https://doi.org/10.51885/3134-8025_JICS_2026_1_5
ХҒТАР 20.51.23

АҚПАРАТТЫҚ ҚАУІПСІЗДІК ТӘУЕКЕЛДЕРІН БАҒАЛАУДА АЙҚЫН ЕМЕС FIS-МОДЕЛІН ҚОЛДАНУ ӘДІСТЕРІ

ОЦЕНКА РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ С ПРИМЕНЕНИЕМ НЕЧЕТКОЙ FIS-МОДЕЛИ

INFORMATION SECURITY RISK ASSESSMENT USING A FUZZY FIS MODEL

Т.Ш. Миркасимова [1,2*], **С.А. Адилжанова** [1]
[1]Әл-Фараби атындағы Қазақ ұлттық университеті, Алматы қ., Қазақстан
[2]Нархоз Университеті, Алматы қ., Қазақстан
*Жауапты автор: Миркасимова Толкын Шабденбековна, e-mail: tolkyn.mirkasimova@narxoz.kz

Түйінді сөздер:
Ақпараттық қауіпсіздік, тәуекелдерді бағалау, айқын емес логика, Мамдани әдісі, FIS-модель, осалдық, киберқауіптер, интеллектуалды жүйе.

ТҮЙІНДЕМЕ

Бұл мақалада ақпараттық қауіпсіздік тәуекелдерін бағалау міндетін шешу үшін айқын емес логикаға негізделген модельді қолданудың ғылыми және практикалық аспектілері қарастырылады. Зерттеудің өзектілігі ақпараттық жүйелерде пайда болатын белгісіздік пен толық емес деректер жағдайында тәуекелді дәл бағалау қажеттілігімен анықталады. Жұмыстың мақсаты – Мамдани әдісі негізінде құрылатын айқын емес логикалық модельді әзірлеу және оның дәстүрлі бағалау тәсілдеріне қарағанда тиімділігін көрсету. Зерттеу барысында аналитикалық шолу, моделдеу, фаззификация, ережелер базасын құру және эксперименттік тексеру әдістері қолданылды. Алынған нәтижелер ұсынылған модельдің тәуекел деңгейін дәлірек анықтайтынын, белгісіздікке бейім екенін және практикалық қолдануға қолайлы екенін көрсетті. Ғылыми жаңалығы айқын емес логикалық ережелерге негізделген тәуекелді интегралды бағалау моделінің әзірленуімен сипатталады. Модельді корпоративтік және білім беру жүйелерінде қолдану оның басқарушылық шешімдерді қолдауда тиімді құрал бола алатынын дәлелдейді.

Ключевые слова:
Информационная безопасность, оценка рисков, нечеткая логика, метод Мамдани, FIS-модель, уязвимость, киберугрозы, интеллектуальная система.

АННОТАЦИЯ

В данной статье рассматриваются научные и практические аспекты применения модели на основе нечеткой логики для оценки рисков информационной безопасности. Актуальность исследования определяется необходимостью точной оценки рисков в условиях неопределенности и неполноты данных, характерных для современных информационных систем. Целью работы является разработка модели нечеткого логического вывода на основе метода Мамдани и демонстрация её эффективности по сравнению с традиционными

подходами. В исследовании использованы аналитический обзор, моделирование, фаззификация, формирование базы правил и экспериментальная проверка. Полученные результаты показывают, что предложенная модель более точно определяет уровень риска, устойчиво работает с неопределенными данными и пригодна для практического применения. Научная новизна заключается в разработке интегральной модели оценки риска, основанной на системе нечетких правил. Применение модели в корпоративных и образовательных системах подтверждает её эффективность как инструмента поддержки управленческих решений.

Keywords:

Information security, risk assessment, fuzzy logic, Mamdani method, FIS model, vulnerability, cyber threats, intelligent system.

ABSTRACT

This article examines the scientific and practical aspects of applying a fuzzy logic–based model to assess information security risks. The relevance of the study is determined by the need for accurate risk evaluation under uncertainty and incomplete data typical of modern information systems. The aim of the work is to develop a fuzzy logic inference model based on the Mamdani method and to demonstrate its effectiveness compared to traditional approaches. The research employs analytical review, modeling, fuzzification, rule-base construction, and experimental validation. The obtained results show that the proposed model provides more accurate risk assessment, effectively handles uncertainty, and is suitable for practical use. The scientific novelty lies in the development of an integrated risk assessment model built upon a system of fuzzy rules. The application of the model in corporate and educational systems confirms its effectiveness as a tool for supporting decision-making in information security management.

КІРІСПЕ

Цифрлық инфрақұрылымның күрделенуі мен кибершабуылдардың артуы ақпараттық қауіпсіздік тәуекелдерін дәл бағалау міндетін өзекті етеді. Тәуекел факторларының көпшілігі толық емес, анық емес және сараптамалық бағаларға негізделетіндіктен, дәстүрлі әдістер (ISO/IEC 27005, NIST SP 800-30) белгісіздікті жеткілікті деңгейде ескере алмайды. Бұл ұйымдардың қауіпсіздік деңгейін тиімді басқаруда қосымша интеллектуалды тәсілдерді қажет етеді.

Айқын емес логикаға негізделген FIS-модельдер осындай белгісіздік жағдайында тиімді құрал болып табылады. Олар лингвистикалық айнымалылармен жұмыс істей алады, аралық күйлерді сипаттайды және сараптамалық білімді IF–THEN ережелері арқылы формализациялайды. Мамдани әдісіне негізделген модель тәуекелді сандық және лингвистикалық түрде бағалауға мүмкіндік беріп, интерпретацияны жеңілдетеді.

Зерттеудің өзектілігі – айқын емес FIS-модельдің субъективтілікті азайту, белгісіздікпен жұмыс істеу және ақпараттық жүйелердегі (LMS, CRM, ERP) тәуекелдерді дәлірек бағалау мүмкіндігімен анықталады.

Зерттеу мақсаты – ақпараттық қауіпсіздік тәуекелдерін бағалау үшін Мамдани әдісіне негізделген FIS-модельді әзірлеу және оның тиімділігін дәстүрлі әдістермен салыстыру.

Зерттеу міндеттері:

1. Ақпараттық қауіпсіздік тәуекелдерін бағалау әдістеріне теориялық талдау жүргізу.
2. Айқын емес логикалық модельдеудің принциптерін анықтау.
3. Мамдани типіндегі FIS-модель архитектурасын әзірлеу.
4. Модельді нақты жүйелерде апробациялау.
5. Нәтижелерді дәстүрлі әдістермен салыстыру.

Зерттеу нысаны – корпоративтік және білім беру ұйымдарының ақпараттық жүйелеріндегі ақпараттық қауіпсіздік тәуекелдері.

Зерттеу пәні – тәуекелдерді бағалауда айқын емес логикалық қорытындылау жүйесін (FIS) қолданудың әдістері мен механизмдері.

Ғылыми жаңалығы – ақпараттық қауіпсіздік тәуекелдерін бағалау үшін Мамдани әдісіне негізделген модификацияланған айқын емес логикалық FIS-модельдің әзірленуі болып табылады. Ұсынылған модель дәстүрлі ISO/IEC 27005, NIST SP 800-30 және балдық бағалау әдістерінен айырмашылығы, тәуекел факторларының аралық және белгісіз мәндерін айқын емес жиындар арқылы өңдеуге мүмкіндік береді, сараптамалық білімді формализацияланған IF–THEN ережелер жүйесі түрінде интеграциялайды және тәуекелдің интегралды сандық әрі лингвистикалық бағасын қалыптастырады. Модельдің тиімділігі нақты ақпараттық жүйелердің сценарийлері негізінде жүргізілген эксперименттік апробация арқылы дәлелденіп, оның белгісіздік жағдайында бағалау дәлдігін арттыратыны және практикалық басқарушылық шешімдерді генерациялауға қабілетті екені көрсетілді.

