Қ. И. Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университеті

ӘӨЖ 004.056.5 Қолжазба құқығында

ЖУМАНГАЛИЕВА НАЗЫМ КЕНЖЕГАЛИЕВНА

Шабуылдарды табу жүйесіне арналған параметрлер күйінің ауытқымалығын бақылау технологиясы

6D070400 – Есептеу техникасы және бағдарламалық қамтамасыз ету

Философия докторы (PhD)
дәрежесін алу үшін дайындалған диссертация

Ғылыми кеңесшілері
техника ғылымдардың докторы,
профессор Ахметов Б.С.
Шетелдік ғылыми кеңесші:
техника ғылымдардың докторы,
профессор Корченко А.Г.

Қазақстан Республикасы
Алматы, 2017

МАЗМҰНЫ

НОРМАТИВТІК СІЛТЕМЕЛЕР

Бұл диссертациялық жұмыста келесі стандарттарға сәйкес сілтемелер берілген:

ҚР МЖМБС 5.04.034 – 2011 «Қазақстан Республикасының Мемлекеттік жалпыға міндетті білім беру стандарты. Жоғары оқу орнынан кейінгі білім. Докторантура ». Негізгі ережелер ҚР білім және ғылым министрімен бекітілген. «17» маусым 2011 ж. №261 ж. Астана 2011.

«Диссертацияларды және авторефераттарды рәсімдеу бойынша нұсқаулық», ҚР БҒМ, Жоғары аттестаттау комитеті, Алматы 2004

МЕСТ 7.32-2001.- Ғылыми зерттеу жұмыстары туралы есеп. Рәсімдеудің ережесі мен құрылымы. – Астана, 2001.

МЕСТ 7.1-2003. Библиографиялық жазба.

ҚРСТ 34.007-2002. Ақпараттық технология. Телекоммуникациялық желілер. Негізгі терминдер мен анықтамалар.

Қазақстан Республикасының 2004 жылдың 5-ші шілдедегі № 567-II «Байланыс туралы» Заңы.

АНЫҚТАМАЛАР

Бұл диссертациялық жұмыста келесі терминдерге сәйкес анықтамалар қолданылған:

Компьютерлік жүйелер - ақпараттық қауіпсіздік саласындағы ең маңызды ғылыми мәселелердің бірі ақпараттық қауіпсіздік саласындағы ең маңызды ғылыми мәселелердің бірі ресурстарына кибер шабуылдарды идентификациялауге байланысты бағыт болып табылады.

Катыстылық функция - ҚФ объект кез келген лингвистикалық анықтамаға сәйкес келу мүмкіндігі туралы түсінік береді.

Лингвистикалық термдердің статистикалық мәліметтерін қолдану (ЛТСМҚ) әдісі анық емес жиынтықпен сұралатын элементтерді бағалау жиілігі негізінде сипаттайды.

Деңгейлік жиындар әдісі(ДЖ) тиянақталған α-деңгейлерінде X жиындарының элементтерін таңдау мүмкіндігін қолданады.

Сандық әдіс (СӘ) қарастырылған әрбір кластың сандық мәнін анықтайтын сарапшылар тобының сұранысымен байланысты және барлық n сарапшылардың мәліметтері бойынша орташасы, яғни $\tilde{\mu_A}(x) = (\tilde{\mu_A}(x_1) + \ldots + \tilde{\mu_A}(x_n))/n$ анықталады.

Numbers of Virtual channels (*NVC*) – Виртуал арналар саны,

Virtual Channel Age(*VCA*) – Виртуал арнаның жасы,

Number of concurrent connections to the server(*NCC*) – Бір мезеттегі серверге қосылулар саны,

Speed of processing requests from the clients(*SPR*) – Клиенттердің сұранысын өңдеу,

The delay between requests from the single user(*DBR*) – Бір қолданушының сұраныстарының арасындағы кідіріс.

Number of packages with the same sender and receiver address(*NPSA*) – Бірдей мекен - жайы бар жөнелтуші мен алушының пакеттер саны.

-

БЕЛГІЛЕУЛЕР МЕН ҚЫСҚАРТУЛАР

АДА - α-Деңгейлі арақашықтық
МБВ - Базалық шама моделі
КД - Кіріс деректері
ШД - Шығыс деректері
АЖ - Ақпараттық жүйелер
КМ - Коэффициент маңыздылығы
КЖ - Компьютерлік жүйе
АЕА - Анық емес айнымалылар
СДЛТӘ - Статистикалық деректерді пайдаланылатын лингвистикалық терм әдісі
АЕАӘ - Анық емес арифметика әдісі
КАӘМ - Коэффициентті анықтау әдісінің маңыздылығы
ТСФӘ - Тиістілік салыстыру функциясының әдісі
ТҚФМ - Тиістілік функция қалыптастыру моделі
МЭВ - Эталонды шамалармоделі
АЕЖ - Анық емес жиыны
АЕС - Анық емес саны
АЕЭ - Анық емес эталоны
ОЖ - Операциялық жүйе
БҚ - Бағдарламмалық қамтамасыздандыру
АЖР - Ақпараттық жүйе ресурсы
ШТЖ - Шабуылдарды табу жүйесі
ШБЖ - Шабуылдарды болдырмау жүйесі
ОР - Орташа ранг
ЭШМ - Эталонды шама моделі
ТФ - Тиістілікфункциясы
ШЕ - Шешу ережесі
ЭТ - Эксперттік топ
ЭА - Эксперттік ақпарат
ЭБ - Эксперттік баға
MI - Матрица инициализациясы
DBR - The delay between requests from the single user
IDS - Intrusion detection system
IPS - Intrusion prevention system
NCC - Number of concurrent connections to the server
NPSA - Number of packages with the same sender and receiver address
NVC - Numbers of Virtual channels
SPR - Speed of processing requests from the clients
VCA - Virtual Channel Age

КІРІСПЕ

Зерттеудің өзектілігі. Ақпараттық технологиялардың қарқынды дамуы адамның, қоғамның, мемлекеттің және барлық салаларына жағымды әсер етуде. Сонымен қатар алғашқы кезекте ақпараттық жүйелердің (АЖ) ресурстарына зиянды әсер ететін жаңа кибершабуылдарды туындататын қатерлер компьютерлік жүйелер мен желілерге байланысты жағымсыз әсерлер де байқалады. Осыған байланысты айтылған қорғау жүйелері талдауға, болжауға, бақылауға мүмкіндік беретін қажеттілік туындатады. АЖ ресурстарының (АЖР) кең таралған қауіпсіздік шешімі ретінде ең алдымен компьютерлік желілер арқылы рұқсатсыз қолжеткізуді анықтау фактілеріне бағдарламалық немесе бағдарламалық–аппараттық құралдарға негізделген шабуылдарды табу жүйесі (ШТЖ) болып табылады. Шығарылған шешімдер шабуылдарды анықтаудың сигнатуралық (шаблонды) және ауытқымалы ұстанымдарына негізделген. Заманауи ауытқымалы ұстанымның ШТЖ негізінен статистикалық мәліметтерді алуға көп уақыт қажет ететін, оқыту үрдісін жүзеге асыруға (нейро желілік жүйелер үшін) және басқа күрделі және ұзақ дайындық барысын қажет ететін математикалық модельдерге негізделген. Бұл тұрғыда сарапшылардың пайымдарын қалыптастыруға негізделген және оларды компьютерлік желілер мен жүйелер шабуылдаушы әрекеттерді жүзеге асыру мүмкіндігі туралы шешім қабылдау барысында қолданылатын ұстанымдар нәтижелі болып табылады.

АЖР рұқсат етілмеген әрекеттер олардың қоршаған ортасына әсер етіп, белгілі аутықушылықтар тудыратыны белгілі. Ол әлсіз қалыптасқан, анық емес және осындай ортада ауытқушылық тудырған шабуылдарды анықтауға арналғандықтан арнайы модельдер, әдістер мен жүйелер қолданылуы керек. Желілік қарама-қарсылық жүйесінің нәтижелілігін жоғарылату және функционалды мүмкіндіктерін кеңейтуге анық емес жағдайда қызмет атқаруға бағытталған жаңа, сәйкес шешімдерді қолдану арқылы жеткізуге болады.

Анық емес әлсіз қалыптасқан ортада ақпаратты қалыптастыру және оның нәтижелі өңдеуін жүзеге асыру үшін негіздерін Л.Заде (А.Алексеев, А.Борисов, Д.Дюбуа, А.Кофман, В.Кузьмин, Ю.Минаев, С.Орловский, А.Орлов, Д.Поспелов, А.Прада, А.Ротштейн, Р.Ягерь, ақпаратқа қатысты –А.Корченко еңбектерінде дамытылды) қалады, ал аталған арнайы әдістер мен модельдерге негізделген қабылданған шешімдерді жүзеге асыру барысында (шабуылдаушы әрекеттерді анықтау бойынша) сәйкес құралдар қажет.

Осында сонымен қатар бірінші бөлімнің 1.1 бабының талдауын енгіземіз (Шабуылдарды анықтаудың заманауи әдістері мен құралдары).

Осы түрдегі тапсырмаларды шешу ұстанымдарының бірі [1-16] анық емес жиындарға негізделген, АЖР рұқсатсыз ену фактілерін анықтау мақсатында әлсіз құрылымдалған мәліметтерді өңдеуге бағытталған, мысалы компьютерлік желілер арқылы шабуылдарды анықтаудың сәйкес құралдары, әдістер мен жүйелерді қолдануға негізделеді.

Көрсетілген шабуылдарды анықтау тапсырмаларын шешу үшін қолданылатын біршама нәтижелі, жекелеген әзірлемелер белгілі, мысалы:

шабуылдарды анықтаудың анық емес ұстанымдары[1-2]; және ауытқушылықтарды детектрлеу [3]; сәйкес анық емес моделдер (менің еңбектерім) және әдістер [4]; шабуылдарды анықтау жүйесі[5-12]; анық емес ережелер жиыны [1;2;4;6;7;9-14]; лингвистикалық айнымалыларды [13;15]және анық емес эталондарды құру әдістері [13]; сонымен қатар басқа анық емес жағдайда қорғау міндеттерін шешуге [16]; қолданылатын әзірлемелер. Аталған зерттеулер анық емес жиындардың математикалық аппаратын сәйкес қолданудың нәтижелілігін көрсетті, ал оны кибершабуылдарды анықтаудың ұстанымын қалыптастыруға қолдану шабуылдарды анықтаудың сәйкес жүйелерін құру үрдісін жетілдіруге мүмкіндік береді. Аталған және басқа дерек көздерінде кибершабуылдардың сәйкес класының әсерінен туындаған ауытқушылық жағдайын анықтауға болатын, берілген уақыт аралығында анық емес жағдайда қоршаған ортаның шамаларын бақылау үшін қолданылатын қажет компоненттер жиынын қалыптастыруға қажет ұстаным қалыптаспағанын есепке алған жөн.

Ғылыми зерттеу тақырыбының өзектілігі желілік сигнатуралық емес кибершабуылдар туындайтын анық емес жағдайда ауытқуды анықтау жүйесінің және технология, әдіс, моделі негізінде қазіргі заманғы шабуылдарды табу жүйесінің (ШТЖ) мүмкіндіктерін кеңейтетін құралдарды өңдеу қажеттілігімен анықталады.

Диссертациялық жұмыстың мақсаты. Компьютерлік желілерде сигнатуралық емес кибершабуылдар түрін анықтау жүйесінің мүмкіндіктерін арттыру үшін, ауытқу күйін идентификациялау үшін модельлер мен құралдарды әзірлеу болып табылады.

Зерттеудің негізгі міндеттері:

1. Компьютерлік желілердегі шабуылдарды анықтау үшін қолданылатын теориялық және тәжірибелік базалардың қазіргі заманғы даму жағдайын зерттеу;
2. Компьютерлік желілердегі кибершабуылдардың белгілі бір, қоршаған ортадағы ауытқу жағдайын өлшемін көрсететін және базалық шамалар моделі мен эталонды шамалар моделін құрастыру;
3. Базалық шамалар моделі мен эталонды шамалар моделінің негізінде қалыптастыру үшін ауытқу жағдайын анықтауға арналған шешуші ережелер моделін құру;
4. Базалық шамалар моделі, эталонды шамалар моделі және шешуші ережелер модельдерінің негізінде тіркелмеген әрекеттерді тудырған ауытқу жағдайын анықтау технологиясын әзірлеу;
5. Ауытқу жағдайын анықтау технологиясы негізінде сигнатуралық емес кибершабуылдарға бағытталған шабуыл жүйесінің функционалдық мүмкіндіктерін кеңейту үшін құрылымдық шешім шығару;
6. Компьютерлік желілердегі шабуылдаушы әрекеттерді анықтауға мүмкіндік беретін жаңа техникалық шешімдерді әзірлеу және эксперименталды зерттеу жүргізу.

Зерттеу нысаны және мәні. Зерттеу нысаны - компьютерлік желілерде шабуыл әрекеттерімен жинақталатын ауытқымалы жай-күйін анықтау үрдісі.

Зерттеу пәні - модельдер, әдістері, тәсілдері және компьютерлік желілерді шабуыл жүйесінің әрекеттері мен жинақталатын ортада анық емес аутқымалыны табу жүйесі.

Диссертациялық жұмыстың ғылыми жаңалығы. Диссертациялық зерттеуді орындау аясында төмендегідей ғылыми зерттеулер алынды:

1. Белгілі бір желілік шабуылдардың жиынтығына тән, анық емес айнымалы эталондарын құру процесін қалыптастыруға мүмкіндік береді және қоршаған ортадағы ауытқу жағдайын өлшемін көрсету «шабуыл: түйіндес жұп жиынтығы» және «шабуыл: шамалар» жұп жиынтығының негізінде енгізілген шамалардың есебінен, базалық шамалардың моделі және эталонды шамалардың моделі ұсынылды; ары қарай дамытылды;

2. Компьютерлік желілердегі ауытқу жағдайын сарапшылық жолмен анықтауға арналған шешуші ережелер жиынын қалыптастыру мүмкіндігін береді, эталонды шамалар жиынының есебінен түйіндес жұп пен анық емес идентификациялау матрицасын сарапшылық бағалаудың әдістерімен қалыптасқан шешуші ережелер моделі ары қарай дамытылды;

3. Тұңғыш рет шабуылдарды анықтау жүйесі үшін кез келген Лингвистикалық эталондарды жалпы түрде құруға арналған ұстаным құрастырылды.

Әдіс базалық шамалар моделі мен эталонды шамалар моделіне негізделген:

Әдісте қолданылады:

- лингвистикалық бағалардың идентификация жиыны;
- аралықтар идентификация жиыны;
- шамалардың ағымдағы күйін шабуылдарға қатысты сипаттайтын
- сарапшы пайымдарын бейнелейтін базалық жиілік матрицасы;
- шамалардың ағымдағы күйін шабуылдарға қатысты сипаттайтын-
- сарапшы пайымдарын бейнелейтін туынды жиілік матрицасы;
- сарапшы бағаларының берілген аралықтарда кездесу жиілігін
- қалыптастыру үрдісі;
- анық емес термдердің ішкі жиындарының берілген аралықтарда
- кездесу жиілігін
- қалыптастыру үрдісі;

Лингвистикалық эталондар нақты гетерогенді параметрлі қоршаған ортада ауытқушылықтың түрлі жағдайын сипаттайды;

4.Базалық шамалар, эталонды шамалар және шешуші ережелер моделі негізінде тіркелмеген әрекеттері табу, сарапшылық ұстаным негізінде және қалыптасқан анық емес ағымдағы шамалар арқылы кибершабуылдардың сигнатуралық емес түрлерін идентификациялау құралдарын құруға мүмкіндік беретін ауытқу жағдайларды анықтау технологиясы құрылды;

5. Анық емес арифметика модулі және ішкі жүйелердің есебінен ауытқушылық жағдайын анықтау технологиясының көмегімен жүзеге асырылған шабуылдарды анықтау жүйесінің құрылымдық шешімі; желілік шамалардың анық емес эталондарын қалыптастыру; шешуші ережелерді және алғашқы өңдеуді қалыптастыру қоршаған ортадағы белсенділікті

бақылау шабуылдарды анықтаудың қазіргі заманғы жүйесінің функционалды мүмкіндіктері ары қарай дамытылды**.**

Зерттеу әдістері анық емес теориясы, жиынтықтар, шешім қабылдау алгоритмдерін, модельдеу, ақпараттық процестер мен құрылымдардың модельдеу, сондай-ақ сараптама және есептеу әдістеріне негізделген.

Кіріспеде зерттеудің өзектелігі, зерттеу мәселесіне байланысты проблемалар нақтыланды. Жұмыстың идеялары, зерттеудің мақсаттары мен міндеттері, жұмыстың ғылыми жаңалықтары мен практикалық бағалығы келтірілген.

Бірінші бөлімде. Әдістер және шабуылдарды жүзеге асыру құралдарына сараптама жасалды, олар біршама кең спектрді құрайтыны, үздіксіз жетілдірілетіні компьютерлік жүйелер мен желілердегі тіркелмеген әрекеттерді жүзеге асыруда қолданылады. Нейрожелілік ұстанымдар статистикалық әдісінің қолданылатын бағытты негізінен ШТЖ кең таралған. Статистикалық мәліметтердің жеткіліксіз іріктемесіне, қоршаған ортадағы күтпеген өзгерістерге, жүйені оқытудағы қателіктерге, белгісіз шабуылдарға (мысалы «0-day» және белгілі шабуылдардың түрленуі анықтауда белгілі қиындықтарға әкеледі) біршама сезімтал болып келеді.

Екінші бөлімде ШТЖ ауытқу жағдайын анықтау моделдерін жасауға арналған. “шабуыл : шамалар” және “ шабуыл**:** түйіндес жұптар жиыны ”жұптар жиынын ескере отырып, базалық шамалар модельдері мен эталонды шамалар модельдері негізінде кибершабуылдардың нақты түрі туындатқан ауытқушылық жағдайын көрсетуге мүмкіндік беретін шешуші ережелер моделі ұсынылды.

ШЕМ құру үшін анық емес идентификаторлар жиыны еңгізілді (fuzzyidentifiers).

Үшінші бөлімде желілік шабуылдардан пайда болатын ауытқушылықты анықтаудың технологиясын әзірлеуге және ауытқуды табу жүйелеріне арналған жаңа құрылымдық шешімдерге арналған. Ұсынылған технология екінші тарауда әзірленген математикалық модельдер, анық емес логиканың әдістеріне және бірінші бөлімде талданды, түйіндемелерге негізделген. Онда сегіз негізгі кезеңдер бар, ол кибершабуылдың нақты түрімен туындаған ауытқулар жағдайын анықтау үдерісін анықтайды.

Төртінші бөлім компьютерлік желілердегі ауытқушылықтарды анықтау құралдарын зерттеу мен тәжірибелік жүзеге асыруларға арналған. Порттардды сканерлеу туындатқан, ұсынылған ауытқушылықтарды алгоритмдік қамсыздандыру және типтік жүйе негізінде сканерлеуші құралдарды анықтаудың бағдарламалық жүйесіне және шабуылдаушы әрекеттер туындатқан ауытқушылықтарды анықтаудың қолданбалы жүйесіне тәжірибелік зерттеу жүргізілді**.** Сонымен бірге ұсынылған әдісті жүзеге асыратын жүйенің негізігі жұмысы көрсетілген, түрлі кибершабуылдардың үшін алынған түрлі ауытқушылық жағдайлардың графикалық түсіндірмесі берілген,ал негізгі эксперимент Ұлттық авиациялық университеттің ақпараттық технологиялар қауіпсіздігі

кафедрасының жұмыс бекеттеріне 1500 шабуылдарды модельдеу жолымен жасалды.

Осымен бірге шабуылдарды анықтау 29,3 % жағдайда SR_{15} = “Егер $\underset{\sim}{t}_{VCA}$ $\underset{\sim}{T}^{e}_{VCA}$ енетін $\underset{\sim}{Y}^{e}$ неғұрлым жақын болса және $\underset{\sim}{t}_{NVC}$ $\underset{\sim}{T}^{e}_{NVC}$ енетін $\underset{\sim}{VB}^{e}$ неғұрлым жақын болса, онда *SN* тудырған ауытқушылық жағдайының деңгейі LIM болады”ережесін ал 38,7 % және 32 % сәйкесінше SR_{14} және SR_{13} ережелерін бастамашылыққа алатынын атап өткен жөн.

Жүргізілген верификация нәтижелерінен барлық шабуылдарсарапшының түрлі сенім дәрежесін көрсететін түрлі ережелер арқылы анықталғаны көрінеді. Осыған сәйкес ұсынылған моделдер мен жүйелерді жүзеге асыру үлгіленетін әрекеттерге реакция бейнелейтіні туралы қорытынды жасауға болады.

Қорытындыда диссертациялық жұмыстың негізгі нәтижелері және қорытындылары көрсетілген.

Жұмыстың тәжірибелік маңыздылығы.

Диссертациялық жұмыста алынған нәтижелер ауытқушылықтарды анықтау үшін программалық-аппаратты модульдер немесе программалық модульдер түрінде техникалық шешімдер құрғанда және автономды немесе қазіргі заманғы ШТЖ функционалдығын кеңейткіш ретінде қолданылуы мүмкін. Тәжірибелік маңыздылығы келесіде:

құрылған модельдер және технология негізінде 1701 «Ақпараттық қауіпсіздік» саласында мамандарын дайындайтын оқу барысында қолданылатын лабораториялық жұмыс және дәрістік материал құрылды. Диссертациялық зерттеудің тәжірибелік қолданылуы Ұлттық авиациялық университет (Киев, Украина) оқу процесіне еңгізу актімен (17.02.2017ж) расталады.

ауытқу күйді анықтау ұсынылған технологиясы негізінде анық емес нақты қалыптасқан ортада ақпараттық жүйелер ресурстарына кибершабуылдарды анықтауға мүмкіндік беретін «Анық емес логика негізінде порттарды сканерлеуді анықтау» компьютерлік программасы құрылды, ол ақпараттық жүйе қорғалу дәрежесін жақсарту және қорғау желілік жүйесінің жұмыс тиімділігін оңтайландыруға мүмкіндік берді, ол «Сайфер БІС» ЖАҚ жұмысына енгізу актімен расталады (03.02.2017).

Зерттеу нәтижелерінің аппробациясы

Зертеудің негізгі нәтижелері төмендегі конференцияларда баяндалды:

Ақпараттық және телекоммуникациялық технологиялар: білім, ғылым, тәжірибе» атты II Халықаралық ғылыми-тәжірибелік конференция еңбектер. Қ.И Сатпаев атындағы ҚАЗҰТУ Алматы. Шабуылдарды табу жүйесіне арналған бағалау сараптамасының әдісін талдау

«Қазіргі ақпараттық және телекоммуникациялық технологиялар»: Халықаралық ғылыми-тәжірибелік конференция Украина, Киев 2015 ж Шабуылдарды табу жүйелерін құру үшін анық емес жинақтар әдістерін талдау.

Басқару және автоматтандыру жүйелер бойынша 16-шы халықаралық конференция / ICCAS.2016 Gyeongju, Оңтүстік Корея, 2016 Шаблонды және өлшеу шабуылдары мен ақпарат құнының критериясы бойынша желілік модельді бағалау.

«Ақпараттық және телекоммуникациялық жүйелердің қауіпсіздігі мен жағдайы» (SITS-2016). //-Николаев-Коблева: Халықаралық технологиялық университеті Кибер қауіпсіздік ақпараттық-психологиялық аспектілері

ITSEC - VI Халықаралық ғылыми-техникалық конференциясы 2016. Украина, Киев Ұлттық авиациялық университеті. Ақпараттық ресурстардағы шабуылдардың параметрлерін анықтау үшін ақпараттық-аналитикалық жүйе

Киберқауіпсіздікті және ақпаратты қорғауды қамтамасыз етудің өзекті мәселелері: II Халықаралық ғылыми- тәжірибелік конференция (Украина, Киев 2016) Кибершабуылды анықтау жүйелеріне арналған шартты анықтау анықтамаларын құру әдістемесі

Киберқауіпсіздіктің өзекті мәселелері және ақпараттық қауіпсіздік: III Халықаралық ғылыми-тәжірибелік конференция:(Украина, Киев Еуропалық университет, 2017 ж) Сниффинг шабуылдарды анықтау үшін Лингвистикалық стандарттарды құру

Басылымдар. Берілген ғылыми зерттеу 23 жұмыс жарияланған, оның 8 -ҚР БҒМ - Білім және ғылым саласындағы бақылау комитеті ұсынған басылымдарда жариаланған, 4 мақала Scopus мәліметтер қорына кіретін баылымдар жарияланған, 4 мақала ғылыми журналдарда және ғылыми еңбектер жинақтарында жарияланды: халықаралық конференциялар жинағында (Украина) 5 мақала, халықаралық конференцияның материалдарында 2 мақала жарияланды (Қазақстан).

Диссертация құрылымы мен көлемі. Диссертация кіріспеден, төрт бөлімнен, жалпы қортындылардан, қосымшалардан, қолданылған әдебиеттер тізімнен тұрады және негізгі мәтін 146 парақты, 41 сурет, 23 кесте, әдебиеттер тізімі 124 атаудан тұрады. Жұмыстың жалпы беттер саны 175 бет.

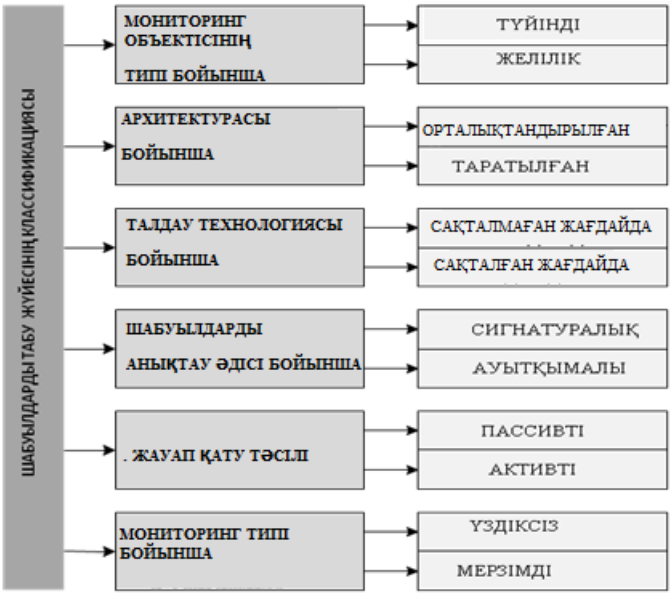
1 ШАБУЫЛДАРДЫҢ ІС- ӘРЕКЕТТІНЕН ТУЫНДАЙТЫН АУЫТҚУЛАРДЫ АНЫҚТАУҒА АРНАЛҒАН ЗАМАНАУИ КӨЗ-ҚАРАС

1.1 Шабуылдарды табудың қазіргі заманғы әдістері мен құралдарын анықтау

Қоғамның барлық салаларындағы заманауи компьютерлік технологияларды қолдану үлкен деректер көлемін автоматтандырылған түрде өңдеуге мүмкіндік берді. Қоғамның жаппай автоматтандыру пайдаланушылардың кең ауқымына ақпаратпен жұмыс істеуіне мүмкіндік берді. Сонымен қатар, ол түрлі ақпараттық ресурстарға рұқсатсыз қол жеткізу мүмкіндігін көбейтті. Бұл жаңа кибершабуылдар туындататын ақпараттық жүйелер ресурстарына енетін қауіп-қатердің жаңа түрлерінің пайда болуына байланысты теріс әсер етеді.

Сондықтан, қазіргі ақпараттық қауіпсіздік саласындағы ең маңызды ғылыми мәселелердің бірі компьютерлік жүйелердің (КЖ) ресурстарына кибер шабуылдарды идентификациялауға байланысты бағыт болып табылады.

Әлемдік тәжірибеде КЖ және желілерді кибершабуылдардан қорғау үшін ШТЖ (шабуылдардан табу жүйесі) және ШБЖ (шабуылдарды болдырмау жүйесі) жиі қолданылады. Тұңғыш ШТЖ тұжырымдамасы түрлі бұзушылықтарды талдаудың жүйелік журналында қарастырылған жұмыста [17] ұсынылды. Сонымен қатар [18] жұмыста жүйенің қалыпты белсенділігінің профилі, мәліметтердің статистикалық сараптамасы және т.б. аспектілерге ерекше назар аударылған сараптамалық ШТЖ сипатталды. Қазіргі заманғы ШТЖ міндеттері негізінен шынайы уақыт режиміндегі ақпарат ағынын өңдеуге, бейімділікті қамтамасыз етуге, сонымен қатар ШБЖ кейбір қызметтерін орындауға, яғни анықталған шабуылға сәйкес жедел жауап әрекеттерін жүзеге асыруға бағытталған [19]. Бұл жүйелер әдетте екі құрамдас бөліктен: бағдарламалық немесе бағдарламалық-аппараттық қамтамасыздандыру түрінде жүзеге асырылған және бастапқы деректерді жинауға бағытталған түрлі датчик, детектор, сенсорлар сияқты бақылау модульдері; бақылау модульдерін конфигурациялау және жиналған ақпаратты өңдеуге жауапты консоль, менеджерлер түріндегі басқарушы модульдерден тұрады. Сонымен қатар оның құрылымына құрамы ШТЖ түріне байланысты көмекші құрамдас бөліктер (мысалы, жүйе жұмысымен байланысты мәліметтерді сақтауға арналған қорды басқару жүйесі) енуі мүмкін [20].Олардың негізгі қасиеттеріне басымдық беру үшін төмендегі негізгі белгілерін жалпыланған негізде қолайлы көрінетін топтастыруды жүзеге асырамыз[19, 21-24].



Сурет 1.1- ШТЖ жалпыланған топтастырылуы

1. Мониторинг объектісінің типі бойынша (ақпарат жиыны): түйінді,желілік. Түйінді ШТЖ желідегі белгілі бір торапқа бақылау жүргізеді. Олар операциялық жүйеге тәуелді және [25] сәйкес олар тым болмаса келесі функциялардың біреуін орындауы тиіс: файл жүйесін бақылау(файлдар мен директорийлер тұтастығын тексеру); оқиғалар журналының сараптамасы (оқиғалар журналынан күдікті шаблондарды іздеу); желілік бірігулерді бақылау(қауіпсіздік саясаты бұзылыстарына бастапқы және шығыс желілік бірігулеріне сараптама); операциялық жүйенің түйіні негізінде сараптама (кез келген операцияны бұғаттауға мүмкіндік беретін айрықша артықшылықтары бар жүйені бақылау). Желілік ШТЖ белгілі желілік сегментті бақылауды жүзеге асырады және оған бағытталған шабуылдарды детектрлеуге арналған. Ақпараттың қайнар көзі желі трафигі, желілік пакеттің тақырыпаты мен мазмұны болып табылады. Бұл жүйелер әдетте таратылған болып табылады және келесі құрамдас бөліктерден тұрады [18]: сенсор (мәліметтерді жинау және оларды алғашқы сараптамадан өткізу қызметін атқарады); басқарушы топтама(сенсорлардан мәліметтерді жинау, олардың қайталама сараптамасы мен өзара байланыстылығына жауапты); мәліметтер қоры(әдетте жеке сервер түрінде орындалған және оқиғалар туралы ақпараттың сақтау орны болып табылады); консоль(жүйені басқарудың интерфейсі**)**.

2. Архитектурасы бойынша – орталықтандырылған, таратылған; орталықтандырылған ШТЖ бір жұмыс бекетінде жүргізілетін есептеулерге, ал таратылған ШТЖ желі бойынша таратылған сенсорлар, есептеулер орталығы және басқарушы консолі сияқты элементтер қатарын қарастырады [19].

3.Талдау технологиясы бойынша – сақталмаған жадайда, сақталған жағдайдың сақталуымен, жағдайдың сақталуынсыз. Алғашқысы әрбір оқиға

өзгелерден тәуелсіз қарастырылады, ал екіншісінде өткен оқиғалар туралы ақпарат сақталады және шешім қабылдағанда ескеріледі. [19].

4.Шабуылдарды анықтау әдісі бойынша – сигнатуралық, ауытқымалы; сигнатуралық (белгілік), ауытқымалы. Бұл ШТЖ бар белгілер бойынша желілік трафиктегі белгілі шабуылдардың дайын модельдерін немесе жоғары деңгейдегі мәліметтерді іздеу жүзеге асырылады және бүгінгі күнге олар ең кеңінен таралған болып табылады[26]. Белгілер (сигнатуралар) әдетте бір пакетті, кестелерді сараптау негізінде қызмет атқаратын және сегменттерді жинақтауды талап ететін түрлерге бөлінеді[20].Белгілік тәсілдеме шабуылдарды сипаттаудың дайын моделіне және оны бақылауға алынған кеңістіктен(мысалы желілік трафикте, хаттамаларда, тіркеу журналында т.б.) іздеуге негізделеді. Бұл технология мейлінше қарапайым, бірақ белгілерді сипаттау механизмін құру және шабуылдарды барлық мүмкін өзгерістерін айқындау мәселесі туындайды. Егер бірінші мәселе кейбір өнімдерде шешілсе (мысалы Advanced Packets Exchange), ал екіншісін тәжірибелік тұрғыдан іске асыру өте қиын [27]. Екінші типті жүйелер ауытқушылықты анықтауға бағытталған. Олар жүйенің қалыпты(қалыпты емес) пішінін құрайды және одан ауытқушылықты детектрлейді [27]. Бұл ШТЖ жүйенің ауытқушылық жағдайы қалыпты тәртіптен ауытқу ретінде қарастырылатын болжамға негізделеді. Бұл жағдайға мысал ретінде қысқа уақыт аралығындағы желілік қосындылардың көп мөлшері, орталық процессіордың жоғары жүктемесі немесе қолданушы іске қоспаған жабдықтың қолданылуы т.б. Кейде ауытқымалы жағдай үнемі шабуыл болмайды, мысалы, жүйелік әкімшінің бекеттердің белсенділігі туралы монополиялық сұранысы [28] dos –шабуыл ретінде қабылдануы мүмкін. Осыларды ескере келе шабуыл болып табылмайтын ауытқушылық жағдайды анықтау және топтастыру; ауытқушылық жағдай кейпіне жатпайтын шабуылдарды өткізіп жіберуі мүмкін. Қорғалатын объектілер үшін екінші жағдай біріншіге қарағанда қауіпті болуы мүмкіндігін ерекше атаған жөн. Ауытқушылық жағдайды анықтау үшін мәліметтер жиынтығын анық белгілеріне қарай бөлуді(ол үшін түрлі метрикалар, мысалы Евклид, Хэмминг т.б. [19, 29]; тораптық ШТЖ қолданушылардың жүйелі әрекеттерін модельлеуге арналған тораптық ШТЖ қолданылатын Марк модельдерін, мысалы, желілік пакеттердегі өріс жүйелілігі[30]; мәліметтерді сараптап түрлендіруге арналған Вейвлет сараптамасы [31]; білдіретін кластерлеу алгоритмі сияқты ұстанымға негізделген математикалық статистикалық аппараты жиі қолданылады. Сонымен қатар нейрондық желілер, мысалы, көпқабатты персептронда [32], мәліметтерді ұсыну форматы ретінде жұмыстардың көпшілігінде[33] сипатталған әдіс қолданылады; иммунитетті жауаптың бір аспектісін қолданатын қарапайым аспектілерге [35, 36] негізделген, сонымен қатар адамзаттық иммунитеттің күрделі, бірнеше механизмдеріне [37, 38] еліктейтін жасанды иммунды жүйелер қолданылады. Сонымен қатар иммунокомпьютинг – протеиндердің өзара әрекеттестігін модельлеуге негізделген машиналық оқытудың тұжырымдамасы қолданылады. Қалыптасқан иммунды желі негізгі модель

болып табылады. Бұл ұстанымды желілік және арнайы шабуылдарды, мысалы web-серверге бағытталған шабуылдар анықтау үшін қолдануға тырысады [40]. Ауытқушылығы бар ШТЖ кемшіліктеріне жалған іске қосылудың жоғары деңгейі (кез келген, тіпті қауіпті емес қалыпты белсенділіктен ауытқу жүйенің реакциясын тудырады); жаттықтырушы іріктеме құру қиындығы; есептеуіш ортаның ерекшелігіне тәуелді жаттықтырушы іріктемеге арналған оқыту стратегиясы мен мәліметтер сипаты енгізу мен баптау қиындығы болып табылады. Қазіргі заманғы ауытқушылығы бар ШТЖ елеулі кемшілігіне жүйенің қалыпты жағдайының сәйкес кейпін құру үрдісінің ұзақтығымен байланысты. Ал қайта конфигурациялау, түрлендіру және т.б. өзгерістерде алынған статистика өзекті емес немесе толық емес болып қалады. Жүйе туралы барлық статистика зерттелген, бірақ қажеттілігі жоқ күйде болған кезде ғана тіршілігін тоқтататынын ерекше атаған жөн [26].

5. Жауап қату тәсілі – пассивті, активті; [19]. пассивті, ШТЖ белгілер арқылы өзгертеді және оқиғалар журналына жазба енгізіледі. [41]. активті ШТЖ шабуыл анықталғаннан кейінгі белгілі тәртіппен, яғни ықтимал тәртіп бұзушыларға серверлердің қолжетімділігін жоя отырып, мысалы, қосылыстардың жойылуына, IP мекен-жай т.б. бұғатталуы, түзетуші (мысалы сақтандыруды жою) немесе белсенді іс-әрекеттер қолдануы мүмкін [41].

6. Мониторинг типі бойынша - үздіксіз, мерзімді: [18]. Үздіксіз ШТЖ бақыланатын жүйенің тұрақты бақылауын жүзеге асырады [41] және шабуылдарды жүзеге асыру барысында анықтауға, яғни шынайы (немесе шынайыға жақын уақытта) уақыт режимінде мүмкіндік береді [26]. Мерзімді ШТЖ жүзеге асырылған шабуылдарды анықтау мақсатында сараптама жүргізу [41] үшін уақытша қосылуымен сипатталады. Оларды тұтастылықты бақылау жүйесі мен тіркеу журналының талдауының жүйесіне ажыратуға болады [26].

Неғұрлым белгілі ШТЖ - ге Snort, Ossec, Bro, Proventia Network ADS, RealSecure, Open Source Tripwire, AirSnare, Prelude Hybrid IDS, AAFID, ASAX, NetSTAT, Prelude, SHADOW, lynis – Security and system auditing tool т.б. жатады. Snort жүйесі бұл ШТЖ және ШБЖ ережелерді сипаттау тілін қолданатын ашық бастапқы коды бар бірлестік болып табылады. Бүгінгі күнде пакеттерді тіркеп және шынайы мерзімде IP желілерінде трафикті сараптауды жүзеге асыруға қабілетті, кеңінен қолданылатын технология болып табылады. Ол протоколдау, талдау, ішіндегісі бойынша іздеу, сонымен қатар белсенді емес бірқатар шабуылдарды және бұрғылауды анықтауға арналған немесе бұғаттау кеңінен қолданылады. Snort тәжірибелік түрде ШТЖ түрлі кластарын құруға арналған аспаптық құрал болып табылады[42]. Сонымен қатар Ossec жүйесі ашық бастапқы коды бар аспаптық коды бар құрал болып табылады және журналдарды талдау, файлдар тұтастығын тексеру, руткиттерді шынайы уақыт режимінде табу т.б. бағытталған [43]. Bro желілік жүйесі келген деректерді талдайды және қосымшалар негізінде мағынаны таңдайды, жүйеге зияны тиетін модельлердің белсенділігін салыстыратын оқиғаға бағытталған

анализаторларда орындалады. Bro датчиктер іске қосылғанда, жаңа шабуылдар анықталғанда немесе көп көлемдегі мәліметтерді сканерлеу үшін жоғары жылдамдықтағы қосылуға бағытталған жағдайда басшылыққа алынатын саясатты жазуға арналған өз тілін қолданады. Алғашында шабуылдардың және тәжірибелі мамандар үшін зерттеу платформасы ретінде құрылған болатын[44]. Proventia Network ADS қалыпты трафик бейнесін қалыптастыруға және оның келесі ауытқушылығын бақылауға негізделген. Желілік инфрақұрылым мәліметтер ағынының жиыны мен белсенді ШТЖ желіде орын алатын оқиғалардың жалпы бейнесін алу және күдікті белсенділікті анықтау міндетін шешеді[45]. RealSecure желілік белгілік (сигнатуралық) ШТЖ шынайы мерзімде корпоративтік желі тораптарына және Web – сервер қосымшаларына, мәліметтер қорына, бағытталған жұмыс бекеттеріне, бағдарлауыштар, желі аралық экрандар және т.б. шабуылдарды анықтауға мүмкіндік беретін шабуылдарға әсер ету және автоматты анықтауын қамтамасыз етеді. RealSecure желілік пакеттер және тіркеу журналдарының сараптамасының технологиясын қолданады және желінің толық сегментін (network-based), сонымен бірге корпоративті желінің нақты торабын (host-based) қорғауға бағытталған[46]. Open Source Tripwire тораптық ШТЖ жүйе ішінде файлдарды бақылау және өзгерістерді сараптауды жүзеге асырады. Ол құрылған кезде файл жүйесін сканерлейді және мәліметтер қорында табылған барлық файлдар туралы ақпаратты өзгерістерді бақылау үшін сақтайды. Жүйе шабуылдарды анықтаудан басқа тұтастылықты қамтамасыз ету, өзгерістер мен қауіпсіздік саясатына сәйкестілікті басқару үшін қолданылады[47]. AirSnare жүйесі сымсыз желілер үшін және негізінен өз жергілікті желісінің трафигін бақылауға және барлық бірлестіктерді қарауға бағытталған [48]. Prelude Hybrid IDS жүйесі транзитті желілік трафиктің талдауышы ретінде қызмет атқарады, сервАС жұмысын, қолданушылардың белсенділігін, лог жағдайын сараптайды және соңғы хостағы неғұрлым маңызды файлдардың тұтастылығын бақылайды[49]. AAFID және ASAX сигнатуралық жүйелері тек қосымшалардың және операциялық жүйенің тіркеу журналдарымен жұмыс істейді[50]. AAFID құрамында алдын-ала бағдарламаланған шабуыл сипаттамаларын ашық түрде қолданатын агенттер жинағы бар. Агенттер анықтауға арналған шабуылдардың белгілері қатаң анықталған бағдарламалық модульдер болып табылады. Белгілі шабуылдар сипаттамасының қорын ұйымдастыру қиын кеңейтілетін болып табылады. ASAX жүйесі сценарийлер мен тіркеу журналында құрылымына тәуелсіз мәліметтер форматын сипаттау тілі қолданылады. Ол мәліметтердің жаңа қайнар көзін шабуылдар сценарийі мен сәйкес конвертер қосылған кезде қолдану мүмкін. NetSTAT жүйесі шабуылданушы ресурстың бірізділік жағдайында шабуылдар сценарийінің сипаттамасы тілін қолданады. Осылайша, бұл жүйе формальды әдістерге жақын анықтау әдісін қолданады. SHADOW жүйесі Perl тіліндегі фильтрлер жиынын, шабуылдарды сипаттайтын желілік пакеттердің нақты белгілеріне қатысты ШТЖ құрастырушыларының білімін пайдаланатын сенсорлар мен

талдауыштар қолданады. AAFID сияқты ол да қиын конфигурациясының про файлын құру шабуылды куәландыруы мүмкін ауытқушылықтарды анықтау үшін қолданылады[51].

Барлық қарастырылған жүйені жасаушылар жүйелер құрылған математикалық аппарат туралы айтпайды, сонымен қатар олардың негізгі бөлігі сигнатуралық анықтау технологияларына бағытталған, ал ауытқушылығы бар ШТЖ әдетте өзімен бірге белгілі кемшіліктерге ыңғайы бар статистикалық ұстанымдарға негізделеді. Бұдан бөлек ауытқушылық түрін анықтайтын құралдар ауытқушылық бейнеге қарағанда неғұрлым жоғары жағдайлар санын есепке алу қажеттігін тудыратын жүйедегі қалыпты белсенділіктің бейнесін құруға бағытталған. Бұл жүйені баптаудағы елеулі қиындықтарға әкеледі, ол әсіресе, қоршаған ортаны қамтитын параметрлер анық емес және әлсіз қалыптасқан болған жағдайда анық сезіледі.

1.2 Шабуылдарды табу жүйесін құруға арналған анық емес жиындардың әдістері

Белгілі қатыстылық функциясын (ҚФ) қалыптастыру әдістерін анық емес ортада ауытқушылық жағдайларын анықтау үрдісінде бастапқы деректерді өңдеу міндетін шешу мүмкіндіктерін анықтау үшін қарастырайық. Параметрлерді түзеу әдісі (ПТ) [52, 53] сарапшы неғұрлым сәйкес келетін графикті таңдап, оның параметрлерін анықтап және қажеттілік туындаса түзететін ҚФ стандартты графиктер қорына бағытталған. Осындай қорға, мысалы, келесі функциялар енуі мүмкін [53]: $\mu_1(x,a,b) = 0$ осындағы $x \le a$, $\mu_1(x,a,b) = 2(x-a)^2/(b-a)^2$, осындағы $a < x \le (a+b)/2$, $\mu_1(x,a,b) = 1 - 2(b-x)^2/(b-a)^2$, осындағы $(a+b)/2 < x < b$, $\mu_1(x,a,b) = 1$ осындағы $x \ge b$, $\mu_2(x,a,b) = exp(-(x-a)^2/2b^2)$.Келген деректер(КД) әдісі түрлі түрлі коэффициенттерді немесе ҚФ әсер ететін параметрлерді қолданады. Сандық жұптық салыстыру (СЖС) әдісінде [54-56] $\underset{\sim}{A} = \{\mu_{\underset{\sim}{A}}(x_1)/x_1, \ldots, \mu_{\underset{\sim}{A}}(x_n)/x_n\}$, түріндегі анық емес ішкі жиынтық қолданылады, осындағы $\mu_{\underset{\sim}{A}}(x_1) + \ldots + \mu_{\underset{\sim}{A}}(x_n) = 1$.Жиынтық элементтеріне қатыстылық дәрежесі жұптық салыстырулар негізінде анықталады, ал сарапшыға сұраныс мөлшері $n(n-1)/2$ құрайды және оның пайымдамасы бойынша жұптық салыстырулар қалыптамасы қалыптасады $A = \|a_{ij}\|$, осындағы a_{ij} 1.1.кестесі бойыншатаңдалады. КД әдісінде пайымдау қалыптамасын құру үшін 1.1. кестесінен таңдаймыз. Көріп тұрғанымыздай бұл әдіс еңбекті көп қажетсінеді, әсіресе салыстыратын шамалардың саны көбейгенде меншікті шаманы табу процессі күрделенеді.

Кесте 1.1 - Пайымдау матрицасын құру шкаласы

Маңыздылық бағасы	Сапалық бағасы
1; 3	Бірдей мәнділік; әлсіз артықшылық
5	мықты (немесе маңызды) артықщылық
7; 9	анықартықшылық; абсолюттік артықшылық
2, 4, 6, 8	аралық мағына

Шаршы түбірі анықталған сандық жұптық салыстыру (ШТАСЖС) әдісінде [57] ҚФ (салмақтық коэффициентін) $\mu_{\tilde{A}}(x_i)=\omega_i=\sqrt[n]{a_{i1}\ldots a_{in}}$, арақатынасы бойынша анықтайды, осындағы барлық a_{ij}КД болып табылады және жұптық салыстырулар матрицасы коэффициентін білдіреді.Жеке салыстыруды табатын сандық жұптық салыстыру (ЖСТСЖС) әдісі [58] жұптық салыстырулар матрицасына негізделеді, ал $\mu_{\tilde{A}}(x_1)$, ..., $\mu_{\tilde{A}}(x_n)$ x_1, ..., x_nнүктелерінде $\mu_{\tilde{A}}(x_i)=a_{ij}/(a_{1j}+\ldots+a_{nj})$, формуласымен анықталады, осындағы $i, j \in I=\{1, ..., n\}$. Бұл жерде $\mu_{\tilde{A}}(x_i)$, $(i\in I)$ анықтау үшін еркін $j(j\in I)$, бағаны, A матрицасы анықталады және a_{ij} элементерінің j бағанының барлық элементтерінің қосындысына қатысы есептеледі. КД қалыптастыруға арналған әдісте жұптық салыстырулар матрицасы қолданылады. Интервалды бағалауға негізделген әдіс (ИБН) [59], ҚФ объект кез келген Лингвистикалық анықтамаға сәйкес келу мүмкіндігі туралы түсінік береді. Сарапшы "тамаша" объект пайымына жауап беретін y критерийінің $[y_{min}, y_{max}]$ мәндерінің интервалын анықтайды. Егер $y_x - Y$ объектісінің сипаттама өлшемінің нәтижесі болса, онда y_{max} "мінсіз" облыс шекарасы бар, яғни $y_x \geq y_{max}$, болғанда объект "мінсіз" ұғымына сәйкес келеді деп танылады.Бұл пікірдің мүмкіндігі $\mu_{\tilde{A}}(x)=1$. Осындағы $\tilde{A}$ – сарапшының пайымдауынша "мінсіз" субъектілі оқиға, Егер $y_x=y_{min}$, болса, онда $\mu_{\tilde{A}}(x)=0$, егер $y_{min}< y_x< y_{max}$ онда $0<\mu_{\tilde{A}}(x)<1$.Егер сарапшы y_x мәнін y_{max} шекарасына жақындатса объектінің "мінсіз" болып танылу мүмкіндігі өседі деп пайымдаса, онда

$$\mu_{\tilde{A}}(x)=\begin{cases}0, & при\ y_x \leq y_{min};\\ (y_x - y_{min})/(y_{max} - y_{min}), & при\ y_{min} < y_x < y_{max};\\ 1, & при\ y_x \geq y_{max}.\end{cases} \quad (1.1)$$

Сарапшыларға бірнеше x нүктелерінде y_{min}, y_{max}және y_xбағалау ұсынылады. Мәліметтерді жуықтата отырып, $y_{min}=f_{min}(x)$ и $y_{max}=f_{max}(x)$,сонымен қатар [59] сәйкес пайымдарды сипаттайтын $y_x=f_x(x)$, деңгейлік шектеулерді аламыз. x үшін (1.1) формуласы бойынша $\mu_{\tilde{A}}(x_i)$, сарапшылардың бағаларының нәтижесі бойынша КД есептеледі.

Лингвистикалық термдердің статистикалық мәліметтерді қолдану (ЛТСМҚ) әдісі [60] анық емес жиынтықпен (АЕЖ) сұралатын элементтерді бағалау жиілігі негізінде сипаттайды.Ол үшін [0,1] шкаласында ЛА$X=\{x_i\}$ ($i=\overline{1,n}$)мәні орналасады және әрбір шкала интервалына сарапшылардың айтылуы бірдей саны түседі деп болжайды, керісінше өңдеу жағдайда матрицасы арқылы іске асырылады. Мысалы, ЛА мәнінде ағымдағы өлшемдерді сипаттайтын "Сұраныстар аралығындағы кідіріс уақыты" параметрдің ауытқуын $\Delta B \in [0, B]$ (B – максимальды мүмкін ауытқушылық) бағалау керек. $n=5$мәні үшін ЛА$\{x_i\}$ ($i=\overline{1,5}$),(өте кішкентай, орташа, үлкен, өте үлкен), ал интервалы $[0,B]$және $\Delta B/B$ (бағаланушы қатынас) сарапшы қолданатын ЛА мәнінің жиілігін білдіретін статистика қалыптастыратын k қиындыларына бөлінген. Сарапшының қателіктерін азайту үшін кестеге мәліметтер енгізіледі, нөлдер тұрған жолдың оң, сол жақтарынан жекелеген элементтер өшіріледі. Қайталап айту матрицасы ретінде $k_j = b_{1j} + \ldots + b_{nj}$, $j=\overline{1,5}$, элементтері бар жол қолданылады, одан кейін $k_{max} = max k_j$ таңдалады, ал $k_j = 0$, $c_{ij} = (c_{ij-1} + c_{ij+1})/2,\ i,j=\overline{1,5}$ бар бағандар үшін және кестенің барлық элементтері $c_{ij} = b_{ij} k_{max}/k_j$, өрнегіне өзгереді. Тұжырымды нұсқасы $\mu_{ij} = c_{ij}/c_{imax}$, где $c_{imax} = \max\limits_j c_{ij}$. Бұл әдісте КД ретінде сарапшы пайымдауларымен түсіндірілетін статистикалық зерттеулер нәтижесі қолданылады.

Параметрлерді тағайындау әдісі (ПТ)[61]A параметрі, оның анықтау диапазоны $[a, c]$, лингвистикалық термдер саны (m)және олардың атаулары туралы сараптау ақпаратын(СА) қолдана отырып трапеция тектес және үшбұрышты ТФ қалыптастыруға мүмкіндік береді. Трапеция тектес параметрлік ТФ анықтаймыз, $\tilde{A} = (a, b_1, b_2, c)_{LR}$, осындағы aжәнеc – $\alpha = 1$; $b_1(b_2)$ – $\tilde{A}$ деңгейінің ТФ төменгі және жоғарғы шекарасы, $\alpha = 1$, а L и R [54] -сызықты функциялар. Сәйкесінше $[b_1, b_2]$және$[a, c]$ интервалдары
А параметрінің оптимистік және пессимистік бағасын қамтып көрсетеді. ТФ келесі түрге ие: $\mu_{\tilde{A}}(x) = 0$осындағы $x < a$, $\mu_{\tilde{A}}(x) = (x - a)/(b_1 - a)$ осындағы $a \le x < b_1$, $\mu_{\tilde{A}}(x) = 1$осындағы $b_1 \le x < b_2$, $\mu_{\tilde{A}}(x) = (c - x)/(c - b_2)$ осындағы $b_2 \le x \le c$, $\mu_{\tilde{A}}(x) =$ 0 осындағы $x > c$. Бұл жерде $[a, c]$ интервалы ҚФ тасымалдаушысы болады, б $\tilde{A}$, а $[b_1, b_2]$-оның өзегі болып табылады.α-деңгейіндегі сипаттама $\tilde{A} = \bigcup\limits_{\alpha \in [0,1]} (a_\alpha, b_\alpha)$: $a_a = a + (b_1 - a)a;\ c_a = c - (c - b_2)\alpha.$ түрінде ұсынылады. Әдіске сәйкес $b_1 = b_2$ жағдайында үшбұрышты ҚФ анықтауға болады.Бұл КД әдісі үшін сарапшы тағайындаған ҚФ параметрлері болып табылады. Сауалнама әдісінде(СӘ) [62] сарапшылардың

m қолданылады, олардың ішіндегі $n_1(n_2=m-n_1$айырмашылығы) $x \in X=\{x_1, x_2, \ldots, x_m\}$ НМ $\tilde{A}$ элементінің қатыстылығына байланысты өз пайымдарын болымды түрде білдіреді. Бұл жағдайда $\mu_{\tilde{A}}(x) = n_1 / (n_1 + n_2)$ және $\tilde{A}$ класына енетін x объектісініңқолдану жиілігінің ықтималдығын білдіреді.Бұл жерде КД ретінде n_1 и n_2 мәндері қолданылады.

Тура және керісінше бағалау әдісі (ТКБ) [63] ҚФ алудың екі ұстанымы – тура және кері бағалауға негіделген. $\tilde{A}$ субъектілік ұғымы Xзерттеуаймағын X_0, X_1и $X_н$ бөліктеріне бөледі. Осында X_0 и $X_1[x_{min}]$ и $[x_{max}]$объектілерімен құрылған, сәйкесінше субъектіде оның бойында $\tilde{A}$ қасиеттері бар - жоғын, ал $X_н$бөлігі белгісіздік аймағы жөнінде күдік туындамайды. Енді субъект $\tilde{A}$ қасиеті x объектісі $x_0 \in X_0$ и $x_1 \in X_1$ әрбір жұбымен арақатынасқа қалай түсетіні жөнінде баға қоя алады. Бұл үшін ол X тен xx_0 и x_1x_0 интервалдары үшін құрылған жабдықтардың екі өзгешеліктерінің дәрежесін салыстырады және бұл ерекшеліктердің арақатынасын бағалайды. Сонымен, субъектіні X_1 и X_0, анықтауды сұрайды, сонымен қатар оларға сәйкестілікке ерікті $\mu_{\tilde{A}}(x_{min})$ и $\mu_{\tilde{A}}(x_{max})$ қоюды сұрайды.Ары қарай кездейсоқ тәсілмен оған бірнеше рет $x \in X_H$ нүктелер жиынын ұсынады және $X_H(x) \in [\mu_{\tilde{A}}(x_{min}), \mu_{\tilde{A}}(x_{max})]$әрбір бағасын $\tilde{A}$ қасиеттерін x объектісінде қабылдауын, яғни $x\tilde{A}$ қасиеттеріне ие деген келісім дәрежесін анықтайтындай етіп бейнелеуін сұрайды. Бұл $(r(x) - \mu_{\tilde{A}}(x_{min}))/(\mu_{\tilde{A}}(x_{max}) - \mu_{\tilde{A}}(x_{min}))$өрнегі $\tilde{A}$ қасиеттерінің x_{min}объектісінен x объектісіне және $\tilde{A}$ қасиеттерінің $x_{min}x_{max}$ ауысуы кезінде өсім арақатынасын білдіреді деген пікірге сәйкес келеді. $\mu_{\tilde{A}}(x_{min})$ және $\mu_{\tilde{A}}(x_{max})$ бағалары $\tilde{A}$ жиынтығының сәйкесінше x_{min}және x_{max}қатыстылық дәрежесінің мәндеріне жауап берсе, онда $r(x)$ x–тің $\tilde{A}$ қатыстылық дәрежесі болып табылады. Тура бағалауда ұсынылған объектілер үшін сарапшы тағайындаған қатыстылық дәрежесі; кері бағалауда – сәйкес объектілерді таңдау үшін қажет қатыстылық дәрежесі рәсімін бірдей ҚФ және КД беретінін атап өткен жөн.

Ең аз шаршыларды жуппен салыстыру әдісі (ЕАШЖС) [54, 64]СЖС әдісіндегі бинарлық қатынастар матрицасына негізделген, яғни ізделіп отырған мәндер оптимизациялық теңдеу негізінде қалыптасады $f = \sum_{i=1}^{n} \sum_{j=1}^{n} (a_{ij} - \omega_i / \omega_j)^2 \to min; \sum \omega_i = 1, \omega_i > 0$. Бұл жерде КД СЖС, (ШТАСЖС)және (ЖСТСЖС) әдістеріне ұқсас қалыптасады, бірақ бұл әдіс еңбекті көп қажетсінеді және қолданылмайды деуге болады.

Дәрежелік бағаларды жұппен салыстыру әдісі (ДБЖС) [57] КД ретінде жұппен салыстыру қалыптамасын қолданады. Бұл жерде ҚФ құру алгоритмі келесі кезеңдерден тұрады:

а) ЛА анықтау;

б) ЛА анықтамасының әмбебап жиынын қалыптастыру;

в)анық емес термдердің жиынтығын анықтау$\{S_1, S_2, ..., S_n\}$; г) әрбір S_j матрицасы үшін $A=\begin{bmatrix} 1 & r_2/r_1 & \dots & r_n/r_1 \\ \dots & \dots & \dots & \dots \\ r_1/r_n & r_2/r_n & \dots & 1 \end{bmatrix}$ қалыптастыру, осындағы $r_i=r(x_i)$ ($i=\overline{1,n}$) $-x_i\in X$, S сипаттайтын қасиеттер қалыптастырудағы элемент мәнінің дәрежесі; д) кез – келген терм үшін ҚФ элементтерін формулалар бойынша есептеп шығару: $\mu_{\tilde{A}}(x_1)=(1+r_2/r_1+\dots+r_n/r_1)^{-1}$, $\mu_{\tilde{A}}(x_2)=(r_1/r_2+\dots+r_n/r_2)^{-1}$, $\mu_{\tilde{A}}(x_n)=(r_1/r_n+r_2/r_n+\dots+1)^{-1}$; е) қалыптасқан ҚФ тұрақтандыру. Формулалар бойынша ҚФ анықтаудың екі тәуелсіз әдісі бар: 1)9 балдық шкала (9-ең жоғары дәреже,1-ең төменгі дәреже) бойынша r_i ($i=\overline{1,n}$) деңгейін анықтаудың абсолютті бағасы; 2) дәрежелердің салыстырмалы бағасы бойынша $a_{ij}=r_j/r_i$($i,j=\overline{1,n}$). Бұл жерде КД пайымдау қалыптамасын анықтау үшін (СЖС, ШТАСЖС, ЖСТСЖС және ЕАШЖС сияқты) Саати шкаласы (1.1.кестені қараңыз) қолданыла отырып дәрежелік бағалар қалыптасады.

Деңгейлік жиындар әдісі(ДЖ) [65] тиянақталған α-деңгейлерінде Xжиындарының элементтерін таңдау мүмкіндігін қолданады. Негізгі жиынтық элементтерінің $X=\{x_1, ..., x_n\}$ қатыстылық дәрежесі $\tilde{A}$ анық емес ішкі жиынтығына белгілі ($\mu_{\tilde{A}}(x_i)$ белгіленеді) және $\mu_{\tilde{A}}(x_i)\geq\mu_{\tilde{A}}(x_j)$ болғанда осындағы $i>j$ жол беріледі. $\tilde{A}$ ішкі жиынтығы НМ $\tilde{A}$ деңгейлік жиындары деп аталатын X жиындарының анық емес ішкі жиындарына сәйкестілігі қойылады.α-деңгейінің жиыны $A_\alpha=\{x:\mu_{\tilde{A}}(x)\geq\alpha, x\in X\}$ анықталады. Егер$\alpha_1>\alpha_2$, онда A_α α параметрінің өспелі функциясы, сонымен қатар егер кейбір α_kпараметрлері үшін $\mu_{\tilde{A}}(x)\geq\alpha_k$, элементтер болмаса, онда $A_\alpha=\varnothing$ $A_\alpha=\varnothing$ үшін $\alpha\geq\alpha_k$. Ары қарай $\mu_{\tilde{A}}(x_i)\,\mu_{\tilde{A}}(x_1)=nP(x_1)$; $\mu_{\tilde{A}}(x_2)=(n-1)P(x_2)+P(x_1)$; ... $\mu_{\tilde{A}}(x_k)=(n-k+1)P(x_k)+\sum_{i=1}^{k-1}P(x_i)$; ... $\mu_{\tilde{A}}(x_{n-1})=2P(x_{n-1})+\sum_{i=1}^{n-2}P(x_i)$; $\mu_{\tilde{A}}(x_n)=\sum_{i=1}^{n}P(x_i)$, ретінде анықтаймыз, осындағы n- X- тегі элементтер саны, $\mu_{\tilde{A}}(x_i)$ $-\tilde{A}$ ішкі жиынтығына x_i қатыстылығының дәрежесі,

$P(x_i)$ –x_i.таңдау мүмкіндігі (сараптама). Егер $i \geq j$, онда $\mu_{\tilde{A}}(x_i) \geq \mu_{\tilde{A}}(x_j)$ және $P(x_i) \geq P(x_j)$және керісінше, егер $P(x_i) \geq P(x_j)$, онда $\mu_{\tilde{A}}(x_i) \geq \mu_{\tilde{A}}(x_j)$ екенін ескеру керек. Бос жиын алу мүмкіндігі нөлге тең болғанда, онда $\mu_{\tilde{A}}(x_n) = 1$. $P(x_i)$ есептеу үшін [65] сипатталған алгоритм қолданылады. КД әдісінде сарапшылар тапсырған тиянақталған α-деңгейлерінде Xжиындарының элементтерінің топтары болып табылады.

Сандық әдіс (СӘ) [54] қарастырылған әрбір кластың сандық мәнін анықтайтын сарапшылар тобының сұранысымен байланысты және барлық nсарапшылардың мәліметтері бойынша орташасы, яғни $\mu_{\tilde{A}}(x) = (\mu_{\tilde{A}}(x_1) + \ldots + \mu_{\tilde{A}}(x_n))/n$ анықталады. Бұл жерде КД ретінде [0,1] интервалының қатыстылық дәрежесінде болатын сандық мәндер қолданылады.

Экспоненттік ТФ құру әдісі (ЭҚФҚ) [59, 66] экспоненттті функция, ережелер көмегімен ізделіп отырған ҚФ коэффициенттерін анықтауға арналған сарапшы бағаларына сүйенеді: егер $\alpha \le x \le \beta$, онда $\mu_{(\alpha,\beta)}(x)=1$; егер$x < \alpha$, онда $\mu_{(\alpha,\beta)}(x)=\mu_{(\alpha)}(x);$ егер$x < \beta$, онда $\mu_{(\alpha,\beta)}(x)=\mu_{\beta}(x),$ осындағыαжәне β – анық емес сан шыдамдылығының шегі(АЕС); $\mu_{(\alpha,\beta)}(x)$ -(α, β); $\mu_{(\alpha)}(x)$ және $\mu_{(\beta)}(x)$ интервалындағы ҚФ мәні -αжәнеβ шамамен тең ҚФ сандары. Жақын нүктелік бағалар үшін ҚФ құрылады. Белгісіз K шамамен теңсан үшін ҚФ құру $\mu_K(x)=e^{-\alpha(K-x)^2}$ функциясы арқылы жүзеге асырылады, осындағы $a=-4\ln(0,5)/\beta^2$, ал β – ауысу нүктелері арасындағы арақашықтық (aжәне$в$), яғни $\mu_K(x)=0,5.\beta$анықтау үшін K натурал санын береміз, осындағы q – кіші мәнге ие цифр, оның мүмкін мәндерін қалдықтар класына бөлеміз $mod(3)$. Айнымалы $d\in\{0, 1, 2\}$ енгіземіз және альтернативті $M_d\{d=0, 1, 2\}, d=qmod(3)$. Ары қарай 1-ден 99 аралығындағы бүтін санды U айнымалысын анықтаймыз және оның әрбір мәні үшін $a(u), b(u)$және $\beta(u)$параметрлері белгілі. Сауалнама нәтижесі бойынша Uмәні арқылы 1.2. кестесін қолдана отырып $\beta(u)$ табуға болатыны анықталды, осындағы $E(u/10)$мәні $(u/10)$ мәнінен антьє білдіреді, ал $\beta(u)$ K M_i қай класына жататындығына байланысты. Егер r_q –q- разрядында орналасқан Kсаны болса, онда [66] сипатталған алгоритм әрекет етеді. Бұл әдісте КД жуық нүктелік сарапшылық баға болып табылады. Сарапталған материалды жалпылай келе ПТ, СЖС, ШТАСЖС, ЖСТСЖС, ПТ, СӘ, ЕАШЖС, ДБЖС, СӘ, ЭҚФҚ әдістері үшін КД сарапшылық пікір терім;СЖС, ШТАСЖС, ЖСТСЖС, ЕАШЖС, ДБЖС дәрежелік бағалар негізінде жұппен салыстыру қалыптамалары қолданылады; ИБН –объект үшін белгілі интервалда сипаттамалардың өлшемі; ЛТСМҚ – элемент сипаттамаларының статистикалық мәліметтері; ТКБ - белгілі интервалдың нүктелеріне баға тағайындау; ДЖ - α-деңгейі элементтерінің жиынына қатысты элементтер тобын тағайындау.

Кесте 1.2 -Ауысу нүктелері арасындағы арақашықтық

U	β(u)
1, 2, 3, 4, 6, 7, 8, 9	0,46 u
10, 20, 30, 40, 60, 70, 80, 90	(0,357 – 0,00163u)u
35, 45, 55, 65, 75, 85, 95	(0,213 – 0,00067u)u
5; 15; 25; 50	2,8; 6,48; 6,75; 24
Өзге қос таңбалы сандар	0,5(β(10E(u/10)+5)+β(x–10E(u/10)))

Жүйедегі ауытқушылық жағдайының деңгейін сипаттайтын жүйеге ең жақын модель параметрлерін түрлі анық емес шамаларды салыстыру әдістерінің логикалық шешім шығару іске асыру мүмкіндіктерін қарастырайық. α-деңгейлік арақашықтық(АДА) [67] үшін тапсырылған эталонды АЕСүшін минималды $\forall\mu_y \geq\alpha$: $d(\underset{\sim}{X},\underset{\sim}{Y}) = (\sum_{j=1}^{k}\sum_{i=1}^{m}\left|x_i - y_j\right|)/k$, осындағы α –α-деңгейдің берілген деңгейі $(0\leq\alpha\leq1)$; x_iжәне y_i –сәйкесінше алынған модельді АЕС $\underset{\sim}{X}$ және $\underset{\sim}{Y}$ сәйкесінше; m –АЕС $\underset{\sim}{X}$ құрамдас бөліктерінің саны; k –АЕС $\underset{\sim}{Y}$ ҚФ бар $\mu_y\geq\alpha$. үшін $d(\underset{\sim}{X},\underset{\sim}{Z})$ құрамдас бөліктерінің саны. Бұл әдіс АЕС үздіксіз және параметрлік кластан басқа барлық кластарға қолдануға болады. Максминді әдіс (МӘ) [55, 68] НЧ жұбының $H(\underset{\sim}{X},\underset{\sim}{Y})$функциясын анықтауға негізделген: $\underset{\sim}{X} = \bigcup_{x\in S_X}\mu_{\underset{\sim}{X}}(x)/x$ және $\underset{\sim}{Y} = \bigcup_{y\in S_Y}\mu_{\underset{\sim}{Y}}(y)/y$, онда $H(\underset{\sim}{X},\underset{\sim}{Y}) = \sup_{x\in S_X, y\in S_Y} \min\{\mu_{\underset{\sim}{X}}(x), \mu_{\underset{\sim}{Y}}(y), \mu_V(x,y)\}$, осындағы $\mu_V(x,y)$ – ҚФ x және y анық сандары арасындағы анық емес қарым-қатынас артықшылығы. Ал мысалы V ретінде ҚФ V_1–дің ҚФ – мен $\mu_{V_1}(x,y)=1$, осындағы $x \geq y$және $\mu_{V_1}(x,y)=0$, осындағы $x<y$. $H(\underset{\sim}{X},\underset{\sim}{Y})\tilde{\geq}H(\underset{\sim}{Y},\underset{\sim}{X})$болған жағдайда онда $\underset{\sim}{X}\geq\underset{\sim}{Y}$. [69] сәйкес МӘ дисскретті және параметрлі емес кластардан басқа барлық АЕС кластары үшін қолдануға болады. Реттеу әдісі(РӘ) [59] $P_{\underset{\sim}{X}} = \bigcup_{\substack{z=x/(x+y)\\ x\in X, y\in Y}}\mu_{P_{\underset{\sim}{X}}}(z)/z$ және $P_{\underset{\sim}{Y}} = \bigcup_{\substack{z=y/(x+y)\\ x\in X, y\in Y}}\mu_{P_{\underset{\sim}{Y}}}(z)/z$,анық емес қарым-қатынасты қолданады, осындағы $\mu_{P_{\underset{\sim}{X}}}(z)/z$ және $\mu_{P_{\underset{\sim}{Y}}}(z)/$ z-ҚФ $P_{\underset{\sim}{X}}$ және $P_{\underset{\sim}{Y}}$ сәйкесінше, ал x және y – анық оң сандар. “Көбірек” қатынасы $\underset{\sim}{X}>\underset{\sim}{Y} \Leftrightarrow P_{\underset{\sim}{X}} \subset$ Р ретінде анықталады,осындағы $P=\{(0; z')\}\cup\{(1; z'')\}$, $z'\in[0; 0,5]$, $z''\in[0,5; 1]$; $\underset{\sim}{X}=\underset{\sim}{Y} \Leftrightarrow P_{\underset{\sim}{X}}=P$. Үздіксіз $\underset{\sim}{X}$ және $\underset{\sim}{Y}$ екі жақын НМ $P_{\underset{\sim}{X}}$ және $PD(\underset{\sim}{X},\underset{\sim}{Y}$

$)=\int_{0}^{0,5}[1-\mu_{P_{\tilde{X}}}(z)]\,dz+\int_{0,5}^{1}\mu_{P_{\tilde{X}}}(z)dz$, өрнегінің интегралды бағасында жүзеге асырылады, осындағы $D(\tilde{X},\tilde{Y})\in[0,5;\ 1]\Leftrightarrow \tilde{X}>\tilde{Y}$, а $D(\tilde{X},\tilde{Y})=D(\tilde{Y},\tilde{X})=0,5\Leftrightarrow \tilde{X}=\tilde{Y}$, және дисскретті $\tilde{X}$ және $\tilde{Y}$ үшін $D(\tilde{X},\tilde{Y})=0,5-(b_1-a_1)/n_1\sum_{i=1}^{n_1}\mu_{P_{\tilde{X}}}(z')+(b_2-a_2)/n_2\sum_{i=1}^{n_2}\mu_{P_{\tilde{X}}}(z'')$,өрнегі, осындағы a_iжәне b_i – ҚФ өзгеру шекарасы, n_i – нүктелер саны, $\mu_{P_{\tilde{X}}}(z)\neq 0$, $z'\in[0;\ 0,5]$, $z''\in[0,5;\ 1]$ нүктелер саны. Мысалы, егер $D(\tilde{X},\tilde{Y})<0,5$, яғни $[0;\ 0,5]$ интервалында, онда $\tilde{X}<\tilde{Y}$.[69] сәйкес ДФ қалыпты, шығыңқы, унимодальды, дисскретті, үздіксіз, параметрлі және параметрлі емес АЕС үшін қолданылады.

Қатынастар негізіндегі реттеу әдісі (ҚНРӘ) [59] оптимальды жиынтыққа Альтернативтіны анықтауға негізделген n Альтернативтіның $\{x_1, \ldots, x_n\}$ жиынтығынің әрқайсысы НМ $\tilde{X}_i=\{\mu_{\tilde{X}_i}(x)/x\}$ көрінеді, осындағы $x\in R$. $O=\{\mu_O(i)/i\}$, $i\in N$, оптимальды альтернативті жиынтығын анықтаймыз, осындағы $\mu_O(i)$ –x_i“ең жақсы альтернативті” ұғымының сәйкестік дәрежесі. Осы мақсатта $P_{ij}=\{\mu_{P_{ij}}(x_i,x_j)/(x_i,\ x_j)\}$, $x_j\in R$, анық емес қатынасы енгізіледі, осындағы $\mu_{P_{ij}}(x_i,x_j)$ x_i x_j, -ден артықшылық дәрежесін анықтайды, мысалы, бұл $\mu_{P_{ij}}(x_i,x_j)=x_i-x_j$. функциясы болуы мүмкін. Қолайлы альтернативті жиынтығы бұл анық емес бағалардың және P_{ij}: $O=P_{ij}\bigcap(\tilde{X}_i\times\tilde{X}_j$ артықшылығының қатынасының қиылысуы. x_iқатыстылық дәрежесінің альтернативті O жиынының максимум сәйкес ҚФ : $\mu_O(i)=\sup_{x_i,x_j}\min(\mu_{\tilde{X}_i}(x_i),\ \mu_{\tilde{X}_j}(x_j),\ \mu_{P_{ij}}(x_i,x_j))$, $i\neq j$, $i\in\{1,\ 2\}$. АДА қолданылатын АЕС үшін әдісті қолдануға болады.

