
1	1	0	0	1	7,8	1,27	16	2	0,2	0,6	20	11,4	2,70
2	60	0	0	1	8,47	0,35	17	2	0,2	0,8	20	14,9	2,76
3	90	1	0	1	27,7	4,15	18	55	0,6	0,2	60	52,4	0,38
4	2	0,55	0,55	55	35,7	4,08	19	55	0,6	0,8	60	67,1	0,00
5	50	0,5	0,5	50	52,4	0,19	20	95	0,95	0,05	95	81,2	0,12
6	98	0,55	0,55	55	73,7	3,03	21	95	0,95	0,5	95	99,1	0,00
7	5	0,98	0,98	98	56,2	1,44	22	15	0,15	0,15	50	8,73	0,80
8	50	0,97	0,9	97	99,7	1,12	23	15	0,15	0,15	90	8,73	0,80
9	100	1	1	100	100	0,20	24	40	0,5	0,5	10	51,7	0,58
10	7	0,6	0,2	60	52,2	0,38	25	40	0,5	0,5	90	76,7	0,65
11	7	0,95	0,2	10	31	0,00	26	97	0,97	0,97	7	81,5	0,00
12	55	0,25	0,55	55	38,6	0,52	27	97	0,97	0,97	67	99,6	0,20
13	55	0,85	0,55	55	81,2	0,12	28	5	0,97	0,17	97	31	0,00
14	85	0,25	0,95	95	58,8	0,00	29	5	0,97	0,57	97	32,1	0,94
15	85	95	0,65	0,95	98	0,10	30	5	0,97	0,97	57	52,4	0,38

Выводы

Графики зависимостей принимаемого нечеткого решения от любой входной переменной при фиксированном значении другой переменной представляют собой монотонно возрастающие или монотонно убывающие зависимости как на первом, так и

на втором уровне. Т.е. для предложенных правил нечеткого вывода на каждом из двух уровней исключается возможность принятия противоречивых решений.

Результаты тестирования модели оценки функционирования процесса: все отклонения вызваны разницей функций принадлежности терм-множеств, а также значения относительной погрешности не превышают 5% по сравнению с экспертными данными, что свидетельствует об адекватности модели.

Таким образом, анализ поверхностей нечеткого вывода первого и второго уровней показал высокую адекватность решений, принимаемых на основе предложенных правил нечеткого вывода.

Созданные на основе модели база знаний и механизм вывода решений составляют основу экспертной системы, использование которой в условиях производства позволяет снизить время на технологические простои и улучшить качество продукции. Практической реализацией разработанных алгоритмов является создание программных средств для автоматизированного решения задачи.

Использование экспертной системы в менеджменте качества технологических процессов в хлебопекарном производстве позволит уменьшить затрачиваемое время в 2 - 5 раз по сравнению с традиционными методами.

Разработанная модель позволяет прогнозировать показатель качества производства хлебобулочных изделий и управлять данным показателем с помощью таких факторов, как количество предоставленных услуг, эксклюзивность и стоимость услуг. Это позволит менеджменту хлебопекарни определить соответствующие значения влияющих факторов с целью обеспечения необходимого уровня качества производства хлебобулочных изделий, тем самым обеспечивая себе лидирующие позиции на пищевом рынке с высокой конкуренцией. Перспективой дальнейшего исследования является разработка нечеткой модели конкурентоспособности производства хлебобулочных изделий с добавлением таких факторов, как качество информационных технологий и качество обслуживания, и дальнейшим внедрением в модель интеллектуального управления производства хлебобулочных изделий.

Список использованных источников

1. СТ РК ИСО 9000-2007 (IDT, ISO 9000:2005) Система менеджмента качества. Основные положения и словарь
2. Статистический сборник Казахстана «Статистические показатели социально-экономического развития Республики Казахстан и его регионов». 2010.
3. Указ Президента Республики Казахстан от 19 марта 2010 года № 958 «Об утверждении Государственной программы форсированного индустриально-инновационного развития на 2010-2014 гг».
4. Васин, С.Г. Управление качеством. всеобщий подход: Учебник для бакалавриата и магистратуры / С.Г. Васин. - Люберцы: Юрайт, 2016. - 404 с.
5. Горбашко, Е.А. Управление качеством: Учебник для СПО / Е.А. Горбашко. - Люберцы: Юрайт, 2016. - 463 с.
6. Дунченко, Н.И. Управление качеством в отраслях пищевой промышленности: Учебное пособие / Н.И. Дунченко, М.Д. Магомедов, А.В. Рыбин. - М.: Дашков и К, 2016. - 212 с.
7. Усков А.А. Системы с нечеткими моделями объектов управления. Монография. – Смоленск: СФРУК, 2013. – 153 с.: ил.
8. Леоненков А.В. Нечёткое моделирование в среде MATLAB и fuzzyTECH. - СПб.: БХВ-Петербург, 2003. - 736 с.

9. Sivanandam S.N., Sumathi S., Deepa S.N. Introduction to Fuzzy Logic Using MATLAB
10. Amos Gilat, MATLAB –An Introduction with Applications (Wiley India Pvt. Ltd., New Delhi) 2013
11. Zafer Aydogmus, Implementation of a fuzzy based level control using SCADA, Expert Systems with Applications, 36 (2009), 6593- 6597.

ЭЛЬ-ГАМАЛЬ ШИФРЛАУ АЛГОРИТМІНІҢ МОБИЛЬДІК ҚОСЫМШАСЫН ҚҰРУ

Хомпыш А.
e-mail: ardabek@mail.ru

*ҚР БжҒМ ҒК, Ақпараттық және есептеуіш технологиялар институты,
Қазақстан*

***Аңдатпа.** Бұл мақалада Эль-Гамаль шифрлау алгоритмі қарастырылған. Тәжірибеде қолдану және оңтайландыру мақсатында алгоритм жүзеге асырылды. Ол үшін қазіргі заманауи бағдарламалық тілдердің бірі PHP, javascript, java, android studio және framework7 қолданылып осы шифрлау алгоритмін жүзеге асыратын мобильді қосымша құрылды.*

Ақпараттарды шифрлауда қолданылатын алгоритмдердің бірі ол Эль-Гамаль криптожүйесі. 1985 жылы Эль-Гамаль ұсынған алгоритмі ақпараттарды шифрлау үшін және электронды сандық қолтаңбағада қолданылатын алгоритм [1]. Эль-Гамаль ашық кілтті криптожүйесін Диффи-Хеллмен кілт алмасу моделі ретінде қарастыруға болады. Эль-Гамаль алгоритмінің кәуіпсіздігі дискретті логарифмнің күрделі есептелу мәселесіне негізделген [2].

Мобильды қосымшаның тағайындалуы. «El Gamal» мобильды бағдарламалық қосымшасы, қазіргі таңда жаппай пайдаланатын қалта телефондарында ақпаратты қорғау мәселелерінің бірі ақпаратты жылдам шифрлау және дешифрлау үшін, жасалынып отыр.

Функциональдық мүмкіндігі. El Gamal мобильды бағдарламалық қосымшасын пайдалаушылар келесі мүмкіндіктерге ие:

- Эль-Гамаль дәстүрлі алгоритмдері туралы теориялық мәлімет алады (1-сурет);
- кілттерді жасау үшін примитивті элементті іздейді;
- жабық кілтті есептеп шығарады;
- ақпараттарды шифрлайды және дешифрлайды (2-сурет); .

Негізгі техникалық сипаттамасы.

«El Gamal» бағдарламалық мобильды қосымшасы, 23 МБ орын алады және процессор жиілігі 1.2 ГГц, оперативті жады көлемі 2ГБ жоғары, сиымдылық көлемі 8ГБ жоғары android жүйесіндегі кез-келген телефонға арналған.

Бағдарламалау тілдері:

PHP, Javascript, java, android studio, framework7 [3].

Эль-Гамаль шифрлау алгоритмі.

1. Эль-Гамаль алгоритмінде ақпараттарды шифрлау үшін кілттерді есептеу.

а) Құпия кілтті және ашық кілтті таңдау үшін үлкен P_i жай сандары және G_i үлкен бүтін сандары таңдалып алынады. Мұндағы G_i Z_p сақинасындағы U_p тобының примиттивті элементі деп аталынады және ол $\varphi(p_i)$ жүйесінің p модулі бойынша толық келтірілген жүйесін құрайтын элемент мұндағы $i = \overline{1, n}$.

ә) Пайдаланушылар өздерінің құпия кілттерін x_i $1 < x_i < p_i - 1$ таңдап алады, мұндағы $i = \overline{1, n}$.

б) Пайдаланушылар келесі формула бойынша ашық кілттерін β_i есептейді:

$$\beta_i = \alpha_i (\text{mod } p_i) \quad (1)$$

Пайдаланушылар өздерінің ашық кілттерін $\{\alpha_i, \beta_i, p_i\}$ ашық жариялайды да, жабық кілттерін $\{x_i\}$ құпия ұстайды.

2. Пайдаланушылар m_i ашық мәтінді шифрлау үшін кез-келген бүтін r_i таңдалынып алынады. Таңдап алу талабы $1 < r_i < p_i - 1$, $i = \overline{1, n}$.