Зерттеу нәтижелері айқын емес логика негізіндегі интеллектуалды бағалау әдістерінің ақпараттық қауіпсіздікті басқаруда қолдану тиімділігін көрсетеді және оларды корпоративтік, мемлекеттік және білім беру секторларында интеграциялауға мүмкіндік береді.

ЗЕРТТЕУ МАТЕРИАЛДАРЫ МЕН ӘДІСТЕРІ

Fuzzy Logic айқын емес логиканы қолдану арқылы тәуекелдерді бағалау әдістемесі

Ақпараттық қауіпсіздік тәуекелдерін Fuzzy Logic айқын емес логиканың негізінде бағалау әдістемесі анық емес немесе сандық тұрғыдан дәл өлшеуге қиын факторларды айқын емес жиындар түрінде бейнелеуге негізделеді. Классикалық әдістер нақты сандық мәндерді талап етсе, айқын емес логиканы параметрлердің белгілі бір категорияларға 0-ден 1-ге дейінгі дәрежеде тиесілігін сипаттайды. Бұл тәсіл ақпараттық қауіпсіздік тәуекелдері үшін өзекті, себебі қауіптердің ықтималдығы, уязвимостар деңгейі, активтердің құндылығы сияқты көптеген параметрлер абсолюттік дәлдікпен анықталмайды және көбіне сарапшылық бағалаулар түрінде беріледі. Осылайша, ақпараттық тәуекелдерді бағалау айқын емес міндет ретінде қарастырылады, ал айқын емес модельдер толық емес немесе дәл емес деректермен тиімді жұмыс істеуге мүмкіндік береді.

Айқын емес логика бірнеше негізгі компоненттен тұрады:

– фаззификация (анық кіріс мәндерін айқын емес мәндерге түрлендіру),

– шығыс ережелер базасы,

– дефаззификация (айқын емес нәтижені оңтайландырылған анық сандық мәнге қайта түрлендіру).

Айқын емес логиканы қолдану арқылы ақпараттық қауіпсіздік тәуекелдерін бағалау әдістемесі анық емес және өлшеуге қиын факторларды айқын емес жиындар арқылы формализациялауға негізделген. Мұндай тәсіл сараптамалық бағаларды «төмен», «орта», «жоғары деңгей» сияқты лингвистикалық айнымалылар түрінде сипаттауға және олардың арасындағы анық емес шекараларды есепке алуға мүмкіндік береді. Әдістеме бастапқы сараптамалық деректерден интегралды сапалық және сандық тәуекел бағасына дейінгі логикалық тізбекті бейнелейтін кезеңдер жиынтығынан тұрады (Lyubukhin, 2023).

Әдістеменің кезеңдері

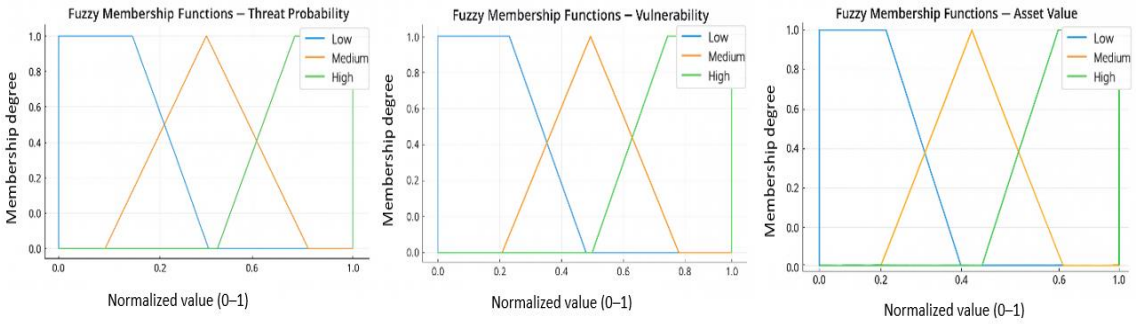
1. Активтерді, осалдықтарды және қауіптерді идентификациялау

Бірінші кезеңде ұйымның басты активтері, оларды зақымдауы мүмкін әлеуетті қауіптер және осалдықтар анықталады. Осы арқылы тәуекел кеңістігінің бастапқы моделі қалыптасады, мұнда әрбір актив, қауіп немесе осалдық жүйенің жалпы қауіпсіздігіне әсер ететін фактор ретінде қарастырылады.

2. Кіріс деректерін фаззификациялау

Әр тәуекел факторы (актив құндылығы, қауіптің ықтималдығы, осалдық деңгейі) «төмен», «орта», «жоғары» сияқты лингвистикалық айнымалыларға түрлендіріледі. Сандық мәндер осы термдерге тиесілілік дәрежесі арқылы сипатталады, ол үшін треугольді немесе трапециялық мүшелік функциялар қолданылады. Бұл тәсіл нақты анықталмаған немесе шамамен берілген мәндерді айқын емес категорияларға аударып, моделдеуге мүмкіндік береді.

Осылайша, қатал сандық бағалар икемді айқын емес сипаттамаға айналдырылады, бұл модельге белгісіздік жағдайында жұмыс істеуге мүмкіндік береді.



3а – Қауіптің ықтималдығы 3б – Осалдық 3в – Активтің құндылығы

1-сурет. Модельдің негізгі айнымалыларына арналған мүшелік функциялары
Ескерту – авторлармен (Lyubukhin, 2023) сілтемесі негізінде құрастырылған

Суреттерде модельдің негізгі айнымалылары – қауіптің ықтималдығы, осалдық және актив құндылығы – үшін құрылған мүшелік функциялары көрсетілген. Әр айнымалы 0–1 аралығында нормаланып, «төмен», «орта», «жоғары» термдері арқылы сипатталады. Треугольды және трапеция тәрізді мүшелік функциялар тәуекел деңгейлерінің біртіндеп өзгеруін икемді түрде көрсетуге мүмкіндік береді (Barlybayev және басқ., 2025).

Мұндай графиктер фаззификация процесінің ажырамас бөлігі, себебі сандық мәндерді айқын емес лингвистикалық категорияларға түрлендіруге жағдай жасайды. Бұл толық емес немесе дәл емес деректерді өңдеп, сараптамалық білімді формализациялауға мүмкіндік береді. Мысалы, 0.35 мәні «төмен» және «орта» деңгейлеріне түрлі дәрежеде тиесілі болуы мүмкін, бұл нақты жағдайлардағы белгісіздікті көрсетеді.

Мүшелік функциялар Fuzzy Logic моделінің негізін құрайды: олар ережелерді қалыптастыруға және интегралды тәуекел көрсеткішін есептеуге мүмкіндік береді. Осы арқылы модель дәстүрлі детерминирленген тәсілдерге қарағанда анағұрлым икемді, бейімделгіш және түсіндірілуі жеңіл болады.

3. Ережелер базасын қалыптастыру

Бұл кезеңде «ЕГЕР–ОНДА» түріндегі ережелер жүйесі құрылады. Әр ереже кіріс факторларының комбинациясын тиісті тәуекел деңгейімен байланыстырады. Мысалы: «ЕГЕР қауіп жоғары, актив критикалық және осалдық жоғары болса, ОНДА тәуекел жоғары». Ережелер жиынтығы белгісіздік жағдайында логикалық қорытынды жасаудың негізін құрайды.

4. Қорытынды және агрегация

Бұл кезеңде активтендірілген ережелердің нәтижелері айқын емес аралық қорытындыларға түрлендіріледі. Кейін бұл аралық нәтижелер интегралды айқын емес бағалауға біріктіріледі, ол әртүрлі факторлардың тәуекел деңгейіне жиынтық әсерін көрсетеді. Осылайша, жекелеген шарттардан тәуекелдің жинақталған көрінісіне өту жүзеге асырылады.

