МРНТИ 28.27/27,81.96

Р.Муратхан[1], Д.Ж.Сатыбалдина[2], А.Есен[3]

[1]Е.А.Бөкетов атындағы Қарағанды мемлекеттік университеті,
Қарағанды, Қазақстан

[2]Л.Н.Гумилев атындағы Еуразия ұлттық университеті,
Астана, Қазақстан

[3]КСИ Фактор
Астана, Қазақстан, e-mail:muratkhan_r@enu.kz

АҚПАРАТТЫҚ ҚАУІПСІЗДІКТІҢ ТӘУЕКЕЛІН БАҒАЛАУДА MATLAB БАҒДАРЛАМАСЫН ҚОЛДАНУ

Түйіндеме. Қазіргі заманғы кәсіпорындардың ақпараттық қауіпсіздігінің тәуекелі – ол бір бірімен байланысқан көптеген айнымалылардан тұратын көпөлшемді күрделі түсінік. Көп жағдайда тәуекел факторының мәні дәлме дәл анықталмайды. Сондықтан ақпараттық қауіпсіздіктің тәуекелін бағалауда бұлдыр логиканы пайдалану қажет. Бұл мақалада ақпараттық қауіпсіздіктің тәуекелін бағалау үшін бұлдыр логика теориясын қолдану қарастырылады. Әдістің негізі лингвистикалық айнымалы түсінігі болып табылады. Ұсынылып отырған әдіс толығымен сапалық болып табылмайды. Сонымен бірге математикалық есептеулерге де негізделеді, бірақ бұл есептеулер «жасырын түрде» жүргізіледі. Бұлдыр модельдегі ережелер •орының орындалу процессі MATLAB бағдарламалық құралының Fuzzy Logic Toolbox арнайы пакетінің көмегімен жүзеге асырылады. Бұлдыр шығару Мамдани алгоритмінің негізінде орындалады. Алынған нәтиженің дәлдігі Microsoft әдісі арқылы алынған нәтижемен салыстырылады.

Түйінді сөздер: бұлдыр логика теориясы, тәуекелді бағалау әдісі, бұлдыр жиын, бұлдыр модель, лингвистикалық айнымалы.

Аннотация. Риск нарушения информационной безопасности современной организации – это многомерное сложное понятие, в том числе набор взаимосвязанных переменных. Часто значение факторов риска не может быть точно определено. Поэтому оценка риска информационной безопасности определяется как нечеткая проблема. Рассматриваются методы реализации оценки рисков информационной безопасности в сочетании с теорией нечетких мер. В основе метода лежит понятие лингвистической перемены. Предложенной метод не является целиком качественным; он опи-

рается и на математические вычисления, но эти вычисления совершаются «за кулисами». Проводится реализация процесса нечеткого моделирования базы правил посредством применения специализированного пакета Fuzzy Logic Toolbox программного средства MATLAB. Выполнение нечеткого вывода реализуется на основе алгоритма Мамдани. Точность полученного результата сравнивается с результатами, полученными методом Microsoft.
Ключевые слова. информационная безопасность, теория нечеткой логики, метод оценки рисков, нечеткое множество, нечеткая модель, лингвистические переменные.

Abstract. Risk of the breach of information security of the modern organization is the multidimensional complex concept which is including set of interconnected variables. Often, the value of risk factors cannot be accurately determined. Therefore, the risk assessment of information security can be defined as a fuzzy problem. This article describes methods of implementation of information security risk assessment in conjunction with the theory of fuzzy measures. The concept about linguistic variable is in the base of method. Approach is not totally quality, it is based and on the mathematical calculations, but these calculations are doing «behind the scenes». Realization of process fuzzy design of rule base conducted by means of application of the specialized package Fuzzy Logic Toolbox of programmatic means MATLAB. Implementation of fuzzy conclusion will be realized on the basis of algorithm of Mamdani. Exactness of the got result is compared to the results by the got method Microsoft.
Key words: theory of fuzzy sets, method of risks assessment, fuzzy set, fuzzy model, linguistic variables.

