ISSN 1563 – 0285
Индекс 75872; 25872

ӘЛ-ФАРАБИ атындағы ҚАЗАҚ ҰЛТТЫҚ УНИВЕРСИТЕТІ

ҚазҰУ ХАБАРШЫСЫ

Математика, механика, информатика сериясы

Арнайы шығарылым

КАЗАХСКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ имени АЛЬ-ФАРАБИ

ВЕСТНИК КазНУ

Серия математика, механика, информатика

Специальный выпуск

AL-FARABI KAZAKH NATIONAL UNIVERSITY

KazNU BULLETIN

Mathematics, Mechanics, Computer Science Series

Special issue

№3/1(90)

Алматы
«Қазақ университеті»
2016

Зарегистрирован в Министерстве культуры, информации и общественного согласия Республики Казахстан, свидетельство № 956-Ж от 25.11.1999 г.
(Время и номер первичной постановки на учет № 766 от 22.04.1992 г.)
Выходит 4 раза в год

Научное издание

Вестник КазНУ

Серия математика, механика, информатика

№ 3/1(90) 2016

Редактор: Г.М. Даирбаева

Компьютерная верстка: Б.А. Аетова

ИБ N 9992

Подписано в печать 05.09.2016 г. Формат 60 × 84 1/8. Бумага офсетная.
Печать цифровая. Объем 10,25 п.л. Тираж 500 экз. Заказ N 3895.
Издательский дом "Қазақ университеті"
Казахского национального университета им. аль-Фараби.

050040, г. Алматы, пр.аль-Фараби, 71, КазНУ.
Отпечатано в типографии издательского дома "Қазақ университеті".

ПРЕДИСЛОВИЕ

Дорогие читатели!
Институт информационных и вычислительных технологий КН МОН РК
21-25 сентября 2016 года отмечает свой 25-летний юбилей.

В этом году исполняется 25 лет со дня обретения независимости Республики Казахстан. За эти 25 лет многого удалось добиться нашей многонациональной стране во главе с такой выдающейся личностью, как наш Президент Нурсултан Назарбаев. Казахстан нашел свой путь развития, направленный на благосостояние и процветание, как всего государства в целом, так и каждого гражданина в частности. Мы гордимся тем, что наш Институт является ровесником независимости нашей страны. Веком информатики и технологий назвал XXI век Президент РК. Сегодня без надлежащей системы информационного обеспечения невозможен прогресс в любой сфере деятельности государства - экономической, политической, социальной, и, естественно, в сфере образования и науки. В настоящее время в Институте трудятся заслуженные деятели науки РК, академики, профессора, доктора и кандидаты наук. Сотрудники Института занимаются изучением, разработкой, апробацией и внедрением эффективных, доступных программных комплексов и робототехнических систем. В Институте проводятся научно-исследовательские работы для построения, анализа и программной реализации системы защиты информации с использованием отечественного симметричного блочного алгоритма шифрования, разработанного на базе непозиционных полиномиальных систем счисления. Разработаны мобильные робототехнические комплексы, оснащённые системой 3-мерного машинного зрения, которые применяются как в военной сфере, так и для обеспечения безопасности в общественных местах. Молодые ученые участвуют в различных выставках («KADEX- 2016», «ҚАЙСАР-2016», «Айбын»), где демонстрируют собственные технические разработки. В течение 25 лет Институт интенсивно развивался, расширяя сферы своей деятельности, рос качественно и количественно. Результаты НИР ИИВТ получили заслуженное признание в республике, о чем свидетельствуют публикации в зарубежных рейтинговых журналах и выигранные сотрудниками гранты по линии INTAS, МНТЦ, CRDF (Американский фонд гражданских исследований и разработок), INCO-Copernicus «STEPICA», UNESCO, Премия фонда Первого Президента за 2015 год. Многие результаты научных исследований, выполненных в Институте, нашли свое практическое применение в развитии информационной инфраструктуры Республики Казахстан. Президент Казахстана всегда пристальное внимание уделял и уделяет развитию науки и инновационных технологий, подчеркивая, что эти процессы невозможны без участия молодежи. За последние годы в Институт пришло много молодых людей. Ведется организационная работа по активизации грантопоисковой деятельности молодых ученых Института и по привлечению их в научные проекты, реализуемые под руководством крупных ученых. Институт активно занимается подготовкой кадров высшей квалификации. В течение 2015 года магистранты и докторанты ИИВТ прошли зарубежные стажировки в России, США, Японии, Франции, Англии, Германии, Польше, Южной Корее, Малайзии. Молодые сотрудники нашего Института принимают активное участие в конкурсе Startup-проектов. В рамках международного сотрудничества заключаются договоры, меморандумы о научно-техническом сотрудничестве, как

с научными, так и с образовательными организациями, в настоящее время заключены соглашения с более чем 20 партнерами. ИИВТ является организацией-членом Технического комитета ТК-34 «Информационные технологии» Госстандарта РК при АО «Национальные информационные технологии», постоянно участвует в рассмотрении и согласовании проектов государственных стандартов РК, разрабатываемых различными организациями. В Институте регулярно проводятся различные конференции и научные семинары. ИИВТ является одним из организаторов ежегодной Международной азиатской школы-семинара «Проблемы оптимизации сложных систем», начиная с 2008 года. Целью проведения этих мероприятий для Института является объединение научных исследований ученых, обмен опытом по ряду проблем современной науки, а также передача этого опыта магистрантам, докторантам. В честь 25-летия Институт информационных и вычислительных технологий проводит Международную научную конференцию «Информатика и прикладная математика», цель которой - обмен информацией с солидными учеными международного уровня, поддержание сотрудничества с различными научными организациями, демонстрация научных достижений института, определение новых задач для дальнейших исследований. Сильная инфраструктура, мощный интеллектуальный и творческий потенциал Института информационных и вычислительных технологий позволяют с уверенностью смотреть в будущее и трудиться на благо народа Республики Казахстан. 25-летний юбилей Института – не только знаменательная дата для самого учреждения, это праздник для всех сотрудников Института, в том числе и тех, кого уже нет с нами. Важны не только результаты деятельности коллектива, выраженные в научных трудах, диссертациях, экспертных заключениях, открытиях, но и та особая аура Института, которую создали знания, интеллект, патриотизм и творческое вдохновение предшествующих поколений. Знаю, что этим живет наш коллектив сегодня. Верю, что так будет всегда.

Ген. директор ИИВТ КН МОН РК,
чл.-корр. НАН РК, д.ф.-м.н.,
профессор М.Н. Калимолдаев

Бөлім	Раздел	Section
Информатика және қолданылмалы математика	Информатика и прикладная математика	Computer Sience and Applied Mathematics

УДК 519.21

Айда-заде К.Р. [1*], Талыбов С.Г.

[1]Институт систем управления НАН Азербайджана, Баку
*E-mail: kamil_ayda-zade@rambler.ru

Применение весовых коэффициентов при использовании N-грамм для определения авторства азербайджанских текстов

Как известно одной из важных проблем обработки текстов является их классификация по авторам, т.е. определение того, кто из заранее заданной группы авторов является предполагаемым автором конкретно данного текста. Автоматизацией решения этой проблемы наиболее интенсивно начали заниматься в 70-х годах прошлого века. Первоначально методы решения этой проблемы базировались на использовании созданных специальных глоссариев для ключевых слов. Сравнительно низкий процент распознавания авторов основанных на монограммах объясняется в основном большой размерностью пространства признаков и близостью значений признаков друг к другу. Это связано с невозможностью отделить множества признаков, характеризующих каждого автора из пространства признаков, обычными линейными гиперповерхностями. С другой стороны это также связано с малым объемом информации в газетных статьях и низкой информативностью этой информации. В статье приводится описание результатов экспериментов для определения авторства газетных статей небольшого объема на азербайджанском языке с применением статистического подхода для анализа используемых авторами N-грамм. Предложены формулы для весовых коэффициентов, определяющих важность того или иного признака при определении авторства.
Ключевые слова: обработка текста, N-граммы, весовые коэффициенты.

Ayda-zade K.R., Talybov S.G.

The use of weight coefficients using N-gram to determine the authorship of the Azerbaijani texts

As you know one of the most important problems of word processing is their classification by the authors, ie, determining which one of a predetermined group of authors is the alleged author of this particular text. Automation solutions to this problem most intensively began to develop in the 70s of the last century. Initially, the methods to solve this problem based on the use of specialized glossaries created for keywords. The relatively low percentage of recognition of the authors based on the monogram is mainly due to large dimension of the space characteristics and the proximity characteristic values to each other. This is due to the impossibility of separating the plurality of features that characterize each of the author of the feature space, the usual linear hypersurfaces. On the other hand it is also associated with a small amount of information in newspaper articles and low information content of the information. The article describes the results of experiments to determine the authorship of newspaper articles a small amount in the Azeri language with the use of a statistical approach to the analysis used by the authors of N-grams. Formulas for the weighting factors that determine the importance of a particular trait in determining authorship.
Key words: word processing, N-grammes, weight coefficients.

Айда-заде К.Р., Талыбов С.Г.

Әзірбайжан мәтіндерінде авторлықты анықтауда N-грамм үшін салмақ коэффициенттерін пайдалану

Өздеріңіз білетіндей мәтінді өңдеудің ең маңызды мәселелердің бірі, авторлары бойынша классификациялау, яғни, авторлардың алдын ала белгілі бір тобының қайсысы мәтіннің болжамды авторы болып табылатын анықтау. Осы мәселені автоматтандыру шешімдері өткен ғасырдың 70-шы жылдарынан аса қарқынды дами бастады. Бастапқыда, бұл мәселені шешу әдістері кілттік сөздер үшін құрылған мамандандырылған сөздіктерге негізделген.Монограмма негізінде авторлар танудың салыстырмалы түрде процентінің аздығы, қасиеттер кеңістігінің үлкен өлшеміне және белгілердің бір-біріне жақын болуынан.Әр авторды сипаттайтын қасиеттер кеңістігін қарапайым гипержазықтықпен бөліп алу мүмкін еместігіне байланысты. Екінші жағынан, бұл сондай-ақ газет мақалаларының ақпараты шағын мөлшерде және ақпараттың мазмұнының толық еместігіне байланысты. Мақалада авторлар талдауға пайдаланатын N-грамм статистикалық тәсілді әзірбайжан тілінде аз көлемде жазылған газет мақалаларын авторлыққа анықтауға негізделген эксперимент нәтижелері сипатталады. Авторлықты анықтауда маңызды қасиеттерді анықтау үшін ауырлық коэффициенттерге арналған формулалар келтірілген.

Түйен сөздер: мәтінді өңдеу, N-граммалар, салмақ коэфициенттері.

1. Введение

Как известно одной из важных проблем обработки текстов является их классификация по авторам, т.е. определение того, кто из заранее заданной группы авторов является предполагаемым автором конкретно данного текста.

Автоматизацией решения этой проблемы наиболее интенсивно начали заниматься в 70-х годах прошлого века. Первоначально методы решения этой проблемы базировались на использовании созданных специальных глоссариев для ключевых слов.

Mosteller [1] был одним из первых, использовавших байесовский анализ для решения проблемы распознавания авторства. Далее Burrows в работе [2] использовал частоты используемых слов авторами, Morton [3] - длины предложений, Brainerd [4] - среднее число слогов, Twedie [5] - отношение числа используемых слов к общему количеству слов в тексте. Фюрнкранц [6] и Тан [7] использовали N-грамм (2-грамм и 3-грамм) для классификации текста. В работе [11] для распознавания авторов русской художественной литературы была использована частота встречаемости букв и буквосочетаний.

В Азербайджане впервые авторами работы [9] для распознавания авторства исследована частота использования букв и длины слов, но тем не менее, до сих пор компьютерной системы по распознаванию авторства текстов на азербайджанском языке нет. В данной работе изучается проблема идентификации авторства на основе анализа авторских статей небольшого объема. Основная трудность распознавания авторства текстов (статей) малого объема на азербайджанском языке заключается в том, что в словах используется большое количество малоинформативных суффиксов, окончаний, а автоматический разбор слов на составные части для азербайджанского языка до сегодняшнего дня остается нерешенной проблемой.

2. Постановка задачи

Формально постановку задачи идентификации авторства текстов можно описать следующим образом.

В базе данных имеются тексты n авторов и от каждого из них m_i текстов $D_{i,j}$ j = 1, ..., m_i, i = 1, ..., n. Класс (группу) текстов i–того автора обозначим через Y_i. Рассматриваемая в статье задача состоит в том, что при появлении нового текста D требуется определить какому из n авторов или, другими словами, к какому классу Y_i эта работа принадлежит.

Введем следующие обозначения, определения и формулы.

Каждому из текстов $D_{i,j}$ и D сопоставим множество значений признаков $\{M^s_{i,j},\ s \in K_i\}$ и $\{d_s,\ s \in K_i\}$, $K = \bigcap_{s=1}^{n} K_s$, i=1,...,n,j=1...,$m_i$, на основе которых происходит классификация текстов по авторам. Здесь K_i – множество признаков для определения авторства i-го автора, i=1,...,n.

Пусть $N_{i,j}$ - длина (объем) j-го текста i-го автора, m_i - количество статей i-го автора, находящихся в базе данных, тогда ясно, что среднее значение s-ого признака i-го автора в j-ой статье определяется формулой

$$\varepsilon^s_{i,j} = \frac{M^s_{i,j}}{N_{i,j}}, s \in K_i, j = 1, ..., m_i, i = 1, ..., n. \quad (1)$$

среднее значение s-го признака во всех статьях i-го автора равно

$$\varepsilon^s_i = \frac{\Sigma^{m_i}_{j=1} M^s_{i,j}}{\Sigma^{m_i}_{j=1} N_{i,j}}, s \in K_i, i = 1, ..., n. \quad (2)$$

Пусть среднее значение s-го признака в новой статье D равно

$$\chi^s_D = \frac{m^s_D}{n_D}, s \in K_i, i = 1, ..., n. \quad (3)$$

здесь m^s_D - значение s-го признака в новой статье D, а N_D – ее длина (объем).

Очевидно, что дисперсия s-го признака для i-го автора равна

$$(d^s_i)^2 = \frac{\Sigma^{m_i}_{j=1}(M^s_{i,j} - \varepsilon^s_i)^2}{\Sigma^{m_i}_{j=1} N_{i,j}}, s \in K_i, i = 1, ..., n. \quad (4)$$

Вариация s-го признака для i-го автора равна

$$\upsilon^s_i = \frac{d^s_i * 100}{\varepsilon^s_i}, s \in K_i, i = 1, ..., n. \quad (5)$$

Рассмотрим величины

$$R^1_i = \Sigma_{s \in K} \alpha_s \mid \chi^s_D - \varepsilon^s_i \mid, i = 1, ..., n. \quad (6)$$

и

$$R^2_i = \Sigma_{s \in K} \alpha_s (\frac{\chi^s_D - \varepsilon^s_i}{\varepsilon^s_i})^2, i = 1, ..., n. \quad (7)$$

определяющие близость (норму) значений признаков нового текста D к значениям признаков, характеризующих i-го автора; α_s – вес (важность) s-го признака для определения авторства статей.

Нормализуем величины R^1_i и R^2_i по следующей формуле

$$RN^1_i = R^1_i / \Sigma^n_{j=1} R^1_j, i = 1, ..., n. \quad (8)$$

$$RN^2_i = R^2_i / \Sigma^n_{j=1} R^2_j, i = 1, ..., n. \quad (9)$$

3. Используемые методы и алгоритмы распознавания авторства текстов

Алгоритмы функционирования систем идентификации авторства в общем случае включают выполнение следующей последовательности процессов:

- Проводится первичная обработка имеющихся текстов (статей, произведений) различных авторов, для каждого автора определяются числовые значения выбранных признаков;
- Проводится анализ значений признаков и определяется множество информативных признаков для каждого автора (множества признаков могут быть не одинаковыми для разных авторов);
- Определяются значения признаков, представленной новой статьи пока неизвестного автора;
- По определенному критерию на основе известных алгоритмов определяется предполагаемый автор представленной статьи.

4. Признаки авторства, основанные на статистическом анализе буквосочетаний

Отметим, что многие известные алгоритмы и системы распознавания авторства текстов применяют признаки, основанные на анализе использования различных буквосочетаний из n букв, называемыми в литературе N-граммами. Таким образом, в данном случае грамм (монограмм), означает, что в качестве единицы берется одна буква, при этом слова, предложения или абзацы всего текста в зависимости от значения n разбиваются на буквосочетания, содержащие n последовательных букв.

Отметим, что число букв, а следовательно, 1-граммов в азербайджанском языке 32, а практические число всевозможных 2-грамм равно 835. Были реализованы следующие 3 алгоритма, использующие признаки, основанные на n-граммах.

Приведем общее описание алгоритма 1, использующего монограммы.

Шаг 1. Для каждого текста (статьи) i-того автора, входящего в класс Y_i, в качестве признаков по формуле (1) определяются частоты использования всех букв алфавита (1-граммы).

Шаг 2. Объединяя все произведения каждого автора в соответствии с формулой (2) рассчитываются средние значения всех признаков.

Шаг 3. Для новой исследуемой статьи D по формуле (3) рассчитывается вектор значений x_D^s признаков, $s \in K$.

Шаг 4. В формуле (6), взяв $\alpha_s = 1$ (все веса равны 1), определяем такое ν, что $R_\nu = min_{1 \le i \le n} R_i$, следовательно автором статьи D является ν-ый автор.

Использованный нами алгоритм 2 на базе диграмм такой же, как алгоритм 1 для монограмм, но анализируется не частота использования отдельных букв, а частота использования всевозможных комбинаций из двух букв алфавита (2-грамм - диграмм), используемых автором в своих статьях.

Приведем описание модифицированного алгоритма 3, использующего монограммы. Основная идея алгоритма, основанного на модифицированных монограммах, состоит в

том, что в этом случае используются устойчивые признаки, не включающие нехарактерные для автора наборы признаков.

В предлагаемом алгоритме для каждого отдельного автора с помощью формулы (5) вычисляется вариация каждого признака. Вес s-ого признака α_s в формуле (6) выбирается в зависимости от значения вариации s-ого признака по всем авторам следующим образом. Обозначим:

$$\nu_s = \begin{cases} min_i\nu_i^s, min_i\nu_i^s > \varepsilon, \\ \varepsilon, min_i\nu_i^s \leq \varepsilon, \end{cases} \quad s \in K$$

Положительная величина ε выбирается исходя из величины значений нехарактерных для авторов признаков. Тогда

$\propto_s = \frac{(\nu^s)^{-1}}{\sum_{j=1}^{k}(\nu_j)^{-1}}, s \in K$

Ясно, что $\propto_s$ удовлетворяют условиям:

$$0 \leq \propto_s \leq 1, \sum_{s\in K} \propto_s = 1$$

Первые два шага предлагаемого алгоритма совпадают с двумя шагами первого алгоритма.

Шаг 3. Используя (4) и (5) для каждого признака класса Y_i, на основании вариации, проверяется устойчивость признаков и устанавливаются значения весов α_s.

Шаг 4. Для новой исследуемой статьи D по формуле(3) рассчитываются значения признаков $x_D^s, s \in K$.

Шаг 5. Определяем ν, при котором $R_\nu = min_i R_i$, следовательно автором статьи D является ν-ый автор.

Таблица 1 – Результаты работы алгоритма

	Алгоритм 1 (N=1)				Алгоритм 2 (N=2)				Алгоритм 3 (N=2)			
	A1	A2	A3	A4	A1	A2	A3	A4	A1	A2	A3	A4
z_1^1	224	260	265	249	253	247	267	231	224	253	243	278
z_2^1	20	263	254	277	257	247	270	224	214	258	248	277
z_1^2	289	210	284	216	226	265	238	269	276	220	278	225
z_2^2	286	223	258	232	232	260	245	261	257	233	264	244
z_1^3	219	249	235	296	257	224	286	231	220	257	215	306
z_2^3	230	221	240	307	232	260	245	226	215	233	264	244
z_1^4	256	249	260	234	252	234	285	275	277	250	240	293
z_2^4	290	212	303	194	235	285	204	263	260	224	293	204

5. Результаты компьютерных экспериментов

Как видно из таблицы 1, при учете весов с абсолютной погрешностью было не правильно установлено лишь авторство статей третьего и четвертого автора, а качество распознавания составляло 75%. Для проверки и сравнения эффективности вышеизложенных алгоритмов для обучения системы в базу данных были включены 50 газетные

информационные статьи четырех авторов, условно названных A1, A2, A3, A4. В качестве признаков в случае применения монограммы (N=1) использовались 32 буквы, в случае диграмм (N=2) использовались 835 реально возможных для азербайджанского языка сочетаний букв. Рассмотрены газетные статьи автора A1 в количестве 13, автора A2 соответственно 11, A3 - 12 и автора A4 - 14. Общее количество букв в статьях составляло от 3438 до 6859. Для распознавания у каждого представленного автора были взяты по 2 статьи, авторство которых было скрыто.В первых четырех столбцах таблиц 1 и 2 приведены результаты работы алгоритма 1, использующего признаки, основанные на монограммах, а в следующих четырех столбцах приведены результаты работы алгоритма 2 а в последних четырех столбцах приведены результаты работы алгоритма 3.В j-той строке i-го столбца таблиц 1 и 2 приведены нормализованные значения соответственно абсолютной погрешности, определяемые по формуле (8) ($RN_i^1(z^j) * 10^(3)$), и относительной погрешности, определяемые по формуле (9) ($RN_i^2(z^j) * 10^(3)$).

Таблица 2 – Результаты работы алгоритма

	Алгоритм 1 (N=1)				Алгоритм 2 (N=2)				Алгоритм 3 (N=2)			
	A1	A2	A3	A4	A1	A2	A3	A4	A1	A2	A3	A4
z_1^1	226	268	267	238	235	257	251	255	235	257	232	256
z_2^1	257	254	218	270	235	250	243	269	235	250	228	248
z_1^2	293	236	242	227	258	233	252	255	258	233	263	229
z_2^2	256	224	264	255	262	224	248	264	262	224	260	224
z_1^3	225	249	245	279	237	252	226	283	237	252	232	253
z_2^3	210	251	233	304	231	253	217	297	231	253	224	250
z_1^4	247	264	266	221	276	242	281	199	276	242	282	236
z_2^4	281	233	258	226	270	244	271	212	270	244	274	244

При учете весов с относительной погрешностью, как видно из таблицы 2, при использовании признаков, основанных на монограммах, было правильно установлено лишь авторство статей четвертого автора, а качество распознавания составляло лишь 50%.

Как видно из таблицы 2, использование алгоритмов, основанных на диграммах, как основного так и модифицированного метода, определили авторство с точностью 100%.

Сравнительно низкий процент распознавания авторов основанных на монограммах объясняется в основном большой размерностью пространства признаков и близостью значений признаков друг к другу. Это связано с невозможностью отделить множества признаков, характеризующих каждого автора из пространства признаков, обычными линейными гиперповерхностями. С другой стороны это также связано с малым объемом информации в газетных статьях и низкой информативностью этой информации.

Литература

[1] Mosteller F., Wallace D.L. "Applied Bayesian and Classical Inference, The Case of the Federalist Papers Reading, MA: Addison-Wesley. – 1984. –p.303.

[2] Burrows J.F. "Not unless you ask nicely: the interpretative nexus between analysis and information Literary Linguist Computing, vol.7, No.2. –1992. –p.91–109.

[3] Morton A.Q. "The Authorship of Greek Prose Journal of the Royal Statistical Society, Series A, vol 128, No 2, – 1965. –p.169–233.

[4] Brainerd B. "Weighting Evidence in Language and Literature"A Statistical Approach, University of Toronto Press. –1974. –p.288

[5] Tweedie F., Baayen H. "How Variable may a Constant be Measures of Lexical Richness in Perspective Computers and The Humanities, vol.32, no.5. –1998. –p.323–352.

[6] F?rnkranz J. "A Study using n-gram Features for Text Categorization Austrian Research Institute for Artifical Intelligence. –1998. –p.10.

[7] Tan C.M., Wang Y.F., Lee C.D. "The Use of Bigrams to Enhance Journal Information Processing and Management, vol.30, no.4. –2002. –p.529–546.

[8] Aida-zade K.R., Talibov S.G. "Analysis of the effectiveness of the methods of recognition of authorship of texts in the Azerbaijani language The 5th International Conference on Control and Optimization with Industrial Applications (COIA-2015), , Baku, Azerbaijan, 27–29 August. –2015. –p.183.

[9] Gasimov S., Ibrahimov I. "Analysis of sentences and words used in azerbaijani texts The Second International Conference "Problems of Cybernetics and Informatics", Baku, September 10–12. –2008. –p.117–119.

[10] Dogan S., Diri B. "Tyurkche Dokyumanlar ichin N-gram Tabanly Yeni Bir Synyflandyrma Yazar, Tur ve Cinsiyet, Tyurkiye Bilishim Vakfy Bilgisayar Bilimleri ve Myuhendisliji Dergisi. –2010. s.11–20.

[11] Хмелёв Д.В. "Распознавание автора текста с использованием цепей А.А.Маркова Вестник МГУ, сер.9: Филология,№2. –2000. –ст.115–126.

References

[1] Mosteller F., Wallace D.L. "Applied Bayesian and Classical Inference, The Case of the Federalist Papers Reading, MA: Addison-Wesley. – 1984. –p.303.

[2] Burrows J.F. "Not unless you ask nicely: the interpretative nexus between analysis and information Literary Linguist Computing, vol.7, No.2. –1992. –p.91–109.

[3] Morton A.Q. "The Authorship of Greek Prose Journal of the Royal Statistical Society, Series A, vol 128, No 2, – 1965. –p.169–233.

[4] Brainerd B. "Weighting Evidence in Language and Literature"A Statistical Approach, University of Toronto Press. –1974. –p.288

[5] Tweedie F., Baayen H. "How Variable may a Constant be Measures of Lexical Richness in Perspective Computers and The Humanities, vol.32, no.5. –1998. –p.323–352.

[6] F?rnkranz J. "A Study using n-gram Features for Text Categorization Austrian Research Institute for Artifical Intelligence. –1998. –p.10.

[7] Tan C.M., Wang Y.F., Lee C.D. "The Use of Bigrams to Enhance Journal Information Processing and Management, vol.30, no.4. –2002. –p.529–546.

[8] Aida-zade K.R., Talibov S.G. "Analysis of the effectiveness of the methods of recognition of authorship of texts in the Azerbaijani language The 5th International Conference on Control and Optimization with Industrial Applications (COIA-2015), , Baku, Azerbaijan, 27–29 August. –2015. –p.183.

[9] Gasimov S., Ibrahimov I. "Analysis of sentences and words used in azerbaijani texts The Second International Conference “Problems of Cybernetics and Informatics”, Baku, September 10–12. –2008. –p.117–119.

[10] Dogan S., Diri B. "Tyurkche Dokyumanlar ichin N-gram Tabanly Yeni Bir Synyflandyrma Yazar, Tur ve Cinsiyet, Tyurkiye Bilishim Vakfy Bilgisayar Bilimleri ve Myuhendisliji Dergisi. –2010. s.11–20.

[11] Хмелёв Д.В. "Распознавание автора текста с использованием цепей А.А.Маркова Вестник МГУ, сер.9: Филология,№2. –2000. –ст.115–126.

УДК 517.9

Байшемиров Ж.Д.[1*], Жанбырбаев А.Б.[1], Асхатулы А.[2]

[1]Казахский национальный педагогический университет имени Абая
[2]Институт информационных и вычислительных технологий КН МОН РК,
Республика Казахстан, г. Алматы
*E-mail: zbai.kz@gmail.com

Моделирование химических методов увеличения нефтеотдачи

Методами увеличения нефтеотдачи (МУН) являются добыча нефти путем закачки материалов, которые обычно не присутствуют в нефтяном пласте. Закачка химических компонентов снижает подвижность жидкости, тем самым повышает эффективности вытеснения. В то время как химическое заводнение в нефтяной промышленности имеет более высокую эффективность нефтедобычи, чем традиционное заводнение, оно является технически гораздо более сложным, дорогостоящим и рискованным. Модель транспорта описывает такие физико-химические явления, как дисперсия, диффузия, адсорбция, химические реакции и образование поверхностно-активных веществ непосредственно в нефтяном пласте при взаимодействии щелочей с органическими кислотами нефти.В данной работе мы разрабатываем и изучаем многокомпонентную многофазную модель вытеснения с использованием технологии «Щелочь–ПАВ–Полимер»+Пена. Данная модель описывает синергетические эффекты в виде функции межфазного натяжения, сопротивления потоку пены в зависимости от концентрации ПАВ и нефти, капиллярного давления, проницаемости, соотношения газ-жидкость и скорости газа, а поведение фазы уравнениями состояния. Уравнениями баланса являются уравнение баланса массы для каждого химического компонента, а также уравнение давления водной фазы и уравнение баланса энергии.
Ключевые слова: химическая композиционная модель, многофазная среда, увеличения нефтеотдачи.

Baishemirov Zh.D., Zhanbyrbayev A.B., Askhatuly A.

Simulation of chemical methods of enhanced oil recovery

The methods of enhanced oil recovery (EOR) are the extraction of oil by pumping materials that are not normally present in the oil reservoir. Download of chemical components reduces the mobility of the fluid, thereby increasing the efficiency of displacement. While chemical flooding in the oil industry has a higher efficiency of oil than conventional waterflooding, it is much more technically complicated, expensive and risky. Transport model describes such physicochemical phenomenon of dispersion, diffusion, adsorption, chemical reactions and the formation of surfactant directly to the oil reservoir by reacting organic acids with alkalis oil. In this paper, the multicomponent multiphase model displacement using technology of "Alkali-Surfactant-Polymer"+ Foam are developed and research. This model describes the synergistic effects as a function of the interfacial tension, the flow resistance of the foam depending on the concentration of oil and surfactant, capillary pressure, permeability, liquid-gas ratio and the gas velocity and the phase state equations behavior. Balance equation are mass balance equation for each chemical component, as well as the pressure of the aqueous phase and the energy balance equation.
Key words: chemical compositional model, multiphase environment , enhanced oil recovery.

Байшемиров Ж.Д., Жанбырбаев А.Б., Асхатулы А.

Мұнай қайтарымын арттыру химиялық әдістерін моделдеу

Мұнай қабатында әдетте табылмайтын материалдарды айдау арқылы мұнай өндіру - мұнай қайтарымын арттыру әдістері (МҚАӘ) болып табылады. Химиялық компоненттерді айдау сұйықтықтың ұтқырлығын азайтады, сонымен қатар ығыстыру тиімділігін арттырады. Мұнай-газ саласында химиялық суландырудың дәстүрлі суландыруға қарағанда мұнай өндіруден жоғары тиімділігі бар болғанымен, ол техникалық әлдеқайда күрделі, қымбат және тәуекелді болып табылады. Көлік моделі дисперсия, диффузия, адсорбция, химиялық реакциялар және сілтілер мен мұнайдың органикалық қышқылдарымен әрекеттесу барысында тікелей мұнай қатабаттарындағы үстірт белсенді заттардың құрылуы сияқты физикалық-химиялық құбылыстарды сипаттайды. Бұл мақалада біз «Сілті-БАЗ-полимер» + Көбік технологиясын пайдалана отырып көп компонентті көп фазалық моделін зерттеп және зерттемелейміз. Берілген модель БАЗ және мұнай концентрациясына байланысты көбік ағымына кедергі, капиллярлық қысым,өткізгіштік, газ-сұйықтық қатынасы және газ жылдамдығы, фаза аралық керіліс функциясы түрінде синергетикалық нәтижелерін, ал фаза құбылысын күй теңдеулерімен сипаттайды. Әрбір химиялық компонент үшін масса теңгерім теңдеуі, сондай-ақ су фазасы қысым мен энергия балансының теңдеулері баланс теңдеулері болып табылады.

Түйін сөздер: химиялық композициялық моделі,көп фазалы орта,мұнай қайтарымын арттыру.

1. Введение

Схема дискретизации, основанная на блочно-центрированном методе конечных разностей, используется для численного решения математической модели. Тщательным выбором основных неизвестных последовательный подход решения используется для решения системы связанных уравнений для этой модели. Последовательный подход разбивает связанную систему нелинейных основных уравнений этой модели на отдельные уравнения и решает каждое из этих уравнений по отдельности и неявно. Этот подход расширен от IMPEC (неявный по давлению и явный по составу) подхода решения, используемого в UTCHEM для композиционного моделирования химического заводнения. Численное моделирование может быть использовано для проведения исследования механизма, оценки осуществимости, оптимизации экспериментального плана и прогноза производительности химического заводнения, чтобы повысить эффективность добычи нефти и снизить эксплуатационные расходы. Наш симулятор применен к трем экспериментам - химическому потоку без массообмена между фазами, лабораторному песчанику и задаче вытеснения с использованием технологии «Щелочь–ПАВ–Полимер»+Пена с массопереносом, а также к реальному месторождению нефти.

2. Математическая модель

Основные дифференциальные уравнения для композиционной модели химического заводнения состоят из уравнения сохранения массы для каждого компонента, уравнения энергии, закона Дарси, уравнения сохранения полной масса или непрерывности для давления и поведения фазы [1-2]. Эти уравнения разработаны в рамках предположений: локального термодинамического равновесия, неподвижной твердой фазы, дисперсии Фика, идеального смешивания, слабо сжимаемой почвы и жидкости и закона Дарси.

Мы рассмотрим общий случай, где n_c химических компонент формируют n_p фаз.

Пусть ϕ и $\overline{\overline{k}}$ обозначают пористость и проницаемость пористой среды, а ρ_α, S_α, μ_α, p_α, $\overrightarrow{u}_\alpha$ и $k_{r\alpha}$ обозначают плотность, насыщенность, вязкость, давление, объемная скорость, и относительная фазовая проницаемость фазы $\alpha = 1, .., n_p$ соответственно [3]. Закон сохранения массы для компонента i выражается относительно полной концентрации этого компонента на единицу объема пор:

$$\frac{\partial}{\partial t}(\phi \tilde{c}_i \rho_i) = -\nabla \cdot \left(\sum_{\alpha=1}^{n_p} \rho_i \left[c_{i\alpha} \overrightarrow{u}_\alpha - \overline{\overline{D}}_{i\alpha} \cdot \nabla c_{i\alpha} \right] \right) + q_i, (i = 1, ..., n_c) \tag{1}$$

где полная концентрация компонента $\tilde{c}_i$ - сумма концентраций компонента по всем фазам, включая компонентов, адсорбированных на твердой фазе:

$$\tilde{c}_i = (1 - \sum_{i=1}^{n_{cv}} \hat{c}_i) \sum_{\alpha=1}^{n_p} S_\alpha c_{i\alpha} + \hat{c}_i,$$

n_{cv}- количество компонентов, занимающих объем (таких как вода, нефть, ПАВ и воздух), $\hat{c}_i$, ρ_i, и q_i - концентрация адсорбированного компонента, массовая плотность и член источник/сток компонента i, а также $c_{i\alpha}$ и $\overline{\overline{D}}_{i\alpha}$ - концентрация и тензор диффузии–дисперсии компонента i в фазе α, соответственно.

Зависимость плотности ρ_i от давления опорной фазы (фазы отсчета) выражается простой формулой через коэффициент сжимаемости:

$$c_i^0 = \frac{1}{\rho_i} \frac{\partial \rho_i}{\partial p_r}\bigg|_T$$

при фиксированной температуре T, где c_i^0 - коэффициент сжимаемости компонента i. Для слабосжимаемой жидкости ρ_i можно записать в виде:

$$\rho_i = \rho_i^0 (1 + c_i^0 (p_r - p_r^0)) \tag{2}$$

где c_i^0 и ρ_i^0 - постоянный коэффициент сжимаемости и плотность при опорном давлении p_r^0, соответственно.

Тензор диффузии-дисперсии $\overline{\overline{D}}_{i\alpha}$ для многофазного течения определяется в следующем виде:

$$\overline{\overline{D}}_{i\alpha}(\overrightarrow{u}_\alpha) = \phi \left\{ S_\alpha d_{i\alpha} \overline{\overline{I}} + |\overrightarrow{u}_\alpha| \left(d_{l\alpha} \overline{\overline{E}}(\overrightarrow{u}_\alpha) + d_{t\alpha} \overline{\overline{E}}^{\perp}(\overrightarrow{u}_\alpha) \right) \right\}$$

где $d_{i\alpha}$ - коэффициент молекулярной диффузии компонента i в фазе α, $d_{l\alpha}$ и $d_{t\alpha}$ - коэффициент продольной и поперечной дисперсий фазы α, соответственно, $|\overrightarrow{u}_\alpha|$ - Эвклидова норма $\overrightarrow{u}_\alpha$:

$$|\overrightarrow{u}_\alpha| = \sqrt{u_{1\alpha}^2 + u_{2\alpha}^2 + u_{3\alpha}^2}, \overrightarrow{u}_\alpha = (u_{1\alpha}, u_{2\alpha}, u_{3\alpha}),$$

$\overline{\overline{E}}(\overrightarrow{u}_\alpha)$ - ортогональная проекция по скорости:

$$\overline{\overline{E}}(\overrightarrow{u}_\alpha) = \frac{1}{|\overrightarrow{u}_\alpha|^2}\begin{pmatrix} u_{1\alpha}^2 & u_{1\alpha}u_{2\alpha} & u_{1\alpha}u_{3\alpha} \\ u_{2\alpha}u_{1\alpha} & u_{2\alpha}^2 & u_{2\alpha}u_{3\alpha} \\ u_{3\alpha}u_{1\alpha} & u_{3\alpha}u_{2\alpha} & u_{3\alpha}^2 \end{pmatrix}$$

$\overline{\overline{E}}^{\perp} = \overline{\overline{I}} - \overline{\overline{E}}(\overrightarrow{u}_\alpha)$ и $\overline{\overline{I}}$ - единичная матрица, $i = 1, ..., n_c$, $\alpha = 1, .., n_p$. Член источника/стока q_i комбинирует все расходы компонента i и выражается в виде:

$$q_i = \phi \sum_{\alpha=1}^{n_p} S_\alpha r_{i\alpha} + (1-\phi) r_{is} + \tilde{q}_i$$

где $r_{i\alpha}$ и r_{is} - скорости реакций компонента i в жидкой фазе α и твердой фазе s, соответственно, $\tilde{q}_i$ - скорость закачки/добычи компонента i на единиу объема.

Объемная скорость $\overrightarrow{u}_\alpha$ выражается по закону Дарси:

$$\overrightarrow{u}_\alpha = -\frac{1}{\mu_\alpha}\overline{\overline{k}} k_{r\alpha}(\nabla p_\alpha - \rho_\alpha g \nabla z), \alpha = 1, .., n_p \tag{3}$$

где g - величина ускорения свободного падения и z - глубина.

Уравнение сохранения энергии:

$$\frac{\partial}{\partial t}\left(\phi \sum_{\alpha=1}^{n_p} \rho_\alpha S_\alpha U_\alpha + (1-\phi)\rho_s c_s T\right) + \nabla \cdot \sum_{\alpha=1}^{n_p} \rho_\alpha \overrightarrow{u}_\alpha H_\alpha - \nabla \cdot (K_T \nabla T) = q_c - q_L \tag{4}$$

где T - температура, U_α и H_α - удельная внутренняя энергия и энтальпия фазы α (на единицу массы), ρ_s и c_s - плотность и удельная теплоемкость твердой фазы s, K_T представляет полную теплопроводность, q_c - источник тепла, q_L - потеря тепла через кровлю и подошву пласта. В уравнении (4), удельная внутренняя энергия U_α и энтальпия H_α фазы α могут быть рассчитаны по следующим формулам [4-5]:

$$U_\alpha = C_{V\alpha} T, H_\alpha = C_{p\alpha} T$$

где $C_{V\alpha}$ и $C_{p\alpha}$ - теплоемкости фазы α при постоянном объеме и постоянном давлении, соответственно.

В IMPEC или последовательном моделировании химического заводнения, уравнение давления для водной фазы получено путем общего баланса массы по компонентам, занимающим объем:

$$p_{c\alpha 1} = p_\alpha - p_1, (\alpha = 1, .., n_p) \tag{5}$$

где $p_{c\alpha 1} = 0$ для удобства. Вводим подвижность фазы в виде:

$$\lambda_{r\alpha c} = \frac{k_{r\alpha}}{\mu_\alpha} \sum_{i=1}^{n_{cv}} \rho_i c_{i\alpha},$$

полную подвижность

$$\lambda_{rTc} = \sum_{\alpha=1}^{n_p} \lambda_{r\alpha c}$$

и удельного веса

$$\gamma_\alpha = \rho_\alpha g$$

Отметим, что:
$\sum_{i=1}^{n_{cv}} \rho_i \overline{\overline{D}}_{i\alpha} \nabla c_{i\alpha} = 0, \sum_{i=1}^{n_{cv}} r_{i\alpha} = \sum_{i=1}^{n_{cv}} r_{is} = 0.$

Теперь суммируя уравнений (1) по $i = 1, .., n_{cv}$, получим уравнение давления:

$$\phi c_t \frac{\partial p_1}{\partial t} - \nabla \cdot (\overline{\overline{k}} \lambda_{rTc} \nabla p_1) = \nabla \cdot \left(\overline{\overline{k}} \sum_{\alpha=2}^{n_p} (\lambda_{r\alpha c} \nabla p_{c\alpha 1}) \right) - \nabla \cdot \left(\overline{\overline{k}} \sum_{\alpha=2}^{n_p} (\lambda_{r\alpha c} \gamma_\alpha) \nabla z \right) + \tilde{Q} \quad (6)$$

где коэффициент полной сжимаемости c_t определяется в виде:
$c_t = \frac{1}{\phi} \frac{\partial}{\partial p_1} \sum_{i=1}^{n_{cv}} \phi \tilde{c}_i \rho_i$
а источник в виде

$$\tilde{Q} = \sum_{i=1}^{n_{cv}} \tilde{q}_i$$

Предположим, что сжимаемость твердой фазы дается в виде:

$$\phi = \phi^0 (1 + c_R (p_r - p_r^0)) \quad (7)$$

где c_R - коэффициент сжимаемости породы, p_r^0 - опорное давление, ϕ^0 - пористость при p_r^0. С $p_r = p_1$ и используя уравнения (2) и (7), имеем:

$$\phi \tilde{c}_i \rho_i = \phi^0 \tilde{c}_i \rho_i^0 (1 + (c_R - c_i^0)(p_1 - p_1^0) + c_R c_i^0 (p_1 - p_1^0)^2).$$

Если пренебречь членами высших порядков в этом уравнении (вследствие слабой сжимаемости породы и жидких фаз), оно примет вид:

$$\phi \tilde{c}_i \rho_i = \phi^0 \tilde{c}_i \rho_i^0 (1 + (c_R - c_i^0)(p_1 - p_1^0)) \quad (8)$$

С использованием уравнения (8) коэффициент полной сжимаемости c_t приводится к следующему простому виду:

$$c_t = \frac{\phi^0}{\phi} \sum_{i=1}^{n_{cv}} \tilde{c}_i \rho_i^0 (c_R + c_i^0)$$

Имеются больше зависимых переменных, чем дифференциальные и алгебраические соотношения; формально в модели присутствуют $n_c + n_{cv} + n_c n_p + 3n_p + 1$ зависимые

переменные: c_i, $\hat{c}_i$, $c_{i\alpha}$, T, $\overrightarrow{u}_\alpha$, p_α и S_α , $i = 1, ..., n_c$, $\alpha = 1, .., n_p$. Уравнения (1) и (3)-(6) обеспечивают $n_c + 2n_p$ дифференциальные или алгебраические независимые соотношения; дополнительные $n_c + n_c n_p + n_p + 1$ соотношения даются ниже следующими ограничениями.

Ограничение на насыщенности фаз:

$$\sum_{\alpha=1}^{n_p} S_\alpha = 1$$

n_p ограничения на концентрации фаз:

$$\sum_{i=1}^{n_{cv}} c_{i\alpha} = 1$$

n_c соотношения концентрации компонент:

$$\sum_{\alpha=1}^{n_p} S_\alpha c_{i\alpha} = c_i$$

n_{cv} ограничения на концентрации адсорбции:

$$\hat{c}_i = \hat{c}_i(c_1, ..., c_{n_c})$$

$n_c(n_p - 1)$ соотношения равновесии фаз:

$$f_{i\alpha}(p_\alpha, T, c_{1\alpha}, ..., c_{n_c\alpha}) = f_{i\beta}(p_\beta, T, c_{1\beta}, ..., c_{n_c\beta})$$

где $f_{i\alpha}$ - функция фугитивности компонента i в фазе α.

Для химического композиционного течения, несколько уравнений состояния могут быть использованы для определения функций фугитивности $f_{i\alpha}$, такие как уравнений состояния Редлиха–Куонга, Редлиха–Куонга–Соава и Пенга–Робинзона. В нашей работе для определения функций фугитивности $f_{i\alpha}$ используется уравнение состояния Пенга–Робинзона.