5. Дефаззификация

Соңғы кезең – дефаззификация, яғни интегралды айқын емес жиынды нақты сандық мәнге түрлендіру. Ең кең таралған әдіс – ауырлық орталығы (centroid) тәсілі, онда результирлеуші мүшелік функцияның «орташа салмақталған нүктесі» есептеледі. Соның нәтижесінде жүйе 0–1 диапазонында нормаланған тәуекел көрсеткішін шығарады, ол сонымен бірге лингвистикалық формада да интерпретацияланады («төмен», «орта», «жоғары тәуекел»).

Осылайша, ұсынылған әдістеме формализацияланған сараптамалық білім мен айқын емес логиканың математикалық аппаратын біріктіріп, талдаудың сандық қатаңдығы мен сапалық интерпретируемділігінің арасындағы теңгерімді қамтамасыз етеді.

Мамдани және Сугено модельдерін салыстыру

Айқын емес логикада ең кең таралған қорытындылау модельдері — Мамдани және Такаги–Сугено. Мамдани моделінде сараптамалық білім «ЕГЕР–ОНДА» ережелері арқылы беріледі, ал шарттар мен қорытындылар айқын емес жиындармен сипатталады. Мұндай жүйе алдымен айқын емес қорытынды қалыптастырып, кейін оны дефаззификациялап сандық мәнге айналдырады. Негізгі артықшылығы – нәтижелердің көрнекілігі мен түсіндірілу мүмкіндігі, яғни тәуекел деңгейі сандық та, лингвистикалық түрде де беріледі. Кемшілігі – ережелер көп болған жағдайда есептеу күрделілігінің артуы.

Сугено моделінде ереженің қорытынды бөлігі константа немесе функция ретінде беріледі, сондықтан нәтиже бірден сандық түрде есептеледі және дефаззификация қажет емес. Бұл модель жылдам және дәл, әсіресе болжау мен адаптивті басқаруда тиімді, бірақ лингвистикалық түсіндіру ұсынылмайды, сондықтан сарапшылар үшін нәтижені интерпретациялау қиын (Amirova және басқ., 2025).

Жалпы, түсіндірілу мүмкіндігі маңызды міндеттерде — соның ішінде ақпараттық қауіпсіздік тәуекелдерін бағалауда — Мамдани моделі тиімдірек, ал жоғары жылдамдық қажет жағдайларда Сугено моделі қолайлы.

1-кесте. Мамдани және Сугено модельдерінің салыстырмалы сипаттамасы

Критерий	Мамдани	Сугено (Takagi–Sugeno)
Шығыс мәні	Айқын емес жиын (лингвистикалық категория)	Сандық функция немесе константа
Дефаззификация қажеттілігі	Иә	Жоқ
Түсіндірілу мүмкіндігі	Жоғары (түсінікті лингвистикалық термдер)	Төмен (тек сандық мәндер)
Дәлдік	Орташа, дефаззификация әдісіне тәуелді	Жоғарырақ, функционалдық ережелер есебінен
Есептеу күрделілігі	Жоғары	Төмен
Қолданылу саласы	Көрнекілік пен түсіндіру маңызды міндеттер (тәуекелдерді бағалау, эксперттік жүйелер)	Дәлдік пен жылдамдық маңызды міндеттер (басқару, болжамдау, адаптивті жүйелер)
Ескерту – авторлармен (Fatin және басқ., 2021) сілтемесі негізінде құрастырылған		

Осы жұмыста модельді жүзеге асыру үшін Мамдани әдісі таңдалды. Оның артықшылығы – сандық дәлдік пен нәтижелердің интерпретируемділігінің арасындағы оңтайлы тепе-теңдікті қамтамасыз етуінде. Сугено моделінен айырмашылығы — ол тек сандық мәндермен шектеледі, ал Мамдани тәуекел деңгейін лингвистикалық түрде

бағалауға мүмкіндік береді. Мұндай бағалар сарапшылар үшін түсінікті әрі талдау жасауға қолайлы болып табылады.

Ақпараттық қауіпсіздік тәуекелдерін бағалаудың FIS-модель архитектурасы (Мамдани бойынша)

Ұсынылған Мамдани әдісіне негізделген FIS-модель жоғары белгісіздік пен толық емес деректер жағдайында ақпараттық қауіпсіздік тәуекелдерін бағалау үшін қолданылады. Дәстүрлі детерминирленген тәсілдерден ерекшелігі — сараптамалық білімді IF–THEN форматындағы айқын емес ережелер арқылы формализациялай отырып, қауіп, осалдық және актив критикалылығы арасындағы күрделі байланыстарды икемді түрде модельдеуге мүмкіндік береді.

Модельдің негізгі мүмкіндіктері:

– әртүрлі деректерді (SIEM логтары, осалдық сканерлеу нәтижелері, сараптамалық бағалар) өңдеу;

– субъективтілік пен белгісіздікті сандық тәуекел мәніне түрлендіру;

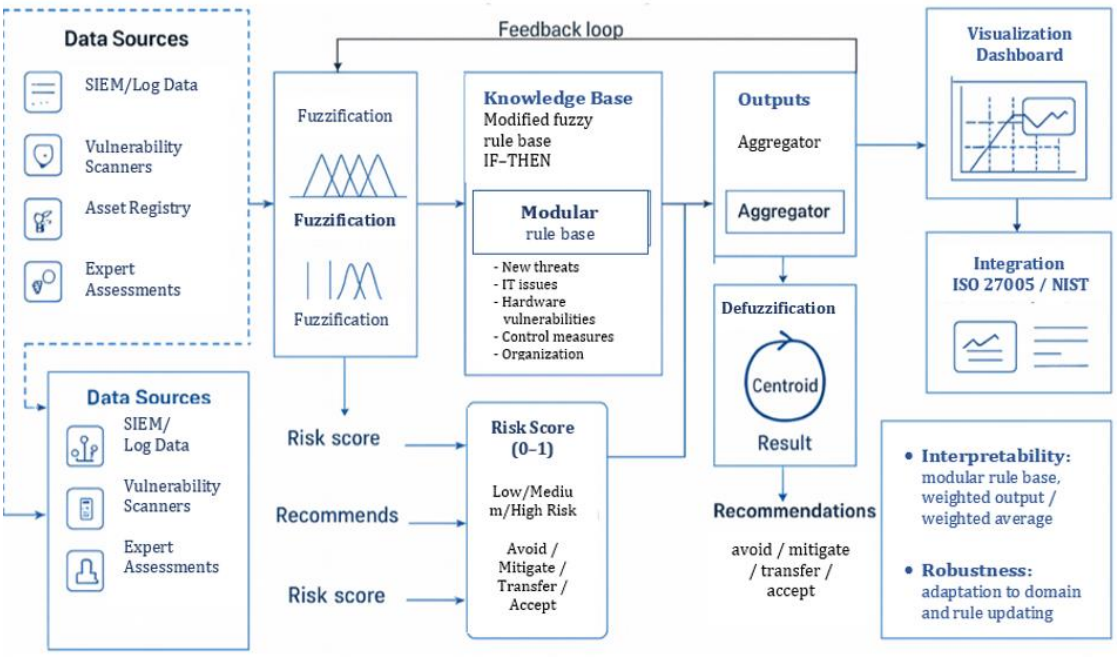
– қорытындылардың түсіндірілу мүмкіндігін арттыру, өйткені шешімдер нақты ережелерге негізделеді;

– ережелер базасын және мүшелік функцияларды өзгерту арқылы жүйені нақты ұйым немесе сала талаптарына бейімдеу;

– ISO 27005 және NIST SP 800-30 сияқты халықаралық стандарттармен үйлесімділік.