Жалпыланған операциялар әдісі (ЖОӘ) [59] екі компонентті НМ анықтауға мүмкіндік береді, $\tilde{X}$ артық немесе $\tilde{Y}$ тең және $V(\tilde{X}\geq\tilde{Y})=\sup_{x\geq y}\min(\mu_{\tilde{X}}(x),\ \mu_{\tilde{Y}}(y))$, белгіленеді, бұл $x\geq y$, ең аз жоғарғы мүмкіндік шегі осындағы $\tilde{X}=(\alpha,\ m,\ \beta)_{LR}$ және $\tilde{Y}=(\gamma,\ n,\ \delta)_{LR}$, осындағы m және n –$\tilde{X}$ және $\tilde{Y}$ максимальды μ және $n\geq m$ АЕС тасымалдаушылары; α және γ – сол , ал β және δ сәйкесінше $\tilde{X}$ және$\tilde{Y}$ оң шекаралары болып табылады. $V(\tilde{X}\geq\tilde{Y})$мәні $\tilde{X}$ және $\tilde{Y}$ максимум, яғни D нүктесінің $\tilde{X}$ және $\tilde{Y}$ үшін теңеседі. Егер АЕС шығыңқы және тұрақтанған емес болса, онда ҚФ максимумының $\tilde{X}$ и $\tilde{Y}$

жауап беретін *x* және *y* мәндері қолданылады. [69] сәйкес ЖОӘ дисскретті және параметрлі емес барлық АЕС үшін қолдануға болады.

Жалпыланған Хэмминг арақашықтығы (ЖХА) [67] $h(\underset{\sim}{X}, \underset{\sim}{Z}) = \sum_{i=1}^{n} |\mu_{\underset{\sim}{X}}(x_i) - \mu_{\underset{\sim}{Z}}(x_i)|$ формуласымен анықталады, осындағы $\mu_{\underset{\sim}{X}}(x_i)$ және $\mu_{\underset{\sim}{Z}}(x_i)$ – ағымдағы $\underset{\sim}{X}$ және модельдегі $\underset{\sim}{Z}$ сәйкес ҚФ болып табылады.Осында минимальды *h*АЕС модельге жақындығы туралы куаландырады. Мысалы, егер $h(\underset{\sim}{Y}, \underset{\sim}{Z}) < h(\underset{\sim}{X}, \underset{\sim}{Z})$ болса, онда $\underset{\sim}{Y}$ $\underset{\sim}{X}$.-ке қарағанда модельге жақынырақ орналасады. [69] сәйкес әдісті қалыпты, субқалыпты, шығыңқы, шығыңқы емес, унимодальды, полимодальды, шыдамды, дисскретті және параметрлі емес АЕС үшін қолдануға болады.

Реттеу функциясы (РФ) [59] *I* бір интервалына негізделген. Егер $\underset{\sim}{X}$ -*I* анық емес ішкі жиынтығы, α-деңгейлі жиынтық $X_\alpha = \{x : x \in I, \mu_{\underset{\sim}{X}} \geq \alpha\}$ және *I* кәдімгі ішкі жиынтығы болып табылады. Егер *V*-*I* ішкі жиынтығы: $V = \{x_1, x_2, ..., x_n\}$, ал $M(V)$-$M(V) = (x_1 + ... + x_n)/n$ формуласы арқылы анықталатын *V* элементтерінің орташа шамасы болып табылады. Егер $V = \bigcup \{a_i \leq x \leq b_i\}$ болса, онда $M(V) = (a+b)/2$, ал $0 \leq a_1 \leq b_1 \leq a_2 \leq b_2 \leq ... \; a_n \leq b_n \leq 1$ және $V = \sum_{i=1}^{n} ((a_i + b_i)/2)(b_i - a_i)/\sum_{i=1}^{n} (b_i - a_i)$ онда орта мән келесі түрде болады: $M(V) =$. Егер $\underset{\sim}{X}$ – $I\alpha_{max}$ мүшелерімен бірге анық емес ішкі жиынтығы болса, онда $F(\underset{\sim}{X}) = \int_0^{\alpha_{max}} M(V)d\alpha$ реттеу функциясын анықтайды. Әдіс АЕС барлық кластарын өңдеуге бағытталған.

Ауырлық орталығы әдісі (АОӘ) [61] α-деңгейлік АЕС бағытталған. Егер $\underset{\sim}{X} = \bigcup_{\alpha \in [0,1]} (\underline{x}_\alpha, \overline{x}_\alpha)$, $k_x\alpha$-деңгейде берілген, ал $\underset{\sim}{Y} = \bigcup_{\alpha \in [0,1]} (\underline{y}_\alpha, \overline{y}_\alpha)$ -$k_y\alpha$-деңгейде, онда:

$\underset{\sim}{X} < \underset{\sim}{Y}$, егер $1/2k_x \sum_{\alpha \in [0,1]} (\underline{x}_\alpha + \overline{x}_\alpha) < 1/2k_y \sum_{\alpha \in [0,1]} (\underline{y}_\alpha + \overline{y}_\alpha)$;

$\underset{\sim}{X} = \underset{\sim}{Y}$, егер $1/2k_x \sum_{\alpha \in [0,1]} (\underline{x}_\alpha + \overline{x}_\alpha) = 1/2k_y \sum_{\alpha \in [0,1]} (\underline{y}_\alpha + \overline{y}_\alpha)$.$(a, b_1, b_2, c)_{LR}$, түрінде берілген сызықты параметрлік АЕС үшін есептеу $(a+b_1+b_2+c)/4$ түрінде жүргізіледі. Әдісті қалыпты және субқалыпты, шығыңқы, унимодальды, шыдамды, дисскретті және параметрлі АЕС жұмыс үшін

қолданады.Компьютерлік жүйелер мен желілерде ауытқуларды табу жүйесінің құралдары мен әдістерін құруға қолдануға болатын АЕС өңдеулерін қарастырайық. АЕС арифметикасын жүзеге асыруға негізгі әдіс ретінде $\tilde{Z} = \tilde{X} \overset{\sim}{*} \tilde{Y} = \bigcup_{i=1}^{n} \bigcup_{j=1}^{m} \{(\mu_X(x_i) \wedge \mu_Y(y_j))/(x_i \circledast y_j)\}$, формуласымен жүзеге асырылатын максминді композиция әдісі [55] қолданылады, осындағы $\tilde{X}$ және $\tilde{Y}$ – АЕС, ал $\circledast$ –+, –, ·, :.максминді операцияларының бірі болып табылады.Ары қарай бірдей тасымалдаушылары бар құрамдас бөліктер $\mu_Z(z_k)/z_k, (k=\overline{1,r})$ бір - $\mu_Z(z_s)/z_s : \mu_Z(z_s) = max(\mu_Z(z_k))$ жұтылады. Әдіс үздіксіз және параметрлі әдістерден басқа барлық АЕС кластарымен жұмыс істейді.

Жолдар немесе бағандардың максималды элементтерінің векторын қалыптастырудағы матрицалық әдіс (ЖБМЭВҚҚ) [70] элементтері жол мен бағанның векторына арифметикалық операцияның нәтижесі $z_{ij}=x_i \circledast y_j$, ал $\mu_Z(z_{ij}) = min(\mu_X(x_i), \mu_Y(y_j))$ болып табылатын матрицаға негізделеді. $\tilde{Z} = \{z_{ij}\} (i=\overline{1,n}; j=\overline{1,m})$ матрицасының әрбір бағанынан (жолынан) $\mu_Z(z_м) = max\{\mu_Z(z_{ij})\}$ элемент түзетін нәтиже таңдалады. Мысалы бағандар үшін $\tilde{Z} = \bigcup \mu_Z(z_м)/z_м = \bigvee_{j=1}^{m} \bigwedge_{i=1}^{n} (\mu_X(x_i), \mu_Y(y_j)/(x_i \circledast y_j))$. Унимодалды АЕС үшін құрамдас бөліктерді біріктіргенде бірнеше $\mu(z_i)/z_i (i=\overline{1,q})$ бірдей $\mu_Z(z)$ бар бір $\bigwedge^{q}$ құрамдас бөлігі $\mu(z_p)/z_p : |z_p - z_м| = \bigwedge_{i=1} |z_i - z_м|$, осындағы $z_м$- максималды $\mu_Z(z)$бар тасымалдаушы; q –бірдей $\mu(z)$ бар тасымалдаушылар саны. Әдісті қалыпты, субқалыпты, шығыңқы, шығыңқы емес, унимодалды, дисскретті және параметрлі емес АЕС үшін қолдануға болады. [71] жұмыста максималды элементі бар жол және бағанның таңдауы бар матрицалық әдіс (МЭЖБҚ) бірмодалды АЕС үшін $\tilde{X} = \{\mu_x(x_i)/x_i\} (i=\overline{1,n})$ және $\tilde{Y} = \{\mu_y(y_j)/y_j\} (j=\overline{1,m}).=\overline{1,m})$. $\tilde{Z} = \tilde{X} \tilde{\circledast} \tilde{Y}$ АЕС операциясын жүзеге асыру барысында $\tilde{X}$ және $\tilde{Y}$ жол мен бағанның векторы ретінде ұсынылады. $\tilde{Z}^{(1)}$ матрицасының $\mu_z(z_{ij}^{(1)})/z_{ij}^{(1)}$ мәндері $\mu_x(x_i) \wedge \mu_y(y_j)/x_i \circledast y_j$ ретінде анықталады. Ары қарай $\tilde{Z}^{(1)}$ (құрамында $\mu_z(z_{pq}^{(1)}) = max(\bigcup_{i=1}^{n} \bigcup_{j=1}^{m} \mu_z(z_{ij}^{(1)}))$суппорты бар) матрицасының жолдары мен бағандарының элементі бар $\mu_z(z_f^{(2)}) > \mu_z(z_{f+1}^{(2)}) (f=\overline{1,c}; c=n+m-1)$: $Z^{(2)} = \{\mu_z(z_1^{(2)})/z_1^{(2)}, \ldots, \mu_z(z_f^{(2)})/z_f^{(2)}, \ldots, \mu_z(z_c^{(2)})/z_c^{(2)}\}$тәртібімен тығыз байланысты $\tilde{Z}^{(2)}$ $\bigwedge$ қалыптасады. Тең $\mu(z)$ бар бір $\mu(z)/z : |z - z| = \bigwedge_{i=1} |z_i - z_m|$, осындағы z_m –

максималды $\mu(z)$ бар суппорт, ал r –бірдей $\mu(z)$ бар тасымалдаушылар саны. Бірнеше $\mu_z(z_k^{(2)})/z_k^{(2)}$, $(k=\overline{1,r})$ жұтылатын $\tilde{Z}^{(3)}$ анықтаймыз. Ары қарай $\tilde{Z}^{(3)}$ оң құрамдас бөліктер бастапқы АЕ өлшемділігіне дейін, яғни $\tilde{Z}^{(3)} \Rightarrow \tilde{Z} = \{\mu(z_k)/z_k\}$, $k=\overline{1,b}$, $b \in \{n, m\}$ қиылады. Әдісті ЖБМЭВҚҚ сияқты АЕС басқа басқа кластарына қолдануға болады.

Матрицалық-бұрыштық әдіс(ҚБӘ) [72] ЖБМЭВҚҚ және МЭЖБҚ ұқсас нәтижелік матрица қалыптасады, ал қосу амалы бойынша ҚФ құру $\mu_Z(x_{11})/x_{11}$ басталып $\mu_Z(x_{nn})/x_{nn}$ аяқталады. Барлық $\mu_Z(x_{ij})/x_{ij}$ үшін $\mu_Z(x_{i+1,j})/x_{i+1,j}$, $\mu_Z(x_{i,j+1})/x_{i,j+1}$ сарапталады және с максималды ҚФ таңдалады. Азайту да осыған ұқсас жүзеге асырылады, бірақ $\mu_Z(x_{1n})/x_{1n}$ элементтерінен бастап $\mu_Z(x_{n1})/x_{n1}$ дейін, ал көршілес $\mu_Z(x_{ij})/x_{ij}$ үшін $\mu_Z(x_{i+1,j})/x_{i+1,j}$ және $\mu_Z(x_{i,j-1})/x_{i,j-1}$ болады. Әдіс қалыпты, субқалыпты, шығыңқы, унимодалды, дисскретті және параметрлі емес АЕС бағытталған.

Үздіксіз АЕС арналған әдіс (ҮАЕС) [59] $\tilde{X} = \int_a^A (x-a)|_x + \int_A^b (b-x)|_x$ және $\tilde{Y} = \int_{a'}^B (x-a')|_x + \int_B^{b'} (b'-x)|_x$, (осындағы a және b – сәйкесінше ҚФ $\tilde{X}$ және $\tilde{Y}$ төменгі, a' және b' – жоғарғы, ал A және B сәйкесінше бірлік ҚФ бар тасымалдаушыларыныңтөменгі шекаралары) $\tilde{Z} = \tilde{X} \underset{*}{\tilde{\times}} \tilde{Y} = \int_{a''}^C \mu_{\tilde{Z}}(x)|_x + \int_C^{b''} \mu_{\tilde{Z}}(x)|_x$ жалпы формуласы бойынша орындалады, осындағы $C=A \circledast B$, a'' және b'' a, b, a' және b' нақты амалға байланысты алынады. Функция $\mu_{\tilde{Z}}$ қызметі амалға және μ.

реттеуге байланысты анықталады. Мысалы, $\mu_{\tilde{Z}} = k_1 x + k_2$ [59] көбейтуді реттеуде $\tilde{X} \cdot \tilde{Y} = \int_{a''}^C ((\sqrt{x} - \sqrt{a''})/(\sqrt{C} - \sqrt{a''}))|_x + \int_C^{b''} ((\sqrt{b''} - \sqrt{x})(\sqrt{b''} - \sqrt{C}))|_x = \tilde{Z}$ болады, осындағы $a'' = aa'$, $b'' = bb'$. Ары қарай еркін аралық x нүктелеріндегі ҚФ есептеледі.Әдіс қалыпты, шығыңқы, унимодалды, үздіксіз және параметрлі АЕС үшін жұмыс істейді.

Матрицалық-көлденең әдіс (ҚК) [72] α-деңгейлік АЕС бағытталған және шын мәнісінде келесі өрнектерге әкеледі: қосу мен көбейту үшін - $\tilde{Z} = \tilde{X} \tilde{\circledast} \tilde{Y} = \bigcup_{i=j=1}^{n} \mu_Z(z_{ij}) = \bigcup_{i=j=1}^{n} \{(\mu_X(x_i) \wedge \mu_Y(y_i))/(x_i \circledast y_j)\}$; азайту мен бөлу үшін - $\tilde{Z} = \tilde{X} \tilde{\circledast} \tilde{Y} = \bigcup_{i=1}^{n} \bigcup_{j=n}^{1} \mu_Z(z_{ij}) \bigcup_{i=1}^{n} \bigcup_{j=n}^{1} \{(\mu_X(x_i) \wedge \mu_Y(y_i))/ \circledast$

$\bigcup_{i=1}^{n}\bigcup_{j=n}^{1}\mu_Z(z_{ij}) = \bigcup_{i=1}^{n}\bigcup_{j=n}^{1}\{(\mu_X(x_i) \wedge \mu_Y(y_i))/ (x_i \circledast y_j)\}$, осындағы n –АЕС құрамдас бөліктерінің саны. Әдіс қалыпты, субқалыпты, шығыңқы, унимодалды, шыдамды, дисскретті және параметрлі емес АЕС үшін қолданылады.

Біртекті амалдарды орындау әдісі (БАО) 59] үздіксіз АЕС шығыңқы, өсетін және кемитін немесе тұрақты АЕС бөлуді қарастырады. Олар деңгей бойынша дискреттелуі мүмкін: $\alpha_i(i=\overline{1,k}$ $(\alpha_1=0, \alpha_k=1))$. Кез - келген i деңгейімен $X_i = \{x_{i_1},....,x_{i_J}\}$, жиыны байланысты, $x_{i_j} \in R,\ \mu(x_{i_j}) = \alpha_i;\ j=\overline{1,J}$, яғни жалпы түрде $\underset{\sim}{X} = \{\alpha_1 / x_{11};\ \alpha_2 / x_{21}; \ldots; \alpha_k / x_{k1}; \ldots; \alpha_2 / x_{22};\ \alpha_1 / x_{12}\}$, ал $\underset{\sim}{X}$ және $\underset{\sim}{Y}$ амалдар нәтижесі ($\underset{\sim}{X} = \{\alpha_1 / x_{11}; \alpha_2 / x_{21};\ \alpha_1 / x_{12}\}$ және $\underset{\sim}{Y} = \{\alpha_1 / y_{11};$ $\alpha_2 / y_{21};\ \alpha_1 / y_{12}\}$), онда $\underset{\sim}{Z} = \underset{\sim}{X} \tilde{\circledast} \underset{\sim}{Y} = \{\alpha_1 /(x_{11} \circledast y_{11});\ \alpha_2 /(x_{21} \circledast y_{21}); \alpha_1 /(x_{12} \circledast$ $y_{12})\}$. Әдіс қалыпты, субқалыпты, шығыңқы, шығыңқы емес, унимодалды, үздіксіз параметрлі және параметрлі емес АЕС үшін қолданылады.

Векторлық әдіс(ВӘ) [73] МЭЖБҚ негізделеді және $\underset{\sim}{X}$ жол-вектор ретінде көрсетіледі, ал $\underset{\sim}{Z}^{(1)} \underset{\sim}{Z}_x^{(1)} = \underset{\sim}{X} \circledast \mu_{y_M} / y_M = \bigcup_{i=1}^{n} (\mu_{y_M} \wedge \mu_{x_i})/(y_M \circledast x_i)$ және $\underset{\sim}{Z}_y^{(1)}$ $= \underset{\sim}{Y} \circledast \mu_{x_M} / x_M = \bigcup_{j=1}^{m} (\mu_{x_M} \wedge \mu_{y_j})/(x \circledast y_j)$ауысады, осындағы μ_{y_M} / y_Mжәне μ_{x_M} / x_M —максималды ҚФ бар құрамдас бөліктер. Сонымен бірге компоненты $\underset{\sim}{X}_x^{(1)}$ және $\underset{\sim}{Y}_y^{(1)}$, яғни $\underset{\sim}{Z}^{(2)} = \underset{\sim}{Z}_x^{(1)} \bigcup \underset{\sim}{Z}_y^{(1)}$ бірігеді. Әдіс МЭЖБҚ негізделетін болғандықтан, ол НЧ біркелкі кластарына негізделген. .α-деңгейлік әдісте (АД) [74] амал жалпыланған формуламен жүзеге асырылады: $\underset{\sim}{Z} = \underset{\sim}{X} \{\alpha_x \tilde{*} \alpha_y\} \underset{\sim}{Y}$ $= \bigcup_{i=1}^{n}\bigcup_{j=1}^{m}{}^{(\forall \mu \geq \alpha_x)} \{(\mu_X(x_i) \wedge \mu_Y(y_j))/(x_i \circledast y_j)\} + \bigcup_{i=1}^{n}\bigcup_{j=1}^{m}{}^{(\forall \mu \geq \alpha_y)} \{(\mu_X(x_i) \wedge \mu_Y(y_j))/ (x_i \circledast y_j)\}$, осындағы $\{\alpha_x \tilde{*}$ $\alpha_y\}$- амалдың таңбалануы, ал α_x және α_y-$\underset{\sim}{X}$ және $\underset{\sim}{Y}$ үшін сәйкесінше α-деңгейлер. Әдіс АЕС барлық кластарын, үздіксіз және параметрлі түрлерінен басқа өңдеуге бағытталған. Белгілі α-деңгейлік (АД) және жалпыландырудың өзгерген ұстанымы (ЖӨҰ) [61] ҚК және БАО тәрізді α-деңгейлік АЕС бағытталған. Егер $\underset{\sim}{y} = f(\underset{\sim}{x}_1, \ldots, \underset{\sim}{x}_n)$ функциясында АЕС АД түрінде ұсынылса: $\underset{\sim}{y} = \bigcup_{\alpha \in [0,1]} (\underline{y}_\alpha, \overline{y}_\alpha)$, $\underset{\sim}{x}_i = \bigcup_{\alpha \in [0,1]} (\underline{x}_{i_\alpha}, \overline{x}_{i_\alpha})$, $(i=\overline{1,n})$, онда кез-келген α-деңгей үшін оның мәні $\underline{y}_\alpha = inf(f(x^*_{1_\alpha}, \ldots, x^*_{n_\alpha}))$ немесе $\overline{y}_\alpha = sup(f(x^*_{1_\alpha}, \ldots, x^*_{n_\alpha}))$, ретінде анықталады, осындағы $x^*_{i_\alpha} \in [\underline{x}_{i_\alpha}, \overline{x}_{i_\alpha}],\ (i=\overline{1,n})$ .. Әдісті қалыпты, субқалыпты, шығыңқы, шыдамды, дисскретті және параметрлі емес АЕС үшін қолдануға болады. ЖӨҰ –да бастапқы функция

$y=f(x_1, ..., x_n)$ келесі шарттарды қанағаттандыруы тиіс: аргументтердің өзгеру аймағы үздіксіз; функцияның анықталу аймағы дифференциаландырылған; $X=\{x_1, ..., x_n\}$ аргументтер жиынын $X = X_1 \cup X_2 \cup X_3$ ретінде көрсетуге болады, яғни $X_1 \cap X_2 = X_3 \cap X_2 = X_1 \cap X_3 = \oslash$; $X_1 = \{x_r : dy/dx_r \geq 0\}$ $(r = \overline{1, p_1})$; $X_2 = \{x_s : dy/dx_s \leq 0\}$ $(s = \overline{1, p_2})$; $X_3 = \{x_t : sign(dy/dx_t) = h_t(x_r, x_s)\}$ $(t = \overline{1, p_3}$; $p_1 + p_2 + p_3 = n)$. $dy/dx_t = g_t(x_r, x_s)$ – айнымалы таңбалы функция және барлық $x_t \in X_3$ үшін туынды таңбасы dy/dx_t x_t, тәуелді емес, яғни $sign(dy/dx_t) \neq h(x_t)$. Егер $y=f(x_1, ..., x_n)$ –n айнымалының функциясы және оның аргументі x_i- АЕС түрі т $\underset{\sim}{x}_i = \bigcup_{\alpha \in [0,1]} (\underline{x}_{i_\alpha}, \overline{x}_{i_\alpha})$, $(i = \overline{1,n})$, онда анық емес $\underset{\sim}{y} = f(\underset{\sim}{x}_1, ..., \underset{\sim}{x}_n)$ $\underset{\sim}{y} = \bigcup_{\alpha \in [0,1]} \{ f(\underline{x}_{r_\alpha}, \overline{x}_{s_\alpha}, x^I_{t_\alpha}), f(\overline{x}_{r_\alpha}, \underline{x}_{s_\alpha}, x^{II}_{t_\alpha}) \}$, саны болады, осындағы $x^I_{t_\alpha} = \underline{x}_{t_\alpha}$ болғанда $g_t(\underline{x}_r, \overline{x}_s) \geq 0$ $x^I_{t_\alpha} = \overline{x}_{t_\alpha}$ осындағы $g_t(\underline{x}_r, \overline{x}_s) < 0$, сонымен бірге $x^{II}_{t_\alpha} = \overline{x}_{t_\alpha}$ болғанда $g_t(\overline{x}_r, \underline{x}_s) \geq 0$ немесе $x^{II}_{t_\alpha} = \underline{x}_{t_\alpha}$ болғанда $g_t(\overline{x}_r, \underline{x}_s) < 0$. Әдісті қалыпты, шығыңқы, шыдамды, үздіксіз және параметрлі НЧ үшін қолдануға болады.

Параметрлі L-R АЕС өңдеу әдісі (ПӨӘ) [55, 69, 72], мысалы, унимодалды $\underset{\sim}{X}$ және $\underset{\sim}{Y}$ L және R функцияларында көрінетін $\underset{\sim}{X} = (m, \alpha, \beta)_{LR}$, $\underset{\sim}{Y} = (n, \gamma, \delta)_{LR}$ (осындағы m және n- $\underset{\sim}{X}$ және $\underset{\sim}{Y}$ АЕС орта мәндері $\alpha, \gamma,$ және β, δ- сәйкесінше $\underset{\sim}{X}$ және $\underset{\sim}{Y}$ анық емес сол және оң коэффициенттер).
$(m, \alpha, \beta)_{LR} + (n, \gamma, \delta)_{LR} = (m+n, \alpha+\gamma, \beta+\delta)_{LR}$; $-(m, \alpha, \beta)_{LR} = (-m, \alpha, \beta)_{LR}$; $(m, \alpha, \beta)_{LR} - (n, \gamma, \delta)_{LR} = (m-n, \alpha+\delta, \beta+\gamma)_{LR}$; $(m, \alpha, \beta)_{LR}(n, \gamma, \delta)_{LR} \approx (mn, \alpha n+\gamma m, \beta n+\delta m)_{LR}$, болғанда $\underset{\sim}{X} > 0, \underset{\sim}{Y} > 0$; $(m, \alpha, \beta)_{LR}(n, \gamma, \delta)_{LR} \approx (mn, \gamma m-\beta n, \delta m-\alpha n)_{LR}$, осындағы $\underset{\sim}{X} > 0, \underset{\sim}{Y} < 0$; $(m, \alpha, \beta)_{LR}(n, \gamma, \delta)_{LR} \approx (mn, \alpha n-\delta m, \beta n-\gamma m)_{LR}$, осындағы $\underset{\sim}{X} < 0, \underset{\sim}{Y} > 0$; $(m, \alpha, \beta)_{LR}$ $(n, \gamma, \delta)_{LR} \approx (mn, -\beta n-\delta m, -\alpha n-\gamma m)_{LR}$, осындағы $\underset{\sim}{X} < 0, \underset{\sim}{Y} < 0$; $(m, \alpha, \beta)^{-1}_{LR} \approx (1/m, \beta/m^2, \alpha/m^2)_{LR}$, болғанда $\underset{\sim}{X} > 0$; $(m, \alpha, \beta)LR : (n, \gamma, \delta)LR \approx (m/n, (\delta m + \alpha n)/n^2, (\gamma m + \beta n)/n^2)_{LR}$, осындағы $\underset{\sim}{X} > 0, \underset{\sim}{Y} > 0$ амалдарымен анықталады.Әдісті қалыпты, шығыңқы, унимодалды, шыдамды,үздіксіз және параметрлі АЕС өңдеу үшін қолдануға болады.

Арифметикалық амалдарды талдамалы орындау әдісі (АТО) [59] үздіксіз $\underset{\sim}{X}$ және $\underset{\sim}{Y}$ $V_X = \{x\}$ и $V_Y = \{y\}$, анықтау аймағы бар, осындағы V_X, $V_Y \subset R$және талдамалы ҚФ үшін қолданылады. $\underset{\sim}{Z}$ үшін анықтау аймағы $V_z = [min(x^\circ y^\circ, x^\circ y^*, x^* y^\circ, x^* y^*), max(x^\circ y^\circ, x^\circ y^*, x^* y^\circ, x^* y^*)] = [z^\circ, z^*]$,

осындағы $x^{\circ}=\min\limits_{x\in V_X} x, x^{*}=\max\limits_{x\in V_X} x,\ y^{\circ}=\min\limits_{y\in V_Y} y, y^{*}=\max\limits_{y\in V_Y} y,\quad z^{\circ}=\min\limits_{z\in V_Z} z,\ z^{*}=\max\limits_{z\in V_Z} z.$

Егер $z\in V_Z$, онда әрбір $x\in V_X' : V_X'=[\max(\min(z\circ y^{\circ}, z\circ y^{*}),\ x^{\circ}),\ \min(\max(z\circ y^{\circ}, z\circ y^{*}),\ x^{*})]$ үшін табуға болады, $y\in V_Y'$: $V_Y'=[\max(\min(z\circ x^{\circ}, z\circ x^{*}),\ y^{\circ}), \min(\max(z\circ x^{\circ},\ z\circ x^{*}),\ y^{*})]$,

$z=x*y,\ x=z\circ y,\ y=z\circ x,$ осындағы $\circ$ – $*$ шамамен кері амал.$*$. Осындағы $\mu_Z(z)=\max\limits_{x\in V_X'}(\mu_X(x)\,|\,\mu_X(x)=\mu_Y(z\circ x)),$ егер $\exists x:\mu_X(x)=\mu_Y(z\circ x)$ немесе $\mu_Z(z)=\min\limits^{(\max\limits_{x\in V_X}\mu_X(x),\max\limits_{y\in V_Y}\mu_Y(y)),}$ егер $\forall x:\ \mu_X(x)\neq\mu_Y(z\circ x).$ Әдіс қалыпты, субқалыпты, шығыңқы, унимодалды, шыдамды, үздіксіз және параметрлі АЕС үшін бағытталған.

Жергілікті максимумдар бойынша сызықты жуықтама әдісі (ЖМСЖ) [75], МК негізделген [76] және құрамына $\tilde{Z}=\tilde{X}\,\tilde{\circledast}\,\tilde{Y}$,рәсімдері енеді, осындағы $\forall x\in\tilde{X}$, $\forall y\in\tilde{Y}$ және $\forall z\in\tilde{Z}$ анық түрде $(x_i<x_{i+1},\ y_j<y_{j+1},\ z_k<z_{k+1})$, ал $\tilde{X}$, $\tilde{Y}$ және $\tilde{Z}$ бөлшектік-сызықтық функция ретінде ұсынылады, құрамында (мысалы, $\tilde{X}$ үшін) *n-1* сызықтық функцияларынан бастап $\mu_x(x)=f_i(x)=\mu_x(x_i)+((\mu_x(x_{i+1})-\mu_x(x_i))/(x_{i+1}-x_i))(x-x_i)$, $x\in[x_i,\ x_{i+1}]$, $\overline{1,n-1}$. *1-рәсім*.МК жүзеге асыру және $z_k^{(1)}<z_{k+1}^{(1)}$ қатынасы негізінде анықталады:

$\tilde{Z}^{(1)}=\{\mu_z(z_1^{(1)})/z_1^{(1)},\ \ldots,\ \mu_z(z_p^{(1)})/z_p^{(1)}\}=\bigcup_{i=1}^{n}\bigcup_{j=1}^{m}\{\max\limits_{(\forall\mu:\exists!\, z_{ij})}\min(\mu_x(x_i),\ \mu_y(y_j))/(x_i\,\circledast\, y_j)\}$, осындағы $z_{ij}=x_i\circledast y_j,\ p\le nm.$ *2-рәсім*.$\tilde{Z}^{(1)}$ мәні $\tilde{Z}^{(2)}$ формула бойынша жуықтатылады: $\tilde{Z}^{(1)}\approx\tilde{Z}^{(2)}=\{\mu_z(z_1^{(2)})/z_1^{(2)},\ \bigcup_{k=2}^{p-1}{}_{(\Omega=1)}\ \mu_z(z_k^{(1)})/z_k^{(1)},\ \mu_z(z_p^{(1)})/z_p^{(1)}\}$, осындағы $\Omega=1$ – жуықтау шарты ([75]қараңыз). *3-рәсім*.Егер $dim(\tilde{Z}^{(\gamma)})\neq dim(\tilde{Z}^{(\gamma+1)})(\gamma=1,2,\ldots)$ болса 2-рәсімді орындау арқылы $\tilde{Z}$ анықтау.Бұл әдісте 1-рәсім МК амалын, ал $dim(\tilde{Z}^{(1)})$нәтижедегі тасымалдаушылар санын анықтайды.Бұл әдіс полимодалды, үздіксіз және параметрлі кластардан басқа барлық АЕС кластары үшін қолданылуы мүмкін.

1.3Шабуылдарды табу жүйесі үшін сараптау әдісін бағалау

Сараптамалық бағалау(СБ) ережеге сәйкес құрамына тәуелсіз мамандар енетін сәйкес сарапшы топпен(СТ) жүргізіледі. Сараптама нәтижелерін жалпыландыру үшін сарапшының қалауын білдіретін параметрді қолдану қажеттігі туындайды. Параметр ретінде көпкритериалды есептерді шешуде

[77-82] және математикалық бағдарламалауда [83-85] кеңінен қолданылатын маңыздылық коэффициенті (МК) бола алады. СБ жүзеге асыру үшін МК қолдану мақсатында АЖ ауытқуларды анықтау есептерін шығарғанда сарапшылар қолданатын (вербалды немесе сандық) сапалық және сандық деп бөлінетін критерийлер басымдығын анықтауды қарастырамыз. Критерийлер басымдығын анықтаудың сапалық әдістеріне “Делфи” әдісін (ДӘ),саралау (СӘ), бинарлы (БӘ) және жиынтық салыстырулар (ЖС), реттеу (РӘ), артықшылықтар векторы (АВ), сонымен қоса кластерлі талдау (КТ) әдістерін жатқызады. Делфи әдісі [86] классикалық нұсқасында сарапшылар пайымдауларға баға беретін интербелсенді сауалнамаға жатқызылады. Бұл әдістің артықшылықтары ретінде беделді сарапшылардың пікірлерінің әсерін тигізбейтін анонимді және сараптама объектісі туралы білімді толықтыру,ал кері байланыс сарапшыларға өз пайымдарын түзетуге мүмкіндік береді.Сараптама бірнеше кезеңнен тұрады. Сарапшылар жеке сауалнама алады және талдаушы топ критерийге, медиана мен квартильге (СБ 25% олардан жоғары немсе төмен) олардан ең жоғары және ең төмен бағаны берген мамандарды анықтайды. Ары қарай орта баға және анонимді түрде ең жоғары және ең төмен бағаларға негіздемелер беріледі. Осыдан кейін СТ мүшелері өз көрсеткіштеріне түзетулер енгізеді және олар қайта сарапталады. Кезеңдер СБ қолайлы келісім негізінде жүргізіледі. Саралау әдісі (СӘ) [86] әдетте бірліктен бастап натурал сандар ұсынатын объектіні дәрежелер бойынша реттеу рәсімі болып табылады. объектілерге бірдей(байланысты) дәрежелер, объектілердің арифметикалық орта дәрежесі $z_{ср} = (z_1 + \ldots + z_k)/k$ болады, осындағы k –байланысты дәрежелер саны. Олар бөлшек сандар болуы мүмкін, ал барлық дәрежелердің қосындысы тұрақты және мәліметтерді ары қарай өңдеуді жеңілдететін 1-ден Zдейін натурал сандар қосындысымен - ең жоғары дәреже мәнімен(Альтернативті санына сәйкес) анықталады.Бинарлы әдіс(БӘ) [87] барлық мүмкін жұптарды салыстыру артықшылықтарын белгілеу рәсімінен тұрады. Сарапшы үшін саралаудан гөрі жұппен салыстыру жеңілірек, бірақ олар жиі өз пайымдарында бірізділік танытпайды. Жиынтық салыстырулар әдісі(ЖС) [86] бинарлық әдістен айырмашылығы сарапшыға жүйелі түрде маңыздылығына байланысты реттейтін немесе сараптама мақсаттарына байланысты кластарға бөлетін объектілердің жұптары емес, үштіктер, төрттіктер ұсынылады. Реттеу әдісі(РӘ) [83] көпкритериалды тапсырмаларда әртүрлі өлшемдегі критерийлер қолданылғанда, оларды салыстыру емес, реттеу қажет болғанда пайдаланылады. Әдебиеттен салыстыруды реттеу, орталандыруды реттеу, Савидж реттеуі т.б. белгілі. Артықшылықтар векторы (АВ)[87] әдісінде сарапшы $A \in \{a_i\}$, $i = \overline{1,n}$ Альтернативті жиынын талдайды және әрқайсысы үшін қандай екенін білдірместен бір-бірінен асатындардың санын анықтайды. Нәтижесінде олардың салыстырмалы артықшылығын сипаттайтын альтернативті үшін қалау векторын аламыз $\Pi \in \{\Pi_i\}$, $i = \overline{1,n}$. КТ әдістер класы [88] көп мөлшердегі критерийлер арқылы бағаланатын объектілердің көлемді ауқымымен жұмыс істеуге мүмкіндік береді. Әдістің

негізі іріктемені бөлшектеп байланыстыруға ішкі жиындардың әрқайсысы максималды ұқсас объектілерден, ал түрлі кластардың объектілері бір-бірінен максималды ерекшеленуге келеді. Сандық әдістер келесі топтарға бөлінеді: жұппен салыстыру (ЖС), дәрежелік түрлендірулер(ДТ), пайдалылық функциясын жуықтату (ПФЖ), жиілікті түрлендіру(ЖТ) және тепе-теңдік нүктесінен ауытқу (ТНА).

1.ЖСматрицаларын талдау әдістерінің класына ең кем шаршы(ЕКШ) және меншік векторлар әдістерінің тобы(МВӘ) енеді.

1.1.(ЕКШ) әдісі Марквардтың итеративті алгоритмі($\sum_{i=1}^{n}\sum_{j=1}^{n}(a_{ij} - \lambda_i/\lambda_j)^2 \rightarrow min$, осындағы n –параметрлер саны, λ_i / λ_j – жұппен салыстырудың нәтижесі ретінде МК қатынасы) бойынша оңтайландыру теңдеуінің шешімімен МК табуға негізделеді.

1.2.ВС әдістер тобы Уэй векторлары (УВ) әдісіне [89], Саати(СӘ) [90], Коггер және Ю (КЮ) [91], сонымен бірге фон Неймана-Моргенштерн әдісі (ФНМ)[86] және Юшманов(ЮӘ)[92].

1.2.1. Алғашқы шкаладан алынған ақпаратты өңдеу әдістеріне ПС матрицасы мәліметтеріне негізделген УВ[89] әдісі жатады. $A = \|a_{ij}\|$, $a_{ij} \in \{-1,0,1\}$, осындағы $a_{ij} = -1$ x_j над x_i,ден артықшылығын білдіреді, $a_{ij} = 0$ теңдігін, ал $a_{ij} = 1$ преимущество x_i x_j-ден артықшылығын білдіреді. Кері сандары бар матрица қолдануға ыңғайлы болғандықтан, Берж [93] оны $A^+ = \|a_{ij}^+\|$, $a_{ij} \in \{0,1,2\}$ түрлендірді, осындағы $\{0,1,2\}$ жоғарыда аталған мазмұнға ие. Әрбір санды қосқан кезде матрицаның әрбір жолында параметрлердің маңыздылығы туралы сандық сипаттамаларды аламыз, ал оларды жалпы қосындыға бөлсек параметрлердің салмақтық коэффициентін аламыз: $\lambda_{ij} = \sum_{j=1}^{n} a_{ij}^+ / \sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}^+$. Бұл формуланың МК анықтаудың жеткілікті түрде дөрекі анықтамасы кемшілігі болып табылады, өйткені “теңбе-тең” және “ұтылысты”салыстырулардың (Х параметрінің артықшылығы) маңыздылығы ескерілмейді. Кемшіліктердің өтемақысы ретінде Берж келесі итеративті үрдісті ұсынды: әрбір k қадамында $P^i(k)$ критерийінің маңыздылығы тең және қосарланған критерийлер үшін жоғары критерийлердің “қосындысы ” ретінде анықталады. Бұл жердегі $P^i(k) = P_1^i + \ldots + P_n^i$, осындағы $P_j^i(k)$ –ЖС матрицасының графикалық түсіндірілуі k жолының ұзындық саны, $i, j = \overline{1,n}$, осындағы n –критерийлер саны. Осылайша МК келесі формуламен анықталады:

$$P_k^i(k) = P^i(k) / (P^1(k) + \ldots + P^n(k)) \qquad (1.2)$$

1.2.2.МСТ негізі[90] параметрлердің салыстырмалы таразысын іздеу векторын- Саати векторын іздеуден тұрады. ЖС параметрлердің нәтижелері олардың МК қатынастарымен сипатталады $A = \left\| \lambda_i / \lambda_j \right\|, (i, j) \in \overline{1..n}$. Онда *(A–nE)* $\overline{\Lambda} = 0$, осындағы *E* –бірлік матрица; $\overline{\Lambda}$ – МК векторы, *n* –параметрлер саны[87] теңдеуі әділетті болады. $\overline{\Lambda}$ таразы векторын табу үшін бұл теңдікті шешу керек. Егер мтарица дәрежесі 1-ге тең болса, онда *n* – жалғыз жекеменшік саны және сәйкесінше $\lambda_1 + ... + \lambda_n = 1$ –теңдеудің нөлдік емес шешімі бар, бұл МК ізделінетін Саати векторы. Коэффициенттерді іздеудің басқа нұсқасы ретінде $\tilde{\lambda}_i = \sqrt[n]{a_{1j} ... a_{nj}}, i = \overline{1,n}$, формуласы бойынша есептеу және МК үшін $\lambda_1 + ... + \lambda_n = 1$ шарты реттелу үшін оны реттеу. Реттеу үшін $\lambda_i = \tilde{\lambda}_i / (\tilde{\lambda}_1 + ... + \tilde{\lambda}_n)$ рәсімі орындалады.

1.2.3.КЮ таразы векторы үшін $D^{-1} T \overline{\Delta} = \overline{\Delta}$ теңдігі ұсынылады, осындағы $T = \left\| t_{ij} \right\|, \; t_{ij} = a_{ij}$ яғни $i = j, t_{ij} = 0$ егер $i \neq j, D = \left\| d_{ij} \right\|$, $d_{ij} = n - i + 1$ онда $i = j$, $d_{ij} = 0$ егер $i \neq j$, *n* –параметрлер саны.

1.2.4. ФНМ әдісін жүзеге асыру үшін үш критерий жағдайын қарастырайық. Егер критерийлер $a_1 ... a_3$,болса, онда $a_1 > a_2 > a_3$.Бір критерийдің екіншісінен жоғары дәрежесін бағалау үшін объектілердің $\beta_1 ... \beta_3$ сандық бағаларын енгізеді. $\beta_3 = 1$ қабылданады және сарапшы $\alpha_1 \beta_1 = \beta_3$ и $\alpha_2 \beta_2 = \beta_3$ шартын қанағаттандыратын $\alpha_1 (0 < \alpha_1 < 1)$ және $\alpha_2 (0 < \alpha_2 < 1)$ мәндерін таңдайды. Ары қарай ол α_3 анықтайды, $\alpha_3 \beta_1 = \beta_2$.Оның бағалары егер $\alpha_3 = \alpha_1 / \alpha_2$ болса, онда келісілген болып саналады, керісінше жағдайда жаңа α_1 немесе α_2 алынады. Сарапшы белгілеген бағалардың жалпы саны $n(n - 1)/2$.

1.2.5. ЮӘ әдісі (“сүйеніш ағашы”) графтар теориясына және белгілі бинарлы әдістер үшін барлық салыстыруларды жайдақтау үшін іріктеу міндетті емес, дұрыс нөмірді анықтап, олардың оңтайлы жиынын таңдау жеткілікті болып табылады. Дұрыс нөмірлерді таңдау алгоритмі графтың еркін төбесінде *n* нөмірін қоюға негізделеді. Егер *k* төбесін *n* –нен *n-k+1*дейін нөмірленсе, онда нөмірі жоқ шектес төбені таңдаймыз да, оған *n-k* нөмірін береміз. Ары қарай тиімді A_n жиынын табамыз. $a_i > a_j$ A_n. арақатынасын орнату оңай болатын жұп таңдалады. Бір g_{ij} қабырғасынан тұратын $G(A_n)$ графы тұрғызылады.Әрбір келесі қадаммен барлық *a* жұптарының ішінен бірінің төбесі $G(A_n)$, екіншісі оған қатысты емес болса, онда арақатынас орнату жеңілірек болатын жұп таңдалады. Оны орнатып, графқа жаңа қабырға қосамыз. Егер $G(A_n)$ граф тұрғызумен қатар *n* –нен *1*дейін бағаланатын критерийлердің қайта жүзеге нөмір асырылса, онда бір мезетте дұрыс нөмір жүзеге асырылады.

2. ДТ әдістерінің класына орта әдіс (ОӘ) және (ДТ) әдістер тобы енеді.

2.1.ОӘ квалиметрия теориясынан[87], белгілі, онын негізіне белгілі бір дәрежеде рекуррент рәсіміне жақын сарапшылардың таразылап бағалау түсінігін енгізу жатады. Егер x_{ij} –i элементінің j сарапшы $i \in \overline{1,n}$, $j \in \overline{1,m}$ бағасы, осындағы nжәнеm –параметрлер менсәйкесінше сарапшылардың саны.Сол кезде топтық мәні сарапшылардың орта арифметикалық бағалаы ретінде анықталады, яғни $x_i = (x_{i1} + \ldots + x_{im})/m$. $x_i = (x_{i1} + \ldots + x_{im})/m$. x_i нақтырақ анықтау үшін рекуррент рәсімімен таразылап бағаланады: $x_i^t = \sum_{j=1}^{m} x_{ij} K_j^{t-1}$, $K_j^t = \sum_{i=1}^{n} x_{ij} x_i^t / \sum_{i=1}^{n} \sum_{j=1}^{m} x_{ij} x_i^t$, осындағы $K_j^0 = 1/m$. Есептеу $t = 1$және $t \to \infty$болғанда рекуррент рәсім жинақталатыны дәлелденді.Өзара бағаланатын элементтер тобын ретті бағалау жағдайында ғана бұл жағдай әділетті болып табылады. Жекелеген элементтердің реттелмеген немесе тәуелсіз бағалау жағдайында топтық мән рекуррент рәсімнен көрінеді: $x_i^t = \sum_{j=1}^{m} x_{ij} K_j^{t-1}$, $K_j^t = (1 - |x_{ij} x_i^t|^2) / \sum_{j=1}^{m} |x_{ij} x_i^t|^2$, $K_j^0 = 1/m$. 2.2.ДТ әдістер тобын біркелкі функциясы бар дәрежені жуықтату әдісі (БФДЖ), әдістердің ішкі тобы және сызықтық біріншілік жүйесінің параметрлерінің дәрежесін жуықтату деп бөлінеді.

2.2.1. БФДЖ әдістері дәрежелердің түрлі өзгерістеріне біртекті төмендейтін функцияның бүтін сандық аргументіне негізделеді.Келесі нұсқалары белгілі[86, 87]:

$$\lambda_i = \lambda_n + (n - i)(\lambda_1 - \lambda_n)/(n - 1), \quad \lambda_i = x(i) / \sum_{i=1}^{n} x_i$$

$$\lambda_i = 2[m(n+1)] - \sum_{k=1}^{n} r_{ik} / mn(n+1), \quad (1.3)$$

осындағы $x_i = i / 2^i - 1$ и ,

осындағы r_{ik} –i параметрінің k сарапшы тағайындаған дәрежесі;n, m – сәйкесінше параметрлер мен сарапшылар саны. 2.2.2. ДТЖ қосалқы әдістеріне Черчмен-Акоф әдісін (ЧА) және Подиновскийдің лексикографиясы (ПЛ) енеді. а) ЧА әдісі сарапшылардың бағаларын жүйелі түрде түзеуден тұрады [94]. Әрбір $x_i (i = \overline{1,n})$ альтернативті нақты $f(x_i)$ оң санына сәйкес қойылады, егер x_i x_{i+1}, альтернативті артық болса, онда $f(x_i) > f(x_{i+1})$, егер x_i және x_{i+1}тең болса,онда $f(x_i) = f(x_{i+1})$, ал егер $f(x_i)$ және $f(x_{i+1})$ үшін x_i және x_{i+1} альтернативтінің бағасы болса, онда $f(x_i) + f(x_{i+1})$ x_i және x_{i+1}альтернативті біріккен есебіне жауап береді. Альтернативті бағаларының қосылғыштығы туралы тұжырым ең маңыздысы болып табылады. ЧА әдісіне сәйкес $x_1, \ldots, x_n$ альтернативті артықшылықтарына байланысты сараланады. Осыдан x_1 альтернатив неғұрлым қалаулы, одан

кейін x_2 және т.с.с. деп шамалауға болады. Сарапшы әрбір альтернатив үшін алдын-ала $f(x_i)$ сандық бағаларын көрсетеді. Кейде неғұрлым басымдырақ болған альтернатив 1 бағасы қойылады, қалған бағалар маңыздылығына байланысты 0 мен 1 аралығында орналасады. Егер x_1 қолайлылығы кемдеу болса, онда бағаларды нақтылау үшін оны артықшылықтары бойынша $x_2,\ldots,x_n$ альтернативті қосындысымен салыстырады және т.с.с. x_1 альтернативті $x_2,\ldots,x_k$ ($k>2$дейін) салыстырғанда қолайлырақ болғанда ол қарастырудан алынады, ал x_1 орнына x_2 альтернативтінің бағасы қарастырылады және түзетіледі. Бұл үрдіс барлық альтернативті бағалары толық түзетілгенше жалғасады. б) ПЛ әдісі Нельсон идеясына негізделеді[95]. Маңыздылығы бойынша реттелген $(f_1,\ldots,f_n)$ параметрлері және келесі шарттардың бірі орындалғанда $X>Y$ болады[96, 97]: $f_1(x) > f_1(y)$ немесе $f_1(x) = f_1(y), f_2(x) > f_2(y)$ немесе $f_r(x) = f_r(y)$, $r = \overline{1,n}$, $f_n(x) > f_n(y)$. Қосылғыштық функция үшін $L(y) = \sum_{r=1}^{n} \lambda_r f_r(y)$ МК ретінде λ_n кез келген оң сан таңдалады, басқа λ_r коэффициенттер дәйекті түрде $\lambda_r \geq 1/\mu_r \sum_{i=r+1}^{n} \lambda_i M_i,$ шартында тағайындалады, осындағы $r = n-1, n-2,\ldots,2,1, 0 < \mu_r < \inf_{x,y\in X} |f_r(x) - f_r(y)|$ және $M_i > \max f_i(x) - \min f_i(x), x \in X$.МК еркін түрде көрсетілген теңсіздіктер шегінде таңдалады. Шерали [98] жұмысында лексикографиялық тұрғыдан реттелген критерийлері бар көпкритериалды тапсырмалардың шешімі жұмыста атап көрсетілген таразымен өлшенген сол тапсырмалардың критерийлерінің қосындысымен сәйкес келетіні дәлелденді. Альтернативті таразыларды табу тапсырмасының шешімі және өлшенген қосынды лексикографиялық оңтайландырудың неғұрлым нәтижелі шешімі екені дәлелденді.

3. АФП әдістер тобына Подиновскийдің жалпыланған критерийлер(ПЖК) және құндылық функциясы(ҚФ) әдістері енеді.

3.1.ПЖК әдістерінің құрамына қосылғыш түйіншек (ҚТ) әдісін және максминді түйіншек әдісі(МТ)кіреді.

3.1.1. ҚТ ішкі әдістерін пайдалылық функциясы қосылғыштық түрде ұсынылғанда $U(f_1(x),\ldots,f_n(x)) = \lambda_1 U_1(f_1(x_1)) + \ldots + \lambda_n U_n(f_n(x_n))$ қолдануға болады және дербестік аксиомалары[87] орындалса, яғни бір критерий бойынша төмен баға өзге критерийдің жоғары бағасымен орны толтырылады және бұл әділ шешім болып табылады. ҚТ ішкі әдістері тобын стратификация әдісіне(СТ) [87, 99],Юттлер(ЮТ) [100]және корреляциялық-регрессивті(КР) [101] деп бөледі. а) СТ әдісі тіпті лингвистикалық критерийлер кезінде де координаталық жазықтықтағы

деңгей(страта) іздерін анықтауға мүмкіндік береді. Әмбебап вербалды шкалалардың сандық шкалаға ауысып және Тангян алогритмін қолданып пайдалылық функциясы және барлық МК анықталады. Критерийлердің маңыздылығы туралы ақпаратқа вербалды түрде (*i* критерийі *j*-ге қарағанда маңыздырақ; *i* критерийі *j*-ге қарағанда біршама маңыздырақ; *i* критерийі *j*-ге қарағанда шамадан тыс маңыздырақ) салмақтық коэффициенті бар қосылғыштық түйіншектер сәйкесінше 2/3, 3/4 және 4/5. б) ЮТ әдісі (тиімді мәндерге жүгіну әдісі) ҚТ әдістер тобының ең қарапайым әдісі болып табылады. МК бойынша жекелеген критерийдің тиімді мәніне кері шамалар қолданылады.) КР әдісі сарапшының пікірінше басымдыққа ие көрсеткішті анықтаудан басталады. Ары қарай басым көрсеткішке қатысты $ln\,U(f(x_i)) = \lambda_1 ln\,x_1 + ... + \lambda_n ln\,x_n$, осындағы $U(f(x_i))$ – пайдалылық функциясы λ_i – МК, x_i – критерий ал *n* –критерийлер саны; регрессияны теңестіру (қосылғыштық түрі) жүргізіледі. Осындай ұстаным бойынша МК критерийлердің орташаршылық ауытқуларынан және жалпы нәтижеге тәуелді $\lambda_i = 0,5$ $\beta_i^2 / \sum_{i=1}^{n} \beta_i^2$, $\beta_i = b_i \sigma_{xi} / \sigma_r \beta$ регрессия коэффициенті арқылы анықталады. 3.1.2.МТ әдісі жиілік параметрлері логикалық түрде жұмаршақтанғанда қолданылады[102]. Қолайлы шешім ретінде минималды көбейтіндіден максималды алу $U(f_1(x),..., f_n(x)) = \min_{i=1..n}[\lambda_i f_i(x_i)]$, осындағы λ_i – МК, $f_i(x_i)$ – критерий ал *n* –критериейлер саны. Максминді көбейтіндіні табу амалы формалды түрде қалыптамалардың ұстаным бойынша көбейту амалына ұқсайды: жолды бағанға көбейтеміз.Бірақ қалыптама элементтерін көбейту амалының орнына сол элементтерден *min* табу амалы орындалады,содан кейін *min* элементтерінің ішінен ең үлкені табылады.

3.2.ҚФ әдістер тобы мультипликативтік функция (МФ) және Кини полиаддитивті түйіншегі (КПТ) бөлінеді.3.2.1.МФ әдістері [77] сипатталған. Мультипликативті пайдалылық функциясы пайдалылығы бойынша өзара тәуелсіз параметрлер, яғни критерийлердің біреуінің төмен бағасы пайдалылық мәнінің төмендеуіне әкеледі.

$$U(f_1(x),...,f_n(x)) = \prod_{i=1}^{n} [f_i(x_i))]^{\lambda_i}, \qquad (1.4)$$

Осындағы λ_i –параметрдің салмақтық коэффициенті. Бұл әдістің кемшілігі түйіншек барлық критерийлер жұппен тәуелсіз болғанда ғана әділ болады. 3.2.2. КПТ әдістері. Интервалдарға қатысты параметрлердің дербестігі жағдайында құндылық функциясы келесі түрге ие болады: $U(x) = a_0 + \sum_{i=1}^{n-1} \sum_{j>i}^{n} a_{ij} U_i(x_i) U_j(x_j)$

$$+ \sum_{i=1}^{n-2} \sum_{j>i}^{n-1} \sum_{k>j}^{n} a_{ijk} U_i(x_i) U_j(x_i) U_k(x_k) + a_{1,2...,n} U_1(x_1) U_2(x_2) ... U_n(x_n)$$

$$+\sum_{i=1}^{n-2}\sum_{j\succ i}^{n-1}\sum_{k\succ j}^{n} a_{ijk}U_i(x_i)U_j(x_i)U_k(x_k)+a_{1,2...,n}U_1(x_1)U_2(x_2)...U_n(x_n)$$

, осындағы n – параметрлер саны, $a_0, a_{ij}...a_{1,2...n}$ – алгебралық ауыр тілмен [77] сипатталған шкала константалары.

4.ТНА әдістерінің класы идеал нүктеден ауытқу (ИНА) және тепе-теңдік нүктесінен ауытқу(ТНА) әдістері тобына бөлінеді.

4.1. ИНА әдістер тобы Чарнс-Купер(ЧК) әдісіне, реттелген баспалдақты метрика(РБМ) және ортақ шешім ауытқу (ОША)әдісіне бөлінеді.

4.1.1.ЧК әдісін қолданғанда барлық параметрлер кейбір идеал нүктеге $в^* = (в_1^*, в_2^* ... в_n^*)$ дейінгі қарастырылатын бағаның арақашықтығы жалпыланған

$$\Phi = \sum_{i=1}^{n} a_i(f(x_i) - в_i^*)$$

Φ параметрінде түйіседі және жиі бұл .Ары қарай чарнс пен Купер сызықтық бағдарламалау тапсырмалары үшін стандартты симплекс әдісін қолданады[103].

4.1.2.РБМ әдістері. Целени [85] келесі метриканы қолданады:

$$L_p(x) = (\sum_{i=1}^{n}(\lambda_i \left| (x_i^* - x_i)/(x_i^* - x_{i\,max}) \right|)^p)^{1/p} \qquad (1.5)$$

,

осындағы x_i^* –i параметрінің тиімді мәні $x_{i\,max}$ – i параметрінің максималды мүмкін мәні λ_i – МК және $1 \le p < \infty$ –кеңістік параметрі.

4.1.3.ОША әдісі $\max\limits_{x\in V} k_i(x) = k_i(x) = k_i^*$, $i \in \overline{1..n}$, $\min\limits_{x\in V}[y, k_i^* - k_i(x)] \le y/x$ түріндегі көпкритериалды тапсырмаларды ортақ шешу рәсімінде орындалады. МК $\lambda_i = 1/(k_i^* - k_i)$, $i \in \overline{1..n}$, $k_i^* = \min\limits_i k_i(x)$, осындағы n – критериейлер саны, теңдіктерімен анықталады. Тиімділік критерийі ымыраның [77] азаюына әкеледі. 4.2.ТНА әдістер тобы (статус-кво) тепе-теңдік нүктесінен түрлі ауытқуларды қолданады және ойындардың кооператив теориясының (ОКТ) әдісі мен ойындық-теориялық (ОТ) модельді қолданады.

4.2.1.ОКТ әдісін Сцидаровский[104] сипаттаған және мына ауытқуды қолданады:

$$g(x) = [x_1 - x_1^*]^{\alpha_1} ... [x_n - x_n^*]^{\alpha_n}, \qquad (1.6)$$

осында x_i^* $(i = \overline{1,n})$ –i параметрінің тепе-теңдік нүктесіндегі мәні, n – сарапшылар саны.

4.2.2.ОТ моделінде [83] келістірілген нұсқа тапсырмалар жиының шығыңқы қолайлы әдіспен ізделеді: $C_i^T \times x \to max$, осында $i = 1,2,...,n$, $Ax \le B$, $x \ge 0$, $x = \lambda_1 x_1 + ... + \lambda_n x_n$, болғанда $\lambda_1 + ... + \lambda_n = 1, \lambda \succ 0$.

5.НС әдістер тобы артықшылықтар әдісіне(АӘ), класқа қатыстылық(КҚ)әдісі және кездейсоқ векторлар(КВ)әдісіне бөлінеді.
5.1.АӘ тобы Терстоун(ТРС) әдісіне және шешім қабылдайтын тұлғаның қалауы әдісіне(ШҚТҚ) жіктеледі.

5.1.1.ТРС әдісі [105] келесі алгоритммен ұсынылған: x_i параметрі x_j параметріне қарағанда (*A* қалыптамасы) маңыздырақ болғандағы жағдайларға кесте құрылады. Ары қарай x_i параметрі x_j параметріне қарағанда маңыздырақ болатын жағдайлардың (қалыптама $P = \|p_{ij}\|$, осындағы $p_{ij} = a_{ij} / m$, яғни *m* –сарапшылар саны). пайыздық үлесін анықтау үшін *P* матрицасы құрылады. *Z* матрицасы $Pв$ матрицасының $Zв$ элементтерін өзгерістің стандартты өлшеуіштеріне айналдыру үшін қолданылады: $P_{ij} = G(z_{ij}) = \int_{-\infty}^{x_{ij}} 1/\sqrt{2\pi} \times \ell^{-x^2/2} dz$. Ары қарай $z_i : z_i = z_{i1} + \ldots + z_{in}; \overline{z_i} = (z_i + \ldots + z_n)/n$ есептеледі: осындағы *n* –параметрлер саны. Ең соңында $\overline{z_i}$ МК мәніне сәйкес қалыпты аудан бөлінісінің пайызына айналдыратын қалыпты бөліністі кестесін қолдану арқылы айналады. Ең қолайлысы 11дәрежеге бөлінген дұрыс екенін ескерген жөн.
5.1.2.ШҚТҚ [106]әдісі Терстоун формализмін қолданады және бастапқы ақпаратты алумен, яғни *A*және *P* матрицаларын қалыптастырумен ерекшеленеді.
5.2.КҚ әдісі (Рознер әдісі[107]). Сарапшыға *n*-реттік параметрлерді көрсету арқылы *M* ұяшықтарының біріне қатысты шартты ықтималдық қалыптамасы түзіледі $P_i(k)$, осындағы $k = \overline{1,M}$.Таразыны анықтау үшін $(\lambda_i - \lambda_j)^2 = f(p_i(k), p_j(k))$ арақатынасы қолданылады. Параметрлер арасындағы орта шкаладік айырмашылықтар қосындысында параметрлердің шкаладенген таразы шамасын құрайды.
5.3.КВ әдісі(рандомизация) [91].Таразы мүмкін мәндердің соңғы жиынтығын қабылдайды $\lambda_i \in R_N = \{0,1/N,\ldots,N-1/N,1\}$, осындағы λ_i – МК, *N* – берілген натурал сан, *N*>*n*, осындағы *n* –параметрлер саны.Жалпы саны L ықтимал n-өлшемді кездейсоқ вектордың соңғы іске асырудың жалпы саны $P = (N + n - 1)$.Таразы векторы Дирихле бөлінісіне тәуелді $(\lambda_i,\ldots,\lambda_n) \in Д(\alpha_i',\ldots,\alpha_n')$, ал бөлініс тығыздығы $f(\lambda_i,\ldots,\lambda_n) = \Gamma(\alpha_i',\ldots,\alpha_n') \prod_{i=1}^{n} p_i^{\alpha_i - 1} / \Gamma(\alpha_i')$. Кез –келген $k \le n$ үшін таразы векторы кездейсоқ шамада бөлінгенге дейін функцияда тоғысады, $y_i,\ldots,y_k$, $(\lambda_i,\ldots,\lambda_k) \to (y_1,\ldots,y_k)$, яғни $y_1,\ldots,y_k, (1 - (y_1 +$

$...+y_k))\in Д(1,...,n-k)$.КВ сәйкес стандарт ауытқуларды МК анықтау мәндері 0-ден 1-ге дейін аралықта өзгеретін әдісті жатқызады.

Бірінші тарау бойынша тұжырым

1.Шабуылдарды анықтауға арналған теориялық және практикалық қордың қазіргі жағдайына жүргізілген сараптама олардың негізгі бөлігі табудың сигнатуралық технологияларына бағытталғанын, ал ауытқымалы ШТЖ әдетте белгілі кемшіліктерге жол беретін статистикалық ұстанымдарға негізделетінін көрсетті.Бұдан бөлек ауытқымалы түрді анықтау құралдары жүйедегі қалыпты белсенділікті қалыптастыруға бағытталған және бұл ауытқымалы бейнеге қарағанда біршама жоғары айнымалылар мен жағдайлардың кең диапазонын ескеру қажеттігін туындатады.Бұл жүйені баптауда, әсіресе қоршаған ортаны бейнелейтін анық емес және әлсіз қалыптастыру болса сезілетін айтарлықтай қиындықтарға әкеледі.Компьютерлік жүйелер мен желілердегі шабуылдарды анықтаудың қазіргі заманғы жүйесі анық емес әлсіз қалыптастырылған ортада сигнатуралық емес және кибершабуылдардың жаңа түрін анықтау мүмкіндіктеріне қатысты өзінің жетілдірілмегендігін көрсетті.

2.Қатыстылық функциясын қалыптастыру әдістеріне, анық емес арифметика амалдарын жүзеге асыру және анық емес сандардың түрлі кластарын өңдеу критерийлерін анық емес шамаларды салыстыру әдістерін және компьютерлік жүйелер мен желілердің сәйкес қорғау құралдарын өңдеу үшін көрсетілген әдістерді нәтижелі қолдану мақсатында қолданылатын бастапқы деректерге сараптама жүргізілді. Шабуылдаушы іс-әрекет тудырған ауытқушылықтарды анықтау құралдарын құру үшін анық емес жиындардың модельлер мен әдістерін қолдану бар шабуылдарды анықтау жүйесін жетілдіруге және қоршаған ортадағы белсенділікті бақылау арқылы қауіпті ауытқушылық жағдайын анықтауға мүмкіндік береді.

3.Ауытқуларды анықтауға және сарапшылық ұстанымды қолдануға бағытталған жүйе мен әдістерді нәтижелі жүзеге асыруға үшін сарапшының көзқарасын білдіретін пайымдарды ескерген жөн. Бұл үшін ең ұтымды тәсіл маңыздылық коэффициенттерін анықтау әдістері болып табылады.Сапалық және сандық әдістердің кең спектрін негізге ала отырып, шабуылдарды анықтау жүйесін құру мүмкіндігін қолдану үшін олардың сараптамасы жүргізілді. Зерттеулер олардың күрделі көпкритериалды тапсырмаларды шешуде қолданыла алатынын, бірақ ауытқуларды анықтау тапсырмаларын шешуде нәтижелі қолдану үшін таңдау процессі сәйкес зерттеулер арқылы анықталатын критерийлер қатарынан тұрады.

2 КОМПЬЮТЕРЛІК ЖҮЙЕЛЕРДЕГІ ШАБУЫЛДАРДЫ ТАБУ ЖҮЙЕСІНДЕГІ АУЫТҚУШЫЛЫҚ ЖАҒДАЙЫН АНЫҚТАУ МОДЕЛЬДЕРІҢ ҚҰРУ

АЖР -на рұқсат етілмеген ықпал олардың қоршаған ортасына әсер етеді және оның бойында белгілі ауытқушылықтар тудырады.Осындай орта әдетте әлсіз қалыптастырылған (формализацияланған), айқындалмаған және осы ортада ауытқушылық тудырған шабуылдарды анықтау үшін қажет шамалар жиынын айқындау қажет. [2, 8, 28, 109] жұмыстарында осындай тапсырмалардың шешімін табу үшін анық емес жиындардың математикалық аппаратын қолдану тиімділігі көрсетілген, ал оны қажет шамаларды оңтайлы қалыптастыруға арналған ұстанымды қалыптастыру үшін қолдану жетілдірілетін ШТЖ тиімділігін жоғарылатуға мүмкіндік береді. Осыған байланысты қоршаған ортаны сипаттайтын шамалардың ауытқушылық жағдайы бойынша(мысалы, желілік трафиктердің) анықталатын шабуылдарды айқындауды жүзеге асыратын тиімді жұмыс істейтін жүйелерді жинақтауға (синтездеуге) мүмкіндік беретін математикалық моделдерді дамытамыз. Осындай орта ретінде АЖ үрдісіндегі ауытқушылық жағдайын анықтау мақсатында қалыптасқан айнымалылар жиынтығын(мысалы, сұранысты өңдеу уақыты, процессордың жүктемелілігі, ресурстарға жүгіну саны, қосылулар саны және т.б.) бағалауда қолдануға болады.

Қойылған тапсырманы шешу үшін 3 негізгі модель- базалық шамалар моделі(БШМ) [4], эталон шамасының моделі(ЭШМ) [5] және шешуші ережелер моделі(ШЕМ) [15].

2.1 Қоршаған ортаның жағдайын ауытқымалығын бақылау үшін базалық шамалар моделі

Базалық шамалар моделін құру қоршаған ортаның жағдайын сипаттайтын екі жиынға[4] - АЖР мүмкін шабуылдар жиыны (intrusion) ***I***

$$\boldsymbol{I}=\bigcup_{i=1}^{n} I_i = \{I_1, I_2, I_3, \ldots, I_n\}, \ (i=\overline{1,n}) \tag{2.1}$$

және мүмкін шамалар жиынына (value) ***V*** негізделеді.

$$\boldsymbol{V}=\bigcup_{i=1}^{m} V_i = \{V_1, V_2, V_3, \ldots, V_m\}, \ (i=\overline{1,m}) \tag{2.2}$$

(2.2) өрнегіндегі шамалар мәндерінен (2.1) ***I*** жиынының нақты элементі туындатқан АЖ-дегі ауытқушылық жағдайларын анықтауға болады, осындағы *n*–мүмкін шабуылдарсаны, ал *m*- мүмкін шамалардың жалпы саны.

Мысалы, *n=3* (2.1)болғанда:

$$\boldsymbol{I}=\bigcup_{i=1}^{3} I_i = \{I_1, I_2, I_3\}=\{SCANNING, DOS, SPOOFING\}, \tag{2.3}$$

осындағы $I_1=SCANNING$, $I_2=DOS$ және $I_3=SPOOFING$ сәйкесінше шабуылдар идентификациялау болып табылады:

- «Scanning of ports (*SCANNING*)» – « Порттарды сканерлеу»,
- «Denial of service (*DOS*)» – «Қызмет көрсетуден бас тарту»
- «Spoofing (*SPOOFING*)» –«Алмастыру (Спуфинг)».

Мысалы, *m=6* өрнегінде (2.2):

$$\boldsymbol{V}=\bigcup_{i=1}^{6} V_i = \{V_1, V_2, V_3, V_4, V_5, V_6\} = \{NVC, VCA, NCC, SPR, DBR, NPSA\} \quad (2.4)$$

осындағы $V_1=NVC$, $V_2=VCA$, $V_3=NCC$, $V_4=SPR$, $V_5=DBR$, және $V_6=NPSA$ сәйкесінше шамалар идентификациялау болып табылады:

- «Numbers of Virtual channels (*NVC*)» – «Виртуал арналар саны»,
- «Virtual ChannelAge(*VCA*)» – «Виртуал арнаның жасы»,
- «Number of concurrent connections to the server(*NCC*)» – «Бір мезеттегі серверге қосылулар саны»,
- «Speed of processing requests from the clients (*SPR*)» – «Клиенттердің сұранысын өңдеу»,
- «The delay between requests from the single user (*DBR*)»–«Бір қолданушының сұраныстарының арасындағы кідіріс»,
- «Number of packages with the same sender and receiver address (*NPSA*)» – «Бірдей мекен жайы бар жөнелтуші мен алушының пакеттер саны».

I жиынының әрбір элементіне (шабуыл түріне) $\boldsymbol{V_n}$шамаларының (ауытқушылықтарды анықтауға қажет) ішкі жиыны идентификациялауды. Осылайша, «шабуыл **:** шамалар» жұптар жиыны қалыптасады, яғни:

$$\boldsymbol{I: V_n}=\bigcup_{i=1}^{n}\left(I_i : \bigcup_{j=1}^{k_i} V_{ij}\right)=\{(I_1:\{V_{11}, V_{12}, \ldots, V_{1k_1}\}), (I_2:\{V_{21}, V_{22}, \ldots, V_{2k_2}\}), (I_3:\{V_{31}, V_{32}, \ldots, V_{3k_3}\}), \ldots, (I_n:\{V_{n1}, V_{n2}, \ldots, V_{nk_n}\})\}, \ (i=\overline{1,n}, \ j=\overline{1,k_i}) \quad (2.5)$$

Мысалы,егер $k_1=k_3=2$, және $k_2=3$,(2.3) формуласы арқылы $V_{11}=V_1$, $V_{12}=V_2$, $V_{21}=V_3$, $V_{22}=V_4$, $V_{23}=V_5$, $V_{31}=V_3$, және $V_{32}=V_6$ екенін анықтаймыз және сол кезде (2.5) өрнегі (2.4) формуласын ескере отырып келесі түрге ие болады:

$$\boldsymbol{I: V_n}=\bigcup_{i=1}^{3}\left(I_i : \bigcup_{j=1}^{k_i} V_{ij}\right)=\{(I_1:\{V_1, V_2\}), (I_2:\{V_3, V_4, V_5\}), (I_3:\{V_3, V_6\})\}=$$
$$\{(SCANNING:\{NVC, VCA\}), (DOS:\{NCC, SPR, DBR\}), (SPOOFING:\{NCC, NPSA\})\}. \quad (2.6)$$

Әрбір V_{ij} ([24] есепке ала отырып) әрқайсысы кортежбен лингвистикалық айнымалыларды (ЛА) көрсеткен ыңғайлы:

$$<V_{ij}, T_{ij}, U_{ij}> \ (i=\overline{1,n}, \ j=\overline{1,k_i}), \quad (2.7)$$

осындағы V_{ij}ЛА иницализациялау (атауы), T_{ij} – базалық терм-жиын (құрамында T_{ij}^{k} $(k=\overline{1,r})$ термдері бар, U_{ij} –T_{ij} үшін анықталу облысы болып табылатын әмбебап жиын.*m* және V_{ij} шабуылды жүзеге асырудың

ерекшеліктеріне және белгілердің санына байланысты анықталып, ақпараттық жүйенің қоршаған ортасындағы ауытқушылық жағдайы анықталады.

Мысалы (2.6) және (2.7) өрнектерін ескере келе ЛА көрсететін шеру жиыны :

V_{11}жәнеV_{12}<V_{11}, T_{11}, U_{11}>, <V_{12}, T_{12}, U_{12}>*түрге ие*,

яғни<*NVC*, T_{NVC}, U_{NVC}>, <*VCA*, T_{VCA}, U_{VCA}>;

V_{21}, V_{22}және V_{23}– <V_{21}, T_{21}, U_{21}>, <V_{22}, T_{22}, U_{22}>, <V_{23}, T_{23}, U_{23}>,

яғни<*NCC*, T_{NCC}, U_{NCC}>, <*SPR*, T_{SPR}, U_{SPR}>, <*DBR*, T_{DBR}, U_{DBR}>;

V_{31}жәнеV_{32}– <V_{31}, T_{31}, U_{31}>, <V_{32}, T_{32}, U_{32}>,

яғни<*NCC*, T_{NCC}, U_{NCC}>, <*NPSA*, T_{NPSA}, U_{NPSA}>.