3. Численный метод

В используемом нами численном методе временная дискретизация основана на схеме Эйлера с разностями назад, в то время как пространственная дискретизация осуществляется на основе блочно-центрированных конечных разностях с гармонически усредненными коэффициентами (например, коэффициент проницаемости). Наш подход решения расширен из IMPEC, который был использован для композиционного симулятора химического заводнения. IMPEC метод решает уравнение для давления неявно и уравнения

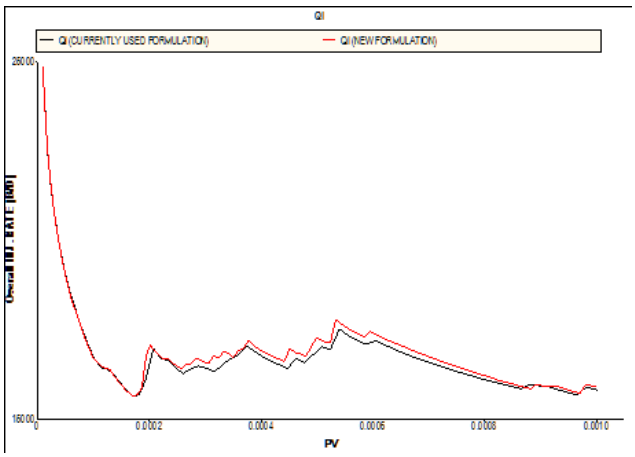

Рисунок 1 – Зависимость полной скорости закачки от суммарного нагнетенного объема пор

для компонентов явно. В рамках данного исследования разработана новая математическая формулировка химической композиционной модели, которая позволяет решать систему основных уравнений модели неявно и последовательно. Из-за явности решения уравнений для компонентов, размер временных шагов должен быть ограничен, чтобы стабилизировать общую процедуру. В противоположность этому, используемый здесь подход представляет собой последовательный подход, который решает и давление, и композиции неявно. Следовательно, этот подход расслабляет ограничение на шаг по времени. Итерации по методу Ньютона-Рафсона для каждого из уравнений давления и состава ограничены максимальными изменениями в этих переменных по итерации, и размер шага по времени определяется автоматически максимальными изменениями по временному шагу. Включены члены межблочного потока (например, для подвижности) и закачки/добычи с разностями против потока. Система линейных алгебраических уравнений решается уменьшенной ширины полосы итерационным методом GMRES. Неявная схема для каждого из уравнений давления и сохранения компонентов и неявное вычисление забойного давления добавляют устойчивость и сохраняют заданные пользователем расходы и ограничения. В самом деле, для численных экспериментов, мы обнаружили, что последовательный подход приблизительно в два раза быстрее, чем IMPEC.

В ходе проведения исследовательских работ создано программное средство для иссле-

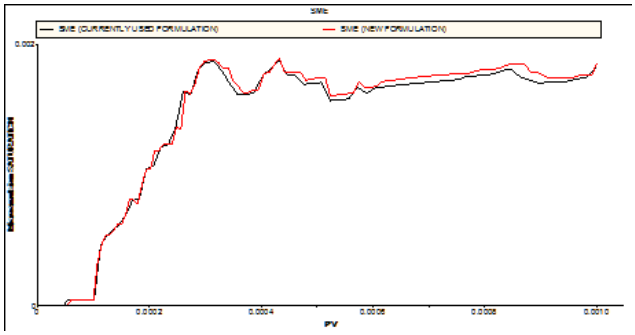

Рисунок 2 – Зависимость насыщенности микроэмульсии от суммарного нагнетенного объема пор

дования химических методов увеличения нефтеотдачи и процессов ремедиации водоносных слоёв поверхностно-активными веществами. В текущем начальном этапе процесса разработки математической и численной моделей цель состоит в том, чтобы оценить, подходит ли наша недавно разработанная новая математическая формулировка для моделирования механизма заводнения «Щелочь–ПАВ–Полимер». Так как, аналитического решения для рассматриваемой задачи химического заводнения, проверка модели основана на сравнениях полученных результатов с результатами симулятора UTCHEM. Сравнение между результатами, полученными с помощью традиционной и новой моделей, приведено на рисунках 1-3 для диапазона 0 - 0,0012 PV для соответствующих переменных.

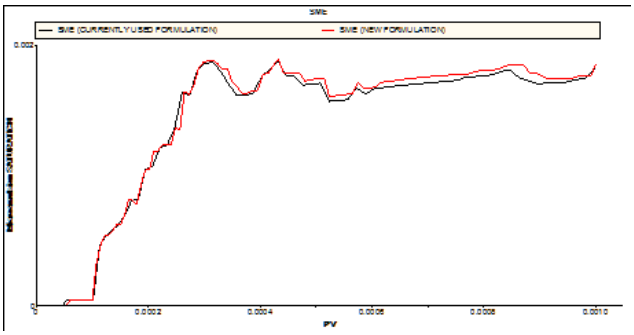

Рисунок 3 – Зависимость объема адсорбированного ПАВ от суммарного нагнетенного объема пор

4. Заключение

Сравнение с UTCHEM также выполнено. Эти эксперименты показывают, что этот симулятор практичен, надежен и точен для моделирования сложных химических процессов заводнения, а последовательный подход является гораздо эффективнее и точнее, чем IMPEC.

Работа выполнена по грантового финансирования научно-технических программ и проектов Комитетом науки МОН РК, грант № 1028/ГФ4.

Литература

[1] Delshad, Mohammad. "Trapping of Micellar Fluids in Berea Sandstone,"Ph.D. dissertation, The University of Texas at Austin. – 1990.

[2] Jin, M. "A Study of Nonaqueous Phase Liquid Characterization and Surfactant Remediation,"Ph.D. dissertation, The University of Texas at Austin. – 1995.

[3] Delshad M., Pope G.A., Sepehrnoori K. UTCHEM Version-9.0, Technical Documentation, Center for Petroleum and Geosystems Engineering. The University of Texas at Austin, Texas, July 2000.

[4] Hirasaki G., Zhang D.L. Surface Chemistry of Oil Recovery From Fractured, Oil-Wet, Carbonate Formation. SPE J. 9 (2), – 2004. –p.151–162.

[5] Yang, H.D. and Wadleigh, E.E. "Dilute Surfactant IOR—Design Improvement for Massive, Fractured Carbonate Applications."paper SPE 59009 presented at The SPE International Petroleum Conference and Exhibition in Mexico, Villahermosa, Mexico, February 1–3. – 2000.

References

[1] Delshad, Mohammad. "Trapping of Micellar Fluids in Berea Sandstone,"Ph.D. dissertation, The University of Texas at Austin. – 1990.

[2] Jin, M. "A Study of Nonaqueous Phase Liquid Characterization and Surfactant Remediation,"Ph.D. dissertation, The University of Texas at Austin. – 1995.

[3] Delshad M., Pope G.A., Sepehrnoori K. UTCHEM Version-9.0, Technical Documentation, Center for Petroleum and Geosystems Engineering. The University of Texas at Austin, Texas, July 2000.

[4] Hirasaki G., Zhang D.L. Surface Chemistry of Oil Recovery From Fractured, Oil-Wet, Carbonate Formation. SPE J. 9 (2), – 2004. –p.151–162.

[5] Yang, H.D. and Wadleigh, E.E. "Dilute Surfactant IOR—Design Improvement for Massive, Fractured Carbonate Applications."paper SPE 59009 presented at The SPE International Petroleum Conference and Exhibition in Mexico, Villahermosa, Mexico, February 1–3. – 2000.

УДК 004.89: 004.4

Денисова Т.Г.

Институт информационных и вычислительных технологий КН МОН РК,
Республика Казахстан, г.Алматы
E-mail: e-mail: elkaz41@mail.ru

Развитие методов нечеткой логики для формирования терапевтических доз лекарственных средств с учетом свойств организма

Для формирования искусственной иммунной модели терапии лекарственными средствами получены нечеткие множества для описания свойств организма. С целью выбора и тактики применения лекарственных средств, рассмотрены такие основные индивидуальные особенности движения лекарственных средств в организме конкретного пациента, как возраст и масса. Сформированы множества «возраст» и «масса», которые наряду с другими свойства организма человека используются для разработки правил нечеткой логики. Разработка множества «возраст» проводится на основе соотношений доз лекарственных средств и возраста, начиная с самого раннего. Особенно выделены детский и пожилой возраст, так как дети и пожилые люди более чувствительны к действию лекарств по сравнению с лицами среднего возраста. Разработка нечетких множеств, связанных со свойством «масса», выполнена на основе индексов массы тела – индекса Кетле и центильных таблиц. Множество «Центили» представлено лингвистическими переменными, обозначенными термами, связанными с уровнями центильной таблицы: «низкий», «норма», «высокий». Для сформированных множеств «Возраст» и «Центили» приведены расчеты, в соответствии с которыми осуществляется дозирование лекарственных средств в зависимости от свойств организма.
Ключевые слова: нечеткая логика, искусственная иммунная модель, свойства организма, терапевтическая доза, лекарственные средства.

Denisova T.G.

Development of methods for generating fuzzy logic therapeutic dosages of drugs based on the properties of the organism

In order to form an artificial model of the immune therapy medicines obtained fuzzy sets to describe the properties of the body. In order to select tactics and use of medicines, are considered the main features of the individual medicines movement in the body of a particular patient such as age and weight to the selection and use of tactics medicines. Form a plurality of "age"and mass which, along with other properties of the human body are used to develop the rules of fuzzy logic. Development of "age"set is based on the ratio of medicines doses and age, starting with the earliest. A particularly marked for children and the elderly age, as children and the elderly are more sensitive to medicines compared to middle-aged persons. Development of fuzzy sets associated with the property "mass"is made on the basis of body mass index – Quetelet index and centile tables set of "cents"is represented by linguistic variables, denoted by terms related to levels of centile table: "low "normal "high". To form a plurality of "age"and "cents"are given calculations, in accordance with which the dispensing of drugs, depending on the body properties.
Key words: fuzzy logic, artificial immune model properties of the organism, the therapeutic dose of drugs.

Денисова Т.Г.

Ағза қасиеттерін ескере отырып, дәрілік құралдардың емдік мөлшерін қалыптастыру үшін айқын емес логика әдістерінің дамуы

Дәрілік құралдармен емдеудің жасанды иммунды моделін қалыптастыру мақсатында ағза қасиеттерін сипаттайтын айқын емес жиындар алынған. Дәрілік құралдарды таңдау және қабылдау мәнері мақсатында, нақты науқастың ағзасымен дәрілік препараттардын қозғалысына науқастың жас мөлшері мен салмағы секілді жеке-дана ерекшеліктері қарастырылған. «жас мөлшері» және «салмақ» деп аталатын жиындар қалыптастырылған, олар адам ағзасының басқа қасиеттерімен бірге айқын емес логика ережелерін қалыптастыру үшін пайдаланылады. «Жас мөлшері» жиыны дәрілік құралдар мөлшерінің жас мөлшеріне қатынасы негізінде өткізіледі (ең алғашқысынан бастап). Әсіресе, бала және кәрі жастағылар арнайы бөлінген, өйткені бұл жастағы науқастар, орта жасты кісілерге қарағанда, дәрелердің әсер етуіне сезімтал болып келеді. «Салмақ» қасиетіне сәйкес айқын емес жиындарды қалыптастыру – дене салмағының индексі– Кетле индексі және центилді кестелер негізінде орындалған. «Центили» жиыны лингвистикалық айнымалылармен, яғни, центильді кесте деңгейіне байланысты: «төмен», «қалыпты», «жоғары» тералармен берілген. Қалыптастырылған «жас мөлшері» мен «центили» жиындар үшін есептеулер келтірілген. Оларға сәйкес, дәрілік құралдар мөлшерлемесі ағза қасиеттеріне байланысты жүзеге асырылады.

Түйін сөздер: айқын емес логика, жасанды иммунды модел, ағза қасиеттері, емдік мөлшер, дәрілік құралдар.

1. Введение

В соответствии с приоритетными направлениями Государственной программы реформирования и развития здравоохранения Республики Казахстан, задачи, связанные с обеспечением соответствующего уровня качества лечения и безопасности лекарственных средств, являются актуальными. Важным условием повышения эффективности и безопасности лекарственных средств (ЛС) является не только грамотная стратегия их применения, но и тактика для каждого конкретного пациента. Тактика выбора и применения ЛС во многом зависит от индивидуальных особенностей движения ЛС в организме конкретного пациента, а точнее, от различных факторов, воздействующих на нее. Знание и учет этих факторов позволяет индивидуализировано подойти к выбору как самого ЛС, так и его режима дозирования, а также к коррекции проводимого лечения, что лежит в основе принципов так называемой персонализированной медицины, применение в клинической практике которых позволит повысить эффективность и безопасность лечения.

Учет индивидуальных свойств организма очень важный фактор для построения математических моделей, описывающих динамику развития заболеваний и процессы терапии. Одними из важнейших свойств организма являются: 1) возраст; 2) масса тела; 3) функциональной состояние; 4) патологическое состояние; 5) пол; 6) генетические особенности. В данной статье приведены результаты системного подхода к обработке структурной информации о возрасте человека, с учетом влияния данного свойства организма на принципы дозирования ЛС.

Изучение особенностей действия и применения ЛС у лиц детского возраста имеет (педиатрическая фармакология) особое значение, так как именно данный возраст требует тщательного подбора доз ЛС [1]. Современные пробелы в наших знаниях (например, отсутствие полных данных о возрастной динамике экспрессии ферментов биотрансформации и транспортёров ЛС) препятствуют использованию простых лекарственных

"антропометрических"подходов к выбору режимов дозирования ЛС у детей младшего возраста. Однако такие подходы могут иметь важное клиническое значение у детей старше восьми лет и у подростков, у которых функции органов приближены к таковым у взрослых.

Также и гериатрическая фармакология приобретает всё большее значение, так как доля пациентов этих возрастных групп среди населения значительно возросла. В работе [1] отмечено, что во всех высокоразвитых странах мира в настоящее время происходит стремительное старение населения. По прогнозам Организации Объединённых Наций, к 2025 году число людей старше 60 лет достигнет 1,2 млрд человек. Это потребует дальнейшего развития гериатрической фармакологии - раздела клинической фармакологии, изучающего принципы дозирования и особенности взаимодействия ЛС у пожилых, а также пути повышения устойчивости организма таких людей к нежелательному воздействию ЛС.

Прогрессирующее уменьшение адаптационных возможностей организма, изменение его реактивности создают условия для развития патологии [2 - 6]. Уровень заболеваемости у пожилых людей (60-74 года) почти в два раза выше, а у лиц старческого возраста (75 лет и старше) - в 6 раз выше, чем у лиц молодого возраста [3]. Имеются существенные различия в развитии патологических процессов у старых и молодых людей. Для большинства болезней в пожилом и старческом возрасте характерны малая выраженность и необычность клинических проявлений. У пожилых людей наблюдается склонность к медленно нарастающим, вялотекущим патологическим процессам [6] .

Целью данного доклада является представление результатов системного подхода к обработке структурной информации о возрасте и о массе человека с учетом влияния данных свойств организма на принципы выбора и методики дозирования лекарственных средств с использованием методологии нечетких множеств. В дальнейших исследованиях будут представлены результаты оценки других свойств организма и их использование при построении искусственной иммунной системы терапии заболеваний человека.

2. Применение нечёткой логики к принципам выбора и методики дозирования лекарственных средств в соответствии с возрастом

Чувствительность организма к лекарственным веществам меняется в зависимости от возраста. Для разных фармакологических средств закономерности в этом отношении различны. Однако, в общем, дети и пожилые люди более чувствительны к действию лекарств по сравнению с лицами среднего возраста [7]. Поэтому выделяют две категории пациентов – дети (до 14 лет) и пожилые люди (старше 65 лет), для которых в силу возрастных особенностей организма отдельно устанавливают дозировки и частоту приема лекарств.

С возрастом увеличивается масса тела и одновременно меняется чувствительность детского организма к лекарственным веществам, причем к различным веществам поразному [8]. Поэтому трудно дать общие рекомендации в отношении дозировки лекарственных веществ для детей. Для того чтобы определить терапевтическую дозу каждого ядовитого или сильнодействующего лекарственного вещества, следует пользоваться Государственной фармакопеей [9]. Для остальных препаратов дозы уменьшают в зависимости от возраста по сравнению с дозами для взрослых (достигших 25-летнего возраста) следующим образом:

– для детей до 1 года: $\frac{1}{24} \div \frac{1}{2}$ дозы для взрослых; для детей 1 года: $\frac{1}{12}$ дозы для взрослых; для детей 2 лет: $\frac{1}{8}$ дозы для взрослых; для детей 4 лет: $\frac{1}{6}$ дозы для взрослых; для детей 6 лет: $\frac{1}{4}$ дозы для взрослых; для детей 7 лет: $\frac{1}{3}$ дозы для взрослых; для детей 14 лет: $\frac{1}{2}$ дозы для взрослых;

– для молодых людей 18 лет: $\frac{3}{4}$дозы для взрослых;

– для взрослых людей от 25 лет: 1 доза.

При назначении лекарственных веществ пожилым людям (старше 60 лет) учитывается их различная чувствительность к разным группам лекарственных средств. "Дозы препаратов, угнетающих центральную нервную систему (снотворные, нейролептические средства, препараты группы морфина, бромиды), а также сердечных гликозидов, мочегонных средств уменьшают до $\frac{1}{2}$ дозы взрослого. Дозы других сильнодействующих и ядовитых лекарственных средств составляют $\frac{2}{3}$ дозы взрослого. Дозы антибиотиков, сульфаниламидов и витаминов обычно равны дозам взрослых [8].

Современные достижения в области возрастной физиологии стареющего организма, а также многочисленные клинические наблюдения и накапливающиеся данные о действии медикаментозных средств в гериатрической практике свидетельствуют о необходимости научного развития фармакологии старческого возраста [10]. Таким образом, изменения процессов всасывания, распределения, биотрансформации и элиминации в пожилом и старческом возрасте способствуют снижению клиренса и увеличению периода полувыведения ЛС. Вследствие этого дозы большинства препаратов, которые назначают гериатрическим больным, советуют уменьшать на $\frac{1}{2} \div \frac{1}{4}$ от рекомендованной и соответственно увеличивать интервалы между их введением.

В настоящее время существует широкий круг работ в области медицины, касающихся развитию методов вычислительных и информационных технологий для получения результатов по обработке данных для диагностики и лечения болезней пациентов. В связи с тем, что задачи, связанные с вопросами медицины, имеют высокую сложность и неопределенность, используются методы интеллектуальных систем, такие как нечеткая логика, искусственные нейронные сети и генетические алгоритмы.

Во многих областях медицины, например при терапии болезней почек, диагностики рака, астмы, разработаны подходы на основе нечеткой логики [11]. Система управления на основе нечеткой логики помогает врачам давать быстрые и эффективные решения относительно дозы лекарственного средства с учетом всех факторов. С помощью этой системы медицинские ошибки сведены к минимуму, предотвращаются возможные осложнения. Более того, надежность этого метода была доказана и принята в статистических исследованиях [12,13].

На рисунке 1 показано представление множества «Возраст» лингвистическими переменными, обозначенными термами: «дети», «молодые люди», «взрослый», «пожилой». В дальнейшем, обозначим множество «Возраст» как x_1. В частности, построены нечеткие множества с функциями принадлежности: $\mu_{\text{дети}}(x_1)$, $\mu_{\text{мол.люди}}(x_1)$, $\mu_{\text{взрослый}}(x_1)$, $\mu_{\text{пожилой}}(x_1)$.

3. Развитие теории нечетких множеств обработки данных для методики дозирования лекарственных средств в педиатрии

В настоящее время в педиатрической практике не достаточно использовать подходы к разработке режимов дозирования ЛС на основе антропометрических характеристик

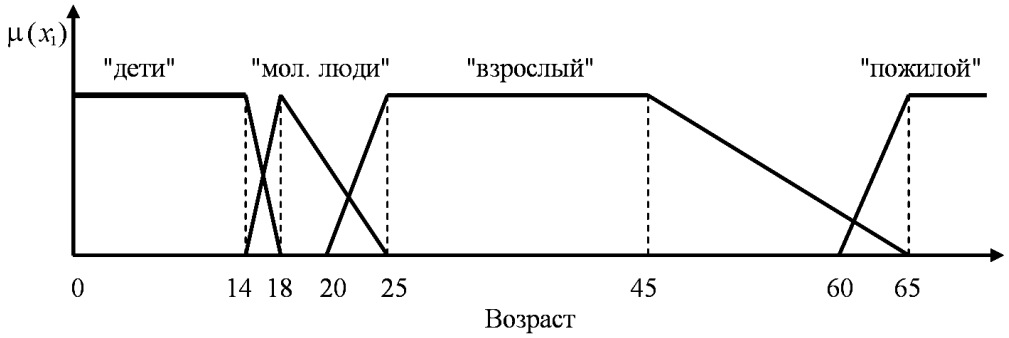

Рисунок 1 – График нечетких множеств свойства «Возраст»

ребёнка. Развитие ребёнка – нелинейный процесс; морфологические и функциональные изменения организма могут идти не параллельно, особенно во время первого десятилетия жизни, поэтому упрощённые подходы к расчёту режимов дозирования ЛС не адекватны для детей различных возрастов. Для проведения эффективной и безопасной фармакотерапии у детей необходимо фундаментальное понимание возрастных аспектов фармакокинетики и фармакодинамики ЛС и учет данных фактов при реализации процессов моделирования.

В соответствии с педиатрическими данными, доза для детей определяется, кроме возраста, полом, массой, длинной тела ребенка, созреванием физиологических функций, а также переносимости детьми тех или иных препаратов [14]. При этом, для установления является ли масса тела ребенка избыточной или недостаточной, с учетом пола, используется индекс Кетле – индекс массы тела(ИМТ) [15]:

1. Массо-ростовой индекс Кетле-I, который используется в периоде новорожденности и отражает пренатальное состояние. Рассчитывается как отношение массы тела (гр) при рождении к его длине (см):

$$\text{ИМТ} = \text{Масса тела при рождении (гр) / длина (см)}. \tag{1}$$

   При нормотрофии величина индекса составляет 60–70. Снижение массо-ростового индекса – свидетельство пренатальной гипотрофии.

2. В пубертатном периоде изменения массы тела происходят не столько за счет нарастания жировой ткани, сколько за счет увеличения, в первую очередь, костной и мышечной массы. Поэтому оценка веса пациентов препубертатного и пубертатного возраста по центильному распределению массы тела относительно его длины является некорректной. В таких случаях массу можно оценивать по индексу Кетле-II:

$$\text{ИМТ} = \text{Масса тела (кг) / квадрат длины тела (м}^2\text{)}. \tag{2}$$

Заведомо здоровых детей относят к разным группам в зависимости от их ИМТ. Пограничные значения ИМТ, отделяющие одну группу от другой, называют центилями. В

работе [14] приведены центильные таблицы с данными по ИМТ для детей от 1 года до 19 лет, соответственно, для мальчиков и для девочек. Центильные распределения наиболее строго и объективно отражают распределение признаков среди здоровых детей.

Колонки центильных таблиц показывают количественные границы признака у определенной доли или процента (центиля) здоровых детей данного возраста и пола. Интервалы между центильными колонками (зоны, коридоры) отражают тот диапазон разнообразия величин признака, который свойственен или 3% (зона от 3-го до 10-го или от 90-го до 97-го центиля), или 15% (зона от 10-го до 25-го или от 75-го до 90-го центиля), или 50% всех здоровых детей возрастно-половой группы (зона от 25-го до 75-го центиля). В зависимости от того, где расположен этот коридор можно формулировать оценочное суждение об уровне массы:

1. зона 1 (до 3-го центиля) – «очень низкий» уровень;
2. зона 2 (от3-го до 10-го центиля) – «низкий уровень»;
3. зона 3 (от 10-го до 25-го центиля) – уровень «ниже среднего»;
4. зона 4 (от 25-го до 75-го центиля) – «средний» уровень;
5. зона 5 (от 75-го до 90-го центиля) – уровень «выше среднего»;
6. зона 6 (от 90-го до 97-го центиля) - «высокий» уровень;
7. зона 7 (от 97-го центиля) – «очень высокий» уровень.

На рисунке 2 показано представление множества «Центили»,x_2, лингвистическими переменными, обозначенными термами, связанными с уровнями центильной таблицы: «низкий», «норма», «высокий». В частности, построены нечеткие множества с функциями принадлежности: $\mu_{\text{низкий}}(x_2)$, $\mu_{\text{норма}}(x_2)$, $\mu_{\text{высокий}}(x_2)$.

Рисунок 2 – График нечетких множеств свойства «масса»

Схема расчета доз с учетом массы и возраста, при нормальной массе тела для нечеткого множества «норма» (рисунок 2) [16]:

$$\text{К}=2^*\text{возраст (полных лет)} + \text{масса тела (в кг)}, \tag{3}$$

где K, % – процент от дозы взрослого, для ребенка определенного возраста и массы тела.

Для расчета сульфаниламидов, к которым дети менее чувствительны, используют формулу

$$\text{К=2*возраст (полных лет) + масса тела (в кг) + 12,} \tag{4}$$

Для детей с избыточной или недостаточной массой тела, для нечетких множеств «низкий» и «высокий» целесообразно определять индивидуальную дозу на основе дозис-фактора [16]. С этой целью дозу для взрослого, выраженной на 1 килограмм веса тела, умножают на дозис-фактор, который индивидуален для каждого возраста ребенка:

– для детей до 1 года: дозис-фактор 1,8; для детей $1 \div 6$ лет: дозис-фактор 1,6; для детей $7 \div 10$ лет: дозис-фактор 1,4; для детей $10 \div 12$ лет: дозис-фактор 1,2; взрослый: дозис-фактор 1.

4. Заключение

Полученные нечеткие множества для свойств организма «возраст», «масса» наряду с другими свойства организма человека используются для разработки правил нечеткой логики и построения искусственной иммунной системы оптимизации терапевтических доз лекарственных средств.

Работа выполнена при поддержке грантового финансирования научно-технических программ и проектов Комитетом науки МОН РК, грант № 0115РК00549.

Литература

[1] Клиническая фармакокинетика: теоретические, прикладные и аналитические аспекты: руководство / под ред. В.Г. Кукеса. – М.: ГЭОТАР-Медиа, 2009. – 432 с.

[2] Газизов Р.М. Основы лекарственной терапии в пожилом и старческом возрасте. – Казань: Практическая медицина. – 2010. – №2 (41). – С. 11-14.

[3] Денисова Т.П., Малинова Л.И. Клиническая геронтология: избранные лекции. – М.: Медицинское информационное агентство, 2008. – 256 с.

[4] Белоусов Ю.Б., Леонов М.В., Вялков А.И. и др. Основы клинической фармакологии и рациональной фармакотерапии: руководство для практикующих врачей. – М.: Бионика. – 2002. – 368 с.

[5] Пожилой больной / под ред. Л.И.Дворецкого. – М.: Русский Врач, 2001. – 144 с.

[6] Руководство по геронтологии и гериатрии. В 4 т. Т.3. Клиническая гериатрия / под ред. В.Н.Ярыгина, А.С. Мелентьева. – М.: ГЭОТАР-Медиа, 2007. – 896 с.

[7] Клиническая фармакология: учебник / сост. Н.В. Кузнецовой. – М.: ГЭОТАР-Медиа, 2013. – 272 с.

[8] Майский В.В., Муратов В.В. Фармакология с рецептурой. – М.: Медицина, 1986. – 448 с.

[9] Государственная Фармакопея Российской Федерации XII. В 5 частях. Часть 2. – М.: Научный центр экспертизы средств медицинского применения, 2008. – 704 с.

[10] Коркушко О.В. Клиническая кардиология в гериатрии. – М.: Медицина, 1980. – 288 с.

[11] Barro S., Marin R. Fuzzy Logic in Medicine // Springer series: Studies in fuzziness and soft computing. – 2001. – Vol. 83. – 310 p.

[12] Dev U., Sultana A., Saha D., Mitra N.K. Application of fuzzy logic in medical data interpretation // Bangladesh J. Sci. Ind. Res. – N. 49 (3). – 2014. – P. 137-146.

[13] Patel A., Gupta S.K., Rehman Q., Verma M.K. Application of fuzzy logic in biomedical iformatics // Journal of Emerging Trends in Computing and Information Sciences. – Vol. 4. – N. 1. – 2013. – P. 57-62.

[14] Справочник по клинической фармакологии и фармакотерапии / Под ред. Чекмана И.С., Пелещука А.П., Пятака О.А. – Киев: Здоровье, 1986. – 736 с.

[15] Карцева Т.В., Дерягина Л.П., Тимофеева Е.П. Физическое развитие детей и факторы, его определяющие. Методы оценки. Учебно-методическое пособие для студентов медицинских ВУЗов. – Новосибирск: Государственное образовательное учреждение высшего профессионального образования Новосибирский государственный медицинский университет федерального агентства РФ по здравоохранению и социальному развитию. – 2008. – 17 с.

[16] Гусель В.А., Маркова И.В. Справочник педиатра по клинической фармакологии. – Л.: Медицина. – 1989. – С. 16-21.

References

[1] Klinicheskaja farmakokinetika: teoreticheskie, prikladnye i analiticheskie aspekty: rukovodstvo / pod red. V.G. Kukesa. – M.: GJeOTAR-Media, 2009. – 432 s. – 653 c.

[2] Gazizov P.M. Osnovy lekarstvennoj terapii v pozhilom i starcheskom vozraste. – Kazan: Prakticheskaja medicina. – 2010. – №2 (41). – S. 11-14.

[3] Denisova T.P., Malinova L.I. Klinicheskaja gerontologija: izbrannye lekcii. – M.: Medicinskoe informacionnoe agentstvo, 2008. – 256 s.

[4] Belousov Ju.B., Leonov M.V., Vjalkov A.I. i dr. Osnovy klinicheskoj farmakologii i racionalnoj farmakoterapii: rukovodstvo dlja praktikujushhih vrachej. – M.: Bionika. – 2002. – 368 s.

[5] Pozhiloj bolnoj / pod red. L.I.Dvoreckogo. – M.: Russkij Vrach, 2001. – 144 s.

[6] Rukovodstvo po gerontologii i geriatrii. V 4 t. T.3. Klinicheskaja geriatrija / pod red. V.N.Jarygina, A.S. Melenteva. – M.: GJeOTAR-Media, 2007. – 896 s.

[7] Klinicheskaja farmakologija: uchebnik / sost. N.V. Kuznecovoj. – M.: GJeOTAR-Media, 2013. – 272 s.

[8] Majskij V.V., Muratov V.V. Farmakologija s recepturoj. – M.: Medicina, 1986. – 448 c.

[9] Gosudarstvennaja Farmakopeja Rossijskoj Federacii XII. V 5 chastjah. Chast 2. – M.: Nauchnyj centr jekspertizy sredstv medicinskogo primenenija, 2008. – 704 s.

[10] Korkushko O.V. Klinicheskaja kardiologija v geriatrii. – M.: Medicina, 1980. – 288 s.

[11] Barro S., Marin R. Fuzzy Logic in Medicine // Springer series: Studies in fuzziness and soft computing. – 2001. – Vol. 83. – 310 p.

[12] Dev U., Sultana A., Saha D., Mitra N.K. Application of fuzzy logic in medical data interpretation // Bangladesh J. Sci. Ind. Res. – N. 49 (3). – 2014. – P. 137-146.

[13] Patel A., Gupta S.K., Rehman Q., Verma M.K. Application of fuzzy logic in biomedical iformatics // Journal of Emerging Trends in Computing and Information Sciences. – Vol. 4. – N. 1. – 2013. – P. 57-62.

[14] Spravochnik po klinicheskoj farmakologii i farmakoterapii / Pod red. Chekmana I.S., Peleshhuka A.P., Pjataka O.A. – Kiev: Zdorove, 1986. – 736 s.

[15] Karceva T.V., Derjagina L.P., Timofeeva E.P. Fizicheskoe razvitie detej i faktory, ego opredeljajushhie. Metody ocenki. Uchebno-metodicheskoe posobie dlja studentov medicinskih VUZov. – Novosibirsk: Gosudarstvennoe obrazovatelnoe uchrezhdenie vysshego professionalnogo obrazovanija Novosibirskij gosudarstvennyj medicinskij universitet federalnogo agentstva RF po zdravoohraneniju i socialnomu razvitiju. – 2008. – 17 s.

[16] Gusel V.A., Markova I.V. Spravochnik pediatra po klinicheskoj farmakologii. – L.: Medicina. – 1989. – S. 16-21.

УДК 004.056.5

Калимолдаев М.Н., Кабылханов А.Б., Магзом М.М.*, Нысанбаева С.Е.

Институт информационных и вычислительных технологий КН МОН РК,
Республика Казахстан, г. Алматы
* E-mail: magzomxzn@gmail.com

Построение модели режима для системы шифрования, разработанной на базе модулярной арифметики

В данной работе предлагается алгоритм криптографического преобразования для системы блочного симметричного шифрования, разработанной на базе непозиционной полиномиальной системы счисления (НПСС). Цель создания этой модели режима – повысить уровень статистической безопасности системы шифрования на базе НПСС. При создании алгоритма криптографического преобразования используется модель режима шифра. Эта модель режима разработана с применением сети Фейстеля и режима стандарта шифрования США. Использованный режим - это режим сцепления блоков по шифртексту для блочных алгоритмов шифрования (на языке оригинала: CBC - Cipher block chaining). Данный режим рекомендован НИСТ США (NIST - The National Institute of Standards and Technology). В связи с этим приведены краткие описания сети Фейстеля, режима сцепления блоков по шифртексту, блочного симметричного алгоритма шифрования на базе НПСС. Приведены полученные результаты проведенных исследований: изложена суть разработанной модели режима для системы шифрования на базе НПСС; приведена блок-схема предложенного алгоритма криптографического преобразования. Для указанных результатов будут проведены работы по анализу статистических свойств получаемых криптограмм с использованием графических и оценочных тестов.
Ключевые слова: криптографическая система, алгоритм шифрования, модулярная арифметика, сеть Фейстеля, режимы шифрования.

Kalmoldayev M.N., Kabylkhanov A.B., Magzom M.M., Nyssabayeva S.E.

Construction of the model of application mode for encryption system developed on the basis of modular arithmetic

In this work, we propose an algorithm for cryptographic transformation for the block symmetric encryption system, developed on the basis of nonpositional polynomial notation system (NPNs). The purpose of this mode model is to increase the level of statistical security of the encryption system based on NPNs. During the creation of the algorithm of cryptographic transformation, the model of the cipher mode is used. This mode model was developed using a Feistel network and the mode of US encryption standard. Used mode is the cipher block chaining mode for block encryption algorithms. This mode is recommended by NIST of USA. In this regard brief descriptions of the Feistel network, cipher block chaining mode and block symmetric encryption algorithm based on NPNs are provided. The results of the research is presented: outlined the essence of the developed mode model for the encryption system based on NPNs; a block diagram of the proposed algorithm of the cryptographic transformation is introduced. Work on the analysis of the statistical properties of the resulting cryptograms will be held for these results using graphical and assessment tests.
Key words: cryptosystems, encryption, block cipher, nonpositional polynomial notation, cryptostrength, Feistel network, cipher mode.

Калимолдаев М.Н., Кабылханов А.Б., Магзом М.М., Нысанбаева С.Е.

Модулярлы арифметика негізінде жасалған шифрлау жүйесіне арналған режим моделін құрастыру

Бұл жұмыста позициондық емес полиномиалдық санау жүйелері (ПЕПСЖ) негізінде іске асырылған симметриялық блоктық шифрлау жүйесі алгоритміне арналған криптографиялық түрлендіру алгоритмі ұсынылып отыр. Режим моделінің құрастыру мақсаты - ол ПЕПСЖ негізіндегі шифрлау жүйесінің статистикалық қауіпсіздігінің деңгейін арттыру. Криптографиялық түрлендіру алгоритмін жасау барысында шифрлау режим моделі қолданылады. Бұл режим моделі АҚШ шифрлау стандартының режимі мен Фейстел желісін қолдану арқылы іске асырылған. қолданылған режим - бұл блоктық шифрлау алгоритмдеріне арналған шифрмәтін бойынша блоктардың тұтасу режимі (түпнұсқа тілінде CBC - Cipher block chaining). Бұл режим АҚШ ҰИСТ (NIST - The National Institute of Standards and Technology) ұсынылған. Осыған байланысты: Фейстел желісі, шифртмәтін бойынша блоктардың тұтасу режимі мен ПЕПСЖ негізіндегі блоктық шифрлау жүйесі алгоритміне қысқаша сипаттаулар келтірілген. қарастырылған зерттеулерден алынған нәтижелері келтірілген: ПЕПСЖ негізіндегі шифрлау жүйесіне арналған режим моделін құрастыру негізі сипатталған; ұсынылған криптографиялық түрлендіру алгоритмінің блок-схемасы келтірілген. Көрсетілген нәтижелерге алынған криптограммалардың статистикалық қасиеттеріне бағалық және графикалық тесттер арқылы сынақтамалар өткізіледі.

Түйін сөздер:криптографическлық жүйе, шифрлау алгоритмі, модулярлы арифметика, Фейстель желісі, шифрлау режимдері.

1. Введение

Одним из основных примеров при разработке блочных алгоритмов криптографического преобразования является многократная, состоящая из нескольких циклов, обработка одного блока открытого текста. На каждом цикле данные подвергаются специальному преобразованию при участии вспомогательного ключа, полученного из заданного секретного ключа. Выбор числа циклов определяется требованием криптостойкости и эффективности реализации блочного шифра. Как правило, чем больше циклов, тем выше криптостойкость и ниже эффективность реализации (больше задержка при зашифровании/расшифровании) блочного шифра, и наоборот. Так, например, в случае алгоритма DES для того, чтобы все биты шифртекста зависели от всех битов ключа и всех битов открытого текста, необходимо пять циклов криптографического преобразования. DES с шестнадцатью циклами обладает более высокой криптостойкостью по отношению к ряду криптоаналитических атак [1].

Существуют разные виды построения блочных алгоритмов шифрования. Один из них строятся на основе схемы Фейстеля. К числу таких алгоритмов относятся бывший американский стандарт Data Encryption Standard (DES) и российский стандарт России - ГОСТ 28147-89 [2]. В 1971 г. Хорст Фейстель (Horst Feistel) запатентовал два устройства, реализовавшие различные алгоритмы шифрования, названные затем общим названием «Люцифер» (Lucifer) [3]. Одно из устройств использовало конструкцию, впоследствии названную «сетью Фейстеля» («Feistel cipher», «Feistel network»). Проект «Люцифер» был скорее экспериментальным, но стал базисом для алгоритма стандарта (DES). В 1977 г. DES стал стандартом США для шифрования данных.

В 2002 г. принят новый американский стандарт Advanced Encryption Standard (AES), который относят к нетрадиционным, поскольку при его разработке был использован алгебраический подход.

В данной работе описывается модель режима шифра, которая построена на совместном использовании режима работы стандарта DES «Режим сцепления блоков по шифртексту» и сети Фейстеля. Затем эта модель применяется к системе шифрования, разработанной на базе НПСС. Систему шифрования на базе НПСС можно отнести к системам со специально разработанными алгоритмами, т.е. к нетрадиционным, поскольку он разработан на основе алгебраического подхода с использованием полиномиальных систем счисления в остаточных классах. Нетрадиционные методы и алгоритмы криптографии, построенные на базе НПСС, позволяют существенно повысить надежность алгоритма шифрования. Криптостойкость в этом случае определяется полным ключом, зависящим не только от длины ключа (ключевой последовательности), но и от выбранной системы полиномиальных оснований, а также от количества перестановок оснований в системе. Синонимами НПСС являются системы счисления в остаточных классах с полиномиальными основаниями или модулярная арифметика [4-6].

Описание режима стандарта шифрования DES «Режим сцепления блоков по шифртексту» приводится на основании документа, изданного Американским Национальным Институтом Стандартов и Технологий (НИСТ).

Сеть Фейстеля имеет следующую структуру [3]. Алгоритм шифрования реализуется несколькими раундами (или итерациями). Преобразование в сети Фейстеля на каждом раунде осуществляется следующим образом. Шифруемый блок разбивается на два равные подблока - H_i (верхний, high) и L_i (нижний, low). К нижнему подблоку применяется функция шифрования f с использованием ключевого элемента k_i (части ключа или модификации части ключа). После этого выполняется сложение результата модификации нижнего подблока с верхним подблоком по модулю два. В результате шифруемым блоком для следующего раунда будет объединение подблоков, полученных по формулам

$$H_{(i+1)} = L_i, \tag{1}$$

$$L_{(i+1)} = H_{(i+1)} \oplus f(L_i, H_i). \tag{2}$$

Схема каждого раунда показана на рисунке 1.

Шифрование при помощи данной конструкции легко реализуется как на программном уровне, так и на аппаратном, что обеспечивает широкие возможности применения. На основе сетей Фейстеля разработано большое количество шифров, среди которых: DES, ГОСТ 28147-89, Blowfish, CAST, FEAL, IDEA, Khufu, Twofish и другие.

DES - федеральный стандарт шифрования США в 1977-2001 гг. [1] для использования во всех несекретных правительственных каналах связи (FIPS PUB 46 «Data Encryption Standard»). Несмотря на то, что в настоящий момент федеральным стандартом шифрования США является алгоритм Rijndael (AES - Advanced Encryption Standard), рассмотрение DES позволяет понять основные принципы блочного шифрования [7-8].

DES является классической сетью Фейстеля с двумя ветвями (подблоками). Данные шифруются 64-битными блоками, используя 56-битный ключ. Алгоритм преобразует за несколько раундов 64-битный вход в 64-битный выход. Длина ключа равна 56 битам. Первоначально ключ подается на вход функции перестановки. Затем для каждого из 16 раундов подключ K_i является комбинацией левого циклического сдвига и перестановки. Функция перестановки одна и та же для каждого раунда, но подключи K_i для каждого раунда получаются разные вследствие повторяющегося сдвига битов ключа [1].

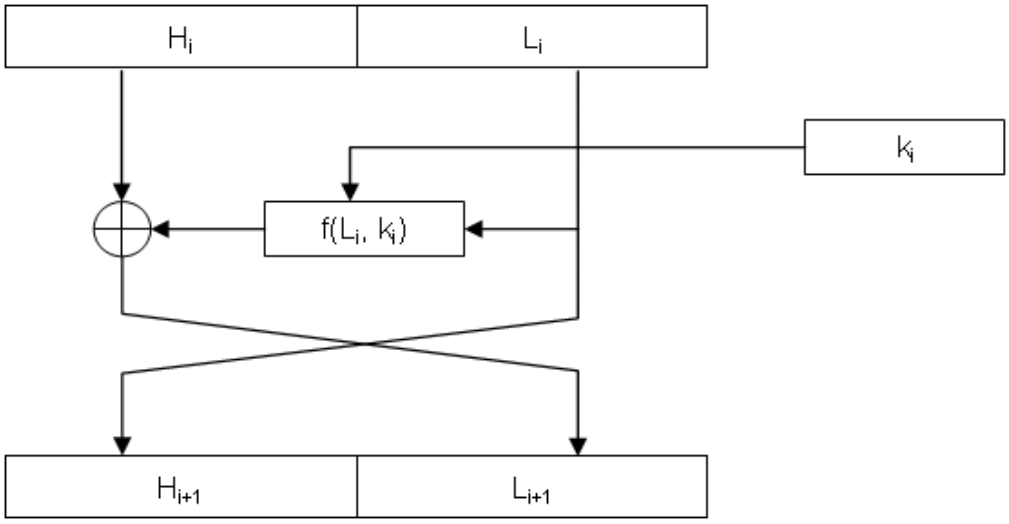

Рисунок 1 – Схема выполнения одного раунда в сети Фейстеля

2. Построение непозиционной полиномиальной системы счисления

Построение непозиционных полиномиальных систем счисления основано на использовании китайской теоремы об остатках, доказанной в I веке китайским математиком Сун Це. Свое развитие они начали после выхода в свет в 1955 году первых работ чешских исследователей - инженера М. Валаха и математика А. Свободы, которые предложили использовать систему остаточных классов для операций над компьютерными числами [9,10].

В 1955 году исследования в этой области были начаты также в СССР и получили широкое развитие благодаря трудам И.Я. Акушского, Д.И. Юдицкого, В.М. Амербаева [11]. Эта идея привлекла внимание ученых и в других странах. В результате возникло новое научное направление - модулярная арифметика. Одним из направлений развития модулярной арифметики являются работы Р.Г. Бияшева по созданию, анализу и использованию НПСС для разработки самокорректирующихся кодов, применяемых для обнаружения и исправления ошибок [6]. Им были обоснованы основные положения алгебры НПСС, которые использованы при разработке симметричной блочной системы шифрования.

2. Модель нетрадиционного алгоритма шифрования

Суть нетрадиционного алгоритма шифрования электронного сообщения заданной длины N состоит в следующем.

Вначале формируется НПСС. Пусть основаниями НПСС выбраны неприводимые многочлены с двоичными коэффициентами

$$p_1(x), p_2(x), ..., p_S(x). \tag{3}$$

степени $m_1(x), m_2(x), ..., m_s(x)$ соответственно. С учетом всех возможных их перестановок (расположений) эти полиномы образуют систему оснований НПСС. Основания

(3) задают основной (рабочий) диапазон НПСС, который определяется многочленом $P(x) = p_1(x)p_2(x)\cdots p_S(x)$ степени $m = \sum_{i=1}^{s} m_i$. В данной системе оснований любой многочлен, степень которого меньше m, имеет единственное представление в виде его остатков (вычетов) по модулям рабочих оснований $p_1(x), p_2(x), ..., p_S(x)$ соответственно.

Тогда сообщение длины N бит можно интерпретировать как последовательность остатков $\alpha_1(x), \alpha_2(x), ..., \alpha_S(x)$ от деления некоторого многочлена $F(x)$ на основания $p_1(x), p_2(x), ..., p_S(x)$ соответственно:

$$F(x) = (\alpha_1(x), \alpha_2(x), ..., \alpha_S(x)), \tag{4}$$

где $F(x) \equiv \alpha_i(x)(mod\ p_i(x)), i = \overline{1,\mathrm{S}}$. Запись $F(x)$ в виде (4) - это позиционное представления многочлена $F(x)$.

В выражении (4) остатки $\alpha_1(x), \alpha_2(x), ..., \alpha_S(x)$ выбираются таким образом, что первым l_1 битам сообщения ставятся в соответствие двоичные коэффициенты остатка $\alpha_1(x)$, следующим l_2 битам - двоичные коэффициенты остатка $\alpha_2(x)$ и так далее, последним l_s двоичным разрядам ставятся в соответствие двоичные коэффициенты вычета $\alpha_S(x)$.

Восстановление позиционного представления $F(x)$ производится по его непозиционному виду (4). В случае хранения, передачи и обработки информации оно осуществляется по следующей формуле:

$$F(x) = \sum_{i=1}^{S} \alpha_i(x)B_i(x), B_i(x) = \frac{\prod_{i=1}^{S} p_i(x)}{p_i(x)} M_i(x) \equiv 1(mod p_i(x)), \tag{5}$$

где $i = \overline{1,\mathrm{S}}$ и значения многочленов $M_i(x)$ выбираются для выполнения указанного в формуле сравнения.