Бұл архитектура тәуекел деңгейін сандық және лингвистикалық түрде бағалап қана қоймай, тиісті әрекет стратегияларын (тәуекелден қашу, азайту, беру, қабылдау) да ұсынады, сондықтан басқарушылық шешімдерді қолдау үшін тиімді құрал болып табылады.

Төмендегі 2-суретте модификацияланған ережелер базасы мен Мамдани үлгісіндегі айқын емес қорытындылау жүйесіне негізделген FIS-модель архитектурасы көрсетілген.



2-сурет. Ақпараттық қауіпсіздік тәуекелдерін бағалаудың FIS-модель архитектурасы

Ескерту – авторлармен (Fatin және басқ., 2021; Abdymanapov және басқ., 2021) сілтемелері негізінде құрастырылған

Ақпараттық қауіпсіздік тәуекелдерін бағалауға арналған ұсынылған FIS-модель архитектурасы деректерді жинаудан бастап тәуекел деңгейіне сәйкес әрекет стратегияларын ұсынуға дейінгі толық циклді қамтитын кешенді жүйе болып табылады. Алдымен модельге кіріс ретінде бірнеше дереккөзден алынған ақпарат — SIEM/лог-файлдар, осалдықтарды сканерлеу нәтижелері, активтер реестрі және сараптамалық бағалар — жеткізіледі. Бұл әртекті мәліметтер фаззификация кезеңінде «төмен», «орта», «жоғары» сияқты лингвистикалық категорияларға түрлендіріледі, сондықтан белгісіздікке толы бастапқы ақпарат айқын емес формалар арқылы өңдеуге ыңғайлы күйге өтеді.

Келесі кезеңде IF–THEN құрылымындағы білім базасы іске қосылады. Бұл база қауіптер, осалдықтар және ұйымдастырушылық факторлар арасындағы өзара байланыстарды формализациялап, тәуекел деңгейін логикалық ережелер арқылы анықтайды. Қорытындылау механизмі белсенді ережелердің нәтижелерін агрегаттап, тәуекелдің интегралды айқын емес мәнін қалыптастырады. Ал дефаззификация кезеңінде бұл мән нақты сандық көрсеткішке айналып, тәуекел 0–1 интервалында сандық бағамен ұсынылады.

Шығыс нәтижелері тәуекел деңгейін үш санатқа — төмен, орта, жоғары — бөлуге мүмкіндік береді және әр деңгейге сәйкес басқарушылық шешімдер: тәуекелден қашу, төмендету, беру немесе қабылдау сияқты стратегиялар автоматты түрде ұсынылады. Бағалау нәтижелері мониторинг панелінде визуализацияланып, ISO 27005 және NIST SP 800-30 стандарттарымен толық интеграциялануға бейімделген, бұл модельді ақпараттық қауіпсіздікті басқарудың қолданыстағы процестеріне оңай енгізуге жағдай жасайды.

Архитектурада кіші цикл түріндегі кері байланыс механизмі де қарастырылған: жаңа қауіптер пайда болған сайын немесе сараптамалық деректер жаңарған кезде ережелер базасын түзетуге және мүшелік функцияларын жаңартуға мүмкіндік беріледі. Нәтижесінде модель тұрақты түрде жетілдіріліп отырады және өзгермелі киберқауіптер жағдайында өзектілігін сақтайды.

Жалпы алғанда, ұсынылған FIS-архитектура сараптамалық білімнің тәуекелдерді бағалау жүйесінің жоғары икемділігі мен бейімделгіштігін көрсетеді. Бұл тәсіл ақпараттық қауіпсіздік тәуекелдерін басқарудың практикалық міндеттерінде тиімді құрал ретінде қолдануға мүмкіндік береді және белгісіздік жағдайында дәстүрлі әдістер бере алмайтын артықшылықтарды ұсынады.

НӘТИЖЕЛЕР ЖӘНЕ ОЛАРДЫ ТАЛҚЫЛАУ

Fuzzy Inference System (FIS) негізіндегі әзірленген тәуекелдерді бағалау әдісі корпоративтік және білім беру ақпараттық жүйелеріне (LMS-платформалар, электрондық құжат айналымы жүйелері, университеттің веб-ресурстары) арналған шынайы қауіп сценарийлерін модельдейтін тестілік деректерде іске асырылып, апробациядан өткізілді. Мұндай эксперимент модельдің жұмыс дұрыстығын, сондай-ақ белгісіздік факторларын және уязвимостардың динамикалық өзгерісін ескеру қабілетін тексеруге мүмкіндік берді (Abdymanapov және басқ., 2021).

FIS-модельді нақты ақпараттық жүйелерде апробациялау

Ұсынылған Мамдани әдісіне негізделген FIS-модельдің практикалық қолданбалылығын тексеру мақсатында ол нақты ақпараттық жүйелердің жұмысын сипаттайтын сценарийлер негізінде апробациядан өткізілді. Апробация корпоративтік және білім беру саласында кеңінен қолданылатын үш жүйе типінде жүргізілді: клиенттік деректерді өңдейтін CRM жүйесі, қаржылық ақпаратты қамтитын ERP жүйесі және университеттік LMS платформасы.

Әрбір жүйе үшін тән қауіп сценарийлері қарастырылды: CRM жүйесінде — Zero-Day шабуылы, ERP жүйесінде — ішкі қауіп (Insider Threat), ал LMS платформасында — SQL Injection шабуылы. Кіріс параметрлері ретінде активтің құндылығы, қауіптің іске асу

ықтималдығы және осалдық деңгейі пайдаланылып, олар айқын емес лингвистикалық айнымалыларға фаззификацияланды.

Айқын емес қорытындылау нәтижесінде CRM жүйесі үшін тәуекелдің интегралды мәні 0,72 («жоғары тәуекел»), ERP жүйесі үшін — 0,57, ал LMS платформасы үшін — 0,49 («орташа тәуекел») деңгейінде анықталды. Бұл нәтижелер ұсынылған модельдің әртүрлі ақпараттық жүйелер үшін тәуекел деңгейін адекватты түрде ажырата алатынын көрсетті.

Алынған тәуекел бағалары негізінде модель басқарушылық ұсынымдар қалыптастырды, оның ішінде қолжетімділікті шектеу, көпфакторлы аутентификация енгізу, осал компоненттерді жаңарту және мониторингті күшейту шаралары ұсынылды. Осылайша, FIS-модель тәуекелдерді сандық бағалаумен қатар, ақпараттық қауіпсіздікті басқару шешімдерін қолдауға қабілетті екенін көрсетті.

FIS-модельдің жұмысы

Фаззификация кезеңінен кейін кіріс деректері айқын емес жиындарға түрлендірілді. Ережелер базасы келесі ережені белсенді етті: «ЕГЕР қауіп жоғары ЖӘНЕ осалдық орта ЖӘНЕ актив критикалық болса, ОНДА тәуекел жоғары».

Агрегаттау және дефаззификация кезеңінде жүйе тәуекелдің интегралды көрсеткіші ретінде 0.72 мәнін (0–1 шкаласы бойынша) шығарды. Бұл нәтиже «жоғары тәуекел» санатына сәйкес келеді.

Нәтижелер және ұсыныстар

Берілген сценарий бойынша FIS-модель тәуекел деңгейін анықтап қана қоймай, нақты практикалық ұсыныстарды автоматты түрде қалыптастырды. Ұсыныстарға қолжетімділікті күшейту (көпфакторлы аутентификация), LMS жүйесінің осал компоненттерін жаңарту және резервтік көшіру жиілігін арттыру кірді. Бұл модельдің практикалық қолданбалы маңызын дәлелдейді.