Кіріспе

Автоматтандырылған жүйелердің (АЖ) жұмыс істеуге қабілеттілігін бағалаудын жалпыға ортақ тәсілі, осы жүйелердің жұмыс істеуін сипаттайтын модельдерді құру мен зерттеуге негізделген модельдеу болып табылады. Мұндай модельдерді қолдану ақпаратты жинау, сақтау және өңдеу процесстерін талдау мен тиімдестіруге мүмкіндік береді. Сонымен бірге берілгендерді қорғау технологиясын да таңдауға болады [1]. Жүйенің әртүрлі процесстерінің физикалық мағынасын сипаттайтын математикалық модель АЖ әртүрлі сипатталарын нақты бағлауға мүмкіндік береді. Бірақ та, модельдеудің классикалық әдістері модельдің кіріс мәліметіне нақты сандық мән еңгізуді талап етеді.

Автоматтандырылған жүйенің қорғалғандығын талдау процессінің ақпараттық қауіпсіздіктің (АҚ) тәуекелін бағалаудан ерекшелігі тәуекелді бағалау кезінде бастапқы берілгендер ретінде эксперттік баға түрінде берілген бұлдыр мәндер қолданылады. Сондықтан бұлдыр модельдерді қолдану қажеттілігі туындайды. Бұлдыр модельді құру барысында дәстүрлі математикалық модельдерге қарағанда модельденетіН жүйе туралы салыстырмалы түрде аз көлемдегі мағлұмат пайдаланылады. Бұл жағдайда автоматтандырылған жүйелердегі тәуекелдерді есептеу сияқты күрделі және ерекше процесстегі бастапқы берілгендер жуық бұлдыр мәнді қабылдауы мүмкін [2-4].

Бұл жұмыстың мақсаты тәуекелді құраушылардың толық немесе біртекті емес жағдайындағы АҚ тәуекелін бағалаудың-моделін құру болып табылады.

1 Модель түрін таңдау

Ақпараттық қауіпсіздіктің тәуекелін бағалаудың бұлдыр моделін құру үшін, бұлдыр жиындар теориясы негізіндегі бар модельдерді талдау қажет.

X жиынында анықталған бұлдыр A жиыны деп $A=\{(x,\mu_A(x))|x\in X\}$ жұбы анықталады. Мұндағы X – мәндер облысы, ал $\mu_A(x)$ – x элементінің A бұлдыр жиынына тиістілік дәрежесін сипаттайтын тиістілік функциясы. Мұнда келесі үш жағдай орындалады:

1) $\mu_A(x)=1$ – x элементінің A бұлдыр жиынына толығымен тиістілігі, яғни $A\in X$;

2) $\mu_A(x)=0$ – x элементі A бұлдыр жиынында жатпайды, яғни $A\notin X$;

3) $0<\mu_A(x)<1$ – x элементінің A бұлдыр жиынына жартылай тиістілігі.

Әдетте, бұлдыр модельдер келесі 4 бөліктен тұратын бұлдыр басқару жүйесі үшін құрылады[5]:

1) лингвистикалық айнымалыларды формальдау;

2) фазификациялау бөлігі (модельдің нақты кіріс параметрлерінің бұлдыр жиынға тиістілік дәрежесін есептейді);

3) шығару бөлігі (бұл бөліктің негізгі элементі – ережелер жиыны, яғни кіріс және шығыс мәліметтер арасындағы қатынастарды сипаттайтын логикалық ережелер жиыны болып табылады);

4) дефазификация бөлігі (шығару механизмінде, тиістілік функциясы негізінде шығыс мәліметінің нақты мәнің есептеу).

Әртүрлі бұлдыр модельдер түрлері осы аталған 4 бөліктің орындалу тәсілімен ерекшеленеді.

Қазіргі таңда бұлдыр модельдердің ішінде ең көп қолданылатыны Мамдани моделі [6]. Мамдани әдісінде модельденетін жүйе, ішінде жүретін физикалық процесс туралы жеткіліксіз ақпаратты сипаттайтын «қара жәшік» ретінде қарастырылады. Модель нақты жүйенің неғұрлым дәл аппроксимациясын қамтамасыз ететін, кіріс мәліметтерінің (X вектор) шығыс мәліметтеріне (Y вектор) бейнелеуін орындайды. Аталған бейнелеу $X \times Y$ декарттық көбейтіндімен берілетін кеңістіктегі, бірқатар геометриялық беттің (бейнелеу беті) бар болуын жобалайды. Мамдани моделі келесі түрдегі көптеген ережеден тұрады:

$$\text{ЕГЕР } (x - A \text{ болса}) \text{ ОНДА } (y - B \text{ болады}),$$

мұндағы A, B – бұлдыр жиындар. Әрбір ереже аталған кеңістікте бірқатар бұлдыр нүктені береді. Осы бұлдыр нүктелер жиыны негізінде бұлдыр график және бұлдыр логика аппараты қолданатын нүктелер арасындағы интерполяция механизмі құрылады

