Р. Муратхан, *аға оқытушысы*
(Е. А. Бөкетов атындағы Қарағанды мемлекеттік университеті)
Е. М. Нұрғалиев, *педагогика және басқару теориясы кафедрасының аға оқытушысы*
(Қазақстан Республикасы ІІМ Б. Бейсенов атындағы Қарағанды академиясы)
Б. Хабдолда, *оқытушы*
(Көпсалалы гуманитарлы-техникалық колледж)

ҮШ ПАРАМЕТРДЕН ТӘУЕЛДІ АҚПАРАТТЫҚ ҚАУІПСІЗДІКТІҢ ТӘУЕКЕЛІН БАҒАЛАУ ӘДІСІ

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

Автоматтандырылған жүйенің қорғалғандығын талдау процесінің 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 процестегі бастапқы берілгендер жуық бұлдыр мәнді қабылдауы мүмкін[2, 3, 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.

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 мәнін 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:

ЕГЕР (x — A болса) ОНДА (y — B *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:

ЕГЕР (*x — A болса*) ОНДА (*y=f*(*x*) болады).

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 бағалау үшін 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*, АҚ-тің қатерінің орындалу ықтималдығы *P(T)* және активтің осалдығының *V* функциясы болып табылады:

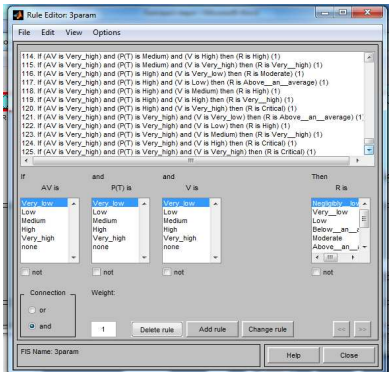
$$R=V*P(T)*AV. \qquad (1)$$

Сонымен, кіріс мәліметтері ретінде лингвистикалық терм-жиындармен сипатталатын үш бұлдыр айнымалының («қатердің орындалу ықтималдығы», «активтің құндылығы» және «активтің осалдығы») эксперттік бағалары енгізіледі. Жүйенің шығыс мәліметі ақпараттық қауіпсіздіктің тәуекелінің мөлшері де лингвистикалық терм-жиындарымен анықталады.

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 бағдарлама құру жүйесінің Fuzzy Logic Toolbox пакетін пайдаланамыз. Бұл мақалада лингвистикалық айнымалылардың тиістілік функциясы үшбұрышты бұлдыр сандармен сипатталады. Өйткені оны бизнестегі, қаржыдағы және қоғамдық ғылымдардағы шешім қабылдау қосымшаларында өте жиі қолданады[8].

Тәуекелді бағалау механизмі, білім қорын кіріс (яғни AV, P(T), V) және шығыс (яғни R) мәліметтері арасындағы логикалық байланысты сипаттайтын ережелер құрайтын эксперттік жүйе болып табылады. Қарапайым жағдайда бұл «кестелік» логика, ал жалпы жағдайда «егер..., онда...» түріндегі продукциондық ереже көмегімен нақты байланысты сипаттайтын күрделі логика болып табылады (сурет 1).



Сурет 1. Білім қорынан үзінді (продукциондық ереже)

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 функциясының максимумына сәйкес келетін нақты санды таңдап алу болып табылады.

Ауырлық центрі әдісі бойынша $\widetilde{A} = \int_{[\underline{u},\bar{u}]} \mu_A(u)/u$ бұлдыр жиынының дефазификациясын келесі формула бойынша есептелінеді[9]:

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

5. Қорытынды.

Жұмыста бір актив үшін АҚ тәуекелінің мөлшерін Microsoft әдістемесімен үш кіріс (AV, P(T), V) мәліметтері бойынша есептелгені келтірілген. Әрі қарай осы мысалдағы мәліметтер бойынша бұлдыр модельді қолдана отырып тәуекелді есептеуді қарастырамыз. 2-суретте бірінші мысал үшін үшбұрышты тиістілік функциясы бар Мамданидің бұлдыр шығару алгоритмінің графикалық интерпретациясы берілген. Кіріс мәліметтері AV=0.6, P(T)=0.9, V=0.6 және шығыс мәліметі R=0.735 (бұл жоғары тәуекел лингвистикалық айнымалысына сәйкес келеді)[10].

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 арқылы есептеу, оқиғалар саны белгісіз болғанда нақты мәннен ауытқып кететін, ықтималдықтар теориясының әдістеріне келтіріледі. Сондықтан да оны АҚ тәуекелін бағалауда қолдануға болады.

Кесте 1. Бұлдыр логика бойынша
АҚ тәуекелін бағалау әдістерінің салыстырмалы талдауы

№	[10] жұмыста	Мамдани әдісі		Сугено әдісі
		Үшбұрышты тиістілік функциясы	Трапециялық тиістілік функциясы	
1 жағдай	Жоғары	0,735	0,71	0,699
2 жағдай	Жоғары	0,777	0,81	0,816
3 жағдай	Төмен	0,271	0,28	0,261

[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. — № 2. — P.127-132.
[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. — Москва, 2004.
[6] Mamdani E. H., Assilian S. An Experiment in Linguistic Synthesis with Fuzzy Logic Controller // Int. J. Man-Machine Studies. — 1975. — № 1. — Vol. 7.
[7] Takagi T., Sugeno M. Fuzzy identification of systems and its applications to modeling and control // IEEE Transactions on Systems, Man and Cybernetics. — 1985. — P. 116-132.
[8] Bojadziev G., Bojadziev M. Fuzzy Logic for Business, Finance, and Management. — 2nd edition. — Singapore, 2007. — P.252.
[9] Хаптахаева Н. Б.. Дамбаева С. В., Аюшеева Н. Н. Введение в теорию нечетких множеств: Учеб. пос. Ч. I. — Улан-Удэ, 2004.
[10] Баранов Д., Конеев И. Вопросы перехода от качественного к количественному анализу рисков // Депозитариум. — 2008. — № 9 (67). — С. 26-31.