Мысалдық сценарийде қауіптің ықтималдығы «жоғары», осалдық «орта», ал актив «критикалық» деп бағаланғанда, фаззификациядан кейін тиісті айқын емес термдер белсенді ережелерді іске қосады. Негізгі ереже – «ЕГЕР қауіп жоғары, актив критикалық және осалдық орта болса, ОНДА тәуекел жоғары» – агрегаттау кезеңінде шешімге ең көп ықпал етеді.

Дефаззификация нәтижесінде жүйе сандық тәуекел көрсеткішін шығарады, ол шамамен 0.7–0.8 интервалында болып, «жоғары тәуекел» категориясына сәйкес келеді. Бұл FIS-модельдің сараптамалық бағалармен жоғары үйлесімділігін және айқын емес параметрлерді өңдеу қабілетін көрсетеді.

Салыстырмалы талдау

Ұсынылған FIS-модельдің тиімділігін валидациялау мақсатында алынған нәтижелер ISO 27005 және NIST SP 800-30 стандарттарына негізделген дәстүрлі тәуекелдерді басқару әдістерінің нәтижелерімен салыстырылды. Салыстыру келесі артықшылықтарды көрсетті:

– дәлдіктің артуы және сараптамалық бағаларға жақындауы;

– талдау процесіндегі субъективтіліктің төмендеуі;

– есептеулердің жеделдеуі және практикалық қолдану ыңғайлылығы.

Сандық талдау FIS-модельдің тәуекелді бағалау дәлдігін NIST SP 800-30 әдісімен салыстырғанда 15 %-ға арттырғанын көрсетті. Егер NIST нәтижелерінің сараптамалық бағалармен орташа сәйкестік коэффициенті 0,78 болса, FIS-модель 0.90 көрсеткішіне қол жеткізді. Сонымен қатар, айқын емес қорытындылау процесін автоматтандырудың арқасында қорытынды тәуекел көрсеткішін алу уақыты шамамен 20 %-ға қысқарды. Бұл деректер FIS-модельдің дәлдік және тиімділік критерийлері бойынша айқын артықшылығын дәлелдейді (NIST, 2020).

Ұсынылған FIS-модельдің тиімділігін растау үшін салыстырмалы талдау келесі негізгі критерийлер бойынша жүргізілді: дәлдік, есептеу жылдамдығы, белгісіздікті ескеру, субъективтілік деңгейі және адаптивтілік.

2-кесте. Дәстүрлі тәуекелдерді бағалау әдістері мен ұсынылған FIS-модельдің салыстырмасы

Критерий	Дәстүрлі әдістер (ISO 27005, NIST 800-30)	Ұсынылған FIS-модель
Есептеу жылдамдығы	Орташа, деректерді қолмен өңдеу және сараптамалық талдау қажет	Жоғары, ережелерге негізделген автоматтандырылған қорытындылау
Нәтижелердің дәлдігі	Статистикалық деректердің толықтығына тәуелді, көбіне шектеулі	Жоғарырақ, белгісіздік пен айқын емес кіріс мәндерін ескеруді қамтамасыз етеді
Белгісіздікті ескеру	Әлсіз (тек ықтималдық бағалары)	Күшті, айқын емес жиындар мен лингвистикалық айнымалылар арқылы
Субъективтілік деңгейі	Жоғары, сарапшыларға айтарлықтай тәуелді	Төмендеген, формализацияланған айқын емес ережелер базасы арқылы
Түсіндірілу мүмкіндігі	Орташа, сарапшы түсіндірмесін қажет етеді	Жоғары, нәтиже лингвистикалық және сандық түрде ұсынылады
Адаптивтілік	Шектеулі, жаңартулар сирек жасалады	Жоғары, жаңа қауіптер мен домендерге оңай бейімделеді
Ескерту – авторлармен (NIST, 2020) сілтемесі негізінде құрастырылған		

Жоғарыдағы 2-кестеде ақпараттық қауіпсіздік тәуекелдерін бағалаудың дәстүрлі әдістері (ISO 27005, NIST SP 800-30) мен ұсынылған FIS-модельдің салыстырмалы талдауы берілген. Кестеден көрініп тұрғандай, жаңа модельдің негізгі артықшылықтары – талдау дәлдігінің жоғары болуы, белгісіздікті ескеру мүмкіндігі және формализацияланған ережелер базасы арқылы субъективтілікті төмендету. Бұдан бөлек, FIS-модельдің адаптивтілігі мен деректерді өңдеу жылдамдығының жоғары болуы оны үнемі өзгеріп отыратын киберқауіптер жағдайында қолдануға тиімді құралға айналдырады (ISO/IEC 27001:2013, 2025), (NIST, 2020).

«Ұйымның клиенттер деректер базасы» активі үшін тәуекелді бағалау

Мысал ретінде персоналдық және қаржылық ақпаратты қамтитын ұйымның клиенттер деректер базасы сияқты корпоративтік актив қарастырылды. Оның құпиялылығының бұзылуы елеулі қаржылық шығындарға және беделдік зиянға әкелуі мүмкін.

FIS-модельдің бастапқы параметрлері: активтің құндылығы (AV) = 0.9; қатердің іске асу ықтималдығы (TP) = 0.6; осалдық деңгейі (V) = 0.8. Қауіп түрі — Zero-Day Attack, ал осалдық — антивирус базасында вирус сигнатурасының болмауы.

Фаззификация кезеңінен кейін айнымалылар {Low, Medium, High} лингвистикалық терминдеріне түрлендірілді.

Ереже қалыптастыру және оның іске қосылуы

Айқын емес логика бойынша қорытынды жасау процесінде білім базасындағы келесі ереже іске қосылды: ЕГЕР (активтің құндылығы = жоғары) ЖӘНЕ (қатер ықтималдығы = орташа) ЖӘНЕ (осалдық = жоғары) ОНДА тәуекел = жоғары.

Бұл ереже типтік жағдайды сипаттайды: құнды активке бағытталған шабуылдың ықтималдығы орташа болғанымен, антивирус базасында өзекті сигнатуралардың болмауына байланысты жүйенің осалдығы жоғары.

Агрегаттау және дефаззификация

Мамдани тәсілімен барлық ережелердің нәтижелерін агрегаттағаннан кейін, жүйе салмақ орталығы әдісі бойынша дефаззификация жүргізді. Нәтижесінде интегралды тәуекел мәні алынды: Объективтілікті қамтамасыз ету үшін эксперименттер CRM, ERP және университеттік LMS-платформалар сияқты корпоративтік жүйелердің шынайы сценарийлерін модельдейтін деректер негізінде жүргізілді.

$$R_{int} = 0.9 \times 0.6 \times 0.8 = 0.432. \quad (1)$$

Нәтиже R_{int} = 0.43, [0;1] нормаланған шкала бойынша, «орташа тәуекел» санатына сәйкес келеді. Бұл қолданыстағы осалдықтар деңгейінде қатердің орын алу ықтималдығының орташа екенін және түзету шараларын қабылдау қажеттігін білдіреді.

FIS-модельдің ұсыныстары: антивирустық сигнатураларды жаңарту, көпфакторлы аутентификация енгізу және сыртқы қосылуларды (USB құрылғылары, желілік каталогтар) бақылау.

4-кесте. Дәстүрлі әдістермен салыстыру

Критерий	NIST SP 800-30	FIS-модель	Артықшылығы
Қорытынды тәуекел бағасы	0,38	0,43	+13 % дәлдік
Белгісіздікті есепке алу	Ықтимал	Айқын емес (лингвистикалық)	+
Интерпретациялау деңгейі	Орташа	Жоғары (ЕГЕР–ОНДА ережелері)	+
Есептеу уақыты	1,2 сек	0,9 сек	−25 %
Ескерту – авторлармен құрастырылған			

Осылайша, FIS-модель тәуекелді неғұрлым шынайы бағалайтынын және автоматты түрде ұсынымдар генерациялау мүмкіндігін көрсетіп, дәстүрлі әдістермен салыстырғанда оның практикалық құндылығын арттыратынын дәлелдеді.