3. Пайдаланушы келесі формулалар арқылы a_{1i} , b_{2i} Шифрмәтінді алады да екінші пайдаланушыға жібереді.

$$a_{1i} = \alpha_i^{r_i} \text{mod } p_i \quad (2)$$

$$b_{2i} = m_i \beta_i^{r_i} \text{mod } p_i \quad (3)$$

Шифрмәтіндер $\{a_{1i}, b_{2i}\}$ тең.

4. Шифрмәтінді қабылдап алған пайдаланушы ақпаратты ашу үшін x_i қолдану арқылы келесі формуламен ашық мәтінді алады [1,2].

$$m_i = b_{2i} (a_{1i}^{x_i})^{-1} \text{mod } p_i \quad (4)$$

Мысалы: $p=7$, ашықмәтін $M=6$ санын шифрлау керек болсын. Мұнда бізде жұмыс негіздерінің саны p_i , яғни $i=1$ тең.

1. Кілттерді жасау.

а) Ол үшін g -і таңдап аламыз, ол $\varphi(p)$ жүйесінің p модулі бойынша толық келтірілген жүйесін құрайтын элементтер g біздің жағыдайда мынаған тең.

$$g = 3;$$

ә) Пайдаланушылар өздерінің құпия кілттерін $1 < x < p - 1$ аралықта таңдап алады.

$$x=5$$

б) (1)-шы формула арқылы β_i ашық кілттерін есептейміз:

$$\beta_i = \alpha_i \pmod{p_i} = 3^5 \pmod{7} = 5$$

Пайдаланушылар өздерінің ашық кілттерін: $\{3, 5, 7\}$ ашық жариялайдыда, жабық кілтті: $\{5\}$ құпия ұстайды.

2. Енді бізге ашық мәтінді $M=6$ шифрлауды бастайық ол үшін бізге кездей соқ r санын $1 < r_i < p_i - 1$ аралықта таңдап алынады. Біздің жағыдайда:

$$r = 5.$$

3. Шифрмәтінді алу үшін (2), (3) формулалар арқылы есептейміз:

$$a_{1i} = \alpha_i^{r_i} \pmod{p_i} = 3^5 \pmod{7} = 5$$

$$b_{2i} = m_i \beta_i^{r_i} \pmod{p_i} = 6 * 5^5 \pmod{7} = 4$$

Шифрмәтін: $\{5, 4\}$.

4. Шифрмәтінді дешифрлау үшін (4) формуламен есептейміз:

$$m_i = b_{2i} (a_{1i}^{x_i})^{-1} \pmod{p_i} = 4 * 5^{p-1-x} \pmod{7} = 4 * 5^{7-1-5} \pmod{7} = 6$$

The image shows a web application interface for the ElGamal algorithm. It is divided into two main sections: a left sidebar with a menu and a main content area on the right.

Left Sidebar:

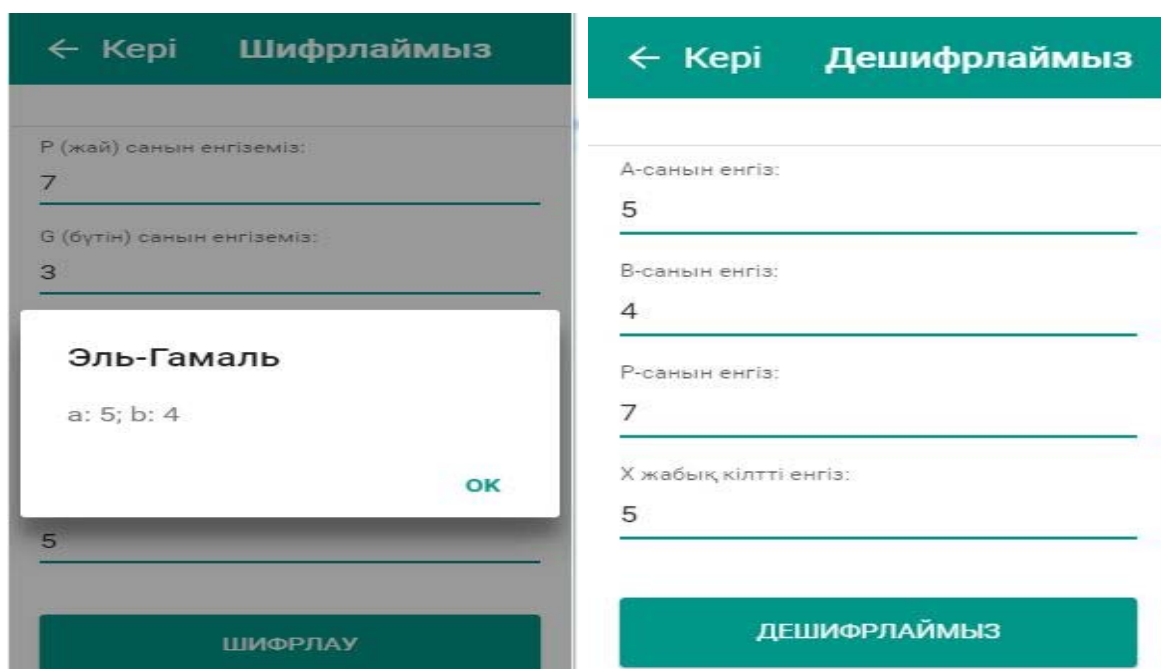
- Menu icon (three horizontal lines).
- Header: Эль-Гамал шифрлау...
- Text: 1985 жылы Эль-Гамаль (T.ElGamal) ұсынған ассиметриялық алгоритм әмбебап. Ол барлық үш негізгі есептерді шешуге пайдалану мүмкін: деректерді шифрлау үшін, цифрлық қолды құрастыру үшін және ортақ кілтті келістіру үшін. Одан басқа, парольді тексеру үшін, хабардың парларлығын дәлелдеу үшін алгоритмды түрлендіруге болады.
- Buttons: ШИФРЛАУ (Encryption) and ДЕШИФРЛАУ (Decryption).

Main Content Area:

- Header: ← Кері Шифрлаймыз
- Input fields:
 - P (жай) санын енгіземіз: 7
 - G (бүтін) санын енгіземіз: 3
 - X санын енгізіңіз: (1 < X < P) 5
 - M санын енгізіңіз: (M < P) 6
 - K санын енгіз: (1 < K < P-1) 5
- Button: ШИФРЛАУ (Encryption)

1-сурет. Теориялық мәліметтер және шифрлау терезелері

Шифрлау батырмасын басу арқылы шифрмәтінді аламыз (2-сурет). Мұндағы шифрмәтіннен ашықмәтінді алу үшін жабық кілттің көмегімен дешифрлау батырмасына кіріп қажетті мәндерді енгіземіз (2-сурет).



2-сурет. Шифрлау және дешифрлеу терезелері

Қортынды. Жасалынып отырған жұмыс ақпаратты қорғауда Эль-Гамаль алгоритмін жан-жақты зерттеп, тиімділігін арттыру, криптотұрақтылығын анықтау, қолданыс аясын кеңейту сонымен қатар бағдарламалық кешенін қолжетімді қосымшаларға арнап жасауды көздеген болатын. Қарастырылған мысалда жұмыс негіздерінің саны p_i , яғни $i=1$ тең болғандағы көрсетілген. Мобильді қосымшаның артықшылығы қалта телефон арқылы жылдам есептеуге, уақытты тиімді пайдалануға ыңғайлы.

Қолданылған әдебиеттер

1. Асамбаев А.Ж. Криптография негіздері. Оқу құралы. – Павлодар, 2012. – 173 бет.
2. Капалова Н.А. Алгоритм шифрования на базе непозиционных полиномиальных систем счисления с использованием системы Эль-Гамалья // Инфокоммуникационные технологии в науке, производстве и образовании: Пятая Межд.науч.-кон.-Ч. II.-г.Ставрополь, Северо-Кавказ.гос.тех.ун-т, 2-6 мая, 2012.-С.225-227.
3. Варакин М.В. Разработка мобильных приложений под Android.- Москва, 2012.- 128 стр.

РАЗРАБОТКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ СИНТЕЗА ИНТЕЛЛЕКТУАЛЬНОЙ СИСТЕМЫ УПРАВЛЕНИЯ СЛОЖНЫМ ОБЪЕКТОМ НЕФТЕГАЗОВОЙ ОТРАСЛИ

Ширяева О.И., Самигулин Т.И.
e-mail: oshiryayeva@gmail.com

*Институт информационных и вычислительных технологий КН МОН РК,
Казахстан*

Аннотация. *Представлены результаты разработки программного обеспечения синтеза интеллектуальной системы управления сложным объектом нефтегазовой отрасли. С использованием генетического алгоритма, в среде MATLAB, с использованием программного обеспечения, GeneticPRegulator получены коэффициенты типовых ПИ-регуляторов изолированных подсистем сложной системы управления процессом очистки газа, обеспечивающих минимум интегрального квадратичного критерия качества. Для решения вопроса влияния взаимосвязей на процессы подсистем использовался механизм построения развязывающей матрицы, при включении в схему которой многоконтурная система вырождается в набор независимых подсистем.*

Введение. В настоящее время задачи разработки программного обеспечения для внедрения интеллектуальной иммунносетевой технологии в производство. Интеллектуальные подходы, лежащие в основе синтеза Smart-систем, такие, как генетические алгоритмы, алгоритмы оптимизации колоний муравьев, роя частиц и нейронные сети стали высокоэффективными инструментами для решения сложных задач оптимизации. Генетическое программирование широко применяется для решения проблем и в нефтегазовой отрасли. В научной работе [1] рассматриваются теоретические особенности алгоритма генетического программирования, описание его основных компонентов, таких как инициализация популяции, оценки индивидов, генетические операторы и схемы селекции. При этом рассматривается применение генетического программирования для выполнения инженерных задач в нефтяной промышленности. В статье [2] предлагается использовать многоцелевой генетический алгоритм (NSGA-II) для оптимизации хранения диоксида углерода и повышения нефтеотдачи в нефтяных пластах. На основе рассмотрения экономических параметров, таких как цены на нефть, налог на углекислый газ и т.д. данный метод позволяет вносить поправки в сценарий управления производством. Актуально применение нечеткой логики и генетических алгоритмов для нефтяной разведки. В научной работе [3] описывается применение таких методов для оценки проницаемости пласта вокруг забоя скважины. В статье [4] рассматривается оптимальное определение реологических параметров буровых растворов с использованием генетических алгоритмов.