Бұлдыр модельдердің басқа типтері бар. Солардың ішіндегі ең негізгілерінің бірі болып Такаги-Сугено-Канга (TSK-моделі) моделі болып табылады. Такаги-Сугено-Канга моделін Мамдани моделінен ережелер формасымен ерекшеленеді [7]. TSK-моделінің ережелері келесі түрде болады:

$$\text{ЕГЕР } (x - A \text{ болса}) \text{ ОНДА } (y=f(x) \text{ болады}),$$

Мұнда әрбір ереженің қорытындысындағы бұлдыр жиынның орнына сызықты емес те болуы мүмкін $f(x)$ функциясы қолданылады. Әдетте $y=ax+b$ түріндегі сызықтық функция қолданылады.

Такаги-Сугено-Канга моделіндегі алынатын қорытынды Мамдани моделіне қарағанда күрделі математикалық өрнекпен сипатталатындықтан, сонымен бірге тәуекелдің пайда болу жолын көрсету кем болғандықтан АҚ-тің тәуекелін бағалау үшін көп жағдайда Мамдани моделі қолданылады. Өйткені АҚ-тің тәуекелін бағалау кезінде оның пайда болу жолы тәуекелдің нақты мәнінен

әлдеқайда пайдалырақ.

2 Лингвистикалық айнымалыларды формальдау

АҚ-тің тәуекелін бағалауда Мамдани моделін қолдану үшін жүйенің кіріс мәліметтеріне қандай мәндерді еңгізетінімізді білуіміз қажет. АҚ-тің тәуекелінің анықтамасынан тәуекел шамасы R мүмкін болатын шығын (ақпарат, ресурс немесе актив құндылығы) AV және АҚ-тің қатерінің орындалу ықтималдығы $R(T)$ функциясы болып табылады:

$$R = P(T)*AN. \quad (1)$$

Сонымен, кіріс мәліметтері ретінде 1-кестедегі лингвистикалық терм-жиындармен сипатталатын үш бұлдыр айнымалының («қатердің орындалу ықтималдығы» және «активтің құндылығы») эксперттік бағалары еңгізіледі. Жүйенің шығыс мәліметі

1-кесте

Лингвистикалық айнымалылар мен олардың мәндер жиыны

Деңгей шкаласы	Қатердің орындалу ықтималдығы ($P(T)$)	Актив құндылығы (AV)	Мәндер жиыны
Өте төмен	Оқиға ешқашан болмайды	Материалдық құралдар мен ресурстар шығыны немесе беделге әсері болмашы	(0; 0; 0,25)
Төмен	Оқиға ара тұра болады	Материалдық активтер шығыны немесе репутацияға әсері елеулі	(0; 0,25; 0,5)
Орташа	Оқиға бірқатар шарттар орындалған жағдайда орындалуы мүмкін	Материалдық активтер шығыны немесе репутацияға әсері әжептәуір	(0,25; 0,5; 0,75)
Жоғары	Оқиғаның орындалу ықтималдығы жоғары	Материалдық активтер шығыны немесе репутацияға әсері айтарлықтай	(0,5; 0,75; 1)
Өте жоғары	Оқиға орындалады	Материалдық активтер шығыны немесе репутацияға әсері өте жоғары. Яғни әрі қарай қызмет ету мүмкін емес.	(0,75;1; 1)