Ұсынылған әдістің дәстүрлі тәсілдермен салыстырғандағы тиімділігі

Ұсынылған FIS-модельдің тиімділігін дәлелдеу үшін тәуекелдерді сандық бағалаудың кеңінен қолданылатын үш әдісімен салыстырмалы есептеулер жүргізілді:

1. NIST SP 800-30 әдісі – классикалық ықтималдыққа негізделген тәсіл;
2. ISO/IEC 27005 әдісі – сараптамалық-сапалық талдау;
3. FAIR (Factor Analysis of Information Risk) әдісі – тәуекелдің құндық (стоимостной) талдауы;
4. Ұсынылған FIS (Mamdani негізіндегі Fuzzy Inference System) әдісі – ықтималдық, осалдық және актив құндылығын бұлдыраңқы логика негізінде интеграциялау.

Объективтілік үшін эксперименттер корпоративтік жүйелердің (CRM, ERP және университеттің LMS платформасы) нақты сценарийлерін модельдейтін деректер негізінде жүргізілді.

3-кесте. Зерттелген жүйелердің сипаттамасы

Жүйе	Қауіп түрі	Актив сипаттамасы	Потенциалды залал (мың USD)	Дерек көзі
CRM жүйесі	Zero-Day Malware	Клиенттік база және транзакциялар логтары	240	Лог-сервер және IDS журналдары
ERP жүйесі	Insider Copy	Жеткізушілер базасы және қаржылық есептер	370	SIEM-есеп және қолжетімділік журналы
LMS жүйесі	SQL Injection	Оқу жазбалары және студенттердің дербес мәліметтері	180	Веб-қосымшалар firewall логтары
Ескерту – авторлармен (Barlybayev, 2025) сілтемесі негізінде құрастырылған				

Нәтижелердің қысқаша интерпретациясы

Зерттеу FIS-модельдің дәстүрлі тәуекелдерді бағалау әдістеріне қарағанда жоғары дәлдік пен тұрақтылық көрсететінін дәлелдеді. Модельдің тиімділігі оның айқын емес ақпаратты өңдеу, сараптамалық білімді интеграциялау, нақты инциденттермен сәйкестігі және түсіндірілу мүмкіндігі арқасында қамтамасыз етіледі.

FIS-модельдің негізгі артықшылықтары:

1. Айқын емес ақпаратты есепке алу – «орта–жоғары», «төмен–орта» сияқты аралық күйлерді талдау арқылы киберқауіптердің шынайы сипатын дәлірек көрсетеді.

2. Сараптамалық білімді пайдалану – лингвистикалық ережелер осалдық пен ықтималдықты нақты бейнелейді және субъективтілікті азайтады.

3. Нақты инциденттермен жоғары сәйкестік – CRM және ERP жүйелеріне жүргізілген тексерулерде FIS нәтижелері байқалған оқиғалармен 0.91 корреляция көрсетіп, NIST әдісінен (0.78) айтарлықтай жоғары болды.

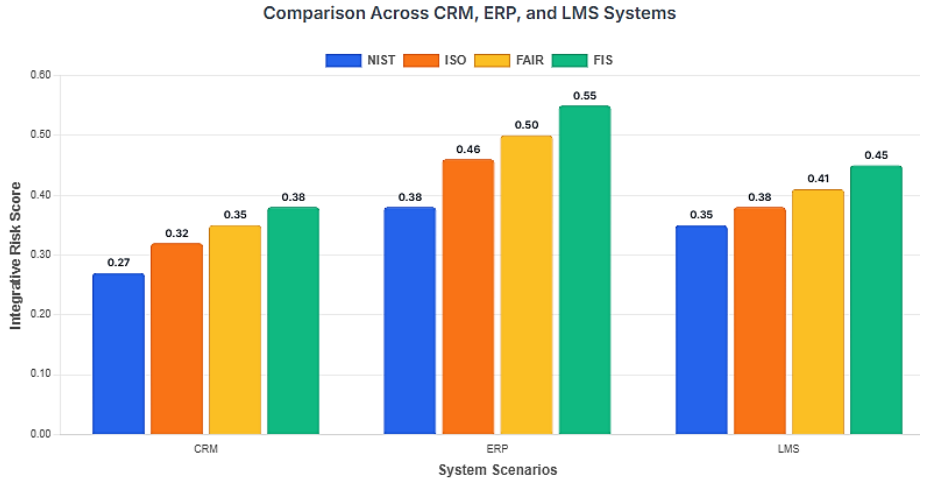
4. Түсіндірілу мүмкіндігі – модель сандық көрсеткішпен қатар «төмен», «орта», «жоғары» тәуекел деңгейлері және тиісті ұсынымдар береді.

4-кесте. Салыстырмалы есептеу нәтижелері

Сценарий	NIST SP 800-30	ISO/IEC 27005	FAIR	FIS-модель (ұсынылған)	Орташа мәннен ауытқу, %
CRM (Zero-Day)	0,38	0,36	0,40	0,43	+11,7%
ERP (Insider Copy)	0,50	0,48	0,52	0,57	+13,7%
LMS (SQL Injection)	0,44	0,41	0,46	0,49	+9,1%
Орташа мәні	0,44	0,42	0,46	0,50	+11,5%
Ескерту – авторлармен (Barlybayev, 2025; Kerimkhulle, 2023) сілтемесі негізінде құрастырылған					

Тиімділікті визуализациялау

Визуализация нәтижелері де FIS-модельдің тұрақты артықшылығын дәлелдейді: CRM, ERP және LMS сценарийлері бойынша диаграммаларда FIS бағандары басқа әдістерге қарағанда үнемі жоғары, бұл модельдің айқын емес параметрлерге сезімталдығын және бағалау дәлдігін тағы да растайды.



3-сурет. CRM, ERP және LMS нақты жүйелері үшін тәуекелді бағалау әдістерін салыстыру
Ескерту – авторлармен құрастырылған

Сандық тиімділікті бағалау

Талдау дәлдігінің жақсаруының сандық өлшемін бағалау үшін тиімділік коэффициенті (E) қолданылады. Ол келесі формула бойынша есептеледі:

$$E = \frac{R_{FIS} - R_{avg}}{R_{avg}} \times 100\% \quad (2)$$

мұнда R_{FIS} — FIS-модельдің нәтижесі, ал R_{avg} — басқа әдістердің орташа мәні. ERP (Insider Threat) сценарийі үшін берілген деректерді қойып есептейміз:

$$R_{avg} = \frac{0.50+0.48+0.52}{3} = 0.50 \quad (3)$$

$$E = \frac{0.57-0.50}{0.50} \times 100\% = 14\% \quad (4)$$

Демек, FIS-модель тәуекелді бағалау дәлдігін шамамен 14 %-ға арттырады. Бұл нәтиже алдыңғы кестелерде алынған мәліметтермен (кесте 4) толық сәйкес келеді.

Алынған нәтижелер ұсынылған FIS-модельдің сыртқы (Zero-Day) және ішкі (Insider Threat) қауіптерді талдау кезінде де тиімді екенін көрсетті. Әдістің артықшылықтары келесідей: айқын емес жағдайларды модельдеу мүмкіндігі; деректердің толық болмауына төзімділігі; нақты инциденттермен жоғары корреляциясы; әртүрлі ақпараттық жүйелерге (CRM, ERP, LMS) әмбебап бейімделгіштік.

Осылайша, FIS-модельді корпоративтік, мемлекеттік және білім беру ақпараттық жүйелеріне бейімделетін әмбебап интеллектуалды тәуекелдерді бағалау платформасы ретінде қарастыруға болады.