Интеллектуальные алгоритмы позволяют решать оптимизационные задачи для процесса синтеза промышленных регуляторов для многомерных и многосвязных объектов управления с высокой точностью и быстродействием вычислений. Однако при анализе и синтезе многомерных и многосвязных систем возникает много проблем, связанных с влиянием взаимосвязей на свойства всего объекта. Методы решения данной проблемы на основе процедур синтеза регулятора с компенсатором взаимосвязей представлены в работах [5-6].

В данной статье решается актуальная задача разработки программного обеспечения синтеза интеллектуальной системы управления сложным объектом нефтегазовой отрасли на основе метода генетического алгоритма и процедуры компенсации взаимосвязей – процедуры развязывания.

1 Дистилляционная колонна, как объект нефтегазовой отрасли. В качестве объекта нефтегазовой отрасли рассматривается дистилляционная колонна, которая является наиболее распространенным инструментом для процесса очистки природного газа от различных примесей.

Перегонка нефти в дистилляционных колоннах является наиболее популярным и важным методом разделения нефтяных (газовых) фракций в нефтегазовой отрасли. Обычная ректификационная колонна (рисунок 1) содержит: вертикальную колонну, в которой тарелки или пластины используются для усиления разделения нефтепродуктов на фракции; нагреватель, обеспечивающий необходимое парообразование в нижней части колонны; конденсатор для охлаждения и конденсации паров из верхней части колонны. Расчет ректификационной колонны в этой статье основывается на проекте завода по переработке газа. Качество выпускаемого продукта определяется чистотой дистиллята x_D (выше или равно 98%) и процентом примесей x_B в нижней части колонны (меньше или равно 2%).

Большинство систем управления процесса перегонки основывается на структуре баланса энергии. В этой структуре входами являются скорость потока жидкости, L , и скорость потока пара, V , а выходами – концентрации продуктов x_D и x_B .

В соответствии с [10] введём обозначения:

$$\begin{vmatrix} u_1 \\ u_2 \end{vmatrix} = \begin{vmatrix} dL \\ dV \end{vmatrix} - \text{два управляемых входа,} \quad \begin{vmatrix} y_1 \\ y_2 \end{vmatrix} = \begin{vmatrix} dx_B \\ dx_D \end{vmatrix} - \text{два выходных сигнала.}$$

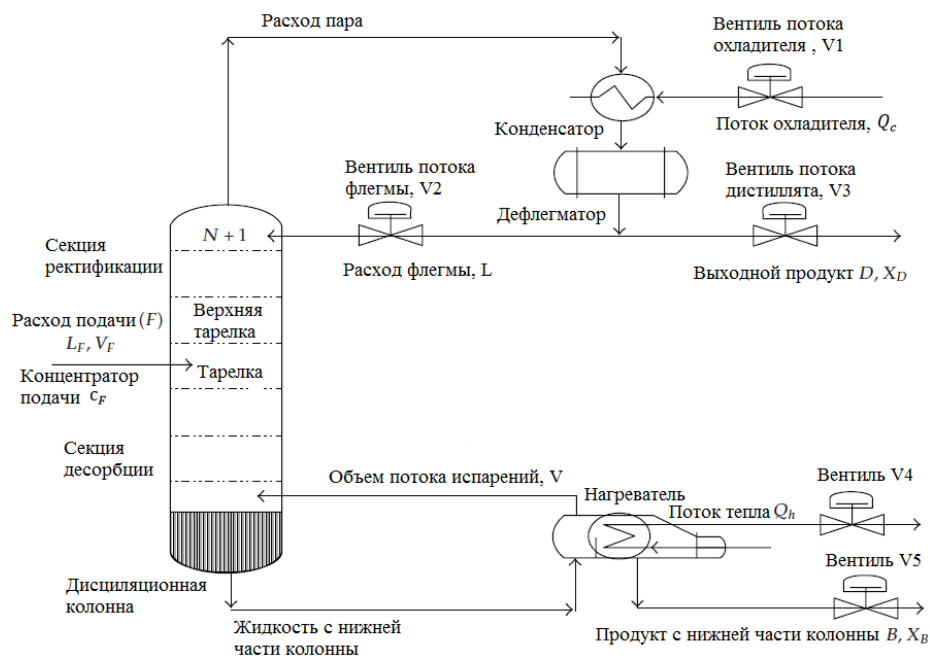


Рис. 1. Схема технологического процесса перегонки

Пусть $G_{p11}, G_{p12}, G_{p21}, G_{p22}$ – передаточные функции объекта, связывающие входы и выходы [10]:

$$\begin{bmatrix} y_1 \\ y_2 \end{bmatrix} = \begin{bmatrix} G_{p11} & G_{p12} \\ G_{p21} & G_{p22} \end{bmatrix} \cdot \begin{bmatrix} u_1 \\ u_2 \end{bmatrix} = \begin{bmatrix} \frac{0.0042}{1.9588s+1} & \frac{-0.0062}{1.9588s+1} \\ \frac{-0.0052}{1.9588s+1} & \frac{0.0072}{1.9588s+1} \end{bmatrix} \cdot \begin{bmatrix} u_1 \\ u_2 \end{bmatrix} \quad (1)$$

Результаты моделирования исходной системы (рисунок 1) с передаточными функциями (1) в пакете прикладных программ MATLAB представлены на рисунке 2.

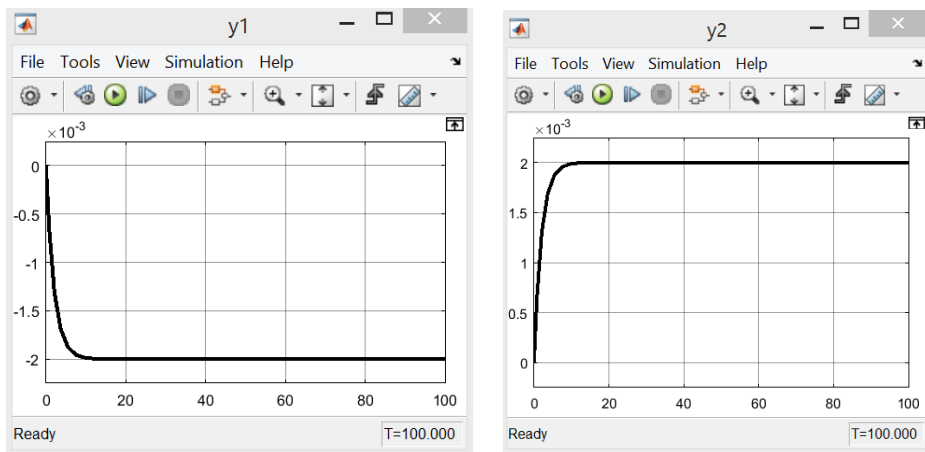


Рис. 2. Переходные процессы исходной системы (1)

2 Синтез типовых регуляторов для изолированных подсистем на основе генетического алгоритма. На основании исходной модели объекта управления и желаемой характеристики необходимо синтезировать интеллектуальный регулятор на основе генетического алгоритма.

Постановка задачи. Необходимо рассчитать параметры ПИ-регуляторов для сложной системы управления процессом очистки газа (1) на основе генетического алгоритма на основании интегрального критерия качества:

$$J_i = \int_{t=0}^{\infty} e_i^2(t) dt, \quad i = \overline{1,2}. \quad (2)$$

Применим процедуру расчёта коэффициентов ПИ-регулятора на основе генетического алгоритма в программном обеспечении «GeneticPRegulator» после децентрализации исходной модели (1). Здесь децентрализация необходима для реализации одномерных методов к МИМО (multi-input multi output) системам.

В результате применения процедуры декомпозиции получены два изолированных контура управления с ПИ-регуляторами:

$$u_i(t) = P_i e_i(t) + I_i \int_{t=0}^{\infty} e_i(t) dt, \quad i = \overline{1,2}, \quad (3)$$

с передаточными функциями: G_{C11}, G_{C22} :

$$G_{Cii}(s) = P_i + I_i \frac{1}{s}, \quad i = \overline{1,2}, \quad (4)$$

где $P_i, I_i, i = \overline{1,2}$ – коэффициенты усиления ПИ-регуляторов.