Ары қарай әрбір ЛА үшін анық емес термдердің *r* қалыптасады:

$$T_{ij}=\bigcup_{k=1}^{r}T_{ij}^{k}=\{T_{ij}^{1},\ T_{ij}^{2},\ T_{ij}^{3},\ ...,\ T_{ij}^{k}\},\ (k=\overline{1,r}). \quad (2.8)$$

Олар $[V_{ij}^{min},\ V_{ij}^{max}]$ анықталу аймағы бар әмбебап U_{ij}жиынына әсер етеді, осындағы V_{ij}^{min} және V_{ij}^{max} сәйкесінше T_{ij} мәндерінің төменгі және жоғарғы шекаралары болып табылады.Мысалы, егер ЛА V_{11}бес терм арқылы анықталса *(r=5)*, ал V_{12} үш (*r=3),* онда (2.8) өрнегін ескере отырып, V_{11}үшін базалық терм-жиын:

$$T_{11}=\bigcup_{k=1}^{5}T_{11}^{k}=\{T_{11}^{1},\ T_{11}^{2},\ T_{11}^{3},\ T_{11}^{4},\ T_{11}^{5}\}=$$
$$\{T_{NVC}^{1},\ T_{NVC}^{2},\ T_{NVC}^{3},\ T_{NVC}^{4},\ T_{NVC}^{5}\}=$$
$$\{\text{«Very small» (VS), «Small» (S), «Average» (A), «Big» (B), «Very big» (VB)}\} \quad (2.9)$$

ретінде анықталады және әмбебап U_{ij} жиынында анықталу облысы $[V_{11}^{min},\ V_{11}^{max}]=[0,\ 256]$, осындағы$T_{11}^{1}=T_{NVC}^{1}=$«*VS*», $T_{11}^{2}=T_{NVC}^{2}=$«*S*», $T_{11}^{3}=T_{NVC}^{3}=$«*A*» ,$T_{11}^{4}=T_{NVC}^{4}=$«*B*»және$T_{11}^{5}=T_{NVC}^{5}=$«*VB*» сәйкесінше инициализациялау болып табылады:

- «Very small (*VS*)» – «Өте аз»,
- «Small (*S*)» – «Аз»,
- «Average (*A*)» – «Орташа»,
- «Big (*B*)» – «Үлкен»,
- «Very big (*VB*)» – «Өте үлкен»,
- ал V_{12}үшін:

$$T_{12}=\bigcup_{k=1}^{3}T_{12}^{k}=\{T_{12}^{1},\ T_{12}^{2},\ T_{12}^{3}\}=\{T_{VCA}^{1},\ T_{VCA}^{2},\ T_{VCA}^{3}\}=\{\text{«Young» (Y), «Average» (A), «Old» (O)}\}, \quad (2.10)$$

ретінде анықталады және әмбебап U_{ij}жиынында анықталу облысы $[V_{12}^{min},\ V_{12}^{max}]=[0,\ 250]$ болып табылады,осындағы$T_{12}^{1}=T_{VCA}^{1}=$«*Y*», $T_{12}^{2}=T_{VCA}^{2}=$«*A*»және $T_{12}^{3}=T_{VCA}^{3}=$«*O*» сәйкесінше инициализациялау болып табылады:

- «Young (*Y*)» –«Жас »,
- «Average (*A*)» –«Орташа»,

- «Old (*O*)»– «Кәрі ».

$T_{ij}(i=\overline{1,n},\ j=\overline{1,m})$термдер жиыны *r* анық емес сандардан(АЕС) көрінеді

$$T_{ij}\in\bigcup_{f=1}^{r}\tilde{T}_{ij}^{f}=\{\tilde{T}_{ij}^{1},\ \tilde{T}_{ij}^{2},\ \tilde{T}_{ij}^{3},\ \ldots,\ \tilde{T}_{ij}^{r}\},\ (f=\overline{1,r}) \qquad (2.11)$$

олар үшін ҚФ белгілі әдістердің бірімен қалыптастыру керек [109].

Мысалы, T_{11} термі *(r=5 болғанда)*және T_{12}(*r=3 болғанда*) (2.10) және (2.11) формулаларын ескере отырып сәйкес АЕС анықтауға болады

$\tilde{T}_{11}^{1}, \tilde{T}_{11}^{2}, \tilde{T}_{11}^{3}, \tilde{T}_{11}^{4}, \tilde{T}_{11}^{5}$ (т.е. $\tilde{VS}, \tilde{S}, \tilde{A}, \tilde{B}, \tilde{VB}$) және

$\tilde{T}_{12}^{1}, \tilde{T}_{12}^{2}, \tilde{T}_{12}^{3}$ (т.е. $\tilde{Y}, \tilde{A}, \tilde{O}$), ҚФ қалыптасады.

ҚФ алу үшін, мысалы, статистикалық мәліметтерді қолдана отырып Лингвистикалық термдер әдісі (ЛТСМҚ) (1.2. п.қараңыз) [28] арқылы интервалдардың *l* нөмірлерін V_{ij}^{min} мен V_{ij}^{max} сәйкес шекара шамалары болып табылатын $N_{ij}^{1}, N_{ij}^{2}, \ldots, N_{ij}^{l}$ мүмкін мәндері қолданылады.Бұл жерде шамалардың ауытқушылық ортада ағымдағы жағдайын жіктеу жүзеге асатын анық емес эталондардың (АЕЭ), яғни шама эталондарының құруға бастапқы дерек ретінде статистикалық, талдаушылық, сарапшылық және басқа ақпарат қолданылуы мүмкін.

Мысалы , T_{11}*l=5* болғанда T_{11} үшін $N_{1j}^{1}=N_{11}^{1}$, $N_{1j}^{2}=N_{11}^{2}$, $N_{1j}^{3}=N_{11}^{3}$, $N_{1j}^{4}=N_{11}^{4}$, $N_{1j}^{5}=N_{11}^{5}$ нөмірлеріне $[V_{11}^{min}=V_{11}^{0}, V_{11}^{1}],]V_{11}^{1}, V_{11}^{2}],]V_{11}^{2}, V_{11}^{3}], \ldots,]V_{11}^{4}, V_{11}^{5}=V_{11}^{max}]$ яғни *[0; 2],]2; 8],]8; 16],]16; 64],]64; 256]* сәйкес келеді, ал *l=3* болғанда T_{12}үшін $N_{1j}^{1}=N_{12}^{1}$, $N_{1j}^{2}=N_{12}^{2}$, $N_{1j}^{3}=N_{12}^{3}$ нөмірлерінің интервалдары $[V_{12}^{min}=V_{12}^{0}, V_{12}^{1}],]V_{12}^{1}, V_{12}^{2}],]V_{12}^{2}, V_{12}^{3}=V_{12}^{max}]$ яғни *[0; 30],]30; 100],]100; 250]* сәйкес келеді.

АЕС ҚФ алынған мәндерінің негізінде әрбір V_{ij} үшін $\tilde{T}_{ij}^{f}$ $(f=\overline{1,r})$ $\tilde{T}_{ij}^{ef}$ ($f=\overline{1,r}$, $i=\overline{1,n}$, $j=\overline{1,m}$), АЕС белгілі класының ұстанымы бойынша қалыптылық, модальді, үздіксіздік және параметрлік [28] белгілерінің негізінде шамаларының эталондары қалыптасады.

Мысалы, V_{11}=*NVC*және V_{12}=*VCA*үшін $\tilde{T}_{11}^{ef}=\tilde{T}_{NVC}^{ef}$, $(f=\overline{1,5})$ және $\tilde{T}_{12}^{ef}=\tilde{T}_{VCA}^{ef}$, $(f=\overline{1,3})$мәндері қалыпты, унимодалды, шығыңқы, дисскретті, еркін тасымалдаушылар саны бар параметрлі емес [28], яғни

$\tilde{T}_{11}^{e1}=\tilde{T}_{NVC}^{e1}=\tilde{VS}^{e}$={0/0,008; 1/0,008; 0,33/0,031; 0/0,063},

$\underset{\sim}{T}_{11}^{e2} = \underset{\sim}{T}_{NVC}^{e2} = \underset{\sim}{S}^{e} = \{0/0{,}008;\ 0{,}5/0{,}008;\ 1/0{,}031;\ 0{,}5/0{,}063;\ 0/0{,}25\},$

$\underset{\sim}{T}_{11}^{e3} = \underset{\sim}{T}_{NVC}^{e3} = \underset{\sim}{A}^{e} = \{0/0{,}008;\ 0{,}33/0{,}031;\ 1/0{,}063;\ 0{,}67/0{,}25;\ 0/1\},$

$\underset{\sim}{T}_{11}^{e4} = \underset{\sim}{T}_{NVC}^{e4} = \underset{\sim}{B}^{e} = \{0/0{,}063;\ 1/0{,}25;\ 0{,}75/1;\ 0/1\},$

$\underset{\sim}{T}_{11}^{e5} = \underset{\sim}{T}_{NVC}^{e5} = \underset{\sim}{VB}^{e} = \{0/0{,}063;\ 0{,}2/0{,}25;\ 1/1;\ 0/1\}$

және сәйкесінше

$\underset{\sim}{T}_{12}^{e1} = \underset{\sim}{T}_{VCA}^{e1} = \underset{\sim}{Y}^{e} = \{1/0;\ 1/0{,}12;\ 0{,}5/0{,}4;\ 0{,}25/1\},$

$\underset{\sim}{T}_{12}^{e2} = \underset{\sim}{T}_{VCA}^{e2} = \underset{\sim}{A}^{e} = \{0{,}2/0;\ 0{,}2/0{,}12;\ 1/0{,}4;\ 0{,}4/1\},$

$\underset{\sim}{T}_{12}^{e3} = \underset{\sim}{T}_{VCA}^{e3} = \underset{\sim}{O}^{e} = \{0/0{,}12;\ 0{,}17/0{,}4;\ 1/1\}.$

ретінде анықталуы мүмкін.

Орта жағдайы шабуылды жүзеге асыру үрдісіне тән екендігі туралы шешімді түйіндес жұптар(matched pair) ***MP*** жиыны негізінде іске асыру қолайлы болып табылады, жиын төмендегідей белгіленеді:

$$\begin{gathered}\boldsymbol{MP}=\bigcup_{i=1}^{n}\left(\bigcup_{j=1}^{c_n} MP_{ij}\right) = \{(\boldsymbol{MP_1}), (\boldsymbol{MP_2}), (\boldsymbol{MP_3}), \ldots, (\boldsymbol{MP_n})\} = \\ \{(MP_{11}, MP_{12}, MP_{13}, \ldots, MP_{1c_1}), (MP_{21}, MP_{22}, MP_{23}, \ldots, MP_{2c_2}), \\ (MP_{31}, MP_{32}, MP_{33}, \ldots, MP_{3c_3}), \ldots, \\ (MP_{n1}, MP_{n2}, MP_{n3}, \ldots, MP_{nc_n})\},\ (i=\overline{1,n},\ j=\overline{1,c_n}),\end{gathered} \tag{2.12}$$

осындағы c_n– *n*-шабуылды анықтауға бағытталған ережелерді құруға қажет жиындағы түйіндес жұптар саны. ***I*** элементі ***MP*** бірге жұптар жиынын қалыптастыруы мүмкін – «шабуыл **:** түйіндес жұптар жиыны»:

$$\begin{gathered}\boldsymbol{I:MP}=\left(\bigcup_{i=1}^{n} I_i : \bigcup_{j=1}^{c_i} MP_{ij}\right) = \{(I_1:\boldsymbol{MP_1}), (I_2:\boldsymbol{MP_2}), (I_3:\boldsymbol{MP_3}), \ldots, (I_n:\boldsymbol{MP_n})\} = \\ \{(I_1:\{MP_{11}, MP_{12}, MP_{13}, \ldots, MP_{1c_1}\}), (I_2:\{MP_{21}, MP_{22}, MP_{23}, \ldots, MP_{2c_2}\}), \\ (I_3:\{MP_{31}, MP_{32}, MP_{33}, \ldots, MP_{3c_3}\}), \ldots, \\ (I_n:\{MP_{n1}, MP_{n2}, MP_{n3}, \ldots, MP_{nc_n}\})\}.\end{gathered} \tag{2.13}$$

Мысалы, егер $c_1=c_2=c_3=5$ болса, [7] ескере отырып (2.13)өрнегі келесі түрге енуі мүмкін:

$$\boldsymbol{I: MP}=(I_1\rightarrow\{MP_{11}, MP_{12}, \ldots, MP_{15}\}), \ldots, (I_3\rightarrow\{MP_{31}, MP_{32}, \ldots, MP_{35}\}) \tag{2.14}$$

MPжиынының негізінде «Егер MP_{ij} тболса, онда …» түріндегі логикалық ережелер құрылады және мысалы (2.14) өрнегі үшін олар келесі түрге ие болады:

1. Егер MP_{11} болса, онда сканерлеу мүмкіндігі LOW (Т);
2. Егер MP_{12} болса, онда сканерлеу мүмкіндігі LTH (ЖҚТ);
3. Егер MP_{13} болса,онда сканерлеу мүмкіндігі HTTL(ТҚЖ);
4. Егер MP_{14}болса, ондасканерлеу мүмкіндігі H (Ж);
5. Егер MP_{15} болса, онда сканерлеу мүмкіндігі LIM(Ш),

осындағы L-LOW (төмен), LTH-LOWER THAN HIGH (жоғарыға қарағанда төмен), HTTL-HIGHER THAN THE LOWEST (төменгеқарағандажоғары), H-HIGH (жоғары), LIM-LIMITS (шекті), ал түйіндес жұптарда қолданылатын «шамалас» ұғымы қолданылатын шамалардың мәндерінің арасындағы Хемминг минималды арақашықтығын [109] көрсетуі мүмкін. Осылайша, ықтимал шабуыллер мен шамалардың мүмкін жиындарына негізделетін ұсынылған шамалар моделіне, сонымен қатар «шабуыл **:** шамалар» және «шабуыл **:** түіндес жұптар жиыны»жұптар жиынында ақпараттық жүйедегі шамалардың ауытқушылық жағдайын анықтауға арналған сәйкес құралдардың нәтижелелігін жоғарылатуға мүмкіндік беретін (шабуылдардың) анықтау жүйесінің моделін құруға болады.

2.2Шабуылдарды табу жүйесіне арналған базалық эталондық шамалар моделі

Кибершабуылдардың белгілі бір түрі тудырған ауытқушылықтарды анықтауға қажет шамалар жиынымен бірге қоршаған ортаның ағымдағы мәндерімен (бұл ортаның мысалы ретінде ***V*** жиынына кіретін шамалар болуы мүмкін) салыстыру арқылы ықтимал шабуыл әрекеттері туралы шешім шығаруға болады.

Эталон шамалардың моделін құру үшін [5] жүйелік лингвистикалық ұстанымды және БШМ қолданамыз, осыған сәйкес қоршаған ортадағы күдікті белсенділікті анықтауға қажет шамалар жиынтығын анықтаған жөн. Мысалы, [8, 28, 110] жұмыстардағы порттарды сканерлеу үрдісін анықтау үшін сәйкесінше <NVC,T_{NVC},X_{NVC}>және<VCA,T_{VCA}, X_{VCA}> тестілеу пайдаланылатын *NVC* және *VCA* ЛА қолданылады.

Виртуалды арна (ВА) IP-пакеттің қабылдағышын алу кезінде құрылады және белгілі бір уақыт бойы қолданылады. Жаңа ВА туындауының белгісі ретінде бұл типті арна болмаған IP-пакеттің портқа қабылдауы жатады. ВА максималды саны max_{NVC} мәнімен анықталады және жиі қолжетімді порттардың санымен, мысалы 65536 анықталады. «Өмір сүру уақыты»(ӨСУ) шамасы ВА қалған уақыт мөлшерін көрсетеді, ал оның құрылу сәті $ӨСУ:= ВЖ_0$, (1 мин $\leq ВЖ_0 \leq$10 мин).Егер $ӨСУ=0$ болса арна өз тіршілігін тоқтатады, кезекті IP-пакетте $ӨСУ:=ӨСУ+ΔӨСУ$ (мысалы, $ΔӨСУ$=100 мс).ВА арналған қарқынды трафикте ӨСУ ұлғайтылады және ұзақ қолданылады, уақыт өткеннен кейінгі $ӨСУ_А$($ӨСУ_А$-ӨСУ ағымдағы мәні) арқылы алмасу тоқтағанда арна өшіріледі, яғни трафик қарқандырақ болған сайын арна

өмір щеңдірек болып келетіні айқын. ВА қасиеттерінің және оған сәйкес ЛА негізінде порттарды сканерлеуді анықтауға арналған эталонды шамалар қалыптасады. АЖР-на басқа ықтимал шабуылдар туындатқан ауытқушылықтарды айқындау процессі қажет шамалар мен олардың қасиеттерін анықтау қажет. Мысалы, [111-114] сүйене отырып серверге DDoS-шабуыл және алмастыру (спуфинг) үшін келесі шамаларды қолданған ойға қонымды: *NCC* серверге; клиенттерден *SPR*; бір қолданушыдан *DBR* және*NPSA*.

Тәжірибе DDoS нәтижелі өткізу үшін шабуыл жасаушылардың дереккөздерінің көп мөлшердегі санын тарту қажеттігін көрсетеді. Сондықтан *NCC* шамасы серверге қосылулар саны көбейгенде шабуылдардың бастау белгісі ретінде қолданылауы мүмкін. Сервер қолдау көрсететін қосылулардың максималды саны оның аппараттық және бағдарламалық мүмкіндіктеріне тәуелді және әртүрлі серверлер үшін мәні түрліше болатын max_{NCC} шамасымен сипатталады.

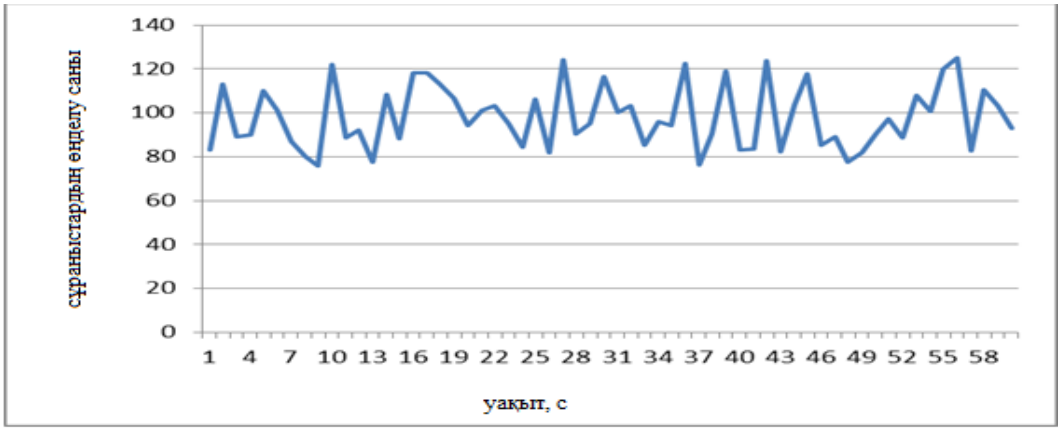
Шабуылдарға қарсы тұру мүмкіндігі уақыт бірлігінде өңделетін(әдетте бір секундта)сұраныстардың ықтимал санын сипаттайтын *SPR* сияқты серверлер жұмысындағы маңызды желілік шамаға аса байланысты болады. DDoS-шабуылдар қатысушылары түрлендіретін сқраныстардың көп мөлшерінде сервер заңды қолданушылардың сұраныстарына толық немесе жартылай әрекет етпейді, яғни жүктемеге шамасы келмейді.Сұраныстарды өңдеудің максималды жылдамдығы тәжірибе жүзінде белгілі қоршаған ортадағы белгілі сервер үшін стресс-тесттердің көмегімен анықталады және max_{SPR} шамасымен беріледі.

*DBR*шамасысерверге қосылған бір клиенттің бірізді сұраныстарының арасындағы уақытты сипаттайды. Кейбір серверлерде шабуылды алдын алу үшін бұл шама қолмен орнатылады (мысалы қолданушыдан 1секундта 1 сұраныс).Сұраныстардың арасындағы кідірістерді азайтусерверді жұмысқа жарамдылық жағдайынан шығаратын сұраныстарды көбірек жіберу мақсат болып табылатын DDoS-шабуылдың басталғанын көрсетеді.*DBR*мәні бағдарламалық қамсыздандыруға(БҚ) және сервердің міндетіне тәуелді max_{DBR} мәнімен анықталады.

Нақты сандық шамаларды алу үшін шынайы жұмыс істейтін Web-серверде эксперимент жүргізілді. Сыналатын сервер ретінде компьютер (процессоры Intel(R) Celeron(R) CPU 2.80GHz 133 МГц шина жиілігі бар; оперативті жадысы 2 Гб DDR2 400 МГц; желілік қосылу – 100 Мбит/с; операциялық жүйе – 32-бит Debian GNU/Linux 6.0.3 (squeeze))негізгі БҚ тізімі бар : Apache 2.2.16, BIND DNS сервер 9.7.1, Exim 4.72, lighttpd 1.4.28, MySQL 5.1.49, OpenSSH 5.5p1, PHP 5.3.2, Tomcat 6.0.28, Iptables қомпьютер таңдалды.

*NCC*шамасының максималды мәні Web-сервердің баптауларында */etc/apache2/apache2.conf*. мекенжайындағы *MaxClients* ретінде анықталады. Жүйе бір мезетте максимум 1024 қосылуды қолдайтындай етіп жасалған. *Netstat* утилитасының көмегімен жиналған статистикаға сәйкес аталған сервер үшін осындай қосылулардың орташа саны 100-ден аспаған.

SPR шамасының мәндері Apache базалық бағдарлама пакетіне енетін және өнімділікті бағалаудың ең кең таралған құралдарының бірі болып табылатын Apache HTTP server benchmarking tool[115, 116] утилитасының көмегімен жүзеге асырылатын стресс-тестің нәтижелері бойынша алынды. Өлшемдер сұраныстың көп мөлшері көлемінде жүргізілді. Өлшемдер аталған Web-сервер жергілікті желіде секундына 1200 сұранысты және Интернет желісінен алынған шамамен 100 шақты (2.1. суретін қараңыз) сұранысты өңдей алатынын көрсетті. Сервер қалыпты режимде секундына шамамен 34 Internet- сұранысқа қызмет ете алады.



Сурет 2.1 - 60 секундтағы Internet-сұраныстарды өңдеудің стресс-тестінің нәтижелері

Түрлі сұраныстар көп болғандықтан(қолданушылық, сонымен қатар қызметтік) бір қолдаунышының ұсынған *DBR* шамасының мәнінің нақты ерекшелігі бар, бұған қоса желілік трафикте олар кездесу жиілігіне және серверде өңделген уақытқа байланысты ерекшеленеді.

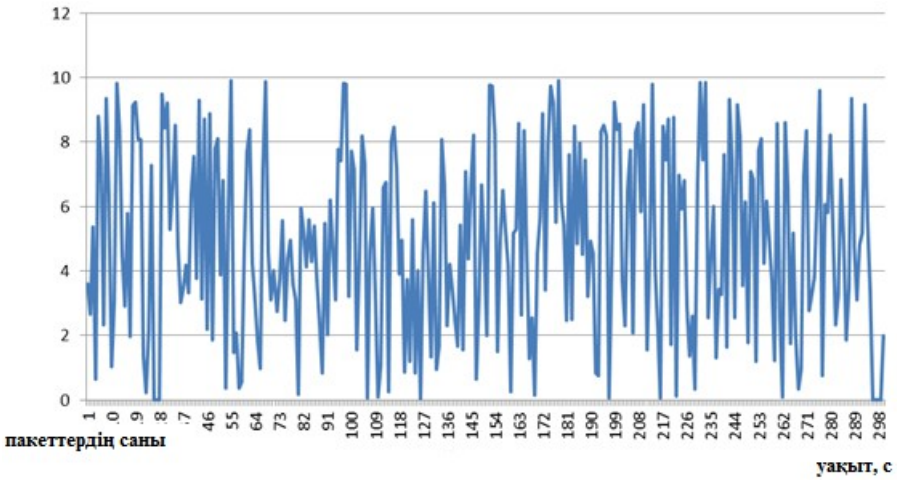
Осыған орай өлшеу әдістемесінің құрамына тек өнімділігі тұрғысынан сервер үшін шығынды болып саналатын сұраныстарды ғана енгізу керек. Сондай-ақ, ICMP- сұраныстар қауіпсіздік саясаты көмегімен құрылған Iptables желі аралық экранында сүзгілеуден өтеді.Web-серверлер үшін жиі қолданылатын GET және POST сұраныстары уақыт интервалдарын өлшеу үшін серверге жолдауларды талдайтын және қолданушыдан GET немесе POST сұраныстарының арасындағы екі бірізді сұраныстардың арасындағы уақытты есептейді, max_{DBR} орта мәні шамамен 200мс және сәйкесінше 1с болатын php-скрипт жазылды.

DoS- шақыру немесе DDoS-шабуылдарды арандатуға бағытталған алмастыру үшін пакеттер тақырып атындағы мекен-жайды ауыстырумен сипатталатын белгілерді қолданамыз.

Сондықтан осындай түрдегі шабуылдарды анықтау үшін *NPSA* шамасын қолданған жөн. Бұл жерде тіркелмеген көп мөлшердегі пакеттердің серверге жөнелтушінің және алушының мекен-жайлары есебінде сұраныстарға жауап бере отырып өз-өзіне шабуыл жасайтын сервер мекен-жайы түрлендіретін алмастыру түрі қарастырылады. Желілік трафиктегі

жөнелтуші мен алушының бірдей мекенжайы бар үлкен мөлшердегі пакеттердің пайда болуы DDoS-шабуыл сияқты шабуылдың бастуын айғақтайды.

NPSA шамасының мәні желі аралық Iptables экранының логтарын өңдеуден алынған мәліметтер негізінде анықталады. Өлшемдер әдістемесі ретінде тақырып аттарында уақыт бірлігінде жөнелтуші мен алушының бірдей мекенжайлары (SRC және DST) мен порттары көрсетілген пакеттер санын есептеу түсіндіріледі.



Сурет 2.2 - Сервер қызметіндегі 5 минут бойындағы *NPSA*мәні 5 минут

Есепке сәйкес (2.2. суретті)сервердің қалыпты жұмысы кезінде бірдей мекенжайлары бар жөнелтуші мен алушының пакеттер саны серверде секунына 10-нан аспайды. Сондықтан бұл мәннің бірнеше есе көбейгені серверге спуффинг-шабуыл белгісі болуы мүмкін.

БШМ негізгі шамаларына әрбір ЛА үшін $<P_{ij}, T_{ij}, U_{ij}>$шеруі арқылы көрінетін шамала эталоны болып табылады. Қалыптасатын эталон термдері $T_{ij}^{e} \bigcup_{k=1}^{r} T_{ij}^{ek} = \{ T_{ij}^{e1}, T_{ij}^{e2}, \dots, T_{ij}^{ek} \}$шабуылдарды анықтау кезінде қолданатын шешуші ережелер құру үшін қажет.

Осыған байланысты эталонды шамалардың моделдерін құрамыз, егер ($i = \overline{2,3}$, $j = \overline{3,6}$)яғни$<NCC, T_{NCC}, U_{NCC}>$, $<SPR, T_{SPR}, U_{SPR}>$, $<DBR, T_{DBR}, U_{DBR}>$және$<NPSA$ сәйкесінше $T_{NPSA}, U_{NPSA}>$шерулері бар**NCC**, **SPR**, **DBR**және **NPSA** ЛА үшін құрамыз.

Жүргізілген сараптаманы ескере отырып$<NCC, T_{NCC}, U_{NCC}>$ үшін базалық эталондар моделі бес анық емес термдері бар терм жиынының негізінде құрамыз:

$$T_{NCC} = \bigcup_{i=1}^{5} T_{NCC}^{i} = \{\text{«Very small» (VS), «Small» (S), «Average» (A), «Big» (B), «Very big» (VB)}\}$$

бұлар $U_{NCC} \in \{0, max_{NCC}$ әмбебап жиынынан көрінуі мүмкін.

2.1. кестесіндегі мәліметтер қорына сүйене отырып сарапшы бағаларын қолдану арқылы жасалған ЛМТСҚ негізге алып T_{NCC} үшін ҚФ қалыптастырамыз (кесте 1.2) [28].

Кесте2.1 - T_{NCC} арналған мәліметтер

ЛА мәндері	Интервал				
	N1	N2	N3	N4	N5
VS	4	1	0	0	0
S	2	3	1	0	0
A	0	1	4	2	0
B	0	0	2	4	3
VB	0	0	0	5	6

Тәжірибе көрсеткендей $max_{NCC}=1024$ (сервердің баптауларындағы *MaxClients* мәні) анықтаған жөн, ал *N1, N2, N3, N4, N5* мәндерін сәйкесінше [0; 8;9; 64;65; 256;257; 512;513; 1024] интервалдарымен анықтау керек.

Ары қарай эталондарды формулаға сәйкес сұрақ матрицасын қалыптастырамыз.

$$\|k_j\| = \left\| \bigcup_{j=1}^{5} \sum_{i=1}^{5} b_{ij} \right\| = \|6,5,7,11,9\|,$$

Осындағы b_{ij}-эмпирикалық мәлімет элементтері(2.1.кестені қараңыз) олар

$$c_{ij} = b_{ij} km / k_j, \quad (2.15)$$

өрнегімен матрицаға айналады, осындағы $(i, j = \overline{1, 5})$, а $km = \sum_{j=1}^{5} k_j = 11$, және

$$\|c_{ij}\| = \begin{Vmatrix} 7,33 & 1,83 & 0 & 0 & 0 \\ 4,4 & 6,6 & 2,2 & 0 & 0 \\ 0 & 1,57 & 6,29 & 3,14 & 0 \\ 0 & 0 & 2 & 4 & 3 \\ 0 & 0 & 0 & 6,11 & 7,33 \end{Vmatrix}.$$

Ары қарай ҚФ өрнегі

$$\mu_{ij} = c_{ij} / cm_i, \quad (2.16)$$

$cm_i = \bigcup_{j=1}^{5} \bigvee_{i=1}^{5} c_{ij}$

бойынша матрица қалыптасады, осындағы ($i, j = \overline{1, 5}$), ал $=\{7,33;\ 6,6;\ 6,29;\ 4;\ 7,33\}$. Алынған мәндер келесі түрге ие болады:

$$\left\| \mu_{ij} \right\| = \begin{Vmatrix} 1 & 0,25 & 0 & 0 & 0 \\ 0,67 & 1 & 0,33 & 0 & 0 \\ 0 & 0,25 & 1 & 0,5 & 0 \\ 0 & 0 & 0,5 & 1 & 0,75 \\ 0 & 0 & 0 & 0,83 & 1 \end{Vmatrix}.$$

$\bigcup_{i=1}^{5} \mu_{ij}$ үшін сәйкесінше $\bigcup_{i=1}^{5} \Delta B_i / B$ $=\{0,008;\ 0,063;\ 0,25;\ 0,5;\ 1\}$ ($\Delta B/B$ -бағалық қатынастарын табамыз, $\Delta B_{NCC} \in [0,\ B_{NCC}]$ шамасының ауытқуы, ал B_{NCC} – ағымдағы өлшемдерді сипаттайтын максималды ықтимал мән) және аралық анық емес сандарды(АЕС) аламыз:

$\tilde{VS}$ $=\{1/0,008;\ 0,25/0,063;\ 0/0,25;\ 0/0,5;\ 0/1\}$;

$\tilde{S}$ $=\{0,67/0,008;\ 1/0,063;\ 0,33/0,25;\ 0/0,5;\ 0/1\}$;

$\tilde{A}$ $=\{0/0,008;\ 0,25/0,063;\ 1/0,25;\ 0,5\ /0,5;\ 0/1\}$;

$\tilde{B}$ $=\{0/0,008;\ 0/0,063;\ 0,5/0,25;\ 1/0,5;\ 0,75/1\}$;

$\tilde{VB}$ $=\{0/0,008;\ 0/0,063;\ 0/0,25;\ 0,83/0,5;\ 1/1\}$.

Лингвистикалық эталондарды қалыптастыру үшін $\forall T_{NCC}^{i}$ мәніне мысалы, егер $i=1$, $\forall x_{VS}: x_{VS_k} < x_{VS_{k+1}}$ ретті қатынасы нақты болар еді. Ары қарай алынған АЕС үшін $T_{NCC}\tilde{X} = \{\mu_1 / x_1,\ \mu_2 / x_2,\ \ldots,\ \mu_i / x_i,\ \ldots,\ \mu_n / x_n\}$ берілген модельде ұсынылады [28]

$T_{NCC}^{e} = \bigcup_{i=1}^{5} T_{NCC}^{ei} = \{T_{NCC}^{e1}, T_{NCC}^{e2}, T_{NCC}^{e3}, T_{NCC}^{e4}, T_{NCC}^{e5}\} = \{\tilde{VS}^{e}, \tilde{S}^{e}, \tilde{A}^{e}, \tilde{B}^{e}, \tilde{VB}^{e}\}$,где

$\tilde{VS}^{e}$ $=\{0/0,008;\ 1/0,008;\ 0,25/0,063;\ 0/0,25\}$;

$\tilde{S}^{e}$ $=\{0/0,008;\ 0,67/0,008;\ 1/0,063;\ 0,33/0,25;\ 0/0,5\}$;

$\tilde{A}^{e}$ $=\{0/0,008;\ 0,25/0,063;\ 1/0,25;\ 0,5\ /0,5;\ 0/1\}$;

$\underset{\sim}{B}^e$ $=\{0/0{,}063;\ 0{,}5/0{,}25;\ 1/0{,}5;\ 0{,}75/1;\ 0/1\};$

$\underset{\sim}{VB}^e$ $=\{0/0{,}25;\ 0{,}83/0{,}5;\ 1/1;\ 0/1\}.$

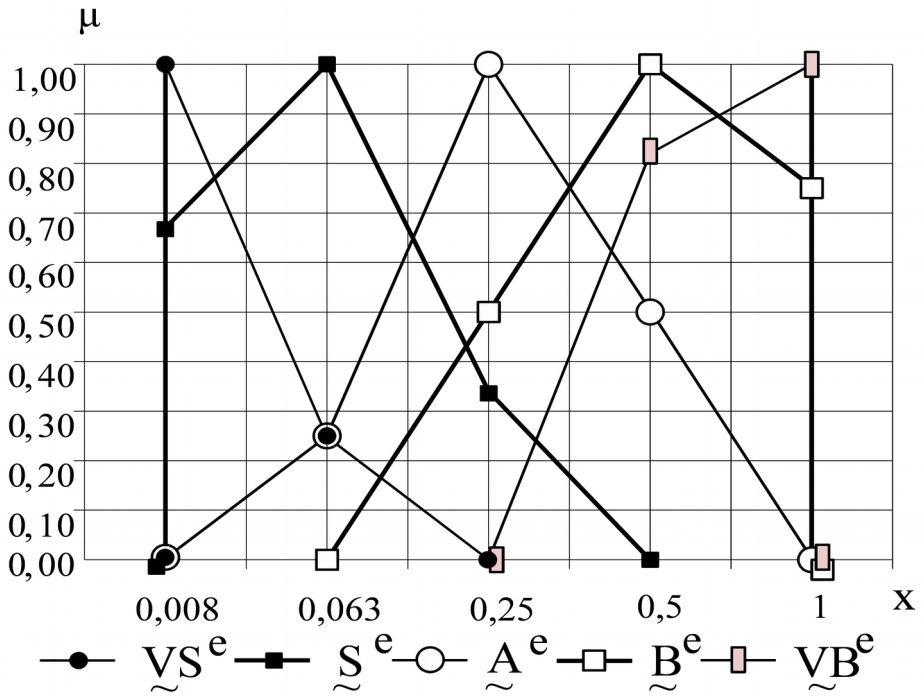
Алынған мәндер **NCC**үшін эталон ретінде қолданылады, олардың графикалық бейнесі 2.3.суретінде берілген.

Жүргізілген сарапшы есебін ала отырып $<SPR, T_{SPR}, U_{SPR}>$үшін эталондардың негізгі моделін үш анық емес термдері бар базалық терм жиының негізінде құрамыз.

$$T_{SPR}=\bigcup_{i=1}^{3} T_{SPR}^{i} =\{\text{«Low» (L), «Average» (A), «High (H)»}\},$$

$U_{SPR}\in\{0, max_{SPR}\}$ әмбебап жиынында көрінуі мүмкін.

2.2. кестесінде берілген сарапшы мәліметтерінің негізінде сәйкесінше [0; 5;6; 25;26; 100] мәндерін қабылдайтын *N1, N2, N3* интервалдары үшін ҚФ қалыптастырамыз. Сарапшыға сәйкес (2.1.қараңыз) стресс-тестің көмегімен интернет желісінен алынған пакеттер санының орта мәнін білдіретін $max_{SPR}=100$ анықтаймыз.



Сурет 2.3- NCCүшін эталонды АЕС

Кесте2.2 - T_{SPR} үшін мәліметтер

T_{SPR} үшін мәліметтер

ЛА мәндері	Интервал		
	N1	N2	N3
L	3	1	0
A	1	2	1
H	0	1	4

$$\|k_j\| = \left\| \bigcup_{j=1}^{3} \sum_{i=1}^{3} b_{ij} \right\| = \|4,4,5\|,$$

формуласы арқылы көмек беру матрицасын қалыптастырамыз, осындағы b_{ij}- эмпирикалық мәліметтер элементі (2.2.кестені қараңыз), олар (2.15) өрнегі бойынша матрицаға айналады, егер $(i,j=\overline{1,3})$, осындағы $km = \bigvee_{j=1}^{3} k_j = 5$, ал

$$\|c_{ij}\| = \begin{vmatrix} 3,75 & 1,25 & 0 \\ 1,25 & 2,5 & 1 \\ 0 & 1,25 & 4 \end{vmatrix}.$$

Ары қарай (2.16) өрнегі арқылы $(i,j=\overline{1,3})$ болғанда, осындағы $cm_i = \bigcup_{j=1}^{3} \bigvee_{i=1}^{3} c_{ij} = \{3,75;\ 2,5;\ 4\}$ ҚФ есептейміз. Есептелген ҚФ мәндері төмендегідей болады:

$$\|\mu_{ij}\| = \begin{Vmatrix} 1 & 0,33 & 0 \\ 0,5 & 1 & 0,4 \\ 0 & 0,31 & 1 \end{Vmatrix}.$$

$\bigcup_{i=1}^{3} \mu_{ij}$ үшін сәйкесінше $\bigcup_{i=1}^{3} \Delta B_i / B = \{0,05;\ 0,25;\ 1\}$ бағалық қатынастарын табамыз ($\Delta B/B$ -$\Delta B_{SPR} \in [0,\ B_{SPR}]$ шамасының ауытқуы, ал B_{SPR} – ағымдағы өлшемдерді сипаттайтын максималды ықтимал мән) және АЕС аламыз:

$\tilde{L} = \{1/0,05;\ 0,33/0,25;\ 0/1\};$

$\tilde{A} = \{0,5/0,05;\ 1/0,25;\ 0,4/1\};$

$\tilde{H} = \{0/0,05;\ 0,31/0,25;\ 1/1\}.$

$\forall T^i_{SPR}$ үшін мысалы $i=1$, $\forall x_L$: $x_{L_k} < x_{L_{k+1}}$ рет қатынасы әділ екенін ескерген жөн. АЕС үшін алынған $T_{SPR} \overset{X}{\sim} \{\mu_1 / x_1,\ \mu_2 / x_2,\ \ldots,\ \mu_i / x_i,\ \ldots,\ \mu_n / x_n\}$ келтірілген модельде ұсынылады [28]

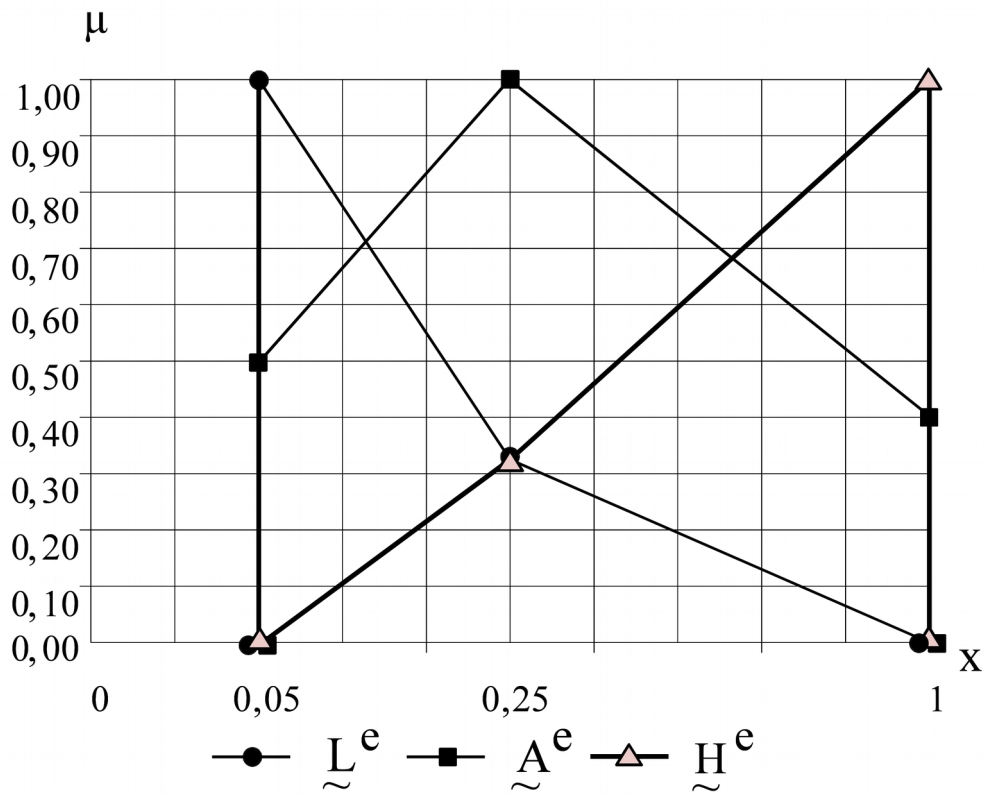
$T^e_{SPR} = \bigcup_{i=1}^{3} T^{ei}_{SPR} = \{T^{e1}_{SPR},\ T^{e2}_{SPR},\ T^{e3}_{SPR}\} = \{\tilde{L}^e,\ \tilde{A}^e,\ \tilde{H}^e\}$, где

$\tilde{L}^e = \{0/0,05;\ 1/0,05;\ 0,33/0,25;\ 0/1\};$

$\tilde{A}^e = \{0/0,05;\ 0,5/0,05;\ 1/0,25;\ 0,4/1;\ 0/1\};$

$\underset{\sim}{H}^{e}$ ={0/0,05; 0,31/0,25; 1/1; 0/1}.

Алынған мәндер **SPR** үшін 2.4. суретінде ұсынылған графикалық кескінге эталон ретінде қолданылады.



Сурет 2.4 –SPRүшін эталонды АЕС

SPR ұқсас <*DBR, T_{DBR}, U_{DBR}*>үшін үш анық емес термді жиынында қолданып:

$$T_{DBR}=\bigcup_{i=1}^{3} T_{DBR}^{i} =\{«Small» (S), «Average» (A), «Big» (B)\},$$

$U_{DBR}\in\{0, max_{DBR}\}$ әмбебап жиынында көрінетін есептеулер жүргіземіз.

2.3. кестесі бойынша*N1, N2, N3*үшін сәйкесінше [0; 10;11; 100;101; 1000] мәндерін береміз.

Сарапшыға сәйкес (2.1 сурет) GET және POST сұраныстарын өңдеу уақыты туралы алынған мәліметтер негізінде $max_{DBR}=1000$ мс анықтаймыз.

Формула бойынша көмек беру матрицасын қалыптастырамыз.

$$\|k_j\| = \left\| \bigcup_{j=1}^{3} \sum_{i=1}^{3} b_{ij} \right\| = \|4,6,7\|,$$

Кесте2.3 - T_{DBR}үшінмәліметтер

T_{DBR}үшінмәліметтер

ЛА мәндері	Интервал		
	N1	N2	N3
S	3	1	0

A	1	3	2
B	0	2	5

осындағы b_{ij}- элементы эмпирикалық мәліметтер элементі (2.3кестені қараңыз), олар $i,j=\overline{1,3}$) болса, онда $km=\bigvee_{j=1}^{3} k_j$ =7, (2.15) өрнегі бойынша матрицаға түрленеді (($i,j=\overline{1,3}$), осындағы $km=\bigvee_{j=1}^{3} k_j$ =7, ал

$$\|c_{ij}\|=\begin{vmatrix} 5,25 & 1,75 & 0 \\ 1,17 & 3,5 & 2,33 \\ 0 & 2 & 5 \end{vmatrix}.$$

$cm_i=\bigcup_{j=1}^{3}\bigvee_{i=1}^{3} c_{ij}$

Ары қарай (2.16) өрнегі ($i,j=\overline{1,3}$)болғанда, осындағы =*{5,25; 3,5; 5}* ҚФ есептейміз. Есептелген ҚФ төмендегідей болады:

$$\|\mu_{ij}\|=\begin{vmatrix} 1 & 0,33 & 0 \\ 0,33 & 1 & 0,67 \\ 0 & 0,4 & 1 \end{vmatrix}.$$

$\bigcup_{i=1}^{3}\mu_{ij}$ үшін сәйкесінше $\bigcup_{i=1}^{3}\Delta B_i / B$ =*{0,01; 0,1; 1}*рет қатынасын табамыз, (*ΔB/B-ΔB*$_{DBR}$*∈[0, B*$_{DBR}$*]* шамасының ауытқуы, ал B_{DBR} – ағымдағы өлшемдерді сипаттайтын максималды ықтимал мән) және АЕС аламыз:

$\underset{\sim}{S}$ =*{1/0,01; 0,33/0,1; 0/1};*

$\underset{\sim}{A}$ =*{0,33/0,01; 1/0,1; 0,67/1};*

$\underset{\sim}{B}$ =*{0/0,01; 0,4/0,1; 1/1}.*

$\forall T^i_{DBR}$ үшін эталондарды қалыптастыруда мысалы $i=1$, $\forall x_S: x_{S_k}<x_{S_{k+1}}$. болғанда рет қатынасы дұрыс болады. Ары қарай АЕС үшін $T_{DBR}\underset{\sim}{X}$ ={ μ_1 / x_1, μ_2 / x_2, …, μ_i / x_i, …, μ_n / x_n } келтірілген модельде ұсынылады [28]

$T^e_{DBR}=\bigcup_{i=1}^{3} T^{ei}_{DBR}$ ={ T^{e1}_{DBR}, T^{e2}_{DBR}, T^{e3}_{DBR} }={ $\underset{\sim}{S^e}$, $\underset{\sim}{A^e}$, $\underset{\sim}{B^e}$ }, где

$\underset{\sim}{S^e}$ =*{0/0,01; 1/0,01; 0,33/0,1; 0/1};*

$\underset{\sim}{A^e}$ =*{0/0,01; 0,33/0,01; 1/0,1; 0,67/1; 0/1};*

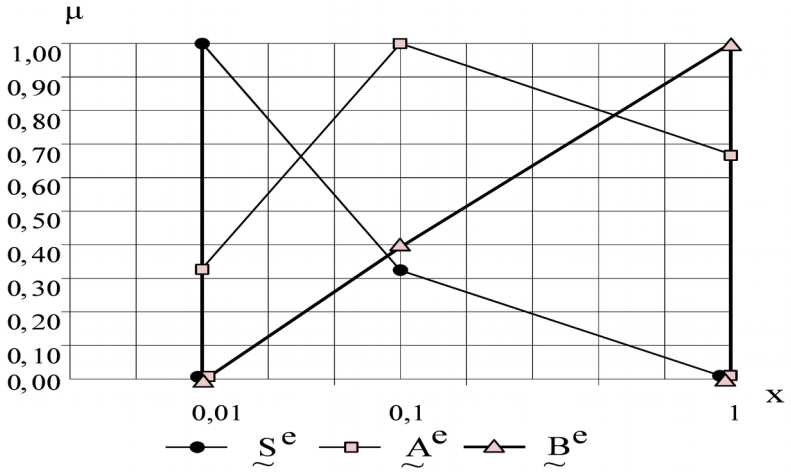
$\underset{\sim}{B^e}$ =*{0/0,01; 0,4/0,1; 1/1; 0/1}.*

Бұл мәндер 2.5. суретінде графикалық кескіні **DBR** үшін эталон ретінде қолданылатын болады.

DBR ұстанымы бойынша $<NPSA, T_{NPSA}, U_{NPSA}>$үшін $T_{NPSA}=\bigcup_{i=1}^{3} T_{NPSA}^{i}$ $=\{«Small» (S), «Average» (A), «Big» (B)\}$ негізінде есептеулер жүзеге асырылады, ал анық емес термдер $U_{NPSA}\in\{0, max_{NPSA}\}$ әмбебап жиынында бейнеленуі мүмкін.

2.4. кестесі бойынша*N1, N2, N3*үшін сәйкесінше [0; 10;11; 100;101; 1000] мәндерін береміз.

Сараптамаға сәйкес (2.2. суретін қараңыз) нақты жұмыс істейтін серверді бақылау негізінде $max_{NPSA}=1000$ пакет (қалыпты пакеттер санынан 100 есе көп) мәнін анықтаймыз.



Сурет 2.5 –DBRүшін эталонды АЕС

Кесте2.4 - T_{NPSA} үшін мәліметтер

T_{NPSA}үшінмәліметтер

ЛА мәндері	Интервал N1	N2	N3
S	3	1	0
A	1	4	2
B	0	2	3

$$\|k_j\| = \left\| \bigcup_{j=1}^{3} \sum_{i=1}^{3} b_{ij} \right\|_{=} \|4,7,5\|,$$

формуласы бойынша көмек беру матрицасын қалыптастырамыз, осындағы b_{ij}- эмпирикалық мәліметтер элементтері (2.4. кестені қараңыз), олар

(2.15) өрнегі бойынша егер ($i,j=\overline{1,3}$) матрицаға түрленеді,осындағы $km=\vee_{j=1}^{3} k_j = 7$, ал

$$\left\| c_{ij} \right\| = \begin{Vmatrix} 5,2 & 1,7 & 0 \\ 5 & 5 & \\ 1 & 4 & 2 \\ 0 & 2,8 & 4,2 \end{Vmatrix}.$$

Ары қарай (2.16) өрнегі ($i,j=\overline{1,3}$) болғанда, осындағы $cm_i = \bigcup_{j=1}^{3} \vee_{i=1}^{3} c_{ij}$ =*{5,25;4;4,2; }* ҚФ есептейміз. Есептелген ҚФ төмендегідей болады:

$$\left\| \mu_{ij} \right\| = \begin{Vmatrix} 1 & 0,33 & 0 \\ 0,25 & 1 & 0,5 \\ 0 & 0,67 & 1 \end{Vmatrix}.$$

$\bigcup_{i=1}^{3} \mu_{ij}$ үшін сәйкесінше $\bigcup_{i=1}^{3} \Delta B_i / B$ =*{0,01; 0,1; 1}*рет қатынасын табамыз, (*ΔB/B-ΔB*$_{NPSA}$*∈[0, B*$_{NPSA}$*]* шамасының ауытқуы, ал*B*$_{NPSA}$ –ағымдағы өлшемдерді сипаттайтын максималды ықтимал мән және АЕС аламыз:

$\tilde{S}$ ={1/0,01; 0,33/0,1; 0/1};

$\tilde{A}$ ={0,25/0,01; 1/0,1; 0,5/1};

$\tilde{B}$ ={0/0,01; 0,67/0,1; 1/1}.

Сонымен бірге $\forall T^{i}_{NPSA}$ үшін мысалы, егер $i=1$, $\forall x_S$: $x_{S_k} < x_{S_{k+1}}$ рет қатынасы әділ болады. Ары қарай АЕС үшін алынған $T_{NPSA} \tilde{X}$ ={ μ_1 / x_1, μ_2 / x_2, …, μ_i / x_i, …, μ_n / x_n } келтірілген формада ұсынылады [28]

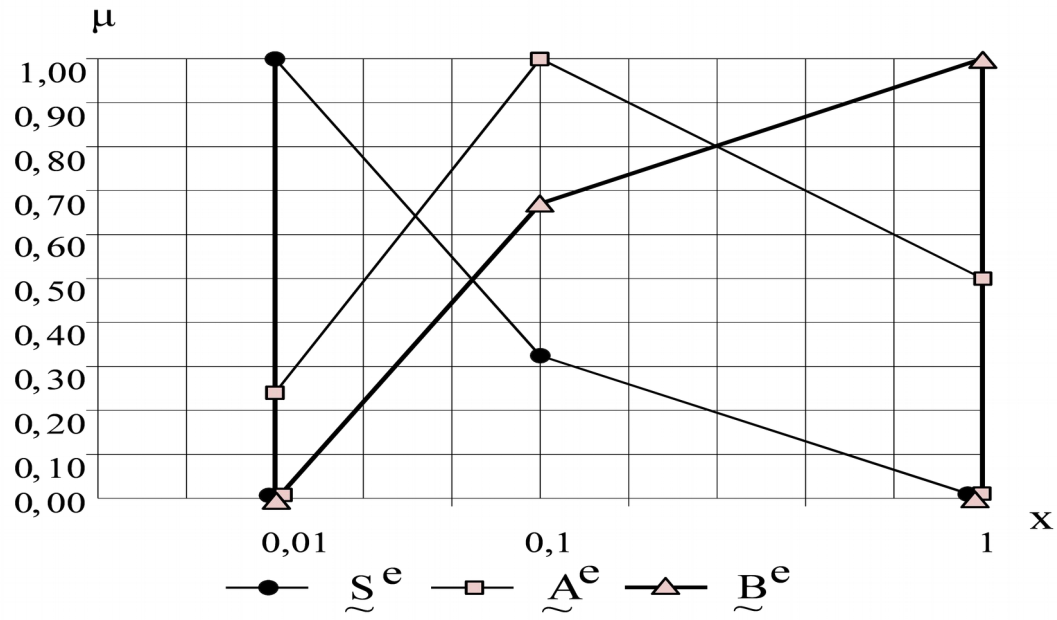
$T^{e}_{NPSA} = \bigcup_{i=1}^{3} T^{ei}_{NPSA}$ ={ T^{e1}_{NPSA}, T^{e2}_{NPSA}, T^{e3}_{NPSA} }={ $\tilde{S}^{e}$, $\tilde{A}^{e}$, $\tilde{B}^{e}$ }, где

$\tilde{S}^{e}$ ={0/0,01; 1/0,01; 0,33/0,1; 0/1};

$\tilde{A}^{e}$ ={0/0,01; 0,25/0,01; 1/0,1; 0,5/1; 0/1};

$\tilde{B}^{e}$ ={0/0,01; 0,67/0,1; 1/1; 0/1}.

Бұрынғы моделдердегі сияқты алынған мәндер 2.6.суретінде графикалық кескіні **NPSA** үшін эталон есебінде қолданылатын болады.



Сурет 2.6-NPSA үшін эталонды АЕС

Осылайша, сарапшылық баға мәліметтерін қолданып БШМ негізіндеNCC, SPR, DBR және NPSA ЛА негізгі эталонды шама моделдері құрылды. Эксперименттік мәліметтерді ескере отырып, АЖ ауытқушылық жағдайды анықтауға негізделген сәйкес қауіпсіздік құралдарының нәтижелілігін жоғарылатуға мүмкіндік беретін жүйелі ережелерді қалыптастыруға қажет нақты эталонды АЕС анықталады. Осындай ережелерді қалыптастыру үрдісін қолдау үшін математикалық ШЕМ құрамыз.

2.3Ақпараттық жүйелердегі ауытқушылықтарды анықтауға арналған шешуші ережелер моделі

ШЕМ құру үшін[15] БШМ және ЭШМ(2.1.2.2.баптарын қараңыз) [4, 5] қолданамыз. Шешуші ережелер ұғымына белгілі теориялық және эксперименталды білімнің (мәліметтің) жалпылануы нәтижесіне негізделген және әлсіз қалыптастырылған тапсырмалардың оңтайлы мағыналық шешімін іздеуді қамтамасыз ететін тұлғаның интуитивтік пайымдарын білдіреді.

Сәйкес модель құру үшін анық емес идентификациялау жиынын((fuzzy identifiers) енгіземіз:

$$\boldsymbol{FI} = \bigcup_{i=1}^{d} FI_i = \{FI_1, FI_2, FI_3, \ldots, FI_d\}, (i = \overline{1,d}), \quad (2.17)$$

осындағы d -ауытқушылық жағдайын көрсетуге қажет элементтер жиыны, ал FI_i $(i = \overline{1,d})$- әрқайсысы белгілі шабуылдар туындататын жүйенің ауытқушылық жағдайының деңгейін анық емес формада сипаттайтын

мәтіндік мәндердің біреуіне ие болатын ***FI*** элементтері мысалы, егер$d=5$ (2.17) өрнегін келесідей анықтауға болады:

$$\boldsymbol{FI}=\bigcup_{i=1}^{5} FI_i = \{FI_1, FI_2, FI_3, FI_4, FI_5\}=\{L, LTH, HTTL, H, LIM\}, \quad (2.18)$$

осындағы $FI_1=L$, $FI_2=LTH$, $FI_3=HTTL$,$FI_4=H$және $FI_5=LIM$сәйкесінше мәндерге ие болады

- «Low (*L*)» – «Төмен»,
- «Lower than high (*LTH*)» – «Жоғарыға қарағанда төменірек»,
- «Higher than the lowest (*HTTL*)» – «Төменге қарағанда жоғарырақ»,
- «High (*H*)» – «Жоғары»,
- «Limits (*LIM*)» – «Шекті».

Ары қарай ***FI*** анық емес идентификация жиыны және ***MP***түйіндес жұптардың негізінде шешуші ержелер жиынын құрамыз(solutionrule)

$$\boldsymbol{SR}=\{\bigcup_{i=1}^{n} \boldsymbol{SR_i}\}=\{\boldsymbol{SR_1}, \boldsymbol{SR_2}, \boldsymbol{SR_3}, \ldots, \boldsymbol{SR_n}\}, \ (i=\overline{1,n}), \quad (2.19)$$

осындағы $\boldsymbol{SR_i}(i=\overline{1,n})$ –*i* шабуылды тудырған *i* ауытқушылық жағдайын анықтауға арналған ықтимал ережелердің ішкі жиыны, осындағы

$$\bigcup_{i=1}^{n} \boldsymbol{SR_i}=\bigcup_{i=1}^{n}\{\bigcup_{j=1}^{r_i} SR_{ij}\}=$$
$$\{SR_{11}, SR_{12}, SR_{13}, \ldots, SR_{1r_1}\},$$
$$\{SR_{21}, SR_{22}, SR_{23}, \ldots, SR_{2r_2}\}, \{SR_{31}, SR_{32}, SR_{33}, \ldots, SR_{3r_3}\}, \ldots,$$
$$\{SR_{n1}, SR_{n2}, SR_{n3}, \ldots, SR_{nr_i}\}, (i=\overline{1,n}, \ j=\overline{1,r_i}), \quad (2.20)$$

яғни SR_{ij} $(i=\overline{1,n}, \ j=\overline{1,r_n})$ –*i* ықтимал ережелердің ішкі жиынының *j*-ережесі ал r_i $(i=\overline{1,n})$ – *i* ауытқушылығын анықтауға бағытталған ықтимал ережелердің жалпы саны.

Әрбір SR_{ij} сәйкес шешуші өрнек (ереже) бар екенін атап өткен жөн, яғни:

$$\begin{aligned}
&\{SR_{11}=(MP_{11}\in FI_{11}), && SR_{12}=(MP_{12}\in FI_{12}), && SR_{1r_1}=(MP_{1r_1}\in FI_{1r_1})\},\\
&\{SR_{21}=(MP_{21}\in FI_{21}), && SR_{22}=(MP_{22}\in FI_{22}), && SR_{2r_2}=(MP_{2r_2}\in FI_{2r_2})\},\\
&\{SR_{31}=(MP_{31}\in FI_{31}), && SR_{32}=(MP_{32}\in FI_{32}), && SR_{3r_3}=(MP_{3r_3}\in FI_{3r_3})\},\\
& && \ldots, && \\
&\{SR_{n1}=(MP_{n1}\in FI_{n1}), && SR_{n2}=(MP_{n2}\in FI_{n2}) && SR_{nr_n}=(MP_{nr_n}\in FI_{nr_n})\}.\\
& && \ldots, &&
\end{aligned} \quad (2.21)$$

(2.21)өрнегін жалпылай келе (2.19) және (2.20) ескере отырып

$$\boldsymbol{SR}=\bigcup_{i=1}^{n}\{\bigcup_{j=1}^{r_i} SR_{ir_j}\}=\bigcup_{i=1}^{n}\{\bigcup_{j=1}^{r_i}(MP_{ir_j}\in FI_{ir_j})\}=$$

$$\{\bigcup_{i=1}^{n}\{\bigcup_{j=1}^{r_i} SR_{ir_j}=(MP_{ir_j}\in FI_{ir_j})\}\},\ (i=\overline{1,n},\ j=\overline{1,r_i}), \qquad (2.22)$$

осындағы SR_{ir_j} i шабуылдарды тудырған ауытқушылықтарды анықтауға арналған r_j ереже,ол дәлме-дәл келесідей түсіндіріледі: «егер MP_{ir_j} шындыққа сай болса,онда i шабуылдарды тудырған ауытқушылық жағдайының деңгейі FI_{ir_j} болады».

Ережелерді құру әдетте сарапшылық ұстанымның негізінде жүзеге асырылады, бұл әсіресе альтернативті артықшылық беру қажет болған жағдайда, мысалы, (2.22) өрнегінде MP_{ir_j} FI_{ir_j} байланысты матрица инициализациясы (МІ) жүйенің жағдайын неғұрлым объективті түрде бейнелейтін болады. Нақты мысал арқылы альтернативті жиындары үшін артықшылықты қалыптастыру үрдісін қарастырайық.

$\boldsymbol{SR_1}$ ережелердің ішкі жиынын құруға түйіндес жұптардың r_1және анық емес идентификациялауды d (2.17), олардың бірі қоршаған ортаның жағдайын ауытқушылыққа байланысты неғұрлым объективті түрде бейнелей алады. Сонымен, ықтимал альтернативті шешімдердің жалпы саны - $d\times r_1$, яғни, SR_{1j} $(j=\overline{1,r_1})$үшін әрбір ережені құруға қажет d ережелердің альтернатив нұсқаларын таңдау үшін МК анықтауға қажет әдістерді қолданамыз. (1.3.бабын қараңыз) [10].

ШЕ әдісін қолданамыз, өйткені ол бірнеше сарапшының қызметін қолдануға мүмкіндік береді, бастапқы деректер ретінде кестелік формалар, бастапқы сызықтық функция қолданылады, ал еңбек сыйымдылығы төмен. ([10] қараңыз).

Ары қарай мысал ретінде $d=r_1=5$ болса, онда

$$\boldsymbol{MP_1}=\{\bigcup_{j=1}^{r_1} MP_{1j}\}=\{MP_{11}, MP_{12}, MP_{13}, MP_{14}, MP_{15}\}=$$

$$\{((\tilde{t}_{SPR}\cong\tilde{L}^e\vee\tilde{t}_{DBR}\cong\tilde{S}^e)\wedge\tilde{t}_{NCC}\cong\tilde{VS}^e),$$

$$((\tilde{t}_{SPR}\cong\tilde{L}^e\vee\tilde{t}_{DBR}\cong\tilde{S}^e)\wedge\tilde{t}_{NCC}\cong\tilde{S}^e),$$

$$((\tilde{t}_{SPR}\cong\tilde{L}^e\vee\tilde{t}_{DBR}\cong\tilde{S}^e)\wedge\tilde{t}_{NCC}\cong\tilde{A}^e),$$

$$((\tilde{t}_{SPR}\cong\tilde{L}^e\vee\tilde{t}_{DBR}\cong\tilde{S}^e)\wedge\tilde{t}_{NCC}\cong\tilde{B}^e),$$

$$((\underset{\sim}{t}_{SPR} \cong \underset{\sim}{L}^{e} \vee \underset{\sim}{t}_{DBR} \cong \underset{\sim}{S}^{e}) \wedge \underset{\sim}{t}_{NCC} \cong \underset{\sim}{VB}^{e})\},$$

ал FI_{1j} $(j=\overline{1,5})$ мәндері ретінде (2.18) формуласындағы мәліметтерді қолданамыз.

Осылайша әрбір MP_{1j} $(j=\overline{1,5})$үшін $d=5$(2.18) өрнегіндегі анық емес идентификациялаудің нақты мәндерімен байланысты ауытқушылықты анықтау мүмкін. Неғұрлым объективті нәтижені РС әдісінің көмегімен анықтаймыз(1.3. бабын қараңыз) [10]

Осы әдіске сәйкес мысал ретінде $d=5$ қатысты әрбір j ережесіне сәйкес SR^{k}_{1j} $(k=\overline{1,d},\ j=\overline{1,r_1})$ ықтимал нәтижесіне 4 сарапшының пайымдарын қолданамыз. Мысалы, альтернативті шешімдердің алғашқы ережесі үшін ішкі жиынына қолданылады.

$$\bigcup_{k=1}^{d} SR^{k}_{11} = \{SR^{1}_{11}, SR^{2}_{11}, SR^{3}_{11}, SR^{4}_{11}, SR^{5}_{11}\} =$$

$$\{((\underset{\sim}{t}_{SPR} \cong \underset{\sim}{L}^{e} \vee \underset{\sim}{t}_{DBR} \cong \underset{\sim}{S}^{e}) \wedge \underset{\sim}{t}_{NCC} \cong \underset{\sim}{VS}^{e}) \in L,$$

$$((\underset{\sim}{t}_{SPR} \cong \underset{\sim}{L}^{e} \vee \underset{\sim}{t}_{DBR} \cong \underset{\sim}{S}^{e}) \wedge \underset{\sim}{t}_{NCC} \cong \underset{\sim}{S}^{e}) \in LTH,$$

$$((\underset{\sim}{t}_{SPR} \cong \underset{\sim}{L}^{e} \vee \underset{\sim}{t}_{DBR} \cong \underset{\sim}{S}^{e}) \wedge \underset{\sim}{t}_{NCC} \cong \underset{\sim}{A}^{e}) \in HTTL,$$

$$((\underset{\sim}{t}_{SPR} \cong \underset{\sim}{L}^{e} \vee \underset{\sim}{t}_{DBR} \cong \underset{\sim}{S}^{e}) \wedge \underset{\sim}{t}_{NCC} \cong \underset{\sim}{B}^{e}) \in H,$$

$$((\underset{\sim}{t}_{SPR} \cong \underset{\sim}{L}^{e} \vee \underset{\sim}{t}_{DBR} \cong \underset{\sim}{S}^{e}) \wedge \underset{\sim}{t}_{NCC} \cong \underset{\sim}{VB}^{e}) \in LIM\}.$$

Ары қарай ШЕ негізінде λ шамасымен белгіленетін МК анықтаймыз. Оның ең төмен деңгейдегі мәні альтернативтінің артық көрінушілігі туралы айғақтайды, яғни оның МК жоғарырақ болады.SR_{11} үшін x^{k}_{1j} және λ^{k}_{1j} әрбір ықтимал SR^{k}_{11} $(k=\overline{1,5})$ нәтижесі үшін есептеулер жүргіземіз:

x^{1}_{11}=(1+3+1+2)/4=1,75; x^{2}_{11}=(2+1+3+2)/4=2;

x^{3}_{11}= (3+2+2+2)/4=2,25; x^{4}_{11}=(2+4+3+3)/4=3;

x^{5}_{11}=(4+4+ 3+4)/4=3,75.

МК мәні $\lambda^{k}_{1j} = x^{k}_{1j} / N$ ретінде анықталады, осындағы N – барлық дәрежелердің қосындысы. ($N=10$) 2.5 кестесіне енгізілген нәтижелерден ең жасы нәтиже SR^{1}_{11} өйткені $\bigwedge_{k=1}^{5} \lambda^{k}_{11} = \lambda^{1}_{11} = 0,18$.

Кесте 2.5 - SR^{k}_{1j} дәрежелері және МК

SR_{1j}^{k} дәрежелері және МК

SR_{1j}^{k}	j	k	Сарапшылар				x_{1j}^{k}	λ_{1j}^{k}
			1	2	3	4		
1	2	3	4	5	6	7	8	9
SR_{11}^{1}	1	1	1	3	1	2	1,75	0,18

2.5 – кестенің жалғасы

1	2	3	4	5	6	7	8	9
SR_{11}^{2}		2	2	1	3	2	2	0,2
SR_{11}^{3}		3	3	2	2	2	2,25	0,23
SR_{11}^{4}		4	2	4	3	3	3	0,3
SR_{11}^{5}		5	4	4	3	4	3,75	0,38
SR_{12}^{1}		1	2	3	1	2	2	0,2
SR_{12}^{2}		2	1	2	1	2	1,5	0,15
SR_{12}^{3}	2	3	3	1	2	3	2,25	0,23
SR_{12}^{4}		4	3	4	2	2	2,75	0,28
SR_{12}^{5}		5	3	2	3	4	3	0,3
SR_{13}^{1}		1	2	3	2	4	2,75	0,28
SR_{13}^{2}		2	3	2	2	1	2	0,2
SR_{13}^{3}	3	3	2	3	1	1	1,75	0,18
SR_{13}^{4}		4	3	4	3	4	3,5	0,35
SR_{13}^{5}		5	4	3	2	4	3,25	0,33
SR_{14}^{1}		1	4	2	2	4	3	0,3
SR_{14}^{2}		2	2	4	3	2	2,75	0,28
SR_{14}^{3}	4	3	3	1	2	2	2	0,2
SR_{14}^{4}		4	1	2	3	1	1,75	0,18
SR_{14}^{5}		5	2	4	4	3	3,25	0,33
SR_{15}^{1}		1	4	4	3	3	3,5	0,35
SR_{15}^{2}		2	2	4	4	3	3,25	0,33
SR_{15}^{3}	5	3	2	4	3	3	3	0,3
SR_{15}^{4}		4	4	3	2	3	3	0,3
SR_{15}^{5}		5	2	2	4	3	2,75	0,28

Осыған ұқсас SR_{1j}^{k} $(j=\overline{2,5})$ есептеулер жүргіземіз:

SR_{12}^{k} – x_{12}^{1}=(2+3+1+2)/4=2; x_{12}^{2}= (1+2+1+2)/4=1,5;

x_{12}^3=(3+1+2+3)/4=2,25; x_{12}^4=(3+ 4+2+2)/4=2,75; x_{12}^5=(3+2+3+4)/4=3;

SR_{13}^k – x_{13}^1= (2+3+2+4)/4=2,75; x_{13}^2=(3+2+2+1)/4=2;

x_{13}^3=(2+3 +1+1)/4=1,75; x_{13}^4=(3+4+3+4)/4=3,5; x_{13}^5=(4+3+2 +4)/4=3,25;

SR_{14}^k – x_{14}^1=(4+2+2+4)/4=3; x_{14}^2=(2+4 +3+2)/4=2,75;

x_{14}^3=(3+1+2+2)/4=2; x_{14}^4=(1+2+3+ 1)/4=1,75; x_{14}^5=(2+4+4+3)/4=3,25;

SR_{15}^k – x_{15}^1=(4+ 4+3+3)/4=3,5; x_{15}^2=(2+4+4+3)/4=3,25;

x_{15}^3=(2+4+3 +3)/4=3; x_{15}^4=(4+3+2+3)/4=3; x_{15}^5=(2+2+4+3)/4= 2,75.

2.5. кестесінде ұсынылған есептеулер нәтижесі бойынша SR_{12}, SR_{13}, SR_{14}, SR_{15}ережелері үшін ең жақсы нәтиже сәйкесінше SR_{12}^2, SR_{13}^3, SR_{14}^4, SR_{15}^5 Альтернативті нұсқаларына ие болады.

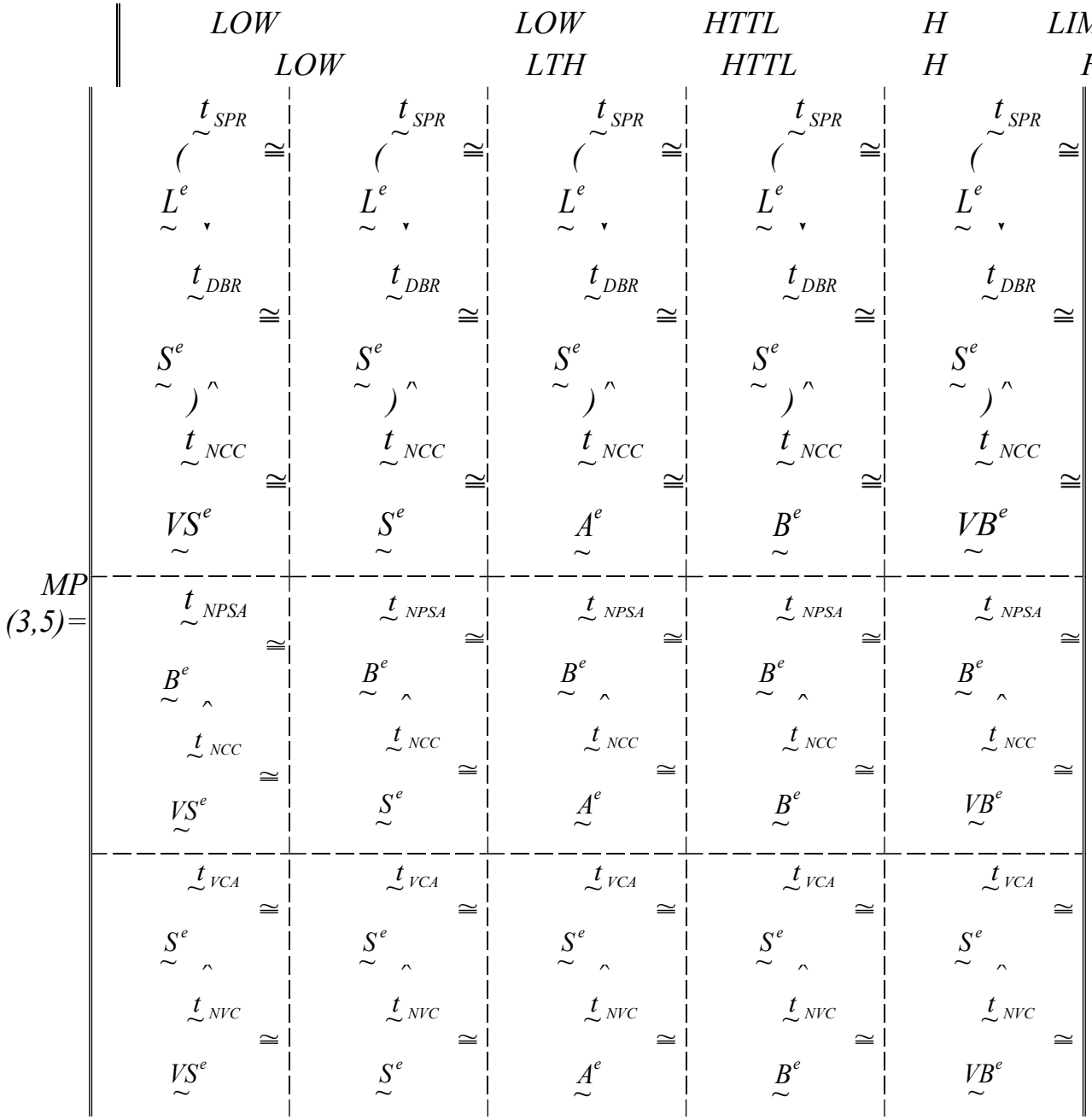
Алынған мәліметтерді шабуылдарды анықтаудың қазіргі заманғы құралдарының тәжірибелік модельлері үшін шынайы ережелер құрғанда нақты мәндер есебінде тікелей қолдануға болады. Осы мақсатта (2.22) ескере отырып, қажет мәліметтерді құрылымдауды ***FI***және***MP*** жиындары үшін инициализация матрицаларын (МІ) енгізу арқылы жүзеге асырамыз. Олар сәйкесінше *FI(n, r_n)* және*MP(n, r_n)*белгіленеді,яғни

$$FI(n, r_n)=\begin{Vmatrix} FI(1,1), & FI(1,2), & FI(1,3), & \dots, & FI(1,r_n) \\ FI(2,1), & FI(2,2), & FI(2,3), & \dots, & FI(2,r_n) \\ FI(3,1), & FI(3,2), & FI(3,3), & \dots, & FI(3,r_n) \\ \dots & \dots & \dots & \dots & \dots \\ FI(n,1), & FI(n,2), & FI(n,3), & \dots, & FI(n,r_n) \end{Vmatrix}$$ және

$$MP(n,r_n)=\begin{Vmatrix} MP(1,1), & MP(1,2), & MP(1,3), & \dots, & MP(1,r_n) \\ MP(2,1), & MP(2,2), & MP(2,3), & \dots, & MP(2,r_n) \\ MP(3,1), & MP(3,2), & MP(3,3), & \dots, & MP(3,r_n) \\ \dots & \dots & \dots & \dots & \dots \\ MP(n,1), & MP(n,2), & MP(n,3), & \dots, & MP(n,r_n) \end{Vmatrix}. \quad (2.23)$$

Мысалы, егер n=3 және r_n=5 сарапшы бағаларының негізінде [10] келесі МІ *FI(3, 5)* және *MP(3, 5)*анықталды, яғни

$$FI(3,5)=\begin{Vmatrix} LOW & LTH & HTTL & H & LIM \end{Vmatrix}$$



$t_{\sim NCC}$ $t_{\sim SPR}$ $t_{\sim DBR}$ $t_{\sim NPSA}$ $t_{\sim VCA}$ $t_{\sim NVC}$

осындағы , , , , , **–NCC**, **SPR**, **DBR**, **NPSA**, **VCA**, **NVC**шамаларының ағымдағы мәндері және қоршаған ортадағы шама идентификациялау [4] болып табылады.