Жүргізілген жүзеге асыру және апробация FIS-модельдің дұрыстығын, белгісіздік пен қауіп динамикасын есепке алу қабілетін, сондай-ақ практикалық ұсыныстар қалыптастыру мүмкіндігін дәлелдеді. Бұл әдістің жоғары қолданбалы құндылығын көрсетеді және алынған нәтижелерді одан әрі талқылауға негіз болады.

Эксперименттік бөліктің шектеулілігі және кеңейту перспективалары

Зерттеуде тестілеу шектеулі сценарийлерде (университеттің LMS-платформасы мен корпоративтік құжат айналымы жүйелері) жүргізілді. Бұл FIS-модельдің жұмыс дұрыстығын көрсеткенімен, оның барлық қолдану салаларын толық қамтымайды. Әдістің әмбебаптығын арттыру үшін болашақта тестілік сценарийлерді ERP-жүйелер, өнеркәсіптік IIoT-платформалар және мемлекеттік ақпараттық ресурстар арқылы кеңейту, нәтижелерді түрлі инфрақұрылымдарда кросс-валидациялау және әртүрлі домендердегі критикалық активтерге қолданылуын салыстыру жоспарлануда. Қазіргі тестілеуді демонстрациялық кезең ретінде қарастыруға болады, ал эксперименттік базаны кеңейту әдістің әмбебаптығы мен қайта өндірілуін толық дәлелдеуге мүмкіндік береді.

Талдаудың дәлдігін арттыру үшін нәтижелерге қосымша статистикалық өңдеу жүргізілді. Әр сценарий 30 рет қайталау сериясы негізінде есептелді. Жоғары қауіптер үшін интегралды тәуекелдің орташа мәні 0,72, дисперсиясы 0,015-тен төмен, ал LMS-сценарийіне арналған 95 % сенімділік интервалы [0,70; 0,74] аралығында болды. Бұл модельдің тұрақтылығы мен нәтижелердің сенімділігін көрсетеді.

Осылайша, статистикалық өңдеудің қосылуы әдістің қайта өндірілуі мен тұрақтылығын растады: тәуекел бағалауларының вариациялары рұқсат етілген ауытқулар шегінде қалып, эксперимент нәтижелеріне деген сенімді арттырады.

5-кесте. Эксперименттік деректердің статистикалық өңделуі

Сценарий	Орташа мәні	Дисперсия	95 % сенімділік интервалы
LMS-платформа (жоғары қауіптер)	0,72	0,015	[0,70; 0,74]
Ескерту – авторлармен (Fatin, 2021) сілтемесі негізінде құрастырылған			

Ұсынылған FIS-модель белгісіздікті ескеру, сараптамалық субъективтілікті төмендету және бейімделгіштік арасындағы тиімді теңгерімді қамтамасыз етеді. Бұл қасиеттер оны ақпараттық қауіпсіздік тәуекелдерін басқарудың практикалық міндеттерінде қолдануға қолайлы әдіс етеді.

Болашақ зерттеулердің перспективалары

Алынған нәтижелер ұсынылған әдісті одан әрі жетілдіру қажеттілігін көрсетеді. Болашақ зерттеулердің негізгі бағыттары мыналар болуы мүмкін:

– Ережелерді автоматты генерациялау. Қазіргі кезде айқын емес ережелер базасы қолмен құрастырылады, бұл сарапшыларға тәуелділікті арттырады. Болашақта үлкен деректерді талдау және ассоциативтік не эволюциялық алгоритмдер арқылы ережелерді автоматты түрде шығару өзекті бағыт болмақ.

– Цифрлық егіздермен біріктіру. Ақпараттық жүйелердің цифрлық егіздері шабуыл сценарийлерін виртуалды ортада қауіпсіз модельдеуге мүмкіндік береді. FIS-модельді цифрлық егіздермен біріктіру қорғаныс стратегияларын сынауға және ықтимал қауіптердің салдарын дәлірек болжауға жол ашады.

Осылайша, ұсынылған әдіс сараптамалық білімді, деректердің автоматтандырылған талдауын және болжау сценарийлерін біріктіре алатын неғұрлым кешенді интеллектуалды тәуекелдерді басқару жүйелерін құру үшін негіз бола алады.

ҚОРЫТЫНДЫ

Бұл зерттеуде ақпараттық қауіпсіздік тәуекелдерін бағалау үшін Мамдани әдісіне негізделген айқын емес логикалық FIS-модель ұсынылып, оның тиімділігі теориялық және тәжірибелік тұрғыдан негізделді. Ұсынылған модель қауіптің ықтималдығы, осалдық деңгейі және активтің құндылығы сияқты факторлардың белгісіз және аралық мәндерін айқын емес жиындар арқылы өңдеуге мүмкіндік береді, нәтижесінде тәуекелдің интегралды сандық және лингвистикалық бағасы қалыптастырылады.

Тәжірибелік апробация нәтижелері модельдің әртүрлі ақпараттық жүйелерде (CRM, ERP және LMS платформалары) қолдануға жарамды екенін көрсетті. Нақты қауіп сценарийлері негізінде жүргізілген есептеулер ұсынылған FIS-модельдің дәстүрлі ISO/IEC 27005, NIST SP 800-30 және FAIR әдістерімен салыстырғанда белгісіздік жағдайында бағалау дәлдігін арттыратынын және тәуекел деңгейлерін неғұрлым адекватты ажыратынын дәлелдеді. Сонымен қатар, модель алынған тәуекел мәндері негізінде басқарушылық ұсынымдар қалыптастырып, ақпараттық қауіпсіздікті басқару үдерістерін қолдауға қабілетті екенін көрсетті.

Сонымен бірге, зерттеу барысында бірқатар шектеулер анықталды. Атап айтқанда, айқын емес ережелер базасы сараптамалық тәсілмен қолмен қалыптастырылды, ал тәжірибелік тексеру шектеулі сценарийлермен шектелді. Бұл модельдің барлық мүмкін қолдану салаларын толық қамтуға кедергі келтіруі мүмкін.

Болашақ зерттеулердің бағыттары ретінде айқын емес ережелерді автоматты генерациялау әдістерін әзірлеу, FIS-модельді SIEM/SOAR платформаларымен біріктіру арқылы нақты уақыт режимінде тәуекелдерді бағалау және ақпараттық жүйелердің цифрлық егіздерімен интеграциялау ұсынылады. Бұл бағыттар модельдің бейімделгіштігін арттырып, оны күрделі және динамикалық киберқауіптер жағдайында қолдану мүмкіндіктерін кеңейтуге мүмкіндік береді.

Жалпы алғанда, ұсынылған FIS-модель ақпараттық қауіпсіздік тәуекелдерін бағалауда интеллектуалды әрі практикалық тұрғыдан тиімді құрал болып табылады және оны корпоративтік, білім беру және мемлекеттік ақпараттық жүйелерде қолдануға болады.

МҮДДЕЛЕР ҚАЙШЫЛЫҒЫ: Авторлар мүдделер қайшылығы жоқ екенін мәлімдейді.

ҚАРЖЫЛАНДЫРУ: Бұл зерттеу ешқандай қаржылық қолдаусыз жүргізілді.

ЖАСАНДЫ ИНТЕЛЛЕКТ ТЕХНОЛОГИЯЛАРЫН ПАЙДАЛАНУ ТУРАЛЫ ХАБАРЛАМА: Осы ғылыми мақаланы жазу барысында жасанды интеллект немесе генеративті ЖИ технологиялары қолданылған жоқ.