Описание программного обеспечения GeneticPRegulator. Программное обеспечение GeneticPRegulator состоит из трех составных частей: скрипт «genp2.m», который организует модель П-регулятора; графический интерфейс (GUI) для расчёта коэффициентов П-регулятора GeneticPRegulator; подпрограмма, выдающая результаты моделирования процесса очистки газа в дистилляционной колонне с учетом П-регулирования.

Входными данными программы GeneticPRegulator, вводимыми со стороны пользователя являются: коэффициент усиления k_1 и постоянная времени T_1 исходной модели, коэффициент усиления k_2 желаемой модели технологического процесса. Выходными данными является рассчитанный коэффициент пропорционального усиления интеллектуального П-регулятора.

Графический интерфейс программы GeneticPRegulator (GUI) состоит из (рисунок 3): а) 3 полей ввода исходных данных (коэффициент k_1 , коэффициент k_2 и постоянная времени T_1); б) окна вывода результата расчётов коэффициента пропорционального усиления интеллектуального П-регулятора; в) двух управляющих кнопок «Рассчитать» и «Очистить»; г) информационной панели, показывающей исходный вид передаточных функций, которые обрабатывает программа.

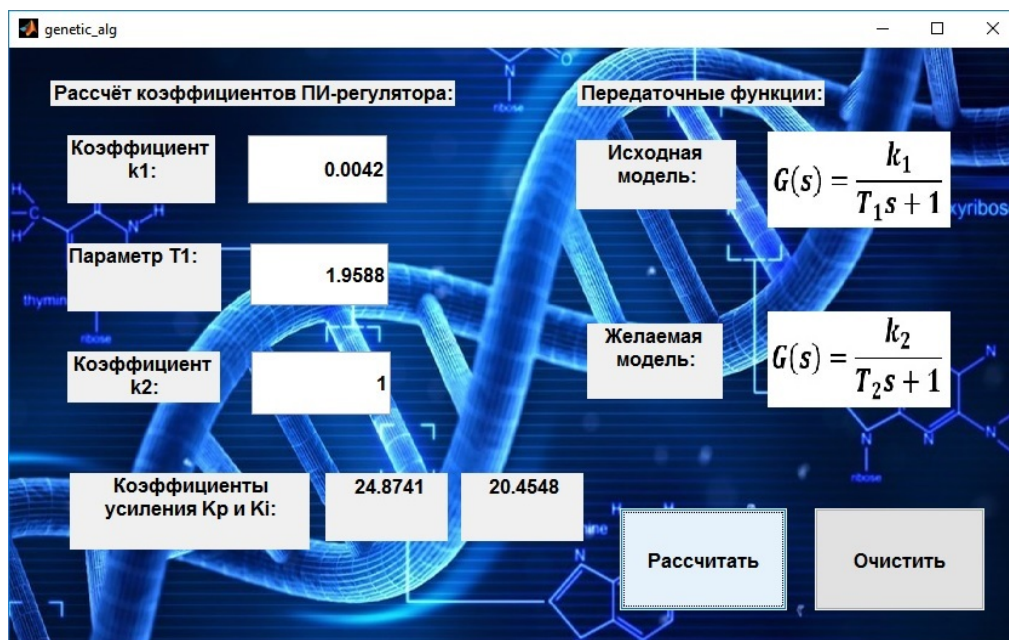


Рис. 3. Графический интерфейс программного обеспечения GeneticPRegulator

Кнопка «Рассчитать» запускает работу генетического алгоритма. В зависимости от быстродействия компьютера производится расчёт пропорционального коэффициента усиления, который может занять от 1 до 10 минут. Кнопка «Очистить» сбрасывает данные со всех полей и присваивает им значение «0». После окончания расчёта выводится диалоговое окно, уведомляющее пользователя об успешном завершении работы алгоритма.

Подпрограмма GeneticPRegulator_Results (рисунок 4) состоит из: а) технологической схемы процесса очистки газа в дистилляционной колонне; б) выпадающего меню; в) кнопки «Построить»; г) графического поля для построения графиков переходных процессов.

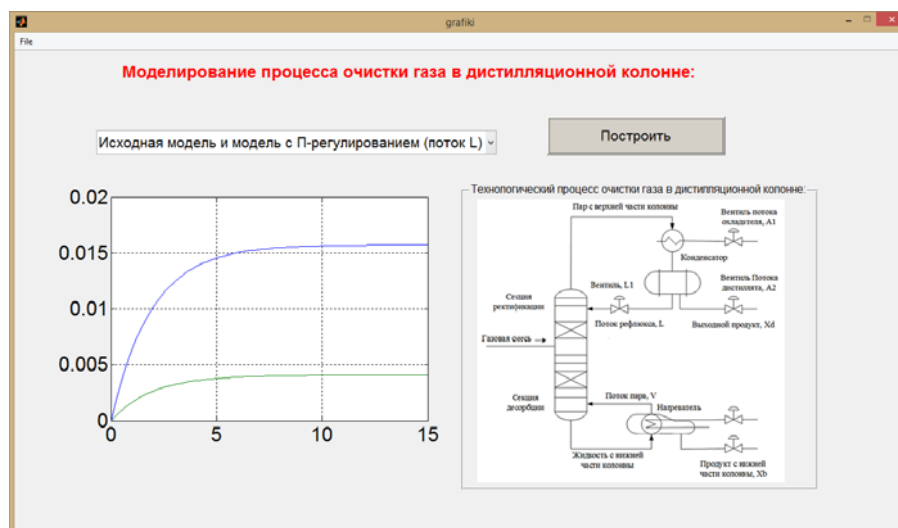


Рис. 4. Переходные характеристики технологического процесса очистки газа в дистилляционной колонне

Выпадающее меню (рисунок 5) позволяет выбрать графики исходной модели, модели с П-регулированием, желаемой модели для потока L и для потока V.

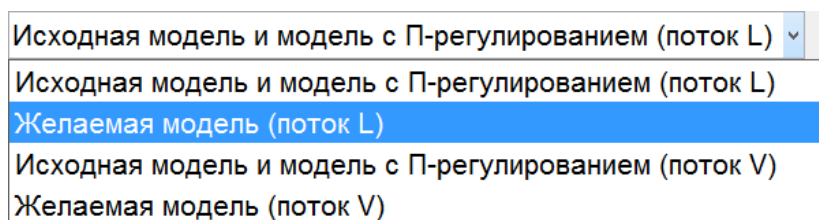


Рис. 5. Выпадающее меню для построения графиков

Пользователь получает доступ к переходным характеристикам исходной модели, желаемой модели и модели с П-регулированием, рассчитанным с помощью программного обеспечения GeneticPRegulator процесса очистки газа для двух потоков. Вывод на печать осуществляется через системное меню через путь «File >> Print».

Полученные коэффициенты для П-регулятора имеют практическое применение для программируемых логических контроллеров (ПЛК), выполняющих функции регуляторов на производстве. В качестве таких ПЛК могут выступать контроллеры фирм Schneider Electric (Modicon M340), Yokogawa или Siemens.

3 Инструкция по запуску программного обеспечения GeneticPRegulator для решения задач синтеза управления сложными объектами

1. Запустить приложение-установщик MyAppInstaller_msr, находящийся в папке for_redistribution, с диска «Программное обеспечение GeneticPRegulator для решения задач управления сложными объектами. Часть 1» (рисунок 6).

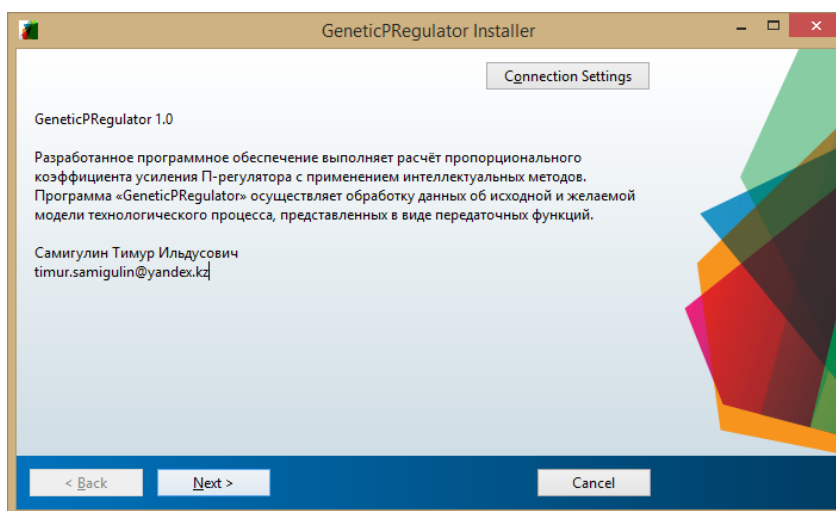


Рис. 6. Приложение-установщик MyAppInstaller_msr

2. Произвести установку приложения, поставить галочку «Add a shortcut to the desktop» для создания ярлыка на рабочем столе (рисунок 7).