Затем производится генерация ключевой (псевдослучайной) последовательности. Используемая ключевая последовательность длины N бит также интерпретируется как последовательность остатков $\beta_1(x), \beta_2(x), ..., \beta_S(x)$, но от деления некоторого другого многочлена $G(x)$ по тем же рабочим основаниям системы:

$$G(x) = (\beta_1(x), \beta_2(x), ..., \beta_S(x)), \tag{6}$$

где $G(x) \equiv \beta_i(x)(mod\ p_i(x)), i = \overline{1,\mathrm{S}}$.

Тогда в качестве криптограммы (шифртекста) $\omega_1(x), \omega_2(x), ..., \omega_S(x)$ может рассматриваться некоторая функция $H(F(x), G(x))$:

$$H(x) = (\omega_1(x), \omega_2(x), ..., \omega_S(x)), \tag{7}$$

где $H(x) \equiv \omega_i(x)(mod\ p_i(x)), i = \overline{1,\mathrm{S}}$.

В соответствии с операциями непозиционной системы счисления операции в функциях $F(x), G(x), H(x)$ могут выполняться параллельно по модулям полиномов $p_1(x), p_2(x), ..., p_s(x)$, выбранных в качестве оснований НПСС.

Секретность нетрадиционного шифрования сообщения заданной длины N определяется не только многочленом (ключом) $G(x)$, но конкретным набором оснований, выбранных из всего множества неприводимых многочленов степени не выше N. Эти секретные составляющие (3) и (7) назвали полным секретным ключом.

Конкретная система оснований НПСС находится он следующим образом.

Пусть n_1 - число неприводимых многочленов с двоичными коэффициентами степени m_1. Тогда полные системы вычетов по модулям этих многочленов содержат все многочлены с двоичными коэффициентами степени не выше $m_1 - 1$, для записи которых используется m_1 бит. Пусть соответственно n_2 - число неприводимых многочленов с двоичными коэффициентами степени m_2, n_3 - число неприводимых многочленов с двоичными коэффициентами степени m_3 и т.д., n_S - число неприводимых многочленов степени m_S. При $S = N$ (степень оснований равна значению N) для записи полных систем вычетов по модулям этих оснований необходимо N бит.

Тогда процедура выбора всех систем рабочих оснований степени от m_1 до m_S сводится к нахождению всевозможных решений алгебраического уравнения

$$k_1 m_1 + k_2 m_2 + ... + k_S m_S = N \tag{8}$$

где $0 \le k_i \le n_i$ - неизвестные коэффициенты, один конкретный набор которых является одним из решений (8) и задает одну систему рабочих оснований; n_i - количество всех неприводимых многочленов степени m_i, $1 \le m_i \le N$, k_i- число выбранных неприводимых многочленов степени m_i, $S = k_1 + k_2 + .. + k_s$ - число выбранных оснований. Уравнение (5) определяет то количество S оснований, вычеты по которым покрывают длину N заданного сообщения. Полные системы вычетов по модулям многочленов степени m_i включают в себя все полиномы степени не выше $m_i - 1$, поэтому для их записи потребуется m_i бит. Выбираются же эти S оснований из общего количества всех неприводимых многочленов различных степеней, но не выше N. Все выбираемые основания должны отличаться друг от друга, даже если они являются неприводимыми полиномами одной степени, поскольку теория НПСС построена на выполнении китайской теоремы об остатках.

3. Моделирование режима шифрования

При шифровании исходного текста произвольной длины блочные шифры используются в различных криптографических режимах. Криптографический режим определяет подробности реализации алгоритма шифрования для различных применений и является методом использования блочного алгоритма шифрования, позволяющий преобразовать последовательность блоков в открытых данных в последовательность блоков зашифрованных данных [12-15].

В 1980 г. в США был принят также стандарт, который определил режимы работы алгоритма DES. Этот стандарт уточнял подробности реализации DES для различных применений (или применения DES в различных приложениях) [1]. Эти режимы обеспечивают требуемые свойства блочных шифрованных текстов, такие как контроль за распространением ошибок, случайность - должна быть скрыта структура открытого текста.

В режиме шифрования CBC (Cipher Block Chaining) происходит «сцепливание» всех блоков сообщения по шифртексту (рисунок 2). При зашифровании первого блока исходного текста в этом «Режиме сцепления блоков по шифртексту» используется специальный входной блок - «вектор инициализации». Вектор инициализации должен быть случайным и в каждом сеансе шифрования быть новой. В процессе шифрования тогда все блоки открытого текста оказываются связанными, а входные данные, поступающие на вход функции шифрования, уже зависят не только от текущего блока шифруемого открытого текста. По этой причине повторяющиеся блоки последовательности в шифрованном тексте не встречаются, а одно и тоже открытое сообщение в разных сеансах шифрования будет переходить в разные шифртексты. При расшифровании если внести искажения в зашифрованный блок, то после расшифрования искаженными окажутся два блока открытых данных - соответствующий и следующий за ним, причем искажения в первом случае будут носить тот же характер, что и в режиме гаммирования, а во втором случае - как в режиме простой замены.

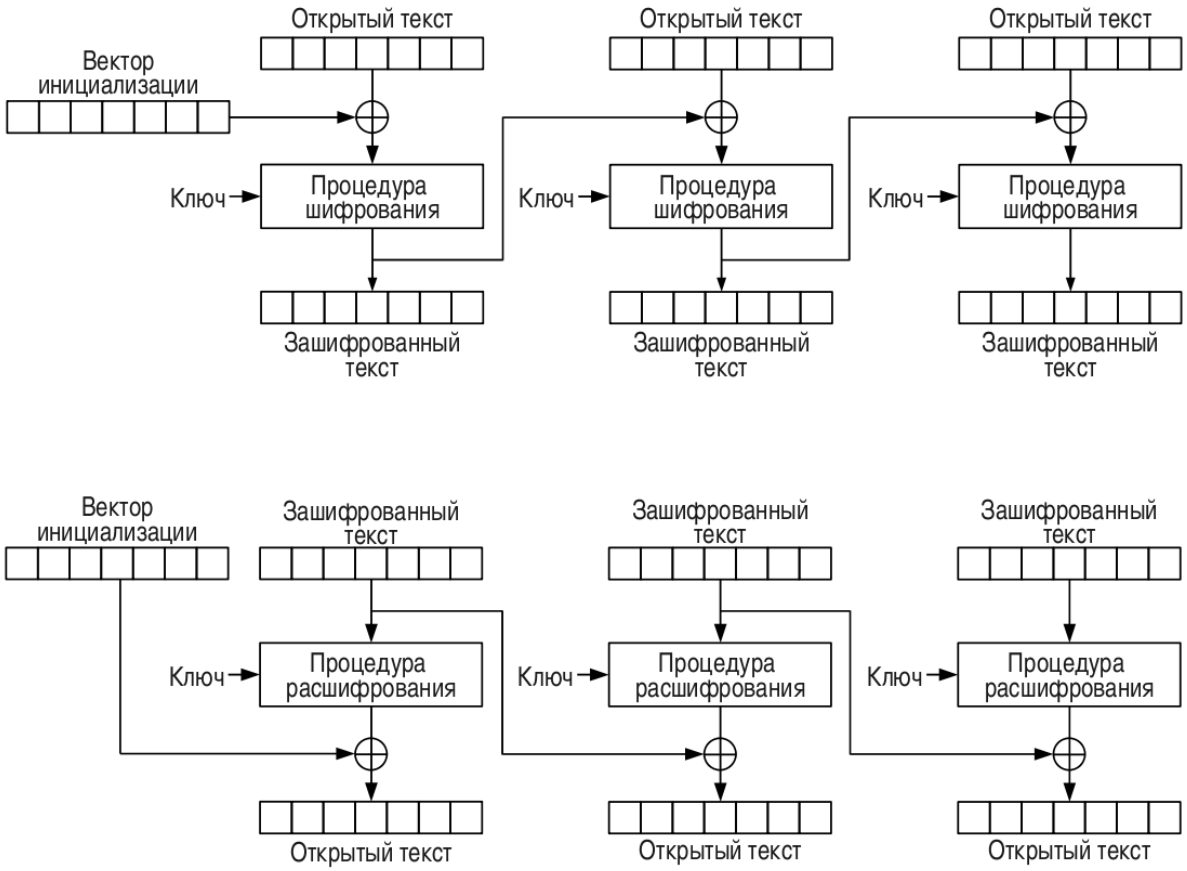

Рисунок 2 – Режим сцепления блоков по шифртексту: а) алгоритм зашифрования, б) алгоритм расшифрования

Как видно из рисунка в алгоритме шифрования на вход функции шифрования $CIPH_K$ (на рисунке 2,а – Процедура шифрования) каждый раз подаётся результат суммиро-

вания по модулю 2 открытых данных очередного блока сообщения и выходных данных функции $CIPH_K$ для предыдущего блока. Поскольку выходные данные функции $CIPH_K$ для очередного блока идут прямо на выход алгоритма CBC, то есть являются шифртекстом этого блока и одновременно поступают на вход этой же функции для зашифрования последующего блока, то происходит сцепление блоков по шифртексту. Первый блок открытых данных суммируется с вектором инициализации (9). Этот вектор инициализации становится известен как отправителю, так и получателю в самом начале сеанса связи (поэтому зачастую его называют просто синхропосылкой). Расшифрование происходит (12), соответственно, в обратном порядке - сначала к шифртексту применяют функцию расшифрования $CIPH_K^{-1}$ (на рисунке 2,б – Процедура расшифрования), а затем суммируют с предыдущим блоком шифртекста для получения на выходе алгоритма очередного блока открытого текста. Первый блок открытого текста, опять же, восстанавливается с помощью вектора инициализации(11).

Таким образом весь алгоритм может быть выражен в виде уравнений следующим образом:

$$C_1 = CIPH_K(P_1 \oplus IV) \tag{9}$$

$$C_j = CIPH_K(P_j \oplus C_j) \tag{10}$$

$$P_K = CIPH_K^{-1}(C_1) \oplus IV \tag{11}$$

$$P_K = CIPH_K^{-1}(C_1) \oplus C_{j-1} \tag{12}$$

В уравнениях приняты следующие обозначения:

IV - вектор инициализации;

P_j - очередной, j -ый блок открытого текста;

C_j - очередной, j -ый блок шифртекста.

В режиме CBC при зашифровании каждая итерация алгоритма зависит от результата предыдущей итерации, то зашифрование сообщения не поддаётся расспараллеливанию. Однако в режиме расшифрования, когда весь шифртекст уже получен, функции $CIPH_K^{-1}$ вполне можно исполнять параллельно и независимо для всех блоков сообщения. Это даёт значительный выигрыш по времени. В этом режиме стоит остановиться ещё на одной детали. Дело в том, что последний блок шифртекста, который получается на выходе алгоритма режима CBC зависит как от ключа блочного шифра и вектора инициализации.

Поскольку алгоритм шифрования представляет собой множество обратимых преобразований электронного сообщения с целью его защиты от несанкционированного прочтения. Переход от открытого текста к шифртексту называется зашифрованием, а обратный переход - расшифрованием или дешифрованием [4]. Необходимым условием выполнения прямого, так и обратного криптографического преобразования является наличие секретного ключа. В связи с этим был предложен алгоритм криптографического преобразования, суть которого состоит в применении разработанной модели режима шифра к алгоритму шифрования на базе НПСС (рисунок 3).

Сообщение разбивается на блоки одинакового размера из n бит. При необходимости последний блок дополняется до длины n.

Для шифрования одного блока открытого сообщения P выполняются следующие действия.

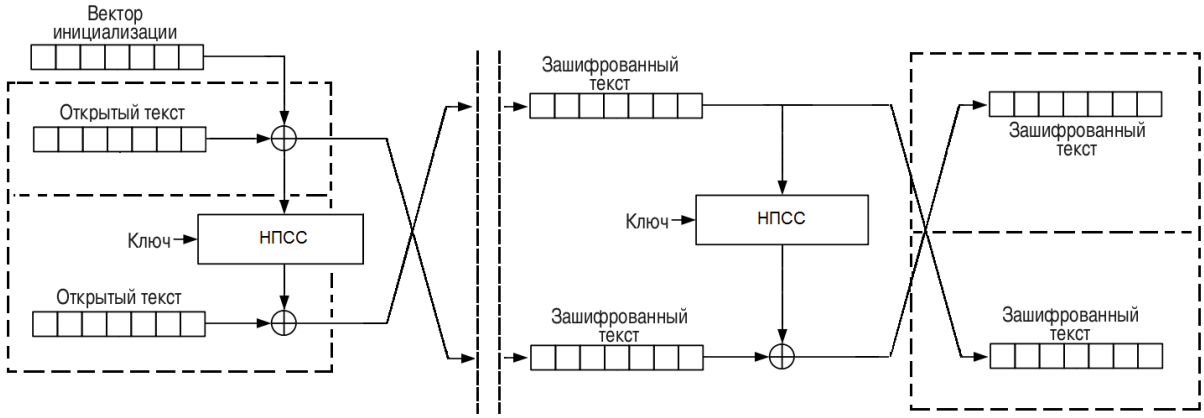

Рисунок 3 – Модель криптографического преобразования одного блока, полученная при комбинировании режима стандарта шифрования США «Режим сцепление блоков по шифртексту» и сети Фейстеля для алгоритма шифрования на базе НПСС

1. Выбранный блок делится на два подблока одинакового размера - «верхний» (U_0) и «нижний» (D_0); 2. Для «верхнего подблока» (U_0) производится сложение по модулю с «вектором инициализации» (IV). Вектор инициализации – псевдослучайная последовательность, размер (длина) (IV) равна размеру блока ($n/2$). «Верхний подблок» (U_0) изменяется функцией шифрования E_k с использованием ключа k.

$$x = E_k(U_0, k). \tag{13}$$

3. Результат складывается по модулю 2 («$\oplus$», «xor») с «нижним подблоком» (D_0):

$$x = x \oplus D_0 \tag{14}$$

4. Результат будет использован в следущем раунде в роли «верхнего подблока» (U_1):

$$U_1 = x. \tag{15}$$

5. «Верхний подблок» (U_0) текущего раунда будет использован в следующем раунде в роли «нижнего подблока» (D_1):

$$D_1 = U_0. \tag{16}$$

Здесь использованы следующие обозначения:

i - номер блока;

k - ключ;

IV - вектор инициализации (синхропосылка);

U_0 - верхний подблок сообщения (открытый текст);

D_0 - нижний подблок сообщения (открытый текст);

x - зашифрованный блок (шифртекст), полученный на предыдущем шаге шифрования;

E_k - функция, выполняющая блочное шифрование.

Перечисленные операции выполняются $N-1$ раз, где N - количество раундов в выбранном алгоритме шифрования.

4. Заключение

Цель полученной модели режима – улучшение статистических характеристик системы шифрования, разработанной на базе непозиционных полиномиальных систем счисления. В связи с этим планируется следующие работы:

- программная реализация предложенного алгоритма криптографического преобразования;

- анализ статистических свойств получаемых криптограмм с использованием графических и оценочных тестов.

Работа выполнена при поддержке программно-целевого финансирования научно-технических программ и проектов Комитетом науки МОН РК №0128/ПЦФ.

Литература

[1] FIPS 46-3. Data Encryption Standard (DES). – 1977. – 27 p.

[2] ГОСТ 28147-89. Система обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. – 1989. – 28 с.

[3] Feistel H. Cryptography and Computer Privacy // Scientific American – 1973. – pp. 15-23

[4] Акушский И.Я., Юдицкий Д.И. Машинная арифметика в остаточных классах. – 1968. – 439 с.

[5] Бияшев Р.Г Разработка и исследование методов сквозного повышения достоверности в системах обмена данными распределенных АСУ. – 1985. – 328 с.

[6] Нысанбаева С. Е. Разработка и исследование криптографических систем на базе непозиционных полиномиальных систем счисления. – 2009. – 240 с.

[7] FIPS PUB 197. Advanced Encryption Standard (AES). – 2002. – 51 p.

[8] FIPS 46-3. Data Encryption Standard (DES). – 1977. – 27 p.

[9] Cvoboda A., Valach M. Operatorve obvody // Stroje na Zpracovani Informaci – 1955. – 122 p.

[10] Свобода А. Развитие вычислительной техники в Чехословакии. Системы счисления в остаточных классах. // Кибернетический сб. – 1963. – с. 115-149

[11] Амербаев В.М., Бияшев Р.Г. Интерполяция и коды, исправляющие ошибки // Теория кодирования и информационное моделирование. – 197. – с. 51-64

[12] Recommendation for Block Cipher Modes of Operation // Recommendation for Block Cipher Modes of Operation. – 2001. – 10 p.

[13] Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тесты на языке Си. – 2003. – 816 с.

[14] Фороузан Б.А. Криптография и безопасность сетей: Учебное пособие. – 2010. – 784 с.

[15] Панасенко С.В. Алгоритмы шифрования. Специальный справочник. – 2013. – 576 с.

References

[1] FIPS 46-3. Data Encryption Standard (DES). – 1977. – 27 p.

[2] GOST 28147-89. Sistema obrabotki informacii. Zashita kriptogaficheskaya. Algoritm kriptogaficheskogo preobrazovanya. – 1989. – 28 p.

[3] Feistel H. Cryptography and Computer Privacy // Scientific American – 1973. – pp. 15-23

[4] Akushski I.Ya., Yidickii D.I. Mashinnaya arifmetika v ostatochnih klassah. – 1968. – 439 p.

[5] Biyashev R.G Razrabotka i issledovanie metodov skvoznogo povisheniya dostovernosti v sistemah obmena dannimi raspredelennih ASY. – 1985. – 328 p.

[6] Nisanbayeva S. E. Razrabotka i issledovanie kriptograficheskih sistem na baze nepozicionnih polinomialnih sistem schisleniya. – 2009. – 240 p.

[7] FIPS PUB 197. Advanced Encryption Standard (AES). – 2002. – 51 p.

[8] FIPS 46-3. Data Encryption Standard (DES). – 1977. – 27 p.

[9] Cvoboda A., Valach M. Operatorve obvody // Stroje na Zpracovani Informaci – 1955. – 122 p.

[10] Svoboda A. Razvitie vichislitelnoi tehniki v Chehoslovakii. Sistemi schisleniya v ostatochnih klassah. // Kiberneticheski sb. – 1963. – p. 115-149

[11] Amerbayev V.M., Biyashev R.G. Interpolyaciya i kodi, ispravlyauchie oshibki // Teoriya kodirovaniya i informacionnoe modelirovanie. – 197. – p. 51-64

[12] Recommendation for Block Cipher Modes of Operation // Recommendation for Block Cipher Modes of Operation. – 2001. – 10 p.

[13] Shnaier B. Prikladnaya kriptografiya. Protokoli, algoritmi, ishodnie testi na yazike Si. – 2003. – 816 p.

[14] Foroyzan B.A. Kriptografiya i bezopasnost setei: Ychebnoe posobie. – 2010. – 784 p.

[15] Panasenko S.V. Algoritmi shifrovaniya. Specialni spravochnik. – 2013. – 576 p.

УДК 004.056.5

Капалова Н.А.*, Дюсенбаев Д.С.

Институт информационных и вычислительных технологий КН МОН РК,
Республика Казахстан, г. Алматы
* E-mail: kapalova@ipic.kz

Криптоанализ алгоритма шифрования на базе непозиционных полиномиальных систем счисления

Создание общей теории обоснования стойкости блочных шифров является одной из центральных проблем современной симметричной криптографии. Существуют различные методы их криптоанализа и появляются новые перспективные направления в этой области. Они в основном остаются полуэвристическими, к их числу относятся классические методы дифференциального и линейного криптоанализа, а также их многочисленные обобщения. Эти методы долгое время основывались на статистических подходах криптоанализа, например как линейный и дифференциальный. Для осуществления такой атаки требуется большое количество открытых текстов и шифротекстов. Кроме того, современные алгоритмы шифрования разрабатывались с учетом обеспечения стойкости к подобного рода атакам. Актуальность алгебраических методов криптоанализа базируется на возможности взлома с их помощью алгоритмов шифрования при наличии у криптоаналитика всего одной пары открытый текст/шифротекст. Данные методы применимы и к стойким современным шифрам. Алгебраические атаки используют внутреннюю структуру шифра, то есть для получения ключа шифрования необходимо представить преобразования шифрования в виде системы многомерных многочленных уравнений и решить данную систему. В данной работе оценивается алгоритм шифрования, разработанный с использованием непозиционных полиномиальных систем счисления (НПСС), с точки зрения его криптостойкости. Для этого строится математический модель алгебраического криптоанализа. В процессе криптоанализа вначале получают систему нелинейных уравнений из функции преобразования открытого текста в шифртекст с помощью ключа. Далее рассматривается возможность перехода от этой нелинейной системы к линейной.

Ключевые слова: криптография, шифрование, непозиционная полиномиальная система счисления, криптостойкость, система остаточных классов, криптоанализ.

Kapalova N.A., Dyusenbayev D.S.

Cryptanalysis of the encryption algorithm based on nonpositional polynomial notation systems

Creation of a general theory of resistance justification of block ciphers is one of the central problems of modern symmetric cryptography. There are various methods of cryptanalysis, and there are promising new directions in this field. They remain largely semi-heuristic, they include the classical methods of differential and linear cryptanalysis, as well as their numerous generalizations. These methods have based for a long time on statistical approaches of cryptanalysis, such as linear and differential. In order to carry out such an attack it requires large amount of plaintexts and ciphertexts. In addition, advanced encryption algorithms have been developed with a view to ensuring resistance to such attacks.

The relevance of the algebraic methods of cryptanalysis is based on the possibility of breaking with their encryption algorithms if a cryptanalyst has just one pair of plaintext / ciphertext. These methods are applicable to persistent modern ciphers. Algebraic attacks use the internal structure of the cipher, that is to obtain the encryption key a one must present the encryption transformation in the form of a system of multivariate polynomial equations and solve this system. In this paper we evaluated the encryption algorithm, developed using nonpositional polynomial notation systems (NPSS), in terms of the reliability. To do this, we construct a mathematical model of an algebraic cryptanalysis. In the process of cryptanalysis, first we prepare a system of nonlinear equations of the transformation functions of plaintext into ciphertext using a key. Next, we consider the possibility of moving from this nonlinear system to linear.
Key words: cryptography, encryption, nonpositional polynominal notations, cryptostrength, residue, cryptanalysis.

Капалова Н.А., Дюсенбаев Д.С.

Позициондық емес полиномиалдық санау жүйелер негізінде жасалған шифрлау алгоритміне криптоталдау жасау

Заманауи симметриялық криптографияның негізгі мәселелерінің бірі болып блоктық шифрлардың беріктілігін негіздейтін жалпы теорияны құру саналады. Түрлі криптоталдау әдістері бар және де осы салада болашағы бар бағыттар пайда болуда. Көп жағдайда олар жартылай эвристикалық болады, олардың қатарына классикалық дифференциалды және сызықтық криптоталдау әдістер және де олардың көптеген түрлендірулері жатады. Ұзақ уақыт бойы бұл әдістер статистикалық криптоталдау тәсілдеріне негізеліп келді, мысалы сызықтық және дифференциалдық. Бұндай шабулдарды жүзеге асыру үшін көп мөлшерде ашық мәтін мен шифрмәтін талап етіледі.Сонымен қатар, заманауи шифрлау алгоритмдері осы тәріздес шабулдарға беріктікті қамтамасыз ететіндей етіп құрылады. Криптоталдаудың алгебралық әдісінің өзектілігі, оның көмегімен шифрлеу алгоритмін криптоталдаушының қолында ашық мәтін мен шифрмәтіннің тек бір ғана жұбы болған жағдайда бұзу мүмкіндігіне негізделген. Бұл әдіс заманауи берік шифрларға да қолданылады. Алгебралық шабуылдар шифрдың ішкі құрлымын қолданады, яғни шифрлеу кілтін алу үшін шифр өзгертулерді көпмүшелі көпмөлшерлі теңдеулер түріне келтіру және ол жүйені шешу. Бұл жұмыста позициялы емес полиномды санау жүйесін қолдана отырып құрылған шифрлау алгортмі критпотұрақтылығы жағынан бағаланған. Ол үшін алгебралық криптоталдаудың математикалық моделі құрылды. Криптоталдау барысында бірінші кілттің көмегімен ашық мәтінді шифрмәтінге бейнелеу функциясынан сызықты емес теңдеулер жүйесін аламыз. Содан соң осы сызықты емес жүйеден сызықты жүйеге өту мүмкіндітері қарастырылады.
Түйін сөздер: криптография, шифрлау, позициондық емес полиномиалдық санау жүйелері, криптотұрақтылық, криптоталдау.

1. Введение

Алгоритмы и методы, созданные на базе непозиционных полиномиальных систем счисления (НПСС), называют также нетрадиционными [1]. В классической системе счисления в остаточных классах (СОК) в качестве системы оснований выбираются положительные целые числа, и в ней целое положительное число представляется своими остатками (вычетами) от деления на эту систему оснований [2]. Построение СОК основано на использовании китайской теоремы об остатках. В соответствии с этой теоремой представление числа в виде последовательности вычетов является единственным, если основания будут попарно просты между собой. В отличие от классических СОК в НПСС основаниями служат неприводимые многочлены над полем GF(2), то есть многочлены с двоичными коэффициентами [3-4].

На базе НПСС разработаны нетрадиционные алгоритмы шифрования, формирования цифровой подписи и обмена криптографическими ключами [3,5]. Данная статья

посвящена исследованию надежности нетрадиционного алгоритма шифрования методами криптоанализа.

Суть исследуемого алгоритма шифрования состоит в следующем.

1. Вначале производится формирование НПСС. Для этого в качестве ее рабочих оснований выбираются неприводимые многочлены

$$p_1(x), p_2(x), ..., p_S(x) \tag{1}$$

над полем GF(2) степеней $m_1, m_2, ..., m_S$ соответственно. Полиномы (1) с учетом порядка их расположения образуют одну систему оснований. Все основания (1) должны быть различными и в том случае, если они имеют одинаковую степень. Рабочий диапазон НПСС определяется многочленом (модулем)

$$P(x) = p_1(x)p_2(x) \cdots p_S(x)$$

степени $m = \sum_{i=1}^{s} m_i$. Тогда сообщение длины N бит можно интерпретировать как последовательность остатков $\alpha_1(x), \alpha_2(x), ..., \alpha_S(x)$ от деления некоторого многочлена $F(x)$ на основания $p_1(x), p_2(x), ..., p_S(x)$ соответственно:

$$F(x) = (\alpha_1(x), \alpha_2(x), ..., \alpha_S(x)). \tag{2}$$

2. Для шифрования используется ключевая последовательность длины N бит, которая также интерпретируется как последовательность остатков $\beta_1(x), \beta_2(x), ..., \beta_S(x)$, но от деления некоторого другого многочлена $G(x)$ по тем же рабочим основаниям системы:

$$G(x) = (\beta_1(x), \beta_2(x), ..., \beta_S(x)), \tag{3}$$

где $G(x) \equiv \beta_i(x)(mod\ p_i(x)), i = \overline{1, \mathrm{S}}$.

3. Для получения криптограммы $H(x) = (\omega_1(x), \omega_2(x), ..., \omega_S(x))$, используется операция умножения многочленов (2) и (3). При этом элементы последовательности вычетов $\omega_1(x), \omega_2(x), ..., \omega_S(x)$ являются остатками от деления произведений $\alpha_i(x)\beta_i(x)$ на соответствующие основания $p_i(x)$:

$$\alpha_i(x)\beta_i(x) \equiv\ \omega_i(x)(mod\ p_i(x)), i = \overline{1, s}. \tag{4}$$

В двоичном виде шифртекст $H(x)$ представляет собой последовательность коэффициентов многочленов $\omega_1(x), \omega_2(x), \ldots, \omega_S(x)$.

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:

$$\beta_i \cdot \beta_i^{-1}(x) \equiv 1(mod\ p_i(x)), i = \overline{1, s}. \tag{5}$$

В результате получается многочлен $G^{-1}(x) = ((\beta_1^{-1}(x), \beta_2^{-1}(x), ..., \beta_S^{-1}(x))$, инверсный к многочлену $G(x)$. Тогда исходное сообщение в соответствии с (4) и (5) восстанавливается через вычеты по следующим сравнениям:

$$\alpha_i(x) \equiv \beta_i^{-1}(x)\omega_i(x)(mod\ (p_i(x)), i = \overline{1, S}. \tag{6}$$

Таким образом, в рассмотренной модели алгоритма шифрования сообщения заданной длины N бит в НПСС полным ключом является выбранная система полиномиальных оснований $p_1(x), p_2(x), ..., p_S(x)$, полученный при генерации псевдослучайных последовательности ключ $G(x) = (\beta_1(x), \beta_2(x), ..., \beta_S(x))$ и инверсный к нему ключ $G^{-1}(x) = ((\beta_1^{-1}(x), \beta_2^{-1}(x), ..., \beta_S^{-1}(x))$, который вычисляется в соответствии с выражением (5).

Для оценки надежности была получена формула криптостойкости из расчета всевозможных вариантов подбора секретных параметров алгоритма. Криптостойкость алгоритма шифрования на базе НПСС определяется количеством всех возможных и отличающихся друг от друга вариантов выбора полных ключей, т.е. их секретностью. Криптостойкость шифрования сообщения заданной длины N бит находится из формулы [6]:

$$Q_{kr} = 2^N \sum_{k_1,k_2,...,k_s} (k_1 + k_2 + ... + k_s)! C_{n_1}^{k_1} C_{n_2}^{k_2} ... C_{n_S}^{k_S}. \tag{7}$$

В случае, когда криптоаналитику известны алгоритм шифрования и хотя бы одна пара открытый – зашифрованный текст, тогда естественным способом анализа является последовательное апробирование всех возможных вариантов выбора ключа. Апробирование производят до тех пор, пока зашифрование открытого текста на очередном ключе не приведет к совпадению имеющегося шифртекста. По формуле (7) определяется максимально возможное количество вариантов перебора секретного ключа. Такой способ анализа получил разные названия: метод полного перебора [6], метод грубой силы [7], метод атаки в лоб [8-9].

В данной статье излагаются результаты некоторых криптографических атак на эту модель алгоритма шифрования.

2. Некоторые методы криптоатак

Криптоанализ связан с такими характеристиками криптосистем, как оценка надежности шифров и разработка способов их вскрытия. Анализ надежности должен проводиться из предположения, что криптоаналитик имеет всю информацию об используемом криптоалгоритме, кроме использованного ключа (принцип Керкгоффса). Стойкость криптосистемы зависит от сложности алгоритмов преобразования, от объема ключевого пространства и метода ее реализации (защита от закладок, вирусов и т. п). Хотя понятие стойкости шифра является центральным в криптографии, количественная оценка криптостойкости в общем виде – проблема до сих пор нерешенная. Наиболее общими являются следующие подходы к оценке качества криптоалгоритмов, используемые на практике [6]:

1. всевозможные попытки их вскрытия;

2. анализ сложности алгоритма дешифрования;

3. оценка статистической безопасности шифра.

В первом случае многое зависит от квалификации, опыта, интуиции криптоаналитика и от правильной оценки возможностей создателей алгоритма шифрования. Обычно считается, что криптоаналитик знает шифр, имеет возможность его изучения, знает некоторые характеристики открытых защищаемых данных, например тематику сообщений, их стиль, стандарты, форматы и т.п.

Во втором случае оценку стойкости шифра заменяют оценкой минимальной сложности алгоритма его вскрытия. Однако получить строго доказуемые оценки нижней границы сложности алгоритмов рассматриваемого типа не представляется возможным. Сложность вычислительных алгоритмов можно оценивать числом выполняемых элементарных операций, при этом, естественно, необходимо учитывать их стоимость и затраты на их выполнение. В общем случае это число должно иметь строгую нижнюю оценку и выходить за пределы возможностей современных компьютерных систем.

В третьем случае криптосистема с точки зрения криптоаналитика является "черным ящиком". Криптосистема считается надежной, если входная и выходная информационные последовательности взаимно независимы и при этом выходная зашифрованная последовательность является псевдослучайной.

Для криптоанализа используются также следующие методы:

- атака на основе шифртекста;
- атака на основе открытых текстов и соответствующих шифртекстов;
- атака на основе подобранного открытого текста (возможность выбрать текст для шифрования);
- атака на основе адаптивно подобранного открытого текста.

Цель атаки на основе шифртекста – нахождение как можно большего числа открытых текстов, соответствующих имеющимся шифртекстам, или нахождение используемого при шифровании ключа. Но данный вид атаки является самым слабым и неудобным.

При выполнении атаки на основе открытых текстов и соответствующих шифртекстов существует два варианта подстановки задачи: 1) найти ключ, использованный для преобразования открытого текста в шифртекст, 2) создать алгоритм, способный дешифровать любое сообщение, зашифрованное с помощью этого ключа. Получение открытых текстов играет решающую роль в осуществлении этой атаки. Открытые тексты извлекают из самых различных источников. Данная атака сильнее атаки на основе одного лишь шифртекста.

Основным отличием атаки на основе подобранного открытого текста от предыдущей атаки является возможность предварительного выбора некоторого количества открытых текстов и их шифрование на искомом ключе. За счет этого такая атака является более мощной.

Атака на основе адаптивно подобранного открытого текста применима в тех случаях, когда криптоаналитик имеет доступ к шифрующему устройству. Также данная атака широко используется для попыток взлома криптографических систем с открытым

ключом. При этой атаке часто используются методы дифференциального и линейного криптоанализа.

Как линейный, так и дифференциальный криптоанализ долгое время основывались на статистических подходах. Как отмечено выше, для осуществления атаки требуется большое количество открытых текстов и шифртекстов. Кроме того, современные алгоритмы шифрования разрабатывались с учетом обеспечения стойкости к подобного рода атакам.

Актуальность алгебраических методов криптоанализа базируется на возможности взлома с их помощью алгоритмов шифрования при наличии у криптоаналитика всего одной пары открытый текст - шифртекст. Также важно отметить, что данные методы применимы к стойким современным шифрам. Алгебраические атаки используют внутреннюю структуру шифра, то есть для получения ключа шифрования необходимо представить преобразования шифрования в виде системы многомерных многочленных уравнений и впоследствии решить данную систему [7].

3. Криптоанализ алгоритма шифрования на базе НПСС

При проведении криптоанализа считаем, что алгоритм шифрования известен. Рассмотрим два подхода. Криптоаналитику нужно определить:

- или открытый текст и ключ по зашифрованному тексту;
- или секретный ключ по паре «открытый текст – зашифрованный текст».

Прежде чем провести алгебраический криптоанализ алгоритма шифрования в НПСС, строится система уравнений с учетом закономерностей выполнения операции умножения (4) в кольце. Эта система связывает ключ, открытые и шифрованные тексты.

4. Алгебраический криптоанализ алгоритма шифрования на базе НПСС

Сначала рассмотрим процесс зашифрования только для одного неприводимого многочлена. Пусть выражение

$$\alpha(x)\beta(x) \equiv \omega(x)(mod\ p(x)) \tag{8}$$

описывает метод шифрования на базе НПСС.

Распишем используемые полиномы.

$\alpha(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + ... + a_2x^2 + a_1x + a_0$ – многочлен, в котором коэффициентами являются битовые последовательности открытого текста.

$\beta(x) = b_{n-1}x^{n-1}+b_{n-2}x^{n-2}+...+b_2x^2+b_1x+b_0$ – многочлен, в котором коэффициентами являются битовые последовательности сгенерированного ключа.

$\omega(x) = c_{n-1}x^{n-1}+c_{n-2}x^{n-2}+...+c_2x^2+c_1x+c_0$ – многочлен, в котором коэффициентами являются битовые последовательности шифртекста.

$p(x) = k_nx^n + k_{n-1}x^{n-1} + k_{n-2}x^{n-2} + ... + k_2x^2 + k_1x + k_0$ – неприводимый многочлен, который выбран рабочим основанием, по модулю которого выполняются операции.

Процедура расшифрования для метода (8) производится по следующей формуле:

$$\omega(x) * \beta^{-1}(x) \equiv \alpha(x)(mod\ p(x)), \tag{9}$$

где $\beta^{-1}(x) = d_{n-1}x^{n-1} + d_{n-2}x^{n-2} + ... + d_2x^2 + d_1x + d_0$ – многочлен, инверсный (обратный) к $\beta(x)$, в котором коэффициентами являются битовые последовательности и где $\beta(x) * \beta^{-1}(x) \equiv 1(mod\ p(x))$.

Из выражения (8) найдется такой полином $s(x) \in GF(2)[x]/(p(x))$, который удовлетворяет уравнению

$$\omega(x) * \beta^{-1}(x) \oplus p(x) * s(x) = \alpha(x), \tag{10}$$

где $s(x) = s_{n-2}x^{n-2} + s_{n-3}x^{n-3} + ... + s_2x^2 + s_1x + s_0$ – многочлен.

Процесс умножения двух многочленов выполняется следующим образом:

$$\begin{gathered} \omega(x) * \beta^{-1}(x) = (c_{n-1}x^{n-1} + ... + c_1x + c_0)* \\ *(d_{n-1}x^{n-1} + ... + d_1x + d_0) \\ \omega(x) * \beta^{-1}(x) = c_{n-1}d_{n-1}x^{2n-2} + \\ +(c_{n-1}d_{n-2} \oplus c_{n-2}d_{n-1})x^{2n-3} + ... + c_0d_0 \end{gathered} \tag{11}$$

$$\begin{gathered} p(x) * s(x) = (k_nx^n + ... + k_1x + k_0)* \\ *(s_{n-2}x^{n-2} + ... + s_1x + s_0) \\ p(x) * s(x) = k_ns_{n-2}x^{2n-2} + (k_ns_{n-3} \oplus k_{n-1}s_{n-2})* \\ *x^{2n-3} + ... + k_0s_0 \end{gathered} \tag{12}$$

Тогда из (10), (11) и (12) получаем следующую систему уравнений:

$$\begin{cases} c_{n-1}d_{n-1} \oplus k_ns_{n-2} = 0 \\ c_{n-1}d_{n-2} \oplus c_{n-2}d_{n-1} \oplus k_ns_{n-3} \oplus k_{n-1}s_{n-2} = 0 \\ \dots \\ c_{n-1}d_1 \oplus \dots \oplus c_1d_{n-1} \oplus k_ns_0 \oplus \dots \oplus k_2s_{n-2} = 0 \\ c_{n-1}d_0 \oplus \dots \oplus k_{n-1}s_0 \oplus \dots \oplus k_1s_{n-2} = a_{n-1} \\ c_{n-2}d_0 \oplus \dots \oplus k_{n-2}s_0 \oplus \dots \oplus k_0s_{n-2} = a_{n-2} \\ \dots \\ c_2d_0 \oplus c_1d_1 \oplus c_0d_2 \oplus k_2s_0 \oplus k_1s_1 \oplus k_0s_2 = a_2 \\ c_1d_0 \oplus c_0d_1 \oplus k_1s_0 \oplus k_0s_1 = a_1 \\ c_0d_0 \oplus k_0s_0 = a_0 \end{cases} \tag{13}$$

Здесь $c = (c_{n-1}, c_{n-2}, ..., c_2, c_1, c_0)$ – коэффициенты многочлена $\omega(x)$, представляющие собой битовую последовательность известного нам шифртекста. Коэффициентами многочленов $\alpha(x)$, $p(x)$, $\beta^{-1}(x)$ и $s(x)$ являются соответственно $a = (a_{n-1}, a_{n-2}, ..., a_2, a_1, a_0)$, $k = (k_{n-1}, k_{n-2}, ..., k_2, k_1, k_0)$, $d = (d_{n-1}, d_{n-2}, ..., d_2, d_1, d_0)$ и $s = (s_{n-2}, s_{n-3}, ..., s_2, s_1, s_0)$. Эти коэффициенты – битовые последовательности неизвестных переменных.

Система уравнений (13) может быть построена для каждого рабочего основания алгоритма шифрования на базе НПСС. Заметим, что количество уравнений в системе (13) равно $(2n-1)$, а количество переменных в системе равно $(4n-2)$.

Рассмотрим частный случай, когда система уравнений является линейной. В этом случае в системе (13) отсутствую переменные k_i и s_i.

Если система уравнений линейная и количество переменных в ней в 2 раза больше количества уравнений, то она имеет 2^n решений. Однако, для каждого конкретного открытого текста $a = (a_{n-1}, a_{n-2}, ..., a_2, a_1, a_0)$ существует единственное решение $d = (d_{n-1}, d_{n-2}, ..., d_2, d, d_0)$.

Теперь рассмотрим общий случай. Если учесть, что у неприводимых многочленов коэффициенты k_n и k_0 всегда равны 1, то тогда переменные s_i в системе уравнения (13) можно представить в следующем виде:

$$s_{n-2} = c_{n-1} \cdot d_{n-1},$$
$$s_{n-3} = c_{n-1} \cdot d_{n-2} \oplus c_{n-2} \cdot d_{n-1} \oplus k_{n-1} \cdot c_{n-1} \cdot d_{n-1},$$

Общую формулу выражения можно записать в рекурсивном виде:

$$s_i = c_{n-1} \cdot d_{i+1} \oplus \ldots \oplus c_{i+1} \cdot d_{n-1} \oplus k_{n-1} \cdot S_{i+1} \oplus k_{n-2} \cdot S_{i+2} \oplus \ldots \oplus k_{i+2} \cdot S_{n-2}, \quad (14)$$

где $i = \overline{0, n-2}$

Если уравнение (14) подставить в виде системы уравнений (13), тогда получим n уравнений вместо $2n-1$. Эти n уравнений состоят из переменных d_i, k_i и a_i. Число произведений, состоящих из переменных k_i и d_i, быстро растет в соответствии с увеличением степени неприводимого многочлена, но количество множителей k_i не превышает половины его показателя степени. Также отметим то, что сумма битового сложения коэффициентов неприводимого многочлена равна 1 (криптоаналитик воспользуется этим свойством). Тогда, система (13) примет вид:

$$\begin{cases} F_1(c,d,k) = a_{n-1} \\ F_2(c,d,k) = a_{n-2} \\ F_n(c,d,k) = a_0 \\ k_{n-1} \oplus ... \oplus k_1 = 1 \end{cases} \quad (15)$$

Эту систему можно линеаризовать путем введения новых переменных, но для этого потребуется открытый текст, длина которого не меньше количества полученных переменных. Теперь рассмотрим случай, когда открытый текст неизвестен. Тогда задача криптоаналитика сводится к задаче полного перебора ключей. В таблице 1 приведена зависимость количества вариантов перебора от длины ключа. Теперь рассмотрим случай, когда криптоаналитик имеет открытый текст и его шифртекст, то есть в уравнении (15) известны переменные a_i. Как отмечено выше, в этом случае приведение к линейному виду не эффективно. Можно искать решение подбором неприводимых многочленов. Подставляя значения выбранных неприводимых многочленов в систему уравнений (15), получим n уравнений с n переменными. Полученные уравнения или имеют решение, или не имеют. Если они не имеют решения, то выбираются другие многочлены этой

же степени. В противном случае, применяя полученное решение как ключ, производим расшифрование последовательных блоков длины m. Если полученный открытый текст бессмысленный, то переходим к следующему решению. В случае, когда полученные результаты соответствуют открытому тексту, считаем, что часть ключа, соответствующая выбранному рабочему основанию, найдена и переходим к поиску следующих частей ключа. Сложность этого подхода будет увеличиваться в соответствии с ростом степени неприводимого многочлена.

Таблица 1 – Количество вариантов перебора в зависимости от длины ключа

Длина ключа	Количество неприводимых многочленов	Количество различных открытых текстов	Количество всех возможных вариантов	Вероятность
3	2	8	16	0,0625
4	3	16	64	0,015625
5	6	32	256	0,003906
6	9	64	832	0,001202
7	18	128	3136	0,000319
8	30	256	10816	9,25E-05
9	56	512	39488	2,53E-05
10	99	1024	140864	7,1E-06
11	186	2048	521792	1,92E-06
12	335	4096	1893952	5,28E-07
13	630	8192	7054912	1,42E-07
14	1161	16384	26076736	3,83E-08
15	2182	32768	97576512	1,025E-08
16	4080	65536	364963392	2,74E-09

Рассмотрим также случай, когда известен тип расширения зашифрованного файла. Тогда, зная стандартное начало файла, можно привести систему уравнений к виду, рассмотренному выше и по аналогии искать ключи частями. В таблице 2 показаны начальные байты для некоторых стандартных типов файлов. Эти байты могут быть использованы для нахождения частей ключа. Также рассмотрим случай, когда открытый текст состоит из символов латинского алфавите в кодировке ASCII. Поскольку каждый 8-й бит является нулевым, то подставив соответствующие биты открытого текста в систему уравнений (15) и выбирая их из каждого последовательного блока длины m получим новую систему уравнений, в которой правая часть определена. Здесь число уравнений зависит от длины открытого текста. Чтобы число уравнений не было меньше числа переменных, длина открытого текста должна превосходить длину ключа не менее чем в 8 раз. Полученная система уравнений далее решается как в предыдущих случаях. С ростом степени многочленов количество вариантов перебора существенно увеличивается, и такой подход становится неэффективным для криптоанализа.

Таблица 2 – Начала файлов для некоторых стандартных типов расширений

Байт	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
.docx	50	4b	03	04	14	00	06	00	08	00	00	00	21	00		
.jpg	Ff	d8	Ff	e0	00	10	4a	46	49	46	00	01	01	01	01	2c
.pdf	25	50	44	46	2d	31	2e									
.pdf*	Ef	bb	Bf	25	50	44	46	2d	31	2e						
.html	3c	21	44	4f	43	54	59	50	45	20	68	74	6d			
.doc	d0	cf	11	e0	a1	b1	1a	e1	00	00	00	00	00	00	00	00
.zip	50	4b	03	04												
.exe	4d	5a	90	00	03	00	00	00	04	00	00	00	ff	Ff	00	00

5. Заключение

Результаты исследования показали, что для алгебраических атак их сложность определяется количеством и степенью неприводимых многочленов, из которых составляется система рабочих оснований.

Полученные результаты могут быть использованы при формировании рекомендаций по практическому использованию алгоритма шифрования.

Работа выполнена при поддержке программно-целевого финансирования научно-технических программ и проектов Комитетом науки МОН РК №0128/ПЦФ.

Литература

[1] Бияшев Р.Г Разработка и исследование методов сквозного повышения достоверности в системах обмена данными распределенных АСУ. – 1985. – 328 с.