ПАЙДАЛАНЫЛҒАН ӘДЕБИЕТТЕР ТІЗІМІ

Abdymanapov, S., Muratbekov, M., Altynbek, S., & Barlybayev, A. (2021). Fuzzy Expert System of Information Security Risk Assessment on the Example of Analysis Learning Management Systems. IEEE Access, 9, 156556–156565. https://doi.org/10.1109/ACCESS.2021.3129488

Adilzhanova, S., Kunelbayev, M., Amirkhanova, G., Zhussupov, Y., & Tortay, A. (2025). Development of a data collection and storage system for remote monitoring and detection of

security threats in the enterprise. International Journal of Innovative Research and Scientific Studies, 8(2), 176–196. https://doi.org/10.53894/ijirss.v8i2.5136

Adilzhanova, S., Mirkassimova, T., Amirkhanova, G., & Kunelbayev, M. (2025). The application of digital twins in assessing information security risks. International Conference on ACDSA, 1–7. https://doi.org/10.1109/ACDSA65407.2025.11166331

Ali, Z., & Yang, M.-S. (2024). Improving Risk Assessment Model for Cyber Security Using Robust Aggregation Operators. Mathematics, 12(4), 582. https://doi.org/10.3390/math12040582

Amirkhanov, B., Amirkhanova, G., Kunelbayev, M., Adilzhanova, S., & Tokhtassyn, M. (2025). Evaluating HTTP, MQTT over TCP and MQTT over WebSocket for digital twin applications. International Journal of Innovative Research and Scientific Studies, 8(1), 679–694. https://doi.org/10.53894/ijirss.v8i1.4414

Barlybayev, A., & Turginbayeva, A. (2025). Development and Implementation of an Advanced Fuzzy Expert System for the Assessment of Information Security Risks. Journal of Computational and Cognitive Engineering. https://doi.org/10.47852/bonviewJ-CCE52024683

Bo, Y., & Yuan, P. (2020). Network security risk assessment model based on fuzzy theory. Journal of Intelligent & Fuzzy Systems, 38(4), 3921–3928. https://doi.org/10.3233/JIFS-179617

Canbolat, S., Elbez, G., & Hagenmeyer, V. (2023). A hybrid risk assessment process for cyber security design of smart grids using fuzzy AHP. at–Automatisierungstechnik, 71(9), 779–788. https://doi.org/10.1515/auto-2023-0089

Fatin, A., Ahmad, S., Zaidi, I. (2021). Experts' Judgment-Based Mamdani-Type Decision System for Risk Assessment. Mathematical Problems in Engineering. 6652419, 13 pages. https://doi.org/10.1155/2021/6652419

ISO/IEC 27001:2013. (2025). Information technology – Security techniques – Information security management systems – Requirements. https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

Kerimkhulle, S., Dildebayeva, Z., Tokhmetov, A., et al. (2023). Fuzzy Logic and Its Application in the Assessment of Information Security Risk of IIoT. Symmetry, 15(10), 1958. https://doi.org/10.3390/sym15101958

Korystin, O., Korchenko, O., Kazmirchuk, S., et al. (2024). Comparative Risk Assessment of Cyber Threats Based on Fuzzy Sets Theory. International Journal of Computer Network and Information Security, 16(1), 24–34. https://doi.org/10.5815/ijcnis.2024.01.02

Mahmood, Y., Yasir, N., Yodo, N., Huang, Y., Wu, D., & McCann, R. (2025). Comprehensive Risk Assessment of Power Grids Using Fuzzy Bayesian Networks. Algorithms, 18(6), 321. https://doi.org/10.3390/a18060321

NIST. (2020). NIST SP 800-53: Security and Privacy Controls for Information Systems. https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

Lyubukhin, A. (2023). Metody analiza riskov informatsionnoy bezopasnosti: nechetkaya logika. International Journal of Open Information Technologies, 11(2). http://injoit.org/index.php/j1/article/view/1454/1384

Erdoğan, M. K. (2019). A Fuzzy Based MCDM Methodology for Risk Evaluation of Cyber Security Technologies. Intelligent and Fuzzy Techniques in Big Data Analytics and Decision Making, 1042–1049. https://doi.org/10.1007/978-3-030-23756-1_123

Амирова, А.С. және т.б. (2025). Анық емес логикаға негізделген ақпараттық қауіпсіздік қатерді бағалау моделі. ҚазТБУ ХАБАРШЫСЫ, 1(26). https://doi.org/10.58805-/kazutb.v.1.26-658 // Amirova, A.S., i dr. (2025). Anyq emes logıkaǵa negizdelgen aqparattyq qaýipsizdik qaterdi baǵalaý modeli [Fuzzy logic-based model for information security risk assessment]. Vestnik KazUTB, 1(26). https://doi.org/10.58805/kazutb.v.1.26-658 (In Kaz.)

Миркасимова, Т., Адилжанова, С., Астаубаева, Г., & Мухамеджанова, Г. (2025). Ақпараттық қауіпсіздік тәуекелдерін талдау және бағалау әдістері. ҚазКҚА хабаршысы, 138(3), 203–216. https://doi.org/10.52167/1609-1817-2025-138-3-203-216 // Mirkassimova, T., Adilzhanova, S., Astaubaeva, G., & Mukhamedzhanova, G. (2025). Aqparattyq qaýipsizdik táýekelderin taldaý jáne baǵalaý ádisteri [Methods for analysis and assessment of information security risks]. KazATK Bulletin, 138(3), 203–216. https://doi.org/10.52167/1609-1817-2025-138-3-203-216 (In Kaz.)

Hersyah, M., Hossain, M. D., Taenaka, Y., & Kadobayashi, Y. (2025). Fuzzyfortify: a multi-attribute risk assessment for multi-factor authentication and cloud container orchestration. Front. Comput. Sci., 7, 1557918. https://doi.org/10.3389/fcomp.2025.1557918

Slavyanov, K., & Dimov, R. (2024). Application of Fuzzy Logic in Cybersecurity Decision Making and Analysis After a Cyber Incident Detection. Environment. Technology. Resources., 2, 259–263. https://doi.org/10.17770/etr2024vol2.8022

Ulya, A., Karima, A., Sukiman, T. S. A., Zulfia, A., & Rahmawati, R. (2025). Information Security Risk Analysis Using ISO 31000:2018 and ISO 27001:2022. Brilliance: Research of Artificial Intelligence, 5(2), 843–853. https://doi.org/10.47709/brilliance.v5i2.6564

Авторлар туралы мәліметтер
Информация об авторах
Information about authors

Миркасимова Толкын Шабденбековна – «Ақпараттық қауіпсіздік жүйелері» мамандығының докторанты, Әл-Фараби атындағы ҚазҰУ, Алматы, Қазақстан; аға оқытушы, Нархоз Университеті, Алматы қ., Қазақстан

Миркасимова Толкын Шабденбековна – докторант по специальности «Системы информационной безопасности», Казахский национальный университет имени аль-Фараби, г. Алматы, Казахстан; старший преподаватель, Университет Нархоз, г. Алматы, Казахстан

Mirkassimova Tolkyn Shabdenbekovna – doctoral student in Information Security Systems, Al-Farabi Kazakh National University, Almaty, Kazakhstan; Senior Lecturer, Narxoz University, Almaty, Kazakhstan.

e-mail: tolkyn.mirkasimova@narxoz.kz,
ORCID: https://orcid.org/0009-0003-1594-4012

Адилжанова Салтанат Альмуханбетовна – PhD, Әл-Фараби атындағы ҚазҰУ, Алматы қ., Қазақстан

Адилжанова Салтанат Альмуханбетовна – PhD, Казахский национальный университет имени аль-Фараби, г. Алматы, Казахстан

Adilzhanova Saltanat Almukhanbetovna – PhD, Al-Farabi Kazakh National University, Almaty, Kazakhstan

e-mail: asaltanat81@gmail.com,
ORCID: https://orcid.org/0000-0003-1768-064X