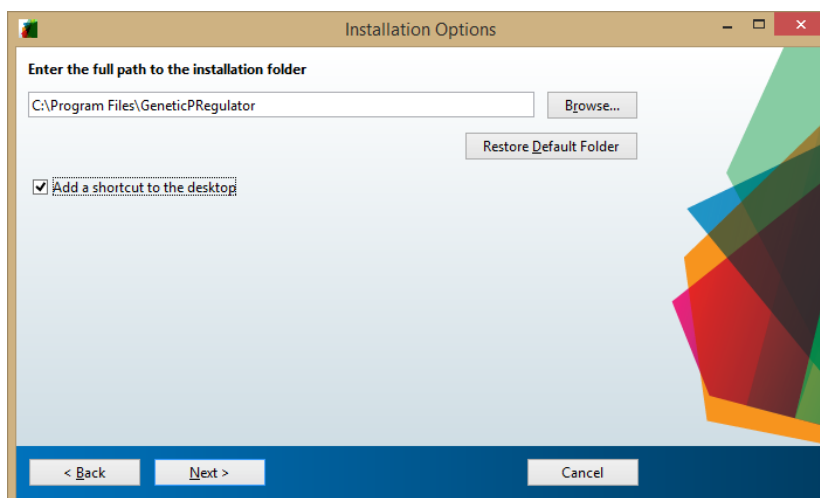


Рис. 7. Выбор папки для хранения программы и создание ярлыка на рабочем столе

3. Запустить ярлык приложения, расположенного на рабочем столе. Либо запустить приложение GeneticPRegulator находящегося в папке Program Files\GeneticPRegulator\application\GeneticPRegulator.exe

4. Повторить действия с 1 по 3 для второго диска «Программное обеспечение GeneticPRegulator для решения задач управления сложными объектами. Часть 2».

С использованием программного обеспечения «GeneticPRegulator» рассчитываются коэффициенты усиления ПИ-регуляторов (рисунок 3). Для этого заданы

следующие параметры для генетического алгоритма: количество популяций – 200 особей; кроссовер и мутация – в зависимости от ограничений; количество элит – 0.05 от размера популяции.

Рассчитанные коэффициенты для изолированных контуров: $P_1 = 24.8741$, $P_2 = 20.1499$, $I_1 = 20.4548$, $I_2 = 18.9873$.

Распределение функции пригодности (fitness function), показывающее наилучшее значение функции в зависимости от поколения (generation) генетического алгоритма изображено на рисунке 8.

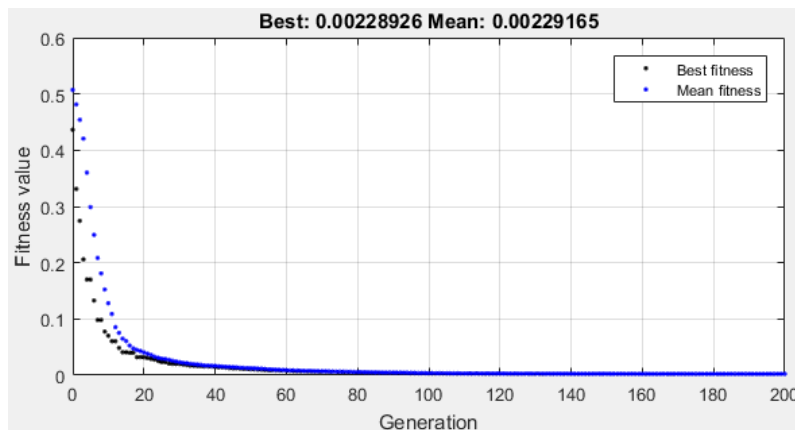


Рис. 8. Распределение функции пригодности в зависимости от количества поколений при выполнении генетического алгоритма

Коэффициенты ПИ-регуляторов, полученные на основе генетического алгоритма:

$$P_1 = 24.8741 ; \quad I_1 = 20.4548 ; \quad P_2 = 20.1499 ; \quad I_2 = 18.9873 . \quad (5)$$

Произведем моделирование изолированных подсистем системы с рассчитанными коэффициентами (5) в среде имитационного моделирования Simulink (рисунок 9):

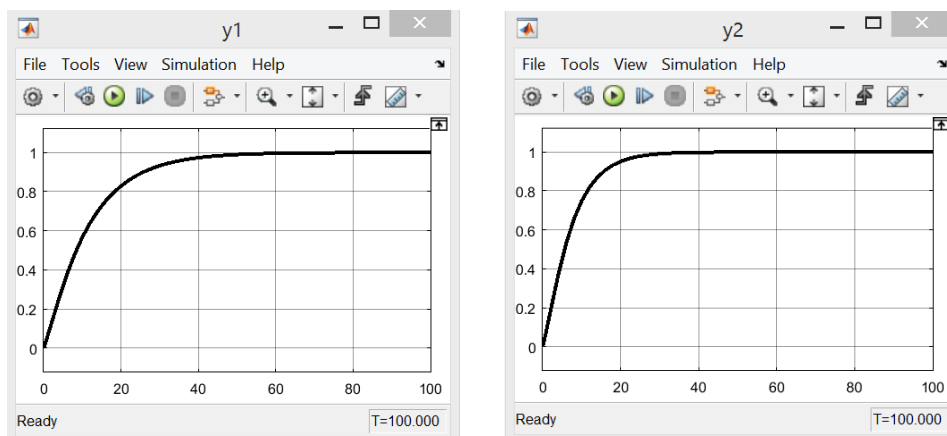


Рис. 9. Переходные процессы изолированных подсистем системы (6) с ПИ-регуляторами

$$\begin{bmatrix} y_1 \\ y_2 \end{bmatrix} = \begin{bmatrix} G_{p11} & 0 \\ 0 & G_{p22} \end{bmatrix} \cdot \begin{bmatrix} u_1 \\ u_2 \end{bmatrix} = \begin{bmatrix} \frac{0.0042}{1.9588s+1} & 0 \\ 0 & \frac{0.0072}{1.9588s+1} \end{bmatrix} \cdot \begin{bmatrix} u_1 \\ u_2 \end{bmatrix}, \quad (6)$$

$$u_1(t) = P_1 e_1(t) + I_1 \int_{t=0}^{\infty} e_1(t) dt, \quad u_2(t) = P_2 e_2(t) + I_2 \int_{t=0}^{\infty} e_2(t) dt.$$

4 Компенсация перекрёстных связей сложной системы

Для синтеза сложной системы управления, с учётом взаимосвязей, актуально применение теории устройств управления с компенсацией перекрёстных связей, основная идея которой заключается в применении дополнительных контроллеров для компенсации влияния взаимосвязей, с целью уменьшения их взаимодействия в контуре управления. В идеале развязывающее управление позволяет влиять только на желаемые регулируемые переменные [7-9].

Динамически развязанные системы – система, у которой каждый выход зависит от одного и только одного входа. Если все перекрестные функции передачи равны нулю или пренебрежимо малы, многоконтурная система вырождается в набор независимых (развязанных) однопетлевых систем.

Пусть матрица $H(s)$ – развязывающая матрица с параметрами H_{C12} и H_{C21} . В соответствии с этим необходимо найти параметры H_{C12} для того, чтобы ликвидировать влияние управляющего взаимодействия u_2 на выход y_1 :

$$G_{p11}u_{12} + G_{p12}u_{22} = 0, \quad G_{p11}H_{C12}u_{22} + G_{p12}u_{22} = 0. \quad (7)$$

Аналогично формуле (2), уравнения для второго входа имеют вид:

$$G_{p22}H_{C21}u_{11} + G_{p21}u_{11} = 0. \quad (8)$$

Для системы (1) с регуляторами (5) развязывающая матрица состоит из элементов:

$$H_{C12} = -13, \quad H_{C21} = -26. \quad (9)$$

На рисунке 10 для сравнения представлены схемы и результаты моделирования переходных процессов системы (6) и системы (1) с развязывающей матрицей (9).

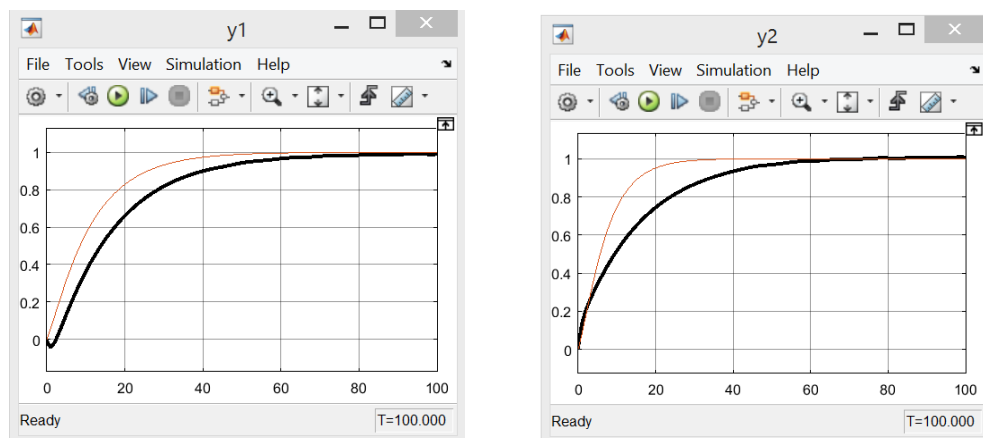


Рис. 10. Сравнение переходных процессов системы (6) и системы с развязывающим управлением

В ходе сравнения переходных процессов изолированных подсистем с регуляторами с переходными процессами (рисунок 10) был сделан вывод о том, что использование метода развязывающего управления позволяет компенсировать влияние взаимосвязей на процессы сложной системы.