[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. – 2005. – 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 – 2014. – pp. 49-54

[4] R. Biyashev, S. Nyssanbayeva, N. Kapalova The Key Exchange Algorithm on Basis of Modular Arithmetic // Proceedings of International Conference on Electrical, Control and Automation Engineering. – 2013. – 16 p.

[5] Бияшев Р.Г., Нысанбаева С. Е., Капалова Н.А. Секретные ключи для непозиционных криптосистем. Разработка, исследование и применение. – 2014. – 126 с.

[6] Иванов М.А. Криптографические методы защиты информации в компьютерных системах и сетях. – 2001. – 308 с.

[7] Ростовцев А.Г., Маховенко Е.Б. Теоретическая криптография. – 2004. – 480 с.

[8] Бабенко Л.К., Ищукова Е.А. Современные алгоритмы блочного шифрования и методы их анализа. – 2006. – 376 с.

References

[1] Biyashev R.G Razrabotka i issledovanie metodov skvoznogo povishenie dostovernosti v sistemah obmena dannimi raspredelennih ASY. – 1985. – 328 p.

[2] Amerbaev V.M., Biyashev R.G., Nisanbaeva S.E. Primenenie nepozicionnih sistem schisleniya pri kritograficheskoi zashite // Izv. Nac. akad. nayk Respubliki Kazakhstan.–Ser. fiz.-mat. – 2005. – p. 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 – 2014. – pp. 49-54

[4] R. Biyashev, S. Nyssanbayeva, N. Kapalova The Key Exchange Algorithm on Basis of Modular Arithmetic // Proceedings of International Conference on Electrical, Control and Automation Engineering. – 2013. – 16 p.

[5] Biyashev R.G., Nyssanbayeva S. E., Kapalova N.A. Sekretnie klychi dlya nepozicionnih kriptosistem. Razrabotka, issledovanie i primenenie. – 2014. – 126 p.

[6] Ivanov M.A. Kriptograficheskie metodi zashiti informacii v kompyuternih sistemah i setyah. – 2001. – 308 p.

[7] Rostovcev A.G., Mahovenko E.B. Teoreticheskaya kriptografiya. – 2004. – 480 p.

[8] Babenko L.K., Ishykova E.A. Sovremennie algoritmi blochnogo shifrovaniya i metodi ih analiza. – 2006. – 376 p.

УДК 531.8

Кудайкулов А.К., Ташев А.А.*, Ногайбаева М.О.

Институт информационных и вычислительных технологий КН МОН РК,
Республика Казахстан, г. Алматы
* E-mail: azattash@mail

Исследование термофизического состояния стержня из жаропрочного сплава АМВ-300 при воздействии точечной температуры и поверхностного теплообмена

На основе фундаментальных законов сохранения энергии строится разрешающая система уравнений, характеризующая теплофизическое состояние стержня, выполненной из жаропрочного сплава АМВ-300. Стержень имеет ограниченную длину, площадь поперечного сечения которого постоянна по всей ее длине. Предполагается, что левый конец стержня жестко-защемлен и совпадает с началом координат. При этом температура окружающей среды, коэффициент теплообмена считается постоянной по всей поверхности стержня. Кроме того, на правом конце стержня приложена осевая растягивающая сила, и стержень находится под воздействием точечной температуры и поверхностного теплообмена. Для этого материала коэффициент теплового расширения зависит от температуры. Для решения задачи сначала стержень разбивается на частей - элементов одинаковой длины. Каждый элемент подвергается квадратичной аппроксимации с тремя узлами. Далее для каждого элемента записывается выражение функционала, которое характеризует полную тепловую энергию с учетом заданных граничных условий. Дифференцируя функционал, которое характеризует полную тепловую энергию по переменным температур в заданных узлах получается система дифференциальных уравнений. Решая эту систему определяются поля температур, составляющие деформации и напряжения. Вычисляются величина возникающего осевого усилия и температурное удлинение стержня.
Ключевые слова: жаропрочные сплавы, конвективный теплообмен, точечная температура, теплопроводность, усилие, напряжение, деформация.

Kudaykulov A.K., Tashev A.A., Nogaybayeva M.O.

Analysis of termophysical condition of AMB-300 heat-resistant alloy rod at spot temperature and surface heat transfer

Based on the basic laws of energy conservation, resolving combined equations are built that outline the thermosphysical condition of the rod, which is made of the AMB-300 heat-resistant alloy. The rod has a limited length, the cross-sectional area which is constant throughout its length. It is assumed that the left end of the rod is rigidly-clamped and coincides with the beginning of coordinates. The ambient temperature, the heat transfer coefficient is considered constant across the surface of the rod. In addition, the axial tensile force is applied on the right end of the rod, and the rod is under the impact of the spot temperature and surface heat transfer. For this material, the heat-expansion coefficient depends on the temperature. At first the rod is divided into parts - elements of the same length to solve the problem. Each element is subjected to a quadratic approximation with three nodes. Then, expression of functional is written for each element which characterizes the total heat energy with the given boundary conditions. The system of differential equations is obtained by differentiating functional, which characterizes the total heat energy on temperatures variables at specified nodes. When solving this system temperature fields that cause distortions and strains are determined. The value of the arising axial force and thermal expansion of the rod are calculated.
Key words: heat-resistant alloys, convective heat transfer, spot temperature, heat conduction, force, strain, deformation.

Құдайқұлов А.К.,Ташев А.А., Ноғайбаева М.О.

Ғылыми-зерттеу жылу физикалық мемлекеттік қорытпаларды штанг 300 AMV - спот жылу және жер үсті температура әсеріне ұшыраған кезде

Энергия сақтау іргелі заңдар негізінде ыстыққа төзімді қорытпасы АТФБ – 300 жасалған жылу физикалық өзек жағдайын сипаттайтын теңдеулер жүйесін шешу қрастырылған. Өзек шектеулі ұзындығы, оның бүкіл ұзындығы бойынша тұрақты қимасының ауданы бар. Бұл өзек сол соңы тығыз – қысып деп болжануда және шығу тегі сәйкес келеді. Бұл жағдайда қоршаған ортаның температурасы, жылу беру коэффициенті өзек бүкіл бетінің тұрақты болып саналады. Сонымен қатар, өзек оң аяғында осьтік созылу күшін қолданбалы және өзек спот температурасын және жылу бетіне ұшырайды. Осы материалға, жылу кеңейту коэффициенті температурасына байланысты. Ұзындығы бірдей элементтері – мәселені шешу үшін алғашқы өзек бөлікке бөлінеді. Әрбір элемент үш тораптары бар квадрат мақсатын ұшырайды. Келесі, әрбір элемент үшін анықталған шекаралық шарттар жалпы жылу энергиясын сипаттайды функционалдық өрнек сақталады. Алдын ала белгіленген алаңдарында температурасын, дифференциалдық теңдеулер жүйесін өзгерту арқылы толық жылу сипаттайды функционалдық дифференциялау. Осы жүйені шешу температуралық өрісті, кернеулер мен деформациялардық компоненттерін анықталады. Біз дамушы әуекеменің штангалы жылу ұзарту мәні есептеу.

Түйін сөздер: жоғары температуралы қорытпалар, конвективті жылуалмасу, спот температура, жылу өткізгіштік, стресс, штамм, деформация.

1. Введение

В настоящее время актуальной проблемой является выбор соответствующих жаропрочных материалов для различного уровня тепловых воздействий. Поэтому научно-исследовательские изыскания в области повышения качества и долговечности жаропрочных изделий является актуальной. Исследование теплопроводности в твердых телах рассматриваются во многих работах. В данной работе на основе фундаментальных законов сохранения энергии строится разрешающая система уравнений, характеризующая теплофизическое состояние стержня, выполненной из жаропрочного сплава АМВ-300. Определяются поля температур, составляющие деформации и напряжения. Вычисляются величина возникающего осевого усилия и температурное удлинение стержня.

2. Постановка задачи

Рассмотрим стержень ограниченной длины L,(см), площадь поперечного сечения которого $F,(\text{см}^2)$, постоянна по ее длине. Стержень изготовлен из жаропрочного сплава $AHB-300$. Значение коэффициента теплового расширение этого материала $\alpha,(1/^\circ C)$ строго зависит от значения температуры, т.е. $\alpha=\alpha\left(T\left(x\right)\right)$. Здесь $T=T\left(x\right)$ -поле распределения температуры по длине стержня, которое необходимо определить с учетом существующих граничных условий. Коэффициент теплопроводности материала стержня обозначим через $K_{xx},(\text{Вт}/(\text{см}^\circ C))$, а модуль упругости через $E,(\text{кГ}/\text{см}^2)$.

Требуется определить поле распределения температуры $T=T\left(x\right)$ по длине стержня с учетом наличия источника тепла и глобального теплообмена. Также необходимо вычислить удлинение стержня от теплового расширения и растягивающей силы P.

3. Решение задачи

Расчетная схема рассматриваемой задачи приводится на рисунке 1.

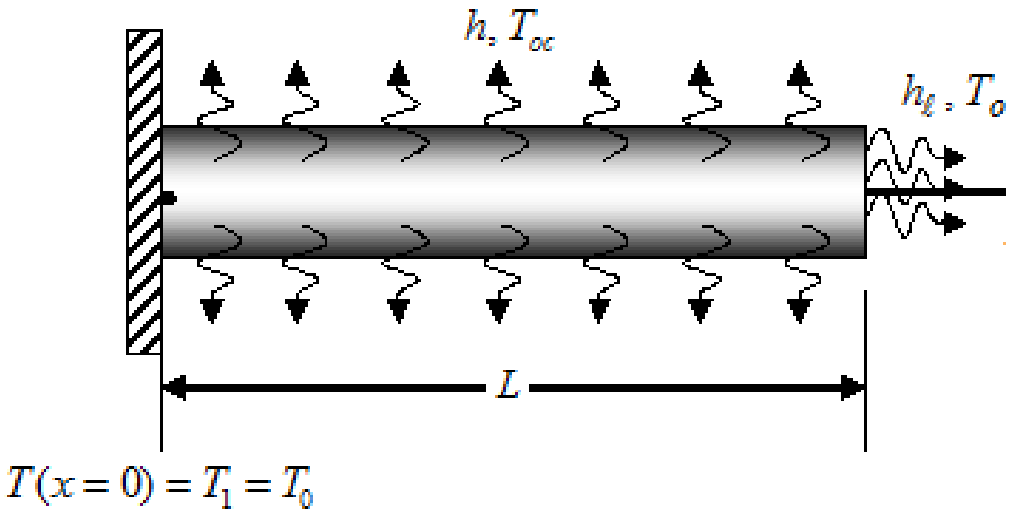

Рисунок 1 – Расчетная схема рассматриваемой задачи

Предположим, что левый конец стержня жестко-защемлен и совпадает с началом координат. На этом конце задана температура $T\,(x=0) = T_1 = T_0$. Через площади боковой поверхности и поперечного сечения правого конца происходит теплообмен с окружающей средой. При этом температура окружающей среды $T_{oc}, (^\circ C)$, коэффициент теплообмена $h, (\text{Вт}/(\text{см}^2{}^\circ C))$ и ее значение также постоянна во всюду. Кроме того, на правом конце стержня приложена осевая растягивающая сила $P, (\text{кГ})$. Требуется определить поле распределения температуры $T = T(x)$ по длине стержня с учетом наличия источника тепла и глобального теплообмена. Также необходимо вычислить удлинение стержня от теплового расширения и растягивающей силы P.

Для этого сначала дискретизируем рассматриваемый стержень n элементами одинаковой длины. Каждый элемент рассмотрим как квадратный конечный элемент с тремя узлами. Тогда число всех узлов будет равно ЧУЗ=2n+1. Далее для каждого элемента напишем выражение функционала, которое характеризует полную тепловую энергию с учетом имеющихся граничных условий. В частности для первого элемента такой функционал имеет следующий вид [1 – 3].

$$J_1 = \int_{V_1} \frac{K_{xx}}{2} \left(\frac{\partial T}{\partial x}\right)^2 dV + \int_{S_{1nbn}} \frac{h}{2} \left(T - T_{oc}\right)^2 dS, \tag{1}$$

где V_1 -объем первого элемента; S_{1nbn} -площадь боковой поверхности первого элемента. С учетом (3) для первого элемента имеем, что

$$\mathrm{T(x)}= \varphi_1(x)\cdot T_1+\varphi_2(x)\cdot T_2+\varphi_3(x)\cdot T_3, 0\le x\le \tfrac{L}{n}; \tag{2}$$

$$\frac{\partial T}{\partial x}=\frac{\partial \varphi_1(x)}{\partial x}\cdot T_1+\frac{\partial \varphi_2(x)}{\partial x}\cdot T_2+\frac{\partial \varphi_3(x)}{\partial x}\cdot T_3, 0\le x\le \frac{L}{n}; \tag{3}$$

где T_1, T_2 и T_3 -значения температур в узлах первого элемента. При этом

$$T_1=T(x=0)=T_0; T_2=T\left(x=\frac{L}{2n}\right); T_3=T\left(x=\frac{L}{n}\right). \tag{4}$$

Будем учитывать, что $\int_{V_1} f(x)\,dV=F\int_0^{\ell} f(x)\,dx$; где F -площадь поперечного сечения рассматриваемого элемента стержня; $\ell=\frac{L}{n}$ -длина элемента стержня; $\int_{S_{1nbn}} f(x)\,dS=\int_0^{\ell} f(x)\,dx$; где P - периметр поперечного сечения, а также интеграла по площади поперечного сечения $\int_{S_{nnc}} TdS=FT_1$.

Тогда для первого элемента интегрированный вид функционала (1) имеет следующий вид

$$J_1=\frac{K_{xx}\cdot F}{2\ell}\left[\frac{7}{3}T_1^2-\frac{16}{3}T_1\cdot T_2+\frac{2}{3}T_1\cdot T_3-\frac{16}{3}T_2\cdot T_3+\frac{16}{3}T_2^2+\frac{7}{3}T_3^2\right]+$$
$$+\frac{Ph}{2}\left[\frac{2\ell}{15}T_1^2+\frac{2\ell}{15}T_1\cdot T_2-\frac{\ell}{15}T_1\cdot T_3+\frac{8\ell}{15}T_2^2+\frac{2\ell}{15}T_3^2+\frac{2\ell}{15}T_2\cdot T_3-\right.$$
$$\left.-\frac{\ell}{3}T_{oc}\cdot T_1-\frac{4\ell}{3}T_{oc}\cdot T_2-\frac{\ell}{3}T_{oc}\cdot T_3+\ell\cdot T_{oc}^2\right] \tag{5}$$

Начиная со второго до $(n-1)$ -го элемента выражение соответствующего функционала для каждого элемента имеет следующий интегрированный вид

$$J_r=\int_{V_r}\frac{K_{xx}}{2}\left(\frac{\partial T}{\partial x}\right)^2 dV+\int_{S_{r\,nbn}}\frac{h}{2}(T-T_{oc})^2\,dS=$$
$$=\frac{K_{xx}\cdot F}{2\ell}\left[\frac{7}{3}T_i^2-\frac{16}{3}T_i\cdot T_j+\frac{2}{3}T_i\cdot T_k-\frac{16}{3}T_j\cdot T_k+\frac{16}{3}T_j^2+\frac{7}{3}T_k^2\right]+$$
$$+\frac{Ph}{2}\left[\frac{2\ell}{15}T_i^2+\frac{2\ell}{15}T_i\cdot T_j-\frac{\ell}{15}T_i\cdot T_k+\frac{8\ell}{15}T_j^2+\frac{2\ell}{15}T_k^2+\frac{2\ell}{15}T_j\cdot T_k-\right.$$
$$\left.-\frac{\ell}{3}T_{oc}\cdot T_i-\frac{4\ell}{3}T_{oc}\cdot T_j-\frac{\ell}{3}T_{oc}\cdot T_k+\ell\cdot T_{oc}^2\right], x_i\le x\le x_k \tag{6}$$

где $r=2\div(n-1)$ -номер элемента; $i=(2r-1)$; $j=2r$; $k=2r+1$; и

$$x_i=\frac{L}{n}\cdot(r-1); x_k=\frac{L}{n}\cdot r.$$

.

Наконец, для последнего n-го элемента выражение функционала, которое характеризует полную тепловую энергию имеет следующий интегрированный вид

$$J_n = \int_{V_n} \frac{K_{xx}}{2} \left(\frac{\partial T}{\partial x}\right)^2 dV + \int_{S_{n\,nbn}} \frac{h}{2} \left(T - T_{oc}\right)^2 dS + \int_{S_{L\,nnc}} \frac{h}{2} \left(T - T_{oc}\right)^2 dS =$$

$$= \frac{K_{xx} \cdot F}{2\ell} \left[\frac{7}{3}T_{2n-1}^2 - \frac{16}{3}T_{2n-1} \cdot T_{2n} + \frac{2}{3}T_{2n-1} \cdot T_{2n+1} - \frac{16}{3}T_{2n} \cdot T_{2n+1} + \frac{16}{3}T_{2n}^2 + \frac{7}{3}T_{2n+1}^2\right] +$$

$$+\frac{Ph}{2} \left[\frac{2\ell}{15}T_{2n-1}^2 + \frac{2\ell}{15}T_{2n-1} \cdot T_{2n} - \frac{\ell}{15}T_{2n-1} \cdot T_{2n+1} + \frac{8\ell}{15}T_{2n}^2 + \frac{2\ell}{15}T_{2n+1}^2 + \frac{2\ell}{15}T_{2n} \cdot T_{2n+1} -\right.$$

$$\left. -\frac{\ell}{3}T_{oc} \cdot T_{2n-1} - \frac{4\ell}{3}T_{oc} \cdot T_{2n} - \frac{\ell}{3}T_{oc} \cdot T_{2n+1} + \ell \cdot T_{oc}^2\right] + \frac{Fh}{2} \left(T_{2n+1} - T_{oc}\right)^2, \qquad (7)$$

где $\ell = L - \frac{(n-1)\cdot L}{n} = \frac{L}{n}$; $S_{L\,nnc}$ - площадь поперечного сечения правого конца стержня.

Тогда выражение функционала, которое характеризует полную тепловую энергию рассматриваемого стержня, в целом имеет следующий вид

$$J = \sum_{r=1}^{n} J_r, \qquad (8)$$

Учитывая, что значение температуры в первом узле задано, т.е. $T_1 = T(x = 0) = T_0$, минимизируя функционал (8) по узловым значениям температуры $T_2, T_3, ..., T_{2n+1}$ построим следующую разрешающую систему линейных алгебраических уравнений

$$\frac{\partial J}{\partial T_r} = 0, r = 2 \div (2n + 1). \qquad (9)$$

Решая последнюю систему, находим значения температур в узлах элементов. Пользуясь соотношением (3), находим закон распределения поля температур в пределах каждого элемента, а по ним по длине рассматриваемого стержня в целом.

В работе [4] для жаропрочного тугоплавкого сплава приводится результаты натурного эксперимента по определению зависимости коэффициента теплового расширения от температуры в виде графиков. Эти данные в первом разделе приведены в табличной форме, в том числе и для сплава $AHB - 300$. Из результатов натурного эксперимента работы [4] видно, что $\alpha\left(T\left(x\right)\right)$ меняется линейно в интервале температур
$T \in [20(^\circ C);\ 100(^\circ C)]$; $T \in [100(^\circ C);\ 200(^\circ C)]$; $T \in [200(^\circ C);\ 300(^\circ C)]$;

$T \in [300(^\circ C);\ 400(^\circ C)]$; $T \in [400(^\circ C);\ 500(^\circ C)]$; $T \in [500(^\circ C);\ 600(^\circ C)]$;

$T \in [600(^\circ C);\ 700(^\circ C)]$; $T \in [700(^\circ C);\ 800(^\circ C)]$.

По этому эти зависимости можно описать математически следующим образом

$$\left.\begin{array}{l}
1)\ \alpha = 0,0225\cdot 10^{-6}\cdot T + 9,65\cdot 10^{-6}\,(1/^{\circ}C) \ \text{ при } \ 20 \le T \le 100(^{\circ}C);\\
2)\ \alpha = 0,013\cdot 10^{-6}\cdot T + 10,6\cdot 10^{-6}\,(1/^{\circ}C) \ \text{ при } \ 100 \le T \le 200(^{\circ}C);\\
3)\ \alpha = 0,015\cdot 10^{-6}\cdot T + 10,2\cdot 10^{-6}\,(1/^{\circ}C) \ \text{ при } \ 200 \le T \le 300(^{\circ}C);\\
4)\ \alpha = 0,023\cdot 10^{-6}\cdot T + 7,8\cdot 10^{-6}\,(1/^{\circ}C) \ \text{ при } \ 300 \le T \le 400(^{\circ}C);\\
5)\ \alpha = 0,013\cdot 10^{-6}\cdot T + 11,8\cdot 10^{-6}\,(1/^{\circ}C) \ \text{ при } \ 400 \le T \le 500(^{\circ}C);\\
6)\ \alpha = 0,02\cdot 10^{-6}\cdot T + 8,3\cdot 10^{-6}\,(1/^{\circ}C) \ \text{ при } \ 500 \le T \le 600(^{\circ}C);\\
7)\ \alpha = 0,017\cdot 10^{-6}\cdot T + 10,1\cdot 10^{-6}\,(1/^{\circ}C) \ \text{ при } \ 600 \le T \le 700(^{\circ}C);\\
8)\ \alpha = 0,012\cdot 10^{-6}\cdot T + 13,6\cdot 10^{-6}\,(1/^{\circ}C) \ \text{ при } \ 700 \le T \le 800(^{\circ}C);
\end{array}\right\} \qquad (10)$$

Кроме того, известно (раздел 1), что поле распределение коэффициента теплового расширения для r-го элемента определяется (1.35), где, α_i, α_j и α_k- узловые значения коэффициента теплового расширения в r -м элементе $i = 2r-1$; $j = 2r$; $k = 2r+1$.

Тогда узловые значения α определяются исходя из закона распределения температуры в каждом элементе и с помощью соотношения (10). А величина удлинение r -того элемента определяется с помощью соотношения

$$\Delta\ell_{T\,r} = \int_0^{\ell} \alpha\left(T\left(x\right)\right)\cdot T\left(x\right)dx = \int_0^{\ell}\left[\sum_{i=1}^{3}\varphi_i\left(x\right)\cdot\alpha_i \times \sum_{i=1}^{3}\varphi_i\left(x\right)\cdot T_i\right]dx, \qquad (11)$$

где $\varphi_i\left(x\right)$ -функция формы для r -го квадратичного элемента; α_i, T_i - узловые значения коэффициента теплового расширения и температуры r-го квадратичного элемента.

Тогда общее удлинение рассматриваемого стержня в целом от теплового расширения определяется следующим образом

$$\Delta\ell_T = \sum_{r=1}^{n}\Delta\ell_{T\,r}. \qquad (12)$$

На основе закона Гука удлинение рассматриваемого стержня от осевой растягивающей силы P определяется следующим образом

$$\Delta\ell_P = \frac{P\ell}{EF}. \qquad (13)$$

Тогда величина общего удлинения рассматриваемого стержня будет

$$\Delta\ell = \Delta\ell_T + \Delta\ell_P. \qquad (14)$$

Для реализации вышеизложенного алгоритма примем за исходные данные следующее $K_{xx} = 72\,(\text{Вт}/(\text{см}^{\circ}C))$; $h = 10/(\text{Вт}/(\text{см}^{2\circ}C))$; $T_{oc} = 40(^{\circ}C)$; $T\left(x=0\right) = T_1 = T_0 = \left[100 \div 800(^{\circ}C)\right]$; $E = 2,1\cdot 10^6(\text{кГ}/\text{см}^2)$; $L = 30(\text{см})$; $n = 300$; $\ell = \frac{L}{n} = 0,1(\text{см})$.

Форма поперечного сечения рассматриваемого стержня является круг радиусом $r = 1(\text{см})$. Площадь поперечного сечения $F = \pi\, r^2 = \pi(\text{см}^2)$, а периметр $P = 2\pi\, r = 2\pi(\text{см})$.

На рисунке 2 приводится поле распределения температур по длине стержня при разных значениях T_0, а в таблице 3.1 приводится значения $\Delta\ell_T$ при разных значениях T_0, т.е. зависимость между T_0 и $\Delta\ell_T$, R ,σ. Из рисунка 2 видно, что поле распределения температуры по длине стержня будет гладкой кривой. Графическая зависимость между величинами источника температуры (T_0) и соответствующего удлинение стержня $(\Delta\ell_T)$ от теплового расширения приводится на рисунке 3.

При $T_0 = 100(^\circ C)$, начиная с $x = 15,5(\text{см})$, т.е. на участке $15,5 \leq x \leq 30(\text{см})$ наблюдается постоянная температура, значения, которого равна $\approx 40(^\circ C)$. В этом случае из за теплового расширения стержень удлиняется на $\Delta\ell_T = 0,014(\text{см})$. Для сравнения, следует сказать, что это удлинение эквивалентно к удлинению стержня, если его растягивать силой $R = 2930,66(\text{кГ})$. Естественно, на основе закона Гука в этом случае в сечении стержня возникало бы растягивающее напряжение величиной $\sigma = 933,33\,(\text{кГ}/\text{см}^2)$).

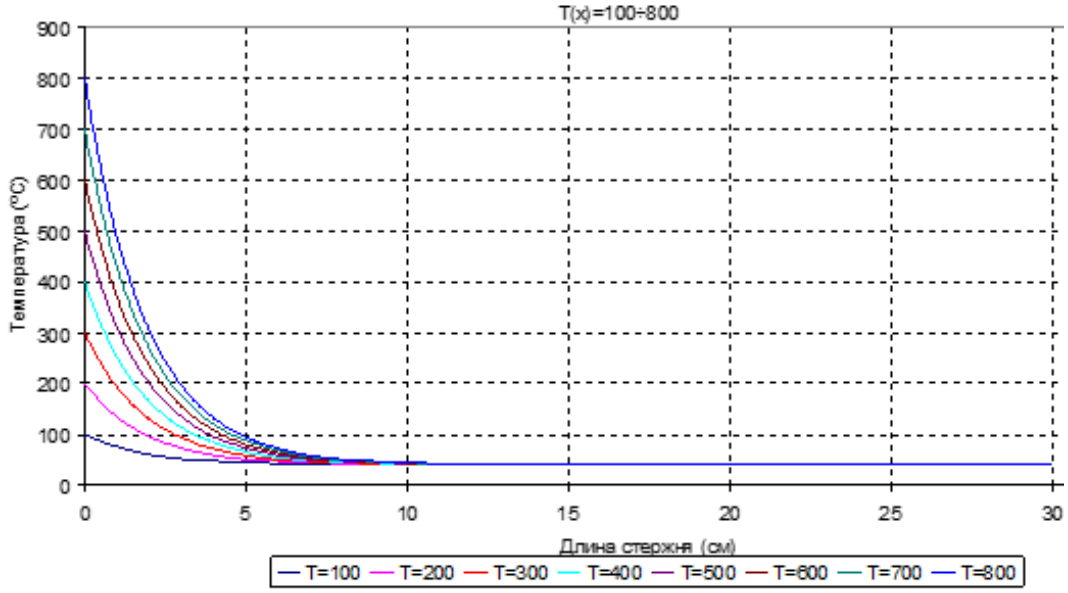

Рисунок 2 – Поле распределения температуры по длине стержня при разных значениях T_0

Таблица 1-Зависимость между T_0 и $\Delta\ell_T$, R, σ

№ п/п	$T_0(^\circ C)$	$\Delta\ell_T$(см)	Эквивалентная «растягивающая» сила R(кГ), при котором получилось бы такое удлинение	Эквивалентное «растягивающее напряжение» $\sigma\left(\text{кГ}/(\text{см})^2\right)$	$\overline{\Delta\ell}_T$(см) при $\alpha = const = 10,1 \cdot 10^{-6}\,(1/^\circ C)$	Относительное удлинение в %	$k = \frac{\Delta\ell_T}{\overline{\Delta\ell}_T}$ (раза)
1.	100	0,014	2930,66	933,33	0,0133	0,047	1,052
2.	200	0,0165	3454	1100	0,0152	0,055	1,085
3.	300	0,0193	4040,1	1286,66	0,0171	0,064	1,129
4.	400	0,02247	4703,72	1498	0,0190	0,075	1,183
5.	500	0,0259	5432,2	1730	0,0209	0,086	1,239
6.	600	0,0297	6217,2	1980	0,0228	0,1	1,303
7.	700	0,03388	7092,2	2258,66	0,0247	0,113	1,372
8.	800	0,038	7954,66	2533,33	0,0267	0,127	1,423

При увеличении значения заданной температуры в два раза, т.е. при $T_0 = 200(^\circ C)$ на участке $19,2 \leq x \leq 30$(см) наблюдается $40(^\circ C)$ -ная поле температуры. В этом случае величина удлинение стержня составляет $\Delta\ell_T = 0,0165$(см) и будет больше на $17,657\%$ чем в случае $T_0 = 100(^\circ C)$. Эта величина удлинение эквивалентно к удлинению стержня находящейся по растягивающей нагрузкой $R = 3454$(кГ). При этом растягивающее напряжение было бы $\sigma = 1100\,(\text{кГ}/\text{см}^2)$). Если увеличить значение точечной температуры в три раза, т.е. при $T_0 = 300(^\circ C)$ величина , $\Delta\ell_T = 0,0193$(см), что превышает на $37,857\%$ чем в случае $T_0 = 100(^\circ C)$. Также следует отметить, что в этом случае на участке $21,1 \leq x \leq 30$(см) стержня наблюдается постоянная температура близко к температуре окружающей стержня среды. В этом случае величина $\Delta\ell_T$ эквивалентно к растяжению рассматриваемого стержня с силой $R = 4040,1$(кГ). При этом значение растягивающего напряжения возникающих в сечениях составляло бы $\sigma = 1286,66\,(\text{кГ}/\text{см}^2)$). Следует отметить, что для обычных сталей это напряжение уже превышает предел пропорциональности.

Теперь увеличивая значение T_0 в четыре раза, т.е. при $T_0 = 400(^\circ C)$ имеем, что $\Delta\ell_T = 0,02247$(см) . Это эквивалентно к удлинению стержня при ее растяжении силой, величина которого $R = 4703,72$(кГ). В этом случае в сечениях стержня возникало бы растягивающее напряжение величиной $\sigma = 1498\,(\text{кГ}/\text{см}^2)$). Естественно для обычных сталей это напряжение считается разрушающей. При $T_0 = 500(^\circ C)$ значение $\Delta\ell_T = 0,02595$(см). Это на 85% больше чем аналогичное значение $\Delta\ell_T$ при $T_0 = 100(^\circ C)$. Здесь следует отметить, для того чтобы получить удлинение стержня в размере $\Delta\ell_T = 0,02595$(см) при ее растяжении необходимо было бы растянуть с силой $R = 5432,2$(кГ). При этом в сечениях стержня появилось бы растягивающее напряжение $\sigma = 1730\,(\text{кГ}/\text{см}^2)$) , которое является большим для обычных стальных конструкции. Необходимо отметить, что при $T_0 = 600(^\circ C)$ величина $\Delta\ell_T = 0,0297$(см) и она будет на $112,14\%$ больше чем $\Delta\ell_T$ при $T_0 = 100(^\circ C)$. Эквивалентная растягивающая сила было бы равно $R = 6217,2$(кГ) и соответствующее растягивающее напряжение будет равно $\sigma = 1980\,(\text{кГ}/\text{см}^2)$). Интересно

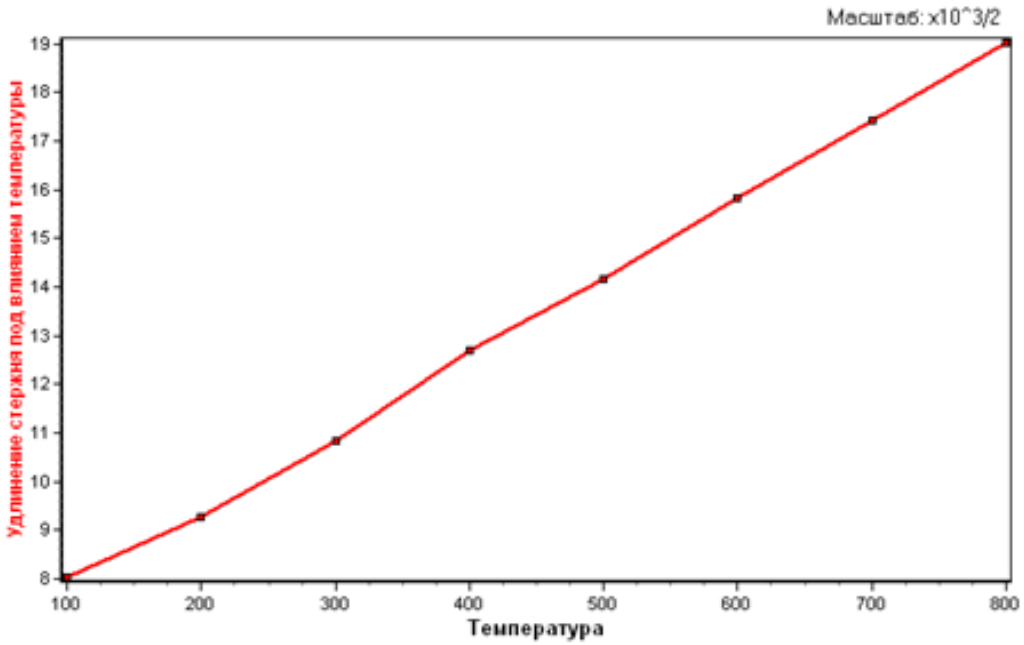

Рисунок 3 – Графическая зависимость между T_0 и $\Delta\ell_T$

отметить, что при увеличение значение температуры T_0 от $T_0 = 100(^\circ C)$ до $T_0 = 600(^\circ C)$, значения $\Delta\ell_T$, R, и σ увеличиваются одинаково на $112,14\%$.

4. Заключение

Получена разрешающая система уравнений, характеризующая теплофизическое состояние стержня, выполненной из жаропрочного сплава АМВ-300. Решая эту разрешающую систему уравнений определены поля температур, составляющие деформации и напряжения для конкретного примера. Вычислены также величины возникающего осевого усилия и температурное удлинение стержня.

Литература

[1] Л. Сегерлинд Применение метода конечных элементов. – М.: Мир, 1979. – 392 с.

[2] О. Зенкевич Метод конечных элементов в технике. – М.: Мир, 1975. – 541 с.

[3] A. Kudaykulov Algorithm For Parameters of the Dearing Elements of Oil Heating Installations.IMPACT: International Journal of Copmutational Sciences and Information Technology (IMPACT:IJCSSIT) @Impact Journals – 2015. –Vol. I. – P.13-20.

[4] Ф.Ф. Химушин Жаропрочные стали и сплавы. 2-ое переработанное и дополненное издания. – М.: Металлургия, 1969. – 749 с.

References

[1] L. Segerlind Primenenie metoda konechnih elementov. – M.: Mir, 1979. – 392 p.

[2] O. Zenkevich Metod konechnih elementov v tehnike. – M.: Mir, 1975. – 541 p.

[3] A. Kudaykulov Algorithm For Parameters of the Dearing Elements of Oil Heating Installations.IMPACT: International Journal of Copmutational Sciences and Information Technology (IMPACT:IJCSSIT) @Impact Journals – 2015. –Vol. I. – P.13-20.

[4] F.F. Himushin Zharoprochnie stali i splavi. 2-oe pererabotannoe i dopolnennoe izdaniya. – M.: Metallyrgiya, 1969. – 749 p.

УДК 519.62:624.131

Рысбайулы Б.*, Карашбаева Ж.О.

Международный университет информационных технологий,
Республика Казахстан, г. Алматы
* E-mail: b.rysbaiuly@mail.ru

Граничная обратная задача для переноса тепла и влаги в многослойной области

В работе изучается граничная обратная задача для системы уравнений переноса тепла и влаги. Рассматривается система уравнений описывающая совместного движения влаги и тепла в многослойной области. Определены граничные условия имеющие практические значения. Полученная начально-граничная задача записывается в безразмерной форме. После этого дается формулировка обратной граничной задачи в безразмерных переменных. В итоге получается квазилинейная обратная граничная задача. В настоящей работе выводится сопряженная система дифференциальных уравнений с частными производными. Определяются граничные и начальные условия сопряженной задачи. Устанавливаются связь между прямой и сопряженной задачи. Чтобы решить обратную граничную задачу строятся функционал. Из минимума этого функционала определяются искомые величины. Минимизируемый функционал записывается в безразмерной форме. Для расчета искомых граничных значений тепла и влаги разработан итерационный метод. Итерационные формулы записываются в явном виде и содержат решений прямой и сопряженной задачи. Итерация осуществляется так, чтобы функционал монотонно убывал в процесса вычислений. Сходимость итерационных процессов контролируется через малые управляющие функций. Проведены численные расчеты доказывающие пригодность разработанного метода. Критерием останова вычислительного процесса является достаточно малость значений безразмерного функционала.

Ключевые слова: влаг о тепло, прямая задача, сопряженная задача, обратная граничная задача, итерация, сходимость, функционал, безразмерные переменные.

Risbaiuly B., Karashbayeva Zh.O.

A boundary inverse problem for the process of heat and moisture transfer in multilayered region

The paper deals with the boundary inverse problem for a system of transfer equations for heat and moisture. A system of equations describe the joint movement of moisture and heat in the multilayer region. Boundary conditions of practical importance have defined. The resulting initial-boundary problem is written in dimensionless form. After that the formulation of the inverse boundary value problem in dimensionless variables was given. The result gives a quasi-linear inverse boundary problem. In the present work we have derived the adjoint system of differential equations with partial derivatives. The boundary and initial conditions of the adjoint problem were defined. A connection between the line and the adjoint problem was established. We have construct a functional for solving the inverse boundary problem. The unknown quantities are determined from the minimum of this functional. The minimizing functional is written in the dimensionless form. An iterative method was developed to calculate the unknown boundary heat and moisture values. Iteration formulas are written in an explicit form and contain the decisions of direct and the adjoint problem. The iteration is carried out so, that the functional decreases monotonically in the calculation process. The convergence of iterative processes is controlled by a small control functions. The numerical calculations proving the suitability of the developed method were conducted. The criterion for stopping the computing process is sufficiently smallness of the dimensionless values of the functional.

Key words: Moisture and heat, direct problem, adjoint problem, inverse boundary problem, iteration, convergence, functionality, dimensionless variables.

Рысбайұлы Б., Қарашбаева Ж.О.

Көп қатпарлы аймақтағы жылу мен ылғал тасымалы үшін шекаралық кері есеп

Жұмыста жылу мен ылғал тасымалы теңдеулер жүйесі үшін шекаралық кері есеп зерттелінеді. Көп қатпарлы аймақтағы ылғал мен жылу қозғалысын сипаттайтын теңдеулер жүйесі қарастырылады. Тәжірибелік маңызды шекаралық шарттар анықталған. Алынған бастапқы-шекаралық есеп өлшемсіз түрде жазылған. Осыдан кейін өлшемсіз айнымалылы шекаралық кері есептің берілуі көрсетілген. Соңында квазисызықты кері шекаралық есеп алынады. ұсынылып отырған жұмыста дербес туындылы түйіндес дифференциалдық теңдеулер жүйесі алынады. Түйіндес есептің шекаралық және бастапқы шарттары анықталады. Түйіндес және тура есеп арасындағы байланыс анықталады. Кері шекаралық есепті шешу үшін функционал құрылады. Осы функционал минимумынан қажетті мәндер табылады. Минималдаушы функционал өлшемсіз түрде жазылады. Жылу мен ылғалдың ізделініп отырған шекаралық мәндерін есептеу үшін итерациялық тәсіл табылған. Итерациялық формулалар анық түрде жазылған және тура және түйіндес есеп шешімінен тұрады. Итерация есептеу барысында функционалдың бірқалыпты кемітініндей етіп жүзеге асырылған. Итерациялық процестердің жинақтылығы кішкетай басқарушы функция арқылы бақыланады. Жасалынған тәсілдің қажеттілігін дәлелдейтін сандық есептеулер жүргізілген. Есептелініп отырған процестің тоқтату критерийі өлшемсіз функционалдың айтарлықтай кішкентай мәні болып табылады.
Түйін сөздер: ылғал мен жылу, тура есеп, түйіндес есеп, шекаралық кері есеп, итерация, жинақтылық, функционал, өлшемсіз айнымалылар.

1. Введение

Движение тепла изучаются отдельно предполагая, что состав влаги в изучаемой области медленно меняется либо остается постоянной. Прямые задачи теплопроводности достаточно хорошо изучены учеными различных стран [1-9]. Предполагая постоянства температуры почвы отдельно изучали процесс переноса влаги в почве в работах [10-19]. Различные виды обратных задач теплопроводности изучены в работах [20-25]. Обратные задачи влагопроводности изучались в работах [26-30]. Некоторые виды обратных задач теплопроводности и влагопроводности были изучены в работе [31-34]. Однако обратные задачи для полного уравнения совместного движения влаги и тепла все еще не изучены. Поэтому в настоящей работе изучается граничная обратная задача для полного уравнения тепло и масса переноса.

2. Постановка задачи

Взаимосвязанный перенос теплоты и массы в твердом теле описывается системой уравнений в частных производных вида [35]:

$$\frac{\partial\theta}{\partial t} = a_q\nabla^2\theta + \varepsilon R\frac{C_m}{C_q}\frac{\partial W}{\partial t}, \tag{1}$$

$$\frac{\partial W}{\partial t} = a_m\nabla^2 W + a_m\delta'\nabla^2\theta. \tag{2}$$

Граничные условия на поверхности тела имеют вид:

$$-\lambda_q(\nabla\theta) + q_q(t) - (1-\varepsilon)Rq_m(t) = 0, \tag{3}$$

$$\lambda_m(\nabla W) + \lambda_m\delta'(\nabla\theta) + q_m(\delta) = 0\ . \tag{4}$$

Первый член выражения (3) $-\lambda_q(\nabla\theta)$ представляет собой количество тепла, поступившего с поверхности внутрь тела теплопроводностью; второй член $q_q(t)$ соответствует количеству тепла, подведенному к поверхности тела; третий член $(1-\varepsilon)Rq_m(t)$ представляет собой количество тепла, затраченного на испарение жидкости. Если испарение происходит только внутри тела ($\varepsilon = 1$), то третий член обращается в ноль, в физическом понимании к поверхности тела подводится только пар. При ($\varepsilon = 0$) - к поверхности тела подводиться только жидкость (смывание платины водой), то испарение происходит только на поверхности тела. Выражение (4) представляет собой уравнение баланса массы вещества. Физический смысл состоит в том, что с поверхности тела в окружающую среду, отводится поток массы влаги $q_m(t)$, а к поверхности тела, влага подводится за счет градиентов потенциала массапереноса $\lambda_m(\nabla W)$, теплопереноса $\lambda_m\delta'(\nabla\theta)$.

Если задать поток тепла $q_q(t)$ и влаги $q_m(t)$, то граничные условия (3) и (4) представляют собой граничные условия второго рода.

Если задать закон взаимодействия тела с влажным воздухом:
Закон Ньютона:

$$q_q(t) = \alpha_q(\theta_! - \theta). \tag{5}$$

Закон Дальтона:

$$q_m(t) = \alpha_m(W_! - W), \tag{6}$$

и представить выражения (5) и (6) в условия (3) и (4), то получаются граничные условия первого рода.

Если коэффициент теплообмена α_q и α_qбольшие, то из граничных условий третьего рода получаются граничные условия первого рода.

Уравнения тепло и массопереноса для одномерной системы введены в [36] и имеют вид:

$$\frac{\partial\theta}{\partial t} = q_q\nabla^2\theta + \frac{\varepsilon r}{c\gamma}\frac{\partial U}{\partial t},$$

$$\frac{\partial U}{\partial t} = a_m\nabla^2 U + a_m\delta\nabla^2\theta.$$

Запишем граничные условия второго и третьего рода для возможных реальных ситуаций на «левой» границе слоя (индекс «с» относится к характеристикам среды с левой стороны слоя).

Рассмотрим трехслойный грунт, так как все внутренние слои описываются аналогично второму слою трехслойной стенки, математическая модель взаимосвязанного тепломассопереноса записывается в виде:

$$C\gamma\frac{\partial\theta}{\partial t} = \frac{\partial}{\partial z}\left(\lambda\frac{\partial\theta}{\partial z}\right) + \varepsilon r\frac{\partial W}{\partial t}, \tag{7}$$

$$\frac{\partial W}{\partial t} = \frac{\partial}{\partial t}\left(D_W \frac{\partial \overline{W}}{\partial z} + D_\theta \frac{\partial \theta}{\partial z}\right). \tag{8}$$

Здесь $\theta(z,t)$ и $W(z,t)$функции, характеризующие изменение температуры и потенциала массопереноса, z – текущие координаты по толщине слоя, t– время.

Граничные условия третьего рода для возможных реальных ситуаций на поверхности земли.

$$\lambda \frac{\partial \theta}{\partial z}\Big|_{z=H} = -\alpha\left(\theta - T_b(t)\right)|_{z=H} + (1-\varepsilon)\, r\alpha_m \left(W - W_b(t)\right)|_{z=H}, \tag{9}$$

$$\left(D_w \frac{\partial \overline{W}}{\partial z} + D_\theta \frac{\partial \theta}{\partial z}\right)\Big|_{z=n} = -\alpha_m \left(W - W_b(t)\right)|_{z=H}. \tag{10}$$

На нижней границе области $z = 0$ ставятся условия

$$\theta(z,t)\,\big|_{z=0} = T_1(t), \qquad \overline{W}(z,t)\big|_{z=0} = \overline{W_1(t)}. \tag{11}$$

в точках перехода от одного слоя к другому ставятся условия

$$[\theta(z,t)]_{h_i} = 0, \qquad \left[\overline{W}(z,t)\right]_{h_i} = 0, \qquad i = 1,2, \tag{12}$$

$$\left[\lambda \frac{\partial \theta}{\partial z}\right]_{z=h_i} = 0, \qquad \left[D_w \frac{\partial W}{\partial z} + D_\theta \frac{\partial \theta}{\partial t}\right]_{z=h_i} = 0. \tag{13}$$

Кроме этого задаются измеренные значения температуры и потенциала влаги на поверхности земли

$$T_g(t), \qquad \overline{W}_g(t).$$

Требуется определить распределение температуры и влаги $Q(z,t)$, $\overline{\mathrm{W}}(z,t)$ и значения температуры и влаги на границе области $T_1(t)$, $\overline{W}_1(t)$.