(2.24) қолданылатын «≅»таңбасы – «Анық емес теңдік»ретінде түсіндіріледі және шаманың ағымдағы мәні (мысалы, $t_{\sim SPR}$ $L^e_{\sim}$) ең жақын«≅ »таңбасының сол жағында орналасқан берілген жиынның (мысалы, $T^e_{SPR} = \{L^e_{\sim}, A^e_{\sim}, H^e_{\sim}\}$),элементтердің біріне (мысалы, $L^e_{\sim}$) ең жақын «≅»таңбасының сол

жағында орналасқан яғни $\underset{\sim}{t}_{SPR} \cong \underset{\sim}{L}^{e}$ жазбасын: «T^{e}_{SPR} енетін $\underset{\sim}{L}^{e}$ ең жақын орналасқан $\underset{\sim}{t}_{SPR}$ » ретінде түсіндіріледі.

Ары қарай MI ескере отырып ($i=1$, $j=\overline{1,5}$ болса) *FI* үшін (n, r_n) және $MP(n, r_n)$ (2.23) және (2.24) өрнектерінің негізінде Dos (DDos) сияқты шабуылдарды туындатуы мүмкін ауытқушылық жағдайын анықтау үшін $\boldsymbol{SR_1}$үшін ережелер ішкі жиынын құрамыз.

$$\boldsymbol{SR_1}=\left\{\begin{array}{l} SR_{11}=((\underset{\sim}{t}_{SPR} \cong \underset{\sim}{L}^{e} \vee \underset{\sim}{t}_{DBR} \cong \underset{\sim}{S}^{e}) \wedge \underset{\sim}{t}_{NCC} \cong \underset{\sim}{VS}^{e}) \in L, \\ SR_{12}=((\underset{\sim}{t}_{SPR} \cong \underset{\sim}{L}^{e} \vee \underset{\sim}{t}_{DBR} \cong \underset{\sim}{S}^{e}) \wedge \underset{\sim}{t}_{NCC} \cong \underset{\sim}{S}^{e}) \in LTH, \\ SR_{13}=((\underset{\sim}{t}_{SPR} \cong \underset{\sim}{L}^{e} \vee \underset{\sim}{t}_{DBR} \cong \underset{\sim}{S}^{e}) \wedge \underset{\sim}{t}_{NCC} \cong \underset{\sim}{A}^{e}) \in HTTL, \\ SR_{14}=((\underset{\sim}{t}_{SPR} \cong \underset{\sim}{L}^{e} \vee \underset{\sim}{t}_{DBR} \cong \underset{\sim}{S}^{e}) \wedge \underset{\sim}{t}_{NCC} \cong \underset{\sim}{B}^{e}) \in H, \\ SR_{15}=((\underset{\sim}{t}_{SPR} \cong \underset{\sim}{L}^{e} \vee \underset{\sim}{t}_{DBR} \cong \underset{\sim}{S}^{e}) \wedge \underset{\sim}{t}_{NCC} \cong \underset{\sim}{VB}^{e}) \in LIM. \end{array}\right\} \quad (2.25)$$

(2.25) өрнегіндегі SR_{15} ережесін тікелей келесі түрде түсіндіруге болады: $\underset{\sim}{t}_{SPR}$ $\underset{\sim}{t}_{DBR} \cong \underset{\sim}{S}^{e}$ $\underset{\sim}{t}_{NCC} \cong \underset{\sim}{VB}^{e}$ «Егер немесе және сонымен бірге болса, онда Dos-шабуыл тудырған ауытқушылық жағдайының деңгейі Limits болады».

(2.25) өрнегінің ережелерінің ішкі жиындарынан әрбір SR_{1j} $(j=\overline{1,5})$ түйіндес жұбы үшін ШЕ әдісінің көмегімен МК есебіне сәйкес қолданыла отырып ***FI***нақты мәндері анықталған. Осы мәліметтерді қолдана отырып алмастыру немесе сканерлеу тудырған ауытқуларды анықтауға арналған ережелерді ережелерді құруға болады[4, 5]. Осылайша (2.23) және (2.24)өрнектерін есепке ала отырып $i=\overline{2,3}$ және $j=\overline{1,5}$ болғанда $\boldsymbol{SR_2}$үшін (2.26) және $\boldsymbol{SR_3}$ (2.27) үшін ережелер жиыны келесі түрге ие болады:

$$\boldsymbol{SR_2}=\left\{\begin{array}{l} SR_{21}=(\underset{\sim}{t}_{NPSA} \cong \underset{\sim}{B}^{e} \wedge \underset{\sim}{t}_{NCC} \cong \underset{\sim}{VS}^{e}) \in L, \\ SR_{22}=(\underset{\sim}{t}_{NPSA} \cong \underset{\sim}{\ }^{e} \wedge \underset{\sim}{\ }_{NCC} \cong \underset{\sim}{S}^{e}) \in \ , \\ SR_{23}=(\underset{\sim}{t}_{NPSA} \cong \underset{\sim}{\ }^{e} \wedge \underset{\sim}{\ }_{NCC} \cong \underset{\sim}{A}^{e}) \in \ , \end{array}\right. \quad (2.26)$$

$$SR_{24}=(\underset{\sim}{t}_{NPSA}\cong\underset{\sim}{B}^{e}\wedge\underset{\sim}{H}_{NCC}\cong\underset{\sim}{\ }^{e})\in\ ,$$

$$SR_{25}=(\underset{\sim}{t}_{NPSA}\cong\underset{\sim}{B}^{e}\wedge\underset{\sim}{t}_{NCC}\cong\underset{\sim}{V}^{e})\in LIM$$

$$\},$$

сонымен қатар

$$SR_{31}=(\underset{\sim}{t}_{VCA}\cong\underset{\sim}{S}^{e}\wedge\underset{\sim}{t}_{NVC}\cong\underset{\sim}{VS}^{e})\in L,$$

$$SR_3=\{$$

$$SR_{32}=(\underset{\sim}{t}_{VCA}\cong\underset{\sim}{S}^{e}\wedge\underset{\sim}{t}_{NVC}\cong\underset{\sim}{S}^{e})\in LTH,$$

$$SR_{33}=(\underset{\sim}{t}_{VCA}\cong\underset{\sim}{S}^{e}\wedge\underset{\sim}{t}_{NVC}\cong\underset{\sim}{A}^{e})\in HTTL,$$

$$SR_{34}=(\underset{\sim}{t}_{VCA}\cong\underset{\sim}{S}^{e}\wedge\underset{\sim}{t}_{NVC}\cong\underset{\sim}{B}^{e})\in H,$$

$$SR_{35}=(\underset{\sim}{t}_{VCA}\cong\underset{\sim}{S}^{e}\wedge\underset{\sim}{t}_{NVC}\cong\underset{\sim}{VB}^{e})\in LIM \qquad 2.27)$$

$$\}.$$

SR_{25} (2.26) өрнегіндегі SR_{25} ережесін тікелей келесі түрде түсіндіруге $\underset{\sim}{t}_{NPSA}\cong\underset{\sim}{B}^{e}$ $\underset{\sim}{t}_{NCC}\cong\underset{\sim}{VB}^{e}$ болады:«Егер және сонымен бірге болса, онда алмастыру тудырған ауытқушылық жағдайының деңгейі Limits болады».

Осылайша, анық емес жүйедегі математикалық модельдер «шабуыл : шамалар», «шабуыл:түйіндес жұптар жиыны» жұптар жиынын қолданатын рәсімдерді жүзеге асыру есебінен әдістер мен жүйелерді құруға мүмкіндік береді, сонымен бірге ЭШМ және БШМ АЖ –дегі кибершабуылдардың белгілі бір түрі тудырған ауытқушылық жағдайын көрсетеді. Осы модель негізінде сканерлеу, спуфинг (алмастыру) және Dos-шабуыл сияқты шабуылдарды анықтауға арналған ережелер модельдері құрастырылды, олар компьютерлік жүйелерде шабуыл әрекеттері туындатқан ауытқушылықтарды анықтау механизмін қолданатын шабуылдардың шынайы жүйесін жетілдіруге тәжірибе жүзінде қолдангылуы мүмкін.

2.4 Альтернативті маңыздылық коэффициенттерін бағалау үшін таңдау критерийлерін анықтау әдістері

1.3 [2, 5, 83, 95] бабындағы зерттеу заманауи МК қалыптастыру әдістеріне арналады, бірақ оларда АЖ ауытқушылық жағдайын анықтауға байланысты міндеттерді шешудегі қолданылу ерекшеліктері ашылған жоқ және СБ іске асыру кезінде маңызды болып табылатын қандай да бір әдістерді таңдауға әсері бар критерийлер тұрғысынан талдау жасалды.Осыған байланысты МК анықтау әлістері (1.3.бабын қараңыз) үшін оларды салыстыруға және тәжірибе жүргізудің нақты жағдайында мақсатқа сәйкес қолдануына әсер ететін факторларды анықтауға болатын критерийлерді анықтадық. Сапалы әдістер сараптама мақсаты берілген

критерийлерге сәйкес объектіні бағалау мақсаты қойылған жағдайларда жарамды екенін атап өткен жөн, ал сандық сипаттама екінші кезектегі міндет болады[95].Керісінше жағдайда сандық бағаларды алу үшін сандық әдістерді қолдану қажет.

Алғашқысы МД болып табылатын сапалық әдістердің ерекшеліктерін қарастырайық(1.3.бабын қараңыз) [2, 5].Сарапшылар әдеттегідей әдістегі өз бағаларын түзейтін кезеңдер саны шектелмеген және СТ жұмысын ұйымдастыруға белгілі қиындықтар тудыратын уақытты созуға әкелетінін ескерген жөн. Бұл жағынан ДӘ қолайлы болып табылады.Оның ерекшеліктерін нақты мысал арқылы қарастырайық.

АЖР үшін сарапшыларға қауіпсіздік шамалары(параметрлері) арқылы көрінетін альтернативті қаралаған жөн:

- ақпараттың құпиялылығы (АҚ);
- рұқсатнама арқылы өту (РАӨ);
- құпиясөзді қауіпсіз сақтау (ҚҚС);
- қауіпсіздік оқиғаларын тіркеу (ҚОТ);
- мамандарды таңдау және тестілеу (МТТ);
- үй-жайларға қолжетімділік (ҮҚ).

2.6. кестесінде әрбір сарапшы ұсынған дәрежелер көрсетілген. Екінші сарапшы үшін РАӨ, ҚҚС және ҮҚ альтернативті шамалас, сондықтан олардың дәрежесін ол 2,3 және 4 дәрежелердің орташа арифметикалық өлшемін анықтады: *(2+3+4)/3=3*. Үшінші сарапшы үшін АҚ мен МТТ шамалары тең дәрежелі болды, олардың дәрежесі *(3+4)/2=3,5*ретінде анықталды.

Кесте 2.6 -ДӘ үшін сарапшылар берген дәрежелер

Шамалар	Сарапшылар			
	1	2	3	4
АҚ	2	1	3,5	3
РАӨ	1	3	2	4
ҚҚС	3	3	1	2
ҚОТ	6	5	5	5
МТТ	5	6	3,5	6
ТҚ	4	3	6	1

Аталған әдістің артықшылығы оның қарапайымдылығы болып табылады, бірақ альтернативті саны өте көп болғанда (10 нан артық) сарапшыға реттілік сақтау қиынға түседі және қателер мүмкіндігі ұлғаяды.

ЖС бағалай келе (1.3.бабын қараңыз) ол БӘ мен ДӘ арасындағы аралық орында болса, екіншіден сарапшылық пайымды анықтауға арналған ақпарат көлемін объектіні қатарынан бір емес бірнеше объектімен салыстыру нәтижесінде БӘ салыстырғанда көбірек ақпарат қолдануға мүмкіндік береді, басқа жағынан көп объектілерді дәрежелеу арқылы тәжірибенің сапасынан білінетін сарапшының жұмысы күрделене

түседі.Соңғы жағдайдағы әдіс ақпарат көлемін қисынды шекке дейін азайуға мүмкіндік береді.

АВ ерекшеліктерін(1.3.бабын) нақты мысал арқылы көрсетейік. Сарапшыға алты шаманы талдап(2.6 кестесін)және олардың салыстырмалы артықшылықтарын анықтау ұсынылды.

$A \in \{КИ, ППП, БХП, ФИБ, ОИТК, ДКП\}$ альтернативті жиынының әрбір шамасы үшін қауіпсіздік шамаларының санын көрсететін, ағымдағыға қарағанда маңыздырақ болатын $П_i$ бағасы анықталады. Нәтижесінде қарапайым түрде сарапшының басымдықтарын көрсететін $П = \{0,3,1,5,4,2\}$ қалау векторын аламыз.

КТ әдістер класы туралы айтқанда(1.3.бабын қараңыз), әрбір кластерде жекелеген өңдеу әдісіне жататын олардың артықшылығы кластерлеу мәліметтерді түсінуді жеңілдетеді.

КЖ және желілердегі ауытқушылық жағдайды анықтауға міндеттерді шешуде альтернативті ережелерді бағалауды жүзеге асыру сандық қалау бағаларын алумен көбірек байланысты. Алғашқысы ЕКШ болып табылатын баяндалған сандық әдістердің (1.3.бабын) ерекшеліктерін қарастырайық. Бұл жерде ЕКШ алу үшін мәліметті матрицалық модельде ұсынған ыңғайлы, нәтижесі – сызықтық, қатынастар шкаласы қолданылады, ал әдістің шығындылығын орташа деп бағалауға болады.

Ары қарай нақты мысал арқылы КЖ ерекшеліктерін көрсетейік.АЖР-да КЖ және желілердегі шабуыл бес қорғаныш шамасын жұптық салыстыру жағдайын қарастырайық. ЖС матрицасы келесі түрге ие:

$$A = \begin{bmatrix} a_{11} & a_{12} & a_{13} & a_{14} & a_{15} \\ a_{21} & a_{22} & a_{23} & a_{24} & a_{25} \\ a_{31} & a_{32} & a_{33} & a_{34} & a_{35} \\ a_{41} & a_{42} & a_{43} & a_{44} & a_{45} \\ a_{51} & a_{52} & a_{53} & a_{54} & a_{55} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 2 & 2 & 1 \\ 2 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 2 & 2 \\ 0 & 2 & 0 & 1 & 1 \\ 1 & 2 & 0 & 1 & 1 \end{bmatrix}$$

Алғашқы итерацияны матрицаның әрбір жолына элементтер қосу арқылы аламыз:

$$P^1(1) = \sum_{j=1}^{5} a_{1j} = 1+0+2+2+1 = 6, \quad P^2(1) = 4, P^3(1) = 6, P^4(1) = 4, P^5(1) = 5.$$

Екі критерий бірінші орында(6балл) және екеуі үшінші орында(4балл). Екінші итерацияны матрица жолдарына туынды элементті және бұрынғы итерацияның сәйкес нәтижесін қосу арқылы жүзеге асырамыз:

$$P^1(2) = a_{11} \times P^1(1) + a_{12} \times P^2(1) + \ldots + a_{15} \times P^5(1) = (1 \times 6) + (0 \times 4) + (2 \times 6) + (2 \times 4) + (1 \times 5) = 31,$$

$$P^2(2) = 22, P^3(2) = 28, \; P^4(2) = 17, \; P^5(2) = 23.$$

Бірінші критерий бірінші орында екені көрінеді және кейінгі итерациялар үшін де бөлініс өзгеріссіз қалады – бірінші критерий бірінші орында болады:

$$P^1(3) = a_{11} \times P^1(2) + a_{12} \times P^2(2) + \ldots + a_{15} \times P^5(2) =$$
$$(1 \times 31) + (0 \times 22) + (2 \times 28) + (2 \times 17) + (1 \times 23) = 144,$$
$$P^2(2) = 112,\ P^3(3) = 130,\ P^4(3) = 84,\ P^5(3) = 115.$$

Осылайша, үшінші итерацияның нәтижесін алмастырып (1.2) және МК анықтауға болады:

$$P_3^1 = 144/(144 + 112 + 130 + 84 + 115) = 144/585 = 0,24,$$
$$P_3^2 = 112/585 = 0,191,$$
$$P_3^3 = 130/585 = 0,22,$$
$$P_3^4 = 84/585 = 0,14,$$
$$P_3^5 = 115/585 = 0,196.$$

Қарастырылған мысалды ескере отырып, бастапқы деректеді көрсету сәйкесінше матрицалық және сызықтық болатынын, шкалада қатынастар қолданылатыны, ал әдістің еңбек сыйымдылығы орташа екенін анықтауға болады.

МСТ ерекшеліктерін (1.3.бабын қараңыз) нақты мысал арқылы қарастырайық. Шкала ретінде салыстырмалы маңыздылық шкаласы қолданылады:

0 – сарапшыға салыстыру қиын,
1 – екі альтернатив тең,
3 – тәжірибе мен пайым бір альтернативтіге қарағанда екіншісіне жеңіл артықшылық береді,
5 – тәжірибе мен пайым бір альтернативтінің екіншісіне қарағанда көбірек қалау береді,
7 – альтернативті бірі екіншісіне қарағанда біршама басымдық береді,
9 – бір альтернативтінің екіншісіне қарағанда артықшылығы анық көрінеді,
2, 4, 6, 8 –ортақ жағдайларда.

Егер бірінші альтернативті екіншімен салыстырғанда алынған жоғарыда аталған сан (3) болса, онда екінші альтернативті біріншімен салыстырғанда керісінше шама шығады(1/3).

КЖ мен желілердегі шабуылдан АЖР төрт қауіпсіздік шамаларының маңыздылығын бағалаған жөн (2.6. кесте). Есептеулер 2.7 кестесінде көрсетілген.

Кесте 2.7 -МСТ бойынша алынған МК есептеулері

МСТ бойынша алынған МК есептеулері

Шамалар	АҚ	ҮҚ	ҚҚС	РАӨ	$\tilde{\lambda}_i$	λ_i
I	***II***	III	IV	V	VI	VII
АҚ	1	3	5	9	3,41	0,581
ТҚ	1/3	1	3	5	1,5	0,255
ДҚС	1/5	1/3	1	3	0,67	0,114
РАӨ	1/9	1/5	1/3	1	0,29	0,050

Қосынды	5,87	1

МСТ қолдану қиындығы арнайы ұсынылған шкала көмегімен берілетін ЖС матрицасының өз векторын табумен байланысты. Бұған қоса есептеу қиындығы шама (анық емес терм) берілген әмбебап жиынның өлшемінің өсуімен ұлғая түседі. Бұл тұрғыдан Коггер және Ю ұсынған әдіс күрделілігі кемдеу болып табылады.

Сонымен қоса бастапқы деректер матрица түрінде, шығыс деректер-кесте түрінде қалыптасады, шкалада қатынастар негізінде жүзеге асады, ал еңбек сыйымдылығы жоғары деп бағаланатынын да атай кеткен жөн.

Осыған ұқсас түрде КЮӘ бағалай отырып шкала, бастапқы және шығыс деректерді ұсыну МСТ ұқсастығын байқаймыз, бірақ одан айырмашылығы КЮӘ еңбек сыйымдылығы орташа.

ФНМ қатысты ол барлық критерийлерді жұптастырып салыстырады және әрбір осындай салыстыруға сандық баға беретінін айтуға болады. Бірақ ары қарай әдісті қолдануды қиындататын үлкен көлемдегі түзетулер енгізу қажеттігі туындайды. Деректерді білдіру түріне, шкаласы мен еңбек сыйымдылығына тоқталса, олар МСТ ұқсас болып келеді.

ЮӘ бағалай отырып, аталған әдіс есептеу күрделілігі тұрғысынан Саати векторлары әдісімен салыстырғанда біршама жақсы шешім береді, бірақ шкала, деректер және еңбек сыйымдылығы критерийлері бірдей болады.

Ары қарай ОӘ ерекшеліктерін (1.3.бабын қараңыз) [2] нақты мысал арқылы қарастырайық. КЖ мен $i=\{1,2,3,4\}$АА, ВВ, СС, DD компания әзірлеушілерінен желілердегі басып кірулерден АЖР қорғаудың төрт жобасы үшін жүлделі орындарды анықтау талап етіледі делік. Барлық жобалар төрт сарапшыға жіберілді $j=\{1,2,3,4\}$. 2.8 кестесінде әрбір сарапшығы тағайындалған жоба дәрежелері берілген.

$x_1 = (1+2+1+1)/4 = 5/4 = 1{,}25;$

$x_2 = 15/4 = 3{,}75;\ x_3 = 8/4 = 2;\ x_4 = 12/4 = 3.$

Кесте 2.8 - ОӘ әдісі бойынша алынған жоба дәрежелері және МКОӘ әдісі бойынша алынған жоба дәрежелері және МК

Жоба	Сарапшылар				x_i	λ_i
	1	2	3	4		
АА (1)	1	2	1	1	1,25	0,12
ВВ (4)	4	4	3	4	3,75	0,37
СС (2)	3	1	2	2	2	0,2
DD (3)	2	3	4	3	3	0,3

МК $\lambda_i = x_i / N$ арқылы анықталады, осындағы N –барлық дәрежелердің қосындысы ($N=10$). Нәтиже бойынша бірінші орын – АА, екінші орын – СС, үшінші орын – DD, төртінші орын –ВВ екені көрінеді. Әдістің артықшылығы қолдану қарапайымдылығы және есептеу жылдамдығы. Сарапшылардың таразылай бағалауы (біліктілік коэффициенті) ұғымын қосымша енгізе отырып нақтылығын жоғарылатуға болады.

Мысалға қарай отырып бастапқы деректерді енгізу түрі - кестелік, шығыс деректерін енгізу-сызықтық, шкала-реттеу тәртібінде, еңбек сыйымдылығы төмен екені көрінеді.

БФДЖ ерекшеліктерін (1.3.бабын қараңыз) [2] нақты мысал арқылы қарастырайық. $n=m=4$үшін ОӘ әдісімен мысалдағы мәліметтерді қолданамыз. Есептеу 2.9 кестесінде берілген:

$$\lambda_1 = [2[4(4+1)] - (1+2+1+1)] / [4 \times 4(4+1)] = 35/80 = 0{,}0625;$$

$$\lambda_2 = 25/80 = 0{,}2;$$

$$\lambda_3 = 32/80 = 0{,}1;$$

$$\lambda_4 = 31/80 = 0{,}15.$$

Кесте 2.9 - БФДЖ әдісі бойынша алынған жоба дәрежелері және МК БФДЖ әдісі бойынша алынған жоба дәрежелері және МК

Жоба	Сарапшылар				λ_i
	1	2	3	4	
АА (1)	1	2	1	1	0,0625
ВВ (4)	4	4	3	4	0,2
СС (2)	3	1	2	2	0,1
DD (3)	2	3	4	3	0,15

Жобалар бойынша орындарды бөлу нәтижесі ОӘ әдісінде алынған нәтижемен сәйкес келетіні айқын.Әдістің кемшілігі сарапшылардың біліктілік коэффициентін есепке алмау болып табылады.Олар тең білім дәрежесіне ие және маңыздылығына қарай критерийлерді топтарға бөлуге болмайды деп саналады.Еңбек сыйымдылығы, шкала және деректерді ұсыну түріне қарай олар ОӘ әдісіне ұқсас болып келеді.

ЧА ерекшеліктерін (1.3.бабы)[2] 2.6кестесіндегі АЖР қауіпсіздік шамаларымен нақты мысал арқылы қарастырайық.Критерийлерді маңыздылық дәрежесіне қарай реттейік:

O_1 – АҚ; O_2 – ҮҚ; O_3 – БҚҚ; O_4 – РАӨ; O_5 – МТТ; O_6 – ҚОТ.

1 мәнін неғұрлым маңыздырақ нәтижеге және кейбір басқа мәндерді басқа нәтижелерге меншіктейміз.Бұл шамаларды $V_1,\ldots V_6$таңбаларымен белгілейміз, осындағы $V_1=1;\ V_2=0{,}7;\ V_3=0{,}6;\ V_4=0{,}5;\ V_5=0{,}4;\ V_6=0{,}3$.

O_1–ді $O_2+O_3+O_4+O_5+O_6$ –мен салыстырамыз. Нәтиже:

$O_1O_2+O_3+O_4+O_5+O_6$ қарағанда аз қолайлырақ, сондықтан $V_1< V_2+V_3+V_4+V_5+V_6$.

$O_1O_2+O_3+O_4+O_5$ қарағанда аз қолайлырақ, сондықтан $V_1<V_2+V_3+V_4+V_5$.

$O_1O_2+O_3+O_4$ қарағанда аз қолайлырақ, сондықтан $V_1<V_2+V_3+V_4$.

$O_1O_2+O_3$ салыстырғанда басымырақ, сондықтан бағалардың мәнін$V_1>V_2+V_3$тенсіздігі орындалу үшін өзгертеміз, ол үшін V_1–ге 1,5 мәнін меншіктейміз.

Келесі қадам: O_2–ні $O_3+O_4+O_5+O_6$-мен салыстырамыз.

$O_2O_3+O_4+O_5+O_6$қарағанда аз қолайлырақ, сондықтан $V_2<V_3+V_4+V_5+V_6$.

$O_2O_3+O_4+O_5$қарағанда аз қолайлырақ, сондықтан $V_2<V_3+V_4+V_5$.

$O_2O_3+O_4$-пен салыстырғанда басымырақ, сондықтан бағалардың мәнін$V_2>V_3+V_4$тенсіздігі орындалу үшін өзгертеміз, ол үшін V_2–ге 1,2мәнін меншіктейміз.

Ары қарай $O_3O_4+O_5+O_6$ –мен салыстырамыз.

$O_3O_4+O_5+O_6$ қарағанда аз қолайлырақ, сондықтан $V_3<V_4+V_5+V_6$.

$O_3O_4+O_5$-пен салыстырғанда басымырақ, сондықтан бағалардың мәнін$V_3>V_4+V_5$ тенсіздігі орындалу үшін өзгертеміз, ол үшін V_3–ге 1 мәнін меншіктейміз.

Осыған ұқсас амалмен $O_4O_5+O_6$ –мен салыстырамыз.

$O_4O_5+O_6$ қарағанда маңыздырақ, сондықтан бағалардың мәнін $V_4>V_5+V_6$ теңсіздігі орындалу үшін өзгертеміз, ол үшін V_4–ге 0,8 мәнін меншіктейміз;

$V_5=0,4$;

$V_6=0,3$.

Ең соңында V_iәрбір оң мәнін шамалардың салмақтық мәнін түрлендіреміз:

$$x_i = V_i \Big/ \sum_{i=1}^{n} V_i$$

және $x_1=0,288,\ x_2=0,23,\ x_3=0,192,\ x_4=0,15,\ x_5=0,08,\ x_6=0,576$ аламыз.

ЧА әдісінің кемшілігі ретінде егер nүлкен болса оның қолданылуы бейнетті болып табылады. Бұл жағдайда Альтернативтіды топтарға бөлу оқтайды, ал альтернативті бірін, мысалы, максималды альтернативті барлық топтарға қосқан жөн. Бұл барлық альтернативті сандық бағаларын әрбір топ шегінде бағалау көмегімен алуға мүмкіндік береді. Қарастырылған мысалда есепке ала отырып ЧА –да мәліметтерді ұсыну түрі сызықтық, рет шкаласы қолданылады, еңбек сыйымдылығы орташа.Көрсетілген критерийлерге сәйкес ПЛ сипаттамалары ұқсас.

ҚТ әдістерінің қосалқы тобына қатысты зерттеулер олар үшін мәліметтерді ұсыну түрі сызықтық, шкала қатынастар негізінде жүзеге асады, еңбек сыйымдылығы жоғары.

МТӘ ерекшеліктерін (1.3.бабын қараңыз) [2] нақты мысал арқылы қарастырайық. КЖ басып кірулерден АЖР қорғау жобаларының ішінен оңтайлысын анықтайық. Сарапшылар жобаларды маңыздылығы сәйкесінше бес балдық шкала бойынша $\lambda_i=[0,5;\ 0,2;\ 0,3]$ үш шама - құны(Қ), еңбек сыйымдылығы (ЕС) және құрушының тәжірибесі (Т) бойынша бағалады. Бағалар 2.10 кестесінде ұсынылған.

$$f(1)=\min[f_1(1)\times\lambda_1; f_2(1)\times\lambda_2; f_3(1)\times\lambda_3]=\min[4\times0,5;3\times0,2;4\times0,3]=0,6;$$

$$f(2)=\min[f_1(2)\times\lambda_1; f_2(2)\times\lambda_2; f_3(2)\times\lambda_3]=\min[3\times0,5;1\times0,2;2\times0,3]=0,2;$$

$$f(3)=\min[0,5;0,4;1,2]=0,4;$$

$$f(4)=\min[1;0,4;0,6]=0,4.$$

Оңтайлы шешім максимум ретінде анықталады:

$$U(f_1(x),\ldots,f_n(x))=\max[f(1);f(2);f(3);f(4)]=[0,6;0,2;0,4;0,4]=0,6.$$

Кесте 2.10 -МТӘ критерийлеріне сәйкес жобалар бағалары МТӘ критерийлеріне сәйкес жобалар бағалары

Жоба	Критерийлер		
	С	Тр	О
АА	4	3	4
ВВ	3	1	2
СС	1	2	4
DD	2	2	2

Осылайша, АА тобының құрушылары ұсынған жоба ең жақсы болады.

Келтірілген мысалға сәйкес бастапқы деректерді ұсыну трі-матрицалық, шығыс деректері –сызықтық, ал еңбек сыйымдылығы төмен деп бағаланатынын атап өткен жөн.

Ары қарай МФӘ ерекшеліктерін (1.3.бабын қараңыз)[2]нақты мысал арқылы қарастырайық. МТӘ арналған мысал моделінде КЖ басып кірулерден АЖР қорғау жобаларының ішінен оңтайлысын анықтайық. (1.4.)сәйкес 2.10. кестесінде көрсетілген бағаларды қолданамыз.

$$U(f(1)) = [f_1(1)]^{\lambda_1} \times [f_2(1)]^{\lambda_2} \times [f_3(1)]^{\lambda_3} = 4^{0,5} \times 3^{0,2} \times 4^{0,3} \approx 4,77;$$

$$U(f(2)) = [f_1(2)]^{\lambda_1} \times [f_2(2)]^{\lambda_2} \times [f_3(2)]^{\lambda_{31}} = 3^{0,5} \times 1^{0,2} \times 2^{0,3} \approx 3,96;$$

$$U(f(3)) = 1^{0,5} \times 2^{0,2} \times 4^{0,3} \approx 3,67;$$

$$U(f(4)) = 2^{0,5} \times 2^{0,2} \times 2^{0,3} \approx 3,79.$$

Олай болса, берілген әдіс бойынша да КЖ мен желілерде басып кірулерден АЖР қорғаудың ең жақсы жобасы АА тобымен құрылған. Қарастырылған мысалды ескере отырып ҚФ әдістер тобы мәліметтерді ұсынудың сызықтық түрін қолданады, шкала негізі ретінде қатынастар алынады, ал еңбек сыйымдылығы жоғары деп бағаланады.

Нақты мысал арқылы ЧК және ИНА тобына енетін басқа әдістерді қарастырайық.ЧК негізінде (1.3.бабын қараңыз)[2]МТӘ арналған мысал моделінде, 2.10.кесте деректері негізінде КЖ басып кірулерден АЖР қорғаудың ең жақсы қауіпсіздік жобасын анықтайық, бірақ осы жолы $x_i^* = [3;2;3]$, $\lambda_i = [0,5; 0,2; 0,3]$ сияқты критерийлер бойынша оңтайлы бағаларды берейік.(1.5.) негізінде $p=2$ үшін метрика құрамыз және оны әрбір жоба үшін есептеу арқылы оңтайлы критерийлерге ең жақын жобаны анықтаймыз.

$$L_1(x) = \sqrt{(0,5((3-4)/(3-4))^2 + (0,2((2-3)/(2-3))^2 + (0,3((3-4)/(3-4))^2} \approx 0,62;$$

$$L_2(x) = \sqrt{(0,5((3-3)/(3-4))^2 + (0,2((2-1)/(2-3))^2 + (0,3((3-2)/(3-4))^2} \approx 0,36;\ L_3(x) \approx 1,04;$$

$$L_4(x) \approx 0,58.$$

Сондықтан, берілген шарттарға сәйкес оңтайлысы ВВ тобының жобасы болып табылады.

Келтірілген мысалды ескере отырып, ИНА әдістер тобының бастапқы деректерді ұсыну түрі – сызықтық, шығыс деректерін ұсыну – графикалық(ЧК үшін) және сызықтық (РБМ және ОША үшін) екенін айтуға болады, ұсынылатын шкала интервалды (ЧК үшін) және қатынастық (РБМ мен ОА үшін), еңбек сыйымдылығы ЧК мен РБМ үшін жоғары, ал ОА үшін төмен деуге болады.

ОКТ нақты мысалының моделі арқылы ТНА әдістер тобының (1.3.бабын қараңыз)[2] ерекшеліктерін қарастырайық. МСТ арналған мысалдан шамалардың ауытқу дәрежесі бойынша (1.6) анықтайық. $\alpha_i = 2$ константа (тұрақты шама) болып табылсын.2.11.кестесінде СБ және шамалар мәні тепе-теңдік нүктесінде болып табылады:

$$g_1(x) = [0,3 - 0,5]^2 [0,9 - 0,5]^2 [0,6 - 0,5]^2 [0,7 - 0,5]^2 = 0,256;$$

$$g_2(x) = [0,7 - 0,4]^2 [0,3 - 0,4]^2 [0,6 - 0,4]^2 [0,8 - 0,4]^2 = 0,576;$$

$$g_3(x) = [0,4 - 0,5]^2 [0,1 - 0,5]^2 [0,2 - 0,5]^2 [0,2 - 0,5]^2 = 0,13;$$

$$g_4(x) = [0,9 - 0,6]^2 [0,3 - 0,6]^2 [0,4 - 0,6]^2 [0,3 - 0,6]^2 = 0,3.$$

Кесте 2.11 - ОКТ әдісі бойынша алынған дәрежелерОКТ әдісі бойынша алынған дәрежелер

Шамалар	Сарапшылар				x_i^*
	1	2	3	4	
АҚ	0,3	0,9	0,6	0,7	0,5
ТҚ	0,7	0,3	0,5	0,8	0,4
ҚҚС	0,4	0,1	0,2	0,2	0,5
РАӨ	0,9	0,3	0,4	0,3	0,6

Қарастырылатын топ үшін бастапқы және шығыс деректерін ұсыну түрі сәйкесінше сызықтық және графикалық, ұсынылатын шкала-интервалдық, ал еңбек сыйымдылығы орташа деп бағаланатынын атап өткен жөн.

АС әдістер класынан (1.3.бабын қараңыз)[2] нақты мысал арқылы ТРС қарастырайық. 10 сарапшыдан тұратын СТ назарына әлеуметтік шабуылдарсаласынан 7 пайымдау ұсынылды.

х={“парольдерді электронды түрде сақтау ”;

“электронды пошта арқылы түскен барлық салымдарды ашуға болады”;

“телефон арқылы сұраныс жіберетін адамдарға ақпарат ұсыну керек ”;

“басшы жұмысшы қасиеттерін қатесіз бағалай алады ”,

“жетекшінің кез келген бұйрықтарын орындауы тиіс”;

“сұраушыны идентификациялау жағдайында ғана ақпарат беру ”}.

СТ әрбір пайымға 1-11 аралығында дәреже беру қажет (2.12.кестесін қараңыз).Әрбір пікірге балл сарапшылардың бағаларының бөлінісімен анықталады, сондықтан келесі кезеңнің басы ретінде (шкала құру) пікірді белгілі топтамаға салған сарапшылардың пайыздарын есептеу болып табылады.

Кесте 2.12 -ТРС әдісі бойынша алынған *X* пайымдырының дәрежесіТРС әдісі бойынша алынған *X* пайымдырының дәрежесі

X	Сарапшылар									
	1	2	3	4	5	6	7	8	9	10
x_1	2	1	5	1	11	5	5	3	8	5
x_2	5	2	3	2	10	4	6	2	10	4
x_3	8	10	6	3	9	3	7	1	11	3
x_4	6	9	7	4	8	2	8	7	9	2
x_5	4	8	4	5	7	1	9	8	1	1
x_6	3	7	11	6	6	10	10	9	2	6
x_7	11	6	1	7	5	9	11	10	3	7

Ары қарай алдыңғы және аталған үдемеге қатысты пікірін білдірген жиынтық (шоғырландыру) сарапшылар пайызы саналады. 2.13. кестесінде жиынтық пайыз ($K_{\%}$) – жинақталған пайыз (дәрежелердің ағымдағы және алдыңғы мәндерінің жиынтығы), *M* – медиана, Q_1 жәнеQ_3 – сәйкесінше бірінші және үшінші квартильдер, Q_3 -Q_1 –МК квартильді ізделінетін .

АӘ (құрамына ТРС кіреді) және ҚҚ мен КВ әдістер тобының кіріс деректерін ұсыну түрі – сызықтық(ТРС, ШҚТҚ және КВ үшін) және матрицалық(ҚҚ үшін), ұсынылатын шкала-интервалды(ТРС, ШҚТҚ және КВ үшін) және ретті(ҚҚ үшін),ал АӘ топтары үшін еңбек сыйымдылығы төмен, ҚҚ мен КВ үшін жоғары деп бағаланады.

Осылайша,сараптаманың қорытынды нәтижесін қалыптастыруға әрқайсысы қағида тұрғысында қолданыла алмайтын МК анықтаудың бірнеше жолы бар екенін көреміз, бәрақ жекелеген жағдайларда бір әдістерге артықшылық берілсе, өзгелері әр түрлі себептерге байланысты қолданылмауы мүмкін.

МК есептеу әдісін таңдауға әсер ететін негізгі фактор ретінде шамаладың физикалық кейпі мен олардың арасындағы қатынас болып табылады. Шамалар сараптама мақсатына сәйкес анықталады. Ары қарай шамалар арасындағы өзара байланы дәрежесін анықтаған жөн – тәуелділігі немесе дербестігі жәнеөзара байланыс сипаты (пайдалылық дербестігі, артықшылығы бойынша, ен жарлығы бойынша және т.б.)

Кесте 2.13 - ТРС әдісі бойынша МК есептеу нәтижелері ТРС әдісі бойынша МК есептеу нәтижелері

$X/K_{\%}$ $X/K_{\%}$	Пайымдар дәрежелері және шоғырландырылмалы пайыз										Бөлініс шамалары			
											M	Q_1	Q_3	Q_3 - Q_1
x_1	1	1	2	3	5	5	5	5	8	11	23	11,5	34,5	23
$K_{\%}$	1	2	4	7	12	17	22	27	35	46				
x_2	2	2	2	3	4	4	5	6	10	10				

$K_{\%}$	2	4	6	9	13	17	22	28	38	48	24	12	36	24
x_3	1	3	3	3	6	7	8	9	10	11	30,5	15,25	45,75	30,5
$K_{\%}$	1	4	7	10	16	23	31	40	50	61				
x_4	2	2	4	6	7	7	8	8	9	9	31	15,5	46,5	31
$K_{\%}$	2	4	8	14	21	28	36	44	53	62				
x_5	1	1	1	4	4	5	7	8	8	9	24	12	36	24
$K_{\%}$	1	2	3	7	11	16	23	31	39	48				
x_6	2	3	6	6	6	7	9	10	10	11	35	17,5	52,5	35
$K_{\%}$	2	5	11	17	23	30	39	49	59	70				
x_7	1	3	5	6	7	7	9	10	11	11	35	17,5	52,5	35
$K_{\%}$	1	4	9	15	22	29	38	48	59	70				

Шынайы тілдесулер мен сараптаманы өткізу мүмкіндіктері арқылы анықталатын сараптаманы өткізу күрделілігі және **СЗ** алудың еңбек сыйымдылығы маңызды фактор болып табылады.

1.3. бабында көрсетілгендей [2, 83] ТРС әдісін саралауға сарапшылармен неғұрлым аз тілдесу уақыты қажет, ал “Дельфи”әдісі сарапшылармен ең көп тілдесу уақыты қажет (саралауға 12 есе көбірек және ЧА әдісіне қарағанда 2 есе көбірек).

МК анықтау әдісін таңдауға сарапшы бағаларының арасындағы келісім дәрежесі де әсер етеді. Келісім дәрежесі бірінші кезекте СТ сарапшылар санына және олардың біліктілік дәрежесіне байланысты. Сонымен қатар оған МК бағалауға таңдалаған әдіс те әсер етеді.

Осылайша, сарапшылар арасындағы ең жоғары келісушілікті МД қамтамасыз етеді, ал ең аз келісім дәрежесін –тікелей сандық бағалау қамтамасыз етеді, оны саралау қарапайымдылығына байланысты барынша нақты МК және ДӘ әдісі арқылы алынған мәндері жақын МК алуға мүмкіндік бар. Сарапшылық деректерді өңдеудің еңбек сыйымдылығы ақпараттық технологиялардың қазіргі заманғы дамуы деңгейінде басты фактор болып табылмайды. Дегенмен СЗ өңдеудің күрделі әдістерін қолдануға сараптаманы жүргізу мерзіміне әсер ететін арнайы БҚ құруды қажет етуі мүмкін.Бұл тұрғыдан алып қарағанда дәрежелік және нүктелік әдістер неғұрлым қарапайымдары болып табылады.

КЖ ауытқушылық жағдайын анықтаудың анықтау міндетін шешуші ережелер неғұрлым оңтайлы әдісін таңдау критерийлеріне шкала арқылы бағалауды жүзеге асыру мен есептеулерді іске асырудың еңбек сыйымдылығына қолданылатын мәліметтерді ұсыну формасы болып табылады.

Көрнекілік пен мүмкіндік (ұсынылған критерийлер негізінде) үшін 2.14.кестесінде берілген жүргізілген зерттеулер нәтижесінде МК анықтау әдістерін салыстыруды жүзеге асырамыз, осындағы кіріс (КД) және шығыс деректері (ШД) матрицалық(М), кестелік(К),сызықтық(С),графикалық (Г) мәліметтерді ұсыну түрі атаулар шкаласы (АШ), реттік(РШ), интервалдық (ИШ), қатынастық (ҚШ) ұсыну шкаласы (ҰШ), еңбек сыйымылығы(ЕС) жоғары(Ж), орташа(О) және төмен (Т) деп бағаланады.

Кесте 2.14 -Шабуылдарды анықтау жүйесі үшін СБ әдістерінің сараптама нәтижелері

Шабуылдарды анықтау жүйесі үшін СБ әдістерінің сараптама нәтижелері							
Әдістер				Бағалау критерийлері			
Әдістер класы	Әдістер тобы	Қосалқы әдістер	Әдіс	Ұсыну түрі		РШ	ТР
				КД	ШД		
МК	НК			М	Л	ШО	С
	СВ		ВУ	М	Л	ШО	С
			МСТ	М	Т	ШО	В
			МКЮ	М	Т	ШО	С
			ФНМ	М	Т	ШО	В
			МЮ	М	Т	ШО	В
КД			СР	Т	Л	ШП	Н
	ТР	АПМФ		Т	Л	ШП	Н
		АРП	ЧА	Л	Л	ШП	С
			ЛКП	Л	Л	ШП	С
АФП	ОКП	АС	СТ	Л	Л	ШО	В
			ЮТ	Л	Л	ШО	В
			КР	Л	Л	ШО	В
		ММС		М	Л	ШО	Н
	ФЦ	МСК		Л	Л	ШО	В
		ПСК		Л	Л	ШО	В
ОТР	ОИТ	ЧК		Л	ГР	ШИ	В
		НСМ		Л	Л	ШО	В
		КО		Л	Л	ШО	Н
	ООТР	КТИ		Л	ГР	ШИ	С
		ТИ		Л	ГР	ШИ	С
ТЧ	МП	ТРС		Л	ГР	ШИ	Н
		ПЛПР		Л	ГР	ШИ	Н
	ПДК			Л	М	ШП	В
	СЛВ			Л	ГР	ШИ	В

2.5 Альтернативті маңыздылық коэффициенттерін бағалау үшін таңдау критерийлерін анықтау әдістері

V_{ij} шамасының ауытқушылық жағдайына қатысты сарапшы пайымдарын бейнелейтін $\mathbf{T}_{ij}^{e}$ (2.1-2.2баптарын) лингвистикалық эталондарының ішкі жиынын құру үшін нақты қоршаған ортаға арналған берілген Лингвистикалық айнымалы топтарының эталондарын алу үрдісін әлсіздендіруге мүмкіндік беретін сәйкес әдіс құрастырамыз. Лингвистикалық эталондарды қалыптастыру әдісі (ЛЭҚӘ) [10] компьютерлік желілердегі шабуылдарды анықтауды анықтау міндеттерін шешуге бағытталған, МЛТС [24] ары қарай даму болып табылады және алты кезеңге негізделеді.

1 кезең –Лингвистикалық бағалар идентификациялаудың ішкі жиынын қалыптастыру. $\mathbf{LE}_{i}$ ішкі жиынын құру

$$\mathbf{LE} = \{\bigcup_{l=1}^{c} LE_l\} = \{LE_1, LE_2, ..., LE_c\}, (l = \overline{1,c}), \tag{2.28}$$

ретінде ұсынылатын және сарапшының Лингвистикалық бағаларының (пайымдарының) барлық ықтимал идентификациялау (С) жиындарының негізінде жүзеге асырылады және олар $\mathbf{V_i}$ шамасының жағдай сипаттамасы үшін қолданылатын сарапшы пайымында (2.1бабын қараңыз) бақылағанда көрінеді, осындағы m-өлщемді гетерогенді параметрлі қоршаған орта, ал c – осындай С саны.

Мысалы егер $c = 10$ (2.28) сәйкес $\mathbf{LE}$ жиынын келесі түрде көрсетуге болады:

$$\begin{gathered}\mathbf{LE} = \{\bigcup_{l=1}^{10} LE_l\} = \{LE_1, LE_2, ..., LE_{10}\} = \\ \{LE_{VS}, LE_S, LE_A, LE_B, LE_{VB}, LE_Y, LE_M, LE_O, LE_L, LE_H\} = \\ \{"VS", "S", "A", "B", "VB", "Y", "M", "O", "L", "H"\},\end{gathered} \tag{2.29}$$

где $LE_1 = LE_{VS} = "VS"$, $LE_2 = LE_S = "S"$, $LE_3 = LE_A = "A"$, $LE_4 = LE_B = "B"$, $LE_5 = LE_{VB} = "VB"$, $LE_6 = LE_Y = "Y"$, $LE_7 = LE_M = "M"$, $LE_8 = LE_O = "O"$, $LE_9 = LE_L = "L"$ и $LE_{10} = LE_H = "H"$ сәйкесінше «VERYSMALL» (егер $l = 1$), «SMALL» (егер $l = 2$), «AVERAGE» (егер $l = 3$), «BIG» (егер $l = 4$), «VERY BIG» (егер $l = 5$), «YOUTH» (егер $l = 6$), «MEDIUM» (егер $l = 7$), «OLD» (егер $l = 8$), «LOW» (егер $l = 9$) және «HIGH» (егер $l = 10$) сияқты сарапшының Лингвистикалық бағаларының (пайымдарының) С болып табылады.

Ары қарай сарапшы пайымдарының С ішкі жиынын қалыптастырамыз

$$\{\bigcup_{i=1}^{n} \mathbf{LE_i}\} = \{\mathbf{LE_1}, \mathbf{LE_2}, \ldots, \mathbf{LE_n}\}, \tag{2.30}$$

осындағы $\mathbf{LE_i} \subseteq \mathbf{LE}$, $(i = \overline{1,n})$

$$\mathbf{LE_i} = \{\bigcup_{j=1}^{m_i} \mathbf{LE_{ij}}\} = \{\mathbf{LE_{i1}}, \mathbf{LE_{i2}}, \ldots, \mathbf{LE_{im_i}}\}, \tag{2.31}$$

ретінде анықтаймыз, осындағы $\mathbf{LE_{ij}} (j = \overline{1,m_i}) V_{ij}$ (2.1 бабын қараңыз) шамасының мәндеріне қатысты сарапшы пайымының С ішкі жиыны болып табылады, осындағы m-өлшемді гетерогенді параметрлі қоршаған орта. (31) формуланы ескере отырып (30) келесі түрде жазамыз:

$$\begin{gathered}\{\bigcup_{i=1}^{n} \mathbf{LE_i}\} = \{\bigcup_{i=1}^{n} \{\bigcup_{j=1}^{m_i} \mathbf{LE_{ij}}\}\} = \{\{\mathbf{LE_{11}}, \mathbf{LE_{12}}, \ldots, \mathbf{LE_{1m_1}}\}, \\ \{\mathbf{LE_{21}}, \mathbf{LE_{22}}, \ldots, \mathbf{LE_{2m_2}}\}, \ldots, \{\mathbf{LE_{n1}}, \mathbf{LE_{n2}}, \ldots, \mathbf{LE_{nm_n}}\}\}.\end{gathered} \tag{2.32}$$

Осылайша, $\mathbf{LE_{ij} \subseteq LE_i}$ есепке ала отырып, j-шамаға қатысты сарапшы r_j жиынтығынан пікір (лингвистикалық бағаларды)

$$\mathbf{LE_{ij}} = \{\bigcup_{k=1}^{r_j} LE_{ijk}\} = \{LE_{ij1}, LE_{ij2}, \ldots, LE_{ijr_j}\}, \tag{2.33}$$

ішкі жиынынан көрінеді, осындағы $LE_{ijk}\ (k = \overline{1, r_j})$ –нақты қоршаған ортаның i-шабуылы кезіндегі j-шаманың күйіне қатысты сарапшының Лингвистикалық бағасының k идентификациялау болып табылады, ал r_j – LE_{ij} идентификациялау саны.

Ары қарай (32) өрнегін (33) есепке ала отырып келесі түрге енеді:

$$\{\bigcup_{\mathbf{i=1}}^{\mathbf{n}} \mathbf{LE_i}\} = \{\bigcup_{\mathbf{i=1}}^{\mathbf{n}} \{\bigcup_{\mathbf{j=1}}^{\mathbf{m_i}} \mathbf{LE_{ij}}\}\} = \{\bigcup_{i=1}^{n} \{\bigcup_{j=1}^{m_i} \{\bigcup_{k=1}^{r_j} LE_{ijk}\}\}\} =$$

$$\{\{\{LE_{111}, LE_{112}, \ldots, LE_{11r_1}\}, \{LE_{121}, LE_{122}, \ldots, LE_{12r_2}\}, \ldots,$$
$$\{LE_{1m_1 1}, LE_{1m_1 2}, \ldots, LE_{1m_1 r_{m_1}}\}\},$$
$$\{\{LE_{211}, LE_{212}, \ldots, LE_{21r_1}\}, \{LE_{221}, LE_{222}, \ldots, LE_{22r_2}\}, \ldots,$$
$$\{LE_{2m_2 1}, LE_{2m_2 2}, \ldots, LE_{2m_2 r_{m_2}}\}\}, \ldots,$$
$$\{\{LE_{n11}, LE_{n12}, \ldots, LE_{n1r_1}\}, \{LE_{n21}, LE_{n22}, \ldots, LE_{n2r_2}\}, \ldots,$$
$$\{LE_{nm_n 1}, LE_{nm_n 2}, \ldots, LE_{nm_n r_{m_n}}\}\}. \tag{2.34}$$

Мысалы, $n = 3$ болса (яғни $I_1 = I_{SN} = SN = SCANNING$, $I_2 = I_{DS} = DS = DOS$ және $I_3 = I_{SP} = SP = SPOOFING$), $m_1 = m_3 = 2$, $m_2 = 3$, $r_1 = 5$, $r_2 = r_3 = 3$ С бар шабуылдар үшін (34) өрнегін келесі түрде анықтауға болады:

$$\{\bigcup_{\mathbf{i=1}}^{\mathbf{3}} \mathbf{LE_i}\} = \{\bigcup_{\mathbf{i=1}}^{\mathbf{3}} \{\bigcup_{\mathbf{j=1}}^{\mathbf{m_i}} \mathbf{LE_{ij}}\}\} = \{\bigcup_{i=1}^{3} \{\bigcup_{j=1}^{m_i} \{\bigcup_{k=1}^{r_j} LE_{ijk}\}\}\} =$$

$$\{\{\{LE_{111}, LE_{112}, LE_{113}, LE_{114}, LE_{115}\}, \{LE_{121}, LE_{122}, LE_{123}\}\},$$
$$\{\{LE_{211}, LE_{212}, LE_{213}, LE_{214}, LE_{215}\}, \{LE_{221}, LE_{222}, LE_{223}\}, \{LE_{231}, LE_{232},$$
$$LE_{233}\}\},$$
$$\{\{LE_{311}, LE_{312}, LE_{313}, LE_{314}, LE_{315}\}, \{LE_{321}, LE_{322}, LE_{323}\}\} =$$
$$\{\{\{LE_{SNNVC1}, LE_{SNNVC2}, LE_{SNNVC3}, LE_{SNNVC4}, LE_{SNNVC5}\},$$
$$\{LE_{SNVCA1}, LE_{SNVCA2}, LE_{SNVCA3}\}\},$$
$$\{\{LE_{DSNCC1}, LE_{DSNCC2}, LE_{DSNCC3}, LE_{DSNCC4}, LE_{DSNCC5}\},$$
$$\{LE_{DSSPR1}, LE_{DSSPR2}, LE_{DSSPR3}\}, \{LE_{DSDBR1}, LE_{DSDBR2}, LE_{DSDBR3}\}\},$$
$$\{\{LE_{SPNCC1}, LE_{SPNCC2}, LE_{SPNCC3}, LE_{SPNCC4}, LE_{SPNCC5}\},$$

$$\{LE_{SPNPSA1}, LE_{SPNPSA2}, LE_{SPNPSA3}\}\}\} =$$
$$\{\{\{"VS", "S", "A", "B", "VB"\}, \{"Y", "M", "O"\}\},$$
$$\{\{"VS", "S", "A", "B", "VB"\}, \{"L", "A", "H"\}, \{"S", "A", "B"\}\},$$
$$\{\{"VS", "S", "A", "B", "VB"\}, \{"S", "A", "B"\}\}\},$$

осындағы: $LE_{111} = LE_{SNNVC1} = "VS"$, $LE_{112} = LE_{SNNVC2} = "S"$, $LE_{113} = LE_{SNNVC3} = "A"$, $LE_{114} = LE_{SNNVC4} = "B"$, $LE_{115} = LE_{SNNVC5} = "VB"$ и $LE_{121} = LE_{SNVCA1} = "Y"$, $LE_{122} = LE_{SNVCA2} = "M"$, $LE_{123} = LE_{SNVCA3} = "O"$ –сәйкесінше 2-өлшемді параметрлі ішкі ортада $V_{11} = V_{SNNVC} = NVC$ және $V_{12} = V_{SNVCA} = VCA$ шамаларының жағдайын бейнелейтін сарапшының лингвистикалық бағаларының C болып табылады;

$LE_{211} = LE_{DSNCC1} = "VS"$, $LE_{212} = LE_{DSNCC2} = "S"$, $LE_{213} = LE_{DSNCC3} = "A"$, $LE_{214} = LE_{DSNCC4} = "B"$, $LE_{215} = LE_{DSNCC5} = "VB"$, $LE_{221} = LE_{DSSPR1} = "L"$, $LE_{222} = LE_{DSSPR2} = "A"$, $LE_{223} = LE_{DSSPR3} = "H"$ и $LE_{231} = LE_{DSDBR1} = "S"$, $LE_{232} = LE_{DSDBR2} = "A"$, $LE_{233} = LE_{DSDBR3} = "B"$ –сәйкесінше 3-өлшемді параметрлі ішкі ортада $V_{21} = V_{DSNCC} = NCC$, $V_{22} = V_{DSSPR} = SPR$ және $V_{23} = V_{DSDBR} = DBR$ шамаларының жағдайын бейнелейтін сарапшының Лингвистикалық бағаларының C болып табылады;

$LE_{311} = LE_{SPNCC1} = "VS"$, $LE_{312} = LE_{SPNCC2} = "S"$, $LE_{313} = LE_{SPNCC3} = "A"$, $LE_{314} = LE_{SPNCC4} = "B"$, $LE_{315} = LE_{SPNCC5} = "VB"$ и $LE_{321} = LE_{SPNPSA1} = "S"$, $LE_{322} = LE_{SPNPSA2} = "A"$, $LE_{323} = LE_{SPNPSA3} = "B"$ – сәйкесінше 2-өлшемді параметрлі ішкі ортада $V_{31} = V_{SPNCC} = NCC$ және $V_{32} = V_{SPNPSA} = NPSA$ шамаларының жағдайын бейнелейтін сарапшының лингвистикалық бағаларының C болып табылады

Сарапшы белгілі қоршаған ортада бақылауға алынған түрлі шамалардың іс жүзіндегі мәндерінің жағдайы туралы өзінің пікірін білдіретінін ескере отырып, ол өзінің **LE** жиынынан көрінетін сәйкес Лингвистикалық пікірлерін қолдана алады. Мысалы $V_{11} = V_{SNNVC} = NVC$ ($LE_{111} = LE_{SNNVC1} = "VS"$) и $V_{21} = V_{DSNCC} = NCC$ ($LE_{211} = LE_{DSNCC1} = "VS"$) шамалары үшін $"VS"$ Лингвистикалық сарапшы бағасының C бар болғаны осы шамалардың нақты мәндерінің лингвистикалық альтернативті болып табылады және сарапшылардың сәйкес бағаларынан көрінетін белгілі салыстырмалы жағдайларын сипаттайды.

2 кезең –базалық жиілік матрицаларын қалыптастыру.Осындай матрицаны алу үшін **N** аралығындағы идентификациялау жиыны енгізіледі және $\mathbf{N_i}$ идентификациялаудың ішкі жиыны

$$\{\bigcup_{i=1}^{n} \mathbf{N_i}\} = \{\mathbf{N_1}, \mathbf{N_2}, \ldots, \mathbf{N_n}\}, \quad (2.35)$$

ретінде бейнеленеді, осындағы $\mathbf{N_i} \subseteq \mathbf{N}$, $(i = \overline{1,n})$ о

$$\mathbf{N_i} = \{\bigcup_{\mathbf{j=1}}^{\mathbf{m_i}} \mathbf{N_{ij}}\} = \{\mathbf{N_{i1}}, \mathbf{N_{i2}}, \ldots, \mathbf{N_{im_i}}\}, \tag{2.36}$$

ретінде анықтаймыз, осындағы $\mathbf{N_{ij}} (j = \overline{1,m_i})$ $-V_{ij}$ (2.1 бабын қараңыз)шамаларының m-өлшемді гетерогенді параметрлі қоршаған ортадағы мәндеріне қатысты сарапшы лингвистикалық бағалауды жүзеге асыратын анықтау аймағының аралықтарының С ішкі жиыны. (36) формуласын ескере отырып (35) келесі түрде жазамыз:

$$\{\bigcup_{\mathbf{i=1}}^{\mathbf{n}} \mathbf{N_i}\} = \{\bigcup_{\mathbf{i=1}}^{\mathbf{n}} \{\bigcup_{\mathbf{j=1}}^{\mathbf{m_i}} \mathbf{N_{ij}}\}\} = \tag{2.37}$$

$$\{\{\mathbf{N_{11}}, \mathbf{N_{12}}, \ldots, \mathbf{N_{1m_1}}\}, \{\mathbf{N_{21}}, \mathbf{N_{22}}, \ldots, \mathbf{N_{2m_2}}\}, \ldots, \{\mathbf{N_{n1}}, \mathbf{N_{n2}}, \ldots, \mathbf{N_{nm_n}}\}\}.$$

Ары қарай, $\mathbf{N_{ij}} \subseteq \mathbf{N_i}$ есепке ала отырып j-шамасына қатысты сарапшы өз бағаларына шекара қалыптастыру үшін

$$\mathbf{N_{ij}} = \{\bigcup_{k=1}^{r_j} N_{ijk}\} = \{N_{ij1}, N_{ij2}, \ldots, N_{ijr_j}\}, \tag{2.38}$$

ішкі жиыны арқылы көрінетін r_j аралықтарының жиынтығын қолдана алады, осындағы $N_{ijk} (k = \overline{1,r_j})$ – белгілі қоршаған ортадағы j-шамасының i шабуылының ағымдағы жағдайына қатысты сарапшы бағасының кездесу жиілігін қалыптастыруға қолданылатын k-аралығының идентификациялау, ал r_j – көрсетілген баға жүзеге асырылатын тиянақталған аралықтар идентификациялаудың саны. Сол кезде (37) өрнегі (38) есепке ала отырып келесі түрге енеді:

$$\{\bigcup_{\mathbf{i=1}}^{\mathbf{n}} \mathbf{N_i}\} = \{\bigcup_{\mathbf{i=1}}^{\mathbf{n}} \{\bigcup_{\mathbf{j=1}}^{\mathbf{m_i}} \mathbf{N_{ij}}\}\} = \{\bigcup_{i=1}^{n} \{\bigcup_{j=1}^{m_i} \{\bigcup_{k=1}^{r_j} N_{ijk}\}\}\} =$$

$$\{\{\{N_{111}, N_{112}, \ldots, N_{11r_1}\}, \{N_{121}, N_{122}, \ldots, N_{12r_2}\}, \ldots, \{N_{1m_11}, N_{1m_12}, \ldots, N_{1m_1r_{m_1}}\}\},$$

$$\{\{N_{211}, N_{212}, \ldots, N_{21r_1}\}, \{N_{221}, N_{222}, \ldots, N_{22r_2}\}, \ldots, \{N_{2m_21}, N_{2m_22}, \ldots, N_{2m_2r_{m_2}}\}\}, \ldots,$$

$$\{\{N_{n11}, N_{n12}, \ldots, N_{n1r_1}\}, \{N_{n21}, N_{n22}, \ldots, N_{n2r_2}\}, \ldots, \{N_{nm_n1}, N_{nm_n2}, \ldots, N_{nm_nr_{m_n}}\}\}\}. \tag{2.39}$$

$\mathbf{LE_{ij}}$ және $\mathbf{N_{ij}}$ ішкі жиындарының элементтерінің негізінде (2.15 кесте) сарапшының ағымдағы тиянақталған куәлігіне (пайымдарына, бағаларына) негізделген жалпыланған бағалар кестесі қалыптасады, осындағы f_{ijsq}

$(s,q=\overline{1,r_j})\_N_{ijq} \stackrel{def}{=} [N_{ijq}^{min};N_{ijq}^{max}]\ (q=\overline{1,r_j})$ идентификациялау аралығындағы j-шамасының жағдайын сипаттайтын бірдей пікірлердің($\mathbf{LE_{ij}}$ ішкі жиының Лингвистикалық бағаларын қолдану) санын (жиілігін) көрсететін эмпирикалық мәліметтер элементтері, осындағы N_{ijq}^{min} және N_{ijq}^{max} сәйкесінше q-аралығының төменгі және жоғарғы шекарасы.

Кесте 2.15 - $\mathbf{LE_{ij}}$ бойынша жалпыланған бағалар кестесі

$\mathbf{LE_{ij}}$	$\mathbf{N_{ij}}$					
	N_{ij1}	N_{ij2}	…	N_{ijq}	…	N_{ijr_j}
LE_{ij1}	f_{ij11}	f_{ij12}	…	f_{ij1q}	…	f_{ij1r_j}
LE_{ij2}	f_{ij21}	f_{ij22}	…	f_{ij2q}	…	f_{ij2r_j}
…	…	…	…	…	…	…
LE_{ijs}	f_{ijs1}	f_{ijs2}	…	f_{ijsq}	…	f_{ijsr_j}
…	…	…	…	…	…	…
LE_{ijr_j}	f_{ijr_j1}	f_{ijr_j2}	…	f_{ijr_jq}	…	$f_{ijr_jr_j}$

Ары қарай $\mathbf{LE_{ij}}$ (2.15 кестесін қараңыз) ішкі жиынының элементтері бойынша жалпыланған бағалар кестесінің негізінде базалық жиілік матрицасы қалыптасады

$$F_{ij}=\|f_{ijsq}\|=\begin{Vmatrix} f_{ij11} & f_{ij12} & \dots & f_{ij1q} & \dots & f_{ij1r_j} \\ f_{ij21} & f_{ij22} & \dots & f_{ij2q} & \dots & f_{ij2r_j} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ f_{ijs1} & f_{ijs2} & \dots & f_{ijsq} & \dots & f_{ijsr_j} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ f_{ijr_j1} & f_{ijr_j2} & \dots & f_{ijr_jq} & \dots & f_{ijr_jr_j} \end{Vmatrix}. \quad (2.40)$$

Мысалы, егер $\mathbf{T_{ij}^e}$ эталондарын құруға негіз болатын $F_{ij}(s,q=\overline{1,r_j})$ матрицасын қалыптастыру қажет және егер $n=3$ болса (яғни $I_1=I_{SN}=SN=SCANNING$, $I_2=I_{DS}=DS=DOS$ мен $I_3=I_{SP}=SP=SPOOFING$), $m_1=m_3=2$, $m_2=3$, $r_1=5$, $r_2=r_3=3$ С бар шабуылдар үшін) (39) өрнегін келесі түрде анықтауға болады:

$$\{\bigcup_{i=1}^{3}N_i\}=\{\bigcup_{i=1}^{3}\{\bigcup_{j=1}^{m_i}N_{ij}\}\}=\{\bigcup_{i=1}^{3}\{\bigcup_{j=1}^{m_i}\{\bigcup_{k=1}^{r_j}N_{ijk}\}\}\}= \quad (2.41)$$

$$\{\{\{N_{111}, N_{112}, N_{113}, N_{114}, N_{115}\}, \{N_{121}, N_{122}, N_{123}\}\},$$
$$\{\{N_{211}, N_{212}, N_{213}, N_{214}, N_{215}\}, \{N_{221}, N_{222}, N_{223}\}, \{N_{231}, N_{232}, N_{233}\}\},$$
$$\{\{N_{311}, N_{312}, N_{313}, N_{314}, N_{315}\}, \{N_{321}, N_{322}, N_{323}\}\} =$$
$$\{\{\{N_{SNNVC1}, N_{SNNVC2}, N_{SNNVC3}, N_{SNNVC4}, N_{SNNVC5}\},$$
$$\{N_{SNVCA1}, N_{SNVCA2}, N_{SNVCA3}\}\},$$
$$\{\{N_{DSNCC1}, N_{DSNCC2}, N_{DSNCC3}, N_{DSNCC4}, N_{DSNCC5}\},$$
$$\{N_{DSSPR1}, N_{DSSPR2}, N_{DSSPR3}\}, \{N_{DSDBR1}, N_{DSDBR2}, N_{DSDBR3}\}\},$$
$$\{\{N_{SPNCC1}, N_{SPNCC2}, N_{SPNCC3}, N_{SPNCC4}, N_{SPNCC5}\},$$
$$\{N_{SPNPSA1}, N_{SPNPSA2}, N_{SPNPSA3}\}\}.$$

Мысалы, (41) сәйкес егер $n=1$, (яғни $I_3=I_{SP}=SP=SPOOFING$) С бар шабуылдар үшін $i=3$ болса, ал $\{N_{321}, N_{322}, N_{323}\}$ $j=2$, $r_j=3$ үшін жалпыланған кестенің негізінде (2.15кестесін қараңыз) $LE_{ijk}=LE_{32k}=LE_{SPNPSAk}$ $(r_2=3,\ k=\overline{1,3})$ ішкі жиындарының элементтері бойынша ағымдағы бағалар кестесін құрамыз (2.16 кестесі), осындағы $LE_{321}=LE_{SPNPSA1}="S"$, $LE_{322}=LE_{SPNPSA2}="A"$, $LE_{323}=LE_{SPNPSA3}="B"$ и $N_{ijk}=N_{32k}=N_{SPNPSAk}$, а $N_{ij1}=N_{321}=N_{SPNPSA1} \stackrel{def}{=} [N^{min}_{SPNPSA1}; N^{max}_{SPNPSA1}] <=> [0;\ 10]$, $N_{ij2}=N_{322}=N_{SPNPSA2} \stackrel{def}{=} [N^{min}_{SPNPSA2}; N^{max}_{SPNPSA2}] <=> [11;\ 100]$, $N_{ij3}=N_{323}=N_{SPNPSA3} \stackrel{def}{=} [N^{min}_{SPNPSA3}; N^{max}_{SPNPSA3}] <=> [101;\ 1000]$.