Литература

1. Luchian H., Băutu A., Băutu E. Genetic programming techniques with applications in the oil and gas industry // Artificial intelligent approaches in petroleum geosciences. – Springer International Publishing, 2015. – P. 101-126.
2. Safarzadeh M., Motahhari S., Co-optimization of carbon dioxide storage and enhanced oil recovery in oil reservoirs using a multi-objective genetic algorithm (NSGA-II) // Petroleum science. – China University of Petroleum, 2014. – Vol.11. – P. 460-468.
3. Cuddy S. J., Glover P.W. The application of fuzzy logic algorithms to oil exploration // Developments in soft computing. – Springer-Verlag Berlin Heidelberg, 2001. – Part 2. – P. 167-174.
4. Rooki R., Ardejani F., Moradzadeh A., Mizraei H., Kelessidis V., Marglione R., Norouzi M. Optimal determination of rheological parameters for Herschel-bulkley drilling fluids using genetic algorithms (Gas) // Korea-Australia Rheology Journal. – Springer, 2012. – Vol. 24. – P. 163-170.
5. Wang J., Ning C., Yang Y. Multivariable PID Decoupling Control Method of Electroslag Remelting Process Based on Improved Particle Swarm Optimization (PSO) Algorithm // Information 2014, 5, 120-133
6. Антипин А. Ф. Способ построения многомерных систем управления с компенсацией взаимного влияния контуров регулирования // Молодой ученый. — 2014. — №18. — С. 220-224.

ПРИМЕНЕНИЕ МЕТОДА АНАЛИЗА ИЕРАРХИИ ПРИ ПРОЕКТИРОВАНИИ СИСТЕМ

Шокишалов Ж.М.
e-mail: jas_moderator@mail.ru

*Институт информационных и вычислительных технологий КН МОН РК,
Казахстан*

Аннотация. В данной работе рассматривается понятие принятия решений и изложен список конфликтов в информационно – коммуникационной системе. В качестве дополнительного математического инструмента был предложен метод анализа иерархии, который можно применить для выявления наиболее правильного решения при работе нескольких экспертов. Предложенный метод имеет широкую сферу применения, в том числе при решении конфликтных ситуаций. В будущем исследовательская работа будет посвящена разработке системы, исключаящей конфликтные ситуации в трансграничном доверительном обмене электронными документами

В безопасной системе в стадии проектирования должны быть охвачены все возможные влияющие факторы. Одним из таких факторов является принятие решений. При реализации систем с доверительными органами немаловажную роль играет мнение экспертов при решении конфликтных ситуаций. Принятие решений должно представлять интерес для каждого человека, и прежде всего для математиков, потому что хотя аспекты порядка и приоритета хорошо исследованы в математике, они не были изучены таким образом, чтобы сделать их применимыми в жизни людей. Каждый человек постоянно должен принимать решения, и сложность нашего мира с численностью населения более 6,8 миллиардов человек требует все в большей и большей степени рассмотрения разнообразных вариантов принятия решений. При этом могут возникать так называемые конфликты интересов, разрешение которых достигается в процессе принятия решений.

Многие люди, в том числе математики, мышление которых базируется на использовании декартовых осей координат на основе шкал измерения, считают, что есть только один способ измерить сущности, и он предполагает наличие физической шкалы измерения с началом отсчета и некоторой естественной единицы измерения. Но это не так. Удивительно, но мы также можем сформировать точные и надежные шкалы отношений, у которых нет начала отсчета или единицы измерения при помощи нашего понимания и суждений, являющихся наиболее фундаментальными первопричинами, определяющими, почему мы хотим измерить что-нибудь. В повседневной жизни мы пользуемся такими шкалами постоянно и делаем это подсознательно, не задумываясь. Физические шкалы помогают нашему пониманию и использованию сущностей, которые мы уже знаем, как измерить. Так как показания, полученные с физической шкалы, имеют произвольную единицу измерения, то сначала они должны быть интерпретированы специалистом экспертом, и только потом, интерпретации, мы сможем понять, насколько объект соответствует нашим потребностям. Но количество сущностей, которые мы не знаем как измерить, гораздо больше, и весьма маловероятно, что мы когда-нибудь найдем способы измерить все с применением шкалы с единицей измерения, потому что, в отличие от физических сущностей, большинство наших идей, чувств, поведение и

действия не являются зафиксированными раз и навсегда, а изменяются время от времени, и от одной ситуации к другой. Шкалы измерения являются изобретениями технологического ума. Наши разум и способы понимания всегда были и всегда будут с нами. Работа разума может быть представлена в виде работы электрического устройства из нейронов, чье возбуждение и синтез дают осмысление и понимание того, что нам нужно, чтобы выжить в сложном мире. Но насколько мы можем положиться на наш разум? Ответ на этот вопрос зависит от того, насколько хорошо мы знаем явления, относительно которых мы применяем наши суждения, и насколько хорошо эти суждения представляют наше понимание. В личных делах мы лучшие судьи по поводу того, что может быть хорошо для нас. В ситуациях с участием большого числа людей необходимо учитывать все имеющиеся суждения. Как показывает практика, всегда есть люди, которые являются экспертами в каких-то областях, и их решения имеют приоритет над суждениями тех, кто знает меньше.

Среди многих приложений, созданных компаниями и правительствами, теперь, пожалуй, исчисляемых в тысячах, метод анализа иерархий (МАИ; the Analytic Hierarchy Process; АНР) был использован компанией IBM в рамках стратегии по улучшению качества проектирования компьютера AS/400, позволившей получить престижную Национальную Премию Качества Малкольма Болдриджа (Malcolm Baldrige National Quality Award). В 2001 году МАИ был использован, чтобы определить наилучшее место для переселения людей после землетрясения, разрушившего турецкий город Адапазари (Adapazari). Компания British Airways использовала этот метод в 1998 году, чтобы выбрать поставщика мультимедийной системы для всего своего парка самолетов. В 1987 году МАИ был использован, чтобы выбрать лучший тип платформы для бурения нефти в Северной Атлантике. Платформа стоила около 3 миллиардов долларов, но стоимость сноса была еще более значимым фактором в принятии решения. МАИ был применен к конфликту между США и Китаем в борьбе за соблюдение прав интеллектуальной собственности в 1995 году, когда граждане Китая нелегально копировали и распространяли музыку, видео и программное обеспечение на лентах и компакт-дисках. Практическое применение МАИ с использованием трех иерархий для выгоды, издержек и рисков показало, что гораздо лучше для США не применять санкции к Китаю. Вскоре после того, как исследование было завершено, США наделили Китай статусом наиболее благоприятной торговой страны и не стали накладывать санкции. Корпорация Xerox использовала МАИ при выделении около миллиарда долларов для своих научно-исследовательских проектов. В 1999 году Ford Motor Company использовала МАИ при установлении приоритетов критериев, которые повышают степень удовлетворенности клиентов. Форд наградил компанию Expert Choice Inc премией Award for Excellence за помощь в достижении большого успеха со своими клиентами. В 1986 году поддерживаемый правительством Институт Стратегических Исследований (Institute of Strategic Studies) в Претории использовал МАИ для анализа конфликта в Южной Африке и рекомендовал осуществить освобождение Нельсона Манделы, а затем отказаться от апартеида и предоставить полное гражданство и равные права черному большинству. Все эти рекомендации были быстро реализованы [1].

Результаты выполнения работ по обеспечению доверия при межгосударственном обмене данными и электронными документами между уполномоченными органами государств-членов должны стать основой для развития трансграничного пространства доверия при создании интегрированной информационной системы членов Евразийского экономического союза (далее – интегрированная система) на основе развития и расширения функциональных возможностей интегрированной информационной системы внешней и взаимной торговли Таможенного союза. Развитие трансграничного

пространства доверия в рамках создания интегрированной системы должно осуществляться в соответствии со стратегией развития интегрированной системы, которая должна учитывать положения настоящей Стратегии в отношении принципов развития трансграничного пространства доверия и механизмов их реализации [2].

Сейчас в разрабатываемых системах безопасного документооборота в ходе обмена электронными документами возможно возникновение конфликтных ситуаций в следующих случаях:

- некорректность входящего электронного документа;
- для корректного электронного документа непризнание отправителем электронного документа факта отправки документа, а также его целостности и подлинности;
- оспаривание факта отправления и (или) получения электронного документа;
- оспаривание времени отправления и (или) получения электронного документа;
- оспаривание содержания, отправленного (полученного) электронного документа;
- оспаривание идентичности экземпляров электронного документа и (или) подлинника и копии электронного документа на бумажном носителе;
- оспаривание целостности электронного документа;
- оспаривание идентификации уполномоченного сотрудника, заверившего электронный документ электронной цифровой подписью;
- оспаривание полномочий уполномоченного сотрудника, заверившего электронный документ электронной цифровой подписью;
- оспаривание действительности и правомочности использования сертификата ключа подписи, использованного для заверения электронного документа;
- недоверие к технологии обмена электронными документами и защиты информации при обмене электронными документами;
- недоверие к используемым структурам и форматам электронного документа;
- недоверие к программно-техническим средствам обеспечения обмена электронными документами и защиты информации при обмене электронными документами;
- недоверие к уполномоченным сотрудникам удостоверяющего центра;
- иные случаи возникновения конфликтных ситуаций в ходе обмена электронными документами.