2-кесте

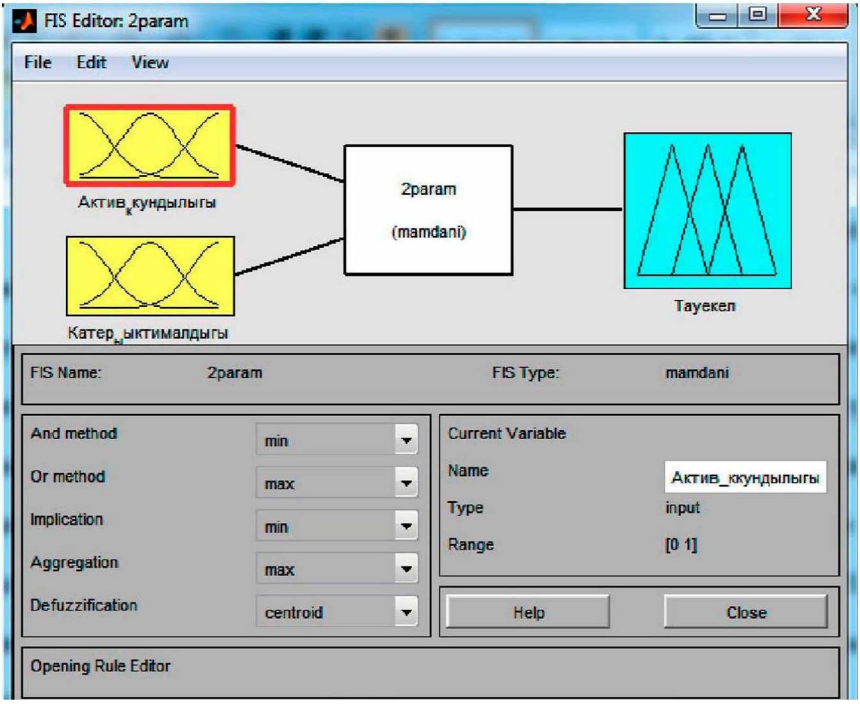
АҚ-тің тәуекел мөлшерінің терм-жиыны

Шкала деңгейі	Тәуекелді сипаттау	Мәндер жиыны
Елеусіз төмен	Тәуекелді ескермеуге болады.	(0; 0; 0,125)
Өте төмен	Бұл тәуекелге контршара қолдану қажеттілігін анықтау немесе тәуекелді сол күйінде қабылдау мүмкіндігінің бар екенін анықтау	(0; 0,125; 0,25)
Төмен	Тәуекел деңгейі жұмыс істеуге мүмкіндік береді. Бірақ қалыпты жұмыс істеуді бұзу алғышарттары бар	(0,125; 0,25; 0,375)
Орташадан төмен	Белгілі бір уақыт мөлшерінде контршара жоспарын құру және оны қолдану қажет	(0,25; 0,375; 0,5)
Орташа	Тәуекел деңгейі қалыпты жұмыс істеуге мүмкіндік бермейді. Тәуекелді төмендетуге байланысты контршара қолдану қажет	(0,375; 0,5; 0,625)
Орташадан жоғары	Тәуекел деңгейі қалыпты жұмыс істеуге мүмкіндік бермейді. Тәуекелді төмендетуге байланысты контршараны неғұрлым ертерек қолдану қажет	(0,5; 0,625; 0,75)
Жоғары	Тәуекел деңгейі жоғары, яғни биснес-процесстер орнықсыз	(0,625; 0,75; 0,875)
Өте жоғары	Тәуекел деңгейін төмендетуге байланысты контршараны дереу қолдану қажет	(0,75; 0,875; 1)
Өте қиын	Тәуекел деңгейі өте жоғары, яғни жүйенің жұмыс істеуін дереу тоқтату қажет немесе тәуекел деңгейін төмендетуге байланысты контршараны шұғыл қолдану қажет	(0,875; 1; 1)

ретінде 2-кестедегі лингвистикалыеқ терм-жиындарымен берілген ақпараттық қауіпсіздіктің тәуекелінің мөлшерін аламыз.

3. Фазификация

Ақпараттық қауіпсіздіктің тәуекелін бағалау үшін Мамдани моделін қолдану мысалын қарастырайық. Мамданидің бұлдыр шығару алгоритмі бойынша «ақпараттық қауіпсіздіктің тәуекелінің» нақты мәнін алуды автоматтандыру үшін MATLAB бағ-