Кесте 2.16 - $\mathbf{LE_{32}}$ бойынша ағымдағы бағалар кестесі

$\mathbf{LE_{32}=}$ $\mathbf{LE_{SPNPSA}}$	$\mathbf{N_{32}=N_{SPNPSA}}$		
	$N_{SPNPSA1}$	$N_{SPNPSA2}$	$N_{SPNPSA3}$
$"S"$	3	1	0
$"A"$	1	4	2
$"B"$	0	2	3

Ары қарай, $s,q=\overline{1,3}$ болғанда (40) өрнекке сәйкес 2.16 кестесінің мәліметтерін қолданып жиілік матрицасын қалыптастырамыз, яғни

$$F_{32}=F_{SPNPSA}=\|f_{32sq}\|=\|f_{SPNPSAsq}\|=$$

$$\left\| \begin{matrix} f_{3211} & f_{3212} & f_{3213} \\ f_{3221} & f_{3222} & f_{3223} \\ f_{3231} & f_{3232} & f_{3233} \end{matrix} \right\| = \left\| \begin{matrix} 3 & 1 & 0 \\ 1 & 4 & 2 \\ 0 & 2 & 3 \end{matrix} \right\|$$

3 кезең –туынды жиілік матрицасын қалыптастыру.Бұл кезеңді жүзеге асыру үшін жиілік матрицасының сәйкес бағандары бойынша қосынды векторы құрылады (40), яғни

$$VS_{ij} = \left\| vs_{ijq} \right\| = \left\| vs_{ij1}, vs_{ij2}, ..., vs_{ijq}, ..., vs_{ijr_j} \right\| =$$
$$\left\| \sum_{s=1}^{r_j} f_{ijs1}, \sum_{s=1}^{r_j} f_{ijs2}, ..., \sum_{s=1}^{r_j} f_{ijsq}, ..., \sum_{s=1}^{r_j} f_{ijsr_j} \right\| = \left\| \bigcup_{q=1}^{r_j} \sum_{s=1}^{r_j} f_{ijsq} \right\|, \ (s,q = \overline{1,r_j}), \tag{2.42}$$

осындағы f_{ijsq} - элементы матрицы F_{ij} матрицасының элементтері. Ары қарай VS_{ij} мүшелерінен

$$vsm_{ij} = \bigvee_{q=1}^{r_j} vs_{ijq}, \tag{2.43}$$

формуласы бойынша максималды мәнді анықтаймыз, ол туынды жиілік матрицасын қалыптастыру үшін қолданылады.

$$F_{ij}^{'} = \left\| f_{ijsq}^{'} \right\| = (vsm_{ij} / vs_{ijq}) \left\| f_{ijsq} \right\| \Leftrightarrow$$
$$F_{ij}^{'} = (vsm_{ij} / vs_{ijq}) F_{ij} =$$
$$\left\| \begin{matrix} f_{ij11}^{'} & f_{ij12}^{'} & \dots & f_{ij1q}^{'} & \dots & f_{ij1r_j}^{'} \\ f_{ij21}^{'} & f_{ij22}^{'} & \dots & f_{ij2q}^{'} & \dots & f_{ij2r_j}^{'} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ f_{ijs1}^{'} & f_{ijs2}^{'} & \dots & f_{ijsq}^{'} & \dots & f_{ijsr_j}^{'} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ f_{ijr_j1}^{'} & f_{ijr_j2}^{'} & \dots & f_{ijr_jq}^{'} & \dots & f_{ijr_jr_j}^{'} \end{matrix} \right\| \tag{2.44}$$

$F_{ij}^{'}$ қалыптастыруды нақты мысал арқылы қарастырайық. Ол үшін $i=3$, $j=2$ болса, (42) өрнекті қолдана отырып жиілік матрицасының бағандарына сәйкес $VS_{ij} = VS_{32}$ қосынды векторын құрамыз, яғни

$$VS_{32} = \left\| vs_{32q} \right\| = \left\| vs_{321}, vs_{322}, vs_{323} \right\| = \left\| \bigcup_{q=1}^{3} \sum_{s=1}^{3} f_{32sq} \right\| \Leftrightarrow$$

$$VS_{SPNPS} = \left\| vs_{SPNPSAq} \right\| = \left\| vs_{SPNPSA1}, vs_{SPNPSA2}, vs_{SPNPSA3} \right\| =$$
$$\left\| \bigcup_{q=1}^{3} \sum_{s=1}^{3} f_{SPNPSAsq} \right\| = \| 4, 7, 5 \|, \ (q = \overline{1, 3}).$$

Ары қарай $VS_{32} = VS_{SPNPSA}$ (43) формуласы арқылы максималды элементті анықтаймыз.

$$vsm_{32} = \bigvee_{q=1}^{3} vs_{32q} = vs_{321} \vee vs_{322} \vee vs_{323} =$$
$$4 \vee 7 \vee 5 = vsm_{SPNPSA} = 7,$$

ал туынды жиілік матрицасын

$$F'_{32} = \left\| f'_{32sq} \right\| = (vsm_{32} / vs_{32q}) \left\| f_{32sq} \right\| = F'_{SPNPSA}$$

(44) өрнекке сәйкес аламыз

$$F'_{SPNPSA} = (vsm_{SPNPSA} / vs_{SPNPSAq}) F_{SPNPSA} =$$
$$\begin{Vmatrix} 5,3 & 1 & 0 \\ 1,8 & 4 & 2,8 \\ 0 & 2 & 4,2 \end{Vmatrix}.$$

4 кезең –анық емес термдерді қалыптастыру. $\mathbf{T_i}$ анық емес термдер ішкі жиынын құру m_i-өлшемді параметрлі ішкі ортада $\mathbf{V_i}$ сәйкес шамасының нақты жағдайларын бейнелейтін барлық ықтимал $\mathbf{T}$ термдерінің жиыны негізінде құрылады, яғни

$$\{\bigcup_{i=1}^{n} \mathbf{T_i}\} = \{\mathbf{T_1}, \mathbf{T_2}, \ldots, \mathbf{T_n}\}, \tag{2.45}$$

осындағы $\mathbf{T_i} \subseteq \mathbf{T}$, $(i = \overline{1,n})$, ал

$$\mathbf{T_i} = \{\bigcup_{j=1}^{m_i} \mathbf{T_{ij}}\} = \{\mathbf{T_{i1}}, \mathbf{T_{i2}}, \ldots, \mathbf{T_{im_i}}\}, \tag{2.46}$$

осындағы $\mathbf{T_{ij}}$ $(j = \overline{1,m_i})$ V_{ij} (2.1 бабын қараңыз) шамасының мәндеріне қатысты анық емес термдердің ішкі жиыны болып табылады. (46) формуланы есепке ала отырып (45) келесі түрде жазамыз:

$$\{\bigcup_{i=1}^{n} \mathbf{T_i}\} = \{\bigcup_{i=1}^{n} \{\bigcup_{j=1}^{m_i} \mathbf{T_{ij}}\}\} =$$
$$\{\{\mathbf{T_{11}}, \mathbf{T_{12}}, \ldots, \mathbf{T_{1m_1}}\}, \{\mathbf{T_{21}}, \mathbf{T_{22}}, \ldots, \mathbf{T_{2m_2}}\}, \ldots, \{\mathbf{T_{n1}}, \mathbf{T_{n2}}, \ldots, \mathbf{T_{nm_n}}\}\}, \tag{2.47}$$
$$(j = \overline{1,m_i}).$$

Осылайша, $\mathbf{T_{ij}} \subseteq \mathbf{T_i}$ және (47) ескере отырып анық емес термдердің ішкі жиынын келесі түрде анықтаймыз:

$$\mathbf{T_{ij}} = \overset{\{\bigcup_{s=1}^{r_j} \underset{\sim}{T}_{ijs}\}}{} = \{\underset{\sim}{T}_{ij1}, \underset{\sim}{T}_{ij2}, \ldots, \underset{\sim}{T}_{ijr_j}\}, \tag{2.48}$$

осындағы $\underset{\sim}{T}_{ijs}\ (s = \overline{1,r_j})$ – анық емес термдер, ал r_j – $\mathbf{T_{ij}}$ мүшелер саны.

Ары қарай (47) өрнегі (48) есепке ала отырып келесі түрге енеді:

$$\{\bigcup_{i=1}^{n} \mathbf{T_i}\} = \{\bigcup_{i=1}^{n}\{\bigcup_{j=1}^{m_i} \mathbf{T_{ij}}\}\} = \{\bigcup_{i=1}^{n}\{\bigcup_{j=1}^{m_i}\{\bigcup_{s=1}^{r_j} \underset{\sim}{T}_{ijs}\}\}\} =$$

$$\begin{gathered}\{\{\{\underset{\sim}{T}_{111}, \underset{\sim}{T}_{112}, \ldots, \underset{\sim}{T}_{11r_1}\}, \{\underset{\sim}{T}_{121}, \underset{\sim}{T}_{122}, \ldots, \underset{\sim}{T}_{12r_2}\}, \ldots, \{\underset{\sim}{T}_{1m_1 1}, \underset{\sim}{T}_{1m_1 2}, \ldots, \underset{\sim}{T}_{1m_1 r_{m_1}}\}\}, \\ \{\{\underset{\sim}{T}_{211}, \underset{\sim}{T}_{212}, \ldots, \underset{\sim}{T}_{21r_1}\}, \{\underset{\sim}{T}_{221}, \underset{\sim}{T}_{222}, \ldots, \underset{\sim}{T}_{22r_2}\}, \ldots, \{\underset{\sim}{T}_{2m_2 1}, \underset{\sim}{T}_{2m_2 2}, \ldots, \underset{\sim}{T}_{2m_2 r_{m_2}}\}\}, \\ \ldots, \\ \{\{\underset{\sim}{T}_{n11}, \underset{\sim}{T}_{n12}, \ldots, \underset{\sim}{T}_{n1r_1}\}, \{\underset{\sim}{T}_{n21}, \underset{\sim}{T}_{n22}, \ldots, \underset{\sim}{T}_{n2r_2}\}, \ldots, \{\underset{\sim}{T}_{nm_n 1}, \underset{\sim}{T}_{nm_n 2}, \ldots, \underset{\sim}{T}_{nm_n r_{m_n}}\}\}\}.\end{gathered} \tag{2.49}$$

Ары қарай $\underset{\sim}{T}_{ijs}$ құрамдас бөлігінің мәнін қалыптастыру қажет, ол үшін келесі түрлендірулерді қолданамыз. F'_{ij} матрицасының элементтері бойынша (50) өрнегіне сәйкес максимум векторы құрылады

$$FM_{ij} = \left\| fm_{ijq} \right\| = \left\| fm_{ij1}, fm_{ij2}, \ldots, fm_{ijq}, \ldots, fm_{ijr_j} \right\| =$$

$$\left\| \underset{s=1}{\overset{\forall j}{\vee}} f'_{ijs1}, \underset{s=1}{\overset{\forall j}{\vee}} f'_{ijs2}, \ldots, \underset{s=1}{\overset{\forall j}{\vee}} f'_{ijsq}, \ldots, \underset{s=1}{\overset{\forall j}{\vee}} f'_{ijsr_j} \right\| = \left\| \bigcup_{q=1}^{r_j} \underset{s=1}{\overset{\forall j}{\vee}} f'_{ijsq} \right\|, (s,q = \overline{1,r_j}). \tag{2.50}$$

FM_{ij} негізінде қатыстылық функциясы матрицасын қалыптастырамыз

$$M_{ij} = \left\| \mu_{ijsq} \right\| = \begin{Vmatrix} \mu_{ij11} & \mu_{ij12} & \ldots & \mu_{ij1q} & \ldots & \mu_{ij1r_j} \\ \mu_{ij21} & \mu_{ij22} & \ldots & \mu_{ij2q} & \ldots & \mu_{ij2r_j} \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ \mu_{ijs1} & \mu_{ijs2} & \ldots & \mu_{ijsq} & \ldots & \mu_{ijsr_j} \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ \mu_{ijr_j 1} & \mu_{ijr_j 2} & \ldots & \mu_{ijr_j q} & \ldots & \mu_{ijr_j r_j} \end{Vmatrix}, \tag{2.51}$$

Оның әрбір элементі $\mu_{ijsq} = f'_{ijsq} / fm_{ijs}\ (s,q = \overline{1,r_j})$ өрнегі бойынша анықталады. (51) қолдана отырып

$$\underset{\sim}{T}_{ijs} = \overset{\{\bigcup_{q=1}^{r_j} \mu_{ijsq} / x_{ijsq}\} =}{} \{\mu_{ijs1} / x_{ijs1}, \mu_{ijs2} / x_{ijs2}, \ldots, \mu_{ijsr_j} / x_{ijsr_j}\}, (q = \overline{1,r_j}), \tag{2.52}$$

өрнегінің негізінде $\underset{\sim}{T}_{ijs}$ анық емес термдерінің жиынтығын анықтаймыз, осындағы

$$x_{ijsq} = N_{ijq}^{max} / N_{ijr_j}^{max}\ (q = \overline{1,r_j}). \tag{2.53}$$

$\underset{\sim}{T}_{ijs}\,(s=\overline{1,r_j})$ АЕС сәйкесінше $\mathbf{LE_{ij}} \subseteq \mathbf{LE}$ ((34)) ішкі жиынының элементтері арқылы көрінетін сарапшылардың лингвистикалық пікірлерінің түсініктемесі болып табылатынын ескерген жөн.

$\mathbf{T_{ij}}$ қалыптасу үрдісін нақты мысал арқылы көрсетейік, егер $n=3$ (яғни $I_1=I_{SN}=SN$, $I_2=I_{DS}=DS$ және $I_3=I_{SP}=SP$ С бар шабуылдар үшін), $m_1=m_3=2$, $m_2=3$, $r_1=5$, $r_2=r_3=3$ (49) өрнегін

$$\{\bigcup_{i=1}^{3} T_i\} = \{\bigcup_{i=1}^{3}\{\bigcup_{j=1}^{m_i} T_{ij}\}\} = \{\bigcup_{i=1}^{3}\{\bigcup_{j=1}^{m_i}\{\bigcup_{s=1}^{r_j} T_{ijs}\}\}\} =$$

$$\{\{\{\underset{\sim}{T}_{111}, \underset{\sim}{T}_{112}, \underset{\sim}{T}_{113}, \underset{\sim}{T}_{114}, \underset{\sim}{T}_{115}\}, \{\underset{\sim}{T}_{121}, \underset{\sim}{T}_{122}, \underset{\sim}{T}_{123}\}\},$$

$$\{\{\underset{\sim}{T}_{211}, \underset{\sim}{T}_{212}, \underset{\sim}{T}_{213}, \underset{\sim}{T}_{214}, \underset{\sim}{T}_{215}\}, \{\underset{\sim}{T}_{221}, \underset{\sim}{T}_{222}, \underset{\sim}{T}_{223}\}, \{\underset{\sim}{T}_{231}, \underset{\sim}{T}_{232}, \underset{\sim}{T}_{233}\}\},$$

$$\{\{\underset{\sim}{T}_{311}, \underset{\sim}{T}_{312}, \underset{\sim}{T}_{313}, \underset{\sim}{T}_{314}, \underset{\sim}{T}_{315}\}, \{\underset{\sim}{T}_{321}, \underset{\sim}{T}_{322}, \underset{\sim}{T}_{323}\}\}\} =$$

$$\{\{\{\underset{\sim}{VS}_{11}, \underset{\sim}{S}_{11}, \underset{\sim}{A}_{11}, \underset{\sim}{B}_{11}, \underset{\sim}{VB}_{11}\}, \{\underset{\sim}{Y}_{12}, \underset{\sim}{M}_{12}, \underset{\sim}{O}_{12}\}\},$$

$$\{\{\underset{\sim}{VS}_{21}, \underset{\sim}{S}_{21}, \underset{\sim}{A}_{21}, \underset{\sim}{B}_{21}, \underset{\sim}{VB}_{21}\}, \{\underset{\sim}{L}_{22}, \underset{\sim}{A}_{22}, \underset{\sim}{H}_{22}\}, \{\underset{\sim}{S}_{23}, \underset{\sim}{A}_{23}, \underset{\sim}{B}_{23}\}\},$$

$$\{\{\underset{\sim}{VS}_{31}, \underset{\sim}{S}_{31}, \underset{\sim}{A}_{31}, \underset{\sim}{B}_{31}, \underset{\sim}{VB}_{31}\}, \{\underset{\sim}{S}_{32}, \underset{\sim}{A}_{32}, \underset{\sim}{B}_{32}\}\}\} =$$

$$\{\{\{\underset{\sim}{T}_{SNNVC1}, \underset{\sim}{T}_{SNNVC2}, \underset{\sim}{T}_{SNNVC3}, \underset{\sim}{T}_{SNNVC4}, \underset{\sim}{T}_{SNNVC5}\}, \{\underset{\sim}{T}_{SNVCA1}, \underset{\sim}{T}_{SNVCA2}, \underset{\sim}{T}_{SNVCA3}\}\}, \quad (2.54)$$

$$\{\{\underset{\sim}{T}_{DSNCC1}, \underset{\sim}{T}_{DSNCC2}, \underset{\sim}{T}_{DSNCC3}, \underset{\sim}{T}_{DSNCC4}, \underset{\sim}{T}_{DSNCC5}\}, \{\underset{\sim}{T}_{DSSPR1}, \underset{\sim}{T}_{DSSPR2}, \underset{\sim}{T}_{DSSPR3}\},$$

$$\{\underset{\sim}{T}_{DSDBR1}, \underset{\sim}{T}_{DSDBR2}, \underset{\sim}{T}_{DSDBR3}\}\},$$

$$\{\{\underset{\sim}{T}_{SPNCC1}, \underset{\sim}{T}_{SPNCC2}, \underset{\sim}{T}_{SPNCC3}, \underset{\sim}{T}_{SPNCC4}, \underset{\sim}{T}_{SPNCC5}\}, \{\underset{\sim}{T}_{SPNPSA1}, \underset{\sim}{T}_{SPNPSA2}, \underset{\sim}{T}_{SPNPSA3}\}\}\} =$$

$$\{\{\{\underset{\sim}{VS}_{SNNVC}, \underset{\sim}{S}_{SNNVC}, \underset{\sim}{A}_{SNNVC}, \underset{\sim}{B}_{SNNVC}, \underset{\sim}{VB}_{SNNVC}\}, \{\underset{\sim}{Y}_{SNVCA}, \underset{\sim}{M}_{SNVCA}, \underset{\sim}{O}_{SNVCA}\}\},$$

$$\{\{\underset{\sim}{VS}_{DSNCC}, \underset{\sim}{S}_{DSNCC}, \underset{\sim}{A}_{DSNCC}, \underset{\sim}{B}_{DSNCC}, \underset{\sim}{VB}_{DSNCC}\},$$

$$\{\underset{\sim}{L}_{DSSPR}, \underset{\sim}{A}_{DSSPR}, \underset{\sim}{H}_{DSSPR}\}, \{\underset{\sim}{S}_{DSDBR}, \underset{\sim}{A}_{DSDBR}, \underset{\sim}{B}_{DSDBR}\}\},$$

$$\{\{\underset{\sim}{VS}_{SPNCC}, \underset{\sim}{S}_{SPNCC}, \underset{\sim}{A}_{SPNCC}, \underset{\sim}{B}_{SPNCC}, \underset{\sim}{VB}_{SPNCC}\}, \{\underset{\sim}{S}_{SPNPSA}, \underset{\sim}{A}_{SPNPSA}, \underset{\sim}{B}_{SPNPSA}\}\}\}$$

ретінде анықтауға болады.

(54) сәйкес егер $\{\underset{\sim}{T}_{321}, \underset{\sim}{T}_{322}, \underset{\sim}{T}_{323}\}$ үшін $i=3$, $j=2$, $r_j=3$ болса $\mathbf{T_{32}} \subseteq \mathbf{T}$, қалыптастырамыз, яғни:

$$\mathbf{T_{32}} = \{\bigcup_{s=1}^{3} \underset{\sim}{T}_{32s}\} = \{\underset{\sim}{T}_{321}, \underset{\sim}{T}_{322}, \underset{\sim}{T}_{323}\} = \{\underset{\sim}{T}_{SPNPSA1}, \underset{\sim}{T}_{SPNPSA2}, \underset{\sim}{T}_{SPNPSA3}\} =$$

$$\{\underset{\sim}{S}_{32}, \underset{\sim}{A}_{32}, \underset{\sim}{B}_{32}\}, (s=\overline{1,3}),$$

Осындағы $\underset{\sim}{T}_{321}=\underset{\sim}{T}_{SPNPSA1}=\underset{\sim}{S}_{32}$, $\underset{\sim}{T}_{322}=\underset{\sim}{T}_{SPNPSA2}=\underset{\sim}{A}_{32}$ және $\underset{\sim}{T}_{323}=\underset{\sim}{T}_{SPNPSA3}=\underset{\sim}{B}_{32}$ сәйкесінше $LE_{SPNPSA1}="S"$, $LE_{SPNPSA2}="A"$ мен $LE_{SPNPSA3}="B"$ арқылы көрінетін $\underset{\sim}{S}_{32}$, $\underset{\sim}{A}_{32}$ мен $\underset{\sim}{B}_{32}$ АЕС болып табылатын сарапшының пікірлерін білдіреді.

Ары қарай (50) өрнегінің негізінде $F'_{32} = F'_{SPNPSA}$ сәйкес жолдар бойынша максимумдар векторын құрамыз, яғни

$$FM_{SPNPSA} = \left\| fm_{SPNPSAs} \right\| = \left\| fm_{SPNPSA1}, fm_{SPNPSA2}, fm_{SPNPSA3} \right\| = \left\| 5,3;\ 4;\ 4,2 \right\|.$$

FM_{SPNPSA} негізінде (51) өрнегі бойынша M_{SPNPSA} қатыстылық функциясы матрицасын аламыз осылайша

$$M_{SPNPSA} = \left\| \mu_{SPNPSA\,sq} \right\| = \begin{Vmatrix} 1 & 0,2 & 0 \\ 0,5 & 1 & 0,7 \\ 0 & 0,5 & 1 \end{Vmatrix},$$

аламыз, осындағы $\mu_{SPNPSAsq} = f'_{SPNPSAsq} / fm_{SPNPSAs}\ (s,q = \overline{1,3})$. (51) $\mu_{SPNPSAsq}$ және (53) $x_{SPNPSAsq}$ есептелген өрнектері негізінде $T_{\sim SPNPSA}$ (52) формуласы бойынша $T_{\sim SPNPSA}$ анық емес термдерінің жиынтығын анықтаймыз,яғни

$T_{\sim 32s} = \{ \mu_{32s1} / x_{32s1},\ \mu_{32s2} / x_{32s2},\ \mu_{32s3} / x_{32s3} \} <=> T_{\sim SPNPSAs} = \{ \mu_{SPNPSAs1} / x_{SPNPSAs1},$
$\mu_{SPNPSAs2} / x_{SPNPSAs2},\ \mu_{SPNPSAs3} / x_{SPNPSAs3} \}, (s = \overline{1,3})$,

осындағы (53) өрнегіне сәйкес $x_{SPNPSAsq} = N^{max}_{SPNPSAq} / N^{max}_{SPNPSA\,r_j}$, $(q = \overline{1,3})$ немесе

$\{ \bigcup_{q=1}^{3} x_{SPNPSAsq} \} = \{0,01;\ 0,1;\ 1\}$.

Осылайша $\mathbf{T_{32}}$ (сандық форма) ішкі жиынының мүшелері сәйкесінше $\mathbf{LE_{32}}$ (34) (лингвистиқалық форма) ішкі жиынының мүшелері болып табылады және келесі түрде ұсынылады:

$T_{\sim 321} = T_{\sim SPNPSA1} = S_{\sim 32} = \{ 1/0,01;\ 0,2/0,1;\ 0/1 \}$,

$T_{\sim 322} = T_{\sim SPNPSA2} = A_{\sim 32} = \{ 0,5/0,01;\ 1/0,1;\ 0,7/1 \}$,

$T_{\sim 323} = T_{\sim SPNPSA3} = B_{\sim 32} = \{ 0/0,01;\ 0,5/0,1;\ 0/1 \}$.

5 кезең –эталонды АЕС қалыптастыру. Бұл кезеңді жүзеге асыру үшін әрқайсысы V_{ij} шамасының ауытқушылық күйіне қатысты сарапшы пайымдарын(1-кезеңді) бейнелейтін $\mathbf{T^e_{ij}}$ (2.1-2.2баптарын) анық емес(лингвистикалық) эталондардың ішкі жиынын қолданайық.

Анық емес эталондарды қалыптастыру $\mathbf{T_{ij} \subseteq T}$ ішкі жиынынан сәйкес АЕС(52) түрлендірулерге негізделеді және үш қадам арқылы жүзеге асырылады.

1 қадам. Барлық $T_{\sim ijs}$ үшін $\forall x_{ijsq} : x_{ijsq} < x_{ijsq+1}\ (q = \overline{1, r_j - 1})$ реті әділ болатындай (52) анық емес термдерді түрлендіру.

2 қадам. Әрбір $\underset{\sim}{T}_{ijs}$ $0/x_{ijs}^{min}$ және $0/x_{ijs}^{max}$ құрамдас бөліктерінің $x_{ijs}^{min} = \underset{q=1}{\overset{M-1}{\wedge}} x_{ijsq}$ при $U1$ $x_{ijs}^{max} = \underset{q=M}{\overset{K_j}{\wedge}} x_{ijsq}$ при $U2$ мен өрнектерінің құрамдас бөліктерінің қатарына сәйкес жұтылуы сәйкесінше жұтылуы жүзеге асырылады, осындағы $U_1 \overset{def}{=} \forall x_{ijsq} < x_{ijsM} : \mu_{ijsq} = 0$, $U_2 \overset{def}{=} \forall x_{ijsq} > x_{ijsM} : \mu_{ijsq} = 0$, ал x_{ijsM} мен M - сәйкесінше $\underset{\sim}{T}_{ijs}$ моды мен оның реттік нөмірі .

Ары қарай, осы өзгерістерді және (52) есепке ала отырып

$$\underset{\sim}{T}'_{ijs} = \{ \mu_{ijs\beta} / x_{ijs\beta}, ..., \bigcup_{q=\beta+1}^{r_j-\gamma} \mu_{ijsq} / x_{ijsq}, ..., \mu_{ijsr_j-\gamma+1} / x_{ijsr_j-\gamma+1} \} = \tag{2.55}$$

$$\{ \mu_{ijs\beta} / x_{ijs\beta}, \mu_{ijs\beta+1} / x_{ijs\beta+1}, ..., \mu_{ijsr_j-\gamma} / x_{ijsr_j-\gamma}, \mu_{ijsr_j-\gamma+1} / x_{ijsr_j-\gamma+1} \},$$

түріндегі аралық термдер жиынтығын анықтаймыз, осындағы $\mu_{ijs\beta} / x_{ijs\beta} = 0 / x_{ijs\beta} = 0/x_{ijs}^{min}$ мен $\mu_{ijsr_j-\gamma+1} / x_{ijsr_j-\gamma+1} = 0 / x_{ijsr_j-\gamma+1} = 0/x_{ijs}^{max}$, ал β мен γ – $x_{ijs(M)}$ сәйкесінше сол және оң жақтарындағы жұтылған $0 / x_{ijsq}$ саны

Осылайша эталондар ішкі жиыны қалыптасады

$$\underset{\sim}{T}^e_{ijs} = \{ \bigcup_{q=1}^{r_{js}} \mu^e_{ijsq} / x^e_{ijsq} \} = \{ \mu^e_{ijs1} / x^e_{ijs1}, \mu^e_{ijs2} / x^e_{ijs2}, ..., \mu^e_{ijsr_{js}-1} / x^e_{ijsr_{js}-1}, \mu^e_{ijsr_{js}} / x^e_{ijsr_{js}} \}, \tag{2.56}$$

$$(q = \overline{1, r_{js}}),$$

осындағы $\mu^e_{ijs1} / x^e_{ijs1} = \mu_{ijs\beta} / x_{ijs\beta}$, $\mu^e_{ijs2} / x^e_{ijs2} = \mu_{ijs\beta+1} / x_{ijs\beta+1}$, ..., $\mu^e_{ijsr_{js}-1} / x^e_{ijsr_{js}-1} = \mu_{ijsr_j-\gamma} / x_{ijsr_j-\gamma}$, $\mu^e_{ijsr_{js}} / x^e_{ijsr_{js}} = \mu_{ijsr_j-\gamma+1} / x_{ijsr_j-\gamma+1}$, $r_{js}\ (s = \overline{1, r_j})$ _ $\underset{\sim}{T}^e_{ijs}$ құрамдас бөліктер саны.

3 қадам. Егер екінші қадамды жүзеге асыру үшін (55) өрнегі үшін $\exists \underset{\sim}{T}'_{ijs} : \{0/x_{ijs}^{min}\} \in \oslash$ немесе $\exists \underset{\sim}{T}'_{ijs} : \{0/x_{ijs}^{max}\} \in \oslash$ (яғни $\mu_{ijs\beta} \neq 0$, $\mu_{ijsr_j-\gamma+1} \neq 0$) болса, онда осындай термдер үшін ары қарай $\underset{\sim}{T}^e_{ijs}$ ішкі жиынын қалыптастыру қосымша $\mu_{ijs\beta-1} / x_{ijs\beta-1}$ және $\mu_{ijsr_j-\gamma+2} / x_{ijsr_j-\gamma+2}$ енгізу арқылы $\underset{\sim}{T}'_{ijs}$ кеңейту арқылы жүзеге асырылады, осыдан кейін АЕС құрамдас бөліктері $q = 1$ бастап қайтадан индекстеледі.

Осыны ескере отырып аралық термдер жиынтығы келесі түрге ие болады

$$\underset{\sim}{T}'_{ijs} = \{ \mu_{ijs\beta-1} / x_{ijs\beta-1}, \mu_{ijs\beta} / x_{ijs\beta}, ..., \bigcup_{q=\beta+1}^{r_j-\gamma} \mu_{ijsq} / x_{ijsq}, ..., \mu_{ijsr_j-\gamma+1} / x_{ijsr_j-\gamma+1},$$

$$\mu_{ijsr_j-\gamma+2} / x_{ijsr_j-\gamma+2} \} = \{ \mu_{ijs\beta-1} / x_{ijs\beta-1}, \mu_{ijs\beta} / x_{ijs\beta}, ..., \mu_{ijsr_j-\gamma+1} / x_{ijsr_j-\gamma+1},$$

$\mu_{ijsr_j-\gamma+2} / x_{ijsr_j-\gamma+2}\}$, осындағы $x_{ijs\beta-1} = x_{ijs\beta}$, $x_{ijsr_j-\gamma+2} = x_{ijsr_j-\gamma+1}$, ал $\mu_{ijs\beta-1} = \mu_{ijsr_j-\gamma+2} = 0$.

Осылайша (56) өрнегіндегі $\tilde{T}^e_{ijs}$ эталондарының ішкі жиынының құрамдас бөліктері $\mu^e_{ijs1} / x^e_{ijs1} = \mu_{ijs\beta-1} / x_{ijs\beta-1}$, $\mu^e_{ijs2} / x^e_{ijs2} = \mu_{ijs\beta} / x_{ijs\beta}$,…, $\mu^e_{ijsr_{js}-1} / x^e_{ijsr_{js}-1} = \mu_{ijsr_j-\gamma+1} / x_{ijsr_j-\gamma+1}$, $\mu^e_{ijsr_{js}} / x^e_{ijsr_{js}} = \mu_{ijsr_j-\gamma+2} / x_{ijsr_j-\gamma+2}$ ретінде анықталады.

Эталонды АЕС қалыптастыру үрдісін нақты мысал арқылы қарастырайық, яғни (13) өрнегіне сәйкес егер $\{\tilde{T}_{321}, \tilde{T}_{322}, \tilde{T}_{323}\}$ үшін $i=3$, $j=2$, $r_j=3$ болса, онда $\mathbf{T^e_{32}} \subseteq \mathbf{T^e}$ қалыптастырамыз, яғни

$$\mathbf{T^e_{32}} = \{\bigcup_{s=1}^{3} \tilde{T}^e_{32s}\} = \{\tilde{T}^e_{321}, \tilde{T}^e_{322}, \tilde{T}^e_{323}\} = \{\tilde{T}^e_{SPNPSA1}, \tilde{T}^e_{SPNPSA2}, \tilde{T}^e_{SPNPSA3}\} = \{\tilde{S}^e_{32}, \tilde{A}^e_{32}, \tilde{B}^e_{32}\}, (s=\overline{1,3}),$$

осындағы $\mathbf{T^e_{32}}$ – $\tilde{S}^e_{32}$, $\tilde{A}^e_{32}$, $\tilde{B}^e_{32}$ ішкі жиынының мүшелері эталонды АЕС болып табылады.

1 қадам. $\tilde{S}_{32}$, $\tilde{A}_{32}$ және $\tilde{B}_{32}$ анық емес термдерін барлық $\tilde{T}_{32s}$ үшін $\forall x_{32sq}: x_{32sq} < x_{32sq+1} (q=\overline{1,2})$ реті әділ болатындай түрлендіреміз. Егер осындай термдердің құрамдас бөліктері үшін 4 кезеңнің мысалы негізінде алынған нақты мәндерді қолданса, онда олар үшін осы арақатынас шынайы болады. Осылайша, мысалы $\tilde{S}_{32}$ үшін бұл $x_{3211} < x_{3212} < x_{3213} = 0,01 < 0,1 < 1$.

2 қадам. $\tilde{S}_{32}$, $\tilde{A}_{32}$, $\tilde{B}_{32}$ үшін U_1 мен U_2 шарты орындалмайды және сондықтан жұтылу операциясы жүзеге асырылмайды. Осыны және (55) өрнегін есепке ала отырып

$\tilde{T}'_{321} = \tilde{T}'_{SPNPSA1} = \tilde{S}'_{32} = \{\mu_{3211} / x_{3211}, \mu_{3212} / x_{3212}, \mu_{3213} / x_{3213}\} = \{1/0,01; 0,2/0,1; 0/1\}$,

$\tilde{T}'_{322} = \tilde{T}'_{SPNPSA2} = \tilde{A}'_{32} = \{\mu_{3221} / x_{3221}, \mu_{3222} / x_{3222}, \mu_{3223} / x_{3223}\} = \{0,5/0,01; 1/0,1; 0,7/1\}$,

$\tilde{T}'_{323} = \tilde{T}'_{SPNPSA3} = \tilde{B}'_{32} = \{\mu_{3231} / x_{3231}, \mu_{3232} / x_{3232}, \mu_{3233} / x_{3233}\} = \{0/0,01; 0,5/0,1; 1/1\}$.

түріндегі аралық термдер жиынын анықтаймыз.

3 қадам. (55) өрнегіндегі екінші қадамды жүзеге асыру кезінде $\tilde{S}'_{32}$ және $\tilde{A}'_{32} \exists \tilde{T}'_{321} : \{0/x^{min}_{321}\} \in \oslash$ и $\exists \tilde{T}'_{322} : \{0/x^{min}_{322}\} \in \oslash$ (яғни $\mu_{3211} = 1 \neq 0$ мен $\mu_{3221} = 0,5 \neq 0$) аралық термдерінің жиынтығы үшін сонымен бірге $\tilde{A}'_{32}$ мен $\tilde{B}'_{32} \exists \tilde{T}'_{322} : \{0/x^{max}_{322}\} \in \oslash$ және $\exists \tilde{T}'_{323} : \{0/x^{max}_{323}\} \in \oslash$ мен (яғни $\mu_{3223} = 0,7 \neq 0$ мен $\mu_{3233} = 1 \neq 0$) болса, онда $\tilde{T}^e_{321}$, $\tilde{T}^e_{322}$ және $\tilde{T}^e_{323}$ ішкі жиындарын қалыптастыру $\tilde{T}'_{321}$, $\tilde{T}'_{322}$ мен $\tilde{T}'_{323}$ кеңейтілуін ((55)қараңыз) қосымша $\mu_{321\beta-1} / x_{321\beta-1} = 0 / 0,01$,

$\mu_{322\beta-1} / x_{322\beta-1} = 0/0{,}01$, $\mu_{322r_j-\gamma+2} / x_{322r_j-\gamma+2} = 0/1$ және сәйкесінше $\mu_{323r_j-\gamma+2} / x_{323r_j-\gamma+2} = 0/1$ енгізу арқылы жүзеге асырылады, осыдан кейін сәйкесінше АЕС алғашқысынан бастап құрамдас бөліктердің қайта индекстелуі жүзеге асырылады.

Осыны ескере отырып $\underset{\sim}{S}'_{32}$ үшін аралық термдер жиынтығы келесі түрге ие болады:

$\underset{\sim}{T}'_{321} = \underset{\sim}{T}'_{SPNPSA1} = \underset{\sim}{S}'_{32} = \{\mu_{3211} / x_{3211}, \mu_{3212} / x_{3212}, \mu_{3213} / x_{3213}, \mu_{3214} / x_{3214}\} =$
$\{0/0{,}01;\ 1/0{,}01;\ 0{,}2/0{,}1;\ 0/1\}$,

осындағы $\mu_{321\beta-1} = 0$. Осыған ұқсас тәсілмен $\underset{\sim}{A}'_{32}$ мен $\underset{\sim}{B}'_{32}$ үшін аралық термдер аламыз осындағы $\mu_{322\beta-1} = \mu_{322r_j-\gamma+2} = \mu_{323r_j-\gamma+2} = 0$.

Осылайша, $\underset{\sim}{T}^e_{321}$ эталондарының ішкі жиынының құрамдас бөліктері (56) өрнекке сәйкес $\mu^e_{3211} / x^e_{3211} = 0/0{,}01$, $\mu^e_{3212} / x^e_{3212} = 1/0{,}01$, $\mu^e_{3213} / x^e_{3213} = 0{,}2/0{,}1$, $\mu^e_{3214} / x^e_{3214} = 0/1$ ретінде және $\underset{\sim}{T}^e_{322}$ мен $\underset{\sim}{T}^e_{323}$ үшін осыған ұқсас амалмен анықталатын болады.

Ары қарай $\underset{\sim}{S}'_{32}$, $\underset{\sim}{A}'_{32}$ мен $\underset{\sim}{B}'_{32}$ үшін (56) өрнегіне сәйкес эталонды мәндерді қалыптастыра аламыз, яғни:

$\underset{\sim}{T}^e_{321} = \underset{\sim}{T}^e_{SPNPSA1} = \underset{\sim}{S}^e_{32} = \{\mu^e_{3211} / x^e_{3211}, \mu^e_{3212} / x^e_{3212}, \mu^e_{3213} / x^e_{3213}, \mu^e_{3214} / x^e_{3214}\} =$
$\{0/0{,}01;\ 1/0{,}01;\ 0{,}2/0{,}1;\ 0/1\}$,

$\underset{\sim}{T}^e_{322} = \underset{\sim}{T}^e_{SPNPSA2} = \underset{\sim}{A}^e_{32} = \{\mu^e_{3221} / x^e_{3221}, \mu^e_{3222} / x^e_{3222}, \mu^e_{3223} / x^e_{3223}, \mu^e_{3224} / x^e_{3224}, \mu^e_{3225} / x^e_{3225}\} =$
$\{0/0{,}01;\ 0{,}5/0{,}01;\ 1/0{,}1;\ 0{,}7/1;\ 0/1\}$,

$\underset{\sim}{T}^e_{323} = \underset{\sim}{T}^e_{SPNPSA3} = \underset{\sim}{B}'_{32} = \{\mu^e_{3231} / x^e_{3231}, \mu^e_{3232} / x^e_{3232}, \mu^e_{3233} / x^e_{3233}, \mu^e_{3234} / x^e_{3234}\} =$
$\{0/0{,}01;\ 0{,}5/0{,}1;\ 1/1;\ 0/1\}$,

осындағы мысалы: $\mu^e_{3231} / x^e_{3231} = \mu_{3231} / x_{3231}$, $\mu^e_{3232} / x^e_{3232} = \mu_{3232} / x_{3232}$, $\mu^e_{3233} / x^e_{3233} = \mu_{3233} / x_{3233}$ и $\mu^e_{3234} / x^e_{3234} = \mu_{3234} / x_{3234}$.

Осы мысалдан $r_1 = r_3 = 4$, $r_2 = 5$ екені көрінеді.

6 кезең – Лингвистикалық эталондарды визуализациялау. Бұл кезеңді жүзеге асыру $\mathbf{T^e_{ij}}$ (2.1-2.2 баптарын қараңыз) ішкі жиындарына қатысты (56) барлық эталонды АЕС геометриялық бейнесін құруға негізделеді. Жазықтықтағы нүктелердің геометриялық орны $\underset{\sim}{T}^e_{ijs}$ АЕС құрамдас бөліктерін x^e_{ijsq} қолдаушылар (тасымалдаушылар) өсу ретімен бейнелейтін бүгілме қосушы сызық арқылы анықталады. Бір модельлік эталонды термді көзбен көру (56) бүгілме сызық түрінде ⊸ 2.7. суретінде көрсетілген.

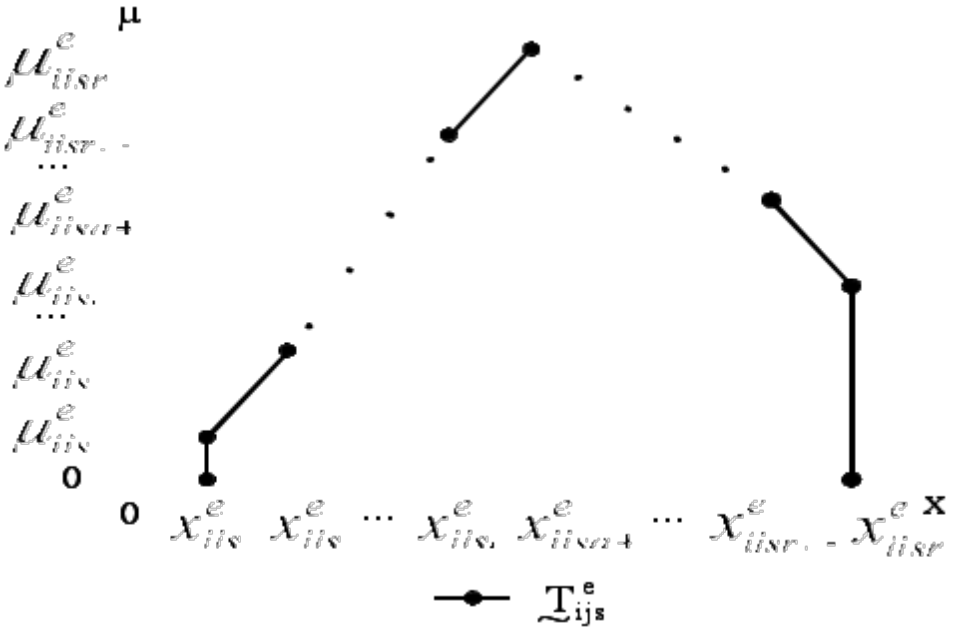
Мысалы, $\mathbf{T}^{e}_{32} = \mathbf{T}^{e}_{SPNPSA}$ эталондарының ішкі жиынын визуализациялау үшін 5кезеңде қалыптасқан эталонды АЕС қолданамыз(мысалды):

$$\underset{\sim}{S}^{e}_{32} = \{0/0{,}01;\ 1/0{,}01;\ 0{,}2/0{,}1;\ 0/1\},$$

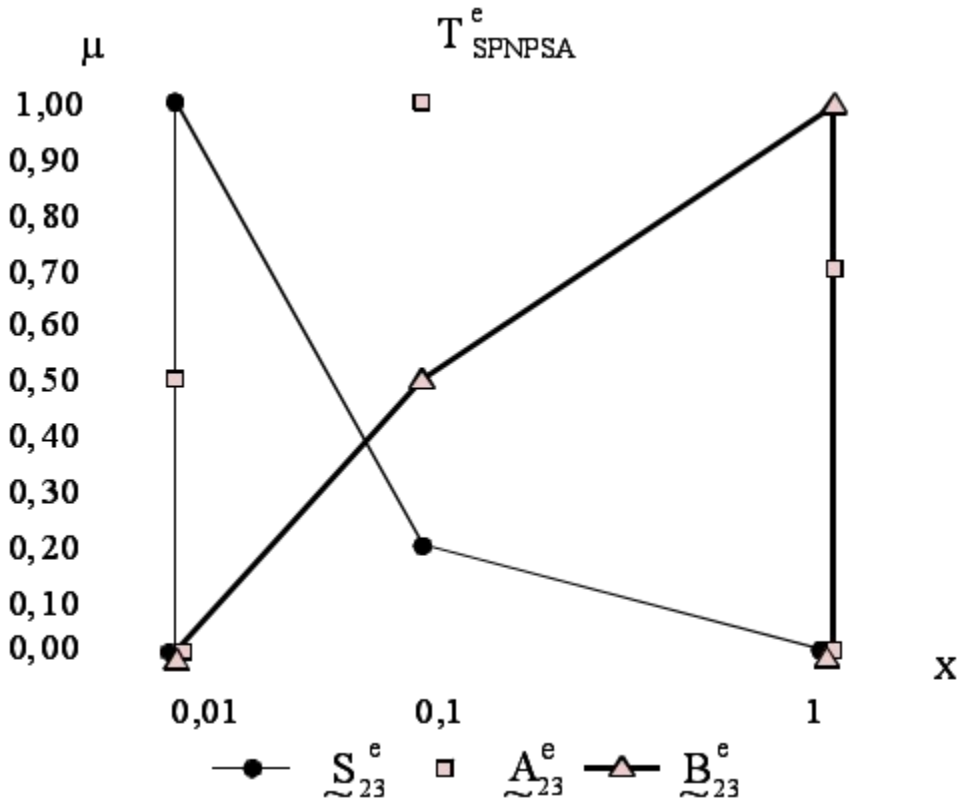
$$\underset{\sim}{A}^{e}_{32} = \{0/0{,}01;\ 0{,}5/0{,}01;\ 1/0{,}1;\ 0{,}7/1;\ 0/1\},$$

$$\underset{\sim}{B}^{e}_{32} = \{0/0{,}01;\ 0{,}5/0{,}1;\ 1/1;\ 0/1\}.$$

Осылардың негізінде $\underset{\sim}{S}^{e}_{32}$, $\underset{\sim}{A}^{e}_{32}$, $\underset{\sim}{B}^{e}_{32}$ эталонды АЕС сәйкес құрамдас бөліктері арқылы бейнеленетін нүктелерді қосу арқылы графикалық түрде 2.8 суретінде түсіндірілетін бес бүгілме сызық • , —■— , ▫ , ▫ , —▫—, құрылады.



Сурет 2.7 - $\underset{\sim}{T}^{e}_{ijs}$ Лингвистикалық эталонның АЕС



Сурет 2.8 - $\mathbf{T^{e}_{SPNPSA}}$ ішкі жиынының Лингвистикалық эталондары

Лингвистикалық бағалар мен аралықтар идентификациялаудың жиынын қолдану, шамалардың ағымдағы жағдайын шабуылдарға қатысты сарапшы пайымдарын сипаттайтын базалық және туынды жиілік матрицаларын сонымен қатар сарапшы бағаларының берілген аралықта кездесу жиілігі мен анық емес термдердің ішкі жиынын қалыптастыру үрдісін қолдану есебінен шабуылдарды анықтау жүйесі үшін жұмыста ұсынылған ЛЭҚМ нақты гетерогенді параметрлі қоршаған ортада түрлі ауытқушылықтар жағдайын сипаттайтын берілген лингвистикалық айнымалылар тобының шамасының эталонды мәндерін алу процедурасын қалыптастыруға мүмкіндік береді. Ұсынылған ЛЭҚМ базалық шамалар моделінің және эталонды шамалар моделінің бөлігі, сонымен қатар анық емес қАСынға негізделген шабуылдарды анықтау жүйесін құруға теориялық іргетас болып табылады.

Екінші тарау бойынша тұжырым

1.Қоршаған ортадағы шабуылдаушы әрекеттерді сипаттайтын айқындалмаған шамаларды қалыптастыру үшін шабуылдардың ресми жиыны және оған сәйкес “басып кіру : шамалар” және “басып кіру **:** түйіндес жұптар жиыны” қалыптасқан жұптар жиынының негізінде ықтимал шабуылдар жиыны ұсынылды, осылайша компьтерлік жүйелер мен желілердегі шамалардың ауытқушылық жағдайын анықтауға негізделген сәйкес шабуылдарды анықтау нәтижелілігін жоғарылатуға

мүмкіндік беретін шабуылдарды анықтау құралдарын жобалауда қолданылатын базалық шамалар моделі алынды.

2.Сарапшылық баға мәліметтерін қолдана отырып базалық шамалар модельдерінің негізінде сәйкес эталонды шамалар модельдері ұсынылды, сарапшы мәліметтерді ескере отырып шешуші ережелерді қалыптастыруға қажет нақты емес әлсіз қалыптастырылған ортадағы ауытқушылық жағдайын айқындауға негізделген сәйкес қауіпсіздік құралдарының нәтижелілігін жоғарылатуға мүмкіндік беретін нақты эталонды анық емес сандар анықталды.

3.“Шабуыл: шамалар” және “шабуыл **:** түйіндес жұптар жиыны ” жұптар жиынын ескере отырып , базалық шамалар модельдері мен эталонды шамалар модельдері негізінде кибершабуылдардың нақты түрі туындатқан ауытқушылық жағдайын көрсетуге мүмкіндік беретін шешуші ережелер моделі ұсынылды. Осы модель негізінде компьютерлік жүйелер мен желілердегі шабуылдаушы әрекеттер тудырған ауытқушылықтарды анықтау жүйесін жетілдіру үшін тәжірибе жүзінде қолданылуы мүмкін сканерлеу, спуфинг (алмастыру) және Dos-шабуылдарды анықтау үшін ережелер модельдері құрастырылды.

4. Тұңғыш рет шабуылдарды анықтау жүйесі үшін лингвистикалық эталондарды қалыптастыру әдісі құрастырылды, ол нақты гетереогенді параметрлі ортада түрлі ауытқушылық жағдайын сипаттайтын берілген лингвистикалық айнымалылар топтарының шамалардың эталонды мәндерін алу процедурасын қалыптастыруға мүмкіндік береді

5. Лингвистикалық бағалар мен аралықтар идентификациялаудың жиынын қолдану, шамалардың ағымдағы жағдайын шабуылдарға қатысты сарапшы пайымдарын сипаттайтын базалық және туынды жиілік матрицаларын сонымен қатар сарапшы бағаларының берілген аралықта кездесу жиілігі мен анық емес термдердің ішкі жиынын қалыптастыру үрдісін қолдану есебінен шабуылдарды анықтау жүйесі үшін жұмыста ұсынылған лингвистикалық эталондарды қалыптастыру әдісі нақты гетерогенді параметрлі қоршаған ортада түрлі ауытқушылықтар жағдайын сипаттайтын берілген лингвистикалық айнымалылар тобының шамасының эталонды мәндерін алу процедурасын қалыптастыруға мүмкіндік береді.

3 КОМПЬЮТЕРЛІК ЖЕЛІЛЕРДЕГІ КИБЕРШАБУЫЛДАРДАН ТУЫНДАЙТЫН АУЫТҚУЛАРДЫ АНЫҚТАУ ҚҰРАЛДАРЫ

3.1 Шабуылдарды табу жүйелері үшін ауытқушылық жағдайын анықтауға арналған технология

Кибершабуылдар тудырған ауытқушылықтарды анықтау міндетін шешу үшін2.1-2.3 [4, 6, 7, 8] баптарында ұсынылған БШМ. ЭШМ және ШЕМ алынған сәйкес құралдарды құрастырамыз. Аталған моделдерді қолдана отырып сегіз негізгі кезең арқылы жүзеге асырылатын сәйкес технологияны [9]құрамыз:

1) Анық емес деректерді өңдеу әдісін таңдау,
2) Маңыздылық коэффициенттін(МК) анықтау әдісін таңдау,
3) Шабуыл мен шамалар жиынын қалыптастыру,
4) Шамалардың эталондарын қалыптастыру,
5) Шамаларды фаззификациялау,
6) Шешуші ережелер (ШЕ) жиынын қалыптастыру,
7) Инициализация матрицаларын анықтау,
8) Нәтижелерді қалыптастыру.

Осы кезеңдердің жүзеге асырылуы 3.1. суретінде көрсетілген. Олардың әрқайсысын сипаттайық.

1 кезең – анық емес деректерді өңдеу әдісін таңдау.

Бұл кезеңде берілген критерийлерге қатысты анық емес деректерді өңдеу әдістерін таңдау жүзеге асырылады. 1.2 [24] бабында сәйкес әдістердің үш негізгі тобы қарастырылған – қатыстылық фунциясын қалыптастыру (ҚФҚӘ) (он төрт әдіс – $ҚФҚӘ_1$, $ҚФҚӘ_2$, $ҚФҚӘ_3$, …, $ҚФҚӘ_{14}$, мысалы , ПТ, ЛТСМҚжәне т.б.), қатыстылық функциясын салыстыру әдістері (ҚФСӘ) (сегіз әдіс– $ҚФСӘ_1$, $ҚФСӘ_2$, $ҚФСӘ_3$, …, $ҚФСӘ_8$, мысалы, АДА,РФ және т.б.) және анық емес арифметика әдістері (АЕАӘ) (он төрт әдіс – $АЕАӘ_1$, $АЕАӘ_2$, $АЕАӘ_3$, …, $АЕАӘ_{14}$, мысалы, МКӘ,АЖӨҰ,ЖМСЖжәне т.б.), осылардың ішіненҚФҚӘ, ҚФСӘ және АЕАӘ таңдау арықылы өкілдердің бірі сұрыпталады. Таңдау процессі берілген критерийлер негізінде жүзеге асырылады. Барлық әдістер тобы үшін негізгі критерийлер ретінде қолданылатын ҚФ және СА класы, ал ҚФҚӘ үшін дәрежелік бағалауды қолдану және тартылатын сарапшылар саны, ал ҚФСӘ үшін $-\alpha$-деңгейлік ұстанымды қолдану болып табылады. Егер бірнеше әдіс бекітілген критерийлерге сәйкес болса, онда таңдау туралы қорытынды шешім сарапшының қалауына негізделетін болады.

Мысалы, қабылданған критерийлерге сәйкес әрбір ықтимал $ҚФҚӘ_i$ ($i=\overline{1,14}$), $ҚФСӘ_j$($j=\overline{1,8}$)және $АЕАӘ_k$ ($k=\overline{1,14}$) топтары үшін таңдау рәсімін жүзеге асырғаннан кейін компьютерлік желілердегі ауытқушылық жағдайын анықтау міндетін шешуде анық емес деректерді өңдеуге бірге қолданылатын сәйкес ЖМСЖ, АДА және ЛТСМҚ әдістері анықталады.

2кезең – маңыздылық коэффициентін анықтау әдісін таңдау (МКАӘТ).

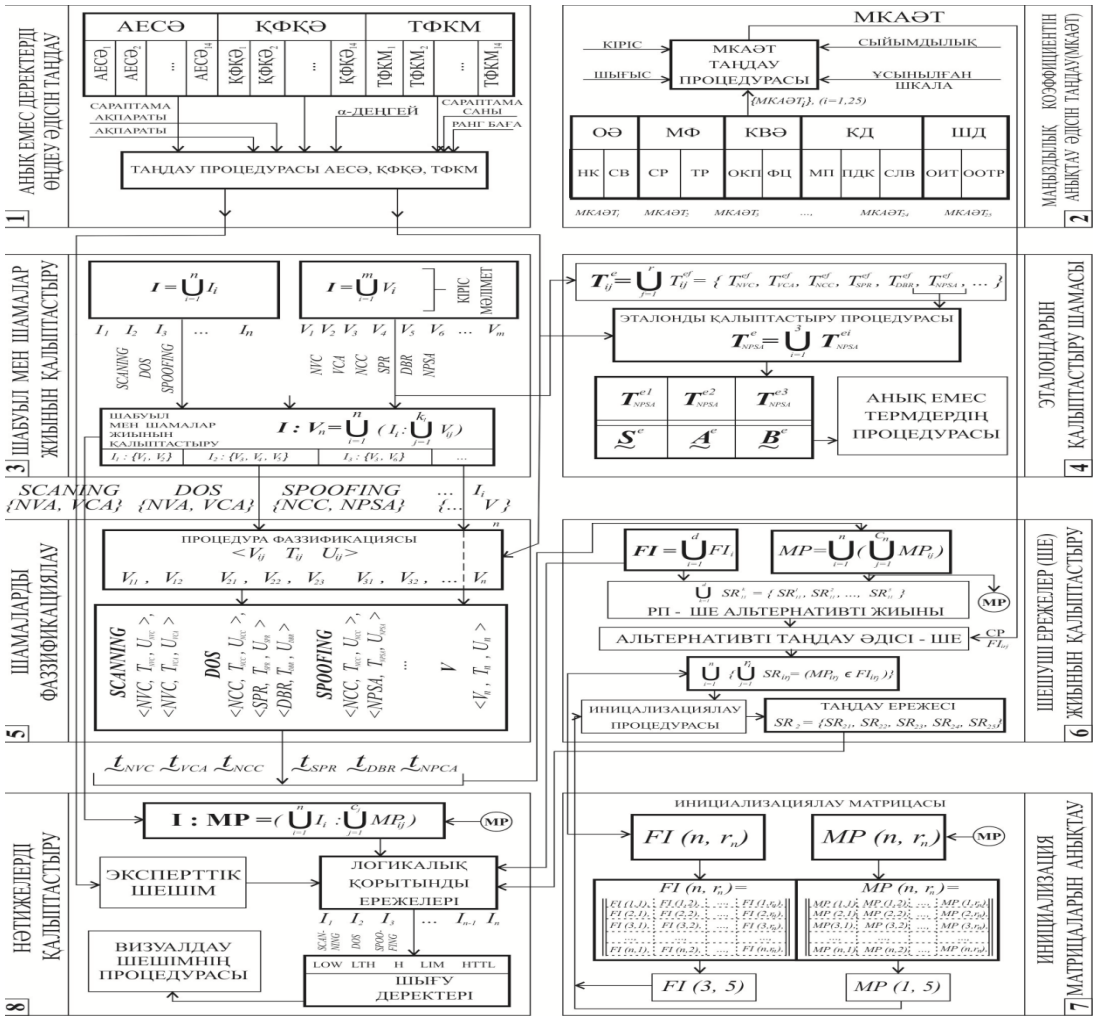
Кезең (қабылданған критерийлерге сәйкес) берілген жиыннан МК қалыптастыру әдісін (МКАӘТ) таңдауға бағытталған. 1.3 [2] бабында

арасынан таңдау рәсімін жүзеге асыру үрдісінде жұмысшы әдіс анықталатын жиырма бес МКАӘТ ($МКАӘТ_1$, $МКАӘТ_2$, $МКАӘТ_3$, …, $МКАӘТ_{25}$, мысалы, ОӘ, МФ, КВӘ және т.б әдістер) қарастырылған.Егер бірнеше әдіс қабылданған критерийлерге жауап берсе, онда таңдау туралы қорытынды шешімді сарапшы қабылдайтын болады.

Әдістің басымдығы МКАӘТ таңдау процессіКД және ШД ұсыну формасы, еңбек сыйымдылығы және ұсынылатын шкала (1.3. бабын қараңыз) [2] сияқты критерийлер арқылы анықталады.

Мысалы, $МКАӘТ_i$ ($i = \overline{1,25}$)жиынынан қабылданған критерийлер мен басымдықтарға сәйкес ОӘ әдісі таңдалады.

Кесте 4.3 - ЖР анықтаудың бағдарламалық жүйелерін сараптамалық зерттеу нәтижелері



Сурет 3.1-Ауытқушылықтарды идентификациялау технологиясының бейнелеу сызбанұсқасы

3 кезең –шамалар мен шабуылдар жиынын қалыптастыру.

Кезең шабуылдар жиыны мен оған сәйкес ауытқушылықтарды анықтауға арналған шамалар жиынын қалыптастыруға арналған. БШМ (2.1.бабын қараңыз) [6] қолдана отырып қоршаған ортаның кіріс

$\bigcup_{i=1}^{n} I_i$ шамаларының негізінде $\boldsymbol{I}$ ықтимал шабуылдар жиыны және $\boldsymbol{I}$ жиынының нақты элементі тудырған ауытқушылық жағдайын сарапшылардың шешімдерін ескере отырып анықтауға болатын мәндері (мысалы, V_1=NVC, V_2=VCA, V_3=NCC, V_4=SPR, V_5=DBR,V_6=NPSA, ..., V_m)$\boldsymbol{V}=\bigcup_{i=1}^{m} V_i$ ықтимал шамалар жиыны қалыптасады, мысалы, (I_1=SCANNING, I_2=DOS, I_3=SPOOFING, ..., I_n)(2.1.бабын қараңыз) [6].

Жүйедегі күмәнді белсенділікті анықтауға болатын $\boldsymbol{V}$ жиынының $\boldsymbol{V_n}$ шамалардың ішкі жиыны $\boldsymbol{I}$ шабуылдың әрбір түріне идентификациялауды. Осылайша әрбір шабуылға (I_1:{V_1, V_2}), (I_2:{V_3, V_4, V_5}), (I_3:{V_3, V_6}), …, (I_n:{…, V_n}) сәйкес шамалар жиыны, мысалы, (SCANNING:{NVC, VCA}), (DOS:{NCC, SPR, DBR}) және(SPOOFING:{NCC, NPSA})«шабуыл **:** шамалар»

$\boldsymbol{I: V_n}=\bigcup_{i=1}^{n}(I_i : \bigcup_{j=1}^{k_i} V_{ij})$ жұптар жиыны қалыптасады.

4 кезең – шамалар эталондарын қалыптастыру.

Бұл кезең қоршаған ортаны сипаттайтын шамалардың ағымдағы мәндерін өлшеуге қажет эталондарды алуға бағытталған. ҚФҚӘ алғашқы кезеңінде таңдалған кіріс деректерінің негізінде (3кезеңді) $\boldsymbol{V}=\bigcup_{i=1}^{m} V_i$ және эталонды шамаларды қалыптастыру процедурасының көмегімен барлық $T_{ij}^{e}=\bigcup_{f=1}^{r} T_{ij}^{ef}$ үшін Лингвистикалық айнымалылар эталондарының мәндерін, мысалы, $\{T_{NVC}^{ef}, T_{VCA}^{ef}, T_{NCC}^{ef}, T_{SPR}^{ef}, T_{DBR}^{ef}, T_{NPSA}^{ef}, \ldots\}$ аламыз.

Осылайша, мысалы, ҚФҚӘ$_6$ = ЛТСМҚ (1.2.бабын қараңыз) [24] қолданылған NPSA [4] үшін $T_{NPSA}^{e}=\bigcup_{i=1}^{3} T_{NPSA}^{ei}$ эталонды мәндерін алуға болады және **NPSA** – $\{T_{NPSA}^{e1}, T_{NPSA}^{e2}, T_{NPSA}^{e3}\}=\{\tilde{S}^{e}, \tilde{A}^{e}, \tilde{B}^{e}\}$үшін лингвистикалық термдерді визулизациялауға болады. Ары қарай визуализациялау процедурасы арқылы $\{\tilde{S}^{e}, \tilde{A}^{e}, \tilde{B}^{e}\}$ лингвистикалық термдерінің эталондарының графикалық бейнесі қалыптасады.

5кезең –шамалардың фаззификациясы.

Бұл кезеңде жүйенің ағымдағы жағдайын сипаттайтын шамалардың ішкі жиынын сәйкес анық емес айнымалыларды ағымдағы мәндеріне түрлендіру жүзеге асырылады.

БШМ негізінде (2.1.бабын қараңыз) [6],таңдалған (бірінші кезеңде)ҚФ алу әдісі және ҚФҚӘ жүзеге асыратын фаззификация процедурасының

көмегімен әрқайсысы $<V_{ij}, T_{ij}, U_{ij}>$ шеруімен ұсынылатын ЛА жиыны қалыптасады.

Ары қарай ***I*** жиынының әрбір шабуылдар ***V*** жиынындағы нақты шамалар жиынымен байланыс құратын процедура негізінде (2.1.бабын қараңыз) [6] $\boldsymbol{I: V_n = \bigcup_{i=1}^{n} (I_i : \bigcup_{j=1}^{k_i} V_{ij})}$ жұптар жиынын аламыз.

Осылайша, «шабуыл**:** шамалар» жұптар жиыны,ҚФҚӘ$_6$=ЛТСМҚ(1кезеңді қараңыз) және *SCANNING*(егерV_{11}, V_{12} – $<NVC, T_{NVC}, U_{NVC}>$, $<VCA, T_{VCA}, U_{VCA}>$), *DOS* (егерV_{21}, V_{22}, V_{23} – $<NCC, T_{NCC}, U_{NCC}>$, $<SPR, T_{SPR}, U_{SPR}>$, $<DBR, T_{DBR}, U_{DBR}>$) және *SPOOFING*(егерV_{31}, V_{32} – $<NCC, T_{NCC}, U_{NCC}>$, $<NPSA, T_{NPSA}, U_{NPSA}>$) шабуылдар үшін сәйкес ЛА мәндерін білдіретін жиынын қолдана отырып сәйкесінше NVC, VCA, NCC, SPR, DBR және NPSA шамаларын білдіретін $\underset{\sim}{t}_{NVC}$, $\underset{\sim}{t}_{VCA}$, $\underset{\sim}{t}_{NCC}$, $\underset{\sim}{t}_{SPR}$, $\underset{\sim}{t}_{DBR}$ және $\underset{\sim}{t}_{NPSA}$ қоршаған ортаның анық емес айнымалыларының ағымдағы мәндері қалыптасады.

6 кезең – шешуші ережелер жиынын қалыптастыру

Кезең эталонды шамаларға қатысты жүйенің ағымдағы жағдайын өлшеуге қажет ШЕ қалыптастыруға бағытталған. Анық емес $\boldsymbol{FI = \bigcup_{i=1}^{d} FI_i}$ (2.3. бабын қараңыз) [7] идентификациялау жиынында және $\boldsymbol{MP = \bigcup_{i=1}^{n} (\bigcup_{j=1}^{c_n} MP_{ij})}$ (2.1. бабын қараңыз) [6] түйіндес жұптар (төртінші кезеңде анықталған Лингвистикалық термдердің нақты мәндерін қолданатын) негізінде SR_{ij}^{k} ($i = \overline{1,n}$; $k = \overline{1,d}$; $j = \overline{1,r_n}$ альтернативті жиыны қалыптасады, осындағы n – шабуылдарсаны, r_n –i шабуылды анықтауға арналған ережелер саны, ал d – бір ережені қалыптастыруға арналған альтернативті нұсқалардың саны).

Мысалы, бірінші шабуыл және бірінші ереже үшін ол $\bigcup_{k=1}^{d} SR_{11}^{k} = \{SR_{11}^{1}, SR_{11}^{2}, SR_{11}^{3}, SR_{11}^{4}, SR_{11}^{5}\}$ болады. $\bigcup_{i=1}^{n} \{\bigcup_{j=1}^{r_i} SR_{ir_j} = (MP_{ir_j} FI_{ir_j})\}$ (2.3. бабын қараңыз) [7]өрнегінде бейнеленген ШЕ құру үшін қолданылады. МҚ қалыптастыру (2 кезеңді) әдістерінің біріне негізделген таңдау процедурасының көмегімен альтернативті жиынының негізінде ереже қалыптастыру жүзеге асырылады.

Ары қарай, таңдалған FI_{ir_j} 7 кезеңде MP_{ir_j} және FI_{ir_j}, нақты мәндерін беретін ымыраласу процедурасы арқылы берілген эвристикалық ережелердің тікелей жиынтығын қалыптастыратын инициализация матрицасы үшін қажет деректер ретінде қолданылады (2.3.бабын қараңыз)[7], мысалы,

$$SR_{21}=(\underset{\sim}{t}_{NPSA} \cong \underset{\sim}{B}^{e} \wedge \underset{\sim}{t}_{NCC} \cong \underset{\sim}{VS}^{e}) \in L,$$

$$\boldsymbol{SR_2}=\{$$

$$SR_{22}=(\underset{\sim}{t}_{NPSA} \cong \underset{\sim}{\ }^{e} \wedge \underset{\sim}{t}_{NCC} \cong \underset{\sim}{S}^{e}) \in LTH,$$

$$SR_{23}=(\underset{\sim}{t}_{NPSA} \cong \underset{\sim}{\ }^{e} \wedge \underset{\sim}{HTTL}_{NCC} \cong \underset{\sim}{A}^{e}) \in \quad ,$$

$$SR_{24}=(\underset{\sim}{t}_{NPSA} \cong \underset{\sim}{B}^{e} \wedge \underset{\sim}{H}_{NCC} \cong \underset{\sim}{\ }^{e}) \in \quad ,$$

$$SR_{25}=(\underset{\sim}{t}_{NPSA} \cong \underset{\sim}{B}^{e} \wedge \underset{\sim}{t}_{NCC} \cong \underset{\sim}{V}^{e}) \in LIM$$

$$\}.$$

7 кезең – инициализация матрицасын анықтау**.**

ШЕ инициализациялау процедурасы үшін (матрица жиынтығы түрінде) шығыс деректерін қалыптастыруға арналған. Барлық FI_{ir_j} алынған нақты мәндерінің негізінде, ШЕ үшін альтернативті таңдау және FI_{ij} (6 кезеңді қараңыз)нақты жұптарының көмегімен сәйкесінше *FI(n, r_n)*анық емес идентификациялау және *MP(n, r_n)* түйіндес жұптары үшін инициализациялау жұптарын анықтаймыз, осындағы *n* – шабуыл саны, алr_n –*i* шабуылды анықтауға арналған ережелер саны.

Мысалы, 6 кезеңде қолдануға арналған осындай матрицалар ШЕ құрғанда *FI(3,5)* және *MP(3, 5)* кейпінде болады, ал олардың нақты элементтері (2.3. бабын қараңыз) [7] бейнеленген.

8 кезең– нәтижені қалыптастыру.

Бұл кезең ауытқушылық жағдайын сипаттайтын шығыс деректерін алуға бағытталаған. Қалыптасқан ықтимал шабуылдар (3кезеңді қараңыз) және түйіндес жұптар (6 кезеңді қараңыз) негізінде – «шабуыл **:** түйіндес жұптар жиыны» қалыптасады $\boldsymbol{I: MP}=(\bigcup_{i=1}^{n} I_i : \bigcup_{j=1}^{c_i} MP_{ij})$ (2.1. бабын қараңыз) [6].

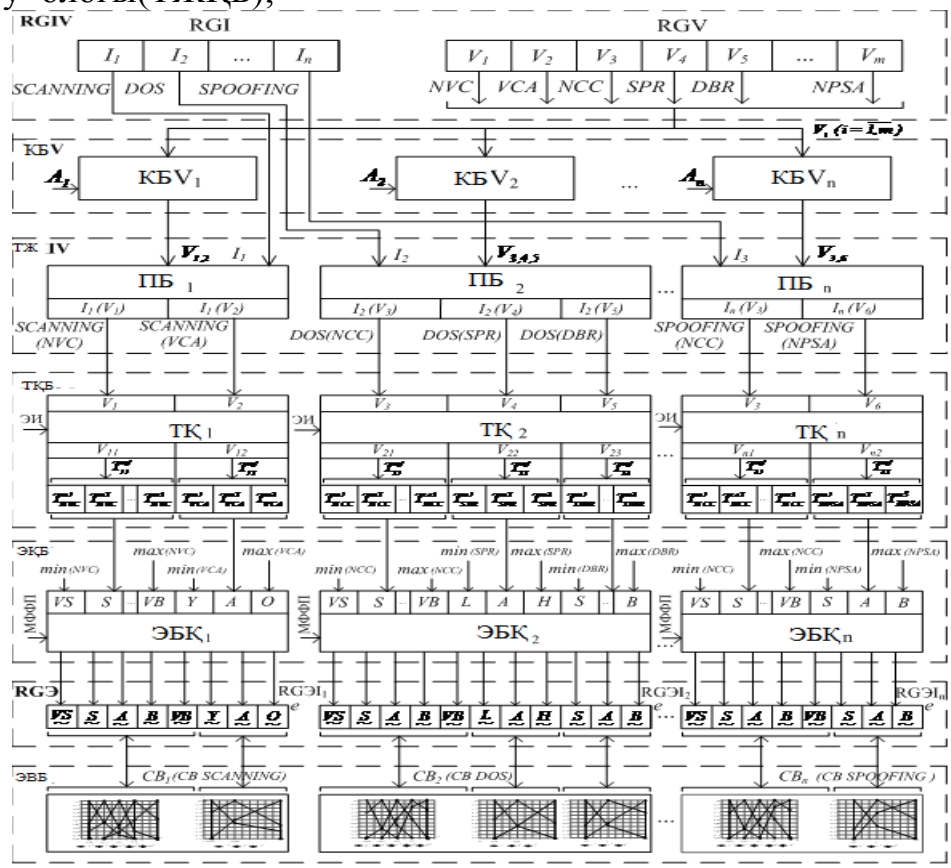
Осы жиынның, қалыптасқан ШЕ және ***FI*** жиынының (6 кезеңді қараңыз) негізінде, (АЕАӘ және ҚФСӘ сарапшыларының таңдалған шешімінің негізінде қызмет ететін) қАСынды қорытынды көмегімен нақты кибершабуыл туындатуы мүмкін ауытқушылық жағдайының деңгейін сипаттайтын, анық емес идентификациялаудың нақты мәндері анықталады. Басқаша айтқанда әрбірI_i–ге FI_i біреуі тағайындалады. Осылайша, мысалы, I_1=*SCANNING,* I_2=*DOS*және I_3=*SPOOFING* сәйкесінше LOW, LTH және H деңгейлері анықталады. Нәтижелерді анықтағаннан кейін ауытқушылықтарға қатысты жүйенің ағымдағы жағдайын сипаттайтын айнымалының мәні сәйкестендірілетін эталонды лингвистикалық термдерді визуализациялау жүзеге асырылады. Бұл технологияның негізінде компьютерлік желілердегі шабуылдаушы әрекеттер туындатқан ауытқушылықтарды анықтаудың шынайы жүйелерін құруға немесе жетілдіруге болады.

3.2Желілік шамалардың анық емес эталондарын қалыптастырудың ішкі жүйесі

ШТЖ ауытқушылық жағдайын (3.1.бабын) анықтау технологиясында АЕЭ қалыптастыру кезеңін жүзеге асыру үшін ауытқушылық жағдайын идентификациялау мақсатында желілік трафиктің ағымдағы мәндерін өлшеуге бағытталған ішкі жүйенің (3.2.бабын) жаңа құрылымдық шешімі ұсынылады.

Ішкі жүйенің құрамына :

- I_i $(i=\overline{1,n}$ $)$шабуылдардың идентификациялау мен V_i $(i=\overline{1,m})$ шамаларының ағымдағы мәндерін қабылдау мен сақтауға арналған шабуыл мен шамалардың регистрі (RGIV);
- шабуылдың сәйкес түріне шамалар ағынын қалылыптастыруды жүзеге асыратын шамалар коммутациясының блогы (БКV);
- шабуылдың идентификациялау жұпты байланыстыруға және оған сәйкес шамаларға арналған шабуыл мен түйіндес шамаларды қалыптастыру блогі (БПIV);
- T_{ij}^{ef} берілген жиынын өндіруге қолданылатын термдер жиынын қалыптастыру блогы(ТЖҚБ);



Сурет 3.2-Желілік шамалардың анық емес эталондарын қалыптастырудың ішкі жүйесінің құрылымы

- әрбір T_{ij}^{ef} үшін сәйкес эталонды анық емес сандарды(АЕС) есептеуді жүзеге асыратын эталондарды қалыптастыру блогы (ЭҚБ);

- есептелген эталонды АЕС қабылдау және уақытша сақтауға қызмет атқаратын эталондар регистрі (RGЭ);

- алынған эталонды АЕС графикалық түрде бейнелеуге арналған эталонды визуализациялау процессоры;

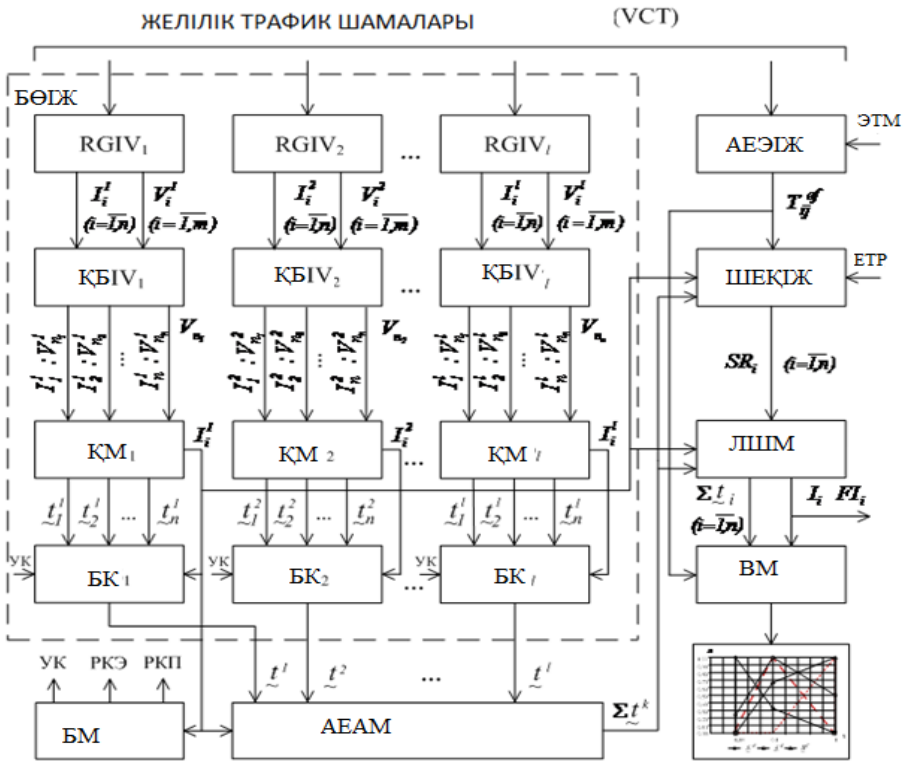
Ішкі жүйе келесі түрде қызмет атқарады (3.2 және 3.3суреттерін қараңыз). (RGI) және RGIVретінде таңбаланатын (RGV) шабуылдар регАСтріне I_i ($i=\overline{1,n}$) идентификациялаудың ағымдағы мәндері жәнеV_j ($j=\overline{1,m}$)кіріс шамаларының (3.3 суретіндегі сәйкесінше 1, 2 және 3, 4 жоғарғы шегін)мәндері есептеу процессі кезеңінде алдын-ала енгізіледі және сақталады.