Этот список в процессе реализации может быть сокращено либо дополнен реальными проблемами системы электронного документооборота. Описанный выше математический метод можно внедрить в систему как вспомогательное средство при принятии решений, когда при решении привлечено несколько экспертов, в нашем случае доверенная третья сторона.

Применение единых криптографических средств ЭЦП при трансграничном электронном обмене данными между органами государственной власти государств-членов в настоящее время невозможно, поскольку в соответствии с нормативно-правовой базой государств-членов к использованию в государствах-членах допускаются только сертифицированные по национальным стандартам криптографические средства [3].

Поиск конфликтных ситуаций в трансграничном доверительном обмене электронными документами носит комплексный характер и сочетает в себе нормативно – законодательные, организационные, программные, технические меры.

Практическая значимость выполнения представляемой исследовательской работы будет способствовать в разработке в трансграничного доверительного обмена

электронными документами в странах СНГ и ЕАЭС системы исключаящий всевозможные конфликтные ситуации [4].

Литература

1. Саати Т. Л. Относительное измерение и его обобщение в принятии решений. Почему парные сравнения являются ключевыми в математике для измерения неосязаемых факторов1 //Cloud of Science. – С. 171.
2. Стратегия развития трансграничного пространства доверия утвержденного Решением Коллегии Евразийской экономической комиссии от 2015 г.
3. Концепция использования при межгосударственном информационном взаимодействии сервисов и имеющих юридическую силу электронных документов, Решение Совета Евразийской экономической комиссии от 18 сентября 2014 года № 73
4. Шокишалов Ж.М., Трансграничное пространство доверия для обмена электронными документами в странах СНГ и ЕАЭС, Тезисы докладов XII международной научной конференции студентов, магистрантов и молодых ученых «Ломоносов - 2016».,

СОДЕРЖАНИЕ

Абдикаликов К.А.	СЛЕПАЯ ЭЛЕКТРОННАЯ ПОДПИСЬ НА ОСНОВЕ КРИПТОСИСТЕМЫ RSA-M	4
Айнакулов Ж.Ж.	АЭРОФОТОСЪЕМКА ОТКРЫТЫХ ГОРНОРУДНЫХ МЕСТОРОЖДЕНИЙ С ИСПОЛЬЗОВАНИЕМ БПЛА	8
Алимхан К., Калимолдаев М.Н., Тасболатұлы Н.	ЖОҒАРЫ РЕТТІ АНЫҚТАЛМАҒАН СЫЗЫҚТЫ ЕМЕС ЖҮЙЕЛЕРДІ ШЫҒЫС КОМПЕНСАТОРЫ ЖӘРДЕМІНДЕ КҮШТІ ПРАКТИКАЛЫҚ БАҚЫЛАУ	14
Амиргалиев Е. Н., Калижанова А.У., Козбакова А.Х. Шамиль-уулу Ш.	О ВИЗУАЛИЗАЦИИ АРХИТЕКТУРНЫХ РЕШЕНИЙ ДЛЯ БЕЗОПАСНЫХ И ЭНЕРГОЭФФЕКТИВНЫХ ЗДАНИЙ	21
Amirgaliyev Ye.N., Mussabayev R.R., Tairova A.T., Kozbakova A.H., Mussabayev T.R.	DEVELOPING OF AN AUTOMATED SYSTEM FOR LEXICAL, SYNTAX AND SYNTAGMATIC ANALYSIS OF KAZAKH TEXTS AND ITS EMOTIONAL CLASSIFICATION	25
Амиргалиев Е., Юнусов Р.	ПРИМЕНЕНИЕ БЕСПРОВОДНЫХ СЕТЕЙ ДЛЯ ОПРЕДЕЛЕНИЯ ПОЛОЖЕНИЯ ВНУТРИ ПОМЕЩЕНИЯ – ТРИЛАТЕРАЦИЯ	29
Арсланов М.З.	ПОИСК КРАТЧАЙШЕГО ПУТИ В ПРЯМОУГОЛЬНОЙ СЕТИ	36
Баев А.Ж., Нурсултанов Е.Д., Тлеуханова Н.Т.	ВОССТАНОВЛЕНИЕ КОЭФФИЦИЕНТОВ ФУРЬЕ-УОЛША	42
Бияшев Р.Г., Варенников А.В., Нысанбаева С.Е.	АЛГОРИТМ ФОРМИРОВАНИЯ ПОЛНЫХ КЛЮЧЕЙ ДЛЯ СИСТЕМЫ ШИФРОВАНИЯ НА БАЗЕ НЕПОЗИЦИОННЫХ ПОЛИНОМИАЛЬНЫХ СИСТЕМ СЧИСЛЕНИЯ	44
Вальдемар Вуйчик, Найзабаева Л.Қ, Оразбеков Ж.Н.	ФИЛИАЛДАР ЖЕЛІСІН БАСҚАРУ ҮШІН ҮЛЕСТІРІЛГЕН ДЕРЕКТЕР ҚОРЫНЫҢ МОДЕЛІ МЕН КОРПОРАТИВТІК АҚПАРАТТЫҚ ЖҮЙЕСІ	48
Калимолдаев М.Н., Голиков А.И., Евтушенко Ю.Г., Посыпкин М.А., Абдилдаева А.А.	МЕТОДЫ ЛОКАЛЬНОЙ МНОГОКРИТЕРИАЛЬНОЙ ОПТИМИЗАЦИИ	55

Жатқанбаев А.А.	ИСПОЛЬЗОВАНИЕ АЛГОРИТМОВ НА ГРАФАХ ДЛЯ ДОБАВЛЕНИЯ ПЕРЕСТАНОВОК В БЛОЧНЫХ ШИФРАХ ПРИ СКРЫТИИ ИНФОРМАЦИИ	59
Исимов Н., Джомартова Ш.А., Мазаков Т.Ж.	ИССЛЕДОВАНИЕ МОДЕЛИ ПРОГНОЗИРОВАНИЯ И УПРАВЛЕНИЯ ЭПИДОБСТАНОВКОЙ С ПРИМЕНЕНИЕ НЕЧЕТКОГО И ИНТЕРВАЛЬНОГО АНАЛИЗА	68
Калимолдаев М.Н., Абдилдаева А.А.	АҚПАРАТТЫҚ МОДЕЛЬДЕРДІ ЖӘНЕ АҚПАРАТТЫҚ ЖҮЙЕНІ ЖҮЗЕГЕ АСЫРУ ӘДІСТЕРІН ҚҰРУ	73
Калимолдаев М.Н., Ахметжанов М.А., Галиева Ф.М.	ЭЛЕКТРОЭНЕРГЕТИКАЛЫҚ ЖҮЙЕЛЕР ҚОЗҒАЛЫСЫН ТҮРАҚТАНДЫРУ	81
Калимолдаев М.Н., Бияшев Р.Г., Рог О.А.	ОСНОВЫ АРХИТЕКТУРЫ ПРОГРАММНЫХ СИСТЕМ ДЛЯ ОСУЩЕСТВЛЕНИЯ ТИПИЗИРОВАННОГО АТРИБУТНОГО РАЗГРАНИЧЕНИЯ ДОСТУПА	88
Калимолдаев М.Н., Дузбаев Т.Т., Ахметжанов М.А., Галиева Ф.М.	ЧИСЛЕННОЕ РЕШЕНИЕ ЗАДАЧИ СТАБИЛИЗАЦИИ СИСТЕМЫ «СИНХРОННЫЙ ГЕНЕРАТОР – ПАРОВАЯ ТУРБИНА»	95
Калимолдаев М.Н., Қосынбай Е.Б.	МОДЕЛИРОВАНИЕ СБОРА И АНАЛИЗА ДАННЫХ ДЛЯ ПРОГРАММНОГО КОМПЛЕКСА СТАБИЛИЗАЦИИ И УПРАВЛЕНИЯ МНОГОСВЯЗНЫМИ ФАЗОВЫМИ СИСТЕМАМИ	100
Капалова Н.А., Алғазы К.Т., Самрат С.М.	КРИПТОАЛГОРИТМДЕРДІҢ СТАТИСТИКАЛЫҚ ҚАУІПСІЗДІГІН ЗЕРТТЕУ	108
Капалова Н.А., Хаумен А.	АЛГОРИТМ ШИФРОВАНИЯ НА SP-СЕТИ	113
Карабеков Б.С., Машеров Д.Е., Плесневич Г.С.	ОДИН ЯЗЫК ДЛЯ СПЕЦИФИКАЦИИ ОНТОЛОГИЙ	119
Кудайкулов А.К., Ташев А.А., Аскарова А.	РАЗРАБОТКА ФИЗИКО-МАТЕМАТИЧЕСКОЙ МОДЕЛИ ТЕПЛОФИЗИЧЕСКОГО СОСТОЯНИЯ ТЕЛ С УЧЕТОМ ОДНОВРЕМЕННОГО НАЛИЧИЯ ЛОКАЛЬНЫХ ТЕПЛОИЗОЛЯЦИЙ, ТЕМПЕРАТУР, ТЕПЛООБМЕНОВ И ТЕПЛОВЫХ ПОТОКОВ И ИХ РЕАЛИЗАЦИЯ НА ПК	128