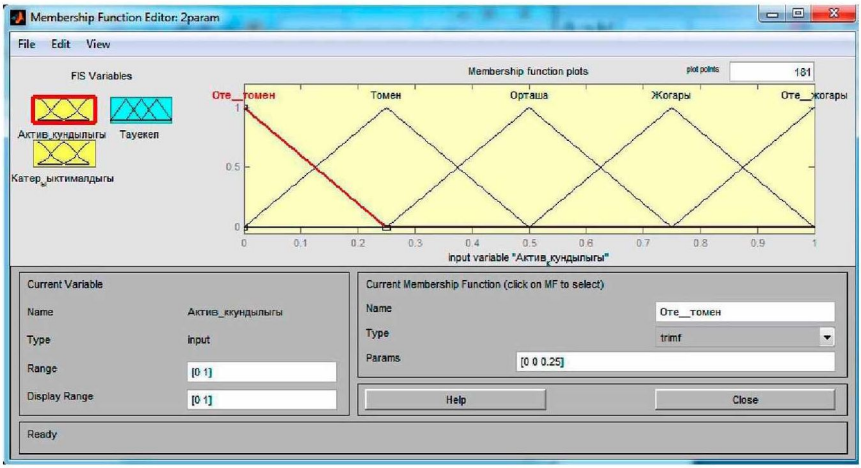
Сурет 1. Fuzzy Logic Toolbox пакетінің кіріс және шығыс мәліметтерін еңгізу терезесі

дарлама құру жүйесінің Fuzzy Logic Toolbox пакетін пайдаланамыз (сурет 1).

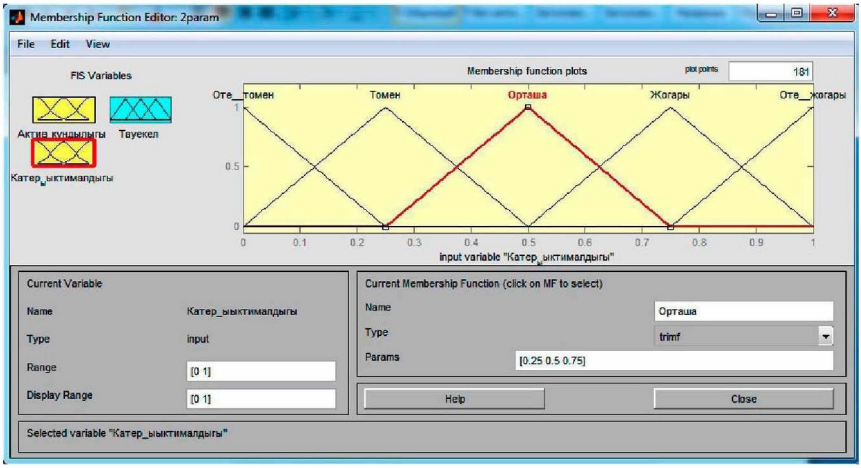
Бұл мақлада лингвистикалық айнымалылардың тиістілік функциясы үшбұрышты бұлдыр сандармен сипатталады. Өйткені оны бизнестегі, қаржыдағы және қоғамдық ғылымдардағы шешім қабылдау қосымшаларында өте жиі қолданады [8]. Төрт бұлдыр жиынның (қатердің орындалу ықтималдығы, актив құндылығы және АҚ тәуекел шамасы) тиістілік функциялары сәйкесінше 2 – 4 суреттерде келтірілген.

Тәуекелді бағалау механизмі, білім қорын кіріс (яғни AV, $P(T)$) және шығыс (яғни R) мәліметтері арасындағы логикалық байла-

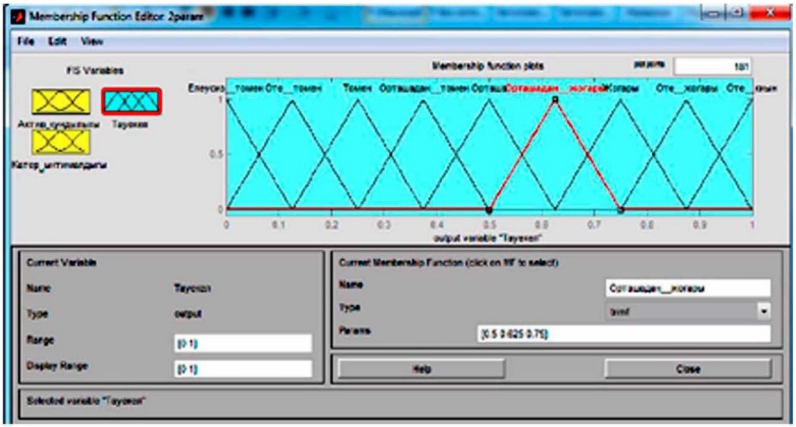
нысты сипаттайтын ережелер құрайтын эксперттік жүйе болып табылады. Қарапайым жағдайда бұл «кестелік» логика, ал жалпы жағдайда «егер..., онда...» түріндегі продукциондық ереже