I_i ($i=\overline{1,n}$) идентификациялаудың (RGI RGIV (КБV$_i$, $i=\overline{1,n}$ түскен ШКV шамалар коммутациясының сәйкес (ШКV$_i$, $i=\overline{1,n}$) торабына белгісі бойынша) және V_j ($j=\overline{1,m}$) шамалар жиынтығының негізінде I_i ($V(A_i)$) ($i=\overline{1,n}$) ауқымды (векторларды) қалыптастыру жүзеге асырылады (A_iбелгісі i тіркелген мәні бойынша $V(A_i)$ өз шамалар жиынтығы коммутацияланады, мысалы, егер$i=1$ RGI –ден I_1 түссе,ал RGV-ден БКV$_1$ арқылы БП$_1$–ге A_1 дабылы бойынша $V(A_1)=V_{1,2}=\{V_1, V_2\}=\{NVC, VCA\}$ шамалар тобы ұқсас, егер $i=2$ болса, $V(A_2)=V_{3,4,5}=\{V_3,V_4,V_5\}=\{NCC, SPR, DBR\}$, ал $i=3$болса,$V(A_3)=V_{3,6}=\{V_3, V_6\}=\{NCC, NPSA\}$, яғни I_1 $(V(A_1))=I_1$ $(V_{1,2})=SCANNING$ (NVC, VCA), I2 (V(A2))=I2 (V3,4,5)=DOS (NCC,SPR,DBR), және I3 (V(A3))=I3 (V3,6)= SPOOFING (NCC, NPSA).

Бұл ауытқулардың атауына шабуыл түрінің идентификациялау сәйкес келеді, ал сәйкес шабуыл тудырған ауытқушылықтарды анықтау үшін қолданылатын шамалар - элементтер болып табылады (3.3 суретіндегі 5,6 жоғарғы қараңыз).

Ары қарай термдерді қалыптастырудың сәйкес тораптарында(УФТ$_i$, $i=\overline{1,n}$) барлық V_i ($i=\overline{1,m}$)үшінT_{ij}^{ef} ($f=\overline{1,r}$; $i=\overline{1,n}$; $j=\overline{1,m}$) мәндері жасалады.

Осындай термдердің саны жән олардың анық емес түсіндірмесі (талдауы) сәйкес пән саласы бойынша мамандардың пайымдарының негізінде алынған сарапшылық ақпаратты (СА) анықталады.



Сурет 3.3-Желілік шамалардың анық емес эталондарын қалыптастырудың ішкі жүйесінің жұмыс алгоритмі

Әрбір жұптарды қалыптастырудың і-торабы (УФТ$_i$) үшін СА қатысты АЕЭҚІЖ өз мәндеріне j' және f' (3.3суретіндегі 7÷10 жоғарғы шегін)сәйкес барлық V_i. үшін T_{ij}^{ef} талап етілетін жиындары қалыптасады. Мысалы, егер $m=$ j' $=2$ және f' $=5$ және

егер $i=3$, $j'=2$мен $f'=3$шығысында Әрбір жұптарды қалыптастырудың і-торабы (УФТ$_1$) ауқым (вектор) қалыптасады:

$$\text{УФТ}_1(\{T_{11}^{e1}, T_{11}^{e2}, T_{11}^{e3}, T_{11}^{e4}, T_{11}^{e5}\}, \{T_{12}^{e1}, T_{12}^{e2}, T_{12}^{e3}\}) =$$
$$(\{T_{NVC}^{e1}, T_{NVC}^{e2}, T_{NVC}^{e3}, T_{NVC}^{e4}, T_{NVC}^{e5}\}, \{T_{VCA}^{e1}, T_{VCA}^{e2}, T_{VCA}^{e3}\}).$$

Әрбір УФЭ$_i$әрбір I_i үшін талап етілетін термдер жиынтығын алғаннан кейін әрбір T_{ij}^{ef} үшін АЕС нақты мәндері анықталады. Осы процедураны жүзеге асыру үшін барлық V_i ($i=\overline{1,m}$)үшін яғни барлық $min\,v_i$ және $max\,v_i$ (3.3суретіндегі 11және 12 жоғарғы шектері) (мысалы, для V_1және V_2шектері $min\,v_1 = min(NVC)$, $max(v_1) = max(NVC)$және $min\,v_2 = min(VCA)$, $max(v_2) = max(VCA)$), сонымен бірге бекітілген критерийлерге сәйкес ҚФҚӘ таңдаймыз (3.1.2кезеңді қараңыз). Осылайша БЭҚ$_i$ шабуыл үшін массив (вектор) T_{ij}^{ef} ауқым (векторы) қалыптасады, мысалы, түйіндес жұп қалыптасу блогі (БФСТ) ұқсас T_{ij}^{ef} арналған n, j' және f' мәндері келесідей болады:

$$\text{УФЭ}_1(\{\tilde{T}^{e1}_{NVC}, \tilde{T}^{e2}_{NVC}, \tilde{T}^{e3}_{NVC}, \tilde{T}^{e4}_{NVC}, \tilde{T}^{e5}_{NVC}\}, \{\tilde{T}^{e1}_{VCA}, \tilde{T}^{e2}_{VCA}, \tilde{T}^{e3}_{VCA}\}) =$$

$$\text{УФЭ}_1(\{\overset{\sim}{VS}^{e}, \tilde{S}^{e}, \tilde{A}^{e}, \tilde{B}^{e}, \overset{\sim}{VB}^{e}\}, \{\tilde{Y}^{e}, \tilde{A}^{e}, \tilde{O}^{e}\}).$$

Ары қарай барлық T^{ef}_{ij} үшін қалыптасқан АЕС жиынтығы RGЭ қайта жазылады,*i* шабуыл (RGЭI$_i$) шамаларына сәйкес эталондарының мәндері сәйкес регистрге тіркеледі және есептеу үрдісінің бойында сонда (3.3.суретінің 13 ÷16 және 17 жоғарғы шегін қараңыз).

Әрбір T^{ef}_{ij} визуализациялау процессоры арқылы (КШП$_i$, $i=\overline{1,n}$) әрбірI_i. үшін шамалар эталондарының графикалық кескіндемесі қалыптасады. Басқа сөзбен айтқанда КШП$_1$$I_1$ үшін эталондарды визуализациялайды КШП$_2$ – I_2үшін,ал КШП$_n$ –I_nүшін мысалы, егер$n=3$КШП$_1$*SCANNING (*СВ *SCANNING*) үшін эталондарды визуализациялау, КШП$_2$–*DOS (*СВ *DOS)* үшін, ал КШП$_3$– *SPOOFING (*СВ *SPOOFING*) үшін эталондарды визуалдау (3.3 суретіндегі 13 ÷ 15 және 18 жоғарғы шектерін қараңыз).

Осылайша ұсынылған ішкі жүйенің құрылымы (3.2 суретін қараңыз) бағдарламалы немесе бағдарламалық –аппаратты түрде жүзеге асырылуы және 3.1 бабында ұсынылған сәйкес технологияны жүзеге асыратын ауытқушылық жағдайын анықтау жүйелерінде қолданылуы мүмкін.

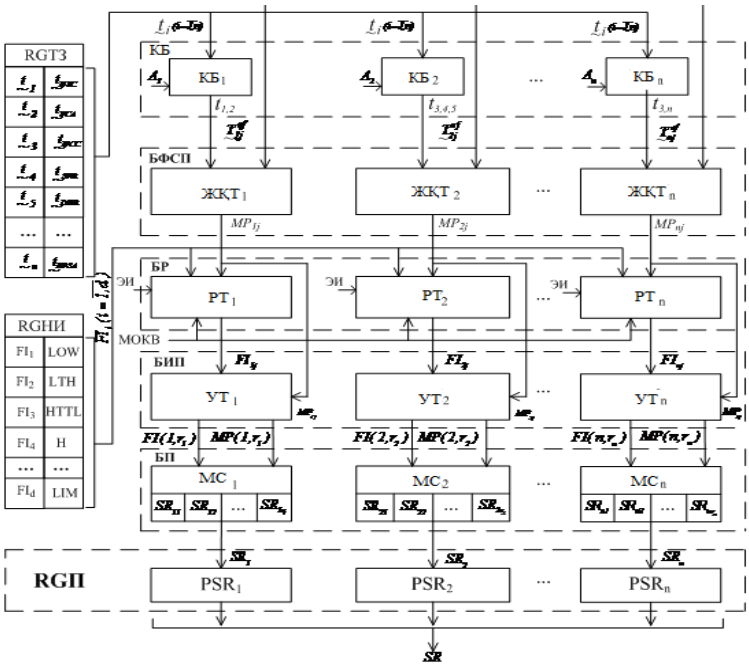
3.3 Желілік белсенділікті бағалауға арналған шешуші ережелерді қалыптастырудың ішкі жүйесі

Компьютерлік желілердегі (3.1бабын қараңыз) кибершабуылдар тудырған ауытқушылық жағдайын анықтау технологиясында ШЕ қалыптастыру кезеңін жүзеге асыру үшін желілік белсенділікті бағалау үшін ағымдағы және эталонды шамалардың өзара байланысының шынайылығын тексеруге бағытталған, шешуші ережелерді қалыптастыруға негізделген сәйкес ішікі жүйенің жаңа құрылымдық шешімі ұсынылады(3.4 суретін қараңыз).

Ішкі жүйенің құрамына :

- эталондар регистрі (RGЭ) (3.2 бабын қараңыз);
- $\tilde{t}_i$ ағынын қалыптастыруға қызмет ететін түйіндес жұптарды қалыптастыру блогы(ТЖҚБ);
- эталонды T^{ef}_{ij} қасынды түрлендіруге арналған ТЖҚБ;
- МК қалыптастыруды жүзеге асыратын саралау блогы (СБ);
- матрица қалыптастыратын $FI(^{i,r_r})$және$MP(^{i,r_r})$ ережелерді инициализациялау блогы (ЕИБ);
- сәйкес деректер секторында (ДС$_i$, $i=\overline{1,d}$) SR_{ir_i}($i=\overline{1,n}$)ережелер жиынтығын сақтауға қызмет ететін ережелер қоры (ЕҚ);
- ағымдағы мәндер (RGTAM) және барлық $\tilde{t}$ менFI_i($i=\overline{1,d}$)мәндерін есептеу үрдісіндегі анық емес идентификациялау регистрі (RGНИ);

- SR_i ережелер ішкі жиынын қабылдау және сақтауға арналған ережелер регАСтрі (RGE).



Сурет 3.4- Желілік белсенділікті бағалауға арналған шешуші ережелерді қалыптастырудың ішкі жүйесінің құрылымы

Ішкі жүйе келесі түрде қызмет атқарады (3.5 суретінен қараңыз)

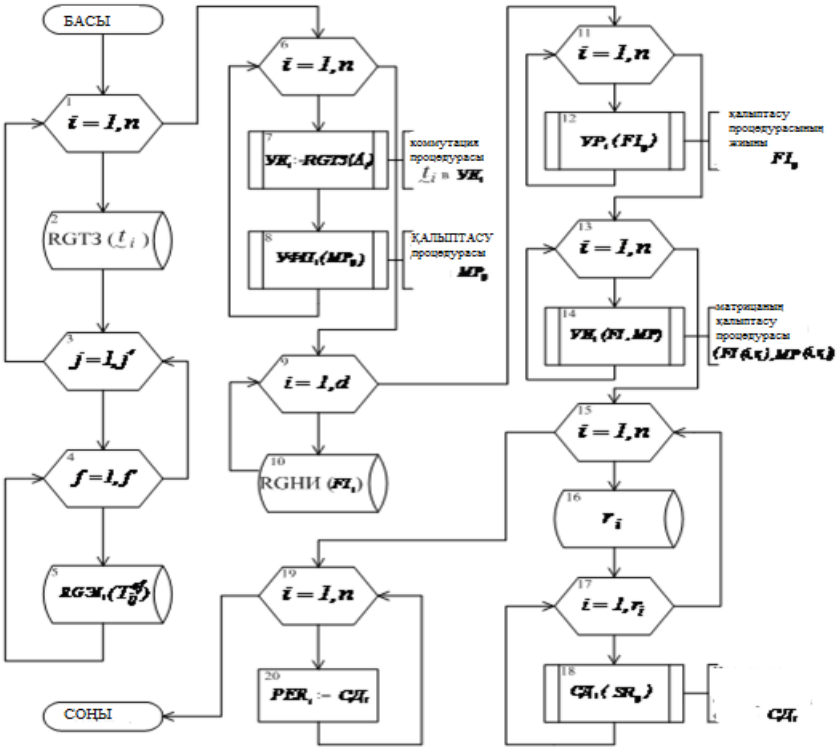
Әрбір RGЭ *i* басып кіруі (RGЭI$_i$, $i=\overline{1,n}$) *i* шабуылға тән $\tilde{T}_{ij}^{ef}$ ($i=\overline{1,n}$)сәйкес шамаларының эталондар тобының мәндерінің есептеу барысында енгізіледі және сақталады, сонымен бірге RGAM $\tilde{t}_i$ ($i=\overline{1,n}$) ағымдағы мәндері енеді (3.5суретіндегі 1-4 жоғарғы шектерін қараңыз).

ТЖҚБ түйіндес жұп қалыптасу блогі $_i$, $i=\overline{1,n}$ ПФРП $\tilde{T}_{ij}^{ef}$ ($i=\overline{1,n}$) эталонды мәндерінің RGЭI$_i$($i=\overline{1,n}$) және $\tilde{t}_i$ ($i=\overline{1,n}$) ТЖҚБ ағымдағы шамаларының ішкі жиынынан түсетін, RGTЗ түскен (КБ$_i$, $i=\overline{1,n}$) коммутация тораптары арқылыКБ A_i ($i=\overline{1,n}$) басқарушы белгі негізінде (мысалы, $i=1$,$i=2$ және$i=n$ мәндерінде ЖҚТ $_1$, ЖҚТ $_2$және ЖҚТ $_n$ с RGAM КБ$_1$, КБ$_2$ жәнеКБ$_n$ арқылы сәйкесінше$t_{1,2}=\{\tilde{t}_1,\tilde{t}_2\}=\{\tilde{t}_{NVC},\tilde{t}_{VCA}\}$, $t_{3,4,5}=\{\tilde{t}_3,\tilde{t}_4,\tilde{t}_5\}=\{\tilde{t}_{NCC},\tilde{t}_{SPR},\tilde{t}_{DBR}\}$және$t_{3,n}=\{\tilde{t}_3,\tilde{t}_n\}=\{\tilde{t}_{NCC},\tilde{t}_{NPSA}\}$)қалыптасады және ЖҚТ $_i$ (3.5суретіндегі 6, 7 және 8 жоғарғы шектерін қараңыз) кіруінеMP_{ij}түйіндес жұптар, мысалы, $MP_{21}=(\tilde{t}_{NPSA}\cong\tilde{B}^e \wedge \tilde{t}_{NCC}\cong\tilde{VS}^e)$ түседі.

RGHИ FI_i ($i=\overline{1,d}$)барлық мәндері енгізілетінін және ережелер қалыптасу үрдісінде сақталады (3.5 суретіндегі 9 және 10 жоғарғы шектерін қараңыз).

Әрбір саралау торабында (СТ$_i$, $i=\overline{1,n}$) СБ әрбір MP_{ij} ($i=\overline{1,n}$)ықтимал шешім ретінде кезекпен RGHИ түскен барлық FI_i ($i=\overline{1,d}$)анық емес идентификациялау сәйкестілікке қойылады. Ары қарай осылай қалыптасқан SR_{ij}^{k} альтернативті ережелер жиыны МКАӘ және негізінде ШЕ инициализациялауға қажет FI_{ij}, жиыны анықталады (3.5 суретіндегі 11және 12жоғарғы шектерін қараңыз)

Ары қарай және ЖҚТ $_i$ мәліметтер қорының ҚЭБ негізінде (УИ$_i$, $i=\overline{1,n}$) инициализациялау тораптарында қажет ережелер жиынтығын негізінде жүзеге асырылатын, екі-екіден $MP(1, r_1)$және$FI(1, r_1)$ матрицасының элементтері қалыптасады (3.5 суретіндегі 11 және 12 жоғарғы шектерін қараңыз).



Сурет 3.5-Желілік белсенділікті бағалауға арналған шешуші ережелерді қалыптастырудың ішкі жүйесінің жұмыс алгоритмі

ИБ $_i$ жасалған матрицалар екі-екіден ЕҚ (ЕҚ$_i$, $i=\overline{1,n}$)мәліметтер секторына енгізіледі, осылайша i шабуылдың туындаған ауытқушылық жағдайына арналған $SR_{ij}(i=\overline{1,n}, j=\overline{1,r_i})$ ережелер жиынтығын қалыптастырады(3.5 суретінен 15-18 жоғарғы шектерін қараңыз)Ары қарай SR_i ($i=\overline{1,n}$)ережелеріSR_i (PSR$_i$,$i=\overline{1,n}$) регистрінде қайта жазылады және ішкі жүйенің қызмет атқару үрдісінде сақталады (сурет3.4).

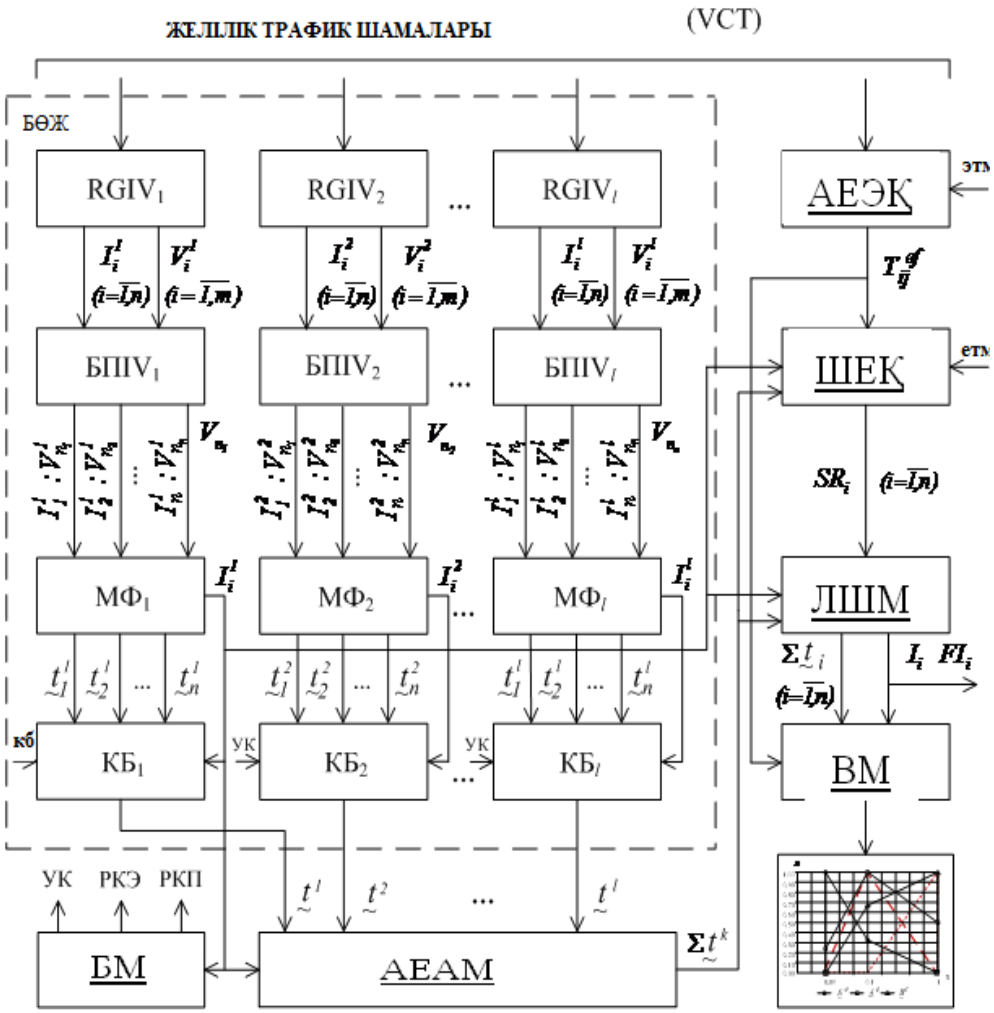
3.4 Ауытқушылық жағдайын анықтау технологиясын жүзеге асыру жүйесі

Қоршаған ортадағы белсенділікті бақылауға бағытталған БШМ, ЭШМ және ШЕМ есепке ала отырып (2.1-2.3 баптарын қараңыз)[6, 7] ауытқушылық жағдайын(3.1.бабын) анықтаудың ұсынылған технологиясын жүзеге асыру арқылы желілік қауіпсіздік жүйесін жетілдіру үшін қолдануға болатын жаңа құрылымдық шешімді[12] құрастырамыз.Бұл шешім жаңа(0-day) және сигнатуралық емес кибершабуыл түрлерін нәтижелі идентификациялауға арналған қазіргі заманғы ШТЖ функционалды мүмкіндіктерін кеңейтуге мүмкіндік береді.

Технологияны жүзеге асыру үшін (3.1бабын қараңыз) [9] құрамына енетін :

- шамалардың және олардың фаззификациясын, шабуылдаржиынын қалыптастыруға арналған алғашқы өңдеудің ішкі жүйесін (АӨІЖ) (3.1бабындағы 3 және 5 кезең) [9];
- желілік шамалардың ағымдағы мәндерін өлшеу мақсатында (3.1 бабындағы 4кезең) [9] әрбір анық емес айнымалы үшін қажет термдерді алуға бағытталған анық емес эталондарды қалыптастырудың ішкі жүйесін(ЭҚІЖ);
- желілік белсенділікті бақылауға арналған ережелер жиынын құруда қолданылатын шешуші ережелерді қалыптастырудың ішкі жүйесін (ШЕҚІЖ) (3.1бабындағы 6 және 7 кезеңдері) [9];
- анық емес және графикалық қабылдауда нәтижені қалыптастыруға арналған анық емес арифметика модулі (АЕАМ), қАСынды шешім әдісі (ҚШӘ) және визуализациялау әдісі (КШӘ) (3.1бабындағы 8кезең) [9];
- басқарушы модуль(БМ), коммутацияны басқаруға арналған модуль (КБАМ), эталондарды түзеу режиміне (ЭТРЖА) және ережелерді түзеу режиміне жүйені аударатын модульден (ЕТРЖАМ)

сәйкес жүйенің құрылымдық шешімін құрастырамыз (3.6 сурет)



Сурет. 3.6 Компьютерлік желілердегі ауытқушылық жағдайын анықтау технологиясын жүзеге асыру жүйесінің құрылымы

Компьютерлік желілердегі ауытқушылық жағдайын анықтау технологиясын жүзеге асыру жүйесі (КЖАЖАТЖА) келесі әдіспен қызмет атқарады.

Есептеу үрдісінің алдында (ЭҚІЖ) желілік трафик шамаларының (VCT) негізінде сәйкес БШМ орай (2.1 бабын қараңыз) [6]I_i ($i=\overline{1,n}$) басып кірулер және V_i ($i=\overline{1,m}$) шамаларының жиыны қалыптасады,олар арқылы таңдалған ҚФҚӘ (бекітілген критерийлерге сәйкес)қолдана отырып (3.1бабындағы 4кезең) [9]әрбір T_{ij}^{ef} термі бойынша нақты ЛА үшін эталондар жасалады.

Компьютерлік желілілердегі шабуылдаушы әрекеттердің ықтимал көріністеріне қатысты желілік белсенділікті бақылау үшін қолданылатын ШЕҚІЖ алынған шамалар эталондарына сәйкес SR_i($i=\overline{1,n}$) шешуші ережелерінің (3.1 бабындағы 6 және 7 кезеңдерін қараңыз) [9] жиынтығының шаблондары құрылады. Бұл шаблондар мен шамалар эталондары

(КЖАЖАТЖА) қызмет атқару барысында өзгермейді, бірақ қажеттілік туындаса оларды ЭТРЖА немесе ЕТРЖАМ түрлене алады.

Ары қарай КЖАЖАТЖА компьютерлік желілердегі *l* тораптарының (жұмыс бекеттеріндегі, серверлердегі және т.б) ауытқушылық жағдайын бақылауға бағытталғанын ескерсе, онда шамалар мен шабуылдардың *l* регистрлеріне ($RGIV_k$, $k=\overline{1,l}$) параллель АӨІЖ -не I_i^k ($i=\overline{1,n}$, $k=\overline{1,l}$) басып кірулерінің идентификациялау және (бекітілген периодты) V_i^k ($i=\overline{1,m}$, $k=\overline{1,l}$ шабуылдың ағымдағы мәндері енгізіледі.

Мысалы, шабуылдың үш түрі I_1^k, I_2^k және I_3^k ($SCANNING^k$, DOS^k және $SPOOFING^k$)алты шама V_1^k, V_2^k, V_3^k, V_4^k, V_5^k және V_6^k (NVC^k, VCA^k, NCC^k, SPR^k, DBR^k және $NPSA^k$ негізінде туындаған ауытқушылық жағдайын идентификациялау мүмкіндік беретін *k* желі торабы үшін *n=3* және $m=6I_i$, және V_i қалыптасады (3.1 бабындағы 3 кезеңді қараңыз) [9] I_1^k, I_2^k және I_3^k ($SCANNING^k$, DOS^k және $SPOOFING^k$)жүзеге асырылады. Егер компьютерлік желі тораптары өз сипаттамалары бойынша әртекті болса, онда сәйкес шабуылдаушы әрекеттер туындатқан белгілі ауытқушылықтар түріне эталондар мәндері өзгеше болатынын ескерген жөн.

Анықтауға қажет шамаларымен бірге (3.1бабының кезеңін қараңыз) [9] нақты басып кіру жұбын қалыптастыру үшін арнайы түрде ұйымдастырылған еске сақтау құрылғысы ретінде ұсынылатын $БПІV_k$($k=\overline{1,l}$)ӨІЖ шабуылдармен шамалардың *l* блоктары қолданылады. Мысалы, сол *n=3*және *m=6*

$$(I_1^k), (I_2^k) \text{ и } (I_3^k)$$

басып кіру идентификациялау бар k торабы үшін сәйкесінше

$$V_{n_1}^k=(V_1^k, V_2^k), V_{n_2}^k=(V_3^k, V_4^k, V_5^k) \text{ и } V_{n_3}^k=(V_3^k, V_6^k), \text{ т.е.}$$

$$SCANNING^k:\{NVC^k, VCA^k\},$$

$$DOS^k:\{NCC^k, SPR^k, DBR^k\} \text{ и}$$

$$SPOOFING^k:\{NCC^k, NPSA^k\}, (k=\overline{1,l})$$

шамалар жұбы қалыптасады.

Бұл мысалда БПІV ұйымдастыруға қатысты $SCANNING^k$, DOS^k және $SPOOFING^k$ идентификациялау арнайы ұйымдастырылған еске сақтау құылғысының мекенжайы болатынын ескерген жөн, ал $\{NVC^k, VCA^k\}$, $\{NCC^k, SPR^k, DBR^k\}$ және $\{NCC^k, NPSA^k\}$сәйкесінше осы мекенжайлар бойынша құрамы болады.

БПІV$_k$($k=\overline{1,l}$) $I_i^k : V_{n_i}^k$ жұбын қалыптастыру процедурасы аяқталғаннан кейін ФМ$_k$($k=\overline{1,l}$) фаззификация модульдері көмегімен (ҚФҚӘ арқылы) түрлендіру жүзеге асырылады (3.1бабындағы 1 кезеңді қараңыз) [9] (белгілі уақыт аралығында бақылауға алынатын) шамалардың ағымдағы мәндерінің жиындарының көмегімен бір анық емес сан АЕС арқылы ($i=\overline{1,n}$), (3.1бабындағы 5 кезеңді қараңыз) [9] және осылайша nАЕС $\tilde{t}_i^k$ ($i=\overline{1,n}$) сәйкес I_i байланысты МҚ$_k$ аламыз.Мысалы, егер $n=6$мәнінде $\tilde{t}_1^k=\tilde{t}_{NVC}^k$, $\tilde{t}_2^k=\tilde{t}_{VCA}^k$, $\tilde{t}_3^k=\tilde{t}_{NCC}^k$, $\tilde{t}_4^k=\tilde{t}_{SPR}^k$, $\tilde{t}_5^k=\tilde{t}_{DBR}^k$ және $\tilde{t}_6^k=\tilde{t}_{NPSA}^k$ болады.

Ары қарай, кезекпен алынған $\tilde{t}_i^k$ ($i=\overline{1,n}$, $k=\overline{1,l}$) k коммутациялау блоктары арқылы КБ$_k$($k=\overline{1,l}$)коммутацияны басқару белгісі (КБД) арқылы I_i^k ($i=\overline{1,n}$, $k=\overline{1,l}$) АӨІЖ шабуыл түріне сәйкес анық емес арифметика модуліне (АЕАМ) барлық КБ$_k$($k=\overline{1,l}$) компьютерлік желінің барлық тораптарындағы белсенділікті сипаттайтын $\sum \tilde{t}^k$ қосынды көрсеткіштерін алу үшін $\tilde{t}^k$ ($k=\overline{1,l}$)ағымдағы шамалары түседі. Анық емес арифметика амалдарын(он төрт бекітілгеннің ішінен) жүзеге асыру үшін берілген критерийлерге сәйкес ең ыңғайлы әдіс таңдалады және АЕАМ(3.1бабынан 1 кезеңді қараңыз) [9] жүзеге асырылады.

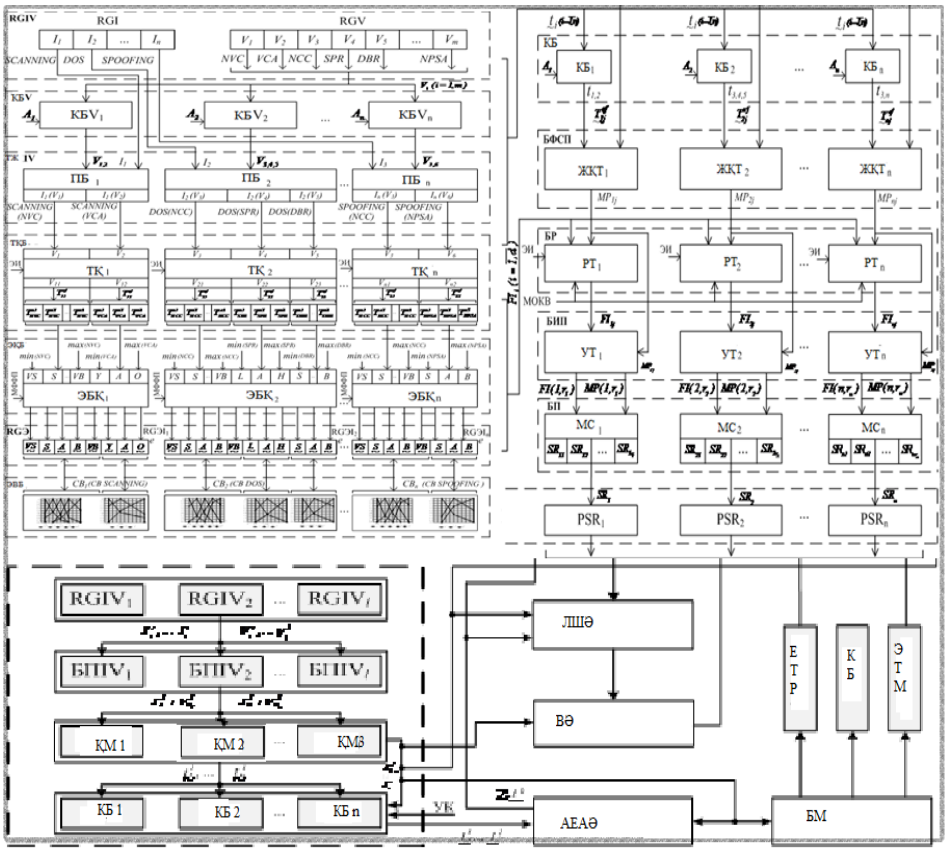
Егер VCT деректері бойынша ауытқушылық жағдайын анықтау процессібір есептеу желісінің торабында жүзеге асырылса, онда АЕАМмөлдір болып табылады, яғни онда ешқандай айнымалы қосындыларының мәндері қосылмайды.

АЕАМ $\tilde{t}^k$ қосынды көрсеткіштерінің негізінде және белгілі технологияға сәйкес ЛШМ нақты I_i бар, белгілі технологияға сәйкес(3.1 бабының 8кезеңін қараңыз) [9] ШЕҚІЖ шешуші ережелерді қалыптастырудың ішкі жүйесі бастамашылық еткен SR_i($i=\overline{1,n}$)ережелер жиынын FI_i($i=\overline{1,d}$)арқылы кибершабуылдардың белгілі түрі тудырған VCT ауытқушылық жағдайдың ағымдағы деңгейін анықтау жүзеге асырылады.

Бұл деңгей анық емес түрде ұсынылуы мүмкін, сондай ақ МВ -арқылы ПФРП қалыптасқан лингвистикалық айнымалылардың эталонды мәндерінде бейнеленген сәйкес АЕС графикалық түрде идентификациялайды.

Осылайша анық емес эталондарды қалыптастырудың, шешуші ережелер мен алғашқы өңдеудің ішкі жүйесіне, сонымен бірге анық емес арифметиканың, қиысынды қорытындының, визуализациялау және басқарушы модульдерге тіректенетін (3.7 суреті) [12] жүйенің негізінде сигнтауралық емес кибершабуылдар әрекеттері тудырған ауытқушылық жағдайын /анықтауға қолданылатын алгоритмдік, бағдарламалық және бағдарламалық қамтамасыздандыру құруға болады. Осындай қамтамасыздандыру автономды түрде немесе компьютерлік желілердегі шабуылдарды анықтаудың қазіргі

заманғы жүйесінің функционалдық мүмкіндіктерін кеңейткіш ретінде қолданыла алады.



Сурет 3.7-Ауытқушылық жағдайын анықтау жүйесі

Үшінші тарау бойынша тұжырым

1.Базалық шамалар моделі, эталонды шамалар моделі, шешуші ережелер моделі мен анық емес шамаларды салыстыру әдісінің, қатыстылық функциясын қалыптастыру, маңыздылық коэффициентінің, анық емес арифметика амалдарын жүзеге асыру, сонымен бірге әлсіз нысанданған анық емес ортадағы шамалардың ағымдағы мәндерінің негізінде қоршаған ортада кибершабуылдардың белгілі түрі тудырған ауытқушылық жағдайын анықтау үрдісін ашатын сегіз негізгі кезеңнен тұратын ауытқушылық жағдайын анықтау технологиясы құрылды.Бұл технология негізінде компьютерлі жүйелер мен желілердегі шабуылдаушы әрекеттер тудырған ауытқушылық жағдайын анықтаудың қазіргі жүйесін жетілдіруге немесе құруға болады.

2. Компьютерлік желілердегі кибершабуылдар тудырған ауытқушылық жағдайын анықтау технологиясындағы шамалар эталондарын қалыптастыру кезеңін жүзеге асыру үшін жұмыс істеу алгоритмі және ауытқушылық жағдайын идентификациялау мақсатында желілік трафик шамаларының ағымдағы мәндерін өлшеуге бағытталған бағдарламалы немесе бағдарламалы-аппаратты түрде жүзеге асырыла алатын сәйкес ішкі жүйенің жаңа құрылымдық шешімі құрылды.

3. Компьютерлік желілердегі кибершабуылдар тудырған ауытқушылық жағдайын анықтау технологиясындағы шешуші ережелер жиынын қалыптастыру кезеңін жүзеге асыру үшін сәйкес ішкі жүйенің құрылымдық шешімі және шешуші ережелерді қалыптастыруға, қоршаған ортадағы желілік белсенділікті бағалауға арналған эталонды және ағымдағы шамалардың өзара байланысының шынайылығын тексеруге бағытталған жұмыс істеу алгоритмі ұсынылды. Ұсынылған шешім бағдарламалы немесе бағдарламалы-аппаратты түрде жүзеге асырылып және ауытқушылықтарды анықтау жүйесінің негізі ретінде қолданылуы мүмкін.

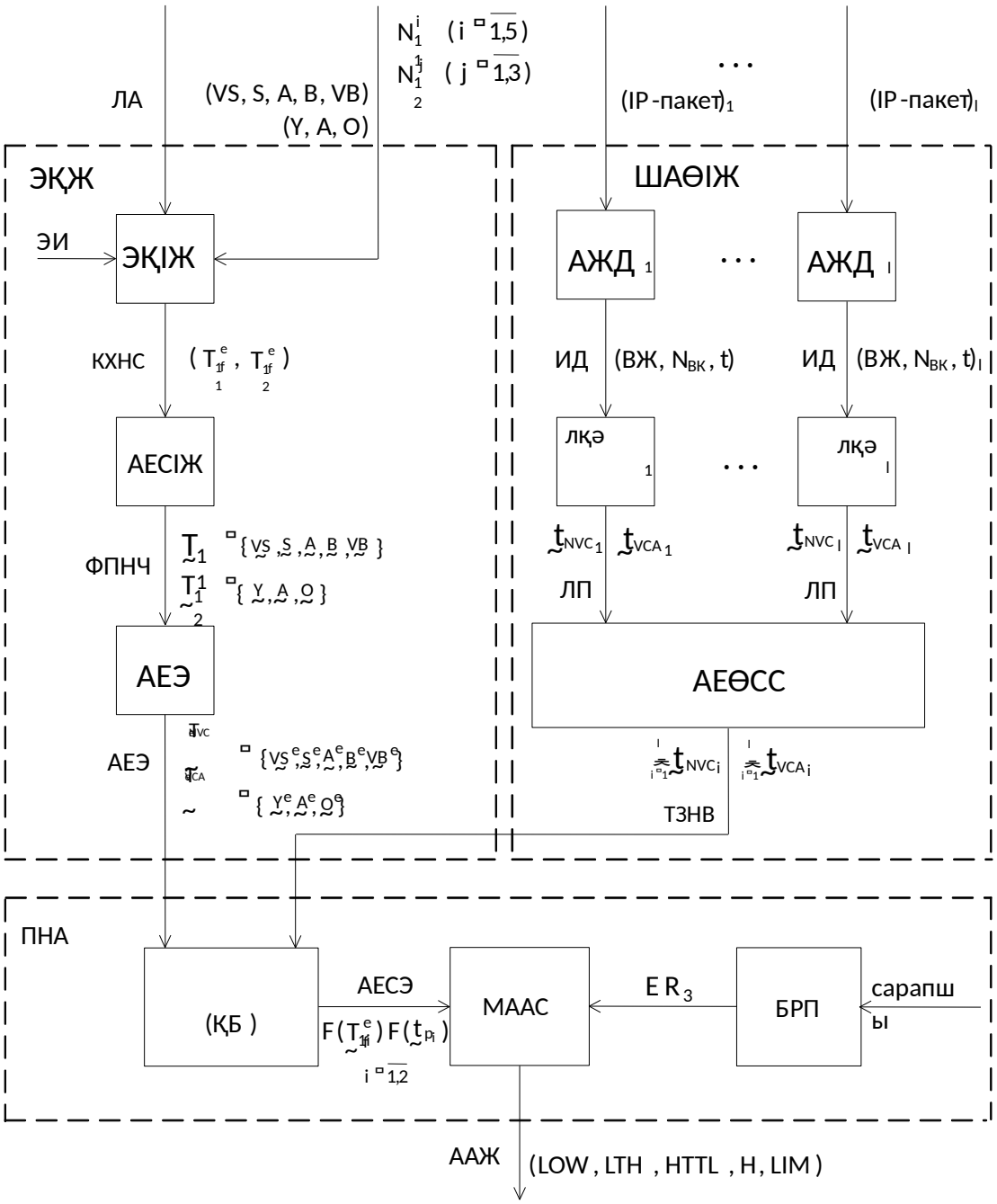
4. Желілік шамаларың анық емес эталондарын қалыптастырудың ішкі жүйесінің және желілік белсенділікті бағалауға арналған шешуші ережелердің негізінде және сонымен бірге базалық шамалар моделін есепке ала отырыпжелілік қауіпсіздік жүесін жетілдіруде қолданыла алатын ауытқушылық жағдайын анықтау технологиясын жүзеге асыратын жаңа құрылымдық шешім құрастырылды. Осындай шешім сондай ақ бағдарламалы немесе бағдарламалы-аппаратты түрде және жаңа(0-day) мен сигнатуралық емес кибершабуылдарды нәтижелі идентификациялаудың есебінен шабуылдарды анықтаудың қазіргі заманғы жүйесінің функционалдық мүмкіндіктерін кеңейткіш ретінде жүзеге асырылуы мүмкін .

4 КОМПЬЮТЕРЛІК ЖЕЛІЛЕРДЕ АУЫТҚУЛАРДЫ АНЫҚТАУ ҚҰРАЛДАРЫН ЗЕРТТЕУ

4.1Порттарды сканерлеуде тудырған ауытқушылықтарды анықтаудың типтік жүйесі

Ұсынылған ауытқушылықтарды анықтаудың жалпы техникалық шешімі негізінде (3.4 бабын)сканерлеуші утилиттер тудырған желілік трафиктегі ауытқушылықтарды анықтаудың желілік жүйесін[12] жаңғыртамыз.4.1. суретте құрамына:

- эталондарды қалыптастырудың ішкі жүйесі(ЭҚІЖ) порттарды сканерлеу жағдайы үшін АЕЭҚІЖ (3.6 суретін қараңыз) кескіндемесі болып табылады) және I_1= *SCANNING* (2.1бабын қараңыз) тудырған ауытқушылықтарға тән шамаларды түзетуге және эталонды ретінде қабылданатын бақылауға алынған қоршаған ортаның нақты тұрақты жағдайын қалыптастыру индикаторы ретінде қолданылатын шамаларды түзетуге арналған);
- шамаларды алғашқы өңдеудің ішкі жүйесі (ШАӨІЖ) ШАӨІЖ (3.6 суретті қараңыз) кескіндемесі болып табылады және желілік трафиктің сипаттамаларын анық емес шамалардың ағымдағы мәндерін қалыптастыратын (АЕШАМҚ) бағытталған);
- анық емес сараптаманың ішкі жүйесі(АЕСІЖ АЕЭ арналған қоршаған ортадағы ауытқушылық жағдайының деңгейін (АЖД)анықтау үшін АЕШАМҚ сараптамасын жүзеге асырады).
- енетін аталған жүйенің құрылымдық сызбасы көрсетілген.
- ЭҚІЖ құрамына енеді:
- анық емес шамаларды өңдеу модулі(АЕШӨМ СА негізінде анық емес оқиғалардың сандық сипаттамаларын (АЕӨСС) қалыптастыруға арналған);



Сурет 4.1 - Сканерлеуші утилиттер тудырған ауытқушылықтарды анықтаудың типтік жүйесінің құрылымы

- АЕС қалыптастыру модулі (АЕСҚМ АЕӨСС негізінде АЕС ҚФ құруды жүзеге асырады);
- эталондарды қалыптастыру модулі(ЭҚМ алынған ҚФ негізінде АЕЭ құруды жүзеге асырады)
- ШАӨІЖ құрамына енеді:
- деректер көзін қалыптастырудың *i*-модулі (ДККМ$_i$- желілік трафик шамаларының (ЖТШ) деректерін қалыптастыруға арналған,осындағы $i = \overline{1,l}$, ал *l*- бірлескен желі тораптарының саны);

- ЛА қалыптастырудың *i*-модулі (ЛАҚ$_i$-деректер көзі (ДК) қалыптастырылған қатары арқылы ЖТШ жағдайын бейнелейтін лингвистикалық жиындар мәндерін құрады);

- анық емес арифметиканы жүзеге асыру модулі (АЕАЖАМ) жиынтық АЕШМҚ бір мезетте түрлі бірлескен желіге басып кіру жүзеге асыруын анықтауға арналған. Егер қауіп-қатер бір компьютерге бағытталса, яғни *l=1*болса, онда өткінші одақ ретінде жұмыс істейді және анық емес арифметика амалы орындалмайды) .

- АЕСІЖВ құрамына енеді:

- АЕС реттелген Альтернативті қалыптастыру модулі (РБҚМ-АЕШАМҚ мен АЕЭ негізінде АЕС Альтернативті (АЕСЭ) құруға арналған және олардың негізінде сәйкес реттелген жиын қалыптастыруға арналған);

- шешуші ережелер базасы (ШЕБ – қоршаған ортадағы ауытқушылық жағдайының ағымдағы деңгейіне қатысты шешім қабылдауды қолдауға бағытталған сарапшылармен алдын-ала қалыптасқан деректер қоры) ;

- ауытқушылық жағдайын сараптау модулі (АЖСМ АЕСЭ мен ШЕ негізінде компьютерлік желілердегі шабуылдаушы әрекеттерді анықтау үшін АЖД нақтылауға бағытталған).

Утилиттерді сканерлеуші әрекеттер тудырған ауытқушылықтарды анықтау жүйесінің жұмысын қарастырайық.

ЛА эталондарын қалыптастыру анық емес оқиғаларды (АЕО) негізінде ЭҚІЖ – де жүзеге асырылады (мысалы, $\overset{\sim}{VS}, \tilde{S}, \tilde{A}, \tilde{B}, \overset{\sim}{VB}$ немесе $\tilde{Y}, \tilde{A}, \tilde{O}$ (2.1, 2.2баптарын қараңыз)).

Бұл үшін (2.7), (2.9) және (2.10) өрнектерін $i=1$мен $j=\overline{1,2}$ ЛА**NVC**мен **VCA**үшін есепке ала отырып сәйкес <*NVC, T_{NVC}, U_{NVC}*>мен<*VCA, T_{VCA}, U_{VCA}*>шерулері арқылы T_{11}жәнеT_{12},құрамыз, яғни

$$T_{11}=T_{NVC}=\bigcup_{i=1}^{5} T^i_{NVC} = \{\overset{\sim}{VS}, \tilde{S}, \tilde{A}, \tilde{B}, \overset{\sim}{VB}\} \text{ и}$$

$$T_{12}=T_{VCA}=\bigcup_{i=1}^{3} T^i_{VCA} = \{\tilde{Y}, \tilde{A}, \tilde{O}\}.$$

Бұл термдер сәйкесінше $U_{NVC}\in\{0, max_{NVC}\}$мен$U_{VCA}\in\{0, max_{VCA}\}$ әмбебап жиындарында бейнеленуі мүмкін, мысалы,егер max_{NVC}= 512 және max_{VCA}=300 болса және анық емес T_{NVC}мен T_{VCA} термдері үшін АЕШӨМ өңделетін және жиынтық АЕӨСС құрайтын (4.1 және 4.2 кестесін қараңыз) сарапшының оқиғаларды тіркеудің нақты интервалында (ОТИ) бастамашылық етеді, (мысалы, $N^i_{11}(i=\overline{1,5})$ және $N^j_{12}(j=\overline{1,3})$ОТИ-да [0; 2;3, 8;9; 16;17; 128;129; 512] және [0; 10;11; 100;101; 300] сәйкесінше).

Кесте 4.1 - T_{NVC} үшін деректер

T_{NVC} үшін деректер

ЛА мәндері	Интервал				
	N1	N2	N3	N4	N5
VS	7	3	1	0	0
S	2	5	2	0	0
A	1	2	7	1	0
B	0	0	3	6	2
VB	0	0	2	4	5

4.1 және 4.2 кестелерінің деректерінің негізінде көмек беру матрицасы қалыптасады (2.2 бабын қараңыз).

$$\|k_j\| = \left\| \bigcup_{j=1}^{5} \sum_{i=1}^{5} b_{ij} \right\| = \|10,10,15,11,7\|$$ және

$$\|k_j\| = \left\| \bigcup_{j=1}^{3} \sum_{i=1}^{3} b_{ij} \right\| = \|7,10,7\|,$$

Кесте 4.2 - T_{VCA}үшін деректер

T_{VCA}үшін деректер

ЛА мәндері	Интервал		
	N1	N2	N3
Y	5	3	2
A	2	4	1
O	0	3	4

сонымен бірге а также (2.15) сүйене отырып $i, j = \overline{1, 5}$ мен $i, j = \overline{1, 3}$ болса, $km = \bigvee_{j=1}^{5} k_j = 15$мен $km = \bigvee_{j=1}^{3} k_j = 10$ анықтаймыз және сәйкесінше

$$\|c_{ij}\| = \begin{Vmatrix} 10,5 & 4,5 & 1 \\ 3 & 7,5 & 2 \\ 1,5 & 3 & 7 \\ 0 & 0 & 3 \\ 0 & 0 & 2 \end{Vmatrix}$$ мен $$\|c_{ij}\| = \begin{Vmatrix} 7,1 \\ 2,9 \\ 0 \end{Vmatrix}$$ м

(2.16) өрнегі бойынша $(i, j = \overline{1,5})$ егер $cm_i = \bigcup_{j=1}^{5} \bigvee_{i=1}^{5} c_{ij}$ ={10,5; 7,5; 7; 8,2; 10,7} және $cm_i = \bigcup_{j=1}^{3} \bigvee_{i=1}^{3} c_{ij}$ ={7,1; 4; 5,7} болса, келесі түрге ие ҚФ есептеп шығарамыз:

$$\| \mu_{ij} \| = \begin{vmatrix} 1 & 0,43 & 0,1 \\ 0,4 & 1 & 0,27 \\ 0,2 & 0,43 & 1 \\ 0 & 0 & 0,37 \\ 0 & 0 & 0,19 \end{vmatrix}$$ және $$\| \mu_{ij} \| = \begin{Vmatrix} 1 & 0 \\ 0,42 & 0,2 \\ 0 & 1 \\ 0,7 & 0,35 \\ 0 & 0 \\ 0,5 & \end{Vmatrix}$$

Ары қарай $\bigcup_{i=1}^{5} \Delta B_i / B$ ={0,004; 0,016; 0,031; 0,125; 1} мен $\bigcup_{i=1}^{3} \Delta B_i / B$ ={0,03; 0,33; 1}үшін бағалық ара қатынасты аламыз, АЕӨСС негізінде АЕСҚМ АЕС ҚФ қалыптасады. Осылайша $\tilde{T}_{NVC}$ = { $\tilde{VS}$, $\tilde{S}$, $\tilde{A}$, $\tilde{B}$, $\tilde{VB}$ үшін:

$\tilde{VS}$ ={1/0,004; 0,43/0,016; 0,1/0,031; 0/0,125; 0/1};

$\tilde{S}$ ={0,4/0,004; 1/0,016; 0,27/0,031; 0/0,125; 0/1};

$\tilde{A}$ ={0,2/0,004; 0,43/0,016; 1/0,031; 0,2/0,125; 0/1};

$\tilde{B}$ ={0/0,004; 0/0,016; 0,37/0,031; 1/0,125; 0,52/1};

$\tilde{VB}$ ={0/0,004; 0/0,016; 0,19/0,031; 0,5/0,125; 1/1},

ал $\underset{\sim}{T}_{VCA} = \{\underset{\sim}{Y}, \underset{\sim}{A}, \underset{\sim}{O}\}$үшін:

$\underset{\sim}{Y}$ ={1/0,03; 0,42/0,33; 0,2/1};

$\underset{\sim}{A}$ ={0,7/0,03; 1/0,33; 0,35/1};

$\underset{\sim}{O}$ ={0/0,03; 0,5/0,33; 1/1}.

Осылардың негізінде ЭҚМ сәйкесінше қалыптасады:

$\underset{\sim}{T}^{e}_{NVC} = \bigcup_{i=1}^{5} \underset{\sim}{T}^{ei}_{NVC} = \{\underset{\sim}{T}^{e1}_{NVC}, \underset{\sim}{T}^{e2}_{NVC}, \ldots, \underset{\sim}{T}^{e5}_{NVC}\} = \{\underset{\sim}{VS}^{e}, \underset{\sim}{S}^{e}, \underset{\sim}{A}^{e}, \underset{\sim}{B}^{e}, \underset{\sim}{VB}^{e}\}$, где

$\underset{\sim}{VS}^{e}$ ={0/0,004; 1/0,004; 0,43/0,016; 0,1/0,031; 0/0,125};

$\underset{\sim}{S}^{e}$ ={0/0,004; 0,4/0,004; 1/0,016; 0,27/0,031; 0/0,125};

$\underset{\sim}{A}^{e}$ ={0/0,004; 0,2/0,004; 0,43/0,016; 1/0,031; 0,2/0,125; 0/1};

$\underset{\sim}{B}^{e}$ ={0/0,016; 0,37/0,031; 1/0,125; 0,52/1; 0/1};

$\underset{\sim}{VB}^{e}$ ={0/0,016; 0,19/0,031; 0,5/0,125; 1/1; 0/1}

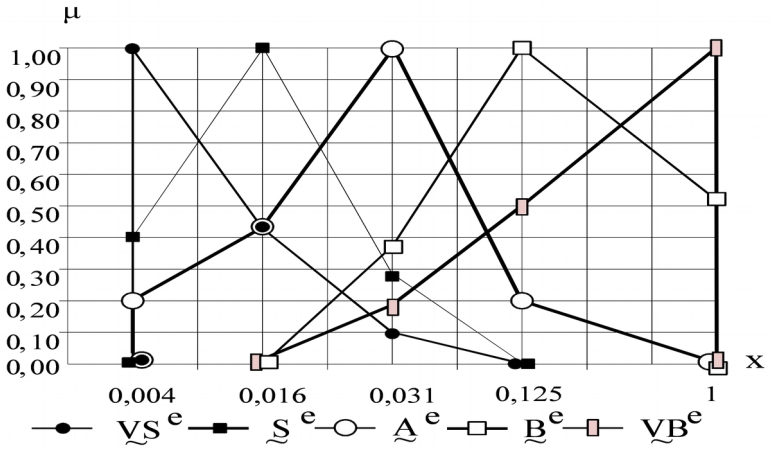
$\underset{\sim}{T}^{e}_{VCA} = \bigcup_{i=1}^{3} \underset{\sim}{T}^{ei}_{VCA} = \{\underset{\sim}{T}^{e1}_{VCA}, \underset{\sim}{T}^{e2}_{VCA}, \underset{\sim}{T}^{e3}_{VCA}\} = \{\underset{\sim}{Y}^{e}, \underset{\sim}{A}^{e}, \underset{\sim}{O}^{e}\}$, осындағы

$\underset{\sim}{Y}^{e}$ ={0/0,03; 1/0,03; 0,42/0,33; 0,2/1; 0/1};

$\underset{\sim}{A}^{e}$ ={0/0,03; 0,7/0,03; 1/0,33; 0,35/1; 0/1};

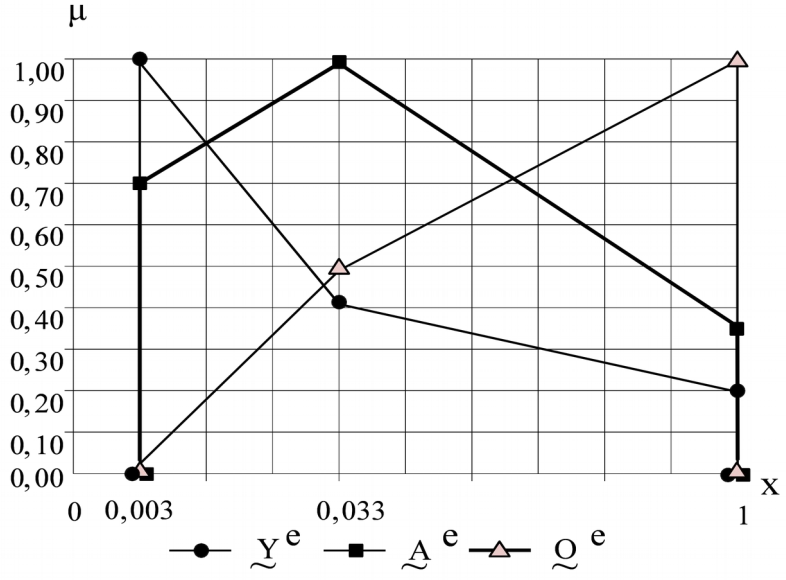
$\underset{\sim}{O}^{e}$ ={0/0,03; 0,5/0,33; 1/1; 0/1}.

NVC мен **VCA** үшін ЛА алынған эталонды мәндері сәйкесінше 4.2 және 4.3 суреттерінде графикалық түрде кескінделген.



Сурет 4.2 -NVC арналған эталонды АЕС

ШАӨІЖнегізінде АЕШАМҚ-ға дайындық, мысалы ВК тудыратын ДККҚМ$_i$ ($i=\overline{1,l}$) ВЖ түрінде ДК қалыптасатын IP-пакеттердің дайындығы $\sum_{i=1}^{l} \underset{\sim}{t}_{NVC_i}$ жүзеге асырылады, $N_{ВК}$, t (2.2 бабын қараңыз). АЕАЖАМ негізінде $\sum_{i=1}^{l} \underset{\sim}{t}_{VCA_i}$ мен қосынды мәндерін анықтау үшін (1.2 бабын)енетін ЛАҚМ$_i$ ($i=\overline{1,l}$) ДК негізінде ЛА ағымдағы мәндерін $\underset{\sim}{t}_{NVC_i}$ и $\underset{\sim}{t}_{VCA_i}$ құрады.



Сурет 4.3-VCA арналған эталонды АЕС

Ары қарай АЕСІЖ $\underset{\sim}{T}^{e}_{NVC}$ мен $\underset{\sim}{T}^{e}_{VCA}$ АЕЭ негізінде (ЭҚІЖ шығу жолында қалыптасқан) және АЕШАМҚ $\underset{\sim}{t}_{NVC_i}$ мен $\underset{\sim}{t}_{VCA_i}$ (мысалы, ШАӨІЖ,*l=1* есептелген), ЭДҚМ енетін,ҚФСӘ негізінде реттелген жиын түрінде РФ арқылы F($\underset{\sim}{T}^{ef}_{1i}$), F($\underset{\sim}{t}_{p_i}$) және $i=\overline{1,2}$ (см. п. 1.2) АЕСЭ қалыптастыру жүзеге асырылады. Ары қарай АЕСІЖ АЖСМ РФ және ШЕБ(ШЕҚІЖ негізінде құрылған (3.4 бабын қараңыз)) ШЕ ***SR₃*** негізінде (2.3бабын қараңыз, (2.23), (2.25)өрнектері)ережелер қалыптасу арқылы :

$SR_{11}=MP_{11} \rightarrow FI(1,1)$,

$SR_{12}=MP_{12} \rightarrow FI(1,2)$,

$SR_{13}=MP_{13} \rightarrow FI(1,3)$,

$SR_{14}=MP_{14} \rightarrow FI(1,4)$,

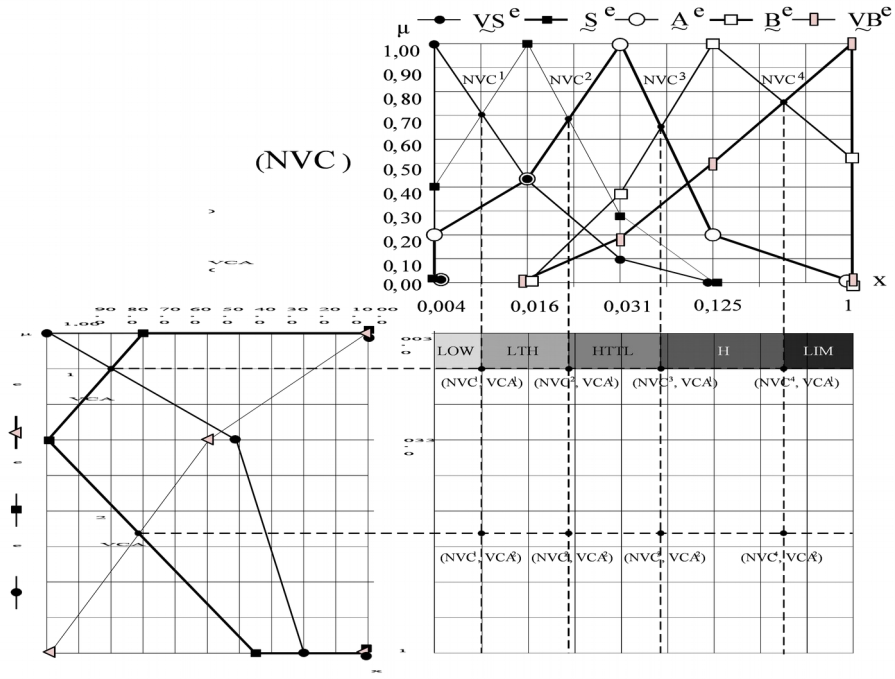
$SR_{15}=MP_{15} \rightarrow FI(1,5)$,

АЖД анық емес түрде анықтау және оның АЕСІЖ АЖСМ шығуы жүзеге асырылады .

АЖД мәндері ережелерді тексеру кезінде анықталатын *L, LTH, HTTL, H, LIM* хабарламаларының бірі арқылы түсіндіріледі:

- SR_{11} = "Егер $\sim^{t_{VCA}}\ \sim^{T^e_{VCA}}$ енетін $\sim^{Y^e}$ неғұрлым жақын болса және $\sim^{t_{NVC}}\ \sim^{T^e_{NVC}}$ енетін $\sim^{VS^e}$ неғұрлым жақын болса, онда *SCANNING*тудырған ауытқушылық жағдайының деңгейі LOW болады";
- SR_{12} = "Егер $\sim^{t_{VCA}}\ \sim^{T^e_{VCA}}$ енетін $\sim^{Y^e}$ неғұрлым жақын болса және $\sim^{t_{NVC}}\ \sim^{T^e_{NVC}}$ енетін $\sim^{Y^e}$ неғұрлым жақын болса, онда *SCANNING* тудырған ауытқушылық жағдайының деңгейі LOWER THAN HIGH болады";
- SR_{13} = "Егер $\sim^{t_{VCA}}\ \sim^{T^e_{VCA}}$ енетін $\sim^{Y^e}$ неғұрлым жақын болса және $\sim^{t_{NVC}}\ \sim^{T^e_{NVC}}$ енетін $\sim^{A^e}$ неғұрлым жақын болса, онда *SCANNING*тудырған ауытқушылық жағдайының деңгейі HIGHER THAN THE LOWEST болады";
- SR_{14} = "Егер $\sim^{t_{VCA}}\ \sim^{T^e_{VCA}}$ енетін $\sim^{Y^e}$ неғұрлым жақын болса және $\sim^{t_{NVC}}\ \sim^{T^e_{NVC}}$ енетін $\sim^{B^e}$ неғұрлым жақын болса, онда *SCANNING*тудырған ауытқушылық жағдайының деңгейі HIGH болады";
- SR_{15} = "Егер $\sim^{t_{VCA}}\ \sim^{T^e_{VCA}}$ енетін $\sim^{Y^e}$ неғұрлым жақын болса және $\sim^{t_{NVC}}\ \sim^{T^e_{NVC}}$ енетін $\sim^{VB^e}$ неғұрлым жақын болса, онда *SCANNING*тудырған ауытқушылық жағдайының деңгейі LIMITS болады".

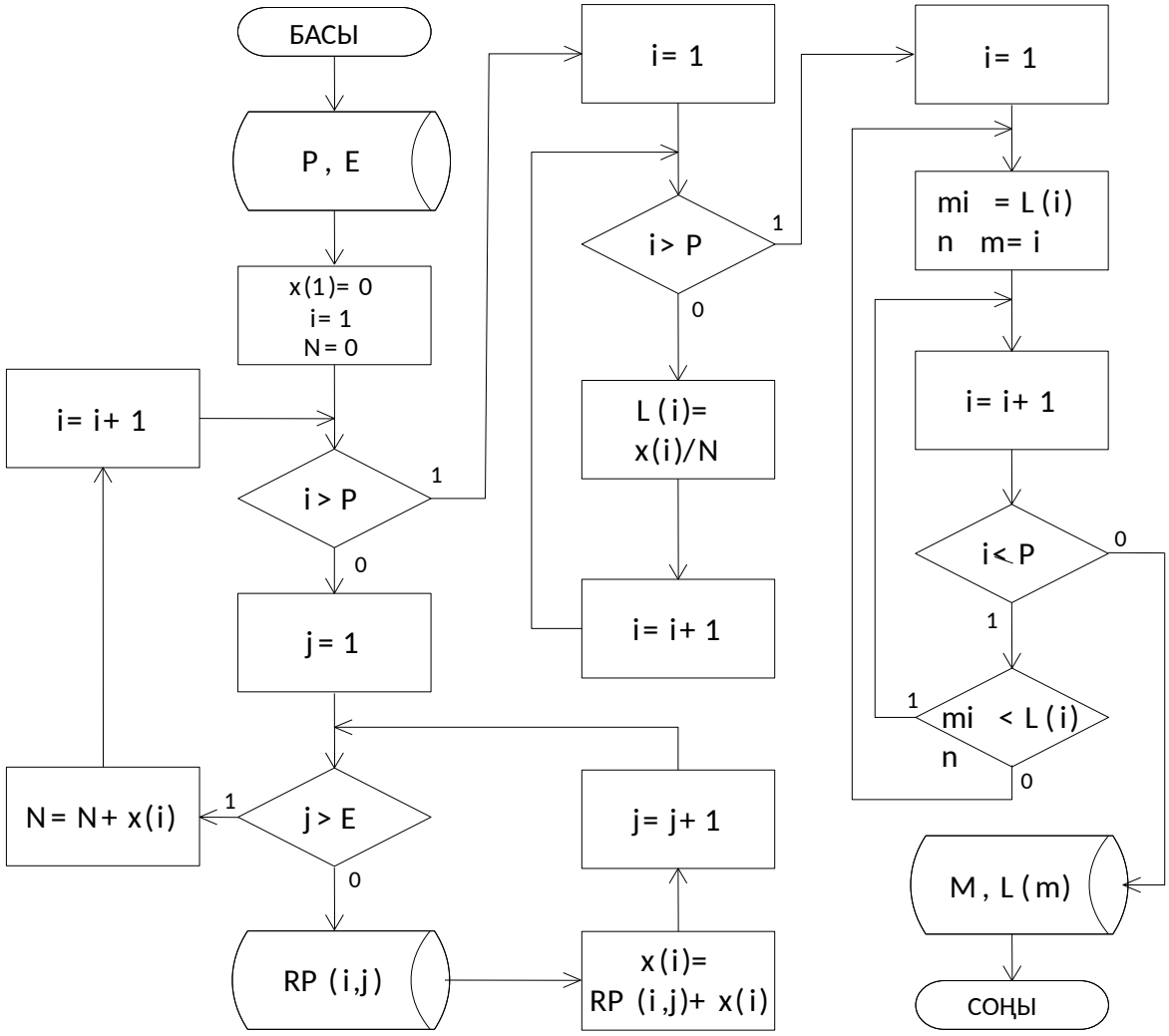
4.4 суретінде I_1=*SCANNING* айқындауға бағытталған ЛА қатысты **NVC** және **VCA** $\boldsymbol{SR_3}$ ережелер топтары үшін ауытқушылық жағдайының деңгейін сипаттайтын области (LOW, LTH, HTTL, H, LIM) анық емес тірек екі өлшемді аумақтары ұсынылған.



Сурет 4.4- *SR3*арналған анық емес тірек блоктары

4.2 Ауытқу идентификация жүйелерінің қолдану алгоритмі

2.1-2.3баптарында құрастырылған модельдер, сонымен бірге 3.2-3.4 баптарындағы ауытқушылықтарды анықтауға бағытталған жаңа құрылымдық шешімдер идентификациялау сәйкес жүйелерінің қызметін қолдайтын алгоритмдік қамтамасыздандыруды құрастыруды талап етеді(мысалы, МКАӘТ, АЕАМ, ҚФСӘ, ҚФҚӘ, ШЕ т.б. қалыптастыру әдістері). 4.5 суретінде ОД әдісінің алгоритмдік шешімі ұсынылған(1.3бабы).



Сурет 4.5- ОД әдісін жүзеге асыру алгоритмінің блок сызба нұсқасы

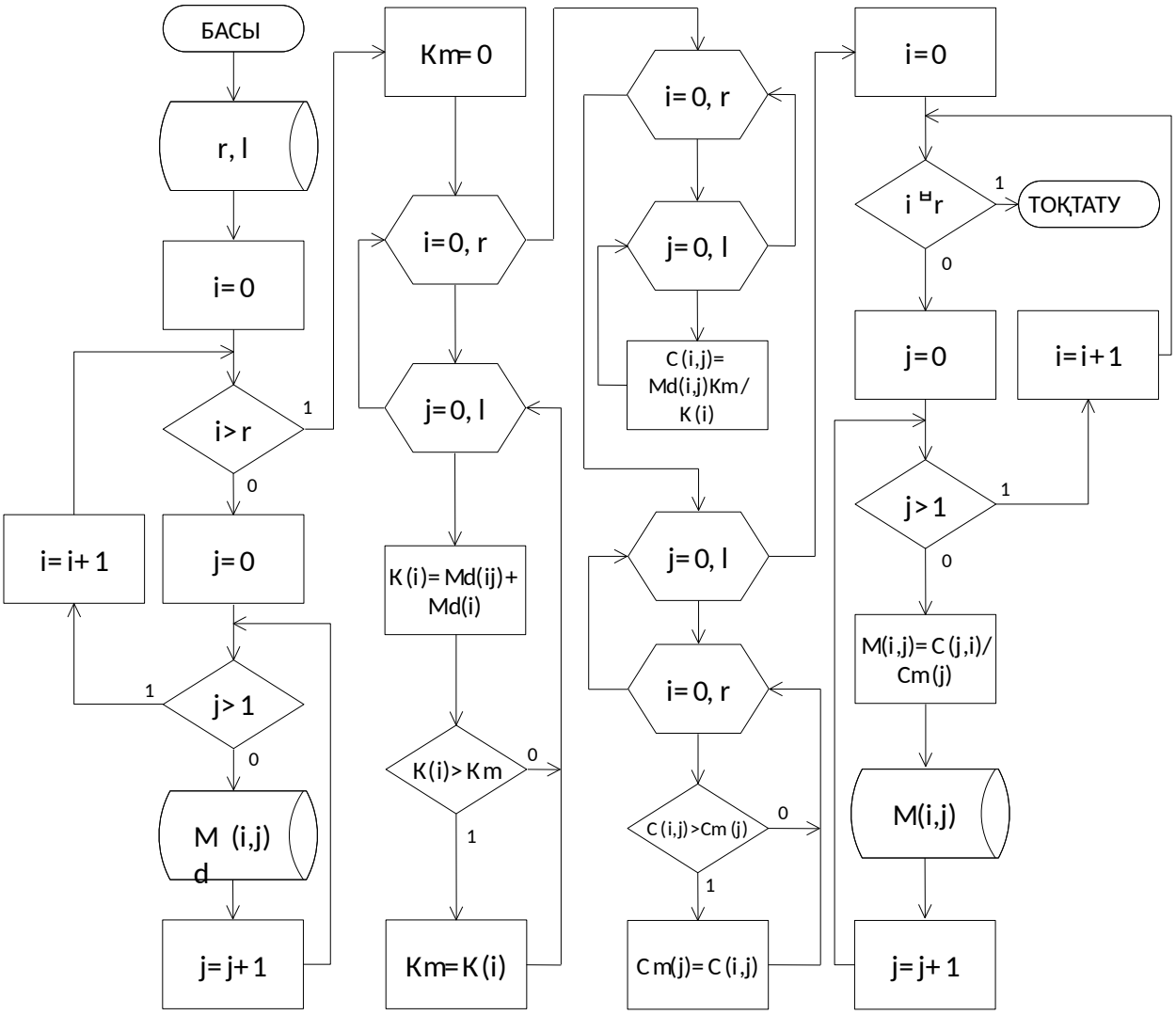
[2],ол ауытқушылық жағдайын анықтау технологиясында (3.1 бабының 6 -кезеңін қараңыз) ШЕ жиынын қалыптастыруға ең жақсы Альтернативті таңдауға бағытталған. ОД әдісіне сәйкес белгілерді енгіземіз: *x(i)*- сарапшылар тағайындаған *i* – жобасының (x_i) дәрежелері; *L(i)*-*i*- жобасының (λ_i)*МК*; *P*- сараптама объектілерінің саны; *E*- сарапшылар саны; *RP(P,E)*- *P* *E* сарапшылардың әрқайсысы белгілеген *P* жобаларының әрқайсысының дәрежелер ауқымы (2.4 бабының ОД мысалын қараңыз).

Алгоритм келесі түрде қызмет атқарады.

Көрсетілген әдіске сәйкес 2.8 кестесінде(2.4 бабын қараңыз) келтірілген әрбір *i*- жобасына сәйкес дәрежелер есептелетін сарапшының пайымын көрсететін *RP(i,j)* деректер ауқым қалыптасады.Есептеп шығарылған x_iнегізінде *L(i)* бір өлшемді ауқымында көрсетілген λ_i мәндері көрсетіледі. Соңғысынан айнымалы *M* кестеленген нөмір(2.8 кестесін)меншіктелетін шешімнің ең жақсы нұсқасын бейнелейтін *(min)* λ_i минималды мәні таңдалады.

Ұсынылған құрылымдық шешімдердің қызметін қолдау үшін ауытқушылық жағдайын анықтау технологиясында эталондарды қалыптастыру үрдісін және шамалардың фаззификациясын жүзеге асыру үшін басқа ҚФҚӘ арасында неғұрлым жиі қолданылатын ЛТСМҚ алгоритмін құрастырамыз. Оның болк-сызбанұсқасы 4.6 суретінде ұсынылған.

Осында шығыс деректері ретінде *Md(r,l)* (*r*және*l*- ЛТСМҚ әдісін жүзеге асыру үшін сарапшылар дайындаған шамалар кестесінің сәйкесінше құрамындағы интервалдар нөмірлері мен термдер санын көрсететін(2.2 бабын) айнымалылар)*Md(r,l)* ауқымы қолданылады. Әдіске сәйкес максималды *Km* (2.2 бабын)мәні таңдалатын *K(i)* көмек беру матрицасын аламыз, таңдаудан кейін матрицаның барлық элементтері (2.15) өрнегіне сәйкес *C(i,j)* элементтерін қалыптастырады және ары қарай (2.16) өрнегіне сәйкес алдын – ала есептелген *Cm(i)* және *C(i,j)* шамаларының негізінде *M(i,j)* ҚФ анықталады.