Решение задачи (7) – (13) ищется в области $Q = (0,H)\times(0,t_{\max})$.

3. Задача в безразмерных переменных

Введем обозначения:

$$\Delta\theta = \theta_b - \theta_*, \qquad \Delta\overline{\mathrm{W}} = \overline{W_*} - \overline{W_b},$$

$$T = \frac{\theta - \theta_*}{\Delta\theta}, \qquad \mathrm{U} = \frac{\overline{\mathrm{W}}_* - \overline{W}}{\Delta W}.$$

Индекс «b» относится к характеристикам внутренней среды, * выбирается в соответствии с конкретной задачей (в рассматриваемых нами задачах – это температура и потенциал переноса массы на правой границе соответствующего слоя), $x = \frac{z}{H}$ безразмерная координата, $F_0 = \frac{\alpha t}{H^2}$ безразмерное время, $a = \frac{\lambda}{c\gamma}$.

Преобразуем уравнение (7) и (8):

$$\frac{\partial T(x,F_0)}{\partial F_0}\cdot\frac{a\Delta T}{H^2}=\frac{0\Delta"}{H^2}\ \frac{\partial^{2"}(E,F_0)}{\partial x^2}-\frac{\varepsilon r}{c\gamma}\cdot\ \frac{\partial \mathrm{u}\,(\mathrm{x},\ \mathrm{F}_0)}{\partial \mathrm{F}_0}\cdot\frac{a\Delta\overline{W}}{H^2},$$

$$-\frac{\partial U(x,F_0)}{\partial F_0}\cdot\frac{a\Delta\overline{W}}{H^2}=-\frac{D_w\Delta W}{H^2}\ \cdot\frac{\partial^2 U\,(x,F_0)}{\partial x^2}+\frac{D_\theta\Delta\theta}{H^2}\cdot\ \frac{\partial^2 T\,(x,F_0)}{\partial x^2}.$$

Или

$$\frac{\partial T\,(x,F_0)}{\partial F_0}=\frac{\partial^2 T\,(x,F_0)}{\partial x^2}\cdot\frac{D_W}{a}-\frac{D_W\delta\Delta\theta}{a\Delta W}\ \frac{\partial U\,(x,F_0)}{\partial F_0},$$

$$\frac{\partial U\,(x,F_0)}{\partial F_0}=\alpha_U\frac{\partial^2 U\,(x,F_0)}{\partial x^2}-\alpha_n P_n\ \frac{\partial^2 T\,(x,F_0)}{\partial x^2}.$$

Итак, уравнений (7) и (8) приняли вид:

$$\begin{cases}\frac{\partial T(x,F_0)}{\partial F_0}=\frac{\partial^2 T(x,F_0)}{\partial x^2}-K_0^*\frac{\partial U(x,F_0)}{\partial F_0},\\ \frac{\partial U(x,F_0)}{\partial F_0}=\alpha_U\frac{\partial^2 U(x,F_0)}{\partial x^2}-\alpha_u P_n\ \frac{\partial^2 T(x,F_0)}{\partial x^2}\end{cases}\tag{14}$$

На поверхности земли имеют место условия 3 – го рода:

$$\lambda\frac{\partial\theta\,(H,t)}{\partial z}+\alpha\,(\theta\,(H,t)-T_b(t))-(1-\varepsilon)\,r\alpha_w\,(W\,(H,t)-W_b\,(t))=0,\tag{15}$$

$$D_w\frac{\partial W\,(H,t)}{\partial z}+D_w\delta\frac{\partial\theta\,(H,t)}{\partial z}-\alpha_w\,(W\,(H,t)-W_b(t))=0.\tag{16}$$

Приведем (15) в безразмерную форму:

$$\lambda\frac{\partial T\,(H,F_0)}{\partial x}\cdot\frac{\Delta\theta}{H}+\alpha\left[T\,(H,F_0)-\bar{T}_b\,(F_0)\right]-(1-\varepsilon)\,r\alpha_W\left[U\,(H,F_0)-W_b\,(F_0)\right]=0.$$

Здесь $\Delta W=-W_b(0)+W_1,\quad \Delta\theta=\mathrm{T_b}(0)-T_1,$

$$\overline{T}_b\,(t)=\frac{T_b\,(t)-T_1}{\Delta\theta},\quad \mathrm{W_b}\,(t)=\frac{-W_b\,(t)+W_1}{\Delta W}.$$

В итоге граничное условие (15) записывается в виде:

$$\frac{\partial T\left(H,F_0\right)}{\partial x}+Bi\left(T\left(H,F_0\right)-\overline{T_b}\left(F_0\right)\right)-p\left(U\left(H,F_0\right)-\overline{W}_b\left(F_0\right)\right)=0,$$

где

$$\mathrm{p}=\left(1-\varepsilon\right)BiKo\cdot\alpha_U.$$

Приведем в безразмерную форму, граничное условие (16):

$$-D_w\frac{\partial U\left(H,F_0\right)}{\partial x}\quad\frac{\Delta W}{H}-D_w\delta\frac{\partial T\left(H,F_0\right)}{\partial x}\cdot\frac{\Delta\theta}{H}+\alpha_w\left(U\left(H,F_0\right)-\overline{W}_b\left(F_0\right)\right)\Delta W=0.$$

В итоге граничное условие (16) записывается в виде:

$$\frac{\partial U(1,F_0)}{\partial x}+P_n\cdot\frac{\partial T(1,F_0)}{\partial x}+Bi,w\left(U(1,F_0)-\underset{b}{\bar{W}}(F_0)\right)=0.$$

Итак, после введения безразмерной формы система (7) - (13) записывается в виде:

$$\frac{\partial T(x,F_0)}{\partial F_0}=\frac{\partial^2T(x,F_0)}{\partial x^2}-K_0^*\frac{\partial U(x,F_0)}{\partial F_0},\tag{17}$$

$$\frac{\partial U(x,F_0)}{\partial F_0}=\alpha_U\frac{\partial^2U(x,F_0)}{\partial x^2}-\alpha_U\cdot P_n\frac{\partial^2T(x,F_0)}{\partial x^2},\tag{18}$$

$$\frac{\partial T(1,F_0)}{\partial x}+Bi\left(T(1,F_0)-\underset{b}{\bar{T}}(F_0)\right)-P_n\left(U(1,F_0)-\underset{b}{\bar{W}}(F_0)\right)=0,P=\left(1-\varepsilon\right)Bi\cdot K_0^*\alpha U,\tag{19}$$

$$\frac{\partial U(1,F_0)}{\partial x}+P_n\frac{\partial T(1,F_0)}{\partial x}+Bi,u\left(U(1,F_0)-\underset{b}{\bar{W}}(F_0)\right)=0,\tag{20}$$

$$T(0,F_0)=0,U(0,F_0)=0,\tag{21}$$

$$T(x,0)=T_0(x),U(x,0)=U_0(x).\tag{22}$$

Введены следующие параметры:
F_0 - критерий Фурье (теплообменный),
$K_0^*=\frac{\varepsilon r}{C\gamma}\cdot\frac{\Delta W}{\Delta\theta}$ - модифицированный критерий Коссовича;
$P_n=\frac{\delta\Delta\theta}{\Delta W}$ - критерий Паскова;
$\alpha_U=\frac{\alpha}{D_W}$ - критерий взаимосвязи массо и теплопереноса (критерий инерционности),

4. Построение сопряженной задачи

Измеренные значения температуры и влаги $T_g(t)$, $\overline{W}_g(t)$ в безразмерном виде записываются так:

$$\bar{W}_g(t) = \frac{W_1 - \bar{W}(t)}{\Delta W}, \bar{T}_g(t) = \frac{T(t) - T_1}{\Delta T}.$$

Поставленная задача решается итерационным методом. Сначала задаются начальные приближения: $T_0(z,n)$, $U_0(z,n)$, при $n=0$,
а следующие приближения определяются из минимума функционалов:

$$J(T_0, U_0) = \int_0^{F_{0\max}} \left(T(1,F_0) - \bar{T}_g(F_0)\right)^2 dF_0 + \int_0^{F_{0\max}} \left(U(1,F_0) - \bar{W}_g(F_0)\right)^2 dF_0. \quad (23)$$

Соответствующие решения задачи (17) - (18) итерации n и $n+1$ обозначим через:

$$T(x,F_0;n) = T_n(x,F_0), U(x,F_0;n) = U_n(x,F_0),$$

$$T(x,F_0;n+1) = T_{n+1}(x,F_0), U(x,F_0;n+1) = U_{n+1}(x,F_0).$$

Тогда для функций
$\Delta T(x,F_0) = T_{n+1}(x,F_0) - T_n(x,F_0)$, $\Delta U(x,F_0) = U_{n+1}(x,F_0) - U_n(x,F_0)$ составляется задача:

$$\frac{\partial \Delta T(x,F_0)}{\partial F_0} = \frac{\partial^2 \Delta T(x,F_0)}{\partial x^2} - K_0^* \frac{\partial \Delta U(x,F_0)}{\partial F_0}, \quad (24)$$

$$\frac{\partial \Delta U(x,F_0)}{\partial F_0} = \alpha_U \frac{\partial^2 \Delta U(x,F_0)}{\partial x^2} - \alpha_U P_n \frac{\partial^2 \Delta T(x,F_0)}{\partial x^2}, \quad (25)$$

$$\frac{\partial \Delta T(1,F_0)}{\partial x} + Bi \Delta T(1,F_0) - P \cdot \Delta U(1,F_0) = 0, \quad (26)$$

$$\frac{\partial \Delta U(1,F_0)}{\partial F_0} + P_n \frac{\partial \Delta T(1,F_0)}{\partial x} - B_{i,u} \Delta U(1,F_0) = 0, \quad (27)$$

$$\Delta T(0,F_0) = 0, \Delta U(0,F_0) = 0, \quad (28)$$

$$\Delta T(x,0) = \Delta T_0(x), \Delta U(x,0) = \Delta U_0(x), \quad (29)$$

$$[\Delta T]_{x=x_i} = 0, [\Delta U]_{x=x_i} = 0, x_i = \frac{h_i}{H}, i = 1,2,...,N, \quad (30)$$

$$\left[\frac{\partial \Delta T(x,F_0)}{\partial x}\right]_{x=x_i} = 0, \left[\alpha_U \frac{\partial \Delta U(x,F_0)}{\partial x} - \alpha_u P_h \frac{\partial \Delta T(x,F_0)}{\partial x}\right]_{x=x_i} = 0. \quad (31)$$

Умножим (24) на произвольную функцию $\psi(z, F_0)$ и проинтегрируем по всей области $Q = (0,1) \times (0, F_{0\max})$. После однократного интегрирования по частям по z и t имеем равенство

$$(\Delta T, \psi)|_{F_0=0}^{F_0=F_{0\max}} - \left(\Delta T, \frac{\partial \psi}{\partial t}\right) = \left(\frac{\partial \Delta T}{\partial t}, \psi\right)\Big|_{x=0}^{x=1} - \left(\frac{\partial \Delta T}{\partial t}, \frac{\partial \psi}{\partial t}\right) -$$

$$- (K_0^* \Delta U, \psi)|_{F_0=0}^{F_0=F_{0\max}} + \left(K_0^* \Delta U, \frac{\partial \psi}{\partial t}\right). \tag{32}$$

Здесь введены обозначения:

$$(f, g) = \int_0^{F_{0\max}} dF_0 \int_0^1 f(x, F_0) g(x, F_0) dx,$$

$$(f, g)|_{x=1} = \int_0^{F_{0\max}} f(1, t) g(1, t) dt,$$

$$(f, g)|_{F_0=F_{0\max}} = \int_0^1 f(x, F_{0\max}) g(x, F_{0\max}) dx.$$

Положим, что $\psi(x, F_{0\max}) = 0$, $\psi(0, F_0) = 0$. Учитывая начально-граничные условия (28), (29) из (32) выводим, что

$$-\left(\Delta T, \frac{\partial \psi}{\partial t}\right) = -(Bi\Delta T - P\Delta U, \psi)|_{x=1} - \left(\frac{\partial \Delta T}{\partial x}, \frac{\partial \psi}{\partial x}\right) +$$

$$+\left(K_0^* \Delta U, \frac{\partial \psi}{\partial t}\right) - (K_0^* \Delta U, \psi)|_{F_0=0} - (\Delta T, \psi)|_{F_0=0}.$$

Второе слагаемое на правой части знака равенства снова интегрируется по частям по переменной z. Принимая во внимание (28) имеем равенство

$$-\left(\Delta T, \frac{\partial \psi}{\partial t} + \frac{\partial^2 \psi}{\partial x^2}\right) = -(Bi\Delta T - P\Delta U, \psi)|_{x=1} - \left(\Delta T, \frac{\partial \psi}{\partial x}\right)\Big|_{x=1} +$$

$$+\left(K_0^* \Delta U, \frac{\partial \psi}{\partial t}\right) - (K_0^* \Delta U, \psi)|_{F_0=0} - (\Delta T, \psi)|_{F_0=0}.$$

Теперь, умножаем (25) на произвольную функцию $\eta(x, F_0)$ и интегрируем по x от 0 до 1, а по F_0 от 0 до $F_{0\max}$. После однократного применения формулы по частям, по x и F_0 составляется равенство

$$-(\Delta U, \eta)|_{F_0=0}^{F_0=F_{0\max}} - \left(\Delta U, \frac{\partial \eta}{\partial t}\right) = \left(\alpha_U \frac{\partial \Delta U}{\partial x}, \eta\right)\Big|_{x=0}^{x=1} - \left(\alpha_U \frac{\partial \Delta U}{\partial x}, \eta\right)\Big|_{x=0}^{x=1} -$$

$$-\left(\frac{\partial \Delta U}{\partial x}, \alpha_U \frac{\partial \eta}{\partial x}\right) - \left(\alpha_U P_n \frac{\partial \Delta T}{\partial x}, \eta\right)\Big|_{x=0}^{x=1} + \left(\frac{\partial \Delta T}{\partial x}, \alpha_U P_n \frac{\partial \eta}{\partial x}\right). \tag{33}$$

Положим $\eta(x, F_{0\max}) = 0$, $\eta(0, F_0) = 0$. Учитывая (27) выводим, что

$$-\left(\Delta U, \frac{\partial \eta}{\partial t} + \alpha_U \frac{\partial^2 \eta}{\partial x^2}\right) = -\left(\alpha_U \Delta U, \eta\right)|_{x=1} - \left(\Delta U, \alpha U \frac{\partial \eta}{\partial x}, \right)\Big|_{x=1} + \left(\Delta T, \frac{\partial}{\partial x}(\alpha_U P_n \frac{\partial \eta}{\partial x})\right) +$$

$$+ \left(\Delta T, \alpha_U P_n \frac{\partial \eta}{\partial x}\right)\Big|_{x=1} - (\Delta U, \eta)|_{F_0=0}. \tag{34}$$

Складываем (33) и (34). Группируем подобные слагаемые, тогда

$$-\left(\Delta T, \frac{\partial \psi}{\partial t} + \frac{\partial^2 \psi}{\partial x^2} + \frac{\partial}{\partial x}(\alpha_U P_n \frac{\partial \eta}{\partial x})\right) - \left(\Delta U, \frac{\partial \eta}{\partial t} + \frac{\partial}{\partial x}\left(\alpha_U \frac{\partial \eta}{\partial x}\right) - K_0^* \frac{\partial \psi}{\partial t}\right) =$$

$$= -\left(\Delta T, Bi\psi + \frac{\partial \psi}{\partial x} + \alpha_U P_n \frac{\partial \eta}{\partial x}\right)\Big|_{x=1} + \left(\Delta U, P\psi - \alpha_U \eta - \alpha_U \frac{\partial \eta}{\partial x}\right)\Big|_{x=1} -$$

$$- (\Delta U, K_0^* \psi + \eta)|_{F_0=0} - (\Delta T, \psi)|_{F_0=0}.$$

Функции $\psi(x, F_0)$ и $\eta(x, F_0)$ подбираются из уравнений

$$\frac{\partial \psi}{\partial t} + \frac{\partial^2 \psi}{\partial x^2} + \frac{\partial}{\partial x}(\alpha_U P_n \frac{\partial \eta}{\partial x}) = 0,$$

$$\frac{\partial \eta}{\partial t} + \frac{\partial}{\partial x}\left(\alpha_U \frac{\partial \eta}{\partial x}\right) - K_0^* \frac{\partial \psi}{\partial t} = 0.$$

И ставятся граничные условия

$$\left(Bi\psi + \frac{\partial \psi}{\partial x} + \alpha_U P_n \frac{\partial \eta}{\partial x}\right)\Big|_{x=1} = 2\left(T(1, F_0) - \underset{g}{\bar{T}}(F_0)\right),$$

$$\left(\alpha U \eta + \alpha_U \frac{\partial \eta}{\partial x} - P\psi\right)\Big|_{x=1} = 2\left(U(1, F_0) - \underset{g}{\bar{W}}(F_0)\right).$$

После этого (34) представляется в виде

$$2\left(\Delta T, T(1, F_0) - \underset{g}{\bar{T}}(F_0)\right) + 2\left(\Delta U, U(1, F_0) - \underset{g}{\bar{W}}(F_0)\right) =$$

$$= -(\Delta T, \psi)|_{F_0=0} - (\Delta U, K_0^* \psi + \eta)|_{F_0=0}. \tag{35}$$

В ходе проведенных вычислений составлена сопряженная задача системы (24) - (31):

$$\frac{\partial \psi}{\partial t} + \frac{\partial^2 \psi}{\partial x^2} + \frac{\partial}{\partial x}(\alpha_U P_n \frac{\partial \eta}{\partial x}) = 0,$$

$$\frac{\partial \eta}{\partial t} + \frac{\partial}{\partial x}\left(\alpha_U \frac{\partial \eta}{\partial x}\right) - K_0^* \frac{\partial \psi}{\partial t} = 0, \left(Bi\psi + \frac{\partial \psi}{\partial x} + \alpha_U P_n \frac{\partial \eta}{\partial x}\right)\Big|_{x=1} = 2\left(T(1, F_0) - \underset{g}{\bar{T}}(F_0)\right),$$

$$\left(\alpha U \eta + \alpha_U \frac{\partial \eta}{\partial x} - P\psi\right)\Big|_{x=1} = 2\left(U(1, F_0) - \underset{g}{\bar{W}}(F_0)\right),$$

$$\psi(x, F_{0\max}) = 0, \eta(x, F_{0\max}) = 0,$$

$\psi(0, F_0) = 0, \eta(0, F_0) = 0.$

5. Итерационная формула

Приращение функционала (23) от итераций n до итераций $n+1$ записывается в виде:

$$J_{n+1}(T_0, U_0) - J_n(T_0, U_0) = 2\int_0^{F_{0\max}} \left(T(1, F_0) - \bar{T}_g(F_0)\right) \Delta T(1, F_0)\, dF_0 +$$

$$+2\int_0^{F_{0\max}} \left(U(1, F_0) - \bar{W}_g(F_0)\right) \Delta U(1, F_0)\, dF_0 + \int_0^{F_{0\max}} (\Delta T(1, F_0))^2\, dF_0 +$$

$$+ \int_0^{F_{0\max}} (\Delta U(1, F_0))^2\, dF_0.$$

На основе (35) последнее равенство записывается в виде:

$$J_{n+1}(T_0, U_0) - J_n(T_0, U_0) = -(\Delta T, \psi)|_{F_0=0} - (\Delta U, K_0^*\psi + \eta)|_{F_0=0} +$$

$$+ \int_0^{F_{0\max}} (\Delta T(1, F_0))^2\, dF_0 + \int_0^{F_{0\max}} (\Delta U(1, F_0))^2\, dF_0.$$

Третье и четвертые слогаемые на правой части знака равенство имеют второй порядок малости. Поэтому знак левой части знака равенство определяется знаком первой и второй слогаемой стоящее на правой части знака равенства. Мы хотим, чтобы функционал от итераций к итераций монотонно уменьшался. Поэтому

$$\Delta T = -\beta_T \int_0^1 \psi(x, 0)\, dx,$$

$$\Delta U = -\beta_U \int_0^1 (K_0^*\psi(x, 0) + \eta(x, 0))\, dx.$$

6. Заключение

На основе модели переноса влаги и тепла многослойной области построена вспомогательная дифференциальная задача. Из нее после некоторых преобразовании выводится сопряженная задача. Из решений сопряженной и прямой задачи составляются итерационные формулы для значений температуры и влаги на границе области. В будущем планируется решать коэффициентные обратные задачи для системы тепло и влага переноса в многослойной области.

Литература

[1] Low, P.F., Anderson, D.M., Hoekstra, P Some Thermodynamic Relationships for Soils at or Below the Freezing Point. 1. Freezing Point Depression and Heat Capacity. - Water Resources Research. 4. – 1968. – 379-394 p.

[2] Li, Q., S. Sun, and Q. Dai The numerical scheme development of a simplified frozen soil model, Adv. Atmos. Sci., 26(5). – 2009. – 940–950 p.

[3] Mordovian, S.D., Pavlov, B.N., Petrov E.E. Mathematical models of a freezing and thawing of frozen soil. Yakutsk , Science and education. – - 1996. – 52-56 p.

[4] Rysbaiuly, B., Adamov, A.A. Investigation of heat phase zone multilayer ground. Vestnik NAN RK. 4. – 2007. – 30-33 p.

[5] Gardner W.R. Mathematics of isothermal water conduction in unsaturated soil. Highway Research board, S.R. 40. –1958. – 78-87p.

[6] Collis-George N., Henin S., Kelley J. A. Etude du mecanisme de la dessi-cation des sols par evaporation. C. R. Ac. Sc. Sc., Vol. – 1963. – 257p.

[7] Hallaire M. Le potenciel efficace de l'eau daus le sol en régime de dessechement. L'eau et la production végétale, Institut National de la Recherche Agronomique. no. – 1964. – 9p.

[8] Geiger S. L. Infiltration in homogeneous sands and a mechanistic model of unstable flow. Soil Sci. Soc. Am. J. Vol. 64. – 2000. – 460-469p.

[9] Golovanov A. I. Mathematical model of the moisture transfer in landscaped catens. Environmental engineering and management, Moscow MGUE. Part II. –2005. – 3-11p. ISBN 5-89231-153-8p.

[10] Rezanezhad F., Vogel H., Roth K. Experimental study of fingered flow through initially dry sand. Hydrol. Earth Syst. Sci. Discuss. no. 3. –2006. – 2595-2620p.

[11] DiCarlo D. A. Experimental measurements of saturation overshoot on infiltration. Water Resour. Res. Vol. 40, no. 4. – 2004. – 147-172p.

[12] DiCarlo D. A. Capillary pressure overshoot as a function of imbibitions flux and initial water content. Water Resour. Res.,Vol. 43. – 2007. – 1-7 p.

[13] Kabanikhin, S.I., Bektemesov, M.A., Nechaev, D.V. Optimization method for continuation of solution to two dimensional elliptic equation. Inverse Problems in Engineering Mechanics, Novosibirsk. – 2003. – 447-456 p.

[14] Hasanee, A.D. Lesnic, D. Determination of a time-dependent heat source from nonlocal boundary conditions. Engineering Analysis with Boundary Elements. 37. – 2013. – 936-956p.

[15] Rysbaiuly B. Newton's method to solve the problem of heat transfer in the freezing soil. France, Paris, Pensee Journal. Volume 76, Issue 1. – 261-275 pp.

[16] Rysbaiuly B., Baymankulov A.T. Variational-difference method for determining the diffusion coefficient of soil water. International Journal of Academic Research. № 5. – 2010. – 84-91p.

[17] Rysbaiuly B. Mathematical properties of the iterative method to calculate the coefficient of thermal conductivity of multilayer ground. Wulfenia Journal, Austria. Volume 20, Issue 12. – 2014.

[18] Silin D. B., Patzek T. W. On Barenblatt's Model of Spontaneous Coun-tercurrent Imbibition. Transport in Porous Media. no. 54. – 2004. – 297-322p.

[19] Chapwanya M., Stockie J. M. Numerical simulations of gravity-driven fingering in unsaturated porous media using a nonequilibrium model. Water Resources Research. Vol. 46, no. 9. – 2010. – 1-14p.

[20] Gallant, J. C. Hutchinson M. F. A differential equation for specific catchment area. Water Resour. Res.,Vol. 47. -2011 W05535, doi:10.1029/2009WR008540

[21] Martynov, G.A. To a conclusion of the main equation of heat conductivity for freezing-through soil. Materials to doctrine bases about frozen zones of crust. Publishing house of Academy of Sciences of the USSR. 4. – 1956. – 55-59 p.

[22] Amiaz, Y., S. Sorek, Y. Enzel, O. Dahan. Solute transport in the vadose zone and groundwater during flash floods. Water Resour. Res.,Vol. 47. – 2011. W10513, doi10.1029/2011WR010747.

[23] Рысбайулы Б., Биртаева З.Б. Вариационно–разностный метод определения коэффициента теплопроводности многослойного грунта с учетом конвекции влаги// Вестник ВКГТУ им. Д.Серикбаева. №2. – 2010. – 135-139с.

[24] Рысбайулы Б., Биртаева З.Б. Сходимость итерационного процесса для определения коэффициента теплопроводности многослойного грунта с учетом конвекции влаги// ДАН НАН РК. №4. – 2010. – 37-41с.

[25] S.V. Fedosov, A.M. Ibragimov, A.V. Gushchin Effect of heat and humidity processing mode of concrete enclosing constructions and products on their strength, Construction Materials. 9. – 2006. – 7-8 p.

[26] B. Rysbaiuly, A. Baimankulov Development and justification of the method of calculation the capillary diffusion of the soil, Wulfenia Journal. Volume 20, Issue 12. – 2014. – 483-500p.

References

[1] Low, P.F., Anderson, D.M., Hoekstra, P Some Thermodynamic Relationships for Soils at or Below the Freezing Point. 1. Freezing Point Depression and Heat Capacity. - Water Resources Research. 4. – 1968. – 379-394 p.

[2] Li, Q., S. Sun, and Q. Dai The numerical scheme development of a simplified frozen soil model, Adv. Atmos. Sci., 26(5). – 2009. – 940–950 p.

[3] Mordovian, S.D., Pavlov, B.N., Petrov E.E. Mathematical models of a freezing and thawing of frozen soil. Yakutsk , Science and education. – - 1996. – 52-56 p.

[4] Rysbaiuly, B., Adamov, A.A. Investigation of heat phase zone multilayer ground. Vestnik NAN RK. 4. – 2007. – 30-33 p.

[5] Gardner W.R. Mathematics of isothermal water conduction in unsaturated soil. Highway Research board, S.R. 40. –1958. – 78-87p.

[6] Collis-George N., Henin S., Kelley J. A. Etude du mecanisme de la dessi-cation des sols par evaporation. C. R. Ac. Sc. Sc., Vol. – 1963. – 257p.

[7] Hallaire M. Le potenciel efficace de l'eau daus le sol en régime de dessechement. L'eau et la production végétale, Institut National de la Recherche Agronomique. no. – 1964. – 9p.

[8] Geiger S. L. Infiltration in homogeneous sands and a mechanistic model of unstable flow. Soil Sci. Soc. Am. J. Vol. 64. – 2000. – 460-469p.

[9] Golovanov A. I. Mathematical model of the moisture transfer in landscaped catens. Environmental engineering and management, Moscow MGUE. Part II. –2005. – 3-11p. ISBN 5-89231-153-8p.

[10] Rezanezhad F., Vogel H., Roth K. Experimental study of fingered flow through initially dry sand. Hydrol. Earth Syst. Sci. Discuss. no. 3. –2006. – 2595-2620p.

[11] DiCarlo D. A. Experimental measurements of saturation overshoot on infiltration.Water Resour. Res.Vol. 40, no. 4. – 2004. – 147-172p.

[12] DiCarlo D. A. Capillary pressure overshoot as a function of imbibitions flux and initial water content. Water Resour. Res.,Vol. 43. – 2007. – 1-7 p.

[13] Kabanikhin, S.I., Bektemesov, M.A., Nechaev, D.V. Optimization method for continuation of solution to two dimensional elliptic equation. Inverse Problems in Engineering Mechanics, Novosibirsk. – 2003. – 447-456 p.

[14] Hasanee, A.D. Lesnic, D. Determination of a time-dependent heat source from nonlocal boundary conditions. Engineering Analysis with Boundary Elements. 37. – 2013. – 936-956p.

[15] Rysbaiuly B. Newton's method to solve the problem of heat transfer in the freezing soil. France, Paris, Pensee Journal. Volume 76, Issue 1. – 261-275 pp.

[16] Rysbaiuly B., Baymankulov A.T. Variational-difference method for determining the diffusion coefficient of soil water. International Journal of Academic Research. № 5. – 2010. – 84-91p.

[17] Rysbaiuly B. Mathematical properties of the iterative method to calculate the coefficient of thermal conductivity of multilayer ground. Wulfenia Journal, Austria. Volume 20, Issue 12. – 2014.

[18] Silin D. B., Patzek T. W. On Barenblatt's Model of Spontaneous Coun-tercurrent Imbibition. Transport in Porous Media. no. 54. – 2004. – 297-322p.

[19] Chapwanya M., Stockie J. M. Numerical simulations of gravity-driven fingering in unsaturated porous media using a nonequilibrium model. Water Resources Research. Vol. 46, no. 9. – 2010. – 1-14p.

[20] Gallant, J. C. Hutchinson M. F. A differential equation for specific catchment area. Water Resour. Res.,Vol. 47. -2011 W05535, doi:10.1029/2009WR008540

[21] Martynov, G.A. To a conclusion of the main equation of heat conductivity for freezing-through soil. Materials to doctrine bases about frozen zones of crust. Publishing house of Academy of Sciences of the USSR. 4. – 1956. – 55-59 p.

[22] Amiaz, Y., S. Sorek, Y. Enzel, O. Dahan. Solute transport in the vadose zone and groundwater during flash floods. Water Resour. Res.,Vol. 47. – 2011. W10513, doi10.1029/2011WR010747.

[23] B. Rysbaiuly, Z.B. Birtayeva Variational-difference method for determining the thermal conductivity of a multilayer soil, taking into account convection moisture // Bulletin of EKSTU named after. D.Serikbaev. №2. – 2010. – 135-139p.

[24] B. Rysbaiuly, Z.B. Birtayeva Convergence of the iterative process to determine the thermal conductivity of a multilayer soil, taking into account convection moisture // DAN NAS RK.. №4. – 2010. – 37-41p.

[25] S.V. Fedosov, A.M. Ibragimov, A.V. Gushchin Effect of heat and humidity processing mode of concrete enclosing constructions and products on their strength, Construction Materials. 9. – 2006. – 7-8 p.

[26] B. Rysbaiuly, A. Baimankulov Development and justification of the method of calculation the capillary diffusion of the soil, Wulfenia Journal. Volume 20, Issue 12. – 2014. – 483-500p.

УДК 004.421

Терехов А.Г.*, Калимолдаев М.Н., Пак И.Т.

Институт информационных и вычислительных технологий КН МОН РК,
Республика Казахстан, г. Алматы
* E-mail: e-mail: aterekhov1@yandex.ru

Компьютерное моделирование и спутниковые данные в задачах мониторинга некоторых гидрологических параметров в бассейнах трансграничных рек, на примере китайской части бассейна реки Иле

Гидрологический мониторинг бассейнов трансграничных рек имеет проблемы полноты и представительности информации. Спутниковая съемка может обеспечить часть объективной информации о состоянии водных объектов вне зависимости от их территориальной принадлежности. Наиболее интересными гидротехническими объектами являются искусственные водохранилища на реках ледового и снежно-ледового питания с существенными сезонными вариациями объёмов хранения воды, построенные после 2000 года. Цифровая модель рельефа SRTM-2000 Elevation для таких водохранилищ представляет собой батиметрию. Мониторинг площади водного зеркала совместно с батиметрией дна водохранилища позволяет рассчитывать суммарный водный баланс системы «река-водохранилище», что способно дополнять гидрологический мониторинг трансграничных бассейнов. На примере бассейна реки Иле (территория Казахстана и КНР) рассмотрен суммарный водный баланс Капчагайского водохранилища, построенного в 2005 году на реке Текес (КНР). Река Текес, основной приток реки Иле, со средним объёмом стока около 250 м^3/сек, имеет снежно-ледовое питание и формируется в горах внутреннего Тянь-Шаня. На основе 157 снимков LANDSAT-5,7,8 периода 2005-2016 гг. и ЦМР дна определены основные гидрологические характеристики водохранилища, параметры суммарного водного баланса системы «река-водохранилище» и расходы воды в основных притоках р. Иле.

Ключевые слова: методы дистанционного зондирования, снимки LANDSAT, площадь водного зеркала, гидрологический режим водохранилища, цифровая модель рельефа, расход воды в реке.

Terekhov A.G., Kalimoldaev M.N., Pak I.T.

The computer modeling and satellite data in monitoring the problems of some hydrological parameter in transboundary river pool, the example of the Chinese part of the pool of river Ili

The hydrological monitoring of the trans-boundary river basins often has the problems of the informational completeness. There are the problems of the access to the operational hydrological information for the objects on the foreigh territory. The satellite data can to provide the part of the objective hydrology information of the total basin territory. The artificial reservoirs on the rivers with the ice and snow/ice supply are most interested. These objects are characterized by the significant seasonal variations of the water storage. The SRTM-2000 Elevation model gives the bathymetry information to the reservoirs which were built since 2000 year. The DEM reservoir bathymetry and LANDSAT monitoring of the water mirror surface can be use for the numerical estimation of the total water balance between the river runoff and reservoir water storage. This information is an important part of the hydrological basin monitoring. For example, the river Ile basin (the territory of Kazakhstan and China) was analyzed. The river Tekes (the main tributary of the river Ile) with average annual water flow is about 250 m^3 / sec is formed in the Inner Tien Shan Mountains. The artificial Kapchagay reservoir on river Tekes was built in 2005. The 157 images of LANDSAT-5,7,8 (2005-2016 years) were processed to monitor of the water mirror surface of the Kapchagay reservoir. The reservoir DEM bathymetry and water mirror area were used for the diagnostics of the total water balance between river Teres runoff, the Kapchagay reservoir water storage and the discharge of the river Kas and Tekes.

Key words: remote sensing, LANDSAT images, water mirror area, hydrological regime of reservoir, digital elevation model, river discharge.

Терехов А.Г., Қалимолдаев М.Н., Пак И.Т.

Мысал ретінде Іле өзені хауызының Қытай бөлігінің бірнеше гидрологиялық параметрлер трансшекралық өзен хауыздарының компьютерлік моделдеуі мен серіктік мәліметтер бақылау тапсырмаларында

Трансшекаралық өзендер хауызының гидрологиялық бақылауы ақпараттың алдын-ала және толықтық мәселелерінен тұрады. Серіктік түсірілім жалпылама ақпараттың бір бөлігін су объектілерінің күйі туралы территориялық иелігіне қарамастан қамтамасыз етеді. Қызықты гидротехникалық объектілерге 2000 жылы құрылған мұзды және қарлы-мұзды қорлар суды сақтау көлемінің маусымдық вариациясы ескерілетін жасанды су қоймаларын жатқызуға болады. SRTM-2000 Elevation рельефтің сандық моделі мұндай су қоймаларына батиметрияны ұсынады. Су қорының түбі батиметриясымен бірге су айнасының ауданын бақылау "өзен-су қоры"жүйенің су баланс қосындысын есептеуге трансшекаралық хауыздарды гидрологиялық бақылауды қосуға мүмкіндік береді. Іле өзені (Қазақстан мен ҚХР шекарасы)хауызына мысал ретінде 2005 ж Текес өзенінде (ҚХР)құрылған Қапшағай су қорының қосынды су балансы қарастырылған. Текес өзені Іле өзенінің негізгі ағымының орташа көлемі шамамен 250 $м^3$ / сек қарлы-мұзды қор мен ішкі Тянь-Шань тауында құрылады. 2005-2016 жж ANDSAT-5,7,8 ширегіндегі 157 түсірілім негізінде және РСМ түбі су қорының гидрологиялық негізгі сипаттамалары Іле өзенінің негізгі ағымдарының шығыны мен "өзен-су қоры"жүйесінің қосынды су баланс параметрі анықталды.

Түйін сөздер: қашықтықтан зондтау әдісі, LANDSAT суреттері, су беті көлемінің айнасы, су қоймасының гидрологиялық режимі, рельефтің сандық моделі, өзен суының шығыны.

1. Введение

Гидрологический мониторинг бассейнов трансграничных рек имеет проблемы полноты и представительности информации. Особенно актуально эта проблема стоит для стран расположенных ниже по течению. Например, для бассейна реки Иле (основной приток озера Балхаш), территория которого относится к юрисдикции Казахстана и КНР. Спутниковая съёмка способна обеспечить часть объективной информации о состоянии водных объектов КНР, расположенных выше по течению, и таким образом улучшать полноту гидрологического мониторинга трансграничного бассейна.

Одним из интересных гидротехнических объектов, состояние которых зависит от водности года и может эффективно диагностироваться спутниковой съёмкой, являются искусственные водохранилища на реках ледового и снежно-ледового питания. Естественная сезонность в объёмах стока таких рек, когда зимний сток может быть в 10 раз меньше летнего, сочетается с гидрологическим режимом работы самого объекта. Всё это приводит к существенным сезонным вариациям объёмов хранения воды, а следовательно и площади водного зеркала, которая может уверено регистрироваться по спутниковым данным.

Расход воды в реках является важной гидрологической характеристикой необходимой для прогноза объема стока и планирования хозяйственного водопользования на территории бассейна Особую актуальность такие данные представляют для трансграничных рек в условиях климатического недостатка увлажнения. Недостаток поверхностных водных ресурсов, усугубляющийся в маловодные годы, способен приносить значительные экономические потери, особенно для стран расположенных в нижнем течении реки. Для трансграничных рек информация по расходу воды в реках на территорию соседних стран может иметь ограничения по оперативности и деталировки или отсутствовать вовсе. Поэтому, методики оценки расхода воды в речных руслах, основанные на спут-

никовых данных представляют значительный интерес.

Требования к пространственному разрешению спутниковых данных в задаче диагностики расхода воды в реках определяются размером русла и сезонной вариативностью объемов стока. Чем крупнее река и больше сезонные вариации в объеме стока, тем меньше требования к пространственному разрешению ДДЗ. С ростом пространственного разрешения спутниковых данных снижается частота сканирования территории, поэтому для более детального по времени мониторинга желательно иметь методику обработки снимков возможно худшего разрешения. В настоящий момент наиболее эффективный мониторинг возможен, если для анализа пригодны снимки с пространственным разрешением 30 м, что позволяет привлечь открытый архив данных LANDSAT, имеющий значительную историческую глубину (с 1983 года).

2. Задача оценки наполненности искусственных водохранилищ

Динамика состояния крупных водных объектов диагностируется на спутниковых платформах путём определения абсолютной высоты водного зеркала, например [1] или через мониторинг водного зеркала [2]. Анализ состояния водохранилищ и параметры суммарного баланса водных потоков в системе «речной сток - водохранилище» также могут строиться на основе спутникового мониторинга площади водного зеркала и 3D модели резервуара [3]. Для территорий покрых водой после 2000 года в качестве батиметрической информации применим продукт SRTM-2000 Elevation, созданный по радарным спутниковым данным до 2000 года.

В настоящее время в китайской части бассейна реки Иле находятся два относительно крупных искусственных водохранилища. Это построенные в 2005-2006 гг. на реке Текес - Капшагайское водохранилище (объём - 2 куб. км) и на реке Каш – Жарынтайское водохранилище (объём – 2.5 куб. км). Реки Текес и Каш являются основными притоками реки Иле, со среднегодовым объёмом стока около 250 м^3/сек 125 м^3/сек, соответственно. Они имеют снежно-ледовое питание и формируются в горах внутреннего Тянь-Шаня. Для Казахстанских организаций оперативная информация о гидрологических режимах рек внутреннего Тянь-Шаня (КНР) малодоступна. Это делает актуальным применение, в данном случае, дистанционных методов диагностики водности сезона. Спутниковый мониторинг суммарного водного баланса между речным стоком и водохранилищами может существенно дополнить информацию о водности рек внутреннего Тянь-Шаня, что важно для прогнозов режима стока реки Иле по территории Казахстана и уровня воды конечного водного объекта – озера Балхаш.

3. Исходные данные и методы исследования

Анализ состояния водохранилища строился на основе спутникового мониторинга площади водного зеркала и ЦМР дна резервуара, рисунок 1.

В качестве мониторинговой спутниковой информации привлекалась малооблачная съёмка спутников LANDSAT-5,7,8 периода 2005-2016 годов с пространственным разрешением 30 м. Всего было использовано 182 снимка, сцены WRS-2: path/row 145x30, 146x30. Информация доступна на сайте агентства геологии США [http://glovis.usgs.gov]. Даты залётов спутников приведены в таблице 1.

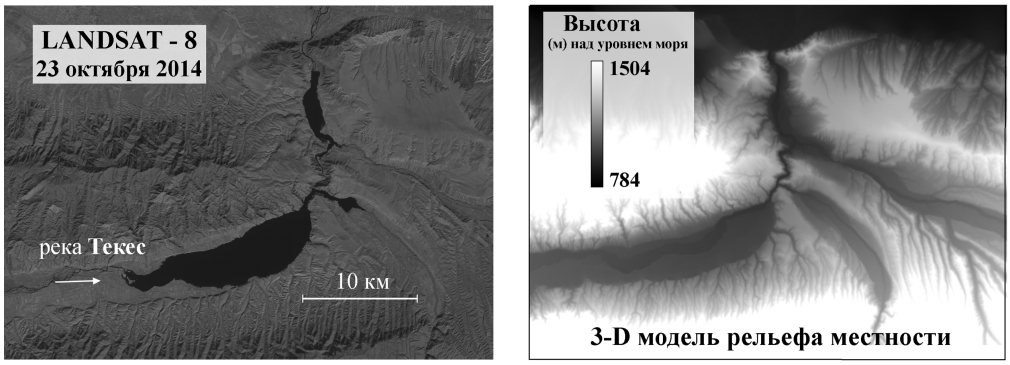

Рисунок 1 – Фрагмент снимка LANDSAT-8 (296 день, 2014 год) с Капшагайским водохранилищем на реке Текес (исходный снимок взят с сайта [http://glovis.usgs.gov]) и соответствующая ЦМР местности по данным SRTM-2000 Elevation, гранула 43n-82e

Таблица 1 – Календарные даты залетов использованных спутниковых снимков LANDSAT-5,7,8

Год	День в течение года
2005	167, 183, 231, 247, 263, 279, 296, 311, 327, 359
2006	106, 154, 170, 186, 202, 210, 218, 234, 242, 250, 274, 282, 298, 346
2007	13, 29, 109, 149, 173, 181, 213, 221, 229, 245, 253, 261, 301, 317, 365
2008	80, 96, 112, 128, 144, 192, 208, 296, 320, 336
2009	2, 66, 82, 114,130, 138, 146, 170, 178, 202, 226, 234, 258, 274, 282, 290, 298, 346
2010	93, 117, 125, 133, 157, 181, 197, 205, 213, 229, 237, 269, 277, 285, 301, 309, 317, 333, 341
2011	96, 104, 112, 136, 160, 176, 184, 192, 200, 208, 216, 224, 232, 248, 256, 344
2012	91, 107, 171, 219, 235, 251, 267, 283, 315
2013	77, 101, 125, 165, 181, 197, 213, 221, 229, 245, 261, 269, 293, 309, 317, 333
2014	88, 128, 136, 152, 160, 168, 192, 200, 208, 224, 232, 240, 248, 256, 264, 288, 296, 304, 320, 336, 344
2015	83,107,123,131,139,147,155, 163,171,187,195,203,219,243,251,259,267,275,283,291,299,315,331,347,355
2016	6, 70, 110, 118, 126, 142, 151, 158

Данные оптических каналов спутников LANDSAT-5,7,8: канал 2: 520-600 нм; канал 3: 630-690 нм; канал 4: 760-900 нм; могут эффективно использоваться для распознавания и картирования водных зеркал. Автоматическая, неконтролируемая классификация ISODATA, с делением фазового спектрального пространства на 10-30 максимально удалённых друг от друга классов, способна с высокой точностью выделять водное зеркало. Экспертный контроль над качеством классификации и коррекция ошибок (пропуски и ложные включения) осуществлялась на основе псевдоцветного изображения с формулой RGB-432. Для безоблачной съёмки, когда спектральное расстояние между водным зеркалом и окружающей подстилающей поверхностью велико, достаточно 10 классовой кластеризации. При наличии остаточной облачности выделение зеркала водохранилища требует более детальную сегментацию (до 30 классов). В случае значительных помех от облачного покрова водное зеркало выделялось на основе экспертной дешифровки и экстраполяции на основе безоблачной съемки на другие даты с близким уровнем наполненности водохранилища. Водное зеркало водохранилища состоит из 40-60 тысяч пикселей, что вполне достаточно для точной оценки его площади, без учета граничных эффектов на смешанных (вода-суша) пикселях

В качестве ЦМР дна водохранилища использовался продукт SRTM-2000 Elevation, с

пространственным разрешением 90 м и средней относительной точностью определения высоты над уровнем моря около 1 м [4]. На рисунке 1 для зоны Капшагайского водохранилища (КНР) приведён фрагмент спутникового снимка LANDSAT-8 за 23 октября 2014 года и 3-D модель рельефа местности SRTM-2000 Elevation (фрагмент гранулы 43n-82e). Продукт SRTM-2000 Elevation был создан ещё до начала строительства плотины. Поэтому, в настоящее время для территории водохранилища ЦМР представляет собой батиметрическую информацию. На основе ЦМР дна водоёма была построена 3D-модель резервуара и определены взаимосвязи между его основными параметрами (абсолютной высотой водного зеркала, площадью и объёмом), рисунок 2 и рисунок 3. Для природных объектов, как правило, все эти взаимосвязи имеют однозначный характер.