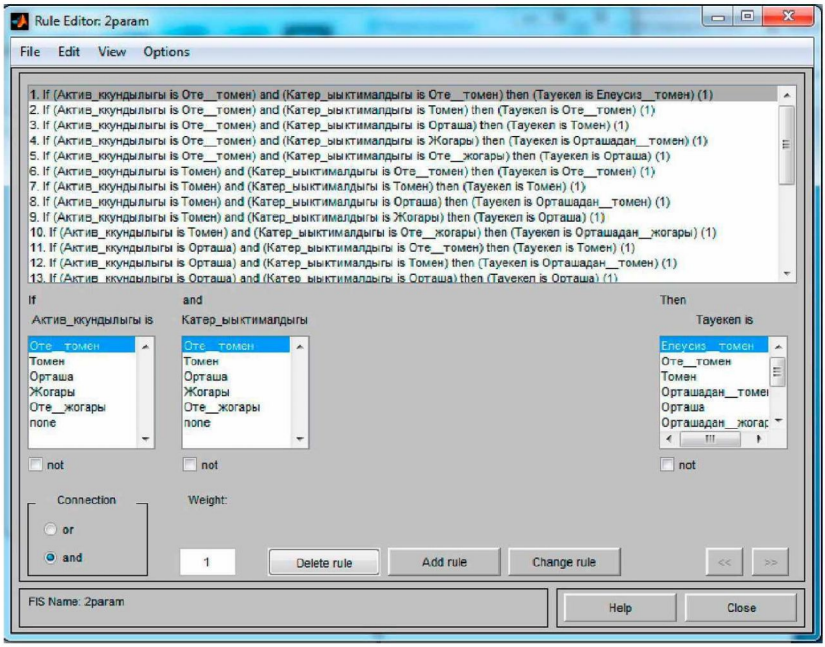
Сурет 2. «Актив құндылығы» лингвистикалық айнымалысының тиістілік функциясы



Сурет 3. «Қатердің орындалу ықтималдығы» лингвистикалық айнымалысының тиістілік функциясы



Сурет 4. «АҚ тәуекелі» лингвистикалық айнымалысының тиістілік функциясы



Сурет 5. Білім қорынан үзінді (продукциондық ереже)

көмегімен нақты байланысты сипаттайтын күрделі логика болып табылады (сурет 5).

4. Дефазификация

Дефазификация (defuzzification) деп бұлдыр жиынды нақты санға түрлендіру процедурасын атаймыз. Бұлдыр жиындар теориясындағы дефазификация процедурасы ықтималдықтар теориясындағы кездейсоқ шамалардың (математикалық күтілім, мода, медиана) сипаттамаларын анықтауға ұқсас. Дефазификация процедурасының қарапайым түрі болып тиістілік функцисының максимумына сәйкес келетін нақты санды таңдап алу болып табылады.

Ауырлық центрі әдісі бойынша

$$\widetilde{A} = \int\limits_{[\underline{u},\bar{u}]} \mu_A(u)/u$$

бұлдыр жиынының дефазификациясын келесі формула бойынша есептелінеді [9]:

$$a = \frac{\int\limits_{\underline{u}}^{\bar{u}} u \cdot \mu_A(u)\, du}{\int\limits_{\underline{u}}^{\bar{u}} \mu_A(u)\, du}$$