Magzom M.M., Begimbayeva Ye.Ye., Biyashev R.G., Nyssanbayeva S.E.	MODELLING SERVICES INFRASTRUCTURE IN THE INTEGRATED SYSTEM OF CROSS-BORDER INFORMATION EXCHANGE	135
Мамырбаев Ө.Ж., Ибраимкулов А.Е., Абдилда Б.Г.	ЖЕКЕ ТҮЛҒАНЫ ДАУЫСЫ АРҚЫЛЫ ТАНУ ЖҮЙЕСІН ЖОБАЛАУ МЕН ҚҰРУ ӘДІСІНЕ СИПАТТАМА	139
Мамырбаев О.Ж., Нурлан К.Е.	СӨЙЛЕУЛЕРГЕ СПЕКТРЛІК ТАЛДАУ ЖАСАУҒА АРНАЛҒАН АЛГОРИТМ	143
Muratkhanova T.A.	SENSOR-DRIVEN ADAPTER FOR CAR DIAGNOSTICS	148
Мусабаев Р.Р.	РАЗРАБОТКА ИНФОРМАЦИОННОЙ СИСТЕМЫ ДЛЯ ФОРМИРОВАНИЯ ЦИФРОВОГО ГОЛОСОВОГО ПОРТРЕТА ЛИЧНОСТИ	151
Mussabayev R.R., Amirgaliyev Ye.N., Tairova A.T., Kozbakova A.H.	DEVELOPMENT OF SPEAKER-INDEPENDENT LIMITED-VOCABULARY KAZAKH SPEECH RECOGNITION SYSTEM	163
Mussabayev R.R., Amirgaliyev Ye.N., Tairova A.T., Kozbakova A.H.	DETERMINATION OF THE OPTIMAL PHONETIC SET OF THE KAZAKH LANGUAGE	169
Мустафин С.А.	МЕТОД ОЦЕНКИ ОДНОРОДНОСТИ СМЕСИ СЫПУЧИХ МАТЕРИАЛОВ	176
Найзабаева Л.К., Нуржанов Ч.А., Мукимбаев М., Сатымбаев М.Н.	МАТЕМАТИЧЕСКАЯ МОДЕЛЬ КИНЕТИКИ РОСТА РАСТЕНИЙ В УСЛОВИЯХ ЗАГРЯЗНЕНИЯ ПОЧВЫ ТЯЖЕЛЫМИ МЕТАЛЛАМИ	178
Нуртазин А.Т.	ПРИМЕР КОМПАНИОН-ТЕОРИИ С ДВУМЯ НЕ ЭЛЕМЕНТАРНО ЭКВИВАЛЕНТНЫМИ ЭКЗИСТЕНЦИАЛЬНО ЗАМКНУТЫМИ СЧЁТНЫМИ МОДЕЛЯМИ	182
Нуртазин А.Т., Хисамиев З.Г.	АВТОМАТИЗАЦИЯ ПРЕДСТАВЛЕНИЯ ТЕКСТА В ВИДЕ ПРАВИЛ ЛОГИЧЕСКОГО ПРОГРАММИРОВАНИЯ	186

Нысанбаева С.Е., Капалова Н.А., Дюсенбаев Д.С., Дузбаев Т.Т.	АЛГОРИТМ ШИФРОВАНИЯ НА БАЗЕ КИТАЙСКОЙ ТЕОРЕМЫ ОБ ОСТАТКАХ	191
Нысанбаева С. Е., Кабылханов А. Б.	РЕАЛИЗАЦИЯ АЛГОРИТМА КРИПТОГРАФИЧЕСКОГО ПРЕОБРАЗОВАНИЯ	196
Рысбайулы Б., Юничева Н. Р.	РАЗРАБОТКА ИТЕРАЦИОННОГО МЕТОДА РАСЧЕТА НЕТОЧНЫХ ТЕПЛОФИЗИЧЕСКИХ ПАРАМЕТРОВ МЕТАСТАБИЛЬНЫХ ГОРНЫХ СИСТЕМ	202
Самигулина Г.А., Масимканова Ж.А.	КОМПЬЮТЕРНЫЙ МОЛЕКУЛЯРНЫЙ ДИЗАЙН ЛЕКАРСТВЕННЫХ ПРЕПАРАТОВ НА ОСНОВЕ АЛГОРИТМОВ РОЕВОГО ИНТЕЛЛЕКТА И ИММУНОСЕТЕВОГО МОДЕЛИРОВАНИЯ	209
Самигулина Г. А., Нюсупов А.Т., Шаяхметова А.С.	СПЕЦИАЛИЗИРОВАННАЯ МУЛЬТИАГЕНТНАЯ SMART-СИСТЕМА ДИСТАНЦИОННОГО ОБУЧЕНИЯ ЛЮДЕЙ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗРЕНИЯ	215
Самигулина Г.А., Самигулина З.И.	РАЗРАБОТКА ГРАФИЧЕСКИХ МОДЕЛЕЙ ДЛЯ ИНТЕЛЛЕКТУАЛЬНОГО АНАЛИЗА ДЕСКРИПТОРОВ СУЛЬФАНИЛАМИДОВ ПРИ СИНТЕЗЕ НОВЫХ ЛЕКАРСТВЕННЫХ ПРЕПАРАТОВ	223
Сатымбеков М.Н., Нуржанов Ч.А.	КЛЕТОЧНЫЕ АВТОМАТЫ	228
Сулейменов И.Э.	НЕКОТОРЫЕ ФИЛОСОФСКИЕ АСПЕКТЫ ИСЧИСЛЕНИЯ ПОНЯТИЙ	232
Сулейменов И.Э., Пак И.Т., Копишев Э.Е., Тасбулатова З.С.	РАЗРАБОТКА МЕТОДИКИ НЕПРЯМОЙ ОЦЕНКИ УРОВНЯ КОРРУПЦИИ В ВЫСШИХ УЧЕБНЫХ ЗАВЕДЕНИЯХ НА ОСНОВЕ ТЕОРИИ СЛОЖНЫХ СИСТЕМ	240
Сулейменов И.Э., Пак И.Т., Шалтыкова Д.Б., Байпакбаева С.Т.	МАКРОСКОПИЧЕСКАЯ ЗАПИСЬ ИНФОРМАЦИИ В РАСПРЕДЕЛЕННЫЕ СИСТЕМЫ КАК ОСНОВА ДЛЯ НАНОПРОГРАММИРУЕМЫХ СИСТЕМ	249
Сундетов Т.Р., Жакупбеков Т.Е.	РАЗРАБОТКА И АНАЛИЗ БИОНИЧЕСКОЙ РУКИ	254

Тлеубергенов М.И., Ибраева Г.Т., Ажымбаев Д.Т.	О ПОСТРОЕНИИ УРАВНЕНИЙ ДВИЖЕНИЯ КОСМИЧЕСКОГО АППАРАТА ПРИ НАЛИЧИИ АЭРОДИНАМИЧЕСКИХ СИЛ	259
Тынымбаев С.Т., Капалова Н.А., Магзом М.М.	РАЗРАБОТКА И РЕАЛИЗАЦИЯ АППАРАТНОГО УМНОЖИТЕЛЯ В НЕПОЗИЦИОННОЙ СИСТЕМЕ СЧИСЛЕНИЯ	263
Утепбергенов И.Т., Хисамиев З.Г., Тойбаева Ш. Д., Исабекова Л.С., Муслимова А.К.	НЕЧЕТКАЯ МОДЕЛЬ МЕНЕДЖМЕНТА КАЧЕСТВА ТЕХНОЛОГИЧЕСКИХ ПРОЦЕССОВ ПИЩЕВОГО ПРОИЗВОДСТВА	270
Хомпыш А.	ЭЛЬ-ГАМАЛЬ ШИФРЛАУ АЛГОРИТМІНІҢ МОБИЛЬДІК ҚОСЫМШАСЫН ҚҰРУ	281
Ширяева О.И., Самигулин Т.И.	РАЗРАБОТКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ СИНТЕЗА ИНТЕЛЛЕКТУАЛЬНОЙ СИСТЕМЫ УПРАВЛЕНИЯ СЛОЖНЫМ ОБЪЕКТОМ НЕФТЕГАЗОВОЙ ОТРАСЛИ	285
Шокишалов Ж.М.	ПРИМЕНЕНИЕ МЕТОД АНАЛИЗА ИЕРАРХИИ В ПРОЕКТИРОВАНИЕ СИСТЕМ	294

МАТЕРИАЛЫ
научной конференции
ИИВТ МОН РК
**«Современные проблемы информатики и
вычислительных технологий»**
29-30 июня 2017 года

(Сборник статей)

Подписано в печать 20.06.2017 г. Формат А4.
Печать ризография. Бумага офсетная. Усл. печ. л. 14,06.
Тираж 300 экз. Заказ № 01164.
Отпечатано в типографии НЦ НТИ.
Алматы, ул. Богенбай батыра, 221.