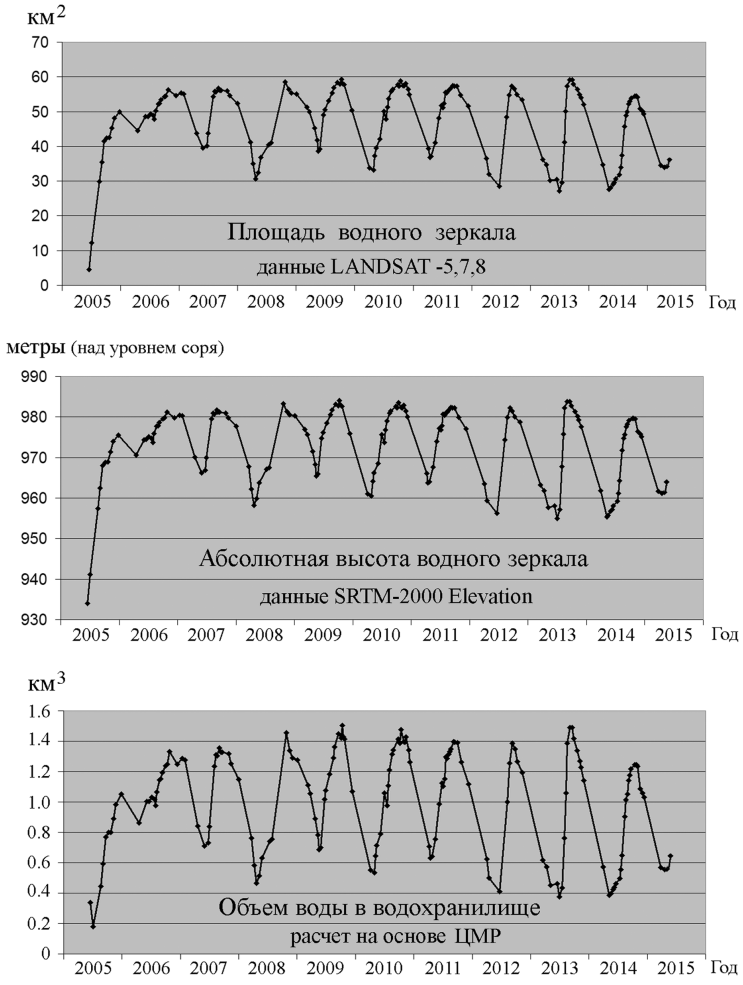

Рисунок 2 – Мониторинг основных характеристик Капшагайского водохранилища на реке Текес (КНР) в период 2005-2015 гг. Построено на основе спутниковой информации LANDSAT и ЦМР (SRTM-2000 Elevation)

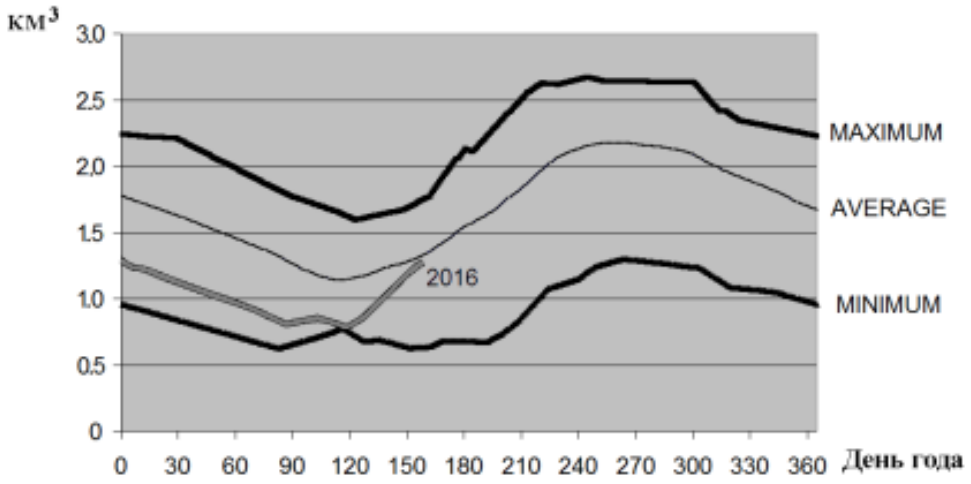

Рисунок 3 – Спутниковый мониторинг суммарных запасов воды в рабочих частях двух доминирующих искусственных водохранилищах (Капшагайское, Жарынтайское) китайского сектора бассейна р. Иле в сезоне 2016 года. Для сопоставления приведены многолетние нормы (максимум, минимум, среднее) запасов воды, регистрировавшиеся ранее в период 2005-2015 гг.

3D модели водохранилищ являлась основой для перехода от регистрируемой на спутнике площади водного зеркала к оценочным объёмам запасов воды. Расчёты ведись для двух доминирующих водохранилищ китайского сектора бассейна реки Иле: Капчагайском (р. Текес) и Жарынтайском (р. Каш). Таким образом, каждый снимок LANDSAT-5,7,8, пригодный для определения величины площади водного зеркала, продуцировал оценку объёма запаса воды в водохранилище. После соотнесения этих оценок к датам залета спутника может быть осуществлен переход к суточному периоду обновления расчетов (интерполяция) и расчёту балансовых характеристик водохранилищ, рисунок 2 и рисунок 3. При этом формировался архив данных, включающий, спутниковые данные площади зеркала и расчётные величины: объёмов воды в водохранилищах, абсолютной высоты водного зеркала и скорости изменения объёма воды в водохранилище [$\pm$м^3/сек] (между двумя соседними по времени залётами спутника).

Соответственно, чем больше снимков пригодных для определения площади водного зеркала доступно для обработки, тем детальнее гидрологический мониторинг. Спутниковая система LANDSAT в климатических условиях верхней части бассейна реки Иле (режим облачности и продолжительность холодного периода с образованием снежно-ледового покрытия, маскирующего водное зеркало) позволяет иметь в течение года от 9 (2012) до 25 (2015) малооблачного спутникового покрытия, пригодного для определения площади водного зеркала.

4. Результаты

Искусственные водохранилища в китайском секторе бассейна реки Иле в течение годового цикла претерпевает значительные изменения своего размера, что может детально регистрироваться на снимках LANDSAT-5,7,8 (разрешение 30 м). Площадь водного зеркала, например Капчшагайского водохранилища, варьируется, от 27 до 60 кв. км. На

основе этих данных была рассчитана динамика суммарного обмена водой между речным стоком и водохранилищем в течение 2005-2015 гг., рисунок 4 и рисунок 5.

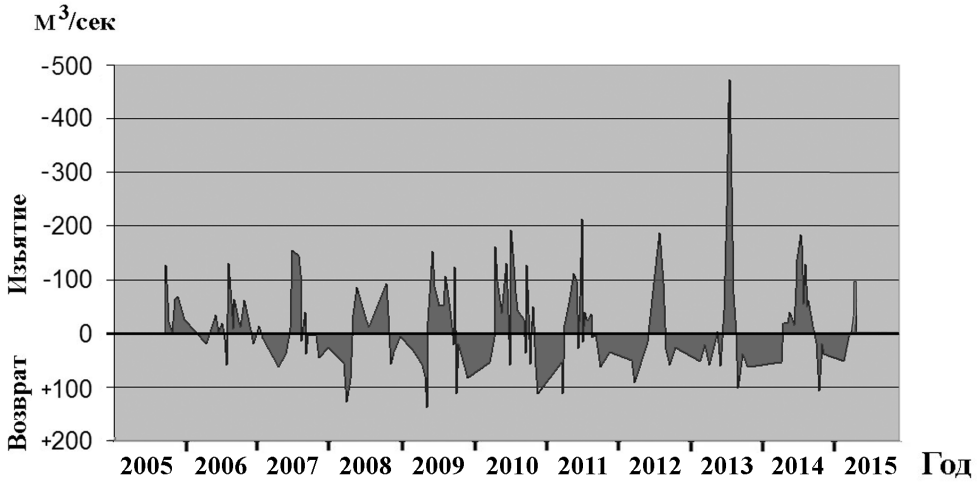

Рисунок 4 – Суммарный баланс водных потоков между стоком реки Текес (КНР) и Капшагайским водохранилищем (КНР) в период с 2005 по 2015 годов по спутниковым данным Landsat 5,7,8

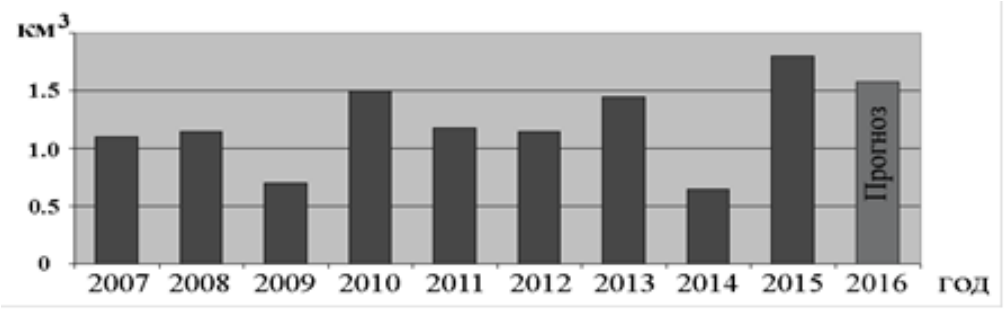

Рисунок 5 – Объёмы воды направленные на пополнение доминирующих водохранилищ Китайского сектора бассейна реки Иле (Капшагайское [р. Текес], Жарынтайское [р. Каш]) в период с мая по сентябрь. Построено по спутниковым данным

Объёмы забора воды в течение мая - августа несут в себе информацию о водности года. Можно выделить два крайних режима весенне-летнего заполнения водохранилища. Первый, отбор относительно небольших объёмов в течение продолжительного времени, с началом в мае (например, 2010 год). Первый режим, при прочих равных условиях, наиболее целесообразен в многоводные годы. Второй режим, это вынужденная схема маловодных лет. Маловодье мая и июня не позволяет изымать воду в Капшагайское водохранилище без ущерба для сельского хозяйства, расположенного ниже по течению. Приходится формировать сезонный запас воды, в основном, в июле-августе, направляя на это существенную часть речного стока (например, режим сезона 2013 года), рисунок 6.

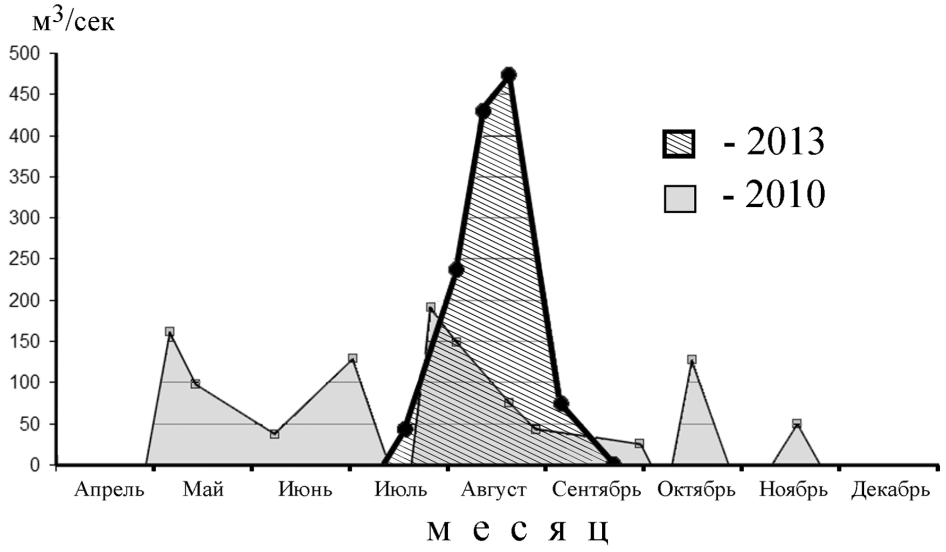

Рисунок 6 – Различные режимы изъятия воды из стока реки Текес в Капчагайское водохранилище (КНР) в контрастные по водности годы: 2010 - исключительно многоводный год; 2013 – маловодный год. Построено на основе спутниковой Диагн Ости ки суммарного водного баланса системы «река-водохранилище»

Расход воды в реке является одним из базовых гидрологических параметров.

5. Задача оценки расхода воды в реках среднегорья по спутниковым данным

Применение спутниковых данных к оценке расхода воды в реках имеет пока ограниченное распространение [5,6]. Однако для рек среднегорья, текущих по нестабильным песчано-гравийным руслам эта задача может эффективно решаться, даже по снимкам, с невысоким пространственным разрешением, например LANDSAT (разрешение 30 м). Увеличение расхода воды в таких реках приводит к возникновению дополнительных русловых потоков изменяющих спутниковый образ реки, рисунок 7.

Первоначально выбирается тестовый участок русла реки, обычно 10-30 км, на котором вариации проективного покрытия водонаполненных русел максимальны. Затем осуществляется калибровка данных между фактическим расходом воды (данные гид-

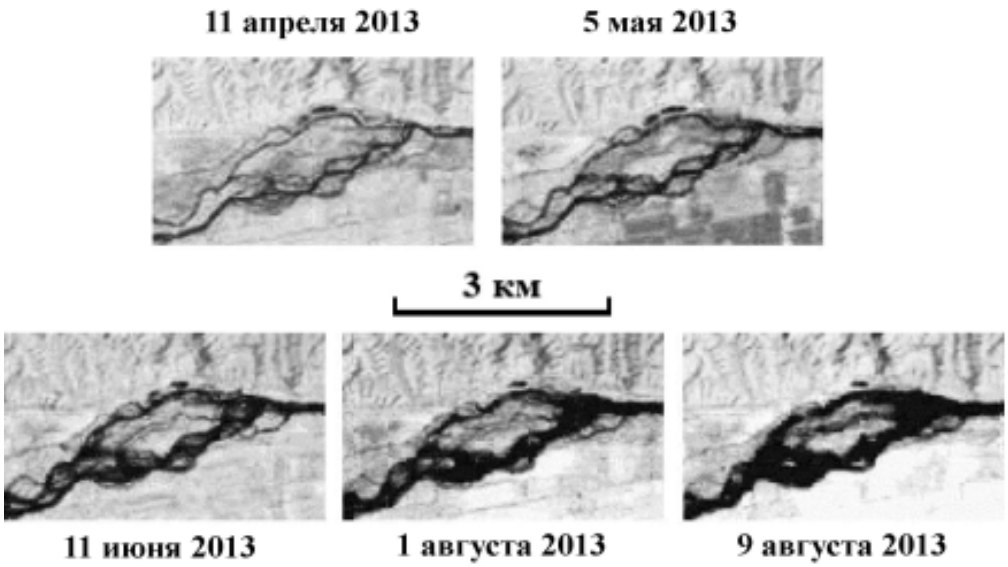

Рисунок 7 – Сезонные вариации наполненности русла р. Текес на тестовом участке в сезоне 2013 года. Данные спутника LANDSAT

ропоста) и спутниковыми параметрами, связанными с проективным покрытием водой русловой территории. Полученные эмпирические зависисмости позволяют строить схемы диагностики расхода воды на основе спутниковых изображений, рисунок 8.

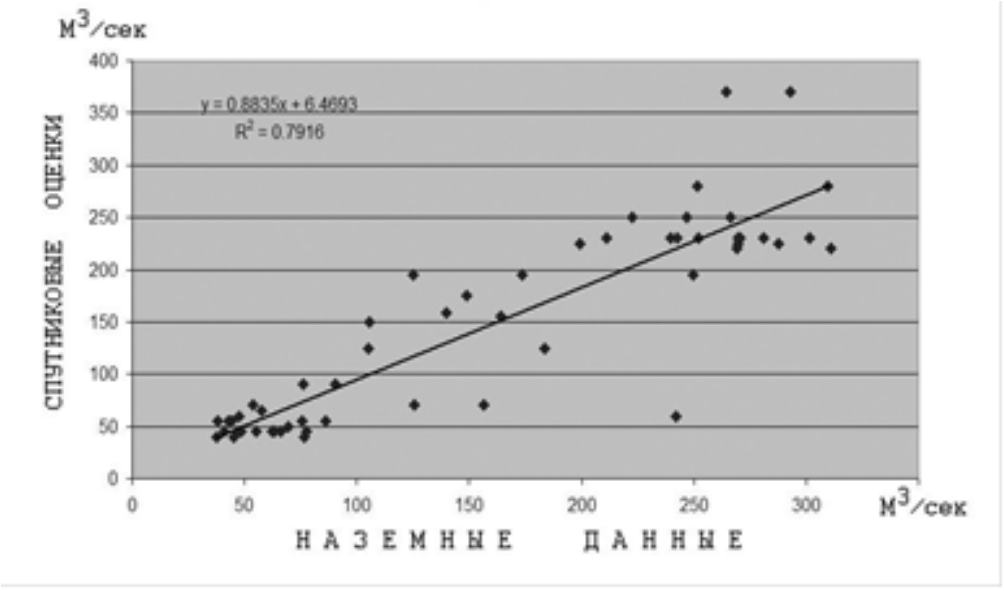

Рисунок 8 – Взаимосвязь между наземными (среднемесячными) и спутниковыми (мгновенными) LANDSAT оценками расхода воды в нижнем течении реки Каш (КНР)

Относительно неплохое соответствие спутниковых и наземных оценок расхода воды в реке (рисунок 8), с учётом сглаженности (среднемесячное значение) наземных данных

позволяет проводить дистанционную диагностику водного режима рек, рисунок 9, и оценку водности сезона рисунок 10.

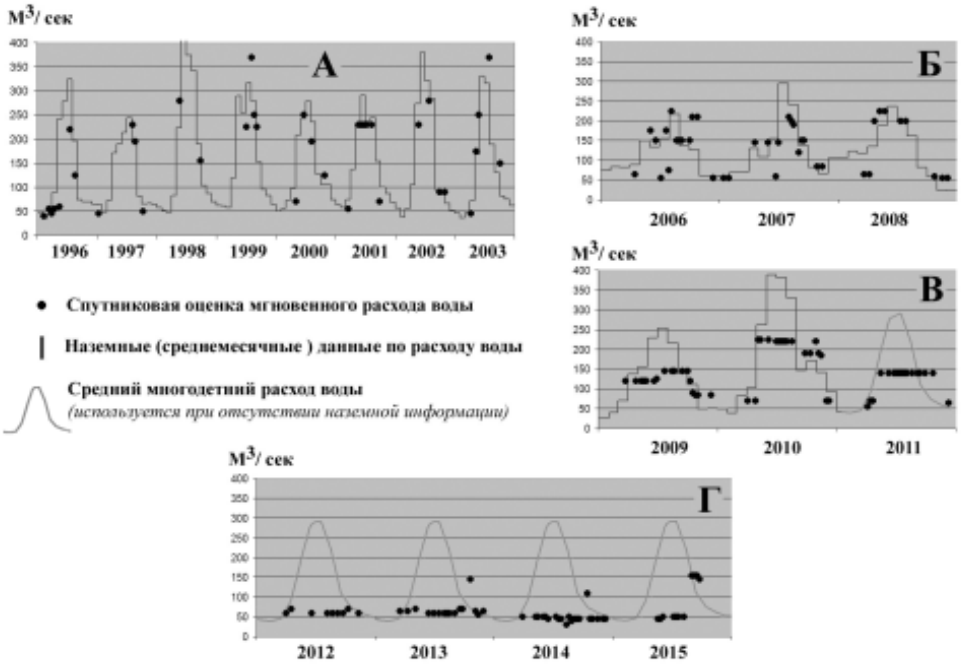

Рисунок 9 – Спутниковый мониторинг расхода воды в нижнем течении реки Каш (КНР) по данным LANDSAT периода 1996-2015 гг.

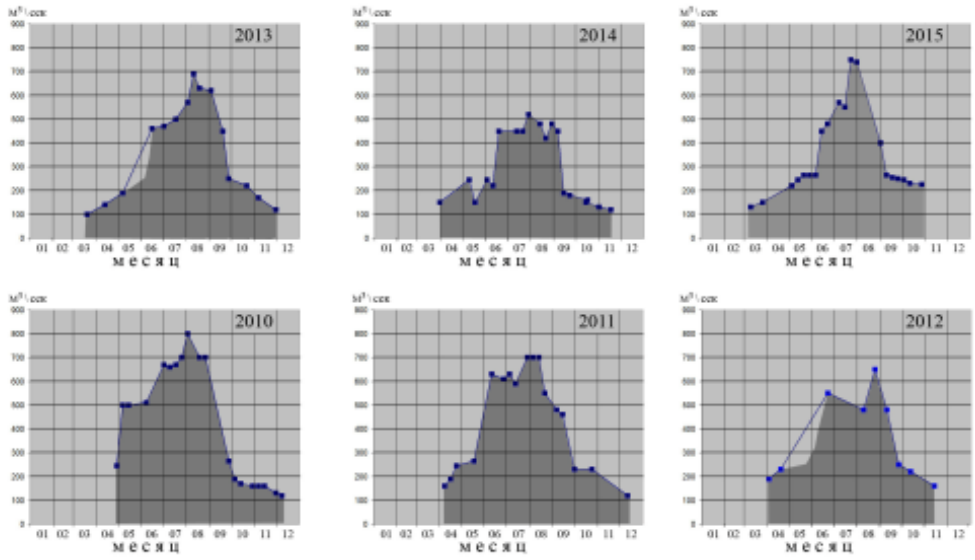

Рисунок 10 – Спутниковая диагностика расхода воды в реке Текес (КНР), выше Капшагайского водохранилища, в сезонах 2010-2015 гг. Построено на основе спутниковых данных LANDSAT

6. Результаты

Спутниковая диагностика расхода воды в нижнем течении реки Каш (рисунок 9) иллюстрирует развитие воднотранспортной инфраструктуры. Начиная с 2012 года, водовод стал забирать до половины годового стока р. Каш в обход её устья. Спутниковая диагностика стока реки Текес (КНР) рисунок 10 позволяет оценивать водность года в бассейне сопредельной страны, рисунок 11.

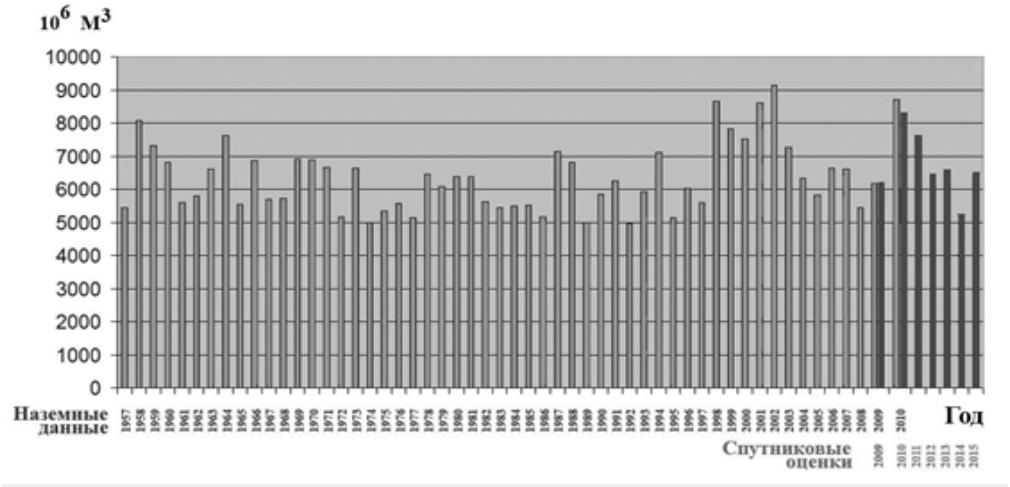

Рисунок 11 – Наземные (1957-2010 гг.) и спутниковые (2009-2015 гг.) данные по объёмам стока р. Текес (КНР) выше Капшагайского водохранилища в течение мая-октября 1957-2015 гг. Спутниковые оценки на основе данных LANDSAT

Крупные гидротехнические объекты на реках ледового и снежно-ледового питания испытывают в течение сезона существенные вариации объёмов запаса воды.

7. Выводы

На основе 3-D моделей резервуаров и спутникового мониторинга водного зеркала появляется возможность дистанционной оценки запасов воды в искуственных водохраниоищах.

Спутниковые методики оценки расхода воды в низовьях реки Каш (КНР) и в среднем течении реки Текес (КНР), опирающиеся на данные LANDSAT (разрешение 30 м) позволяют проводит диагностику водности (расход воды, объём стока) текущих сезонов в верхней части бассейна реки Иле с периодом обновления от 8 дней (периодичностью залетов спутников LANDSAT).

Эти подходы эффективны для гидрологического мониторинга вододефицитных трансграничных бассейнов, когда малодоступна оперативная информация о водности притоков и состоянии гидротехнических объектов, расположенных на территории других стран. Информация о текущих запасах воды в водохранилище и водности сезона необходима для прогнозных оценок режима и объема стока реки Иле на территории Казахстана. Работа выполнена при поддержке грантов министерства образования и науки Республики Казахстан № 2308/ГФ3, № 0115РК00548.

Литература

[1] H. Cheinway, P.Min-Fong, N. Jinsheng, L. Jia, S.Chung-Hsiung Lake level variations in China from TOPEX/Poseidon altimetry: data quality assessment and links to precipitation and ENSO// Geophysical Journal International. 2005. Vol. 161. Issue 1. P. 1–11.

[2] А.Г. Терехов Спутниковая диагностика уровня воды озёр и водохранилищ в районе бассейна реки Иле// Тезисы IX Всероссийской конф. "Современные проблемы дистанционного зондирования Земли из космоса". - М.: Институт космических исследований РАН, 2011.- http://smiswww.iki.rssi.ru/d33conf/thesisshow.aspx?page=30 (дата обращения 10.09.2015)

[3] А.Г. Терехов, И.Т. Пак, С.А. Долгих Данные LANDSAT 5,7,8 и ЦМР в задаче мониторинга гидрологического режима Капчагайского водохранилища на реке Текес (китайская часть бассейна реки Иле) // Ж. Современные проблемы дистанционного зондирования Земли из космоса. ,2015, Т.12, № 6, С. 78-86.

[4] Rodriguez E., Morris C.S., Belz J.E., Chapin E.C., Martin J.M., Daffer W. An assessment of the SRTM topographic products// Technical Report JPL D-31639.Pasadena, California: Jet Propulsion Laboratory, 2005, pp.143.

[5] D.M. Bjerklie, S.L. Dingman, C.J. Vorosmarty , C.H. Bolster, R.G. Congalton Evaluating the potential for measuring river discharge from space // J Hydrol (Amst). 2003. 278:17–38.

[6] L.C. Smith , B.L. Isacks, R.R. Forster, A.L. Bloom , I. Preuss Estimation of discharge from braided glacial rivers using ERS-1 SAR: First results // Water Resour Res .1995. 31:1325–1329.

References

[1] H. Cheinway, P.Min-Fong, N. Jinsheng, L. Jia, S.Chung-Hsiung Lake level variations in China from TOPEX/Poseidon altimetry: data quality assessment and links to precipitation and ENSO// Geophysical Journal International. 2005. Vol. 161. Issue 1. P. 1–11.

[2] A.G. Terehov Sputnikovaya diagnostika urovnya vody ozyor i vodohranilishch v rajone bassejna reki Ile// Tezisy IX Vserossijskoj konf. "Sovremennye problemy distancionnogo zondirovaniya Zemli iz kosmosa". - M.: Institut kosmicheskih issledovanij RAN, 2011 .- http://smiswww.iki.rssi.ru/d33conf/thesisshow.aspx?page=30 (data obrashcheniya 10.09.2015)

[3] A.G. Terekhov , I.T. Pak, S.A. Dolgih Dannye LANDSAT 5,7,8 i CMR v zadache monitoringa gidrologicheskogo rezhima Kapchagajskogo vodohranilishcha na reke Tekes (kitajskaya chast' bassejna reki Ile) // ZH. Sovremennye problemy distancionnogo zondirovaniya Zemli iz kosmosa. ,2015, T.12, № 6, S. 78-86.

[4] E. Rodriguez, C.S. Morris, J.E. Belz, E.C. Chapin, J.M. Martin, W. Daffer An assessment of the SRTM topographic products// Technical Report JPL D-31639.Pasadena, California: Jet Propulsion Laboratory, 2005, pp.143.

[5] D.M. Bjerklie, S.L. Dingman, C.J. Vorosmarty , C.H. Bolster, R.G. Congalton Evaluating the potential for measuring river discharge from space // J Hydrol (Amst). 2003. 278:17–38.

[6] L.C. Smith , B.L. Isacks, R.R. Forster, A.L. Bloom , I. Preuss Estimation of discharge from braided glacial rivers using ERS-1 SAR: First results // Water Resour Res .1995. 31:1325–1329.

УДК 004.67

Утепбергенов И.Т.*, Склярова Ю.В.,
Тойбаева Ш.Д., Муслимова А.К.

Институт информационных и вычислительных технологий КН МОН РК,
Республика Казахстан, г. Алматы
* E-mail: i.utepbergenov@gmail.com,

Формализация анализа функционирования и эффективности СМК для экспертной системы

В данной статье предлагается двухкаскадная система оценки функционирования СМК на основе нечетких множеств с применением алгоритма Мамдани. Актуальность исследований заключается в необходимости в Казахстане улучшения качества промышленных предприятий и уменьшения затрат на производство Гкал энергии в современных условиях повышения требований к ним. Как показывает мировой опыт, перспективным направлением реализации данной задачи является улучшение качества управления предприятием за счет внедрения системы менеджмента качества. Решение поставленной задачи также будет способствовать увеличению инвестиционной привлекательности данной сферы деятельности.
Ключевые слова: нечеткие множества, методы анализа данных, результативность СМК

Utepbergenov I.T., Skliarova I.V., Toibayeva Sh.D., Muslimova A.K.

The formalization of the analysis of the functioning and effectiveness of the QMS for the expert system

In this paper we propose a two-stage system of evaluation of the functioning of the QMS based on fuzzy sets using Mamdani algorithm. The relevance of research is the need to improve the quality of Kazakhstan industrial enterprises and reduce the cost of energy production Gcal in the current context of increased requirements for them. As international experience shows, a perspective direction of this task is to improve the enterprise management quality through quality management system. The solution of the problem will also help to increase the investment attractiveness of this sphere of activity.
Key words: fuzzy sets, methods of data analysis, the effectiveness of the QMS

Утепбергенов И.Т., Склярова Ю.В., Тойбаева Ш.Д., Муслимова А. К.

Сараптамалық жүйесі үшін СМЖ жұмыс істеуі мен тиімділігін талдау рәсімдеу

Бұл мақалада біз Mamdani алгоритмімен нақты емес көптеген негізделген СМЖ жұмыс істеуін бағалау екі сатылы жүйесі ұсынамыз. Зерттеудің өзектілігі Казақстандағы өнеркәсіптік кәсіпорындардың сапасын арттыру және оларға өсті талаптарды ағымдағы мәтінмәнде энергиясын өндіру Гкал құнын төмендетуінің қажеттілігі болып табылады. Халықаралық тәжірибе көрсетіп отырғандай, бұл тапсырма перспективалық бағыты сапа менеджменті жүйесі арқылы кәсіпорынды басқару мәселесінің шешуі сапасын жақсарту болып табылады, сондайақ осы қызмет саласына инвестициялық тартымдылығын арттыруға мүмкіндік береді.
Түйін сөздер: анық жиынтығы, деректерді талдау әдістері, СМЖ тиімділігі

1. Введение

В работе предлагается двухкаскадная система оценки функционирования СМК на основе нечетких множеств с применением алгоритма Мамдани. Актуальность исследований заключается в необходимости в Казахстане улучшения качества промышленных предприятий и уменьшения затрат на производство Гкал энергии в современных

условиях повышения требований к ним. Как показывает мировой опыт, перспективным направлением реализации данной задачи является улучшение качества управления предприятием за счет внедрения системы менеджмента качества. Решение поставленной задачи также будет способствовать увеличению инвестиционной привлекательности данной сферы деятельности.

При решении многих задач качественного характера возникает неопределенность, нечеткость либо отсутствие информации о свойствах рассматриваемой системы. В данных условиях, при отсутствии четкой математической модели используют теорию нечетких множеств, позволяющую построить модель любой системы, используя значения только входных и выходных параметров и работающую с нечеткими лингвистическими понятиями. Данная теория впервые была предложена американским ученым Л. Заде в 1965 г, который выдвинул понятие нечеткого множества и описал его математический аппарат. Основная причина зарождения данной теории - нечеткие и приближенные рассуждения человека при описании процесса, системы, объекта.

2. Постановка задачи и численный алгоритм

Теория нечётких множеств — раздел прикладной математики, посвященный методам анализа неопределённых данных, в которых описание неопределённостей реального явления и процесса приводится множеством, с нечёткими границами [1].

Нечеткое множество (НМ) (рисунок 1) – это множество упорядоченных пар $< \mu(u)/u >$, где u - элемент универсального множества U, а $< \mu(u) >$ – функция принадлежности (ФП), отображающая u в единичный отрезок, принимающий значения от 0 до 1.

Носитель НМ A – множество точек в U (универсальное множество), для которых величина $\mu_A(u)$ положительна.

Высота НМ – величина:

$$\sup_U \mu_A(u) \tag{1}$$

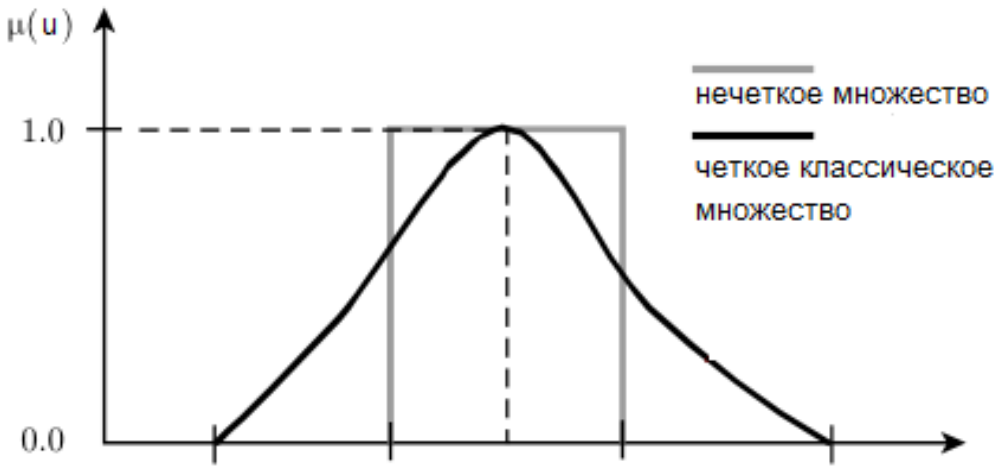

Рисунок 1 – НМ и четкое классическое множество

Базовые операции нечетких множеств:

1. Объединение – логическая связка «или»:

$$A + B = \int_U \mu_A(u) \vee \mu_B(u)/u \tag{2}$$

2. Пересечение – логическая связка «и»:

$$A \cap B = \int_U \mu_A(u) \wedge \mu_B(u)/u \tag{3}$$

3. Дополнение – логическое отрицание:

$$A' = \int_U (1 - \mu_A(u))/u \tag{4}$$

4. Возведение в степень – производится возведение не самого элемента, а его принадлежности:

$$A^\alpha = \int_U (\mu_A(u))^\alpha/u \tag{5}$$

Частные случаи возведения в степень:

CON – концентрация, возведение в квадрат – приводит к уменьшению степени нечеткости $CON(A) = A^2$

DIN – растяжение, взятие квадратного корня – приводит к увеличению степени нечеткости $DIN(A) = A^{0.5}$

5. Произведение:

$$AB = \int_U (\mu_A(u)\mu_B(u))/u \tag{6}$$

$$\alpha A = \int_U \alpha\mu_A(u)/u \tag{7}$$

6. Нормализация НМ – если высота (супремум) множества равна 1, то НМ называется нормальным. Для того чтобы НМ сделать нормальным необходимо пересчитать принадлежность элементов:

$$\mu_A(u) = \mu_A(u)/\sup \mu_A(u) \tag{8}$$

Основными типовыми формами кривых для задания ФП $\mu_A(u)$ являются треугольная, трапецеидальная и гауссова функции принадлежности.

Треугольную ФП (рисунок 2) определяет тройка чисел (a, b, c), выражение для вычисления значения функции в точке x:

$$\mu_A(u) = \begin{cases} 1 - \frac{b-u}{b-a} & a \le u \le b \\ 1 - \frac{u-b}{c-b} & b \le u \le c \\ 0 & \text{в остальных случаях} \end{cases} \tag{9}$$

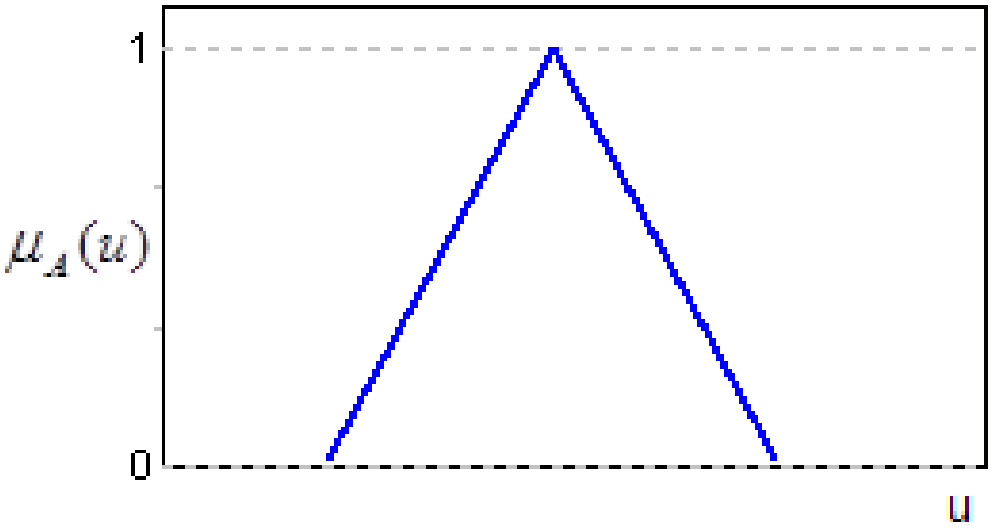

Рисунок 2 – Треугольная ФП

При $(b-a)=(c-b)$ треугольная ФП становится симметричной и задается 2 параметрами из (a,b,c).

Трапецеидальная ФП (рисунок 3) задается четверкой чисел (a,b,c,d):

$$\mu_A(u)=\begin{cases}1-\frac{b-u}{b-a} & a\le u\le b\\ 1 & b\le u\le c\\ 1-\frac{u-c}{d-c} & c\le u\le d\\ 0 & \text{в остальных случаях}\end{cases} \tag{10}$$

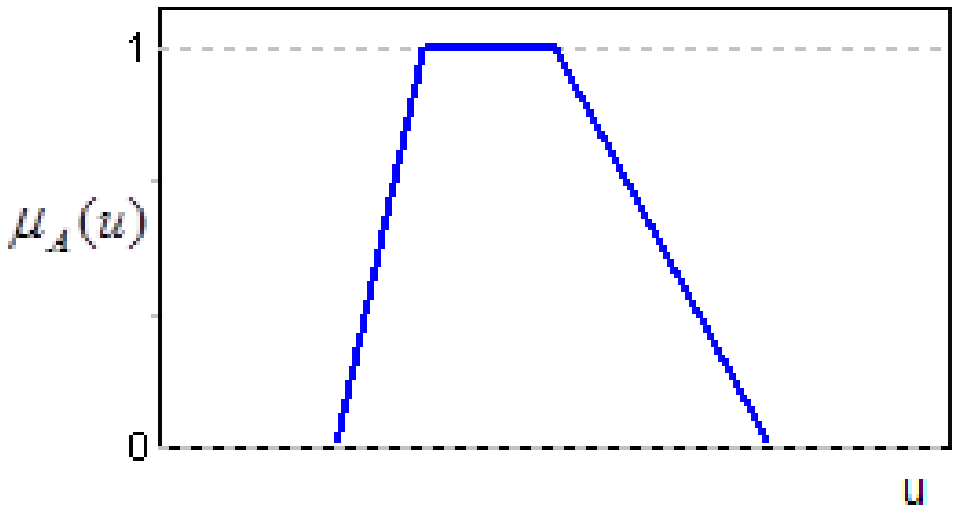

Рисунок 3 – Трапецеидальная ФП

Трапецеидальная ФП является симметричной при: $(b-a)=(d-c)$. Гауссовский тип функции принадлежности (рисунок 4) задается двумя параметрами и описывается

формулой:

$$\mu_A(u) = \exp\left(-\left(\frac{u-c^2}{\sigma}\right)\right) \tag{11}$$

где c – центр нечеткого множества, а параметр σ – крутизна функции.

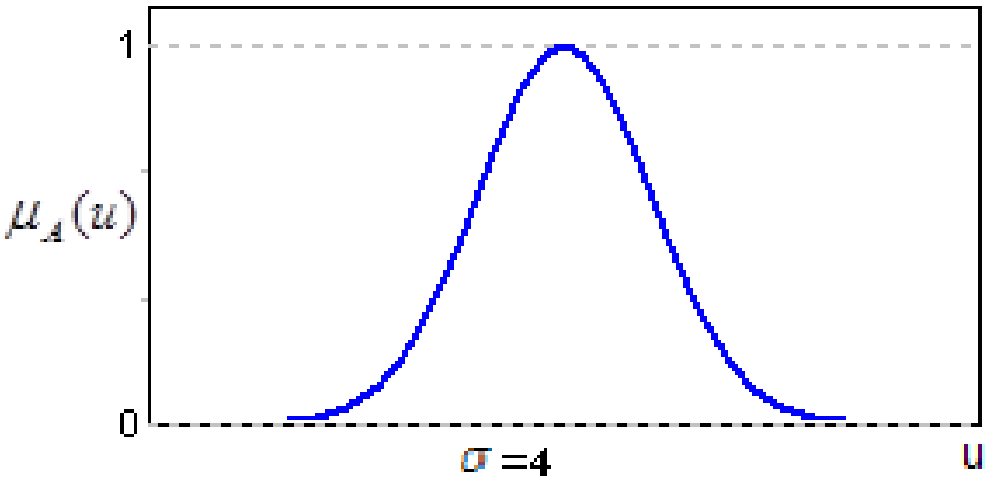

Рисунок 4 – ФП гауссова типа

3. Нечеткий логический вывод

Для получения результатов работы с нечеткими множествами создан нечеткий логический вывод. Нечеткий логический вывод – это получение ответа в виде НМ, который соответствует входным текущим значениям, преобразованным с помощью базы знаний и операций НМ. Операция нечеткого логического вывода невозможна без базы правил: нечетких высказываний типа «Если-то» и ФП для лингвистических термов. Чтобы база правил была полной нужно учесть некоторые условия при ее создании:

1. для получения каждого лингвистического терма выходной переменной должно быть хоть одно правило;

2. каждый терм входной переменной должен участвовать хотя бы в одном правиле (левая часть правила).

Например: база правил содержит m правил вида:

$$\begin{aligned} R_1:&\ \text{ЕСЛИ } x_1 \text{ это } A_{11} \text{ ...И... } x_n \text{ это } A_{1n},\ \text{ТО } y \text{ это } B_1 \\ &\dots \\ R_i:&\ \text{ЕСЛИ } x_1 \text{ это } A_{i1} \text{ ...И... } x_n \text{ это } A_{in},\ \text{ТО } y \text{ это } B_i \\ &\dots \\ R_m:&\ \text{ЕСЛИ } x_1 \text{ это } A_{i1} \text{ ...И... } x_n \text{ это } A_{mn},\ \text{ТО } y \text{ это } B_m \end{aligned} \tag{12}$$

где x_k, $k = 1..n$– входы; y – выход; A_{ik} – заданные НМ с функциями принадлежности.

В механизме логического вывода выделяется четыре этапа (рисунок 5):

1. фаззификация – введение нечеткости;
2. нечеткий вывод;
3. композиция;
4. дефаззификация – приведение к четкости.

4. Применение алгоритма нечеткого логического вывода

Алгоритмами нечеткого логического вывода являются алгоритмы Мамдани, Сугено, Ларсена, Цукамото, имеющие различия в правилах, логических операциях и методах дефаззификации. В качестве математической модели для анализа систем теплоснабжения и показателей СМК выберем нечеткий логический вывод Мамдани, алгоритм которого позволяет уменьшить объемы вычислений и широко применяется в различных отраслях промышленности.

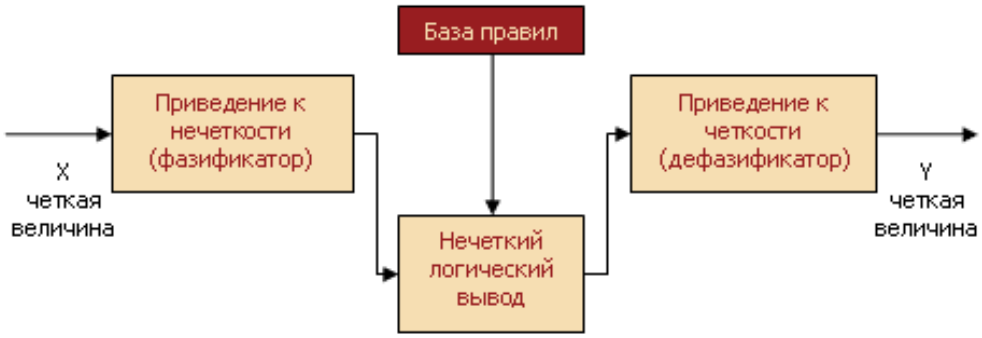

Рисунок 5 – Система нечеткого логического вывода

Алгоритм Мамдани состоит из следующих этапов:

1. формирование базы правил.
2. фаззификация входных параметров – определяет соответствие между конкретным значением входа и значением ФП.
3. агрегирование подусловий в нечетких правилах продукций – определяется степень истинности условий по каждому правилу, используя парные нечеткие логические операции. При степени истинности не равной 0 правило считается активным.
4. активизация подзаключений – определяется степень истинности каждого из подзаключений: метод min-активизации:

$$\mu'(y) = \min\{c_i, \mu(y)\} \tag{13}$$

5. аккумуляция заключений – объединяются степеней истинности подзаключений для получения ФП каждой из выходных переменных:

$$\mu_{\text{Д}}(x) = \max\{\mu_A(x), \mu_B(x)\} \tag{14}$$

6. дефаззификация выходных параметров – получение количественного значения всех выходных параметров методами:

   (a) центра тяжести:

$$y = \frac{\int_{\min}^{\max} x\mu(x)dx}{\int_{\min}^{\max} \mu(x)dx} \tag{15}$$

   (b) центра тяжести для одноточечных множеств:

$$y = \frac{\sum_{i=1}^{n} x_i\mu(x_i)}{\sum_{i=1}^{n} \mu(x_i)} \tag{16}$$

   (c) центра площади:

$$\int_{\min}^{u} \mu(x)dx = \int_{u}^{\max} \mu(x)dx \tag{17}$$

Анализ систем менеджмента качества согласно стандарту ISO 9001 [2] решает задачу непрерывного улучшения функционирования предприятия путем принятия решений после анализа следующих данных:

1. выполнение целей;
2. удовлетворенность потребителей;
3. результаты внутренних и внешних аудитов;
4. правильность функционирования процессов;
5. полнота разработанности документации;
6. степень реализации КД/ПД;
7. выполнение решений предыдущих анализов и рекомендаций по улучшению;
8. предложения по изменениям, которые следует внести в СМК с целью ее улучшения.