5. Қорытынды

[10] жұмыста бір актив үшін АҚ тәуекелінің мөлшерін

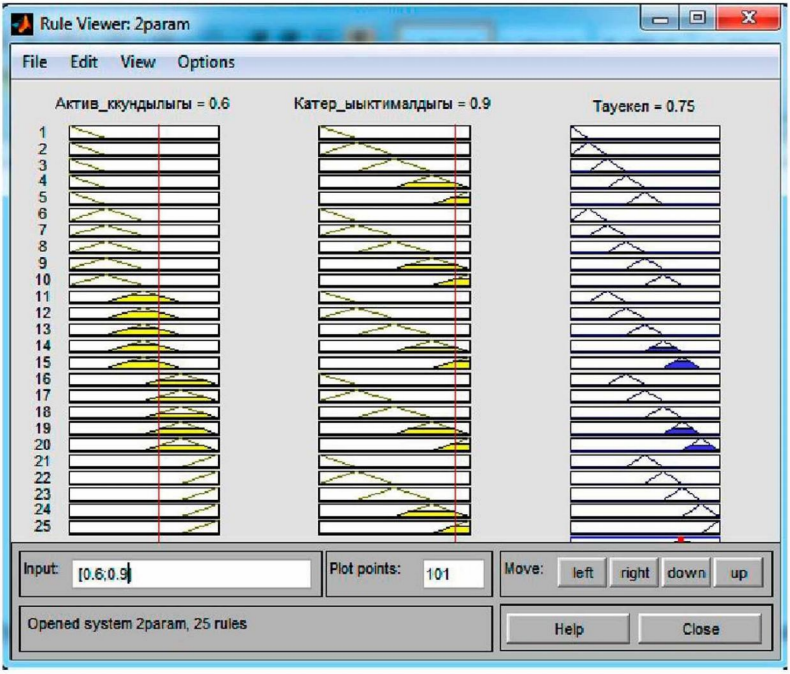
3-кесте

Microsoft әдістемесі бойынша АҚ тәуекелін бағалау [10]

№	Актив атауы	AV	Қатер атауы	$P(T)$	R
1	Клиенттің инвестициясы туралы мәлімет	орташа	Қаржы кеңесшісінің есепке алу жазбасын ұрлау арқылы клиенттің мағлұматтарына рұқсатсыз кіру	жоғары	жоғары
2	Клиенттің инвестициясы туралы мәлімет	орташа	Қаржы кеңесшісінің есепке алу жазбасын ұрлау арқылы клиенттің мағлұматтарына рұқсатсыз кіру	жоғары	жоғары
3	Клиенттің инвестициясы туралы мәлімет	төмен	Қаржы кеңесшісінің есепке алу жазбасын ұрлау арқылы клиенттің мағлұматтарына рұқсатсыз кіру	орташа	төмен

Microsoft әдістемесімен үш кіріс (AV, $P(T)$, V) мәліметтері бойынша есептелгені келтірілген (кесте 3).

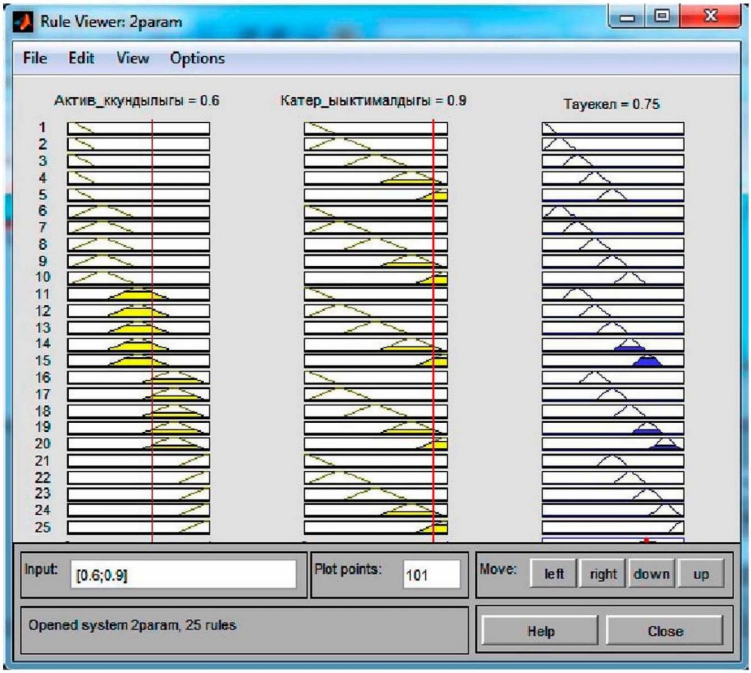
Әрі қарай осы мысалдағы мәліметтер бойынша бұлдыр модельді қолдана отырып тәуекелді есептеуді қарастырамыз. 6-суретте бірінші мысал үшін үшбұрышты тиістілік функциясы бар Мамданидің бұлдыр шығару алгоритмінің графикалық интерпретациясы берілген. Кіріс мәліметтері AV=0,6, $P(T)$=0,9 және шы-



Сурет 6. Үшбұрышты тиістілік функциясы бар Мамданидің бұлдыр шығару алгоритмінің графикалық интерпретациясы

ғыс мәліметі R=0,75 (бұл жоғары тәуекел лингвистикалық айнымалысына сәйкес келеді).