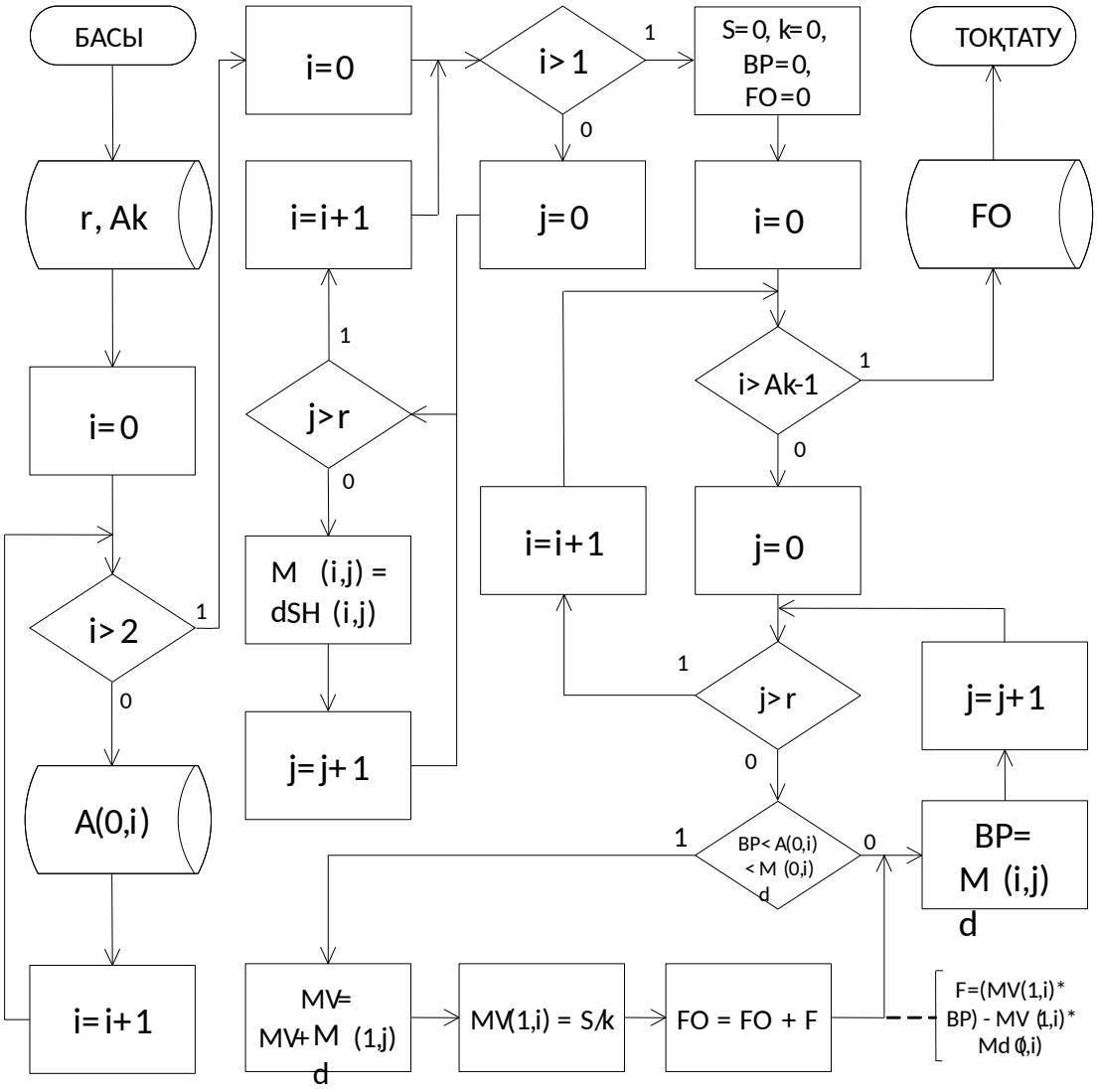


Сурет 4.6 - ЛТСМҚ жүзеге асыру алгоритмінің блок-сызбанұсқасы

Ауытқушылық жағдайын анықтау технологиясында және сәйкес жүйенің (3.6 суретін қараңыз) ЛӘ қисынды қорытынды процедурасын жүзеге асыру үшін(3.1 суретіндегі 8 - кезеңді қараңыз) ҚФСІӘ(4.7. суретін)Осында шығыс деректері ретінде берілген α-деңгейлер меншіктелетін екі өлшемді *Md(i,j)* ауқымы және*A(0,i)* ауқымының нөлдік жолы қолданылады, ал *r ((2.8*) өрнегін қараңыз)АЕС термдер санын көрсетеді.

α - мәндерін қолдана отырып *Md(i, j)* деректер ауқымының АЕС деңгейлік жиындарға бөлеміз және әрбір α-деңгейде *MV* орта мәндерін *M(V)*сәйкес есептейміз (1.2 бабының БС қараңыз. Осында *MV* айнымалысы жиынтық мәндерді есептеу үшін қолданылады.

б

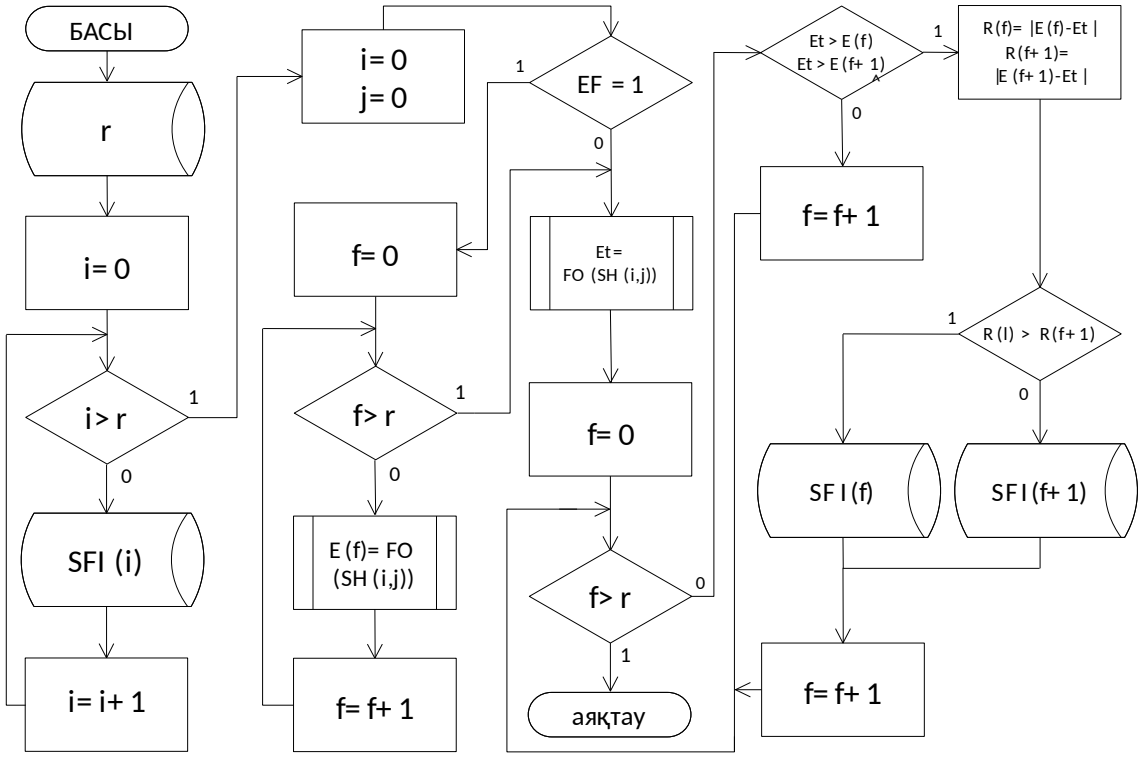


Сурет 4.7 - жүзеге асыру алгоритмінің болк-сызбанұсқасы

ал *BP* деңгей нұсқаларын бақылау үшін буферлі айнымалы болып табылады, ал *k* параметрі айнымалылар санын анықтауға жауапты болады. Алгоритм жұмысының барысында *MV(1, j)* ауқымының алғашқы жолына

сәйкесінше әрбір α-деңгейде орта мәндер меншіктеледі. Ары қарай $F(\tilde{X})$ (1.2бабының БК қараңыз) есептейміз және $FO(F(\tilde{X}))$ реттеу функциясының мәнін табамыз. Ұсынылған блок-сызбанұсқада *BP* және *Md (0, i)* айнымалылары кіріктірудің жоғарғы және төменгі шектерін анықтайды, ал *FO* соңғы нәтиже меншіктеледі.

Сканерлеуші утилиттер тудырған ауытқушылықтарды анықтаудың типтік жүйесінің құрылымдық шешімін жүзеге асыру үшін АЖСМ АЕСІЖ ПНА (4.1 суретін қараңыз) ШЕ нақты тобында алгоритм блок-сызбанұсқасын құрастырамыз.



Сурет 4.8 - ШЕ орындау алгоритмінің блок-сызбанұсқасы

Осы мақсатта $\boldsymbol{SR_3}$-*SFI(i)*анық емес идентификациясы бар ауқымды инициализация (3.1. бабының 7-кезеңін) жүзеге асырылады, ал *r* айнымалысы анық емес ережелер санын анықтайды:

- *SFI* (1)- “Ауытқушылық жағдайының деңгейі LOW”;
- *SFI* (2)- “ Ауытқушылық жағдайының деңгейі LOWER THAN HIGH”;
- *SFI* (3)- “Ауытқушылық жағдайының деңгейі HIGHER THAN THE
- LOWEST”;
- *SFI* (4)- “ Ауытқушылық жағдайының деңгейі HIGH”;
- *SFI* (5)- “ Ауытқушылық жағдайының деңгейі LIMITS”.

БС (сурет 4.7) анықтау алгоритмінің негізінде *(FE=1)*эталондарды қалыптастыру шартын орындағаннан кейін эталонды *E(f)*және ағымдағы *Et* мәні есептеп шығарылады. *EtE(f)*және *E(f+1)* салыстыру нәтижесінде қай

эталонға ағымдағы мәннің неғұрлым жақынырақ екені анықталады. Бұл әрекет *R(f)=E(f)-Et*и *R(f+1)=E(f+1)-Et* есептеуінің көмегімен жүзеге асырылады. Ары қарай келесі тексеру жүргізіледі – егер *R(f)R(f+1)* қарағанда артығырақ болса, онда *f* ережесі орындалады және *SFI(f)* жолдық мәні арқылы *FI(f)* сәйкес мәні шығарылады. Ұсынылған алгоритм негізінде сканерлеу үрдісіне тән ауытқушылық жағдайына қатысты соңғы шешім жүзеге асырылады.

4.3 Сканерлеу құралдарын анықтауда бағдарламалық жүйесіне сараптамалық зерттеу

4.1 бабында ұсынылған порттарды сканерлеу тудырған ауытқушылықтарды анықтаудың типтік жүйесін және оның құрылымдық шешімін негізге ала отырып(4.1 суретін)сәйкес бағдарламалық құралды құрастыру және сараптамалық зерттеу жүргіземіз.

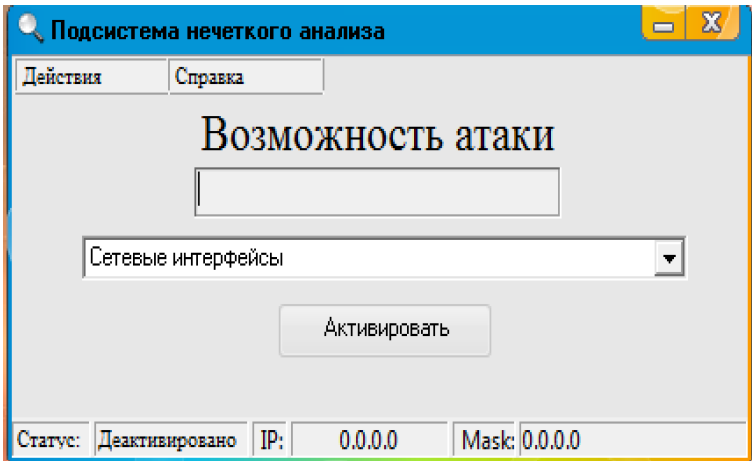
Құрылған алгоритмдерді(4.2 бабын)есепке ала отырып негізгі код (Б қосымшасын қараңыз) және төменде берілген сипаттамалары бар кез келген дербес компьютерде қолдануға болатын бағдарламалық модуль құрылды: процессор жылдамдығы – 1,2 ГГц;

- оперативті жадының көлемі – 512 Мб;
- қатты дАСк – 10 Гб;
- операциялық жүйе – Microsoft Windows.

Бағдарламаны іске қосу үшін **NAnalize.exe** атқару файлы қолданылады, ол үшін алдын-ала 2003 нұсқасынан төмен емес Microsoft Access бағдарламалық қамсыздандыру орнату қажет.

Сканерлеуші құралдарды анықтаудың бағдарламалық жүйесінің негізгі терезесінің(4.9 сурет) құрамына үш негізгі элемент енеді:

- бас мәзір;
- басқару және нәтижелерді бейнелеу панелі;
- бағдарламалық жүйенің ахаулы панелі.



Сурет 4.9 - Бағдарламалық жүйенің негізгі терезесі

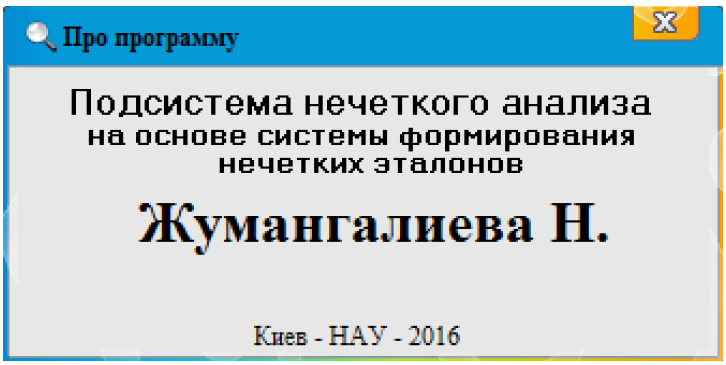
Бас мәзір құрамына екі тармақ кіреді:

- “Әрекеттер” (“Анық емес эталондар”, “Шығу”);
- “Анықтама” (“Бағдарлама туралы”).
- Нәтижелерді бейнелеу және басқару панелінің құрамына кіреді:
- Шабуылдар мүмкіндігін бейнелеу аймағы;
- Жүйедегі қолжетімді тізімнің желілік интерфейсін таңдау элементі;
- Кнопка “Белсендендіру” (“Тоқтату”).

Бағдарламалық жүйенің ахуал панелінің құрамына енеді:

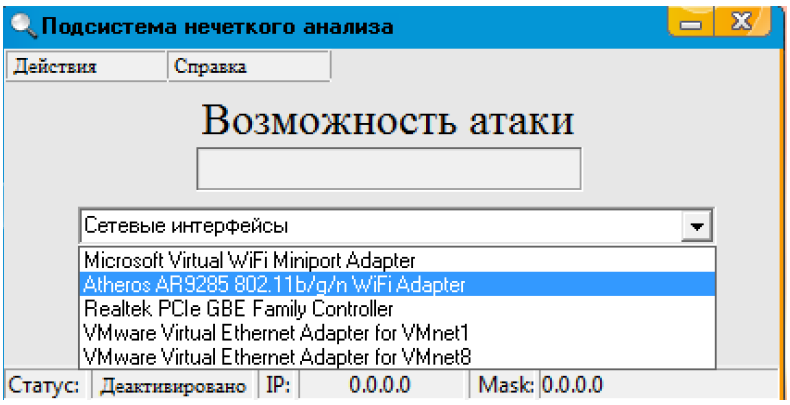
- трафик сараптамасының ахуалын бейнелеу элементі (“Белсенді”, “Белсенді емес”);
- таңдалған желілік интерфейстің бетпердесі мен IP- мекенжайды бейнелеу элементтері.

“Бағдарлама туралы ” терезесін қарау үшін (4.10 сурет) “Анықтама”–“Бағдарлама туралы” батырмаларын басу қажет.

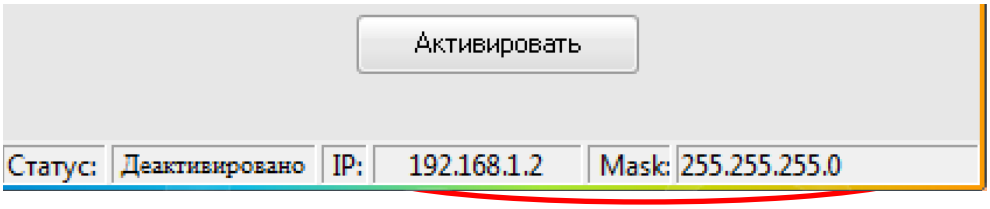


Сурет 4.10 - “Бағдарлама туралы” терезесі

Бағдарламаны іске қосқаннан кейін тізімнен қажет қолжетімді желілік интерфейсті таңдаған жөн. (4.11сурет). Бағдарламалық жүйенің ахуал панелінде интерфейстің желілік параметрлері бейнеленеді (4.12 сурет).

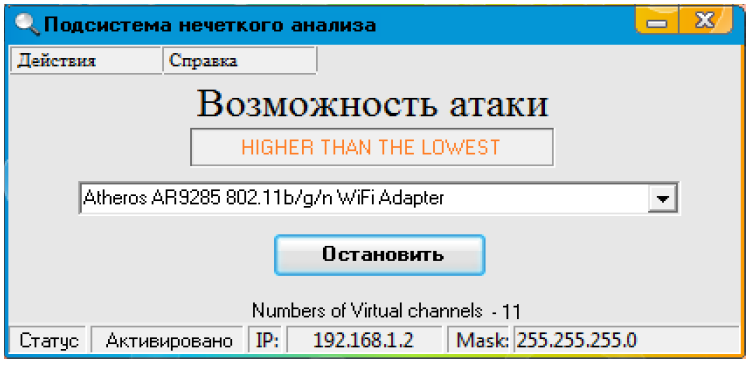


Сурет 4.11 - Қолжетімді желілік интерфейстер тізімі



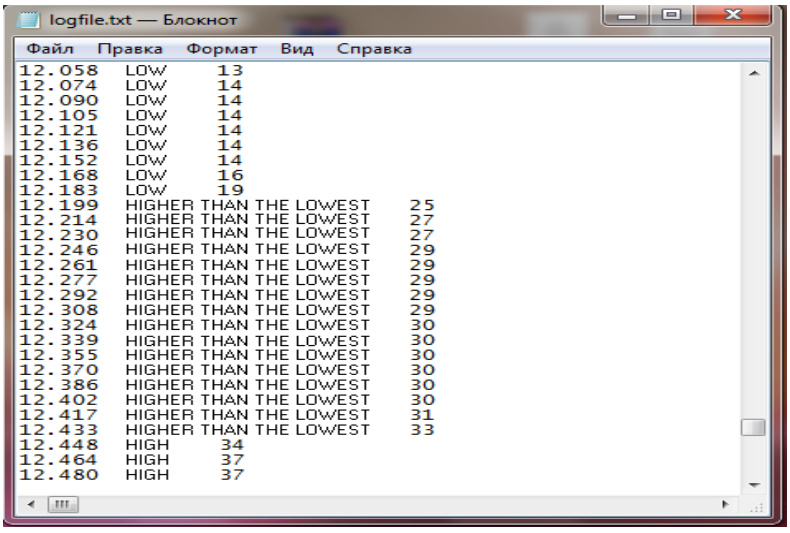
Сурет 4.12 - Ауытқу панелі

Бағдарламалық жүйенің жұмысын бастау үшін “Белсендендіру” батырмасын басу қажет. Осыған сәйкес бағдарламаның ахуалы, статус программы “Белсенді” болып өзгереді, ал жүйені сканерлеу мүмкіндігі туралы ақпарат $FI(1, r_1)$ ($r_1 = \overline{1,5}$) арқылы арнайы аймақта бейнеленеді(4.13 сурет).



Сурет 4.13 - Сканерлеу туралы ақпарат

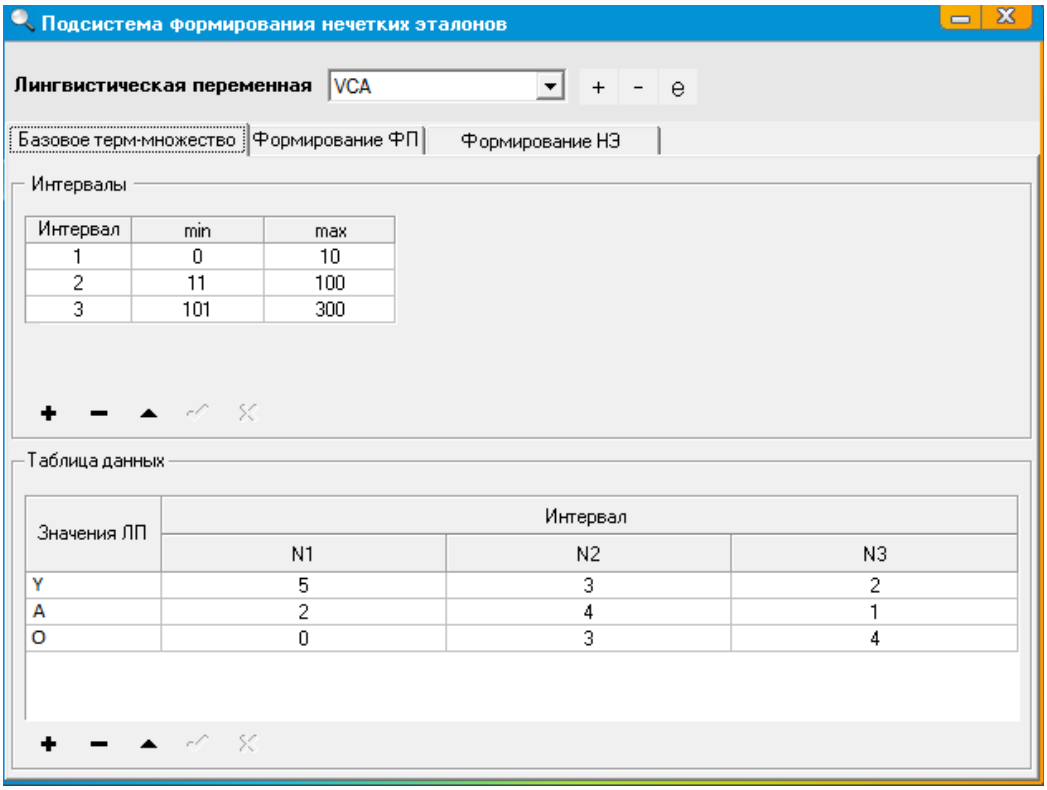
Бағдарламаны аяқтау үшін “Тоқтату” батырмасын басқан жөн және бағдарламаның сәйкесінше “Белсенді емес” болып өзгереді. Бағдарламалық жүйенің жұмыс нәтижесін лог-файлдан көруге болады. (4.14 сурет).



Сурет 4.14 -Лог-файлдың үзіндісі

T^e_{NVC} мен T^e_{VCA} қалыптастыру, түзету және қарау үшін ЭҚІЖ (4.1 сурет) “Әрекеттер”–“Анық емес эталондар” батырмасын басу арқылы

белсендендіру қажет ішкі жүйенің және экранда сәйкес ішкі жүйенің терезесі көрінеді (4.1 сурет).

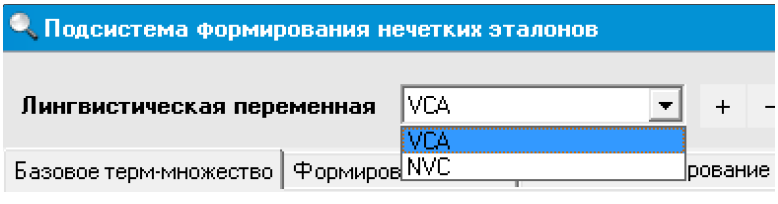


Сурет 4.15 -ЭҚІЖ терезесі

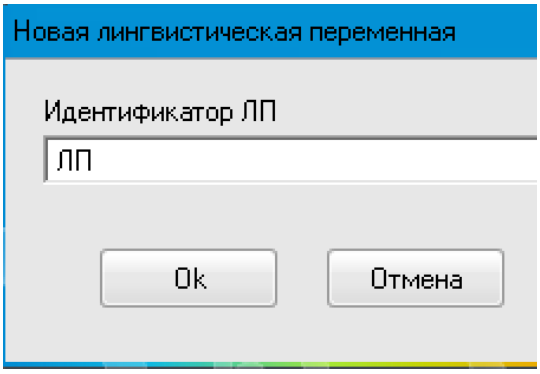
Бұл терезеде қосу,өшіру және ЛА атын өзгерту батырмалары бар **NVC**және**VCA**(4.16 а сурет) ЛА басқару панелі орналасқан. Бұл режим “+” (4.16 б сурет)батырмасы арқылы инициализацияланады. Егер жаңа ЛА құру қажет болса, онда оны басқаннан кейін “Жаңа лингвистикалық айнымалы” терезесі пайда болады,оған ЛА атауы енгізіледі және “Ok” (4.16 в сурет) батырмасын басу арқылы растау жүзеге асырылады.

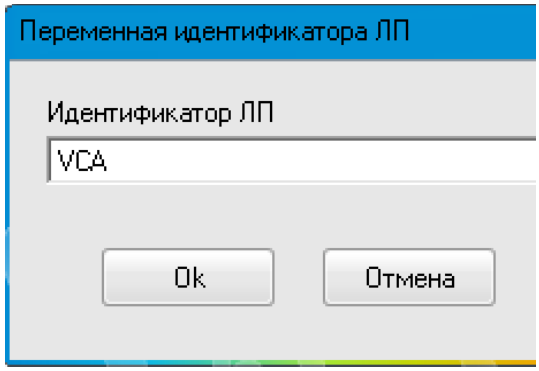
“Лингвистикалық айнымалы” тізімі арқылы онымен жұмыс істеуге ЛА таңдау мүмкіндігін берсе(4.16а сурет) оны өшіру “–” (4.16 а сурет) батырмасы арқылы орындалады. ЛА атауын өзгерту үшін “e” (4.16 а сурет) батырмасы қолданылады “Лингвистикалық айнымалының идентификациясын өзгерту ” (4.16 г сурет).редакциялау терезесі ашылады.

а) ЛА басқару панелі



б)ЛА тізімі

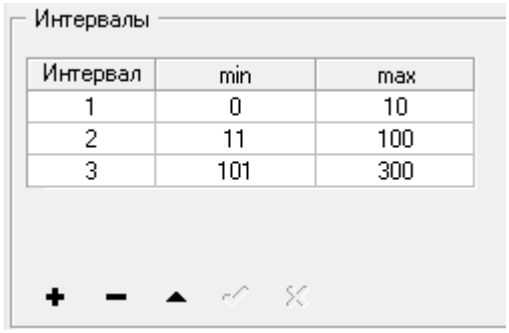




в) ЛА атау беру г) ЛА атауын түзету

Сурет 4.16 -ЛА эталондарын қалыптастыруды қолдау панелі

ЛА атауын құру аяқталғанда ЛА эталондарын құрауда қолданылатын $N_{11}^{i}\,(i=\overline{1,5})$ и $N_{12}^{j}\,(j=\overline{1,3})$ интервалы қалыптасады(4.17 сурет).



Сурет 4.17- N_{11}^{i} және N_{12}^{j} қалыптастыру панелі

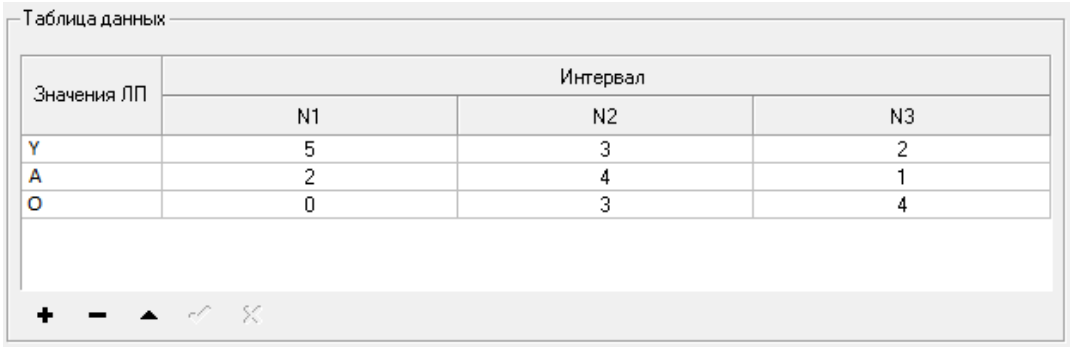
Бұл панелдегі интервалдарды анықтау үшін кестелердің төменгі тұсында орналасқан батырмалар түріндегі аспаптар қолданылады (4.17 сурет):

- жазба қосу;
- жазбаны өшіру;
- жазбаны редакциялау;
- жазбаны сақтау;
- енгізген мәндерді болдырмау.

- Жазбаларды құру “+” батырмасы арқылы жүзеге асырылады, инициализациядан кейін берілген өрісте бастапқы деректерді енгізу орындалады, одан кейін олар “√”батырмасының көмегімен сақталады,ал “X” батырмасы арқылы әрекетті болдырмайды.

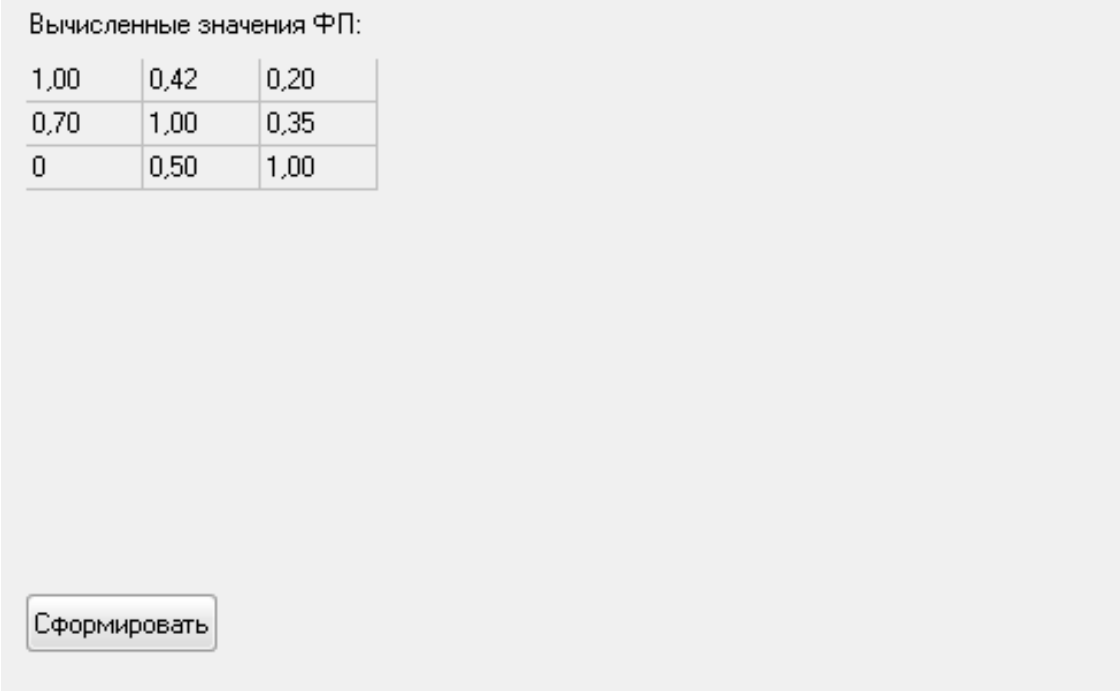
Жазбаны өшіру “–” батырмасы арқылы, ал редакциялау –“▲”батырмасының көмегімен орындалады.Қажет интервалды құру аяқталғанда автоматты “Интервал”өрісі қосылады. “Деректер кестесі” терезесінің төменгі тұсында орналасқан деректер кестесін

инициализациялау атаулары енгізілетін ЛА санын құруды талап етеді(4.18 сурет).



Сурет 4.18 -Деректер кестесі

Құрылған қосымшаның қалыпты жұмысын қамтамасыз ету үшін қажет деректерді толық анықтау және кестеге енгізу қажет. Бұл үрдіс аяқталғаннан кейін құрылған алгоритм негізінде.(4.6 суретті қараңыз "Анық емес эталондарды қалыптастырудың ішкі жүйесі" негізгі терезесінде "Қалыптастыру" батырмасын басқаннан кейін "ҚФ қалыптастыру " қосымша бетінде T^e_{NVC} мен T^e_{VCA} қалыптастыру процедурасы жүктеледі. Есептеуден алынған ҚФ мәндері кестеде бейнеленеді(4.19 сурет).

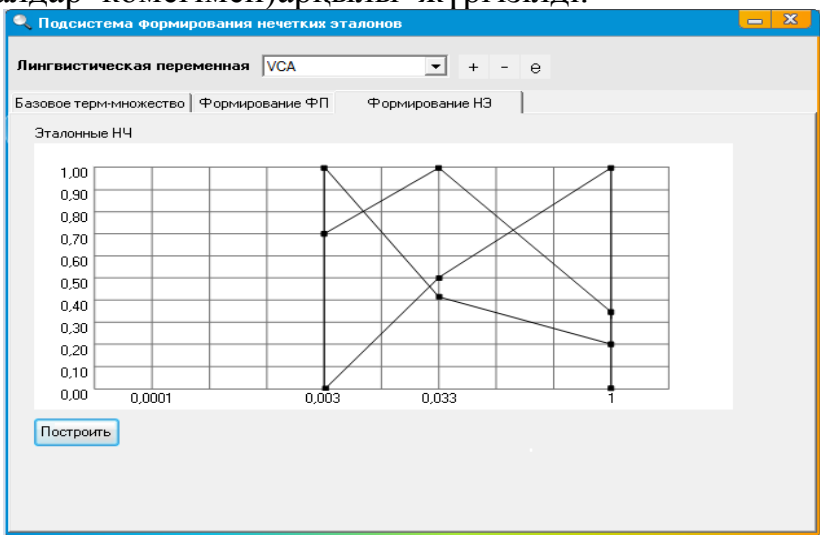


Сурет 4.19 - Қалыптасқан T^e_{NVC} мен T^e_{VCA}

Барлық T^e_{NVC} мен T^e_{VCA} қалыптасады және "Анық емес эталондарды қалыптастыру"қосымша бетінде "Құру"батырмасын басу арқылы сәйкес

базаға енгізіледі, ал олардың графикалық бейнесін “Анық емес эталондарды қалыптастыру” қосымша бетінің көмегімен алуға болады. (4.20 сурет).

Жүйені зерттеу Ұлттық авиациялық университеттің ақпараттық технологиялар қауіпсіздігі кафедрасының жұмыс бекеттеріне порттардың берілген мекенжайларына КлВ=1500 көлемінде шабуылдарды модельдеу ((СкС) XSPider 7.5 Demo Build 1070 (XSP) және Essential NetTools 4.3 Build 266 (ENT) в стандартты (СтР) және жасырын (ЖР) режимдерде сканерлеуші құралдар көмегімен)арқылы жүргізілді.



Сурет 4.20 - T^{e}_{VCA} бейнелеу панелі

4.3 кестесінен көрінетіндей 29,3 % жағдайда $\tilde{t}_{VCA}$ мен $\tilde{t}_{NVC}$ мәні $\tilde{Y}^{e}$ және $\tilde{VS}^{e}$ неғұрлым жақын орналасқан, 38,7 %-$\tilde{Y}^{e}$ мен $\tilde{B}^{e}$,ал 32 %-сәйкесінше $\tilde{Y}^{e}$ мен $\tilde{A}^{e}$ жақын орналасқан.

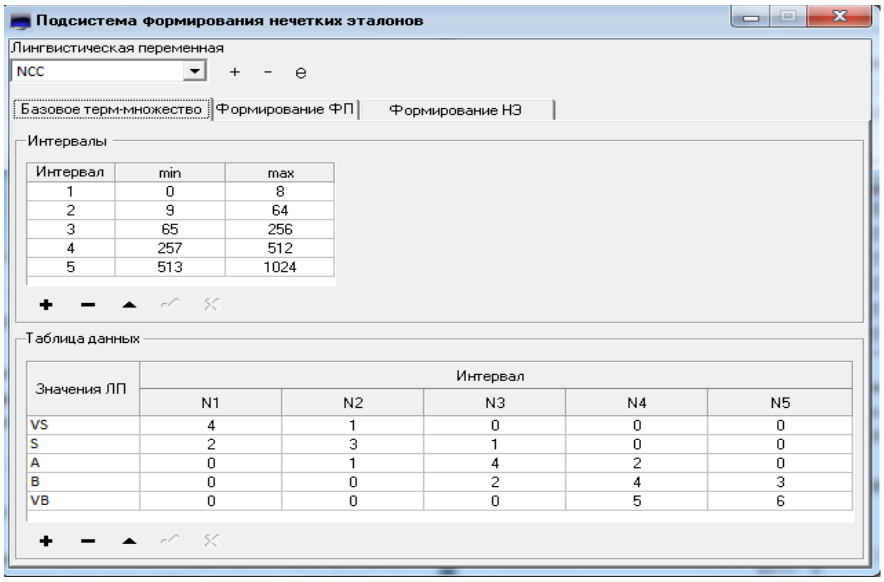
ЖР анықтаудың бағдарламалық жүйелерін сараптамалық зерттеу нәтижелері				
ЖР	АдП	КлВ	LF	SR
XSP	-	250	LIM	SR_{15}
ENT (СтР)	Стандарты	90	LIM	SR_{15}
ENT (СтР)	(10 ÷ 32) (38 ÷ 60)	100	LIM	SR_{15}
ENT (СкР)	(200 ÷ 212) (310 ÷ 328)	230	H	SR_{15}
ENT (СтР)	(400 ÷ 406) (420 ÷ 426)	170	H	SR_{15}
ENT (СкР)	(325 ÷ 335) (355 ÷ 365)	180	H	SR_{15}
ENT (СтР)	(853 ÷ 859) (880 ÷ 886)	260	HTTL	SR_{15}
ENT (СкР)	(1025 ÷ 1027) (1128 ÷ 1130)	220	HTTL	SR_{15}

Кесте 4.3 - ЖР анықтаудың бағдарламалық жүйелерін сараптамалық зерттеу нәтижелері

Осымен бірге шабуылдарды анықтау 29,3 % жағдайда SR_{15} = “Егер $\tilde{t}_{VCA}$ $\tilde{T}^{e}_{VCA}$ енетін $\tilde{Y}^{e}$ неғұрлым жақын болса және $\tilde{t}_{NVC}$ $\tilde{T}^{e}_{NVC}$ енетін $\tilde{VB}^{e}$ неғұрлым жақын болса, онда *SN* тудырған ауытқушылық жағдайының деңгейі LIM болады”ережесін ал 38,7 %және 32 % сәйкесінше SR_{14}және SR_{13} ережелерін бастамашылыққа алатынын атап өткен жөн. Жүргізілген верификация нәтижелерінен барлық шабуылдар сарапшының түрлі сенім дәрежесін көрсететін түрлі ережелер арқылы анықталғаны көрінеді. Осыған сәйкес ұсынылған моделдер мен жүйелерді жүзеге асыру модельденетін әрекеттерге реакция бейнелейтіні туралы қорытынды жасауға болады.

4.4 Сараптамалық қолданбалы жүйе шабуылдардың іс-әрекеттінен туындайтын ауытқуларды анықтау

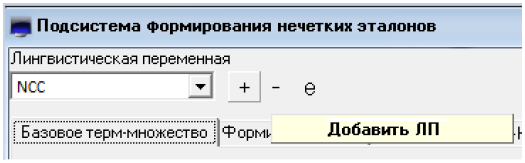
Ұсынылған құрылымдық шешімдер мен құрылған алгоритмдер негізінде (3.2-3.4бап) шабуылдаушы әрекеттер туындатқан ауытқушылықтарды анықтауға арналған қолданбалы бағдарламалық жүйе (Б қосымшасын қараңыз). Ол қажет шамалар жиынын қолдануын кеңейту арқылы өз мүмкіндіктерін арттырады, осы шамалардың ағымдағы мәндері бойынша ауытқушылық жағдайын анықтауды жүзеге асыруға және эталондарды құруға мүмкіндік береді. Берілген жұмыста АЕЭҚІЖ (3.2 суретін қараңыз) ұсынылған құрылымдық шеімі арқылы ЛА эталондары анықталатын бағдарламалық ішкі жүйе құрылды. Осы мақсатта мысалы, құруға қажет $T^{ef}_{33} = T^{ef}_{NVC}(f = \overline{1,5})$, т.е. $T^{e}_{NVC} = \{\tilde{T}^{e1}_{NVC}, \tilde{T}^{e2}_{NVC}, \ldots, \tilde{T}^{e5}_{NVC}\} = \{\tilde{VS}^{e}, \tilde{S}^{e}, \tilde{A}^{e}, \tilde{B}^{e}, \tilde{VB}^{e}\}$ деректер бейнеленген диалогті терезе (4.21 суретін) қолданылады.



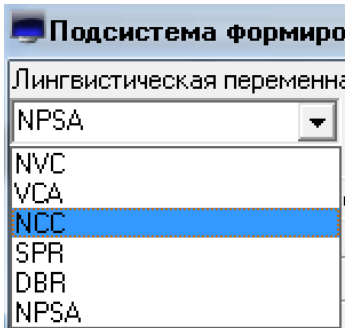
Сурет 4.21- АЕЭҚІЖ диалогті терезесі

ЛА қажет жиынын құру(4.22 а суретті қараңыз), оларды өшіру(соған қатысты деректерімен бірге)және инициализациялау редакциялау(4.22в суреті) “+”, “–” және сәйкесінше “е” батырмалары арқылы орындалады.

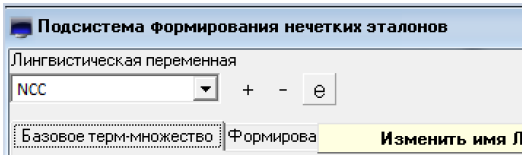
Кезекті айнымалы эталондар есептелетін қажет жиын түзілетін жүйе тізіміне түседі. “лингвистикалық айнымалы ” тізімінің негізінде ары қарай қолдану мақсатында оларды таңдау жүзеге асырылады(4.22б сурет).Эталонды мәндерді құруға қажет интервалдардың бағдарламалық ішкі жүйесінде кестелер және саймандар панелінде кестеге жаңа жазбалар енгізуге, шығыс деректерін енгізуге, оларды сақтауға, қате ақпаратты болдырмауға, жазбаларды өшіруге және оларды редакциялауға кестелер (4.22 г сурет) қолданылады. Қажет қосымша интервалды құру сәйкес кестені саймандар панелінің көмегімен “Мәліметтер кестесі” (4.23 сурет) терезесінің төменгі тұсында көмегімен редакциялау арқылы жүзеге асырылады.



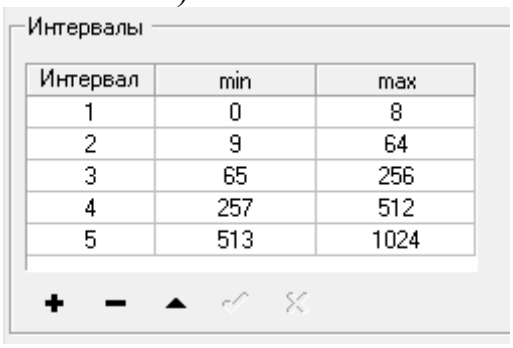
а) ЛА құру батырмасы



б)ЛА тізімі



в) Редакциялау батырмасы



г) Интервалдар кестесінің терезесі

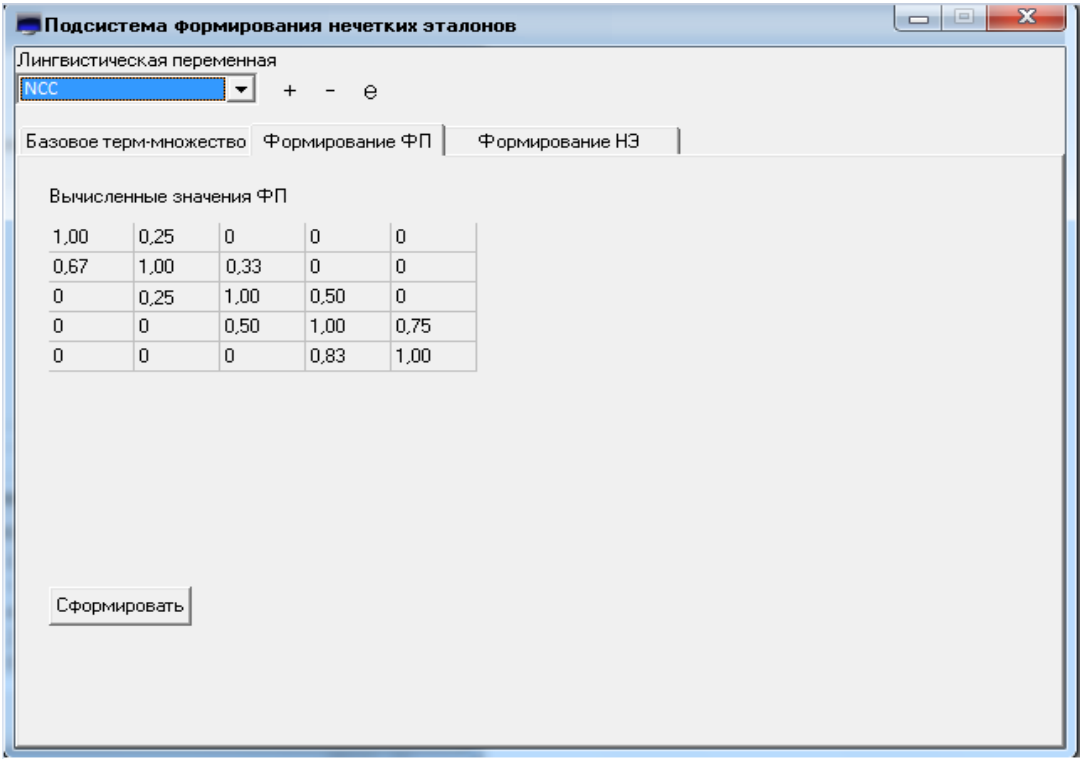
Сурет 4.22-АЕЭҚІЖ диалогті терезелері

Таблица данных

Значения ЛП	Интервал				
	N1	N2	N3	N4	N5
VS	4	1	0	0	0
S	2	3	1	0	0
A	0	1	4	2	0
B	0	0	2	4	3
VB	0	0	0	5	6

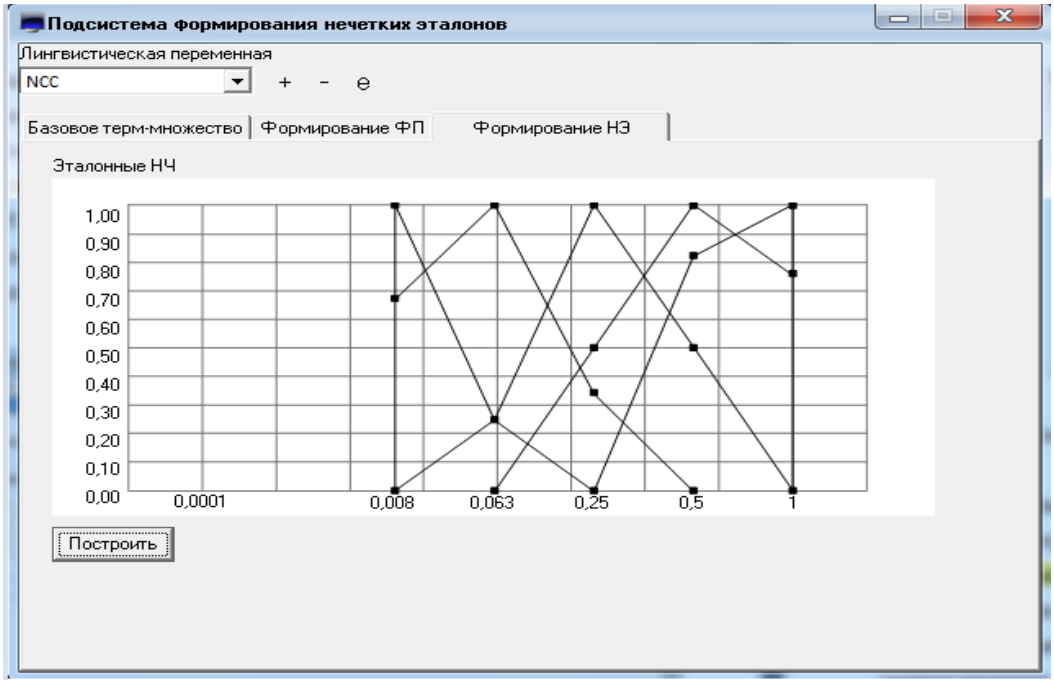
Сурет 4.23- Мәліметтер кестесі

Барлық алынған эталонды сандар жеңіл идентификациялауды(2.2 бабында көрсетілген есептеулерге сәйкес 4.24 суретіндегі деректерді қараңыз) және “Анық емес эталондарды қалыптастыру ”қосымша бетіндегі “Құру” батырмасын басу арқылы сәйкес мәліметтер қорына енгізіледі.



а) ҚФ қалыптастыру

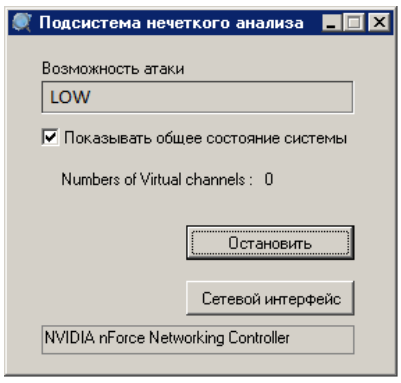
Сурет 4.24 -АЕЭҚІЖ негізгі терезесі, бет 1



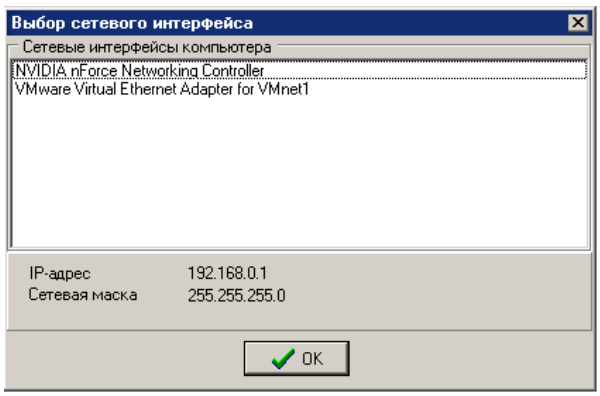
б) Эталонды АЕС графикалық кескіндемесі

Сурет 4.24, бет 2

Эталондарды қалыптастыру аяқталғанда жүйе, мысалы сканерлеуді анықтау режимінде (Б қосымшасын қараңыз) “Желілік интерфейсті таңдау ” (4.25 б сурет) сәйкес терезесінен таңдалған желілік интерфейс негізінде қоршаған орта шамаларының сараптамасын орындайтын АЕСІЖ(4.25а сурет) арқылы шамалардың ағымдағы мәндері бойынша ауытқушылықтарды анықтау режимінде қызмет атқара алады.



а) Негізгі терезе



б) Желілік интерфейсті таңдау терезесі

Сурет 4.25- АЕСІЖ диалогті терезесі

Ауытқушылық жағдайын сараптау “Белсендендіру” батырмасын басу арқылы , ал оны болдырмау “Тоқтату” батырмасы арқылы жүзеге асырылады. Сараптама нәтижесі шабуылдармүмкіндіктерін “LOW”, “LOWER THAN HIGH”, “HIGHER THAN THE LOWEST”, “HIGH” және “LIMITS”

мәндерінің бірі арқылы сипатталатын FI_{35} ($i=\overline{1,n}$, $j=\overline{1,r_n}$) көмегімен сәйкес өрісте (4.25а сурет) бейнеленеді.

Жүйенің жұмысын суреттейтін мысалдарды қарастырайық, ол үшін 5 кезеңдегі компьютерлік желілерде кибершабуылдар туындатқан ауытқушылықтарды анықтау(3.1 бабын)әдісіне сәйкес қажет $\underset{\sim}{t}_{NCC}$, $\underset{\sim}{t}_{NPSA}$, $\underset{\sim}{t}_{SPR}$ және $\underset{\sim}{t}_{DBR}$ мәндерін қалыптастырамыз. $\underset{\sim}{t}_{NCC}$ алу 1024 тең NCC максималды мәнінде 2.2 бабында көрсетілген веб-сервер кескіндемесін қолдануға негізделген (Apache веб-серверінің баптамаларына сәйкес).

Тәжірибе кезінде веб-сервер негізгі болыпт табылатындықтан, оған қосылулар 80/tcp порты арқылы жүзеге асырылады.Бұл утилитінің параметрлері арқылы бір секундтағы дАСкреттеу интервалы *t=60* с мерзіміндегі қосылулар саны тұрақтандырылған кестесін қараңыз).

$\underset{\sim}{t}_{NPSA}$ алуда Iptables түрлендірілген ақпараты қолданылды, ал значения $\underset{\sim}{t}_{SPR}$ арналған мәндер веб-серверінің логын сараптау көмегімен алынған уақыт бірлігіндегі барлық сұраныстар санын есептеу арқылы қалыптасты.

$\underset{\sim}{t}_{DBR}$ қалыптастыруда қосылудың әркімге бірегей IP мекенжайына ағым құруға негізделген өлшем әдістемесі қолданылды. Клиенттен алынған уақыт бірлігіндегі белгілі түрдегі сұраныстар(бұл жағдайда GET-сұраныстар) санын есептеу және жүйелі сұраныстар арасындағы орташа уақытты анықтау арқылы бақылау жүзеге асырылады. 4.4 кестесінен 30 секундтан кейін басып кірудің басталуын айғақтайтын қосылулардың көп мөлшерінде кідірістің азаюы байқалады. *t=60* с уақытындағы өлшем нәтижелері 4.4 кестесінде бейгнеленген.

Кесте 4.4 - $\underset{\sim}{t}_{NCC}$, $\underset{\sim}{t}_{NPSA}$, $\underset{\sim}{t}_{SPR}$ және $\underset{\sim}{t}_{DBR}$ ағымдағы мәндерін қалыптастыруға арналған NCC, NPSA, SPR және DBR модельленген мәндері

t_i *c*	NCC	NPSA	SPR	DBR
1	2	3	4	5
1; 31	17; 234	82; 536	87; 79	154; 80
2; 32	19; 234	89; 512	80; 95	203; 74
3; 33	30; 180	95; 562	86; 91	217; 72

4.4 - кестенің жалғасы

1	2	3	4	5

4; 34	102; 266	92; 559	101; 89	183; 92
5; 35	70; 195	96; 541	82; 92	146; 128
6; 36	258; 193	88; 519	86; 89	151; 93
7; 37	225; 208	86; 559	95; 86	142; 86
8; 38	294; 279	81; 527	99; 99	149; 94
9; 39	181; 283	99; 549	86; 86	191; 89
10; 40	205; 161	88; 514	100; 98	163; 41
11; 41	170; 161	99; 541	85; 95	150; 51
12; 42	253; 81	85; 360	85; 87	215; 35
13; 43	281; 74	524; 357	79; 100	185; 39
14; 44	164; 41	539; 357	81; 59	148; 38
15; 45	208; 51	543; 350	85; 54	145; 46
16; 46	247; 158	518; 365	82; 51	141; 90
17; 47	125; 26	542; 359	87; 65	163; 40
18; 48	266; 235	551; 344	100; 51	168; 60
19; 49	273; 198	540; 345	87; 64	137; 38
20; 50	285; 178	541; 367	84; 55	147; 82
21; 51	230; 167	554; 345	94; 51	123; 54
22; 52	141; 114	540; 345	92; 51	139; 33
23; 53	79; 253	537; 363	84; 68	160; 44
24; 54	205; 276	554; 346	86; 69	143; 57
25; 55	113; 160	543; 347	80; 61	171; 39
26; 56	175; 289	532; 358	90; 55	82; 51
27; 57	144; 163	564; 367	84; 57	94; 60
28; 58	168; 174	511; 367	94; 55	127; 28
29; 59	169; 174	563; 356	87; 67	69; 56
30; 60	288; 174	539; 540	86; 48	103; 33

Ары қарай сәйкес эталонды ЛА T^{e}_{NCC}, T^{e}_{NPSA}, T^{e}_{SPR} и T^{e}_{DBR} қолдана отырып $\underset{\sim}{t}_{NCC}$, $\underset{\sim}{t}_{NPSA}$, $\underset{\sim}{t}_{SPR}$ және $\underset{\sim}{t}_{DBR}$ ағымдағы мәндерін қалыптастыру үшін көрсетілген уақытта *t*NCC, NPSA, SPR және DBR мәндерінің f_{ij} ($i=\overline{2,3}$, $j=\overline{3,6}$) кездесу жиілігінің есебі жүзеге асырылады (4.5 кесте).

Кесте 4.5 - NCC, NPSA, SPR және DBR мәндерінің кездесу жиілігі

NCC, NPSA, SPR және DBR мәндерінің кездесу жиілігі

Жиілік	Эталонды термдер													
	T^{e}_{NCC}					T^{e}_{NPSA}			T^{e}_{SPR}			T^{e}_{DBR}		
	$\underset{\sim}{VS}^{e}$	$\underset{\sim}{S}^{e}$	$\underset{\sim}{A}^{e}$	$\underset{\sim}{B}^{e}$	$\underset{\sim}{VB}^{e}$	$\underset{\sim}{S}^{e}$	$\underset{\sim}{A}^{e}$	$\underset{\sim}{B}^{e}$	$\underset{\sim}{L}^{e}$	$\underset{\sim}{A}^{e}$	$\underset{\sim}{H}^{e}$	$\underset{\sim}{S}^{e}$	$\underset{\sim}{A}^{e}$	$\underset{\sim}{B}^{e}$
f_{ij}	0	6	42	12	0	0	12	48	0	60	0	0	32	28

Көрсетілген айнымалыларға арналған ағымдағы мәндер екі кезеңде түзіледі, оның алғашқысында эталонды АЕС алдын ала түзету кездесу

жиілігін көрсетілген уақыт интервалына көбейту арқылы жүзеге асырылады(4.5 кестесін қараңыз),ал екінші кезеңде сәйкес түзетілген эталонды АЕС қосу арқылы қосу жүзеге асырылады. **NCC** ЛА қажет шамаларды қалыптастыру мысалы арқылы есептеулер жүргіземіз.

1-мысал. $\tilde{t}_{NCC}$ арналған есептеулер жүргіземіз.

1-кезең. $\tilde{t}_{NCC}$ енетін эталонды АЕС кездесу жиілігіне көбейту:

$\tilde{VS}^{e'} = \tilde{VS}^{e} \cdot 0$ *={0/0,008; 1/0,008; 0,25/0,063; 0/0,25}* $\cdot 0$ *={0/0; 1/0; 0,25/0; 0/0};*

$\tilde{S}^{e'} = \tilde{S}^{e} \cdot 6$ *={0/0,008; 0,67/0,008; 1/0,063; 0,33/0,25; 0/0,5}* $\cdot 6$ *={0/0,048; 0,67/0,048; 1/0,378; 0,33/1,5; 0/3};*

$\tilde{A}^{e'} = \tilde{A}^{e} \cdot 42$ *={0/0,008; 0,25/0,063; 1/0,25; 0,5 /0,5; 0/1}* $\cdot 42$ *={0/0,336; 0,25/ 2,646; 1/10,5; 0,5/21; 0/42};*

$\tilde{B}^{e'} = \tilde{B}^{e} \cdot 12$ *={0/0,063; 0,5/0,25; 1/0,5; 0,75/1; 0/1}* $\cdot 12$ *={0/0,756; 0,5/3; 1/6; 0,75/12; 0/12};*

$\tilde{VB}^{e'} = \tilde{VB}^{e} \cdot 0$ *={0/0,25; 0,83/0,5; 1/1; 0/1}* $\cdot 0$ *={0/0; 0,83/0; 1/0; 0/0}.*

2 - Түзетілген эталонды АЕС $\tilde{t}_{NCC}$ алу үшін жалпы санын шығару. Бұл кезеңді жүзеге асыру ЛАЛМ (1.2 бабын қараңыз) әдісіне негізделеді, өйткені ол осы кластағы АЕС өңдеуге ыңғайлы, үнемді және қалыптасатын деректердің физикалық болмысын неғұрлым анық бейнелейді. $\tilde{VS}^{e'}$ және $\tilde{VB}^{e'}$ барлық тасымалдаушылары нөлдік мәндері бар болса, онда $\tilde{t}'_{NCC} = \tilde{S}^{e'} \tilde{+} \tilde{A}^{e'}$

={0/0,384; 0/2,694; 0/10,548; 0/21,048; 0/42,048;
0/0,384; 0,25/2,694; 0,67/10,548; 0,5/21,048; 0,67/42,048;
0/0,714; 0,25/3,024; 1/10,878; 0,5/21,378; 0/42,378;
0/1,836; 0,25/4,146; 0,33/12; 0,33/22,5; 0/43,5;
0/3,336; 0/5,646; 0/13,5; 0/24; 0/45;}=
{0/2,694; 0,25/2,694; 1/10,878; 0,67/42,048; 0/42,048;}, а

$\tilde{t}_{NCC} = \tilde{t}'_{NCC} \tilde{+} \tilde{B}^{e'}$ *={0/3,45; 0/5,694; 0/8,694; 0/14, 694; 0/14,694;*
0/3,45; 0,25/5,694; 0,25/8,694; 0,25/14, 694; 0/14,694;
0/11,636; 0,5/13,878; 1/16,878; 0,75/22,878; 0/22,878;
0/42,804; 0,5/45,048; 0,67/48,048; 0,67/54,048; 0/54,048;

0/42,804; 0/45,048; 0/48,048; 0/54,048; 0/54,048;}=
{0/5,694; 0,25/5,694; 1/16,878; 0,67/54,048; 0/54,048;}/60=
{0/0,095; 0,25/0,095; 1/0,28; 0,67/0,9; 0/0,9;}.

2 -мысал. Алдыңғы мысалға ұқсас тәсілмен $\underset{\sim}{t}_{NPSA}$ үшін есептеулер жүргіземіз.

1-кезең. в T^{e}_{NPSA} енетін эталонды АЕС кездесу жиілігіне көбейту:

$\underset{\sim}{S}^{e\prime} = \underset{\sim}{S}^{e} \cdot 0$
$=\{0/0,01;\ 1/0,01;\ 0,33/0,1;\ 0/1\} \cdot 0 = \{0/0;\ 1/0;\ 0,33/0;\ 0/0\};$

$\underset{\sim}{A}^{e\prime} = \underset{\sim}{A}^{e} \cdot 12$
$=\{0/0,01;\ 0,25/0,01;\ 1/0,1;\ 0,5/1;\ 0/1\} \cdot 12 = \{0/0,12;\ 0,25/0,12;\ 1/1,2;\ 0,5/12;\ 0/12\};$

$\underset{\sim}{B}^{e\prime} = \underset{\sim}{B}^{e} \cdot 48$
$=\{0/0,01;\ 0,67/0,1;\ 1/1;\ 0/1\} \cdot 48 = \{0/0,48;\ 0,67/4,8;\ 1/48;\ 0/48\}.$

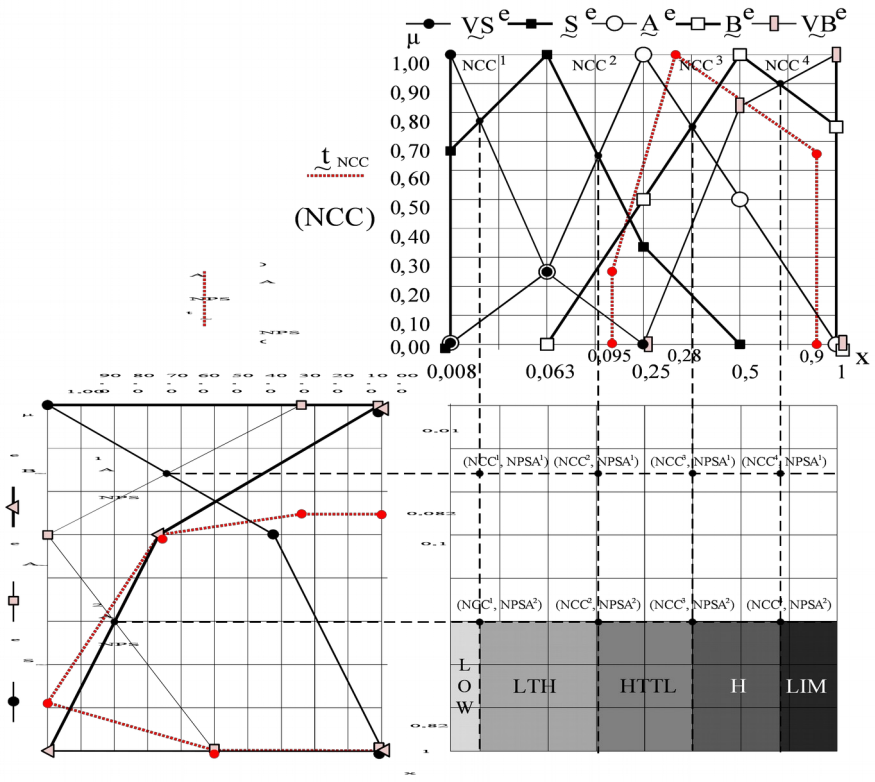
2 – кезең. Алдыңғы мысалға ұқсас тәсілмен $\underset{\sim}{t}_{NPSA}$ алуға арналған $\underset{\sim}{S}^{e\prime}$ түзетілген эталонды АЕС қосындысын алу жүзеге асырылады. тасымалдаушылары нөлдік болса, онда

$\underset{\sim}{t}_{NPSA} = \underset{\sim}{A}^{e\prime} \mathbin{\tilde{+}} \underset{\sim}{B}^{e\prime}$ $=\{0/0,6;\ 0/4,92;\ 0/48,12;\ 0/48,12;$
0/0,6; 0,25/4,92; 0,25/48,12; 0/48,12;
0/1,68; 0,67/6; 1/49,2; 0/49,2;
0/12,48; 0,5/16,8; 0,5/60; 0/60;
0/12,48; 0/16,8; 0/60; 0/60;}=
{0/4,92; 0,25/4,92; 0,67/6; 1/49,2; 0,5/60; 0/60;}/60=
{0/0,082; 0,25/0,082; 0,67/0,1; 1/0,82; 0,5/1; 0/1;}.

4.26 суретінде $\boldsymbol{SR_3}$ шешуші ережелерінің қалыптасқан ішкі жиындарының I_3 қатысты басып кіру туындатқан ауытқушылық жағдайының графикалық түсіндірмесі ұсынылған.

Осында сонымен қатар $\underset{\sim}{t}_{NCC}$ мен $\underset{\sim}{t}_{NPSA}$ для NCC және NPSA арналған эталондарға қатысты есептелген ағымдағы $\underset{\sim}{t}_{NCC}$ мен $\underset{\sim}{t}_{NPSA}$ мәндері ұсынылған. Компьютерлік желілердегі кибершабуылдар туындатқан ауытқушылық жағдайын анықтау технологиясының қисынды қорытынды процедурасының 8 кезеңіне сәйкес (3.1 бабын) $\underset{\sim}{t}_{NCC}$ мен $\underset{\sim}{t}_{NPSA}$ қай эталонға жақын екенін анықтау талап етіледі. Бұл үшін(1.2 бабында келтірілген зерттеулерді ескере отырып) АЕС қажет класын өңдейтін РХ әдісін қолданамыз. Бұл әдісті нәтижелі қолдану α-деңгейлі түрдегі АЕС өңдеу барлық талап

етілетін заттарды ұсыну қарастырылады, мысалы , NCC үшін α мәндері тең 0; 0,25; 0,33; 0,5; 0,67; 0,75; 0,83; 1, ал NPSA үшін – 0; 0,25; 0,33; 0,5; 0,67; 1.



Сурет 4.26 -Iзтуындатқан ауытқушылық жағдайының графикалық кескіндемесі

Қажет шамаларды түрлендіру $x = x_i + \frac{(\mu_x(x) - \mu_x(x_i))(x_{i+1} - x_i)}{\mu_x(x_{i+1}) - \mu_x(x_i)}$, $x \in [x_i, x_{i+1}]$, $\overline{1,n-1}$ (1.2 бабының ЛАЛМ) формуласы арқылы жүзеге асырылады, осылайша ұсынылған α- деңгейге іс жүзінде сәйкес келетін барлық қолданылатын АЕС бір ретке келтіреді.

Егер $\alpha=0$ болса α-деңгейлі $\tilde{VS}^{ea}$ жиыны арқылы $\tilde{VS}^{e}$ ұсынамыз. Егер $\mu_x(x_i)=1$, $x_{i+1}=0,063$, $x_i=0,008$ мен $\mu_x(x_{i+1})=0,25$ болса АЕС графикалық ұсыну (4.26 суретін)және шамалардың ағымдағы мәндерін, қалыптасқан эталондарды(2.2 бабын) ескере отырып келесі мәндерді аламыз:

$\mu_x(x)=0,83$ үшін $x = 0,008 + \frac{(0,83-1)(0,063-0,008)}{0,25-1} = 0,02$;

$\mu_x(x)=0,75$ үшін $x = 0,008 + \frac{(0,75-1)(0,063-0,008)}{0,25-1} = 0,026$;

$\mu_x(x)=0,67$ үшін $x = 0,008 + \frac{(0,67-1)(0,063-0,008)}{0,25-1} = 0,032$;

$\mu_x(x) = 0,5$ үшін $x = 0,008 + \frac{(0,5-1)(0,063-0,008)}{0,25-1} = 0,045$;

$\mu_x(x) = 0,33$ үшін $x = 0,008 + \frac{(0,33-1)(0,063-0,008)}{0,25-1} = 0,057$.

Осылайша АЕС үшін

$\overset{\sim}{VS}^{ea}$ *={0/0,008; 0,25/0,008; 0,33/0,008; 0,5/0,008; 0,67/0,008; 0,75/0,008; 0,83/0,008; 1/0,008; 0,83/0,02; 0,75/0,026; 0,67/0,03; 0,5/0,045; 0,33/0,057; 0,25/0,063; 0/0,25}.*

Осыған ұқсас түрде $\tilde{S}^{ea}$, $\tilde{A}^{ea}$, $\tilde{B}^{ea}$, $\overset{\sim}{VB}^{ea}$ арналған келесі түрге ие АЕС қалыптасады:

$\tilde{S}^{ea}$ *={0/0,008; 0,25/0,00; 0,33/0,008; 0,5/0,008; 0,67/0,008; 0,75/0,021; 0,83/0,035; 1/0,0063; 0,83/0,11; 0,75/0,13; 0,67/0,16; 0,5/0,2; 0,33/0,25; 0,25/0,31; 0/0,5};*

$\tilde{A}^{ea}$ *={0/0,008; 0,25/0,063; 0,33/0,083; 0,5/0,12; 0,67/0,17; 0,75/0,19; 0,83/0,21; 1/0,25; 0,83/0,34; 0,75/0,38; 0,67/0,42; 0,5/0,5; 0,33/0,67; 0,25/0,75; 0/1};*

$\tilde{B}^{ea}$ *={0/0,063; 0,25/0,16; 0,33/0,19; 0,5/0,25; 0,67/0,34; 0,75/0,38; 0,83/ 0,42; 1/0,5; 0,83/0,84; 0,75/1; 0,67/1; 0,5/1; 0,33/1; 0,25/1; 0/1};*

$\overset{\sim}{VB}^{ea}$ *={0/0,25; 0,25/0,325; 0,33/0,349; 0,5/0,4; 0,67/0,45; 0,75/0,48; 0,83/ 0,5; 1/1; 0,83/1; 0,75/1; 0,67/1; 0,5/1; 0,33/1; 0,25/1; 0/1}.*

Ары қарай осыған ұқсас түрде $\tilde{t}_{NCC}$ ағымдағы мәнін $\tilde{t}^{\alpha}_{NCC}$ өзгертеміз.Осында егер $\mu_x(x_i) = 0,25$, $x_{i+1} = 0,28$, $x_i = 0,095$ және $\mu_x(x_{i+1}) = 1$ болса, онда:

$\mu_x(x) = 0,33$ үшін $x = 0,095 + \frac{(0,33-0,25)(0,28-0,095)}{1-0,25} = 0,12$;

$\mu_x(x) = 0,5$ үшін $x = 0,095 + \frac{(0,5-0,25)(0,28-0,095)}{1-0,25} = 0,16$;

$\mu_x(x) = 0,67$ үшін $x = 0,095 + \frac{(0,67-0,25)(0,28-0,095)}{1-0,25} = 0,2$;

$\mu_x(x) = 0,75$ үшін $x = 0,095 + \frac{(0,75-0,25)(0,28-0,095)}{1-0,25} = 0,22$;

$\mu_x(x) = 0,83$ үшін $x = 0,095 + \frac{(0,83-0,25)(0,28-0,095)}{1-0,25} = 0,24$, ал егер

$\mu_x(x_i)=1,\ x_{i+1}=0{,}9,\ x_i=0{,}28$ және $\mu_x(x_{i+1})=0{,}67$ болса, онда:

$$\mu_x(x)=0{,}83 \text{ үшін } x=0{,}28+\frac{(0{,}83-1)(0{,}9-0{,}28)}{0{,}67-1}=0{,}6;$$

$$\mu_x(x)=0{,}75 \text{ үшін } x=0{,}28+\frac{(0{,}75-1)(0{,}9-0{,}28)}{0{,}67-1}=0{,}75.$$

Осылайша АЕС

$\underset{\sim}{t}^{\alpha}_{NCC}$ *={0/0,095; 0,25/0,095; 0,33/0,12; 0,5/0,16; 0,67/0,2; 0,75/0,22; 0,83/0,24; 1/0,28; 0,83/0,6; 0,75/0,75; 0,67/0,9; 0,5/0,9; 0,33/0,9; 0,25/0,9; 0/0,9}.*

Көрнекі болу үшін барлық α-деңгейлі жиынға түрленген мәндер 4.6. кестесінде келтірілген.