Большое количество входных данных увеличивает сложность модели как четких (сложная математическая модель), так и нечетких (большая база правил), поэтому в качестве входных параметров системы нечеткого логического вывода используем часть вышеперечисленных данных и создадим двухкаскадную модель оценки системы.

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.

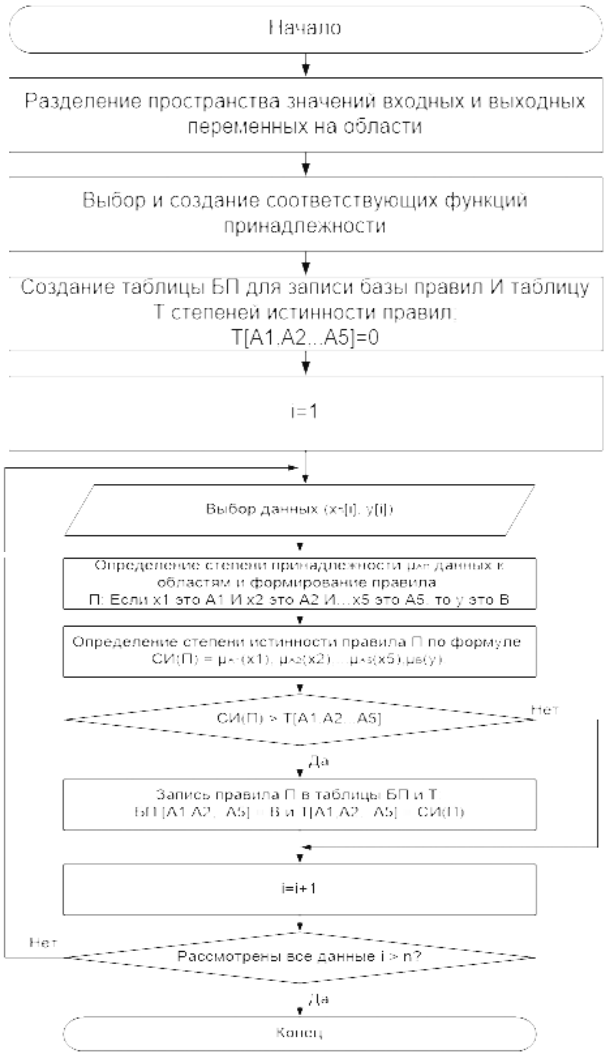

Рисунок 6 – Система нечеткого логического вывода

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.

Создание систем анализа задач качественного характера (СМК) включает в себя качественную (лингвистическую) и количественную информацию (данные), необходимую для построения и реализации системы. Значительная часть нечетких систем использует лингвистический тип знаний, представляемый в виде базы нечетких правил, поэтому если при проектировании нечеткой системы наряду с лингвистическими данными используются численные данные, возникают трудности при создании системы. Одним из путей разрешения является нейро-нечеткие системы, которые обладают многими достоинствами, однако сдерживающим моментом является длительность наполнения

знаниями в процессе итеративного обучения [3]. В виду того, что входные данные для анализа результативности СМК используют численные данные (степень достижения целей, реализации КД/ПД и т.д.), необходимо использовать другой метод проектирования нечетких систем (рисунок 6), позволяющий объединять численную информацию с лингвистической, за счет дополнения имеющейся базы правилами, созданными на основе численных данных.

6. Заключение

Внедрение и оценка эффективности систем управления является необходимым атрибутом для создания конкурентоспособного предприятия с качественным управлением, начиная от уровня технологического процесса и заканчивая стратегическим планированием на уровне руководства. В данной статье была предложена и формализована двухкаскадная система оценки функционирования СМК на основе нечетких множеств с применением алгоритма Мамдани.

Литература

[1] С.Д. Штовба Введение в теорию нечетких множеств и нечеткую логику.

[2] 2. СТ РК ИСО 9001-2009. Системы менеджмента качества. Требования.

[3] Д. Рутковская , М. Пилиньский , Л. Рутковский Нейронные сети, генетические алгоритмы и нечеткие системы: Пер. с польского И.Д. Рудинского. – М.: Горячая линия – Телеком, 2006 – 452 с.: ил.

References

[1] S.D. Shtovba Vvedenie v teoriyu nechetkih mnozhestv i nechetkuyu logiku.

[2] ST RK ISO 9001-2009. Sistemyi menedzhmenta kachestva. Trebovaniya.

[3] D. Rutkovskaya, M. Pilinskiy, L. Rutkovskiy Neyronnyie seti, geneticheskie algoritmyi i nechetkie sistemyi: Per. s polskogo I.D. Rudinskogo. – M.: Goryachaya liniya – Telekom, 2006 – 452 s.: il.

УДК 003.26:519.713

Шарипбай А.А.

Научно-исследовательский институт «Искусственный интеллект» Евразийского национального университета им.Л.Н.Гумилева,
Республика Казахстан, г. Алматы
E-mail: sharalt@mail.ru

Автоматные модели в криптографии

В работе сначала приводится определение последовательного конечного автомата и определение шифратора и дешифратора, используемых в криптографии, затем предлагаются конечно-автоматные модели шифраторов и дешифраторов, в конце показываются возможности структурного синтеза этих моделей, а также обсуждаются их достоинства и недостатки. Шифраторы и дешифраторы широко используются криптографии, их можно моделировать с помощью последовательных автоматов. Предложенные в работе конечно-автоматные модели шифратора показывают возможность использования для решения задач шифрования не традиционных математических моделей. Такие модели могут служит инструментом для исследования алгоритмов шифрования. Однако, как и все шифры замены, эти модели не смогут противостоять частотному анализу при шифровании больших сообщений на одном ключе - автомате. Поэтому автоматное шифрование может быть использована как одна из компонентов какой-либо комбинированной криптосистемы, которая состоит из нескольких моделей и алгоритмов шифрования. Тем не менее, возможность аппаратной реализации конечных автоматов дают преимущества по скорости шифрования и дешифрования перед другими моделями. А наличие памяти и возможности формализации грамматических правил некоторого естественного языка увеличивает криптостойкость предложенной модели.
Ключевые слова: криптография, конечно-автоматные модели, криптостойкость, шифрование, дешифрование

Sharipbay A.A.

Automata models in cryptography

In work at first definition of a consecutive finite-state machine and definition of a shifrator and the decoder used in cryptography is given then final and automatic models of shifrator and decoders are offered, possibilities of structural synthesis of these models are shown at the end, and also their merits and demerits are discussed. Encoders and decoders are widely used cryptography, can be modeled by sequential machines. Proposed in the FSM encoder models show the use of encryption solutions for problems are not traditional mathematical models. Such models can serve as a tool for the study of encryption algorithms. However, as with all replacement codes, these models will not be able to resist the frequency analysis to encrypt large messages on a single key - machine. Therefore encryption automata can be used as one component of a combination cryptosystem, which consists of several encryption algorithms and models. Nevertheless, the possibility of implementing a hardware state machines provide benefits speed encryption and decryption to other models. And the presence of the memory and the possibility of formalizing a certain grammatical rules of natural language increases the cryptographic strength of the proposed model.
Key words: cryptography, finite automata models, cryptographic, encryption, decryption

Шәріпбай А.А.

Криптографиядығы автоматты моделдер

Бұл жұмыста алдымен ретті соңғы автоматты анықтау мен криптографияда қолданылатын шифратор мен дешифраторды анықтау, содан кейін шифраторлар мен дешифраторлардың соңғы автоматты моделі ұсынылады, соңында осы моделдердің құрылымдық синтездеу мүмкіншіліктері көрсетіледі, сонымен қатар олардың артықшылықтары мен кемшіліктері талқыланады. Шифраторлар мен дешифраторлар криптографияда кеңінен қолданылады, оларды ретті автоматтардың көмегімен моделдеуге болады. Жұмыста ұсынылған шифратордың соңғы автоматты моделі дәстүрлі емес математикалық моделдерді шифрлеу тапсырмасын шешу үшін қолдану мүмкіндігін көрсетеді. Осындай моделдер шифрлеу алгоритмін зерттеу құралы ретінде қолданылады. Барлық айырбастау шифрлары сияқты осы моделдер автоматта бір кілттегі көптеген хабарламаларды шифрлау кезінде жиілікті талдауда қарсы әрекет ете алмайды. Сондықтан автоматты шифрлеу бірнеше шифрлеу алгоритмдері мен моделдерінен тұратын қандай да бір құрамдастырылған криптожүйенің бір бөлігі ретінде қолданылуы мүмкін. Соған қарамастан, басқа моделдерге қарағанда соңғы автоматтардың аппаратты жүзеге асырылу мүмкіншілігі шифрлеу және дешифрлеу жылдамдығы бойынша артықшылығын көрсетеді. Кез келген табиғи тілдің грамматикалық ережелерін құрастыру мүмкіншілігі мен жадының болуы ұсынылған моделдің криптотұрақтылығын арттырады.

Түйін сөздер: криптография, соңғы автоматты моделдер, криптотұрақтылық, шифрлеу, дешифрлеу

1. Введение

Конечный автомат – это математическая модель дискретного устройства. Он в зависимости от своей возможности может быть *распознающим* или *преобразующим.* Нас интересуют только преобразующие конечные автоматы, которые распознают входные последовательности и порождают выходные последовательности, т.е. выполняет некоторую функцию, определенную на множестве входной последовательности и выдающую результат из множества выходной последовательности. В свою очередь, преобразующие конечные автоматы подразделяются на *комбинационные конечные автоматы* (автоматы без памяти) и последовательные конечные автоматы (*автоматы с памятью*). Мы будем рассматривать только последовательных конечных автоматов [1].

Шифратор (кодер) – это математическая модель устройства, выполняющего логическую функцию (операцию) преобразование дискретного сигнала (дискретной информации) из одного (исходного) представления в другое (результирующее) представление.

Дешифратор (декодер) - это математическая модель устройства, преобразующего результирующее представление в исходное представление. Другими словами, дешифратор осуществляет выполнение обратной функции

Шифраторы и дешифраторы широко используются криптографии, их можно моделировать с помощью последовательных автоматов.

Ниже описываются последовательные конечные автоматы, строятся конечно-автоматные модели шифратора и дешифратора в криптографии [2].

2. Последовательный конечный автомат

Последовательный конечный автомат помимо входных и выходных сигналов наделен внутренними состояниями, позволяющими автомату быть многотактным. Символы, обозначающие внутренние состояния автомата хранятся в его внутренней памяти. Поэтому последовательный конечный автомат иногда называют конечным автоматом с

памятью.

Формально последовательный автомат определяется как пятерка

$$A =< S, X, Y, \delta, \lambda >, \tag{1}$$

где:
$S = \{s_1, s_2, ..., s_l\}$– конечный алфавит символов состояний;
$X = \{x_1, x_2, ..., x_n\}$– конечный алфавит входных символов;
$Y = \{y_1, y_2, ..., y_m\}$– конечный алфавит выходных символов;
$\delta : S \times X \to S$– функция переходов;
$\lambda : S \times X \to Y$– функция выходов;

Если функции переходов δ и функции выходов λ однозначно определены для каждой пары $(s_k, x_i) \in S \times X$ (k = 1, 2, ..., l; i = 1, 2, ..., n), то последовательный автомат называется *детерминированным автоматом* или *полностью определенным*, а в противном случае - *недетерминированным автоматом* или *частично определенным автоматом*, т.е. область определения функции D(δ) и D(λ) являются подмножествами множества $S \times X$, т.е. D(δ) $\subseteq S \times X$, D(λ) $\subseteq S \times X$. Если автомат имеет выделенное начальное состояние $s_0 \in S$, то он называется *инициальным автоматом*.

Последовательный конечный автомат функционирует в дискретные моменты времени: в каждый момент времени автомат, находясь в определенном состоянии и, распознав очередной входной символ переходит в следующее состояние и порождает следующий выходной символ. Иначе говоря, последовательный конечный автомат для последовательности входных символов $x_{i_1}[1], x_{i_2}[2], x_{i_3}[3]$, ... разворачивает в моменты времени $t = 1, 2, 3, \ldots$ последовательность состояний автомата $s_{k_1}[1], s_{k_2}[2], s_{k_3}[3]$, ... и последовательность выходных символов$y_{j_1}[1], y_{j_2}[2], y_{j_3}[3]$, ...

По способу формирования функций выходов конечные автоматы делятся на *автомат Мили* и *автомат Мура*.

Функционирование автомата Мили в дискретные моменты времени t для всех значений k=*1, 2, ..., l*; i=*1, 2, ..., n*; j=*1, 2, ..., m* может быть описано следующей системой рекуррентных соотношений:

$$\begin{cases} s_{k_{t+1}}(t+1) = \delta(s_{k_t}(t), x_{i_t}(t)) \\ y_{j_t}(t) = \lambda(s_{k_t}(t), x_{i_t}(t)) \end{cases} \tag{2}$$

Функциональная схема автомата Мили представлена на рисунке 1.

Функции $s_{k_{t+1}}(t+1) = \delta(s_{k_t}(t), x_{i_t}(t))$ и $y_{j_t}(t) = \lambda(s_{k_t}(t), x_{i_t}(t))$ можно представить в виде отношений: $< s_{k_t}(t), x_{i_t}(t), s_{k_{t+1}}(t+1) >$ и $< s_{k_t}(t), x_{i_t}(t), y_{j_t}(t) >$.

В автомате Мура значение выходного символа зависет только от состояния автомата, т.е. функция выхода имеет только один аргумент – состояние автомата, а остальные параметры совпадают с параметрами автомата Мили.

Если обозначим функцию выхода автомата Мура через $\mu : S \to Y$, то функионирование автомата Мура можно описать следующей системой рекуррентных соотношений:

$$\begin{cases} s_{k_{t+1}}(t+1) = \delta(s_{k_t}(t), x_{i_t}(t)) \\ y_{j_t}(t) = \mu(s_{k_t}(t)) \end{cases} \tag{3}$$

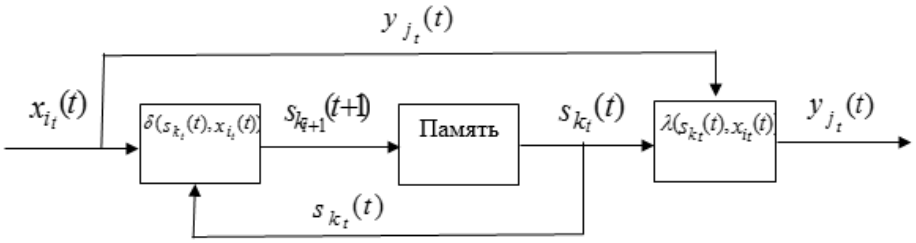

Рисунок 1 – Функциональная схема автомата Мили

Функциональная схема автомата Мура представлена на рисунке 2.

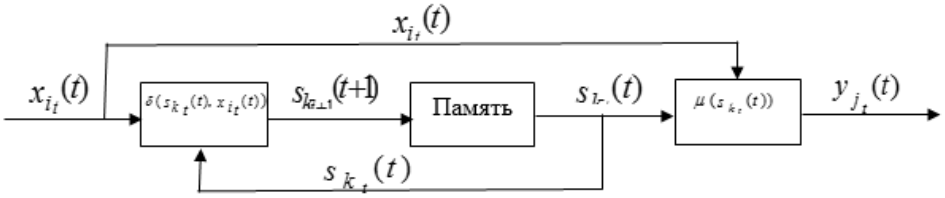

Рисунок 2 – Функциональная схема автомата Мура

Функция выхода автомата Мура ставит метку на выходе каждому его состоянию, поэтому эту функцию называют также функцией меток.

Особенностью автомата Мура является то, что символ $y_{j_t}(t)$ в выходном канале существует все время, пока автомат находится в состоянии $s_{kt}(t)$для любых j=*1*, *2*, ..., m; k=*1*, *2*, ..., l; $t = 1, 2, 3, \ldots$.

Следует отметить, что для любого автомата Мура существует автомат Мили, реализующий ту же самую функцию. И наоборот: для любого автомата Мили существует соответствующий автомат Мура, возможно, со сдвигом по времени:

$$\mu(s_{kt+1}(t+1)) = \lambda(s_{kt}(t), x_{it}(t)),\ \mathrm{t} = 1,\ 2,\ 3,\ \ldots .$$

В автоматах Мили и Мура входные и выходные последовательности вида $x_{i_1}[1], x_{i_2}[2]$, $x_{i_3}[3], \ldots$ и $y_{j_1}[1], y_{j_2}[2], y_{j_3}[3], \ldots$ можно считать словами (цепочками) конечной длины некоторого языка X^* и Y^* соответственно. Здесь $*$ – операция итерации, результат выполнения которой порождает множество всех возможных цепочек (слов) в алфавитах X и Y.

Таким образом, последовательные конечные автоматы (Мили и Мура) $\boldsymbol{A}$, находясь в начальном состоянии s_0, индуцирует автоматное отображение, которое ставит в соответствие входным словам $x_{i_1}\, x_{i_2} \ldots x_{i_n} \in X^*$ выходные слова $y_{j_1}\, y_{j_2} \ldots y_{j_m} \in Y^*$. При этом входные слова определяют множество слов, распознаваемых этим автоматом (входной язык автомата), выходные слова - множество слов, порождаемых этим автоматом (выходной язык автомата).

3. Автоматная модель шифратора в криптографии

Во введении было замечено, шифратор в криптографии является последовательным устройством. Поэтому для построения автоматной модели шифратора в криптографии необходимо дать некоторые определения:

Криптографическим шифратором называется следующая пятерка:

$$C =< K, \tilde{X}^*, \tilde{Y}^*, S, D >, \tag{4}$$

где:

K– множество ключей;

$\widetilde{X^*} \subseteq X^*$множество открытых (исходных) текстов;

$\widetilde{Y^*} \subseteq Y^*$– множество закрытых (зашифрованных) текстов;

$S_k : \ \xi \to \zeta \left(\xi \in \widetilde{X^*}, \ \zeta \in \widetilde{Y^*} \right) \ -$ правило шифрования для $k \in K$;

$D_k : \ \zeta \to \xi \left(\ \zeta \in \widetilde{Y^*}, \ \xi \in \widetilde{X^*} \right) -$ правило дешифрования для $k \in K$;

При этом должны выполняться следующие свойства:

$1. \forall \xi \ \in \widetilde{X^*}, \forall k \in K : \quad D_k \left(S_k \left(\xi \right) \right) = \xi;$

$2. \widetilde{Y^*} = \bigcup\limits_k \bigcup\limits_\xi S_k(\xi)$

Последовательный автомат, который будет моделировать работу шифратора (3) должен иметь функции переходов и выходов, зависимые от ключа $k \in K$, т.е. формальное определение такого автомата будет иметь вид:

$$A =< S * K, \ X, \ Y, \ \delta, \ \lambda > \tag{5}$$

В этом случае функциональная модель автомата Мили выглядит так:

$$\begin{cases} \delta \left(\left(S_{k_t} \left(t \right), \ k \right), \ x_{i_t} \left(t \right) \right) = \delta(S_{k_t} \left(t \right), x_{i_t} \left(t \right) = \left(S_{k_{t+1}} \left(t+1 \right), \ k \right) \\ \lambda \left(\left(S_{k_t} \left(t \right), \ k \right), \ x_{i_t} \left(t \right) \right) = \lambda(S_{k_t} \left(t \right), x_{i_t} \left(t \right) = y_{j_t} \left(t \right) \end{cases} \tag{6}$$

Для решения задачи дешифрования (задачи моделирования дешифратора) необходимо построить обратный автомат, которое может обратить автоматное отображение входных последовательностей в выходные. Обращение отображения имеет направление: левое и правое. Мы рассмотрим левое обращение и дадим следующее определение:

Автомат $A^{-1} =< \tilde{S}, \ X, \ Y, \ \widetilde{\delta}, \ \widetilde{\lambda} >$ называется обратным слева к автомату $A =< S, \ X, \ Y, \ \delta, \ \lambda >$

Если $\forall s \in S \exists \tilde{s} \in \tilde{S}$ такое, что $\forall \xi \in X^*$ выполняется равенство $A_s^{-1} \left(A_s \left(\xi \right) \right) = \xi$.

Для существования обратного автомата необходимо и достаточно инъективность автоматного отображения A_s для любого начального состояния s. Инъективность автоматного отображения достигается требованием инъективности функции выхода λ при фиксированном состоянии s, то есть частичной функции $\lambda_s : X \to Y$, что означает $|\lambda_s^{-1}(y)| \leq 1$.

Итак, для получения однозначности дешифрования шифрующий автомат (5) и (6) должен иметь инъективную частичную функцию выходов λ_s, что приводит к следующему алгоритму построения обратного автомата:

1. Если $|\lambda_s^{-1}(y)| = 1$, то $\tilde{\lambda}(s,y) = \lambda_s^{-1}(y)$ и $\tilde{\delta}(s,y) = \delta(s, \lambda_s^{-1}(y))$.

2. В противном случае, когда $|\lambda_s^{-1}(y)| = 0$,$\tilde{\lambda}(s,y)$ – произвольный $x \in X$,

$\tilde{\delta}(s,y)$ – произвольное $s \in S$.

Если мощности алфавитом X и Y совпадают, то обратный автомат строится однозначно. В общем случае должно выполняться $|X| \leq |Y|$. Если неравенство строгое, то обратный автомат является частичным.

Заметим, что для обратимости автомата необходимо и достаточно, чтобы в его табличном представлении в каждом столбце таблицы выходов все выходные сигналы были различны.

Для демонстрации предложенных моделей и алгоритмов рассмотрим шифр замену на основе автомата Мили.

Рассмотрим многозначную замену (подстановку), которая моделируется автоматом Мили $\boldsymbol{A}$ и представляется в таблице 1.

Таблица 1 – Многозначная замена – выходы автомат Мили $\boldsymbol{A}$

Состояние	Входные символы							
	000	001	010	011	100	101	110	111
00	010	111	100	110	001	000	101	011
01	011	010	000	101	110	111	001	100
10	110	100	001	111	010	011	000	101
Состояние	Выходные символы							

При использовании шифров многозначной замены возникает трудности, связанные с необходимостью запоминания ключа. Для задания порядка выбора подстановок требуется построить функцию-распределитель.

Чтобы решить эту проблему нужно интерпретировать таблицу 1 как таблицу выходов автомата Мили $\boldsymbol{A}$ и определить таблицу переходов. Поскольку замена трехвариантная, то автомат должен иметь три состояния. Тогда переходы автомата представляется таблицей 2.

Функциональная модель автомата $\boldsymbol{A}$ представляется системой логических (булевых) функций, зависящих от пяти переменных:

$$\begin{cases} y_{1_t} = \delta_1(s_{1_t}, s_{2_t}, x_{1_t}, x_{2_t}, x_{3_t}) \\ y_{2_t} = \delta_1(s_{1_t}, s_{2_t}, x_{1_t}, x_{2_t}, x_{3_t}) \\ y_{3_t} = \delta_1(s_{1_t}, s_{2_t}, x_{1_t}, x_{2_t}, x_{3_t}) \\ s_{1_{t+1}} = \lambda_1(s_{1_t}, s_{2_t}, x_{1_t}, x_{2_t}, x_{3_t}) \\ s_{2_{t+1}} = \lambda_2(s_{1_t}, s_{2_t}, x_{1_t}, x_{2_t}, x_{3_t}) \end{cases} \tag{7}$$

Функции выходов и функции переходов строятся стандартным образом согласно каноническому методу структурного синтеза автомата. Далее в качестве памяти возьмем элементы задержки и полученную систему логических уравнений минимизируем методом Квайна – Мак-Класски, который позволит минимизацию логической функции, заданной таблицей истинности или совершенной дизъюнктивной нормальной формой. В результате каноническая система уравнений автомата примет вид:

$$\begin{cases} y_{1t} = s_{1t}s_{2t}x_{1t}x_{2t} \vee \overline{s}_{2t}\overline{1t}x_{3t} \vee \overline{s}_{1t}s_{2t}x_{1t}\overline{x}_{2t} \vee \overline{s}_{1t}\overline{s}_{2t}x_{2t}x_{3t} \vee \overline{s}_{1t}s_{2t}x_{2t}x_{3t} \vee s_{1t}\overline{s}_{2t}x_{2t}x_{3t}, \\ y_{2t} = \overline{s}_{2t}\overline{x}_{1t}\overline{x}_{2t}\overline{x}_{3t} \vee \overline{s}_{1t}\overline{x}_{1t}\overline{x}_{2t} \vee \overline{s}_{2t}\overline{x}_{1t}x_{2t}x_{3t} \vee \overline{s}_{1t}s_{2t}\overline{x}_{2t} \vee s_{1t}\overline{s}_{2t}x_{1t}\overline{x}_{2t} \vee \overline{s}_{1t}\overline{s}_{2t}x_{2t}x_{3t}, \\ y_{3t} = \overline{s}_{1t}s_{2t}\overline{x}_{1t}\overline{x}_{2t}\overline{x}_{3t} \vee \overline{s}_{1t}\overline{s}_{2t}\overline{x}_{1t}\overline{x}_{2t}x_{3t} \vee \overline{s}_{1t}s_{2t}\overline{x}_{1t}x_{2t}x_{3t} \vee s_{1t}\overline{s}_{2t}x_{1t}x_{2t} \vee \\ \qquad \vee\overline{s}_{1t}s_{2t}x_{1t}\overline{x}_{2t}x_{3t} \vee \overline{s}_{1t}\overline{s}_{2t}x_{1t}x_{3t} \vee \overline{s}_{1t}x_{1t}x_{2t}\overline{x}_{3t} \vee \overline{s}_{1t}\overline{s}_{2t}x_{1t}x_{2t} \vee s_{1t}\overline{s}_{2t}x_{1t}x_{3t}, \\ s_{1t+1} = \overline{s}_{1t}s_{2t}\overline{x}_{1t}\overline{x}_{2t} \vee \overline{s}_{1t}\overline{s}_{2t}x_{2t}\overline{x}_{3t} \vee \overline{s}_{2t}x_{1t}x_{2t}\overline{x}_{3t} \vee \overline{s}_{1t}s_{2t}x_{2t}x_{3t}, \\ s_{2t+1} = s_{1t}\overline{s}_{2t}\overline{x}_{1t}x_{2t} \vee s_{1t}\overline{s}_{2t}\overline{x}_{1t}x_{3t} \vee \overline{s}_{1t}\overline{s}_{2t}\overline{x}_{2t}\overline{x}_{3t} \vee \overline{s}_{2t}x_{1}\overline{x}_{2t}\overline{x}_{3t} \vee \overline{s}_{1t}x_{1t}\overline{x}_{2t}x_{3t} \vee s_{1t}\overline{s}_{2t}x_{2t}x_{3t} \end{cases} \tag{8}$$

Последний этап синтеза автомата – построение комбинационной части логической схемы по системе логических функций не представляет трудности. Из-за громоздкости этого построения мы не будем показывать построенную логическую схему требуемого автомата $\boldsymbol{A}$, и построим только его структурную схему, представленная на рисунке 3.

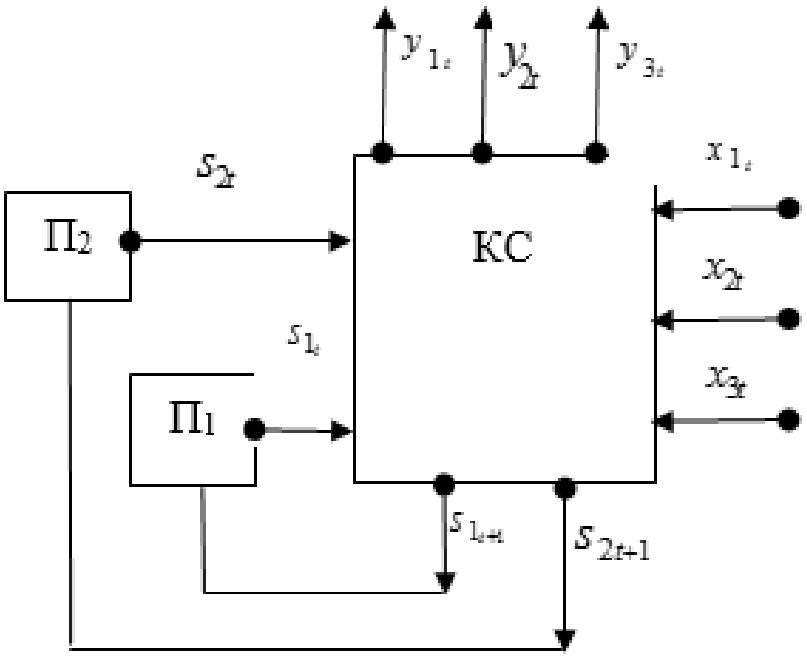

Рисунок 3 – Структурная схема автомата Мили - шифратора $\boldsymbol{A}$

По структурной схеме видно, что сначала в память запоминается начальное (предыдущее) состояние, которое подается на вход КС, чтобы инициировать функции выходов

и функции переходов, затем порожденные новые состояния опять записываются в память и т.д. автомат продолжает работать пока не выполняться условия для останова.

Таблица 2 – Таблица переходов автомата Мили $\boldsymbol{A}$

Состояние	Входные символы							
	000	001	010	011	100	101	110	111
00	01	00	10	00	01	01	10	00
01	10	10	00	10	00	01	00	10
10	00	01	01	01	01	00	10	01
Состояние	Состояния переходов							

Для расшифровки необходимо существования обратного автомата, который строится однозначно, если будет выполняться следующие условия:

Для обеспечения однозначности расшифровки необходимо и достаточно, чтобы в шифраторе в каждой последовательности выходных сигналов, соответствующих одному состоянию, все значения были различны.

По таблице 1 несложно проверить, что это требование выполнено: в пределах одной строки кодовые комбинации не повторяются.

Для проверки правильности синтеза шифратора $\boldsymbol{A}$ и дешифратора $\boldsymbol{A}^{-1}$ сводится к последовательному применению их к некоторому открытому тексту $\tau \in X*$, чтобы выполнялось условие:

$$\tau = A^{-1}(A(\tau)). \tag{9}$$

Заметим, что построенный автомат $\boldsymbol{A}_2$ одинаковых фрагментов входной последовательности шифруют различными блоками. Например, кодовая комбинация «000» может быть зашифрована одним из трех способов: «010», «011» или «110», в зависимости от того, в каком состоянии находится автомат.

4. Заключение

Предложенные в работе конечно-автоматные модели шифратора показывают возможность использования для решения задач шифрования не традиционных математических моделей. Такие модели могут служит инструментом для исследования алгоритмов шифрования. Однако, как и все шифры замены, эти модели не смогут противостоять частотному анализу при шифровании больших сообщений на одном ключе – автомате. Поэтому автоматное шифрование может быть использована как одна из компонентов какой-либо комбинированной криптосистемы, которая состоит из нескольких моделей и алгоритмов шифрования. Тем не менее, возможность аппаратной реализации конечных

автоматов дают преимущества по скорости шифрования и дешифрования перед другими моделями, а наличие памяти и возможности формализации грамматических правил некоторого естественного языка увеличивает криптостойкость предложенной модели, так как для атакующего - хакера нужно знать помимо прочего и грамматические правила этого языка, если в качестве ключа использовать эти правила.

Литература

[1] Ожиганов А.А. Теория автоматов: Учебное пособие. СПб.: НИУ ИТМО, 2013. – 84 с.

[2] Богаченко Н.Ф. Применение теоретико-автоматных моделей в криптографии. Математические структуры и моделирование. – 2007. – vol. 17. – С. 112-120.

References

[1] Ojiganov A.A. Teoriya avtomatov: Uchebnoe posobie. Spb.: NIU ITMO, 2013. – 84 s.

[2] Bogachenko N.F. Primenenie teoretiko-avtomatnyh modelei v kriptografii. Matematicheskie struktury i modelirovanie. – 2007. – vol. 17. – C. 112-120.

УДК 004.89: 004.4

Ширяева О.И.

Институт информационных и вычислительных технологий КН МОН РК,
Республика Казахстан, г. Алматы
E-mail: oshiryayeva@gmail.com

Принципы построения нечетких нейронных сетей для искусственной иммунной системы терапии сульфаниламидами

В данной статье рассматриваются вопросы развития теории нечётких нейронных сетей на класс искусственных иммунных систем. На основе теории нечеткой логики разработана функциональная схема нечеткой иммунной системы оптимального управления терапевтическими дозами сульфаниламидов для терапии пиелонефрита с блоком логического вывода. Для блока логического вывода разработана нечеткая многослойная нейронная сеть, состоящая из четырёх слоёв, которые осуществляют процедуры с нечеткими множествами: первый слой осуществляет процедуру фазификации для нечётких множеств свойств сульфаниламидов и лабораторных показателей пиелонефрита; второй слой сети осуществляет вычисление результирующих функций принадлежности предпосылок нечетких правил, сформированных в соответствии с требованиями терапии с использованием сульфаниламидов; третий слой, состоящий из двух нейронов, осуществляет суммирование и взвешенное суммирование выходных сигналов второго слоя; четвертый слой формирует управляющее воздействие для объекта управления - иммунной системы оптимального управления воздействия лекарственных средств. В соответствии с разработанной схемой управляющее устройство на основе нечётких нейронных сетей вырабатывает четкое управление на основе нечеткого множества управляющих воздействий с целью достижения желаемых значений переменных искусственных нечетких систем: количественного представления ресурсов организма, изменения количества микроорганизмов при пиелонефрите в зависимости от времени; изменения количества обнаруженных микроорганизмов.

Ключевые слова: нечеткие нейронные сети, искусственная иммунная система, терапевтические дозы, лекарственные средства, сульфаниламиды.

Shiryayeva O.I.

Principles of fuzzy neural networks for artificial immune system therapy sulfonamides

This article deals with the development of the theory of fuzzy neural networks to a class of artificial immune systems. On the basis of fuzzy logic developed a functional diagram of a fuzzy immune system of optimum control therapeutic doses of sulfonamides for the treatment of pyelonephritis with inference unit. For inference unit designed multilayer fuzzy neural network consisting of four layers, which is carried out by fuzzy sets procedure: first layer provides fuzzification procedure for the fuzzy sets of properties sulfonamides and laboratory parameters pyelonephritis; second network layer computes the resulting membership functions of fuzzy rules prerequisites, formed in accordance with the requirements of therapy with sulfonamides; a third layer comprising two neurons, and performs a weighted summation the summation of output signals of the second layer; the fourth layer forms the manipulated variable to the control object - immune system effects an optimal control drugs. In line with the pattern control device based on fuzzy neural network generates precise control based on fuzzy set of control actions in order to achieve the desired values of the variables of artificial fuzzy systems: quantification of the resources of the body, changes in the number of microorganisms in pyelonephritis, depending on the time; changing the number of microorganisms detected.

Key words: fuzzy neural networks, artificial immune system, therapeutic dose, medicines, sulfonamides.

Ширяева О.И.

Сульфаниламидпен емдеудің жасанды иммунды жүйесі үшін айқын емес нейронды желілерді құрудың принциптері

Берілген мақалада жасанды иммунды жүйелер классы үшін айқын емес нейронды желілер теориясының даму мәселелері қарастырылады. Айқын емес логика теориясының негізінде пиелонефритті емдеудегі сульфаниламидтің терапевттік мөлшерін тиімді басқарудың логикалық шығыс блогы бар айқын емес иммунды жүйесінің функционалдық сұлбасы жасалған. Логикалық шығыс блогы үшін айқын емес көпдеңгейлі нейронды желі жасалған. Ол айқын емес жиындармен процедуралар жүргізетін төрт деңгейден тұрады: бірінші деңгей физификация процедурасын сульфаниломид қаситеттері мен пиелонефриттің лабораториялық көрсеткіштерінің айқын емес жиындары үшін жүзеге асырады; желінің екінші деңгейі сульфаниламидті пайдаланудағы терапия талаптарымен сәйкес қалыптасқан айқын емес ережелердің алғышарттарын меншіктейтін нәтижелік функциялардың есептеуін жүзеге асырады; үшінші деңгей екі нейроннан тұрады. Ол - қосындылауды және салмақты қосындылауды жүзеге асырады; төртінші деңгей басқару объектісі, яғни дәрілік заттар әсер етуінің тиімді басқарудың иммунды жүйесі үшін басқару әсерін қалыптастырады. Құрастырылған сұлбаға сәйкес, айқын емес нейронды желілер негізіндегі басқару құрылғысы, басқару әсерлерінің айқын емес жиыны негізінде нақты басқаруды - жасанды айқын емес жүйелердің айнымалыларын: ағза ресурстарын мөлшерлік көрсету, пиелонефрит кезіндегі микроағзалардың санының уақытқа байланысты өзгеруі, анықталған микроағзалардың санының өзгеруі, қалаулы міндерге жету мақсатында қалыптастырады.

Түйін сөздер: айқын емес нейронды желілер, жасанды иммунды жүйе, емдік (терапевтік) дозалар, дәрілік құралдар, сульфаниламидтер

1. Введение

В настоящее время проблема исследования систем автоматического управления с применением нечеткой логики особенно актуальна. Один из успешных подходов решения задачи синтеза нечетких устройств управления в настоящее время - применение нейронной сети. В связи с этим, существует широкий круг работ, касающихся развития методов теории нечетких нейронных сетей.

В работе [1] рассмотрены принципы построения систем, основанных на нечеткой логике, кроме того, определен принцип построения логического вывода. Также рассматривается структура организации нечетких нейронных сетей на примере сети Ванга - Менделя. Описывается схема организации такой сети, ее структура, в частности, определены слои нейронной сети и описаны принципы функционирования каждого слоя. Кроме того, рассмотрен процесс обучения нечеткой нейронной сети Ванга - Менделя, включающий в себя подстройку весовых коэффициентов сети и настройку параметров функции Гаусса. А также рассмотрен процесс обучения сети в случае, когда нахождения решения процесса обучения невозможно, а поиск параметров осуществляется таким образом, что все условия выполняются в некоторой степени. Также в статье проведен сравнительный анализ различных типов архитектур интеллектуальных систем.

В работе [2] предложен метод моделирования слабо формализованного процесса с учетом не только количественных оценок, но и качественных, нечетко заданных, не поддающихся формализации критериев и связей между ними. Модель разрабатывается для последующего исследования этого процесса, прогнозирования его поведения, оптимизации функционирования. Метод базируется на технологии нечетких нейронных сетей. Показан метод оптимизации процесса с использованием факторного анализа.

Преимущества, которые предоставляет подход нейронных нечетких систем обуславливает его применение к совершенно различным областям. В работе [3] рассмотрены подходы применения метода искусственных нейронных сетей к решению задач диагностирования изделий. В работе [4] описаны экспериментальные результаты полученные при применении методов машинного обучения для обработки данных электрического каротажа скважин на урановых месторождениях пластово-инфильтрационного типа. В работе [5] предлагается подход к построению адаптивной экспертной системы, ядром которой является множество параллельных нейросетевых моделей. Приводятся результаты экспериментов, показывающих практическую целесообразность предлагаемого подхода. В работе [6] рассматривается система управления канализационной насосной станцией (К.Н.С.) с использованием регулятора на основе нейронной сети с нечеткой логикой. Произведено моделирование работы классического и нечеткого регулятора. Показана возможность реализации регулятора в виде адаптивной многослойной нейронной сети. В работе [7] рассматривается построение модели интеллектуальной системы управления безопасностью объекта информатизации ОВД, основанной на интеграции механизмов нечеткого логического вывода и нейронных сетей для формализации сложных процессов управления. В работе [8] рассматриваются возможности применения нейронных систем в структуре регуляторов, используемых в комплексе АСУТП химических и нефтяных производств. Анализируются основные преимущества и недостатки нейросетевых устройств. В работе [9] решается задача выявления и распознавания технологических событий и состояний узла инженерной сети на основе анализа временных рядов, характеризующих протекающие на объекте процессы. В работе [10] предлагается использование нечеткой нейронной сети для прогнозирования изменения эксплуатационного состояния автомобильных дорог. В работе [11] представлена методика краткосрочного прогнозирования электрических нагрузок с использованием модели нечеткого логического вывода, будем использовать модель вывода типа Сугено.

Вышеприведенный литературный обзор показывает какой широкий круг задач решается в настоящее время с применением нейронных сетей и нечеткой логики. В данном докладе представлены результаты применения нечётких нейронных сетей для искусственной иммунной системы терапии сульфаниламидами.

2. Нечеткие множества искусственной иммунной системы управления

Функциональная схема нечеткой иммунной системы оптимального управления терапевтическими дозами лекарственных средств представлена на рисунке 1.

В соответствии с результатами, полученными работе [12] представлен расчет оптимальных доз для пиелонефрита, для терапии которого используются сульфаниламиды. В соответствии с данными результатами схеме соответствуют переменные:
$L(t)$ – количественное представление ресурсов организма (связано с функциями принадлежности фаз хронического пиелонефрита в зависимости от количества лейкоцитов, активных лейкоцитов, СОЭ);
$P(t)$ – изменение количества микроорганизмов при пиелонефрите в зависимости от времени;
$C(t)$ – изменение количества обнаруженных микроорганизмов и угнетение, за счет сульфаниламидов, у микробов фермента, синтезирующего фолиевую кислоту, которая является для микроорганизмов фактором роста и размножения.

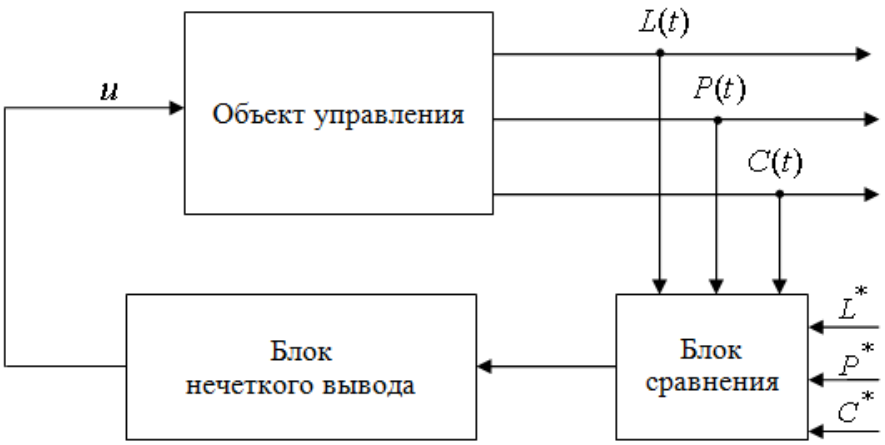

Рисунок 1 – Функциональная схема нечеткой иммунной системы оптимального управления воздействия лекарственных препаратов

В соответствии с результатами формирования нечетких множеств для нечеткой иммунной системы оптимального управления терапевтическими дозами лекарственных средств функции принадлежности обозначены следующим образом [13]:

1. **свойства сульфаниламидов:**

   (a) $\mu_{A1}(x)$ – функция принадлежности длительности выведения из организма сульфаниламидов с нечёткими термами:

   S – кратковременного действия;

   M – средней длительности действия;

   L – длительного действия;

   XL – сверхдлительного действия;

   XXL – сульфаниламиды, плохо всасывающиеся из желудочно-кишечного тракта и медленно выделяющиеся из организма.

   (b) $\mu_{A2}(x)$ – функция принадлежности ацетилирования сульфаниламидов:

   Б – быстрые ацетиляторы (ацетилирование сульфадимезина составляет более 50%);

   М – медленные ацетиляторы;

2. **лабораторные показатели пиелонефрита:**

   (a) $\mu_{B1}(x)$ – функция принадлежности фаз хронического пиелонефрита в зависимости от количества лейкоцитов с нечёткими термами:

   А – фаза активного воспалительного процесса;

   Л – фаза латентного воспалительного процесса;

   Р – фаза ремиссии, или клинического выздоровления;

(b) $\mu_{B2}(x)$ – функция принадлежности фаз хронического пиелонефрита в зависимости от количества микроорганизмов с нечёткими термами А, Л, Р;

(c) $\mu_{B3}(x)$ – функция принадлежности фаз хронического пиелонефрита в зависимости от количества активных лейкоцитов с нечёткими термами А, Л, Р;

(d) $\mu_{B4}(x)$ – функция принадлежности фаз хронического пиелонефрита в зависимости от СОЭ с нечёткими термами А, Л, Р.

В соответствии с разработанной схемой нечеткое управляющее устройство вырабатывает четкое управление u на основе нечеткого множества управляющих воздействий U с целью достижения желаемых значений L^*, P^*, C^*. Вся исходная информация о стратегии управления хранится в базах функций принадлежности $\mu(x)$ и базе правил условного логического вывода "если..., то...". Нечеткому множеству управляющих воздействий соответствует функция принадлежности $\mu(u)$, которое формируются на основе выбранного критерия качества и ограничений [12].