7-суретте бірінші мысал үшін трапециялық тиістілік функциясы бар Мамданидің бұлдыр шығару алгоритмінің графикалық интерпретациясы берілген. Кіріс мәліметтері AV=0,6, $P(T)$=0,9



Сурет 7. Трапециялық тиістілік функциясы бар Мамданидің бұлдыр шығару алгоритмінің графикалық интерпретациясы

және шығыс мәліметі $R=0,71$ (бұл жоғары тәуекел лингвистикалық айнымалысына сәйкес келеді).

Дәл осылай қалған екі жағдай үшін де алынған нәтижелер 4-кестеде келтірілген. 4-кестедегі мәндер арқылы бұлдыр жиындар немесе бұлдыр логика аппаратын қолданып алынған АҚ тәуекелінің мөлшері әлемдік практикадағы қолданылып жүрген Microsoft әдістемесі арқылы алынған мәнмен сәйкес келетінін көреміз. Бұл жоғарыда қарастырылған АҚ тәуекелін бағалаудың бұлдыр моделінің баламалығының дәлелі болады.

АҚ тәуекелін бағалаудың сапалық әдістері алынатын мәндердің жеткілікті дәлдігін бере алмайды. Ал сандық әдістер

4-кесте

Бұлдыр логика бойынша АҚ тәуекелін бағалау әдістерінің салыстырмалы талдауы

№	[10] жұмыста	Мамдани әдісі	
		Үшбұрышты тиістілік функциясы	Трапециялық тиістілік функциясы
1 жағдай	Жоғары	0,75	0,75
2 жағдай	Жоғары	0,74	0,72
3 жағдай	Төмен	0,345	0,369

арқылы есептеу, оқиғалар саны белгісіз болғанда нақты мәннен ауытқып кететін, ықтималдықтар теориясының әдістеріне келтіріледі. Бұлдыр жиындар және бұлдыр логика теориясына негізделген модельдер мұндай жетіспеушіліктерден ада болып табылады. Сондықтан да оны АҚ тәуекелін бағалауда қолдануға болады.

Әдебиеттер

1 *Buldakova T.I., Dzalolov A.Sh.* Analysis of Data Processes and Choices of Data-processing and Security Technologies in Situation Centers // Scientific and Technical Information Processing. – 2012. – Vol. 39, no 2. – P. 127-132. DOI:10.3103/S0147688212020116.

2 *Zadeh L.A.* Fuzzy sets // Information and Control. – 1965. – P. 338-353.

3 *Satybaldina D., Muratkhan R., Kabenov D.* Ontology and Fuzzy Measures Based System for Information Security Risk Assessment // WOSIS – 9th International Workshop on Security in Information Systems. – Wroclaw, 2012. – P. 77-85.

4 *Балашов П.А., Кислов Р.И., Безгузиков В.П.* Оценка рисков информационной безопасности на основе нечёткой логики // Безопасность компьютерных систем. Конфидент: Информационно-методический журнал. – 2003. – № 6. – С. 60-65.

5 *Ярушкина Н.Г.* Основы теории нечетких и гибридных систем. – М.: Финансы и статистика, 2004. – 320 с.

6 *Mamdani E.H., Assilian S.* An Experiment in Linguistic Synthesis

with Fuzzy Logic Controller // Int. J. Man-Machine Studies. – 1975. – Vol. 7, no. 1. – P. 1-13.

7 *Takagi T., Sugeno M.* Fuzzy identification of systems and its applications to modeling and control // IEEE Transactions on Systems, Man and Cybernetics. – 1985. – Vol. SMC-15, no 1. – P. 116-132. DOI: 10.1109/TSMC.1985.6313399.

8 *Bojadziev G., Bojadziev M.* Fuzzy Logic for Business, Finance, and Management. – 2nd edition. – Singapore: World Scientific. 2007. – P. 252.

9 *Хаптахаева Н.Б., Дамбаева СВ., Аюшеева Н.Н.* Введение в теорию нечетких множеств: учеб. пособие. Ч. I. – Улан-Удэ: Изд-во ВСГТУ, 2004. – 68 с.

10 *Баранов Д., Конеев И.* Вопросы перехода от качественного к количественному анализу рисков // Депозитариум. – 2008. – № 9 (67). – С. 26-31.