Кесте 4.6 - NCC және $\underset{\sim}{t}_{NCC}$ ЛА АЕС бейнеленуі

NCC және $\underset{\sim}{t}_{NCC}$ ЛА АЕС бейнеленуі

$\mu_x(x)$		0	0,25	0,33	0,5	0,67	0,75	0,83	1	0,83	0,75	0,67	0,5	0,33	0,25	0
АЕС тасымалдаушылары	$\underset{\sim}{VS}^{ea}$	0,008	0,008	0,008	0,008	0,008	0,008	0,008	0,008	0,02	0,026	0,03	0,045	0,057	0,063	0,25
	$\underset{\sim}{S}^{ea}$	0,008	0,008	0,008	0,008	0,008	0,021	0,035	0,063	0,11	0,13	0,16	0,2	0,25	0,31	0,5
	$\underset{\sim}{A}^{ea}$	0,008	0,063	0,083	0,12	0,17	0,19	0,21	0,25	0,34	0,38	0,42	0,5	0,67	0,75	1
	$\underset{\sim}{B}^{ea}$	0,063	0,16	0,19	0,25	0,34	0,38	0,42	0,5	0,84	1	1	1	1	1	1
	$\underset{\sim}{VB}^{ea}$	0,25	0,325	0,349	0,4	0,45	0,48	0,5	1	1	1	1	1	1	1	1
	$\underset{\sim}{t}^{\alpha}_{NCC}$	0,095	0,095	0,12	0,16	0,2	0,22	0,24	0,28	0,6	0,75	0,9	0,9	0,9	0,9	0,9

Ары қарай РХ әдісінің негізінде (1.2 бабын)С. $h(\underset{\sim}{X},\underset{\sim}{Z})=\sum_{i=1}^{n}|\mu_{\underset{\sim}{X}}(x_i)-\mu_{\underset{\sim}{Z}}(x_i)|$ (осындағы $\mu_{\underset{\sim}{X}}(x_i)$ и $\mu_{\underset{\sim}{Z}}(x_i)$ формуласы арқылы – сәйкесінше эталонды $\underset{\sim}{X}$ және ағымдағы $\underset{\sim}{Z}$ АЕС ҚФ ең төмені ағымдағы АЕС эталонды неғұрлым жақын h функциясының мәндері анықталады. Келесі есептеулерді жүргіземіз:

$h(\underset{\sim}{VS}^{ea},\underset{\sim}{t}^{\alpha}_{NCC})=(0{,}008–0{,}095)+(0{,}008–0{,}095)+(0{,}008–0{,}12)+(0{,}008–0{,}16)+(0{,}008–0{,}2)+(0{,}008–0{,}22)+(0{,}008–0{,}24)+(0{,}008–0{,}28)+(0{,}02–0{,}6)+(0{,}026–0{,}75)+$

*(0,03–0,9)+(0,045–0,9)+(0,057–0,9)+(0,063–0,9)+(0,025–0,9)=0,087+0,087+0,112+0,152+0,192+0,212+0,232+0,272+0,58+0,73+0,874+0,87+0,855+0,837+0,65=**6,74**;*

S^{ea} $\tilde{t}^{\alpha}_{NCC}$
h(~ ,) =0,087+0,087+0,112+0,152+0,192+0,199+0,205+0,217+0,49+0,62+0,74+0,7+0,65+0,59+0,4=5,44;

A^{ea} $\tilde{t}^{\alpha}_{NCC}$
h(~ ,) =0,087+0,032+0,037+0,04+0,03+0,03+0,03+0,03+0,26+0,37+0,48+0,4+0,23+0,15+0,1=2,31;

B^{ea} $\tilde{t}^{\alpha}_{NCC}$
h(~ ,) =0,032+0,065+0,07+0,09+0,14+0,16+0,18+0,22+0,24+0,25+0,1+ 0,1+0,1+0,1+0,1+0,1=1,95;

VB^{ea} $\tilde{t}^{\alpha}_{NCC}$
h(~ ,) =0,155+0,23+0,229+0,24+0,25+0,26+0,26+0,72+0,4+0,25+0,1+0,1+0,1+0,1+0,1+0,1=3,5.

Есептеулерден ең төменгі мән *1,95*екені көрінеді, яғни $\tilde{t}^{\alpha}_{NCC}$ ағымдағы шамасы эталонды $\tilde{B}^{e\alpha}$ неғұрлым жақын болып табылады, ал $\tilde{t}^{\alpha}_{NCC}$ және $\tilde{B}^{e\alpha}$ мен $\tilde{t}_{NCC}$ $\tilde{B}^{e}$ бейнесі болғандықтан, онда $\tilde{t}_{NCC}$ эталонды $\tilde{B}^{e}$ неғұрлым жақын орналасқан.

Жоғарыда аталған формуланы ескере отырып (1.2 бабының ЛАЛМ қараңыз) **NCC** ұқсас **NPSA** арналған мәндерді қалыптастырамыз.

Осылайша, мысалы $\mu_x(x_i)=1,\ x_{i+1}=0,1,\ x_i=0,01$ және $\mu_x(x_{i+1})=0,33$ болса, онда :

$\mu_x(x)=0,67$ үшін $x=0,01+\frac{(0,67-1)(0,1-0,01)}{0,33-1}=0,054$;

$\mu_x(x)=0,5$ үшін $x=0,01+\frac{(0,5-1)(0,1-0,01)}{0,33-1}=0,077$,

$\mu_x(x_i)=0,33,\ x_{i+1}=1,\ x_i=0,1$ және $\mu_x(x_{i+1})=0$ $\mu_x(x)=0,25$үшін :

$x=0,1+\frac{(0,25-0,33)(1-0,1)}{0-0,33}=0,32$ аламыз.

Осылайша АЕС

$\tilde{S}^{e\alpha}$ = *{0/0,01;0,25/0,01; 0,33/0,01; 0,5/0,01; 0,67/0,01; 1/0,01; 0,67/0,054; 0,5/0,077; 0,33/0,1; 0,25/0,32; 0/1}.*

Осыған ұқсас келесі түрге ие $\tilde{A}^{e\alpha}$ мен $\tilde{B}^{e\alpha}$ АЕС қалыптасады:

$\underset{\sim}{A}^{e\alpha}$ ={0/0,01;0,25/0,01; 0,33/0,02; 0,5/0,04; 0,67/0,06; 1/0,1; 0,67/0,7; 0,5/1; 0,33/1; 0,25/1; 0/1};

$\underset{\sim}{B}^{e\alpha}$ ={0/0,01;0,25/0,04; 0,33/0,05; 0,5/0,08; 0,67/0,1; 1/1; 0,67/1; 0,5/1; 0,33/1; 0,25/1; 0/1}.

Ары қарай $\underset{\sim}{t}_{NPSA}$ ағымдағы мәнін $\underset{\sim}{t}^{\alpha}_{NPSA}$ өзгертеміз, осындағы $\mu_x(x_i)$ =0,25, x_{i+1}=0,1, x_i=0,082 және $\mu_x(x_{i+1})$=0,6 болса,онда:

$\mu_x(x)$=0,33 үшін $x = 0{,}082 + \frac{(0{,}33 - 0{,}25)(0{,}1 - 0{,}082)}{0{,}67 - 0{,}25} = 0{,}085$;

$\mu_x(x)$=0,5 үшін $x = 0{,}082 + \frac{(0{,}5 - 0{,}25)(0{,}1 - 0{,}082)}{0{,}67 - 0{,}25} = 0{,}093$,

$\mu_x(x_i)$=1, x_{i+1}=1, x_i=0,82 мен $\mu_x(x_{i+1})$=0,5 $\mu_x(x)$=0,67болса,онда:

$x = 0{,}82 + \frac{(0{,}67 - 1)(1 - 0{,}82)}{0{,}5 - 1} = 0{,}94$ аламыз.

Осылайша АЕС

$\underset{\sim}{t}^{\alpha}_{NPSA}$ ={0/0,082; 0,25/0,082; 0,33/0,085; 0,5/0,093; 0,67/0,1; 1/0,82; 0,67/0,94; 0,5/1; 0,33/1; 0,25/1;0/1}.

Көрнекі болу үшін барлық түрлендірілген мәндер 4.7 кестесінде көрсетілген.

Кесте 4.7 - NPSA мен $\underset{\sim}{t}_{NPSA}$ үшін ЛА АЕС бейнеленуі

NPSAмен $\underset{\sim}{t}_{NPSA}$ үшін ЛА АЕС бейнеленуі

$\mu_x(x)$		0	0,25	0,33	0,5	0,67	1	0,67	0,5	0,33	0,25	0
АЕС тасымалдаушылары	$\underset{\sim}{S}^{e\alpha}$	0,01	0,01	0,01	0,01	0,01	0,01	0,054	0,077	0,1	0,32	1
	$\underset{\sim}{A}^{e\alpha}$	0,01	0,01	0,02	0,04	0,06	0,1	0,7	1	1	1	1
	$\underset{\sim}{B}^{e\alpha}$	0,01	0,04	0,05	0,08	0,1	1	1	1	1	1	1
	$\underset{\sim}{t}^{\alpha}_{NPSA}$	0,082	0,082	0,085	0,093	0,1	0,82	0,94	1	1	1	1

Ары қарай РХ әдісінің негізінде келесі есептеулерді жүргіземіз:

$h(\underset{\sim}{S}^{e\alpha}, \underset{\sim}{t}^{\alpha}_{NPSA})$=(0,01–0,082)+(0,01–0,082)+(0,01–0,085)+(0,01–0,093)+(0,01–0,1)+(0,01–0,82)+(0,054–0,94)+(0,077–1)+(0,1–1)+(0,32–1)+(1–1)=0,072+0,072+0,075+0,92+0,09+0,81+0,886+0,923+0,99+0,68+1=**5,69**;

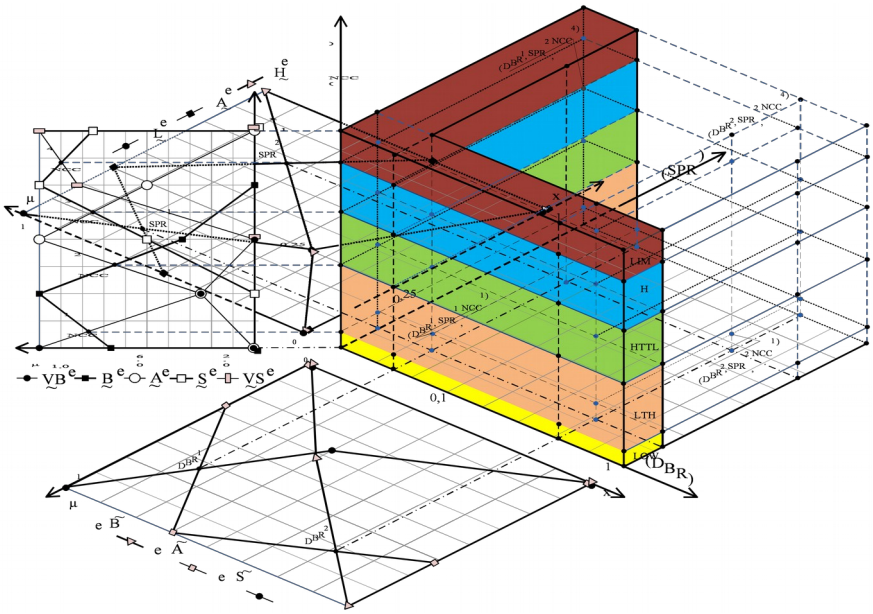
$h(\underset{\sim}{A}^{e\alpha}, \underset{\sim}{t}^{\alpha}_{NPSA})$=0,072+0,072+0,065+0,053+0,04+0,72+0,24=**1,26**;

$h(\underset{\sim}{B}^{e\alpha}, \underset{\sim}{t}^{\alpha}_{NPSA})$=0,072+0,072+0,035+0,013+0+0,18+0,06=**0,43**.

Есептеулерден ең төменгі мән *0,43*екені көрінеді, яғни $\underset{\sim}{t}^{\alpha}_{NPSA}$ ағымдағы шамасы эталонды $\underset{\sim}{B}^{e\alpha}$ неғұрлым жақын болып табылады, ал $\underset{\sim}{t}^{\alpha}_{NPSA}$ және $\underset{\sim}{B}^{e\alpha}$ мен $\underset{\sim}{t}_{NPSA}$ $\underset{\sim}{B}^{e}$ бейнесі болғандықтан, онда $\underset{\sim}{t}_{NPSA}$ эталонды $\underset{\sim}{B}^{e}$ неғұрлым жақын орналасқан.

Жүргізілген есептеулер негізінде, компьютерлік шабуылдар туындатқан ауытқушылық жағдайын анықтау технологиясының 8-кезеңіне сәйкес(3.1 бабын қараңыз) ауытқушылық жағдайын идентификациялау “Егер $\underset{\sim}{t}_{NPSA} \cong \underset{\sim}{B}^{e}$ және $\underset{\sim}{t}_{NCC} \cong \underset{\sim}{B}^{e}$ болса, онда спуффинг туындатқан ауытқушылық жағдайының деңгейі HIGH болады ” деп түсіндірілетін (2.27) – $SR_{34}=(\underset{\sim}{t}_{NPSA} \cong \underset{\sim}{B}^{e} \wedge \underset{\sim}{t}_{NCC} \cong \underset{\sim}{B}^{e}) \rightarrow H$ өрнегінің ережелерін бастамашылыққа алады. Графикалық түрде бұл жағдай 4.26 суретінде бейнеленген ауытқу аймағында орналасқан. Ол H литерімен таңбаланған аумақта қою сұр түспен ерекшеленген.

NCC, **SPR** және **DBR** ЛА арналған эталондар мен ағымдағы мәндер негізінде ұқсас есептеулерді 4.27 суретінде аумақтары сұр түстің түрлі реңктерімен және LIM, H, HTTL, LTH мен LOW литерлерімен таңбаланған, сәйкес шабуылдартуындатқан қоршаған ортадағы ауытқушылық жағдайын идентификациялауге қатысты сарапшының сенімділік дәрежесін бейнелеген I_2 туындатқан ауытқушылықтарды анықтау үшін де жүргізуге болады.



Сурет 4.27 - I_2 туындатқан ауытқушылық жағдайының графикалық түсіндірмесі

Төртінші тарау бойынша тұжырым

1. Ауытқушылық жағдайын анықтау бойынша жалпыланған техникалық шешім және лингвистикалық айнымалылардың нақты жиыны, қалыптасқан анық емес эталондардың мәндері, нақты түйіндес жұптар және құрылған шешуші ережелер жиынының негізіндетүрлі сканерлеуші утилиттер әрекеттерін желік трафиктің ағымдағы шамалары бойынша бағдарламалық немесе бағдарламалы-аппаратты түрде жүзеге асырылатын ауытқушылықтарды анықтаудың модельдік жүйесі ұсынылды.

2. Маңыздылық коэффициенттерін, анық емес арифметиканы анықтау әдістерін жүзеге асырудың құрастырылған алгоритмдері, анық емес шамаларды салыстыру мен қатыстылық функциясын қалыптастыру, сонымен бірге порттар сканерлеуі туындатқан және оның құрылымдық шешімі негізінде негізгі код және сканерлеуші құралдарды анықтау үшін дербес компьютерде қолданыла алатын сәйкес орындалатын бағдарламалық модуль құрылды. Жүргізілген бағдарламаны жүзеге асыру верификациясы шабуылдарды рұқсат етілмеген әрекеттерге қатысты сарапшының түрлі сенім дәрежесін білдіретін түрлі ережелер арқылы барлық шабуылдарды анықтаудың тәжірибелік мүмкіндіктерін көрсетті, осыған сәйкес ұсынылған моделдер мен жүйелерді жүзеге асыру модельдеуші әрекеттерге сәйкес реакцияны бейнелейді деп қорытынды жасауға болады

3. Құрастырылған құрылымдық шешімдер мен алгоритмдер негізінде шабуылдаушы әрекеттердің нақты түрлері туындатқан ауытқушылықтарды анықтауға арналған өспелі мүмкіндіктері бар қолданбалы бағдарламалық жүйе құрылды. Ол қолданылатын қажет шамалар жиынын кеңейту арқылы эталондар құруға және осы шамалардың ағымдағы берілген мәндерін қоршаған ортадағы ауытқушылық жағдайын анықтауды жүзеге

асыруды жүзеге асыруға мүмкіндік береді. Сипатталған әзірлемелер Ұлттық авиациялық университеттің және ООО«Сайфер БІС» қызметіне енгізілген.

4. Тұңғыш рет лингвистикалық бағалар мен аралықтар идентификациялаудың жиынын қолдану, шамалардың ағымдағы жағдайын шабуылдарға қатысты сарапшы пайымдарын сипаттайтын базалық және туынды жиілік матрицаларын сонымен қатар сарапшы бағаларының берілген аралықта кездесу жиілігі мен анық емес термдердің ішкі жиынын қалыптастыру үрдісін қолдану есебінен шабуылдарды анықтау жүйесі үшін жұмыста ұсынылған лингвистикалық эталондарды қалыптастыру әдісі нақты гетерогенді параметрлі қоршаған ортада түрлі ауытқушылықтар жағдайын сипаттайтын берілген лингвистикалық айнымалылар тобының шамасының эталонды мәндерін алу процедурасын қалыптастыруға мүмкіндік беретін шабуылдарды анықтау жүйесі үшін лингвистикалық эталондарды қалыптастыру әдісі құрастырылды.

ҚОРЫТЫНДЫ

Орындалған жұмыстың нәтижесі ретінде компьютерлік желі ресурстарына сигнатуралық емес және жаңа модельдегі шабуылдартуындатқан анық емес әлсіз қалыптасқан ортада нәтижелі идентификациялауге мүмкіндік беретін шабуылдарды анықтау құралдарын жетілдіруге немесе автономды қолдануға арналған технологияда ұсынылған моделдер кешенін құру ғылыми міндетін шешу болып табылады. Диссертациялық жұмыстың орындалу барысында келесі нәтижелер алынды:

1. Компьютерлік жүйелердегі шабуылдарды анықтауға қолданылатын теориялық және тәжірибелік базаның қазіргі жағдайын зерттеу анық емес әлсіз қалыптасқан ортада сигнатуралық емес және и жаңа модельдегі кибершабуылдарды идентификациялау мүмкіндіктеріне қатысты сәйкес қауіпсіздік құралдарының жетілдірілмегендігін көрсетті. Шабуылдаушы әрекеттер туындатқан ауытқушылықтарды анықтау құралдарын құруға арналған анық емес моделдер мен әдістерді қолдану шабуылдарды анықтау жүйесін жетілдіруге және қоршаған ортада бақылау арқылы қауіпті ауытқушылық жағдайларын идентификациялауге мүмкіндік береді.

2. Тұңғыш рет анық емес әлсіз қалыптасқан орта үшін базалық шамалар моделі және басып кіру : шамалар ” мен “ басып кіру**:** түйіндес жұптар жиыны” қалыптасқан жұптар жиыны есебінен қоршаған орта үшін эталонды мәндерді құру үрдісін қалыптастыруға, басып кіру түрі мен оны идентификациялауге қажет атрибуттарының арасында сәйкестік орнатуға, сонымен қатар компьютерлік жүйелердегі кибершабуылдардың нақты жиындарына тән желілік белсенділіктің ауытқушылық жағдайын өлшеуге мүмкіндік береді.

3. Ұсынылған эталонды шамалар жиыны, түйіндес жұптар мен анық емес идентификациялауді инициализациялау матрицаларының есебінен шешуші ережелерінің моделі құрылды, ол компьютерлік желілердегі шабуылдардың нақты түрі туындатқан ауытқушылық жағдайын анықтауға арналған шешуші ережелер жиынын калыптастыру үрдісін қаоыптастыруға мүмкіндік береді.

4. Тұңғыш рет ұсынылған базалық шамалар моделі, құрастырылған эталонды шамалары мен шешуші ережелер моделі, сонымен бірге анық емес әлсіз қалыптасқан ортада қалыптасқан ағымдағы шамалардың есебінен авторизацияланбаған жақ әрекеттері туындатқан ауытқушылық жағдайларын анықтау технологиясы құрастырылды, ол ақпараттық жүйе ресурстарына бағытталған сигнатуралық емес және жаңа модельдегі кибершабуылдарды анықтау құралдарын құруға мүмкіндік береді.

5. Ұсынылған ауытқушылық жағдайын анықтау технологиясын жүзеге асыру, желілік шабуылдардыҒ сигнатуралық емес және жаңа түрлерін нәтижелі идентификациялау есебінен заманауи шабуылдарды анықтау жүйесінің функционалды мүмкіндіктерін кеңейтуге мүмкіндік беретін қоршаған ортадағы белсенділікті бақылау арқылы желілік қауіпсіздік жүйесін жетілдіруге арналған жаңа құрылымдық шешім ұсынылды

6. Құрылған моделдер, технологиялар және жаңа құрылымдық шешімнің негізінде заманауи шабуылдарды анықтаудың функционалды мүмкіндіктерін кеңейту ретінде немесе автономды түрде қолданыла алатын кибершабуылдар әрекеттері туындатқан ауытқушылық жағдайын анықтау үшін алгоритмдік және бағдарламалық қамсыздандыру құрастырылды.

7. Құрылған бағдарламалық қамсыздандыру негізінде құрылған моделдердің жеткіліктілігі мен диссертациялық жұмыстың теориялық және тәжірибелік нәтижелерінің дұрыстығын дәлелдейтін кіріс тест әсерлерінің бастамашылығымен желілік шамалардың анық емес эталондарын қалыптастырудың ішкі жүйесін, шешуші ережелерді жүзеге асырудың ішік жүйесін, порттарды сканерлеу мен ауытқушылықтарды анықтау жүйесіне тәжірибелік зерттеу жүргізілді. Көрсетілген әзірлемелер Ұлттық авиациялық университеттің және ООО «Сайфер БІС» қызметіне енгізілген.

ПАЙДАЛАНЫЛҒАН ӘДЕБИЕТТЕР ТІЗІМІ

1 Ахметов Б.С.,КорченкоА.А., Жумангалиева Н.К. использование методов нечетких множеств в системах обнаружения вторжений // Інформаційна безпека. – 2014. – №1 (13); №2 (14). – С. 42-55.

2 АхметовБ.С. , КорченкоА.А. , АхметоваС.Т., Жумангалиева Н.К.использование методов експертного оценивания в системах обнаружения вторжений // Інформаційна безпека. – 2014. – №3 (15); №4 (16). – С. 34-43.

3 Ахметов Б.С.,КорченкоА.А., Жумангалиева Н.К. Анализ методов нечетких множеств для построения систем обнаружения вторжений //«Современные информационно-телекоммуникационные технологии»: Междунар. науч.-тех. конф.: Матер. конф. – К.: ГУТ, 2015. – С. 38-40.

4 АхметовБ.С., Абдрахманов Р.Б., КорченкоА.А., Жумангалиева Н.К.Базовые модели эталонных величин для систем обнаружения вторжений // Вестник Международного Казахско-Турецкого университета. им. А.Ясави. – 2015. – №5-6 (97-98). – С. 15-26.

5 АхметовБ.С., КорченкоА.А., Ахметова С.Т., Жумангалиева Н.К.Анализ методов экспертного оценивания для систем обнаружения вторжения // «Информационные и телекоммуникационные технологии: образование, наКБа, практика»: II междунар. науч.-практич. конф.: труды. – Алматы, 2015. – Т. 2. – С. 28-31.

6 Ахметов Б.С.,КорченкоА.А., ЖумангалиеваН.К.Модель базовых величин для контроля аномальности состояния среды окружения // Известия Национальной Академии наук Республики Казахстан. Серия физико-математическая. – 2016. – №1 (305). – С. 26-33.

7 Ахметов Б.С.,КорченкоА.А., Жумангалиева Н.К.Модель решающих правил для обнаружения аномалий в информационных сАСтемах // Известия Национальной Академии наук Республики Казахстан. Серия физико-математическая. – 2016. – №4 (308). – С. 91-100.

8 КарпинскийН.П., КорченкоА.А., АхметоваС.Т., Жумангалиева Н.К.Метод построения условных детекционных выражений для сАСтем обнаружения кибератак // Актуальні питання забезпечення кібербезпеки та захисту інформації: II міжнар. наук.-практ. конф.: Тези доп. – Київ, 2016. – С. 65-69.

9 Ахметов Б.С.,КорченкоА.А., Жумангалиева Н.К. Технология выявления аномального состояния для сАСтем обнаружения вторжений // Вестник КазНУ. Серия математика, механика, информатика. – 2016. – №1 (88). – С. 106-113

10 Akhemtov Bakhytzhan, Korchenko Anna, Akhmetova Sanzira, Zhumangalieva Nazym. Improved method for the formation of linguistic standards for ofintrusion detection systems // Journal of The oreticaland Applied Information Technology. - 2016. - Vol.87, №2. – P. 221-232.

11 Корченко А.А.,ЖумангалиеваН.К., Викулов П.А.Построение лингвАСтических эталонов для выявления сниффинг атак // Актуальні питання

забезпечення кібербезпеки та захАСту інформації : III міжнар. наук.-практ. конф. : Тези доп. – Київ, 2017.– С. 93-97.

12 Ахметов Б.,Иванов А., Алибиева Ж., Мукапил К., Бекетова Г. Prospects for Multiple Reductions in Test Samples with a Multivariate, Multicriteria, The Neural Network Statistical Analysis of Biometric Data // Medwell Journals.Research Journal Applied Scienses. - 2015. -№10(12). – P.956-967

13 Karpinski Mikolaj, Martsenyuk Vasyl, GvozdetskaIryna, Akhmetov Bakhytzhan, Zhumangalieva Nazym. Estimation Problem for Network Model at State and Measurements Attacks and Information Cost Criterion// 16th International Conference on Control, Automation and Systems. –Gyeongju; South Korea, 2016. – P. 45-50 // doi: 10.1109/

14 Kłos-Witkowska Aleksandra, Akhmetov Bakhytzhan, Karpinskyi Volodymyr, Gancarczyk Tomasz. Bovine Serum Albumin stability in the context of biosensors//2016 16th International Conference on Control, Automation and Systems ICCAS). –2016. – P. 976 80 // DOI: 10.1109/ICCAS.2016.7832427EEE.

15 АхметовБ.С., КорченкоА.А.,Смагулов С.К, Жумангалиева Н.К. Ақпараттық жүйенің жағдайын бақылауға арналған базалық ауытқымалық шаманың модельдері// Семей Қаласының Шәкәрім Атындағы Мемлекеттік Университетінің хабаршысы. - 2016. - № 2 (74).-С. 87 -91.

16 Ахметов Б.С., Корченко А.А. Смагулов С.К, Жумангалиева Н.К . Ақпараттық жүйенің аномалиялық жағдайын бақылауға арналған базалық шаманың модельдері// Семей Қаласының Шәкәрім Атындағы Мемлекеттік Университетінің хабаршысы. - 2017.-№ 1 (77).-С. 111-115.

17 Akhmetov B., Korchenko A., Kultan J.,Zhumangalieva N.Model decision rules to detect anomalies in Information Systems//Informational Technology Application. - Словакия, 2016. - №1. – P. 126-136.

18 Бекетова Г. С., Ахметов Б.С., Абишева Г.К., Жумангалиева Н.К . Жеке биометриялық мәліметтерді қорғаудың нейрожелілік технологиясы//«Қазақстанның жаңа экономикалық саясатын таратуда жас ғалымдардың орны мен рөлі» халықаралық Сәтбаев оқуларының еңбектері. -2015.-Т.4. – Б. 719-724.

19 МКБапил., Бекетова Г. С., Төлімесова В., Жумангалиева Н.К . Ақпаратты қорғаудың биометриялық әдістері// Хабаршысы КазҰТУ. -2015.-№2. - С.250-261.

20 Мукапил., Бекетова Г. С., Төлімесова В., Жумангалиева Н.К ., Култан Я.. Biometricmethodsofnformationalprotection// Informational Technology Application, Словакия.- 2016. - №1. - 126-136

21 АхметовБ.., Алимсеитова Ж., Коренко А., Жумангалиева Н.К . Система выявления аномального состояния в информационных системах//Қазақстан Республикасы Ұлттық ғылым академиясының баяндамаларыФизика -математика 2017. – №5 (308). – С. 28-37

22 АхметовБ.., Корченко А., Жумангалиева Н.К., Култан Я..Model decision rules to detect anomalies in Information Systems// Informational Technology Application. - Словакия, 2016. - №1. – P.126-136.

23 Гнатюк С.О., Шаховал О.А., Бекетова Г., Жумангалиева Н.К.. Информационно-психологический аспекткиберзащиты// «Состояние и совершенствование безопасности информационно-телекоммуникационных систем» (SITS-2016). - Николаев-Коблево: Международный технологический университет, 2016. – С. 32-34.

24 Anderson J. Computer security threat monitoring and surveillance // Computer Security Resource Center of National Institute of Standards and Technology // Computer Security Laboratory Department of Computer Science University of California at Davis. – Electronic data. – Gaithersburg, MD, USA : NIST, 1980. – Mode of access: World Wide Web // http://csrc.nist.gov/publications/history/ande80.pdf. – Language: English. – Description based on home page (viewed on Oct. 20, 2015).

25 Denning D. An intrusion detection model // Proc. of IEEE Symposium on Security and Privacy. – 1987. – P. 118-131.

26 Котов В.Д.,Васильев В.И. Современное состояние проблемы обнаружения сетевых вторжений // Вестник УГАТУ. – 2012. – Т. 16, №3(48). – С. 198-204.

27 ЛКБацкий А. САСтемы обнаружения атак: Взгляд изнутри // Электроника : НТБ. – Электрон. дан. – М. : Техносфера, 1999. – Режим доступа: WorldWideWeb. – URL: http:// www.electronics.ru/journal/article/1714. – (viewedonOct. 28, 2015).

28 Новак Дж.,Стивен Норткатт, Дональд Маклахен Как обнаружить вторжение в сеть. Настольная книга специалАСта по сАСтемному анализу = Network Intrusion Detection. An Analyst's Handbook/пер. И. Дранишниковa. –М.: Лори, 2012. – 384 с.

29 Russell J.,Ronald Cohn. Intrusion detection system – Stoughton; WI, USA : Book on Demand Ltd.,2012. – 158 p.

30 ЛКБацкий А. Обнаружение атак. – СПб.: BHV, 2003. – 596 с.Шаньгин В.Ф.Защита информации в компьютерных сАСтемах и сетях. – М.: ДМК-Пресс, 2012. – 592 с.

31 Boer P. de.,Martin Pels. Host-based Intrusion Detection Systems Revision 1.10 // Universiteit van Amsterdam. – Electronic data. – Amsterdam : Universiteit van Amsterdam, 2005. – Mode of access: World Wide Web. – URL: http://staff.science.uva.nl/~delaat/rp/2004-2005/p19/ report.pdf. – Language: English. – Description based on home page (viewed on Oct. 26, 2015).

32 Медведовский И.,Лукацкий Алексей.Системы обнаружения атак // Типовая политика безопасности для компаний малого и среднего бизнеса. – Электрон. дан. – СПб. : DigitalSecurity, 2003 // WorldWideWeb. – URL: http://www.lghost.ru/lib/ security/kurs6/theme03_chapter04.htm. – Загл. с экрана.

33 Лукацкий А.В.Системы обнаружения атак. – М. : НИП “Информзащита”, 1999 // WorldWideWeb. – URL: http://doc.marsu.ru/sec/pub/p01.html.

34 Корченко О.Г. Построение систем защиты информации на нечетких множествах : Теория и практические решения. – К. : МК-Пресс, 2006. – 320 с.

35 Portnoy L.,EskinE., Stolfo S. J. Intrusion detection with unlabeled data using clustering // Proc. of ACM Workshop on Data Mining Applied to Security. – 2001. – P. 5-8.

36 Callegari C.,VatonS., Pagano M. A new statistical approach to network anomaly detection // Proc. of Performance Evaluation of Computer and Telecommunication Systems (SPECTS). – 2008. – P. 441-447.

37 Callegari C.,GiordanoS., Pagano M. Application of wavelet packet transform to network anomaly detection // Proc. of Int. Conf. on Next Generation Teletraffic and Wired/Wireless Advanced Networking (NEW2AN). – 2008. – P. 246-257.

38 Planquart J.-P. Application of neural networks to intrusion detection / Jean-Philippe Planquart ; SANS Institute // SANS Information Security Reading Room. – Electronic data. – USA : SANS Institute, 2001. – Mode of access: World Wide Web // http://www.sans.org/reading_room/whitepapers/ detection/application-neural-networks-intrusion-detection_336. – Language: English. – Description based on home page (viewed on May. 10, 2015).

39 Cost-based modeling and evaluation for data mining with application to fraud and intrusion detection [Electronic resource] : Results from the JAM project / Salvatore J. Stolfo, Wei Fan, Wenke Lee, Andreas Prodromidis, Philip K. Chan// Columbia UniversityComputer Science Department. – Electronic data. – New York : Columbia University, 1999. – Mode of access: World Wide Web. – URL: http://www.cs.columbia.edu/~wfan/PAPERS/JAM99.pdf. – Language: English. – Description based on home page (viewed on Oct. 15, 2015).

40 Искусственные иммунные сАСтемы и их применение /под ред. Д. Дасгупты; пер с англ.; под. ред. А.А. Романюхи. – М.: ФИЗМАТЛИТ, 2006. – 344 с.

41 Forrest S. et al.Self-nonself fiscrimination in a computer // Proc. of 1994 IEEE Symp. on Research in Security and Privacy. – 1994. – P. 202-212.

42 Котов В.Д. Система обнаружения вторжений на основе технологий АСкусственных иммунных сАСтем // Интеллектуальные системы управления. – М. : Машиностроение, 2010. – С. 525-535.

43 Kim J.,Bentley P.An artificial immune model for network intrusion detection. Department of Computer Science, University Collge London// BSTU Laboratory of Artificial Neural Networks. – Electronic data. – USA, 2010. – Mode of access: World Wide Web. – URL: http://neuro.bstu.by/ our/immune3.pdf. – Language: English. – Description based on home page (viewed on Oct. 20, 2016).

44 Kotov V.,Vasilyev V.Immune approach to network intrusion detection // Proc. of Security of Information and Networks. – 2010. – P. 233-237.

45 Tarakanov A.O. Immunocomputing for intelligent intrusion detection // IEEE Computational Intelligence Magazine. – Vol.3, issue 2. – P. 23-30.

46 Kotov V.,Vasilyev V. Detection of web server attacks using principles of immunocomputing// Proc. of 2nd World Congress on Nature and Biologically Inspired Computing. – 2010. – P. 25-30.

47 Системы обнаружения вторжений / подготовил Артем Бобров // Institute of continuous media mechanics UB RAS. – Электрон. дан. – Perm :

Institute of continuous media mechanics UB RAS, 2010. – Режим доступа: World Wide Web. – URL: http://www.icmm.ru/~masich/win/lexion/ids/ids.html. – Загл. с экрана.

48 Snort [Electronic resource] / Sourcefire, Inc. – Electronic data. – [Columbia, MD, USA] : [Sourcefire, Inc], 2010. – Mode of access: World Wide Web. – URL: http://www.snort.org. – Language: English. – Description based on home page (viewed on Mar. 25, 2015).

49 OSSEC [Electronic resource] : [Open Source Host-based Intrusion Detection System Project] / Trend Micro Incorporated. – Electronic data. – [Tokyo, Japan] : [Trend Micro, Inc], 2011. – Mode of access: World Wide Web. – URL: http://www.ossec.net/. – Language: English. – Description based on home page (viewed on Oct. 20, 2016).

50 The Bro Network Security Monitor [Electronic resource] / The Bro Project. – Electronic data. – [USA] : The Bro Project, 2011. – Mode of access: World Wide Web. – URL: http://www.bro-ids.org/. – Language: English. – Description based on home page (viewed on Oct. 20, 2015).

51 IBM Proventia Network Anomaly Detection System [Electronic resource] / IBM // IBM. – Electronic data. – [Armonk, New York, USA]: IBM, [2011]. – Mode of access: World Wide Web. – URL: http://www.ibm.com/ru/services/iss/proventia_network_ anomaly_detection_system.html. – Language: English. – Description based on home page (viewed on Oct. 20, 2016).

52 IBM RealSecure Network [Electronic resource] / IBM // IBM. – Electronic data. – [Armonk, New York, USA]: IBM, [2010]. – Mode of access: World Wide Web. – URL: http://www.ibm.com/ru/services/iss/realsecure_network.html. – Language: English. – Description based on home page (viewed on Mar. 08, 2015).

53 Tripwire [Electronic resource] / [Tripwire, Inc.]. – Electronic data. – [Portland, OR, USA] : [Tripwire, Inc.], 2011. – Mode of access: World Wide Web. – URL: http://www.tripwire.org/. – Language: English. – Description based on home page (viewed on Oct. 20, 2015).

54 AirSnare [Electronic resource] : [Intrusion Detection Software for Windows] / [AirSnare Project]. – Electronic data. – [USA;2011]. – Mode of access: World Wide Web. – URL: http://home.comcast.net/~jay.deboer/airsnare/. – Language: English. – Description based on home page (viewed on Oct. 07, 2015).

55 Prelude-IDS [Electronic resource] : [Universal Open-Source Security Information & Event Management system] / The Prelude Team. – Electronic data. – [USA] : CS Systèmes d'Information, 2012. – Mode of access: World Wide Web. – URL: https://www.prelude-ids.org/. – Language: English. – Description based on home page (viewed on Oct. 20, 2015).

56 Гамаюнов Д.Ю. Современные некоммерческие средства обнаружения атак// REDSecure : [Научно-АСследовательский проект] / Лаборатория вычислительных комплексов факультета Вычислительной математики и кибернетики МГУ имени М. В. Ломоносова. – Электрон. дан. – М. : МГУ им. М. В. Ломоносова, 2002 //WorldWideWeb. – URL: http://redsecure.ru/papers/free-ids-survey.pdf. – Загл. с экрана.

57 Обнаружение атак [Электронный ресурс] / MaximChirkov // Проект OpenNet : Портал по открытому ПО, Linux, BSD и Unix сАСтемам. – Электрон. дан. – [РФ;2010]. – Режим доступа: WorldWideWeb. – URL: http://www.opennet.ru/prog/sml/85.shtml. – Загл. с экрана.

58 Кофман А. Введение в теорию нечетких множеств. – М.: Радио и связь, 1982. – 432 с.

59 БорАСовА.Н., АлексеевА.В., Крумберг О.А. и др.Модели принятия решений на основе лингвистической переменной. – Рига : Зинатне, 1982. – 256 с.

60 АверкинА.Н., БатыршинИ.З., Блишун А.Ф.и др.Нечеткие множества в моделях управления и искусственного интеллекта /под ред. Д.А. Поспелова. – М.: НаКБа, 1986. – 312 с.

61 БорисовА.Н., АлексеевА.В., Меркурьева и Г.В. др.Обработка нечеткой информации в системах принятия решений – М.: Радио и связь, 1989. – 304 с.

62 Саати Т.Л. Принятие решений. Метод анализа иерархий. – М. : Радио и связь, 1993. – 320 с.

63 Ротштейн А.П. Интеллектуальные технологии идентификации. – Винница: Универсум Винница, 1999. – 320 с.

64 Мелихов А.Н.,БерштейнЛ.С., КоровинС.Я.Расплывчатые ситуационные модели принятия решений: учебн. пособие – Таганрог : ТРТИ, 1986. – 92 с.

65 БорАСов А.Н.,КрумбергО.А., ФедоровИ.П.Принятие решений на основе нечетких моделей. Примеры использования – Рига: Зинатне, 1990. – 184 с.

66 Сваровкий С.Т. Аппроксимация функций принадлежности значений лингвАСтической переменной // Мат. вопр. анализа данных. – Новосибирск : ВЦ СО АН СССР. – 1980. – С.127-131.

67 РотштейнА.П. ШтовбаС.Д.Нечеткая надежность алгоритмических процессіов.– Винница: Континент-ПРИМ, 1997. – 142 с.

68 Борисов А.Н.,Осис Я.Я. Методика оценки функции принадлежности нечеткого множества // Кибернетика и диагностика. – Рига: Риж. политехн. ин-т, 1970. – Вып. 4. – С.125-134.

69 Норвич А.М.,Туркcен И.Б.Построение функций принадлежности // Нечеткие множества и теория возможностей. Последние достижения / под ред. Р.Р. Ягера. – М. : Радио и связь, 1986. – С.64-71.

70Chu A.T.W.,KalabaR.E., Spingarn J. A comparison of two methods for determining the veights of belonging to fuzzy sets // Journal of Optimization Theory and Applications. – 1979. – Vol. 27. – P. 531-538.

71 Ягер Р.Р. Множества уровня для оценки принадлежности нечетких подмножеств // Нечеткие множества и теория возможностей. Последние достижения / под ред. Р.Р. Ягера. – М. : Радио и связь, 1986. – С. 71-78.

72 Скофенко А.В. О построении функций принадлежности нечетких множеств, соответствующих количественным экспертным оценкам / А.В. Скофенко // НаКБоведение и информатика. – К. : НаКБ. думка, 1981. – С.70-79.

73 Корченко А.Г. Расстояние α-уровня для сравнения нечетких чАСел / А.Г. Корченко, Л.Г. Черныш // Проблемы информатизации и управления : Сб. науч. тр. - К. : КМУГА, 1997. – Вып. 2. -С. 117-124.

74Baldwin J.F. Comparison of Fuzzy Sets on the Same Decision space / J.F. Baldwin, N.C.F. Guild // Fuzzy Sets and Systems. – 1979. – Vol.2, №3. – P. 213-231.

75 Корченко А.Г. Классификация нечетких чАСел для рационального применения в методах и моделях систем защиты информации / А.Г. Корченко, В.А. Рындюк, Е.В. Пацира // Правове, нормативне та метрологічне забезпечення сАСтем захАСту інформації в КБраїні : НаКБ.-техн. зб. – К. : НДЦ "Тезіс" НТУУ "КПІ", 2002. – Вип. 5. - С.166-169.

76 Минаев Ю.Н. Системы линейных уравнений с нечеткими коэффициентами и алгоритмы их решения // Электронное моделирование. – 1991. – Т.13, №4. – С.65-69.

77 Минаев Ю.Н. К вопросу анализа и выбора показателей надежности программного обеспечения вычислительных систем // Кибернетика и системный анализ. –1992. – №2. – С.46-60.

78 АлтунинА.Е.,Семухин М. В.Модели и алгоритмы принятия решений в нечетких условиях – Тюмень: Изд-во Тюмен. гос. Ун-та, 2000. – 352 с.

79 Корченко А.Г. Векторные операции нечеткой арифметики и их аппаратная реализация // Вісн. Центрального наКБ. центру Транспорної академії КБраїни. – К. : ЦНЦ ТАУ, 2000. -№3. -С. 22-23.

80 Корченко А.Г. Методы и аппаратные средства реализации нечетких операций / // Автоматизированные системы обработки информ. : Сб. науч. тр. – К. : КМУГА, 1996. – С. 17-25.

81 Корченко А.Г. Нечеткие арифметические операции с линейной аппроксимацией по локальным максимумам // Зб. наКБ. пр. Ін-ту пробл. моделювання в енергетиці. - Л.: Світ, 1998. - Вип. 4. – С.3-6.

82 Заде Л. Понятие лингвистической переменной и его применение к принятию приближенных решений. – М. : Мир, 1976. – 166 с.

83 Кини Р.Л.,РайфаХ.Принятие решений при многих критериях предпочтения и замещения – М.: Радио и связь, 1981. –560 с.

84 Тоценко В.Г. Методы и системы поддержки принятия решений. Алгоритмический аспект. – К. : НаКБ. думка, 2002. – 381 с.

85 Гафт М.Г. Принятие решений при многих критериях. – М. : Знание, 1979. – 64 с.

86 Березовский Б.А.,Кемпнер Л.М. Об одном способе упорядочения критериев по важности // АиТ. – 1979. – № 4. – С. 67-71.

87 Лебензон А.Б.,Литвак Б.Г.Принцип упорядочения критериев при многокритериальных оценках // Изв. АН СССР. Техн. кибернетика. – 1988. – № 6. – С. 49-53.

88 Многокритериальные задачи принятия решений / под ред. Д.М. Гвишиани, С.В. Емельянова. – М. : Машиностроение, 1978. – 192 с.

89 Фарберов Д.С.,Алексеев С.Г. Сравнение некоторых методов решения многокритериальных задач линейного программирования // Журн. вычАСл. математики и мат. физики, 1974. – Т. 14, № 6. – С. 178-180.

90 Тухвалов М.Б. Весовые методы в математическом программировании. – Ташкент : ФАИ, 1981. – 158 с.

91 Zeleny M. Compromise Programming // Multiple Criteria Decision Making / editors J. Cochrane, M. Zeleny. – Columbia : University of South Carolina Press, 1973. – P. 262-301.

92 Литвак Б.Г. Экспертная информация. Методы получения и анализа. – М. : Радио и связь, 1982. – 185 с.

93 АнохинА.М., ГлотовВ.А., Павельев В.В. и др.Методы определения коэффициентов важности критериев // Автоматика и телемеханика. – 1997. – № 8. – С. 3-35.

94 Мандель И.Д. Кластерный анализ. – М. : Финансы и статистика, 1988. – 176с.

95 Wei T.H. The algebraic foundations of ranking theory : [Ph.D. Thesis] / T.H. Wei. – Cambridge : University of Cambridge, 1952. – 138 p.

96 Saaty T. Eigenvector and logarithmic least squares // Eur. J. Oper. Res. – 1990. – Vol. 48, № 1. – P. 156-160.

97 Cogger K.O.,Yu P.L. Eigenweight vectors and least-distance approximation for revealed preference in pairwise weight rations // J. Optimiz. TheoryandAppl. – 1985. – Vol.46, №4. – P. 483-491.

98 Юшманов С.В. Метод нахождения весов, не требующий полной матрицы попарных сравнений // Автоматика и телемеханика. – М. : НаКБа, 1990. – №2. – С. 186-189.

99 Берж К. Теория графов и ее применения. – М. : Изд-во иностр. лит., 1962. – 320 с.

100 Churchmen C.W.,Ackoff R.An approximate Measure of Value // Operations Research. – 1954. – №2. – P. 171-181.

101 Nelson W.L. On the use of optimization Theory for Practical Control System Design // IEEE Trans. on Automatic Control. – 1964. – Vol. 9, № 4. – P. 469-477.

102 Подиновский В.В. Лексикографические задачи линейного программирования// Журн. вычисл. матем. и мат. физики. – 1972. – Т. 12, № 6. – С. 568-571.

103 Орлов А.И. Теория принятия решений: учебник. – М. : Экзамен, 2006. – 573 с.

104 Sherali Hanit D. Equivalent weight for lexicographic multiobject programs,

105 characterization, and computation // Eur. J.Oper. Res. – 1982. – V. 11, № 4. – P. 367-379.

106 Малаков И. Класификация на методи за определяне приоритета на критериите при избор на оптимален вариант на сАСтеми за нАСкостойностна автоматизация// Научни известия на НТС по Машиностроене. – 2008. – № 3 (106). – С. 29-40.

107 Юттлер Х. Линейная модель с несколькими целевыми функциями / Х. Юттлер // Экономика и мат. методы. – 1977. – Т. 3, № 3. – С. 356-361.

108 Сербин И.В. Оценка значимости факторов в маркетинговых АСследованиях банков // Сб. науч. труд. – Пятигорск: СевКавГТУ. – 2005. – № 2. – С. 54-60.

109 Гермеер Ю.Б. Введение в теорию исследования операций. – М.: НаКБа, 1971. – 324 с.

110 Charsnes A.,CooperW.W.Management Models and Industrial Applications of Linear Programming // Management Science. – 1957. – Vol. 4,№1. – P. 38-91.

111 Szidarovszky F.I. Use of cooperative games in a multiobjective analysis of maning and environment BogardiI., L. Duckstein // Proc. and International Conference on Applied numerical Modeling. Madrid. Spain. – 1978. – № 9. – P. 11-15.

112 Thurstone L.L. The measurement of valnes / L.L. Thurstone. – Chicago : The University of Chicago Press, 1959. – 322 p.

113 Глотов В.А. Метод определения коэффициентов относительной важности / В.А. Глотов // Приборы и системы управления. – 1976. – № 8. – С. 17-22.

114 Rosner B.S. A new scaling technique for absolute judgement / B.S. Rosner // Psychometrica. – 1956. – V. 21, № 4. – P. 377-381.

115 Раев А.Г. Об одном способе определения весовых коэффициентов частных критериев при построении аддитивного интегрального критерия / А.Г. Раев // Автоматика и телемеханика. – М. : НаКБа, 1984. – № 5. – С. 162-165.

116 Корченко О.Г. Системи захисту інформації : Монографія / О.Г. Корченко. – К. : НАУ, 2004. – 264 с.

117 Gavrilis D. Real-time detection of distributed denial-of-service attacks using RBF networks and statistical features / D. Gavrilis, E. Dermatas // Computer Networks. – 2005. – №48. – P. 235-245.

118 McClure S. Hacking exposed, network security secrets & solutions / S. McClure, J. Scambray, G. Kurtz. – 6th Edition. – New York : McGraw-Hill Osborne Media, 2009. – 720 p.

119 Patrikakis C. Distributed denial of service attacks / C. Patrikakis, M. Masikos, O. Zouraraki // The Internet Protocol Journal. – 2004. – Vol. 7. – № 4. – P. 13-35.

120 Угрозы DDoS – риски, устранение и лучшие практические приемы [Электронный ресурс] : Технический отчет / [Cisco Systems, Inc.] // Cisco : [Официальный веб-сайт]. – Электрон. дан. – San Jose, CA, USA : [Cisco Systems, Inc.;2011]. – Режим доступа: World Wide Web. – URL: http://www.cisco.com/web/RU/netsol/ns480/networking_solutions_white_paper0900aecd8032499e.html. – Загл. с экрана.

121 ab :Apache HTTP server benchmarking tool [Electronic resource] / The Apache Software Foundation // The Apache Software Foundation. – Electronic data and programs. – Forest Hill, MD, USA : The Apache Software Foundation, 2011. – Mode of access: World Wide Web. – URL: http://httpd.apache.org/docs/2.0/programs/ab.html. – Language: English. – Description based on home page (viewed on Apr. 28, 2015).

122 Performance Benchmarks a Webserver : [Howto] / [Vivek Gite] // NixCraft. – Electronic data and programs. – [Scottsdale] : NixCraft, 2008. – Mode of

access: World Wide Web. – URL: http://www.cyberciti.biz/tips/howto-performance-benchmarks-a-web-server.html. – Language: English. – Description based on home page (viewed on Apr. 08, 2015).

123 Стасюк О.І. Побудова ефективних моделей сАСтем захАСту інформації / О.І. Стасюк, М.В. Захарова, А.О. Корченко// Защита информации : Сб. науч. трудов. – К. : НАУ, 2007. – Вып.14. – С. 186-190.

124 Корченко А.О. Система виявлення аномалій на основі нечітких моделей/ В.В. Волянська, А.О. Корченко, Є.В. Паціра // Зб. наКБ. пр. Інституту проблем моделювання в енергетиці НАН КБраїни ім. Г. Є Пухова. – Львів : ПП "САСтеми, технології, інформаційні послуги", 2007. – [Спец. випуск]. – Т.2. – С. 56-60.

ҚОСЫМША А

Компьютерлік бағдарламаның бастапқы кодының фрагменті
“Белгісіз логика негізінде портты қарап шығуды анықтау”

```
#include <vcl.h>
#pragma hdrstop
#include "USniffThrd.h"
#include "Unit1.h"
#include "winsock2.h"
#pragma package(smart_init)
extern unsigned long LocalAddrs[10];
extern unsigned long LocalMasks[10];
//---------------------------------------------------------------------------
__fastcall TSniffThrd::TSniffThrd(bool CreateSuspended)
        : TThread(CreateSuspended)
{
}
//---------------------------------------------------------------------------
void __fastcall TSniffThrd::Execute()
{
        FreeOnTerminate = true;
        SOCKET sock;
        SOCKADDR_IN saddr;
        u_long flags;
        BYTE buf[MAX_PACKET_SIZE];
        int cnt;
        tcp_hdr tcp;
        udp_hdr udp;
        ip_hdr ip;
        char caddr[128];
        protoent *pe;
        servent *se;
        pe = new protoent;
        se = new servent;
        sock = socket (PF_INET,SOCK_RAW,IPPROTO_IP);
        ZeroMemory(&saddr,sizeof(saddr));
        saddr.sin_family = AF_INET;
        saddr.sin_family = AF_INET;
        if (Form1->ComboBox1->ItemIndex == Form1->ComboBox1->Items-
>Count /* - 1*/)
        {
                saddr.sin_addr.S_un.S_addr = INADDR_ANY;
        }
        else
        {
```

```
                saddr.sin_addr.S_un.S_addr = LocalAddrs[Form1->ComboBox1-
>ItemIndex];
        }
        bind(sock,(SOCKADDR*)&saddr,sizeof(SOCKADDR));
        flags = 1;
        ioctlsocket(sock,SIO_RCVALL,&flags);
        while (true)
        {
            if (Terminated) break;
            cnt = recv(sock,buf,sizeof(buf),0);
            if (Terminated) break;
            if (cnt>=sizeof(ip_hdr))
            {
                if (!CheckFilter(buf)) continue;
                memcpy(&ip,buf,sizeof(ip));
                saddr.sin_addr.S_un.S_addr = ip.sender;
                saddr.sin_addr.S_un.S_addr = ip.receiver;
                pe = getprotobynumber(ip.proto);
                if (ip.proto == 17)
                {
                    memcpy(&udp,&buf[(ip.ver_len&0x0f) * 4  ],sizeof(udp));
                    udp.sender = ntohs(udp.sender);
                    udp.receiver = ntohs(udp.receiver);
                    se = getservbyport(htons(udp.sender),"udp");
                    se = getservbyport(htons(udp.receiver),"udp");
                }
                if (ip.proto == 6)
                {
                    memcpy(&tcp,&buf[(ip.ver_len&0x0f) * 4 ],sizeof(tcp));
                    tcp.sender = ntohs(tcp.sender);
                    tcp.receiver = ntohs(tcp.receiver);
                    se = getservbyport(htons(tcp.sender),"tcp");
                    se = getservbyport(htons(tcp.receiver),"tcp");
                    if (se) Form1->inputd((USHORT )tcp.receiver);
                    else Form1->inputd((USHORT )tcp.receiver);
                }
                if (Terminated)
                {
                    break;
                }
            }
        }
        closesocket(sock);
    }
    void TSniffThrd::DoOnTerminate(SOCKET sock)
```

```
{
    closesocket(sock);
}
void TSniffThrd::SetFilter (ULONG Src, ULONG Dst, int Proto,int sPort,int
dPort)
{
    if (Src) sAddr = Src; else sAddr = 0;
    if (Dst) dAddr = Dst; else dAddr = 0;
    if (Proto) Protocol = Proto; else Protocol = 0;
    if (sPort) SrcPort = sPort; else SrcPort = 0;
    if (dPort) DstPort = dPort; else DstPort = 0;
}
bool TSniffThrd::CheckFilter (byte *buff)
{
    ip_hdr ip;
    udp_hdr udp;
    tcp_hdr tcp;
    memcpy (&ip,buff,sizeof(ip));
    if (sAddr)
    {
        if (ip.sender!=sAddr) return false;
    }
    if (dAddr)
    {
        if (ip.receiver!=dAddr) return false;
    }
    if (Protocol)
    {
        if (ip.proto != Protocol) return false;
    }
    if (DstPort)
    {
        if (ip.proto == 6)
        {
            memcpy(&tcp,&buff[(ip.ver_len&0x0f) * 4],sizeof(tcp));
            tcp.receiver = ntohs(tcp.receiver);
            if (tcp.receiver != DstPort) return false;
        }
        else if (ip.proto == 17)
        {
            memcpy(&udp,&buff[(ip.ver_len&0x0f) * 4 ],sizeof(udp));
            udp.receiver = ntohs(udp.receiver);
            if (udp.receiver != DstPort) return false;
        }
    }
```

```
        if (SrcPort)
        {
                if (ip.proto == 6)
                {
                        memcpy(&tcp,&buff[(ip.ver_len&0x0f) * 4 ],sizeof(tcp));
                        tcp.sender = ntohs(tcp.sender);
                        if (tcp.sender != SrcPort) return false;
                }
                else if (ip.proto == 17)
                {
                        memcpy(&udp,&buff[(ip.ver_len&0x0f) * 4],sizeof(udp));
                        udp.sender = ntohs(udp.sender);
                        if (udp.sender != SrcPort) return false;
}
        }
returntrue;

}
```

Фрагмент АСходногокодапрограммного обеспечения
“Методов, моделей и сАСтем выявления аномалий”

Модуль для ПФЭ

```
#include <vcl.h>
#pragma hdrstop
#include "Unit1.h"
#include "Unit2.h"
#include <math.h>
#pragma package(smart_init)
#pragma link "DBGridEh"
#pragma link "PropStorageEh"
#pragma link "PrViewEh"
#pragma link "DBSumLst"
#pragma link "PrnDbgeh"
#pragma resource "*.dfm"
TForm1 *Form1;
int td[10][10];
float ne[20][10];
__fastcall TForm1::TForm1(TComponent* Owner)
        : TForm(Owner)  {   }
void __fastcall TForm1::build_lz(int i)
{   ComboBox1->Items->Clear();
  ADOTable2->Filtered=false;
  ADOTable2->First();
  while (!ADOTable2->Eof)
```

```
        {    ComboBox1->Items->AddObject(ADOTable2->FieldByName("Name")-
>AsString,(TObject *) ADOTable2->FieldByName("_Index")->AsInteger);
          ADOTable2->Next();  }
        int j=0;   if (i == 0)   ComboBox1->ItemIndex = 0;   else
        {    for (j=0; j < ComboBox1->Items->Count; j++)    {
           if ((int)(ComboBox1->Items->Objects[j]) == i)      {
             ComboBox1->ItemIndex = j;    break;       }     }    }
        ADOTable2->Filter="_Index="+IntToStr((int)(ComboBox1->Items-
>Objects[j]));
        ADOTable2->Filtered=true;
        ADOTable4->Filter="Lz_Index="+ADOTable2->FieldByName("_Index")-
>AsString;
        ADOTable4->Filtered=true;
        ADOTable3->Filter="Lz_Index="+ADOTable2->FieldByName("_Index")-
>AsString;
        ADOTable3->Filtered=true;
        for (i=1; i < ADOTable4->RecordCount; i++)
          DBGridEh1->Columns->Items[i+1]->Visible=true;
        for (; i < 10; i++)
          DBGridEh1->Columns->Items[i+1]->Visible=false;   }
      void __fastcall TForm1::SpeedButton1Click(TObject *Sender)
      {   TForm2* NewForm = new TForm2(this);   try
        {
          NewForm->Caption="Нова лігвістична змінна";
          if (NewForm->ShowModal() == mrOk)
          {   ADOTable2->Filtered=false;
            ADOTable2->Insert();
            ADOTable2->FieldByName("Name")->AsString=NewForm-
>LabeledEdit1->Text;
            ADOTable2->Post();
            build_lz(ADOTable2->FieldByName("_Index")->AsInteger);    }  }
__finally
        {    delete NewForm;   } }

      void __fastcall TForm1::ComboBox1Change(TObject *Sender)
      {  ADOTable2->Filter="_Index="+IntToStr((int)(ComboBox1->Items-
>Objects[ComboBox1->ItemIndex]));
        ADOTable2->Filtered=true;
        ADOTable4->Filter="Lz_Index="+ADOTable2->FieldByName("_Index")-
>AsString;
        ADOTable4->Filtered=true;
        ADOTable3->Filter="Lz_Index="+ADOTable2->FieldByName("_Index")-
>AsString;
        ADOTable3->Filtered=true;
        int i=0;   for (i=1; i < ADOTable4->RecordCount; i++)
```

```
          DBGridEh1->Columns->Items[i+1]->Visible=true;
         for (; i < 10; i++)   DBGridEh1->Columns->Items[i+1]->Visible=false;  }
        void __fastcall TForm1::FormCreate(TObject *Sender)
        {  build_lz(0);
         TGridRect myRect;
         myRect.Left = -1;   myRect.Top = -1;   myRect.Right = -1;   myRect.Bottom
= -1;
         StringGrid1->Selection = myRect;
         Image1->Canvas->Brush->Color=clWhite;
         Image1->Canvas->FillRect(Rect(0,0,Image1->Width,Image1->Height));  }
        void __fastcall TForm1::Button4Click(TObject *Sender)
        {   int i,j, mp[10]={0,0,0,0,0,0,0,0,0,0}, kmax, imax, jmax, mi;
         float c[10][10], cmax[10]={0,0,0,0,0,0,0,0,0,0}, fn[10][10], b[10], nch[20]
[10];
         imax=ADOTable3->RecordCount;  jmax=ADOTable4->RecordCount;
         ADOTable3->First();   while (!ADOTable3->Eof)
         {     for (j=0; j<=jmax; j++)     {
            td[ADOTable3->RecNo-1][j]=ADOTable3->Fields-
>FieldByNumber(j+4)->AsInteger;    }  ADOTable3->Next();  }
         kmax=0;
        for (j=0; j < jmax; j++)
         {     for (i=0; i < imax; i++)     {       mp[j]+=td[i][j];     }
          if (mp[j] > kmax)     kmax=mp[j];     }
         for (i=0; i < imax; i++)
         {     for (j=0; j < jmax; j++)     {     c[i][j]=td[i][j]*kmax/(mp[j]*1.0);     }   }
         for (j=0; j < jmax; j++)
         {  for (i=0; i < imax; i++)  {   if (c[i][j] > cmax[i])    cmax[i]=c[i][j];     }   }
         for (i=0; i < imax; i++)
          for (j=0; j < jmax; j++)
            fn[i][j]=c[i][j]/cmax[j];
         StringGrid1->ColCount=imax;  StringGrid1->RowCount=jmax;
         for (i=0; i < imax; i++)
          for (j=0; j < jmax; j++)
          {   if (fn[i][j] == 0)   StringGrid1->Cells[j][i]=fn[i][j];   else
             StringGrid1->Cells[j][i]=FloatToStrF(fn[i][j],ffFixed,2,2);    }
         ADOTable4->Last(); mi=ADOTable4->FieldByName("max")->AsInteger;
         ADOTable4->First();   while (!ADOTable4->Eof)
         {  b[ADOTable4->RecNo-1]=ADOTable4->FieldByName("max")-
>AsInteger*1.0/mi;  ADOTable4->Next();  }
         for (i=1; i <= imax*2; i+=2)
         {   for (j=0; j < jmax; j++)   {  nch[i-1][j]=fn[j][(i-1)/2];   nch[i][j]=b[j];  } }
         int n,k;
         for (i=1; i <= imax*2; i+=2)
         {  if (nch[i-1][0] != 0)   {
             ne[i-1][0] = 0;   ne[i][0] = nch[i][0];   n=0;   }
```

```
            else  {    for (j=1; j < jmax; j++)  { if (nch[i-1][j] != 0)  { ne[i-1][0] = 0;
                ne[i][0] = nch[i][j-1];  n=j;  break;  }   }  }
            for (j=n, n=1; j < jmax; j++, n++)
            {ne[i-1][n] = nch[i-1][j]; ne[i][n] = nch[i][j]; }
            for (j=n; j < 10; j++)
            {    ne[i-1][j] = -1;  ne[i][j] = -1;  }
            if (ne[i-1][n-1] != 0)  {  ne[i-1][n] = 0;  ne[i][n] = ne[i][n-1];   k=n-1;  }
            else      {
              for (j=n-2; j >= 0; j--)
              {if (ne[i-1][j] != 0)   { break;  } else  { ne[i-1][j+1] = -1; ne[i][j+1] =
-1;}}}} }
          for (i=imax*2; i < 20; i++)
            for (j=0; j < 10; j++)
             ne[i][j] = -1;}
        float __fastcall TForm1::coord_conv(int n, float k_max, float x)
        {  if (x >= k_max/(pow(10,n)))   {    if (x != 0)  return (k_max/
(n+1.0))*log10(pow(10,(n+1))*x);   else  return 0;} else return x; }
```

Модуль для ППОВ

```
        #include <vcl.h>
        #pragma hdrstop
        #include <Iphlpapi.h>
        #include <winsock2.h>
        #include "Unit1.h"
        #pragma package(smart_init)
        #pragma resource "*.dfm"
        TForm1 *Form1;
        __fastcall TForm1::TForm1(TComponent* Owner)
              : TForm(Owner) {
        } void __fastcall TForm1::Button1Click(TObject *Sender)
        { TListItem  *ListItem;
        String nume;
        ListView1->Items->Clear();
        PMIB_TCPTABLE pTcpTable;
        in_addr       addrLoc, addrRem;
        pTcpTable = (MIB_TCPTABLE*) malloc(sizeof(MIB_TCPTABLE));
        DWORD dwSize = 0,dwRetVal;
        if (GetTcpTable(pTcpTable, &dwSize, TRUE) ==
        ERROR_INSUFFICIENT_BUFFER) {
          GlobalFree(pTcpTable);
          pTcpTable = (MIB_TCPTABLE*) malloc ((UINT) dwSize); } if ((dwRetVal
= GetTcpTable(pTcpTable, &dwSize, TRUE)) == NO_ERROR) {
          for (int i = 0; i < (int) pTcpTable->dwNumEntries; i++) {
          { char szLocAddr[100], szRemAddr[100];
        DWORD dwLocIP = htonl(pTcpTable->table[i].dwLocalAddr);
```

```
DWORD dwRemIP = htonl(pTcpTable->table[i].dwRemoteAddr);
unsigned short nRemPort = htons(pTcpTable->table[i].dwRemotePort);
unsigned short nLocPort = htons(pTcpTable->table[i].dwLocalPort);
addrLoc.S_un.S_addr = ntohl(dwLocIP);
addrRem.S_un.S_addr = ntohl(dwRemIP);
strcpy(szLocAddr, inet_ntoa(addrLoc));
strcpy(szRemAddr, inet_ntoa(addrRem));

void TSniffThrd::DoOnTerminate(SOCKET sock)
{   closesocket(sock);    }
void TSniffThrd::SetFilter (ULONG Src, ULONG Dst, int Proto,int sPort,int
dPort) {
        if (Src) sAddr = Src; else sAddr = 0;
        if (Dst) dAddr = Dst; else dAddr = 0;
        if (Proto) Protocol = Proto; else Protocol = 0;
        if (sPort) SrcPort = sPort; else SrcPort = 0;
        if (dPort) DstPort = dPort; else DstPort = 0;        }
    bool TSniffThrd::CheckFilter (byte *buff)  {
        ip_hdr ip;
        udp_hdr udp;
        tcp_hdr tcp;
        memcpy (&ip,buff,sizeof(ip));
        if (sAddr)    {
            if (ip.sender!=sAddr) return false;             }
        if (dAddr)      {   if (ip.receiver!=dAddr) return false;    }
        if (Protocol)   {  if (ip.proto != Protocol) return false;    }
        if (DstPort)        {  if (ip.proto == 6)   {
                    memcpy(&tcp,&buff[(ip.ver_len&0x0f) * 4],sizeof(tcp));
                    tcp.receiver = ntohs(tcp.receiver);
                    if (tcp.receiver != DstPort) return false;    }   else if (ip.proto ==
17)
                {     memcpy(&udp,&buff[(ip.ver_len&0x0f) * 4 ],sizeof(udp));
                    udp.receiver = ntohs(udp.receiver);
                    if (udp.receiver != DstPort) return false;       }    }
        if (SrcPort)
        {  if (ip.proto == 6) {
                    memcpy(&tcp,&buff[(ip.ver_len&0x0f) * 4 ],sizeof(tcp));
                    tcp.sender = ntohs(tcp.sender);
                    if (tcp.sender != SrcPort) return false;   }
                else if (ip.proto == 17)    {
                    memcpy(&udp,&buff[(ip.ver_len&0x0f) * 4],sizeof(udp));
                    udp.sender = ntohs(udp.sender);
                    if (udp.sender != SrcPort) return false;   }    } return true;  }
```

Модуль для ПНА

```
#include <vcl.h>
#pragma hdrstop
#include "Unit1.h"
#include <Math.hpp>
#include <math.h>
#include "UAdaptCase.h"
#include "USniffThrd.h"
#pragma package(smart_init)
#pragma link "trayicon"
#pragma resource "*.dfm"
TForm1 *Form1;
int stat[250][150],  aport[250], buf[2][250], sn, d, m06=0, m07=0, m08=0,
m09=0, m10=0, n, k, res;
double kxp[10], snal[250][150], m1[10], kx[10][10], km[10][10], tm[10][10],
nch[2][5], kvk[20][10], max, max1, nch1;
bool mnz=false;
AnsiString id,id1;
TSniffThrd *Thrd;
u_long LocalAddrs[10];
u_long LocalMasks[10];
__int64 LocalMACs[10];
HINSTANCE iphlpapi_dll;
DWORD (__stdcall * GetAdaptersInfo)(PIP_ADAPTER_INFO pAdapterInfo,
PULONG pOutBufLen);
__fastcall TForm1::TForm1(TComponent* Owner)
      : TForm(Owner) {    }
void __fastcall TForm1::GetRes()
{   int n,k=0, i, j;
  for (i=0; i<250; i++)
    for (j=0; j<150; j++)
    {      snal[i][j]=-1;     }
  m06=0;   m07=0;   m08=0;   m09=0;   m10=0;
  for (i=0; i<250; i++)
    for (j=0; j<150; j++)
    {      if (stat[i][j] != -1)       {
      if ((stat[i][j]/max >= 0) && (stat[i][j]/max <= kx[0][0]) || ((stat[i][j]/max
>kx[2][2]) && (stat[i][j]/max <= 1)))
      {          snal[i][j]=1;          k+=1;        }
      if ((stat[i][j]/max > kx[0][0]) && (stat[i][j]/max <= kxp[0]))
      {  snal[i][j]=(Floor(0.5+0.0000001+10*(km[0][0]+(((km[0][1]-km[0]
[0])*((stat[i][j]/max)-kx[0][0]))/(kx[0][1]-kx[0][0])))))*0.1;  k+=1; } } }
   for (i=0; i<250; i++)
    for (j=0; j<150; j++)
    {  if (snal[i][j] == 0.6)       m06+=1; if (snal[i][j] >= 0.7 && snal[i][j] < 0.8)
      m07+=1; if (snal[i][j] == 0.8)   m08+=1;  if (snal[i][j] == 0.9)  m09+=1;
```

```
            if (snal[i][j] == 1)  m10+=1;  }
          n=0;  if (m06 != 0)  {  nch[0][n]=0.6; nch[1][n]=m06; n+=1;  }
          if (m07 != 0)
          {  nch[0][n]=0.7;  nch[1][n]=m07/max1;  n+=1;   }
          if (m08 != 0)
          {  nch[0][n]=0.8;  nch[1][n]=m08/max1; n+=1;   }
          if (m09 != 0)
          {   nch[0][n]=0.9;  nch[1][n]=m09/max1;  n+=1;   }
          if (m10 != 0)
          { nch[0][n]=1;  nch[1][n]=m10/max1;  n+=1;       }
          for (;n<5;n++)
          {  nch[0][n]=-1;   nch[1][n]=-1;     }
          for (i=0;i<5;i++)
          {  if (nch[0][i] == 1)  {  nch1=nch[1][i];  break;   }  }
          if (m1[0]>nch1)  {  res=0;    }   else
          { for (i=0;i<9;i++)
            {       if (m1[i+1]!=-1)     {  if (m1[i+1]-nch1>=0 && nch1-
m1[i]<=m1[i+1]-nch1)
               {  res=i;  break;    }  else    {  if (i==9)  res=10;   }  } else
             {   res=i;  break;  }  }  }  Alarm(res);   }
        void __fastcall TForm1::Alarm(int res)
        {  if (res < 2)   { Edit1->Font->Color=clGreen; TrayIcon1->Animate=false;  }
          else   { TrayIcon1->Animate=true;  if (mnz == true)  TrayIcon1-
>Restore();  }
          if (CheckBox1->Checked)
          { if (res == 0)  Edit1->Text="Низька";  if (res == 1)  Edit1->Text="Більше
низька, ніж вАСока";   }
          else   {   if (res == 0)   Edit1->Text="";  if (res == 1)  Edit1->Text="";  }
          if (res == 2)
          { Edit1->Text="Більше вАСока, ніж низька";  Edit1->Font-
>Color=0x000045FF;  }
          if (res == 3 || res == 4)
          { Edit1->Text="ВАСока";  Edit1->Font->Color=clRed; }  }
        void __fastcall TForm1::FormCreate(TObject *Sender)
        { sn=0;  int i, j;  for (i=0; i<250; i++)
          { buf[0][i]=-1; buf[1][i]=-1;  aport[i]=-1;
         for (j=0; j<150; j++)    stat[i][j]=-1;   }
          d=18;   Timer1->Interval=10;   Timer2->Interval=10;
          WORD vers;
          WSADATA WSAData;

            {       for (j=0; j<10; j++)       {
               tm[ADOQuery1->RecNo-1][j]=ADOQuery1->Fields-
>FieldByNumber(j+3)->AsFloat;       }
            ADOQuery1->Next();     n+=1;          }
```

```
            for(i=n; i<20; i++)
            {       for (j=0; j<10; j++)       {       tm[i][j]=-1;     }      }
            ADOQuery1->Close();
            ADOQuery1->SQL->Clear();
            ADOQuery1->SQL->Add("SELECT * FROM result WHERE
lz_id="+id1+" ORDER BY id");
            ADOQuery1->Open();
            ADOQuery1->First();
            n=0;   while (!ADOQuery1->Eof)     {
              for (j=0; j<10; j++)
              {   kvk[ADOQuery1->RecNo-1][j]=ADOQuery1->Fields-
>FieldByNumber(j+3)->AsFloat;    }
              ADOQuery1->Next();   n+=1;   }
            for(i=n; i<20; i++)
            {     for (j=0; j<10; j++)      {         kvk[i][j]=-1;       }     }     k=0;
            for(i=0; i<n; i+=2)
            {for (j=0; j<10; j++) {if (kvk[i][j] == 1) {m1[k]=kvk[i+1][j];  k+=1; } } }
            for (i=k; i<10; i++)
              m1[i]=-1;
            for (i=1; i<20; i=i+2)
            {   n=0;
          for (j=1; j<10; j++)
              {     if (tm[i][j] != -1) { if (tm[i][j] != tm[i][j-1])  {
                    kx[(i-1)/2][n]=tm[i][j-1];  km[(i-1)/2][n]=tm[i-1][j-1];  n+=1; } } else
                { kx[(i-1)/2][n]=tm[i][j-1]; km[(i-1)/2][n]=tm[i-1][j-2]; break; } }
              ADOQuery1->Next(); }
        kxp[0]=(((km[0][1]-km[0][0])/(kx[0][1]-kx[0][0]))*kx[0][0]-((km[1][1]-km[1]
[0])/(kx[1][1]-kx[1][0]))*kx[1][0]+km[1][0]-km[0][0])/(((km[0][1]-km[0][0])/(kx[0]
[1]-kx[0][0])) - ((km[1][1]-km[1][0])/(kx[1][1]-kx[1][0])));
        kxp[1]=(((km[1][2]-km[1][1])/(kx[1][2]-kx[1][1]))*kx[1][1]-((km[2][2]-km[2]
[1])/(kx[2][2]-kx[2][1]))*kx[2][1]+km[2][1]-km[1][1])/(((km[1][2]-km[1][1])/(kx[1]
[2]-kx[1][1])) - ((km[2][2]-km[2][1])/(kx[2][2]-kx[2][1])));  }
```