3. Нечеткая нейронная сеть искусственной иммунной системы

Исходные данные в значительной мере являются субъективными и не всегда адекватно отражают поведение реальной системы. Для устранения этого недостатка, эффективно использование нечетких многослойных нейронных сетей, в которых слои выполняют функции элементов системы нечеткого вывода [14]. Для искусственной иммунной системы разработана нечеткая многослойная нейронная сеть, в которой слои выполняют функции элементов системы нечеткого вывода (рисунок 2). Нейроны данной сети характеризуется набором параметров, настройка которых производится в процессе обучения, как у обычных нейронных сетей.

На рисунке 2 показана разработанная четырёхслойная нечеткая нейронная сеть, реализующая нелинейную зависимость:

$$u = \frac{\sum_{r=1}^{6} \omega_r \alpha_r}{\sum_{r=1}^{6} \alpha_r} \tag{1}$$

где ω – весовые коэффициенты;

α – произведение соответствующих функций нечетких множеств $\mu(x)$.

Слой 1 осуществляет процедуру фазификации. Функции принадлежности $\mu(x)$ соответствуют посылкам нечетких правил, а настраиваемыми параметрами этого слоя являются параметры функций принадлежности. Слой 2 рассматриваемой сети осуществляет вычисление результирующих функций принадлежности предпосылок нечетких правил. В данном случае этот слой не имеет настраиваемых параметров. Слой 3, состоящий из двух нейронов, осуществляет суммирование и взвешенное суммирование выходных сигналов слоя 2. Параметрами данного слоя являются весовые коэффициенты ω. Слой 4 реализует операцию деления:

$$u = \frac{f_1}{f_2}, \tag{2}$$

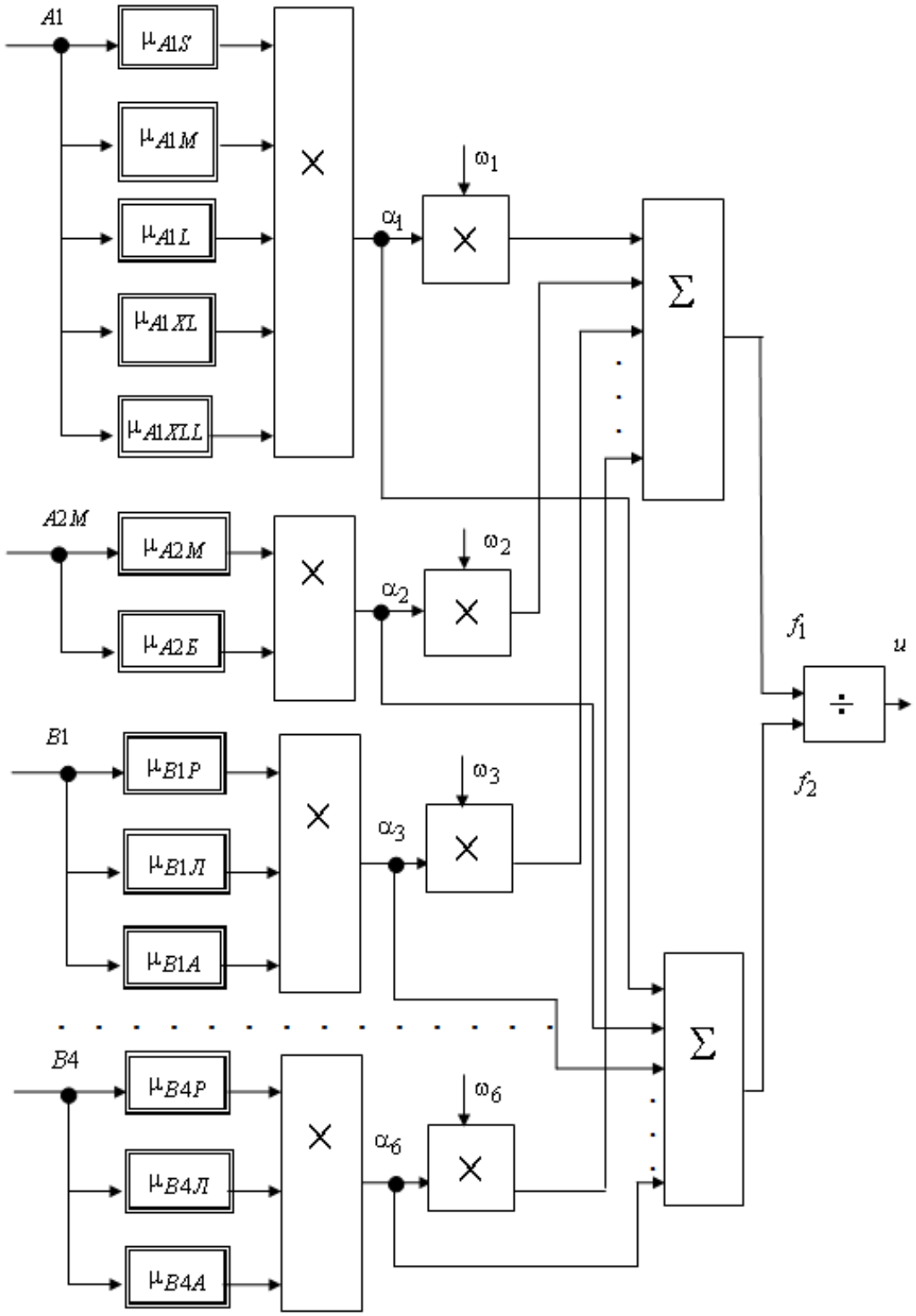

Рисунок 2 – Нечеткая нейронная сеть искусственной иммунной системы

и не содержит настраиваемых параметров.

Величина (2) представляет собой управляющее воздействие, подаваемое на вход объекта управления. В процессе обучения нечеткой нейронной сети определяются оптимальные значения изменяемых (настраиваемых) параметров.

4. Заключение

Разработана функциональная схема нечеткой иммунной системы оптимального управления терапевтическими дозами сульфаниламидов для терапии пиелонефрита на основе методологии нечеткой логики. Для блока логического вывода разработана нечеткая многослойная нейронная сеть, в которой слои выполняют функции элементов системы нечеткого вывода.

Исследования выполнены по гранту №ГР 0115РК00549 МОН РК по теме: Компьютерный молекулярный дизайн лекарственных препаратов на основе иммунносетевого моделирования (2015-2017 гг.).

Литература

[1] Мищенко В.А., Коробкин А.А. Принципы нечеткой логики на примере нечетких нейронных сетей // Современные проблемы науки и образования. – 2012. – №1.

[2] Левченко Н. Г. Оптимизация слабо формализованных процессов с использованием нечеткой нейронной модели // Вестник государственного университета морского и речного флота им. адмирала С.О. Макарова. – 2012. – №4(16). – С. 105-114.

[3] Кацуба Ю. Н., Власова И.В. Применение искусственных нейронных сетей для диагностирования изделий. – 2015. – С. 21-29.

[4] Бектемысова Г.У., Искаков С.Х., Кучин Я.И., Мухамедиев Р.И., Саинова С., Абдильманова А. Сравнительный анализ "обучаемости"искусственных нейронный сетей прямого распространения и алгоритма $k - nn$ в задаче интерпретации данных электрического каротажа. – 2015. – № 2. – С. 134-137.

[5] Еськин А.О., Костюк В.П. Разработка и исследование параллельных нейросетевых моделей для диагностики сложных систем // Вестник Саратовского государственного технического университета. – 2013. – № 1(73). – С. 142-150.

[6] Есилевский В.С., Кузнецов В.Н., Панов В.П. Управление насосными агрегатами к.н.с. с помощью систем нечетко-нейронного управления // Вестник Воронежского государственного технического университета. – 2012. – №9. – С.12-16.

[7] Дунин В.С., Бокова О.И., Хохлов Н.С. Построение модели интеллектуальной системы управления безопасностью объекта информатизации ОВД на основе нечеткой нейронной продукционной сети // Вестник Воронежского института МВД России. – 2011. – №2. – С. 48-58.

[8] Мишта П.В., Бызов П.Г. Нейронные сети. Перспективное направление развития регулирующих устройств в АСУТП // Известия Волгоградского государственного технического университета. – 2011. – №3. – С.127-130.

[9] Вульфин А.М., Фрид А.И. Нейросетевая модель анализа технологических временных рядов в рамках методологии data mining // Информационно-управляющие системы. – 2011. – №5. – С.31-38.

[10] Щербаков В.М., Скоробогатченко Д.А., Авдеев А.А., Аль-гунаид М.А. Проблемы проектирования систем прогнозирования эксплуатационного состояния автомобильных дорог на основе нечетких нейронных сетей // Известия Волгоградского государственного технического университета. – 2015. – № 10. – С.82-87.

[11] Сахно Е.П., Дьяченко Р.А., Решетняк М.Г., Капустин К.Ю. К вопросу краткосрочного прогнозирования электрических нагрузок с применением нечетких нейронных сетей // Современные проблемы науки и образования. – 2013. – №2. – 7 с.

[12] Ширяева О.И., Денисова Т.Г. Функциональная схема нечеткой иммунной системы оптимального управления воздействия лекарственных препаратов // Труды XI Международной азиатской школы-семинара "Проблемы оптимизации сложных систем". – Иссык-Куль, 2015. – С. 685-693.

[13] Shiryayeva O.I. Investigation of artificially immune system with using of fuzzy logic // Новосибирск: Вычислительные технологии (совместный сборник журналов с "Вестник КазНУ. Серия математика, механика, информатика"). – 2015. – С. 209-217.

[14] Усков А.А. Системы с нечеткими моделями объектов управления: Монография. - Смоленск: Смоленский филиал АНО ВПО ЦС РФ "Российский университет кооперации 2013. – 153 с.

References

[1] Mishhenko V.A., Korobkin A.A. Principy nechetkoj logiki na primere nechetkih nejronnyh setej // Sovremennye problemy nauki i obrazovanija. – 2012. – №1.

[2] Levchenko N. G. Optimizacija slabo formalizovannyh processov s ispolzovaniem nechetkoj nejronnoj modeli // Vestnik gosudarstvennogo universiteta morskogo i rechnogo flota im. admirala S.O. Makarova. – 2012. – №4(16). – S. 105-114.

[3] Kacuba Ju. N., Vlasova I.V. Primenenie iskusstvennyh nejronnyh setej dlja diagnostirovanija izdelij. – 2015. – S. 21-29.

[4] Bektemysova G.U., Iskakov S.H., Kuchin Ja.I., Muhamediev R.I., Sainova S., Abdilmanova A. Sravnitelnyj analiz "obuchaemosti"iskusstvennyh nejronnyj setej prjamogo rasprostranenija i algoritma $k-nn$ v zadache interpretacii dannyh jelektricheskogo karotazha. – 2015. – № 2. – S. 134-137.

[5] Eskin A.O., Kostjuk V.P. Razrabotka i issledovanie parallelnyh nejrosetevyh modelej dlja diagnostiki slozhnyh sistem // Vestnik Saratovskogo gosudarstvennogo tehnicheskogo universiteta. – 2013. – № 1(73). – S. 142-150.

[6] Esilevskij V.S., Kuznecov V.N., Panov V.P. Upravlenie nasosnymi agregatami k.n.s. s pomoshhju sistem nechetko-nejronnogo upravlenija // Vestnik Voronezhskogo gosudarstvennogo tehnicheskogo universiteta. – 2012. – №9. – S.12-16.

[7] Dunin V.S., Bokova O.I., Hohlov N.S. Postroenie modeli intellektualnoj sistemy upravlenija bezopasnostju obekta informatizacii OVD na osnove nechetkoj nejronnoj produkcionnoj seti // Vestnik Voronezhskogo instituta MVD Rossii. – 2011. – №2. – S. 48-58.

[8] Mishta P.V., Byzov P.G. Nejronnye seti. Perspektivnoe napravlenie razvitija regulirujushhih ustrojstv v ASUTP // Izvestija Volgogradskogo gosudarstvennogo tehnicheskogo universiteta. – 2011. – №3. – S.127-130.

[9] Vulfin A.M., Frid A.I. Nejrosetevaja model analiza tehnologicheskih vremennyh rjadov v ramkah metodologii data mining // Informacionno-upravljajushhie sistemy. - 2011. - №5. - S.31-38.

[10] Shherbakov V.M., Skorobogatchenko D.A., Avdeev A.A., Al-gunaid M.A. Problemy proektirovanija sistem prognozirovanija jekspluatacionnogo sostojanija avtomobilnyh dorog na osnove nechetkih nejronnyh setej // Izvestija Volgogradskogo gosudarstvennogo tehnicheskogo universiteta. – 2015. – № 10. – S.82-87.

[11] Sahno E.P., Djachenko R.A., Reshetnjak M.G., Kapustin K.Ju. K voprosu kratkosrochnogo prognozirovanija jelektricheskih nagruzok s primeneniem nechetkih nejronnyh setej // Sovremennye problemy nauki i obrazovanija. – 2013. – №2. – 7 s.

[12] Shiryaeva O.I., Denisova T.G. Funkcionalnaja shema nechetkoj immunnoj sistemy optimalnogo upravlenija vozdejstvija lekarstvennyh preparatov // Trudy XI Mezhdunarodnoj aziatskoj shkoly-seminara "Problemy optimizacii slozhnyh sistem". – Issyk-Kul, 2015. – S. 685-693.

[13] Shiryayeva O.I. Investigation of artificially immune system with using of fuzzy logic // Novosibirsk: Vychislitelnye tehnologii (sovmestnyj sbornik zhurnalov s "Vestnik KazNU. Serija matematika, mehanika, informatika"). – 2015. – S. 209-217.

[14] Uskov A.A. Sistemy s nechetkimi modeljami obektov upravlenija: Monografija. – Smolensk: Smolenskij filial ANO VPO CS RF "Rossijskij universitet kooperacii 2013. – 153 s.

УДК 681.5

Юничева Н.Р.

Институт информационных и вычислительных технологий КН МОН РК,
Республика Казахстан, г. Алматы
E-mail: naduni@mail.ru

Исследование динамических свойств нелинейных систем с неточными данными

Развитие прямого метода Ляпунова, успешно зарекомендовавшего себя при решении многих задач теории управления, на класс интервально-заданных объектов приводит к необходимости исследования множеств решений интервальных матричных уравнений Ляпунова, Сильвестра. Сложность математического описания таких множеств приводит к экспоненциальному росту вычислительных затрат при решении поставленных задач теории управления. Однако в большинстве случаев на практике достаточно ограничиться рассмотрением внешних либо внутренних интервальных оценок этих множеств. Использование S-процедуры и методов интервального анализа позволило избежать громоздких вычислительных трудностей. В статье на основе прямого метода Ляпунова предложен алгебраический критерий абсолютной устойчивости нулевого положения равновесия интервальной динамической системы с векторной нелинейностью секторного типа. Изучение свойств нелинейных динамических систем в условиях параметрической неопределенности интервального типа представляет большой научный интерес. В данной работе рассматривается нелинейность секторного типа. Полученные достаточные условия абсолютной устойчивости нулевого положения равновесия рассматриваемой нелинейной интервальной динамической системы не требуют больших вычислительных затрат для их проверки, в связи с чем эти условия могут быть успешно применены на практике.
Ключевые слова: Неточные данные, устойчивость динамической системы, допустимое множество решений.

Yunicheva N.R.

Study of dynamic properties of nonlinear systems with imperfect data

The development of Lyapunov's direct method, successfully proven in solving many problems of control theory, a class of interval-specified objects leads to the necessity of the study of solution sets of interval matrix Sylvester and Lyapunov equations. The complexity of the mathematical description of such sets leads to an exponential growth in computing costs in solving the problems of control theory. However, in most cases in practice it suffices to consider the outer or inner interval estimates of these sets. Using the S-procedure and methods of interval analysis thus avoiding cumbersome computational difficulties. Based on the direct Lyapunov method proposed algebraic criterion for the absolute stability of the zero equilibrium position interval dynamic system with vector nonlinearity of sector type. Studying the properties of nonlinear dynamic systems with unknown parameters interval type is of great scientific interest. In this paper, we consider the nonlinearity of sector type. Obtained sufficient conditions for zero equilibrium position of absolute stability of the nonlinear interval dynamic systems do not require computationally expensive to test them, in connection with which these conditions can be successfully applied in practice.
Key words: Inaccurate data, the stability of dynamic system, the feasible set of solutions.

Юничева Н.Р.

Анық емес мәліметтерден тұратын сызықты емес жүйелердің динамикалық күйін зерттеу

Ляпуновтың тура әдісінің дамуы басқару теориясының көптеген тапсырмаларын шешуде, берілген-аралық объектілер класы үшін аралық Ляпунов, Сильвестрдың матарицалық теңдеулер шешімдерін зерттеу қажеттілігіне әкеліп, жақсы жағынан көрсете білді. Мұндай жиындардың математикалық сипаттамасының күрделілігі басқару теориясының қойылған тапсырмаларын шешуде экспоненциалды өсуіне әкеледі. Бірақ көп жағдайда тәжірибеде бұл жиындардың ішкі не сыртқы аралық бағалауын қарастыру жеткілікті. S-процедурлар мен интервалды талдау әдістерін қолдану үлкен көлемдегі есептеулер қиындықтарын жойды. Мақалада Ляпуновтың тура әдісі негізінде тепе-теңдік нөлдік күйінің абсолютті тұрақтылығының векторлы сызықты емес секторлы типті аралық динамикалық жүйенің алгебралық критерийі ұсынылды. Сызықты емес динамикалық жүйелерді параметрлі белгісіздік шартындағы интервалды типі үлкен ғылыми қызығушылық тудырады. Берілген зерттеуде сызықты емес секторлы тип нөлдік күйдегі тепе-теңдіктегі абсолютты тұрақтылық нәтижесінде алынған жеткілікті шарттары қарастырылып отырған сызықты емес аралық динамикалық жүйе үлкен көлемдегі есептеулер шығынын қажет етпейтіндіктен тәжірибеде табысты қолдануға болады.

Түйін сөздер: анық емес мәліметтер, динамикалық жүйенің тұрақтылығы, ұйғарымды жиын шешімі.

1. Введение

Математическое описание явлений и процессов природы чаще всего осуществляется с той или иной долей погрешности. Такие погрешности приводят к тому, что математическая модель не достаточно полно отражает все свойства исследуемых процессов. Желание устранить этот недостаток способствовало развитию нового научного направления в современной теории управления, которое приобретает в настоящее время все большую актуальность и востребованность на практике. В рамках данного направления погрешности моделирования, обусловленные причинами различного типа, учитываются непосредственно в самой математической модели путем введения интервальных параметров с заданными нижними и верхними границами. Такой подход к проблеме позволяет судить о наличии тех или иных свойств исследуемого явления или процесса в условиях, так называемой, параметрической неопределенности. Наиболее развитым в смысле богатства идей и методов исследования свойств в условиях параметрической неопределенности оказался класс линейных математических моделей, которому и посвящена большая часть научных работ в этой области. Однако, на практике есть случаи, когда нельзя ограничиться рассмотрением только линейных математических моделей. Более того, ряд других особенностей природных процессов таких, как наличие конечной памяти, не может быть оставлен без внимания для более адекватного описания этих процессов. К сожалению, на сегодняшний день арсенал методов исследования динамических свойств процессов, описываемых нелинейными математическими моделями в условиях параметрической неопределенности, представлен в современных научных работах крайне скупо. В этой связи особую актуальность приобретают задачи разработки новых и развитие существующих методов исследования свойств нелинейных динамических моделей процессов в условиях параметрической неопределенности [1]. Изучение свойств нелинейных динамических систем в условиях параметрической неопределенности интервального типа представляет большой научный интерес. Многие из вопро-

сов, касающиеся исследования устойчивости нелинейных интервальных динамических систем, заданных в пространстве состояний, до сих пор остаются открытыми. В настоящей работе рассматривается нелинейность секторного типа. Задачи исследования динамических систем с нелинейностью секторного типа, математические модели которых точно известны, восходят к работам А.И.Лурье [2] и В.М.Попова [3] и составляют два взаимосвязанных направления современной теории абсолютной устойчивости. Наличие интервальной неопределенности обусловило появление нового витка актуальности задач исследования нелинейных систем А.И.Лурье в условиях параметрической неопределенности. Так, например, в работе [4] получены робастные модификации частотных критериев абсолютной устойчивости при неопределенности в линейной части системы. В отличие от указанной работы, в которой линейная часть задана в виде семейства полиномов, наибольший интерес в этой области представляет исследование нелинейных систем, заданных в пространстве состояний. В работе [5], используя функционалы Ляпунова-Красовского, получены достаточные условия абсолютной устойчивости нелинейной интервальной системы с запаздыванием в состоянии и нелинейностью секторного типа.

2. Постановка задачи

Рассматривается нелинейная динамическая система, математическая модель которой может быть представлена в пространстве состояний в условиях интервальной неопределенности параметров в виде следующего соотношения

$$\dot{x}(t) \in Ax(t) + B\varphi(\sigma), x(t_0) = x_0, t \in [t_0, \infty), \tag{1}$$

где t – независимая переменная (время); $x(t) = (x_i(t))$ – вектор состояний, компонентами которого являются непрерывные на $[t_0, \infty)$ функции $x_i(t)$, т.е. $x_i(t) \in C[t_0, \infty)$, $1 \le i \le n$; в начальный момент времени t_0 значение вектора состояний предполагается известным x_0. $A \in IR^{n\times n}$,$B \in IR^{n\times m}$ – постоянные интервальные матрицы размерности $n \times n$ и $n \times m$ соответственно. $\varphi(\cdot)$ – непрерывно дифференцируемая вектор-функция $\varphi : R \to R^m$, компоненты φ_i, $1 \le i \le m$, которой удовлетворяют ограничениям секторного типа (график функции $\varphi_i(\varsigma)$ расположен в секторе между прямыми $\varphi_i = 0$ и $\varphi_i = \mu_{1i}\varsigma$, $\mu_i > 0$, $1 \le i \le m$). Класс вектор-функций, обладающих указанными свойствами, обозначим через Φ_m, т.е.

$$\varphi \in \Phi_m = \left\{\phi_1(\varsigma) \in C^1([t_0, \infty), R, R^m) \;\middle|\; 0 \le \phi_i(\varsigma)\varsigma \le \mu_i\varsigma^2,\ \phi_i(0) = 0,\ 1 \le i \le m\right\}.$$

Здесь $C^1([t_0, \infty), R, R^m)$ – пространство непрерывно дифференцируемых на $[t_0, \infty)$ вектор-функций $\varphi : R \to R^m$. Величина определяется согласно выражению

$$\sigma = r^T x(t), \tag{2}$$

где $r \in R^n$ – вектор размерности $n \times 1$. Определение 1. *Под решением* (1) – (2) *будем понимать всякую абсолютно непрерывную функцию* $x(t, t_0, x_0) = x(t)$*, удовлетворяющую при некоторых значениях* $A \in A$ *и* $B \in B$ *следующей нелинейной системе дифференциальных уравнений*

$$\begin{cases} \dot{x}(t) = Ax(t) + B\varphi(\sigma), \\ \sigma = r^T x(t), \end{cases} \qquad x(\mathrm{t}_0) = x_0, \quad \mathrm{t} \in [\mathrm{t}_0, \infty). \tag{3}$$

В силу свойств функции φ существует тривиальное решение $x(t) \equiv 0$ системы (1), которое является ее положением равновесия.
Определение 2. *Будем говорить, что нелинейная интервальная динамическая система* (1) – (2) *обладает некоторым свойством P, если этим свойством обладает любая система* (3) *для* $A \in A$ *и* $B \in B$.
Задача: определить условия абсолютной устойчивости положения равновесия $x(t) \equiv 0$ нелинейной интервальной динамической системы (1) – (2) с векторной нелинейностью секторного типа в смысле определения 2.

3. Основной результат

Будем предполагать, что пара интервальных матриц (A, B) стабилизируема, т.е. для любых $A \in A$ и $B \in B$ стабилизируемой является пара (A, B).
Решение поставленной задачи будет осуществлено на основе прямого метода Ляпунова посредством выбора функции Ляпунова в виде квадратичной формы

$$V(x) = x^T H x,$$

где $H \in R^{n\times n}$, $H = H^T$ – симметрическая положительно определенная матрица.
Для того, чтобы сформулировать основной результат введем в рассмотрение некоторые объекты и приведем необходимые определения из интервального анализа [6].
Введем в рассмотрение вектор $\mu \in R^m$

$$\mu = (\mu_1, \mu_2, \ldots, \mu_m)^T$$

и диагональную матрицу $\Lambda \in R^{m\times m}$

$$\Lambda = \mathrm{Diag}\{\lambda_i, 1 \le i \le m\}.$$

Определение 3. *Интервальную квадратную матрицу* $G \in IR^{n\times n}$, $G = (g_{\mathrm{ij}})$,$g_{\mathrm{ij}} = \left[\underline{g}_{\mathrm{ij}},\overline{g}_{\mathrm{ij}}\right]$, $1 \le i, j \le n$ *будем называть положительно определенной и записывать* $G \triangleright 0$, *если положительно определена любая матрица* $G \in G$, *т.е.* $\forall G \in G$ *квадратичная форма* $x^T G x > 0 \ \ \forall x \in R^n \backslash \{0\}$.
Определение 4. *Множество матриц вида*

$$G^{sym} = \left[\underline{G}^{sym}, \overline{G}^{sym}\right] = \left\{G \in R^{n\times n} \ \middle|\ G{=}G^T, \underline{G}^{sym} \le G \le \overline{G}^{sym}\right\},$$

где знак неравенства понимается в поэлементном смысле, будем называть симметрической интервальной матрицей и записывать $G^{sym} = (G^{sym})^T$.
Пусть G_{11}^{sym} – некоторая интервальная симметрическая положительно определенная матрица размерности $(n \times n)$, $G_{12} \in IR^{n\times m}$ – некоторая интервальная матрица размерности $(n \times m)$ и $G_{22} = G_{22}^T \triangleright 0$ – некоторая симметрическая положительно определенная матрица размерности $(m \times m)$ такие, что интервальная симметрическая матрица следующего блочного вида

$$G^{sym} = \begin{pmatrix} G_{11}^{sym} & G_{11} \\ G_{21} & G_{22} \end{pmatrix} = \begin{pmatrix} G_{11}^{sym} & G_{11} \\ G_{12}^T & G_{22} \end{pmatrix}$$

положительно определена. Для точечных значений $A \in A$, $B \in B$, $G_{11} \in G_{11}$, $G_{12} \in G_{12}$ и G_{22} введем в рассмотрение следующую систему нелинейных матричных алгебраических уравнений

$$\begin{cases} A^T H + HA + SS^T = -G_{11}; \\ HB + 1/2\Lambda r\mu^T + S\Gamma = -G_{12}; \\ -\Lambda + \Gamma\Gamma^T = -G_{22}; \end{cases} \tag{4}$$

относительно матриц $H \in R^{n\times n}$, $S \in R^{n\times m}$ и $\Gamma \in R^{m\times m}$, которую для краткости обозначим $X(H, S, \Gamma) = 0$.

Уравнения системы (4) называют также [2] разрешающими уравнениями Лурье.

Определение 5. *Множество троек* (H, S, Γ) *декартового произведения* $R^{n\times n} \times R^{n\times m} \times R^{m\times m}$ *вида*

$$\Sigma_{tol}(A, B, G_{11}^{sym}, G_{12}) = \{(H, S, \Gamma) \in R^{n\times n} \times R^{n\times m} \times R^{m\times m} \,|(\forall A \in A) \times \tag{5}$$

$$\times (\forall B \in B)(\exists G_{11} \in G_{11}^{sym})(\exists G_{12} \in G_{12})(X(H, S, \Gamma) = 0)\}$$

называется допустимым множеством решений интервальной системы нелинейных матричных алгебраических уравнений [7]

$$\begin{cases} A^T H + HA + SS^T = -G_{11}^{sym}; \\ HB + 1/2\Lambda r\mu^T + S\Gamma = -G_{12}; \\ -\Lambda + \Gamma\Gamma^T = -G_{22}. \end{cases} \tag{6}$$

По аналогии с (4) интервальные уравнения системы (6) будем называть интервальными разрешающими уравнениями Лурье.

Теорема. *Пусть для заданных интервальных матриц* $A \in IR^{n\times n}$, $B \in IR^{n\times m}$, *векторов* $r \in R^n$, $\mu \in R^m$, *некоторых интервальных матриц* $G_{11}^{sym} \triangleright 0$, $G_{12} \in IR^{n\times m}$ *и некоторой диагональной матрицы* $\Lambda \in R^{m\times m}$ *выполнены следующие условия:*

1. *допустимое множество решений (5) системы интервальных разрешающих уравнений Лурье (6) непусто, т.е.* $(H^*, S^*, \Gamma^*) \in \Sigma_{tol}(A, B, G_{11}^{sym}, G_{12})$;
2. *матрица* H^* *является симметрической положительно определенной.*

Тогда нулевое положение равновесия $x(t) \equiv 0$ *нелинейной интервальной динамической системы* (1) – (2) *абсолютно устойчиво для суперпозиции выбранных классов нелинейностей.*

Доказательство. В соответствии с прямым методом Ляпунова вычислим первую производную функции Ляпунова при произвольных, но фиксированных значениях на траекториях движения системы (3).

$$\dot{V}(x)\Big|_{(4)} = (Ax + B\varphi(\sigma))^T Hx + x^T H(Ax + B\varphi(\sigma)).$$

Для определения условий отрицательной определенности производной $\dot{V}(x)$ в части пространства $R^n \times R^m$, выделяемой ограничениями секторного типа, воспользуемся S-процедурой [8]. Предполагая существование положительных чисел $\lambda_i > 0$, $i = 1, 2, \ldots, m$, и опуская выкладки, запишем окончательное выражение для S-формы [8]

$$S(x, \varphi) = x^T \left(A^T H + HA\right) x + \varphi^T \left(B^T H + {}^1\!/_2 \Lambda\mu r^T\right) + x^T \left(HB + {}^1\!/_2 r\mu^T \Lambda\right) \varphi - \varphi^T \Lambda\varphi. \tag{7}$$

Используя матрицы G_{11}^{sym}, $G_{12} \in IR^{n\times m}$ и G_{22}, построим интервальную симметрическую положительно определенную матрицу G^{sym}, представимую в блочном виде следующим образом

$$G^{sym} = \begin{pmatrix} G_{11}^{sym} & G_{12} \\ G_{12}^T & G_{22} \end{pmatrix},$$

и сформируем следующее множество отрицательно определенных квадратичных форм переменных x и φ

$$\Xi(x,\varphi) = \left\{ -\left(S^T x + \Gamma\varphi\right)^T \left(S^T x + \Gamma\varphi\right) - \begin{pmatrix} x^T & \varphi^T \end{pmatrix} G \begin{pmatrix} x \\ \varphi \end{pmatrix} \;\middle|\; G \in G^{sym} \right\},$$

которое для удобства запишем в виде

$$\Xi(x,\varphi) = -\left(S^T x + \Gamma\varphi\right)^T \left(S^T x + \Gamma\varphi\right) - \begin{pmatrix} x^T & \varphi^T \end{pmatrix} G^{sym} \begin{pmatrix} x \\ \varphi \end{pmatrix}. \tag{8}$$

Потребуем, чтобы для любых значений $A \in A$ и $B \in B$ S-форма (7) принадлежала множеству (8). Данное требование будет удовлетворено, если для любых значений $A \in A$ и $B \in B$ существует такая матрица $G \in G^{sym}$ или, что эквивалентно, существуют такие матрицы $G_{11} \in G_{11}^{sym}$ и $G_{12} \in G_{12}$ что имеет место равенство

$$S(x,\varphi) = -\left(S^T x + \Gamma\varphi\right)^T \left(S^T x + \Gamma\varphi\right) - \begin{pmatrix} x^T & \varphi^T \end{pmatrix} G \begin{pmatrix} x \\ \varphi \end{pmatrix}. \tag{9}$$

Расписывая последнее равенство в развернутом виде, получим

$$x^T\left(A^T H + HA\right)x + \varphi^T\left(B^T H + {}^1\!/_2 \Lambda\mu r^T\right) + x^T\left(HB + {}^1\!/_2 r\mu^T\Lambda\right)\varphi - \varphi^T\Lambda\varphi =$$

$$= x^T\left(SS^T + G_{11}\right)x - \varphi^T\left(\Gamma^T S^T + G_{12}^T\right)x - x^T\left(S\Gamma + G_{12}\right)\varphi - \varphi^T\left(\Gamma^T\Gamma + G_{22}\right)\varphi.$$

Последнее равенство будет выполнено, если система уравнений (4) является совместной. По условию теоремы $(H^*, S^*, \Gamma^*) \in \Sigma_{tol}(A, B, G_{11}^{sym}, G_{12})$. Это означает, что для любых значений существуют такие матрицы $G_{11} \in G_{11}^{sym}$ и $G_{12} \in G_{12}$, что матрицы H^*, S^*, Γ^* являются решением (4). Далее справедливой является следующая цепочка импликаций (для любых $A \in A$ и $B \in B$ существуют такие $G_{11} \in G_{11}^{sym}$ и $G_{12} \in G_{12}$, что имеет место равенство (9))⇒(для любых $A \in A$ и $B \in B$ S-форма (7) принадлежит множеству (8)) ⇒ (для любых $A \in A$ и $B \in B$ S-форма (7) является отрицательно определенной формой переменных x и φ) ⇒ (для любых $A \in A$ и $B \in B$ первая производная $\dot{V}(x)$ по времени функции Ляпунова на траекториях движения (3) будет отрицательной в части пространства $R^n \times R^m$, выделяемой ограничениями секторного типа) ⇒ (для любых $A \in A$ и $B \in B$ в силу положительной определенности H^* (условие 2 теоремы) положение равновесия $x(t) \equiv 0$ динамической системы (3) абсолютно устойчиво для выбранного класса векторной нелинейности) ⇒
(положение равновесия $x(t) \equiv 0$ нелинейной интервальной динамической системы (1) – (2) абсолютно устойчиво для выбранного класса векторной нелинейности в смысле определения 2).

Теорема доказана.

4. Заключение

Таким образом, как указывалось выше, развитие прямого метода Ляпунова на класс интервально-заданных объектов (или объектов с неточными данными) приводит к необходимости исследования множеств решений интервальных матричных уравнений Ляпунова, следовательно, математическое описание таких множеств приводит к экспоненциальному росту вычислительных затрат при решении поставленных задач теории управления как при решении вопросов синтеза, так и при исследовании динамических свойств подобных систем. Использование S-процедуры и методов интервального анализа позволило избежать громоздких вычислительных трудностей. Полученные достаточные условия абсолютной устойчивости нулевого положения равновесия рассматриваемой нелинейной интервальной динамической системы не требуют больших вычислительных затрат для их проверки, в связи с чем эти условия могут быть успешно применены на практике.

Примечание

Данная работа выполнена при финансовой поддержке научно – исследовательского проекта № 3329 / ГФ4 КН МОН РК.

Особую благодарность автор выражает Ивлеву Руслану Сергеевичу за ценные замечания и поправки.

Литература

[1] С.П.Соколова, Р.С.Ивлев Экспоненциальная устойчивость интервальной нелинейной системы // Труды СПИИРАН, 2006. – Вып. 3. – Том 2. –С. 366-376..

[2] А.И.Лурье Некоторые нелинейные задачи теории автоматического регулирования. –М.:Гостехиздат, 1951.

[3] В.М. Попов Гиперустойчивость автоматических систем. – М.: Наука, 1970.

[4] Э.И.Джури, К.Премаратне, М.М. Эканайаке Робастная абсолютная устойчивость дискретных систем //Автоматика и Телемеханика. – 1999. –№3. – С.97-118.

[5] Р.С.Ивлев Абсолютная устойчивость нелинейных динамических систем с параметрической неопределенностью интервального типа и запаздывающим аргументом //Материалы Межд. конференции “Вычислительные технологии и математическое моделирование в науке, технике и образование”, ВТММ-2002. – Новосибирск - Алматы, 2002. – С. 27-34.

[6] С.А. Калмыков,Ю.И. Шокин, З.Х.Юлдашев Методы интервального анализа. – Н.: Наука СО, 1986. – 224с.

[7] Л.Жолен ,М. Кифер ,О. Дидри , Э.Вальтер Прикладной интервальный анализ. М.: Институт компьютерных исследований. – 2007. – 467с.

[8] А.Х.Гелиг, Г.А.Леонов, В.А.Якубович Устойчивость нелинейных систем с неединственным состоянием равновесия. – М.: Наука. 1978. –289 с.

References

[1] S.P.Sokolova, R.S.Ivlev Eksponensialnaya ystoichivost intervalnoi nelineinoi sistemi // Trudi SPIIRAN, 2006. – №.3. – Tom 2. –P. 366-376.

[2] A.I.Lurie Nekotorie nelineinie zadachi teorii avtomaticheskogo regulirovaniya. –M.:Gostehizdat, 1951.

[3] V.M. Popov Giperystoichivost avtomaticheskih sistem. – M.: Nayka, 1970.

[4] E.I.Dzhuri, K.Premaratne, M.M. Ekanaike Robastnaya absolyutnaya ystoichivost diskretnih sistem //Avtomatika i Telemehanika. – 1999. –№3. – P.97-118.

[5] R.S.Ivlev Fbsolyutnaya ystoichivost nelineinih dinamicheskih sistem s intervalnogo tipa i zapazdivayuchim argumentom //Materiali Mazhd. konferensii "BVichislitelnie tehnologii i matematicheskoe modelirovanie v nayke, tehnike i obrazovanie", VTMM-2002. – Novosibirsk - Almaty, 2002. – P. 27-34.

[6] S.A. Kalmikov,Yu.I. Shokin, Z.H.Yuldashev Metodi intervalnogo analiza. – N.: Nayka SO, 1986. – 224p.

[7] L.Zholen, M. Kifer ,O. Didri, E.Valter Prikladnoi intervalni analiz. M.: Institut kompyuternih issledovanii. – 2007. – 467p.

[8] A.H.Gelig, G.A.Leonov, V.A.Yakubovich Ystoichivost nelineinih sistem s needinstvennim sostoyaniem ravnovesiya. – M.: Nayka. 1978. –289 p.

СВЕДЕНИЯ ОБ АВТОРАХ

1. *Айда-заде Камиль Раджабович* - заведующий лаборатории Института систем управления НАН Азербайджана, доктор физико-математических наук, профессор

2. *Байшемиров Жарасбек Дуйсембекович* - старший научный сотрудник Института информационных и вычислительных технологий КН МОН РК, PhD доктор

3. *Дюсенбаева Дилмуханбет Самуратович* - научный сотрудник Института информационных и вычислительных технологий КН МОН РК

4. *Денисова Татьяна Геннадиевна* - ведущий научный сотрудник Института информационных и вычислительных технологий КН МОН РК, кандидат медцинских наук

5. *Жанбырбаев А.Б.* - доцент Казахского национального педагогического университета имени Абая, кандидат физико-математических наук

6. *Калимолдаев Максат Нурадилович* - генеральный директор Института информационных и вычислительных технологий КН МОН РК, доктор физико-математических наук, член-корреспондент НАН РК, профессор

7. *Кудайкулов Анарбай Кудайкулович* - профессор Института информационных и вычислительных технологий КН МОН РК, доктор физико-математических наук

8. *Капалова Нурсулу Алдажаровна* - ведущий научный сотрудник Института информационных и вычислительных технологий КН МОН РК, кандидат технических наук

9. *Кабылханова А.Б.* - магистр Института информационных и вычислительных технологий КН МОН РК

10. *Карашбаева Ж.О.* - научный сотрудник Института информационных и вычислительных технологий КН МОН РК

11. *Магзом Мирас Мухтарулы* - младший научный сотрудник Института информационных и вычислительных технологий КН МОН РК, PhD докторант

12. *Муслимова А.К.* - PhD докторант Института информационных и вычислительных технологий КН МОН РК

13. *Нысанбаева Сауле Еркебулановна* - главный научный сотрудник Института информационных и вычислительных технологий, доктор технических наук, ассоциированный профессор

14. *Рысбайулы Болатбек* - зав. кафедрой Международного университета информационных технологий, доктор физико-математических наук, профессор

15. *Пак Иван Тимофеевич* - главный научный сотрудник Института информационных и вычислительных технологий КН МОН РК, доктор технических наук, профессор

16. *Тойбаева Шара Джолдаспековна* - PhD докторант Института информационных и вычислительных технологий КН МОН РК

17. *Ташев Азат Арипович* - ведущий научный сотрудник Института информационных и вычислительных технологий КН МОН РК, доктор технических наук, профессор

18. *Талыбов Сахават Гурбан оглы* - ведущий научный сотрудник Института систем управления НАН Азербайджана

К СВЕДЕНИЮ АВТОРОВ

1. В журнал "Вестник КазНУ. Серия математика, механика, информатика" принимаются набранные только в текстовом формате LaTeX2ε на казахском, русском или английском языках, ранее не опубликованные проблемные, обзорные, дискуссионные статьи в области естественных наук, где освещаются результаты фундаментальных и прикладных исследований.

2. Материалы следует направлять по адресу: 050040 Алматы, ул. аль-Фараби, 71, корпус 13, Научно-исследовательский институт механики и математики КазНУ им. аль-Фараби, каб. 125, тел. 377-32-23. Электронная почта: Lazat-dairbayeva@mail.ru (ответственному секретарю редколлегии, Даирбаева Л.М.)

3. Статья должна сопровождаться письмом от учреждения, в котором выполнена данная работа, где указываются сведения об авторах: Ф.И.О. полностью, место их работы, должность (название вуза, центра без сокращений, факультета, кафедры), рабочий телефон, факс, e-mail, домашний адрес и контактный телефон.

4. В редакцию необходимо представить электронную версию статьи: tex-файлы работы и файлы рисунков на одном диске. Для файлов рисунков рекомендуется использовать средства основного пакета LaTeX2ε или формат eps [см. п.7]. Указывается код по УДК. В редакцию также представляется оттиск работы в двух экземплярах.

5. Объем статьи, включая список литературы, таблицы и рисунки с подрисуночными надписями, аннотации, не должен превышать 15 страниц печатного текста. Минимальный объем статьи - 5 страниц. В начале работы после заголовка и фамилий авторов работы помещается её аннотация в объеме 200-250 слов на том же языке, на котором набран основной текст. Кроме сведений, которые можно почерпнуть из заголовка, аннотация должна отражать методы исследования, основные результаты статьи, их новизну и указывать на смежные работы.

   После аннотации задаются ключевые слова. Для каждой работы задайте 5-6 ключевых слов в порядке их значимости, т.е. самое важное ключевое слово статьи должно быть первым в списке.

   Название работы, ФИО авторов, аннотация и ключевые слова должны быть представлены в статье на трех языках: казахском, русском и английском.

   Использованная литература должна быть оформлена в соответствии с ГОСТ 7.1-2003 "Библиографическая запись. Библиографическое описание. Общие требования и правила составления". Список литературы должен состоять не более чем из 20 наименований. Ссылки на источники в тексте статьи даются только в квадратных скобках (без цитирования [12], при цитировании или пересказе авторского текста [12, с. 29]). Нумерация ссылок в статье производиться по порядковому номеру источника в пристатейном списке литературы. Архивные материалы в список не включаются, ссылки на них помещаются в тексте в круглых скобках. При использовании в статье источников из электронных ресурсов или удаленного доступа (Интернета) в списке литературы приводится библиографическая запись источника и ссылка на сетевой ресурс с полным сетевым адресом в Интернете. Желательно указывать дату обращения к ресурсу.

   Список литературы на языке оригинала сопровождается списком литературы (references) в английской транслитерации.

6. Журнал придерживается единого стиля и поэтому предъявляет ряд общих требований к оформлению работ. Исходный (неоттранслированный) tex-файл должен целиком помещаться в горизонтальных рамках экрана за возможным исключением матриц и таблиц и транслироваться без протестов LaTeX2ε и сообщений о кратных и неопределенных метках, больших переполненных и незаполненных боксах. Не следует определять много новых команд, изобретая собственный сленг. Авторы могут подгружать другие стандартные стилевые пакеты, но только те, которые не входят в противоречие с пакетами amsmath и amssymb. Естественно файл, кроме всего прочего, должен быть проверен на отсутствие грамматических и стилистических ошибок. Статьи, не удовлетворяющие этим требованиям, возвращаются на доработку.

Эталонный образец работы с демонстрацией графики, с преамбулой устраивающей редакцию, списки типичных ошибок оформления и методы их устранения можно получить в редакции или на сайте КазНУ им. аль-Фараби http://journal.kaznu.kz.

7. Графические файлы с рисунками должны быть только качественными черно-белыми в формате .eps , либо выполненными в латеховском формате. Рисунки в этих форматах делаются, например, с помощью мощных математических пакетов Maple, Mathematica или с помощью пакета Latexcad. Качественные графические файлы сделанные другими графическими программами должны быть сконвертированы в формат .eps с помощью Adobe Photoshop или конвертера Conversion Artist. Все рисунки должны быть уже импортированными в tex-файл и представляются в редакцию вместе с основным файлом статьи. Графические форматы,отличные от выше указанных, отвергаются.

   Редакция вправе отказаться от включения в работу рисунка, если автор не в состоянии обеспечить его надлежащее качество.

МАЗМҰНЫ - СОДЕРЖАНИЕ

УСПЕЙТЕ ПОДПИСАТЬСЯ НА СВОЙ ЖУРНАЛ

АКЦИЯ!!!

Каждому подписчику
ПУБЛИКАЦИЯ СТАТЬИ
БЕСПЛАТНО!!!

- **Акция действительна при наличии квитанции об оплате годовой подписки.**
- **Статья должна соответствовать требованиям размещения публикации в журнале.**
- **Статья печатается в той серии журнала, на которую подписался автор.**
- **Все нюансы, связанные с публикацией статьи, обсуждаются с ответственным секретарем журнала.**

Издательский дом
«Қазақ университеті»
г. Алматы,
пр. аль-Фараби, 71
8 (727) 377 34 11, 221 14 65

АО «КАЗПОЧТА»
г. Алматы,
ул. Богенбай батыра, 134
8 (727 2) 61 61 12

ТОО «Евразия пресс»
г. Алматы,
ул. Жибек Жолы, 6/2
8 (727) 382 25 11

ТОО «Эврика-пресс»
г. Алматы,
ул. Кожамкулова, 124, оф. 47
8 (727) 233 76 19, 233 78 50